



Common Criteria Configuration Guidance

Network Device Collaboration Protection Profile

Target of Evaluation: Aruba 2930F, 2930M, 3810M and 5400R Switch Series

Version 1.7
November 30, 2022

Table of Contents

1 Introduction.....	5
Purpose	5
Intended Audience.....	5
Evaluated Configuration.....	5
Assumptions.....	6
2 Delivery and Operation	7
Secure Delivery.....	7
Installation and Configuration.....	7
Console Ports	7
Reset and Clear Buttons	8
Management Console	9
USB Console Port Driver Download	9
USB Console Port and RJ-45 Console Port Interaction.....	9
Configuring the Management Console Connection	10
Setting up a Console Connection	10
3 Setting up Common Criteria Configuration	11
Prerequisites	11
Use of the CLI	11
Use of the Menu.....	11
Updating Switch Software	12
Updating Switch Software via USB.....	12
Downloading Switch Software using USB (CLI Only).....	13
Downloading Switch Software from SFTP Server.....	13
Rebooting the Switch	14
Software Signing and Verification.....	14
Flash Verification.....	14
Running Version Verification	15
Signature Verification.....	15
Enabling Enhanced secure mode	15
Network Configuration	16
Configuring an IP Address and Subnet Mask	16
Creating a Secure Management VLAN	22
Date and Time Configuration	23
Updating Date and Time Manually	23
Management Interfaces.....	24
Web UI.....	24
Using HTTPS secure connection	25
Console.....	26
SSH	27

Trust Anchors and Credentials for Syslog.....	31
Creating a Trusted Channel with a Remote Syslog Server	32
TLS	33
User, Password, and Session Management	39
General password rules:.....	39
Password minimum length.....	40
User Based Lockout Delay	40
Protecting Credentials.....	41
Configuring Login Banner.....	43
Configuring Session Timeouts	44
Finalizing Configuration.....	44
Disabling Services Not Under Evaluation	44
Booting to Evaluated Configuration.....	45
Audit Functionality.....	45
Accessing Audit Logs	45
Audit log format	47
List of Auditable Events (CC Required).....	48
Local Command Audit log	56
Enable Command logging.....	56
Display Commands logged	56
Clear command log	57
Self Tests	57
4 Documentation References.....	59
Aruba Switch Series Documentation References.....	59
Technical support.....	59

TABLE OF TABLES and FIGURES

Table 1- Evaluated Configuration.....	5
Table 2 - Assumptions	6
Table 3- Reset and Clear Buttons	8
Table 4 - X509v3 Validation.....	39
Table 5 - Audit Log Entry Items	48
Table 6 - Security Functional Requirements and Auditable Events	48
Table 7 - Self Tests.....	58

Figure 1 - Main Menu.....	12
Figure 2 - Example output of the "show flash" command	14
Figure 3- Example output of the "show version" command.....	15
Figure 4 - VLAN Names menu	18
Figure 5- VLAN name entry screen.....	18
Figure 6 - VLAN names menu with configured VLAN.....	19
Figure 7 - IP Configuration menu	19
Figure 8- IP Configuration menu with Default Gateway set	20
Figure 9 - IP Configuration menu with default VLAN disabled.....	20
Figure 10 - IP Configuration menu with Manual configuration for Management VLAN	21
Figure 11 - IP Configuration menu with configured IP	21
Figure 12 - Configured IP Configuration menu	22
Figure 13 - Traditional UI.....	25
Figure 14 - Warning When Running Command "Encrypt Credentials"	41
Figure 15 - Compatibility Warning When Running Command "include-credentials"	42
Figure 16 - Security Warning When Running Command "include-credentials".....	42
Figure 17 - Default Login Banner.....	43
Figure 18 - Configured message of the Day Banner.....	44
Figure 19 - Configured Exec Banner with Previous Login Message	44
Figure 20 - Sample Log	47
Figure 21- Audit Log Entry Format	47

1 Introduction

Purpose

This document serves as a supplement to the official Aruba User Documentation, consolidating configuration information specific to the Common Criteria Network Device collaborative Protection Profile (NDcPP). 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 evaluate 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 2930F, 2930M, 3810M and 5400R Switch Series running version 16.08, which was evaluated under version 2.1 of the NDcPP. Customers are advised to use the newest available 16.08 release in order to take advantage of defect fixes, which may include fixes for security vulnerabilities.

The evaluated configuration consists of the following Aruba Switch Series:

TABLE 1- EVALUATED CONFIGURATION

Series Identifier	Hardware Models
Aruba 2930F Switch Series	2930F 24G 4SFP+ Switch (JL253A) 2930F 48G 4SFP+ Switch (JL254A) 2930F 24G PoE+ 4SFP+ Switch (JL255A) 2930F 48G PoE+ 4SFP+ Switch (JL256A) 2930F 8G PoE+ 2SFP+ Switch (JL258A) 2930F 24G 4SFP Switch (JL259A) 2930F 48G 4SFP Switch (JL260A) 2930F 24G PoE+ 4SFP Switch (JL261A) 2930F 48G PoE+ 4SFP Switch (JL262A) 2930F 24G PoE+ 4SFP+ Switch (JL263A) 2930F 48G PoE+ 4SFP+ Switch (JL264A) 2930F 48G PoE+ 4SFP 740W Switch (JL557A) 2930F 48G PoE+ 4SFP+ 740W Switch (JL558A) 2930F 48G PoE+ 4SFP+ 740W Switch (JL559A)
Aruba 2930M Switch Series	2930M 24G 1-slot Switch (JL319A) 2930M 24G PoE+ 1-slot Switch (JL320A) 2930M 48G 1-slot Switch (JL321A) 2930M 48G PoE+ 1-slot Switch (JL322A) 2930M 40 Port 1G + 8 Port SmartRate PoE+ (JL323A) 2930M 24 Port SmartRate PoE+ (JL324A)

Series Identifier	Hardware Models
	2930M 40G 8 HPE Smart Rate PoE Class 6 1-slot Switch (ROM67A) 2930M 24 HPE Smart Rate PoE Class 6 1-slot Switch (ROM68A)
Aruba 3810M Switch Series	3810M 24G 1-slot Switch (JL071A) 3810M 48G 1-slot Switch (JL072A) 3810M 24G PoE+ 1-slot Switch (JL073A) 3810M 48G PoE+ 1-slot Switch (JL074A) 3810M 16SFP+ 2-slot Switch (JL075A) 3810M 40G 8 HPE Smart Rate PoE+ 1-slot Switch (JL076A)
Aruba 5400R Switch Series	5406R z12 Switch (J9821A) 5412R z12 Switch (J9822A) 5406R/5412R-24-port 10/100/1000Base-T PoE+ MACsec (No PSU) v3 z12 Card (J9986A) 5406R/5412R-24p 1000BASE-T (No PSU) v3 z12 Card (J9987A) 5406R/5412R-24p SFP (No PSU) v3 z12 Card (J9988A) 5406R/5412R-12p PoE+ / 12p 1GbE SFP (No PSU) v3 z12 Card (J9989A) 5406R/5412R-20p PoE+ / 4p SFP+ (No PSU) v3 z12 Card (J9990A) 5406R/5412R-20p PoE+ / 4p 1/25/5/XGT PoE+ (No PSU) v3 z12 Card (J9991A) 5406R/5412R-20p PoE+ / 1p 40GbE QSFP+ (No PSU) v3 z12 Card (J9992A) 5406R/5412R-8p 1G/10GbE SFP+ v3 (No PSU) v3 z12 Card (J9993A) 5406R/5412R-2-port 40GbE QSFP+ (No PSU) v3 z12 Card (J9996A)

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 2 - 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 Delivery and Operation

Secure Delivery

To ensure no one has tampered with the goods during delivery, inspect the Networking switch physical package and check as follows:

1. Outer Package Inspection

- 1) Check that the outer carton is in good condition.
- 2) Check the package for an HPE Quality Seal or IPQC Seal, and ensure that it is intact.
- 3) Check that the IPQC seal on the plastic bag inside the carton is intact.
- 4) If any check failed, the goods shall be treated as dead-on-arrival (DOA) goods.

2. Packing List Verification

Check against the packing list for any possible discrepancy in material type and quantity. If any discrepancy is found, the goods shall be treated as DOA goods.

3. External Visual Inspection

Inspect the cabinet or chassis for any defects, loose connections, damages, and/or illegible marks. If any surface defect or material shortage is found, the goods shall be treated as DOA goods.

4. Confirm Software/firmware

- 1) Version verification

To verify the software version, start the networking device, view the self-test result during startup, and use the **show version** command to check the software version. If software loading failed or the version information is incorrect, please contact HPE for support.

- 2) RSA with SHA-256 verification

To verify that software/firmware has not been tampered with, run **verify signature flash <primary/secondary>** on the networking device. The command will return a pass or fail message.

5. DOA (Dead on Arrival)

If the package is damaged, any label/seal is incorrect or tampered with, stop unpacking the goods, retain the package, and report to HPE for further investigation. The damaged goods will be replaced if necessary.

Installation and Configuration

Console Ports

There are two serial console port options on the switch, an RJ-45 or Micro USB. These ports are used to connect a console to the switch either by using the RJ-45 serial cable supplied with the switch, or a standard Micro USB cable (not supplied). The Micro USB connector has precedence for input. If both cables are plugged in, the console output is echoed to both the RJ-45 and the Micro-USB ports, but the input is only accepted from the

Micro-USB port. For more information about the console connection, see “Connect a management console” in Chapter 2 of “Installing the Switch” of the “Switch Series Installation and Getting Started Guide”.

Reset and Clear Buttons

The Reset and Clear buttons are recessed from the front panel (to protect them from being pushed accidentally) and are accessible through small holes on the top of the front panel. Use pointed objects, such as unbent paper clips, to push them.

The Reset and Clear buttons are used singly or in combination, as follows:

TABLE 3- RESET AND CLEAR BUTTONS

To accomplish this:	Do this:	This will happen:
Soft Reset	Press and release the Reset button	The switch operating system is cleared gracefully (such as data transfer completion, temporary error conditions are cleared), then reboots and runs self tests.
Hard Reset	Press and hold the Reset button for more than 5 seconds (until all LEDs turn on), then release.	The switch reboots, similar to a power cycle. A hard reset is used, for example, when the switch CPU is in an unknown state or not responding.
Delete console and management access passwords	Press Clear button for more than 5 seconds, but within 15 seconds (in between 5 – 15 seconds)	Clears all passwords. Will flash Global Status Green LED, after 5 seconds has expired to indicate passwords have cleared.
Turn off UID LED	Press Clear button and release within 5 seconds (in between 0.5 – 5 seconds)	Clears the UID LED
Restore the factory default configuration	<ol style="list-style-type: none"> 1. Press Clear and Reset simultaneously. 2. While continuing to press Clear, release Reset. 3. When the Global Status LED begins to fast flash orange (after approximately 5 seconds), release Clear. 	The switch removes all configuration changes, restores the factory default configuration, and runs self test.
<p>Note: These buttons are provided for your convenience. If you are concerned with switch security, make sure that the switch is installed in a secure location, such as a locked wiring closet. You can also disable these buttons by using the front-panel-security command.</p>		

WARNING

The clear button is provided for user convenience. **Do not use the clear button unless you wish to return to the switch to its factory default configuration. Using the clear button will take the switch out of evaluated configuration.**

Management Console

The switch has a full-featured, easy to use console interface for performing switch management tasks including:

- Monitor switch and port status and observe network activity statistics
- Modify the switch's configuration to optimize switch performance, enhance network traffic control, and improve network security
- Read the event log and access diagnostic tools to help in troubleshooting
- Download new software to the switch
- Add passwords to control access to the switch from the console and network management stations (i.e., SSH).

To connect a console to the switch, use the RJ-45 console cable shipped with the switch. Alternatively, you can use a USB cable (not supplied) for a console connection. (See "USB Console Port Notes" below.) Connect a PC or VT-100 terminal to either of the Console ports. The connected PC or terminal then functions as a management console connected directly to the switch.

The switch can simultaneously support one out-of-band console session, through one of the console ports, and in-band Telnet console sessions. The console ports are used only for out-of-band management, not for Telnet sessions.

USB Console Port Driver Download

When using the Micro USB Console Port, the connected PC first requires "virtual COM port" USB drivers to be installed. USB drivers are available for Windows XP, Windows Vista, and Windows 7. The USB console drivers are available at www.hpe.com/networking/support. On the web, follow these steps:

1. Type a product name (e.g. 2930F) or product number in the Auto Search textbox.
2. Select one of the switches from the drop-down list.
3. Click the Display selected button.
4. From the options that appear, select Software downloads (on the right-hand side). Download the "USB Console Port Drivers and Information."

USB Console Port and RJ-45 Console Port Interaction

Note that you cannot use both the RJ-45 Console Port and USB Console Port at the same time. When the USB Console Port is connected to a live PC, it has priority over the RJ-45 Console Port. By default, the RJ-45 console port is active (accepts input). To activate the USB console port, connect it to a live PC. If the USB console session is closed by the inactivity timer, the RJ-45 console port becomes active again to allow remote access via a terminal server. To reactivate the USB console port, unplug it, then reconnect it to a live PC.

Configuring the Management Console Connection

To configure a console to manage the switch through the console port connection:

1. Configure the PC terminal emulator as a DEC VT-100 (ANSI) terminal, or use a VT-100 terminal.
2. Configure the terminal with the following settings:
 - a. A baud rate from 1200 to 115200 (the switch senses the speed)
 - b. 8 data bits, 1 stop bit, no parity, and flow control set to Xon/Xoff
 - c. For the Windows Terminal program, disable (uncheck) the “Use Function, Arrow, and Ctrl Keys for Windows” option.
 - d. For the Hilgraeve HyperTerminal program, select the “Terminal keys” option for the “Function, Arrow, and Ctrl Keys act as” parameter.
 - e. For Putty, set connection type to “Serial” and change “Serial Line” to the COM port associated with the serial connection.

If you use a management console with different configuration settings, be sure to reconfigure the settings on both the terminal and the switch in the following order so that both configurations are compatible:

1. Reconfigure the switch and save the new settings.
2. Reconfigure the terminal and save the new settings.
3. Reboot the switch and re-establish the console session

Setting up a Console Connection

To access the Switch through a Console port (out-of-band) connection, follow these steps:

1. Configure the management console as described above under Section: Configuring the management console connection.
2. For a direct console connection, connect the PC or terminal to the Console serial port using one of these console cables:
 - a. A DB9-to-RJ45 cable (shipped with the switch).
 - b. A micro-USB cable (not provided).
3. Power on the management console (terminal or PC). If you are using a PC, start the PC terminal program.
4. For a direct console connection through the Console port:
 - a. Press Enter two or three times to display the copyright page and the message
`Press any key to continue.`
 - b. Press any key to display the switch console command (CLI) prompt; for example:
`Aruba-Switch#`
 - c. Continue the console session to configure the switch by following the procedure in “Minimal Configuration through the Out-of-Band Console Connection”.

3 Setting up Common Criteria Configuration

In the factory default configuration, the switch has no IP (Internet Protocol) address and subnet mask, and no passwords. 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

Prerequisites

Use of the CLI

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

```
Aruba-Switch#
```

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

```
Aruba-Switch(config)#
```

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

```
Aruba-Switch#configure
```

Use of the Menu

The menu allows the configuration of some switch settings from a Graphical User Interface. The operator must issue the following command to enter the menu:

```
menu
```

If there are pending changes, the switch will prompt for confirmation to save the running configuration before entering the menu:

```
Do you want to save the current configuration (y/n?)
```

Press **[Y]** to save the current configuration. The Main Menu is then displayed:

```
Aruba-3810M-24G-1-slot                               19-Dec-2017   8:45:05
===== CONSOLE - MANAGER MODE =====
Main Menu

1. Status and Counters...
2. Switch Configuration...
3. Console Passwords...
4. Event Log
5. Command Line (CLI)
6. Reboot Switch
7. Download OS
8. Run Setup
9. Testmode...
0. Logout

Provides the menu to display configuration, status, and counters.

To select menu item, press item number, or highlight item and press <Enter>.
```

FIGURE 1 - MAIN MENU

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/>) to ensure the validated version of the product software is used.

Updating Switch Software via USB

The switch's USB port (labeled as Auxiliary Port) allows the use of a USB flash drive for copying files to and from the switch, given the following rules and prerequisites:

- Unformatted USB flash drives must first be formatted on a PC (Windows FAT format). For devices with multiple partitions, only the first partition is supported. Devices with secure partitions are not supported.
- If they already exist on the device, subdirectories are supported. When specifying a <filename>, you must enter either the individual file name (if at the root) or the full path name (For example, /subdir/filename).
- To view the contents of a USB flash drive, use the `dir` command. This lists all files and directories at the root. To view the contents of a directory, you must specify the subdirectory name (that is, `dir <subdirectory>`).
- The USB port supports connection to a single USB device. USB hubs to add more ports are not supported.

Some USB flash drives may not be supported on your switch. Consult the latest Release Notes for information on supported devices.

Downloading Switch Software using USB (CLI Only)

This procedure assumes that:

- A software version for the switch has been stored on a USB flash drive. (The latest software file is typically available from the Aruba website at <https://h10145.www1.hp.com/support/SupportLookUp.aspx>.)
- The USB device has been plugged into the switch's USB port.

Issue the following command to copy the switch image to secondary flash:

```
copy usb flash <filename> secondary
```

Example:

To copy a switch software file named KB_16_08_0001.swi from a USB device to secondary flash:

Execute the copy command:

```
Aruba-Switch# copy usb flash KB_16_08_0001.swi secondary
The Secondary OS Image will be deleted, continue [y/n]? y
```

When the switch finishes copying the software file from the USB device, it displays the progress message:

```
Validating and Writing System Software to FLASH...
```

When the CLI prompt re-appears, the switch is ready to reboot to activate the downloaded software. Remove the USB drive, as it is no longer needed.

Downloading Switch Software from SFTP Server

The image can be downloaded securely from SFTP server with the help of the following command:

To copy a switch software file named KB_16_08_0001.swi from a SFTP Server to secondary flash:

Execute the copy command:

```
Aruba-Switch(config)# copy sftp flash KB_16_08_0001.swi
secondary The Secondary OS Image will be deleted, continue
[y/n]? y
```

When the switch finishes copying the software file from the SFTP server, it displays the progress message:

```
Validating and Writing System Software to FLASH...
```

When the CLI prompt re-appears, the switch is ready to reboot to activate the downloaded software.

Rebooting the Switch

The switch must boot from the secondary flash to run the installed software update. Issue the following command to reboot the switch:

```
Aruba-Switch(config)# boot system flash secondary
```

The switch will prompt for confirmation:

Press **[Y]** to reboot. Once the switch boots, login as directed in Setting up a Console Connection.

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:

```
show flash
```

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:

NOTE: The switch must be in the Enhanced security mode for the 'Enh. Security Capable' and 'Signed to be displayed'.

```
Aruba-3810M-24G-1-slot# show flash
Image                Size (bytes) Date      Version      Attributes
-----
Primary Image       :   33111135 12/14/17 KB.16.04.0011J  Enh. Security Capable
Secondary Image     :   33111706 12/15/17 KB.16.04.0011K  Enh. Security Capable

Boot ROM Version
-----
Primary Boot ROM Version : KB.16.01.0009, Signed
Secondary Boot ROM Version : KB.16.01.0009, Signed

Default Boot Image   : Secondary
Default Boot ROM     : Primary

Aruba-3810M-24G-1-slot#
```

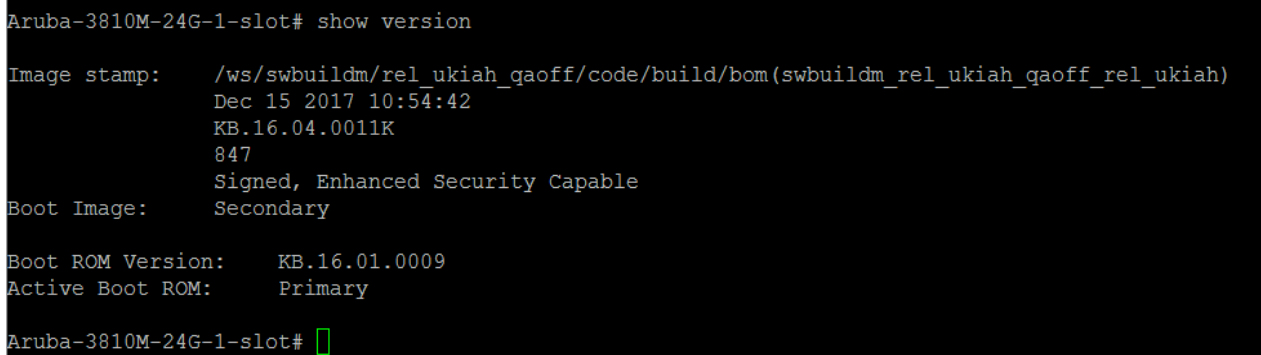
FIGURE 2 - EXAMPLE OUTPUT OF THE "SHOW FLASH" COMMAND

Verify that the version number for the **Secondary Image** matches the version installed. The version displayed should be KB_16_08_0001 for file KB_16_08_0001.swi.

Running Version Verification

Issue the following command to verify the version of the software currently running on the switch:

```
Aruba-Switch# show version
```

A screenshot of a terminal window showing the output of the 'show version' command on an Aruba switch. The output includes the image stamp (Dec 15 2017 10:54:42, KB.16.04.0011K, 847, Signed, Enhanced Security Capable), the boot image (Secondary), the boot ROM version (KB.16.01.0009), and the active boot ROM (Primary).

```
Aruba-3810M-24G-1-slot# show version
Image stamp:    /ws/swbuildm/rel_ukiah_gaoff/code/build/bom(swbuildm_rel_ukiah_gaoff_rel_ukiah)
                Dec 15 2017 10:54:42
                KB.16.04.0011K
                847
                Signed, Enhanced Security Capable
Boot Image:     Secondary
Boot ROM Version:  KB.16.01.0009
Active Boot ROM:  Primary
Aruba-3810M-24G-1-slot# █
```

FIGURE 3- EXAMPLE OUTPUT OF THE "SHOW VERSION" COMMAND

Confirm that the version displayed matches the version installed, as indicated by the `show flash` command. The version displayed should be KB.16_08_0001 for file KB_16_08_0001.swi.

Signature Verification

The signature will be verified when a software is downloaded into the switch, if the signature verification fails, error will be displayed and the software download will be unsuccessful.

Also, there is a command to verify that the images in flash are with valid signature:

Issue the following command to verify the digital signature of the software installed:

```
Aruba-Switch(config)# verify signature flash secondary
```

If the signature is valid, the switch will display the following method:

```
Signature is valid.
```

Because signature validation is processor intensive, the switch may appear to hang for up to 30 seconds during the execution of this command.

Enabling Enhanced secure mode

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

NOTE: The switch should not have stacking enabled and user should be logged to commander to execute 'secure-mode enhanced'.

Issue the following command to enable Enhanced secure mode:

```
secure-mode enhanced
```

Prior to enabling Enhanced secure mode, the switch will issue a warning:

```
The system will be rebooted and all management module files except
software images will be erased and zeroized. This will take up to 60
minutes and the switch will not be usable during that time. A power-
cycle will then be required to complete the transition.
```

```
Continue (y/n)?
```

Press **[Y]** to enable Enhanced secure mode. The switch will erase and zeroize all stored passwords, certificates, and keys. The switch configuration will be reset to the factory default.

Once zeroization is complete, the switch will reboot. Once the reboot is complete, proceed to the next section.

Network Configuration

By default, the switch is configured to automatically receive IP addressing on the default VLAN from a DHCP/BOOTP 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:

- Creating a VLAN
- Assigning IP addresses
- Assigning a default gateway
- Disabling OOBM access and unused connections
- Establishing a Secure Management VLAN

Configuring an IP Address and Subnet Mask

Changing the IP Configuration via CLI

To comply with the evaluated configuration, the user must assign the switch a static IP address on a non-default VLAN.

NOTE: The following command includes both the IP address and the subnet mask. You must either include the ID of the VLAN for which you are configuring IP addressing or go to the context configuration level for that VLAN.

Execute the following command to configure an IP address:

```
Aruba-Switch(config)# vlan 200 ip address <ip-address/mask-length>
```


Or

```
Aruba-Switch(config)# vlan 200 ip address <ip-address> <mask-bits>
```

The IP address and subnet mask must be compatible with the test network.

Example:

To assign an IP address of 192.168.1.2 issue the following command:

```
Aruba-Switch(config)# vlan 200 ip address 192.168.1.10 255.255.255.0
```

This example configures the same IP address as the preceding example, but specifies the subnet mask by mask length:

```
Aruba-Switch(config)# vlan 200 ip address 192.186.1.10/24
```

Next, the default VLAN must be disabled to ensure it does not gain an IP address. Issue the following command to disable the default VLAN:

```
no vlan 1 ip address
```

Finally, the user must assign a default gateway to allow the switch to communicate with servers on the network. Issue the following command to establish a default gateway:

```
ip default-gateway <ip-address>
```

Example:

To assign a default gateway of 192.168.1.1, enter:

```
Aruba-Switch(config)# ip default-gateway 192.168.1.1
```

Changing the IP Configuration via Menu

From the Main Menu, select **2.Switch Configuration...** then **8.VLAN Menu...** then **2. VLAN Names.**

```

Aruba-3810M-24G-1-slot                               19-Dec-2017  9:07:05
=====-- CONSOLE - MANAGER MODE -----
                Switch Configuration - VLAN - VLAN Names

802.1Q VLAN ID          Name
-----
1                        DEFAULT VLAN

Actions->  Back      Add      Edit      Delete      Help
Return to previous screen.

Use up/down arrow keys to change record selection, left/right arrow keys to
change action selection, and <Enter> to execute action.

```

FIGURE 4 - VLAN NAMES MENU

Press **[A]** to add a new VLAN. The VLAN name entry screen is displayed:

```

Aruba-3810M-24G-1-slot                               19-Dec-2017  9:11:24
=====-- CONSOLE - MANAGER MODE -----
                Switch Configuration - VLAN - VLAN Names

802.1Q VLAN ID : 1
Name :

Actions->  Cancel      Edit      Save      Help
Enter VLAN ID - 1..4094

Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.

```

FIGURE 5- VLAN NAME ENTRY SCREEN

Enter a VLAN ID of 200. Press **[Tab]** to highlight the Name field and enter the name "Management". Press **[Enter]** to confirm and **[S]** to save. The switch will return to the VLAN Names menu:

```

Aruba-3810M-24G-1-slot                               19-Dec-2017   9:12:56
=====-- CONSOLE - MANAGER MODE -----=====
                Switch Configuration - VLAN - VLAN Names

802.1Q VLAN ID          Name
-----
1                       DEFAULT VLAN
200                     Management

Actions->   Back   Add   Edit   Delete   Help
Add a new record.

Use up/down arrow keys to change record selection, left/right arrow keys to
change action selection, and <Enter> to execute action.

```

FIGURE 6 - VLAN NAMES MENU WITH CONFIGURED VLAN

Press **[B]** to go back, then select 4. **Return to Previous Menu...**, then 5. **IP Configuration**. The IP configuration menu is displayed.

```

Aruba-3810M-24G-1-slot                               19-Dec-2017   9:14:50
=====-- CONSOLE - MANAGER MODE -----=====
                Switch Configuration - Internet (IP) Service

IP Routing : Disabled

Default Gateway :
Default TTL    : 64
Arp Age       : 20

          VLAN          IP Config    IP Address    Subnet Mask
-----+-----
DEFAULT VLAN | DHCP/Bootp
Management  | Disabled
            | DHCP/Bootp

Actions->   Cancel   Edit   Save   Help
Edit the fields displayed above.

Use arrow keys to change action selection and <Enter> to execute action.

```

FIGURE 7 - IP CONFIGURATION MENU

Press **[E]** to edit the configuration. The first field selected will be the **Default Gateway**. Enter the IP address of the default gateway on the network. The example uses IP addresses in the 192.168.1.xxx range.

```

Aruba-3810M-24G-1-slot                               19-Dec-2017   9:16:25
=====-- CONSOLE - MANAGER MODE -----
                Switch Configuration - Internet (IP) Service

IP Routing : Disabled

Default Gateway : 192.168.1.1
Default TTL     : 64
Arp Age        : 20

          VLAN          IP Config      IP Address      Subnet Mask
-----+-----
DEFAULT_VLAN | DHCP/Bootp
Management  | Disabled
            | DHCP/Bootp

Actions->  Cancel  Edit  Save  Help
Enter the IP address of the default gateway.

Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.

```

FIGURE 8- IP CONFIGURATION MENU WITH DEFAULT GATEWAY SET

Press **[Tab]** three times to highlight IP Config field (reading DHCP/Bootp) in the DEFAULT_VLAN row. Press **[Space]** until the field displays Disabled.

```

Aruba-3810M-24G-1-slot                               19-Dec-2017   9:18:14
=====-- CONSOLE - MANAGER MODE -----
                Switch Configuration - Internet (IP) Service

IP Routing : Disabled

Default Gateway : 192.168.1.1
Default TTL     : 64
Arp Age        : 20

          VLAN          IP Config      IP Address      Subnet Mask
-----+-----
DEFAULT_VLAN | Disabled
Management  | Disabled
            | DHCP/Bootp

Actions->  Cancel  Edit  Save  Help
Select the method to enable IP access for switch management.

Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.

```

FIGURE 9 - IP CONFIGURATION MENU WITH DEFAULT VLAN DISABLED

Press **[Tab]** to highlight the IP Config field in the Management row. Press **[Space]** until the field displays Manual.

```

Aruba-3810M-24G-1-slot                               19-Dec-2017  9:19:36
=====-- CONSOLE - MANAGER MODE -----=====
                Switch Configuration - Internet (IP) Service

IP Routing : Disabled

Default Gateway : 192.168.1.1
Default TTL    : 64
Arp Age       : 20

-----+-----+-----+-----
      VLAN      | IP Config | IP Address | Subnet Mask |
-----+-----+-----+-----
DEFAULT_VLAN   | Disabled |             |              |
Management     | Manual  |             |              |
                | DHCP/Bootp |             |              |

Actions->  Cancel  Edit   Save   Help
Select the method to enable IP access for switch management.

Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.

```

FIGURE 10 - IP CONFIGURATION MENU WITH MANUAL CONFIGURATION FOR MANAGEMENT VLAN

Press **[Tab]** to highlight the IP Address field. Enter an IP address compatible with the test network. This example uses IP addresses in the 192.168.1.xxx range. When finished, press **[Tab]** to highlight the Subnet Mask field. Enter the IP address’s accompanying subnet mask. CIDR notation is **not** supported.

```

Aruba-3810M-24G-1-slot                               19-Dec-2017  9:20:55
=====-- CONSOLE - MANAGER MODE -----=====
                Switch Configuration - Internet (IP) Service

IP Routing : Disabled

Default Gateway : 192.168.1.1
Default TTL    : 64
Arp Age       : 20

-----+-----+-----+-----
      VLAN      | IP Config | IP Address | Subnet Mask |
-----+-----+-----+-----
DEFAULT_VLAN   | Disabled |             |              |
Management     | Manual  | 192.168.1.10 | 255.255.255.0 |
                | DHCP/Bootp |             |              |

Actions->  Cancel  Edit   Save   Help
Enter the subnet mask for the IP network.

Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.

```

FIGURE 11 - IP CONFIGURATION MENU WITH CONFIGURED IP

Press **[Tab]** to select the Management VLAN's secondary IP Config field (reading DHCP/Bootp). Press **[Space]** until the field displays Disabled.

```

Aruba-3810M-24G-1-slot                               19-Dec-2017   9:22:02
=====-- CONSOLE - MANAGER MODE -----
                Switch Configuration - Internet (IP) Service

IP Routing : Disabled

Default Gateway : 192.168.1.1
Default TTL     : 64
Arp Age        : 20

      VLAN          IP Config    IP Address    Subnet Mask
-----+-----
DEFAULT_VLAN      | Disabled
Management        | Manual      192.168.1.10  255.255.255.0
                  | Disabled

Actions->  Cancel  Edit  Save  Help
Edit the fields displayed above.

Use arrow keys to change action selection and <Enter> to execute action.

```

FIGURE 12 - CONFIGURED IP CONFIGURATION MENU

When finished, press **[Enter]** to confirm, then **[S]** to save.

Finally, select 0. **Return to Main Menu...**, then 5. **Command Line (CLI)** to return to the CLI.

Creating a Secure Management VLAN

This feature creates an isolated network for managing the Aruba Switches that offer this feature. When a secure management VLAN is enabled, switch access is restricted to ports configured as members of the VLAN.

Before creating the management VLAN, the Out-Of-Band Management (OOBM) port must first be disabled. Issue the following command to disable the OOBM port:

```
Aruba-Switch(config)# oobm disable
```

Next, issue the following command to create the management VLAN.

```
Aruba-Switch(config)# management-vlan 200
```

Connect a network cable to port 1 on the switch. The operator must ensure that the switch does not have any network connections other than port 1.

Issue the following commands to add port 1 to the management VLAN:

```
Aruba-Switch(config)# vlan 200 untagged 1
```

The switch is now connected to the network.

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 using a manual adjustment.

Updating Date and Time Manually

If needed, issue the following command to manually set the date and time on the switch:

```
time hh:mm MM/DD/YYYY
```

hh	Hours
mm	Minutes
MM	Month (1 – 12)
DD	Day (1 – 31)
YYYY	Year (e.g., 2016)

NOTE: The CLI uses a 24-hour clock scheme; that is, hour (hh) values from 1 p.m. to midnight are input as 13 - 24, respectively.

Example:

To set the switch to 9:45 a.m. on November 17, 2016:

```
Aruba-Switch(config)# time 9:45 11/17/2016
```

NOTE: Warm booting or power-cycling the switch will reset the date and time to their default values unless a time synchronization service is configured.

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:

```
time timezone <minutes>
```

Where <minutes> is the number of **minutes** +/- UTC. The programmed time zone must match the time zone for the locality in which the switch resides during testing.

Example:

To configure the switch for Eastern Standard Time (UTC-5:00), issue the following command:

```
Aruba-Switch(config)# time timezone -300
```

For India Standard Time (UTC+5:30), issue the following command:

```
Aruba-Switch(config)# time timezone 330
```

For Greenwich Mean Time (UTC+0:00), issue the following command:

```
Aruba-Switch(config)# time timezone 0
```

Management Interfaces

The user can login to the switch different management interfaces like SSH, WebUI, Console. User should restart the session when the session gets disconnected unintentionally.

Web UI

Management and configuration of Aruba-OS Switch can occur through a web interface. Two interfaces are available, the Legacy UI and the Next Generation UI.

The Legacy UI provides full functionality for the monitoring and configuration of switches running ArubaOS.

The Next Generation UI provides a subset of the Legacy UI functionality. Additional functionality will be added in future releases and it will eventually replace the Legacy UI.

Accessing the Aruba-OS Switch Web UI

To log into the web management UI, open a browser and enter an IP address configured on the switch. For example, <https://X.X.X.X>

IP addresses are configured on the switch by the VLAN. Use show ip command to view the configured IP addresses.

Accessing the Aruba-OS Switch Next Generation UI

Access the Aruba-OS Switch Improved UI by clicking the Access Improved GUI link displayed in the upper right corner of the Traditional UI.

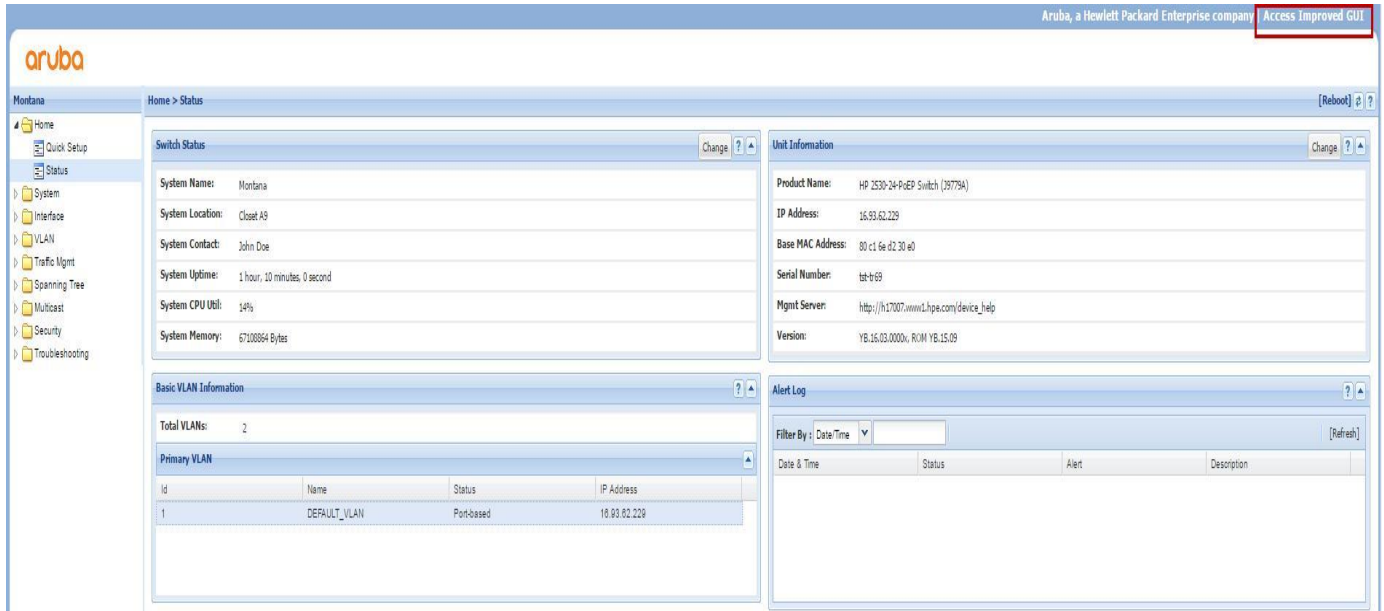


FIGURE 13 - TRADITIONAL UI

Using HTTPS secure connection

To secure connections to the web management UI, it is required in the evaluated configuration to enable HTTPS and disable HTTP access to the switch. HTTPS is HTTP traffic running on a Secure Sockets Layer (SSL) / Transport Layer Security (TLS) connection, which requires a certificate to be present on the switch. The user can login to the session by providing the proper credentials and can logout by pressing the logout button on WebUI interface.

To negotiate either RSA or ECDHE cipher suites, the admin should ensure that the TLS web server has an RSA authentication certificate and to negotiate ECDHE cipher suites, ensure that the TLS web server has an ECDSA authentication certificate.

To generate a certificate; enable HTTPS, and to disable HTTP, the steps are as follows:

Enter the configuration context using the command:

```
Aruba-Switch# configure
```

Create a self-signed SSL/TLS certificate.

```
Aruba-Switch(config)# crypto pki enroll-self-signed certificate-  
name <name of certificate> subject common-name <common name of  
device>
```

View the SSL/TLS certificate information.

```
Aruba-Switch(config)# show crypto pki local-certificate web-mgmt
```

The certificate details will be displayed.

To enable HTTPS web management:

```
Aruba-Switch(config)# web-management ssl
```

It is recommended to disable HTTP web management:

```
Aruba-Switch(config)# no web-management
```

Verify the web-management configuration:

```
Aruba-Switch(config)# show web-management
```

```
Web Management - Server Configuration
```

```
HTTP Access      : Disabled  
HTTPS Access     : Enabled  
SSL Port         : 443
```

Console

In the factory default configuration, the switch has no 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 a Manager and Operator username and passwords to control access privileges from the console and other management interfaces. After the username and passwords are configured, log off of the interface, access to the management interface requires entries of both the Manager or Operator user name and password. To log out from the session, the user should execute either the “exit” or “logout” command.

SSH

In the evaluated configuration, SSH is enabled by default. When in evaluated configuration, the switch supports data integrity validation through HMAC-SHA1 and key exchange method through diffie-hellman-group14-sha1.

The command “show ip ssh” can be used to view the current status of the SSH on the switch:

```
Aruba-Switch(config)# show ip ssh
SSH Enabled   : Yes           Secure Copy Enabled : No
TCP Port Number : 22         Timeout (sec)      : 120
Rekey Enabled  : No           Rekey Time (min)   : 60
                                   Rekey Volume (KB)   : 1048576
Host Key Type  : RSA          Host Key/Curve Size : 2048
```

If the SSH is not enabled, following are the steps to be followed to enable SSH.

Configuring the switch for client Public-Key SSH authentication

Prerequisites

Before you can use this option, you must do the following:

1. Create a key pair on an SSH client.
2. Copy the client's public key into a public-key file (which can contain up to 10 client public keys.)
3. Copy the public-key file into a TFTP or SFTP server accessible to the switch and download the file to the switch.

Procedure

1. Copy the public-key file into the switch.

```
copy tftp pub-key-file <ipv4-address|ipv6-address> <filename>
```

A specific client public-key also can be configured by below command.

```
ip ssh public-key < manager | operator > keystack
```

2. Configure the switch to authenticate a client public key at the login level with an optional secondary password method.

```
aaa authentication ssh login public-key
```

3. Configure a password method for the primary and secondary enable (manager) access. If an optional secondary method is not specified, it defaults to none.

```
aaa authentication ssh enable <local|tacacs|radius|public-key>
<local|none|authorized>
```

Generating a Public/Private Key Pair

To comply with the evaluated configuration as described in the Security Target, keys must be generated with the following algorithm:

- RSA with a key size (modulus) of 2048 bits or greater.

Issue the following command to generate a public/private key pair using this algorithm.

```
Aruba-Switch(config)# crypto key generate ssh rsa bits 2048
```

The switch will display the following notice:

```
Installing a new key pair.  If the key/entropy cache is
depleted, this could take up to a minute.
```

When the key pair is successfully generated, the switch will display the following method:

```
The installation of a new key pair is successfully completed.
```

Enabling SSH

Prior to enabling SSH services, a public/private key pair must be generated. The operator must successfully complete the steps described in Section: Generating a Public/Private Key Pair before continuing.

If a public/private key pair was successfully generated, the switch is ready to enable SSH services. Issue the following command to enable SSH:

```
Aruba-Switch(config)#ip ssh
```

Disabling Unsupported Algorithms

In order to comply with the evaluated configuration, the switch must ensure that the following algorithms are used for SSH transport encryption:

- AES-CBC-128
- AES-CBC-256

To guarantee the use of the above algorithms, the following SSH transport encryption algorithms must be disabled:

- AES-CBC-192
- AES-CTR-192
- AES-CTR-256
- AES-CTR-128
- rijndael-cbc@ysator.liu.se

Issue the following commands to disable unsupported SSH transport algorithms.

```
no ip ssh cipher aes192-cbc
no ip ssh cipher aes128-ctr
no ip ssh cipher aes192-ctr
no ip ssh cipher aes256-ctr
no ip ssh cipher rijndael-cbc@ysator.liu.se
```

Securing File Transfers

For secure file transfer, issue the following command to disable TFTP and enable SFTP:

```
Aruba-Switch(config)# ip ssh filetransfer
```

The switch will respond with the following message:

```
TFTP and auto-TFTP are now disabled because they cannot be secured with
SSH.
```

```
TFTP can be re-enabled with the 'tftp' command.
```

SSH Rekey

Every SSH session uses a session key to encrypt and decrypt the packets between the SSH peers.

Session Re-Keying ensures that, when certain constraints are met, for example, “1GB of data has been encrypted” or “1 hour has passed since the connection establishment” or “65535 packets have been encrypted”, re-key is initiated. This will result in a new set of encryption and integrity keys to be exchanged between them. Once the re-key is complete, new keys will be used for further communication. This ensures that the same key is not used for a long duration and the security of the session increases.

Within a SSH connections the same session keys are used for a threshold of no longer than one hour, and no more than one gigabyte of transmitted data. After either of the thresholds are reached a rekey needs to be performed.

Following are set of commands related to rekey:

1. Issue ssh rekey

```
Aruba-Switch(config)# ip ssh rekey
```

2. Configure ssh rekey threshold time

```
Aruba-Switch(config)# ip ssh rekey time 20
```

3. Configure ssh rekey threshold volume

```
Aruba-Switch(config)# ip ssh rekey volume 2048
```

4. Show ip ssh output

```
Aruba-Switch(config)# show ip ssh
```

```
SSH Enabled           : Yes           Secure Copy Enabled  : No
TCP Port Number       : 22            Timeout (sec)       : 120
Rekey Enabled         : Yes           Rekey Time (min)    : 20
```

```
Host Key Type      : RSA
Rekey Volume (KB) : 2048
Host Key/Curve Size : 2048
```

```
Ciphers : aes256-cbc,aes128-cbc
MACs    : hmac-sha1-96,hmac-sha1
```

Ses	Type	Source IP	Port
1	console		
2	inactive		
3	inactive		
4	inactive		
5	inactive		
6	inactive		
7	inactive		

5. Show running-config output:

```
Aruba-Switch# show run
Running configuration:

; JL323A Configuration Editor; Created on release #WC.16.03.0000x
; Ver #0d:3b.ef.7c.5f.fc.6b.fb.9f.fc.f3.ff.37.ef:21

hostname "Aruba-2930M-40G-8SR-PoEP"
module 1 type jl323a
ip ssh rekey
ip ssh rekey time 20
ip ssh rekey volume 2048
snmp-server community "public" unrestricted
oobm
    ip address dhcp-bootp
    exit
vlan 1
    name "DEFAULT_VLAN"
    untagged 1-48
    ip address dhcp-bootp
    exit
```

6. Commands used to reset the thresholds to default:

```
no ip ssh rekey
no ip ssh rekey time
no ip ssh rekey volume
```

7. Command to log out of the SSH session:

```
logout
exit
```

Trust Anchors and Credentials for Syslog

The evaluated configuration requires the switch to establish a trusted channel over TLS between the switch and a syslog server. In order to use TLS to establish a trusted channel, the switch must first generate a certificate request that can be used to validate connections between the switch and an application server. This section will walk through the following steps:

- Generate a trust anchor and identity profile on the switch
- Generate a certificate signing request
- Generate keys and CA certificates.
- Install the signed certificate on the application server
- Install the signed certificate on the switch

The installation and generation of signed certificates requires the use of third-party software. It is the operator's responsibility to ensure signed certificates are generated and installed correctly.

The operator must perform the following steps to secure TLS:

1. Issue the following command to establish a Trust Anchor on the switch:

```
crypto pki ta-profile HPE
```

2. Issue the following command to establish an identity profile on the switch:

```
crypto pki identity-profile 5400R subject common-name 5400R org HPE
org-unit RND state CA country US
```

3. Issue the following command to create the certificate signing request:

```
crypto pki create-csr certificate-name syslog_cert ta-profile HPE usage all key-type rsa key-size 2048
```

The switch will generate and display a unique certificate signing request.

4. Copy the text of this certificate signing request (including -----BEGIN CERTIFICATE REQUEST----- and -----END CERTIFICATE REQUEST-----) as plaintext and paste it to an external file named "syslog_request.csr". This file must be copied to the workstation that will generate the certificates.
5. Make sure CA certificate is used to sign the certificate request.
6. Copy the trust anchor/CA certificate, private key, and server certificate and copy them to a location on the syslog server. These files will be used in Section 3.7.2.3 to setup the trusted channel.
7. Copy the trust anchor/CA certificate to an SFTP server accessible to the switch. The switch must be able to copy the certificate from this server via SFTP.

8. Copy the text of the signed certificate (`syslog_cert.pem` in the above example). This text will be pasted into the console on the switch.
9. Install the trust anchor certificate on the switch by issuing the following command:

```
copy sftp ta-certificate HPE <sftp-ip-addr> hp-ca.pem
```

`<sftp-ip-addr>` must be a valid connection string for an SFTP server containing the trust anchor/CA certificate. For example, to connect to an SFTP server at IP address 192.168.10.1 with user name "admin", issue the command:

```
copy sftp ta-certificate HPE admin@192.168.10.1 hp-ca.pem
```

The switch may prompt for acceptance of the remote SFTP server's host key:

```
The authenticity of host '192.168.10.1' cannot be established. DSA
key fingerprint is xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx.
```

```
Do you want to accept this host key? [(y)es/(n)o/(o)nce]
```

Press **[Y]** or **[O]** to connect to the remote SFTP server. Input the password, when prompted

10. Install the signed certificate by issuing the following command:

```
crypto pki install-signed-certificate
```

The switch will prompt for a new certificate:

```
Paste the certificate here and enter:
```

Paste the contents of the signed certificate copied in step 8

Certificate installation is complete. Proceed to the next section to create a trusted channel.

Creating a Trusted Channel with a Remote Syslog Server

In order to comply with the evaluated configuration, the switch must establish a trusted channel to a remote syslog server over TLS.

This section requires the establishment of signed certificates on both the switch and the remote syslog server. The steps in Section: Generating Trust Anchors and Credentials for Syslog must be successfully completed before establishing the trusted channel.

Additionally, the syslog server must be configured to authenticate over TLS using signed certificates.

Once signed certificates are generated and installed, the operator must configure the switch to send logs to the syslog server. Issue the following command on the switch to establish a trusted channel between the switch and the remote syslog server:

```
Aruba-Switch(config)# logging <ip-address/domain name> tls
```

The `<ip-address>` parameter must be the IP address of a remote syslog server capable of establishing a trusted channel with the switch over TLS. For example, to establish a trusted channel with a server at IP address 192.168.1.25, issue the following command:


```
Aruba-Switch(config)# logging 192.168.1.25 tls
```

If properly configured, events will appear on the syslog server in the file `/var/log/2930F.log`

SAN/CN (Subject Alternate Name /Common Name) Validation for Syslog over TLS

When SAN/CN check is enabled on the switch, the SAN or CN in the server certificate is validated against the configured domain-name of the syslog server.

Following command is used to enable SAN/CN check :

```
Aruba-Switch(config)# crypto pki application syslog validate-cert-extension
san-cn
```

To verify SAN/CN is enabled or not

```
Aruba-Switch(config)# show crypto pki application
Certificate Extension Validation:
Application          SAN/CN
-----
syslog              Enabled
```

Refer to the ArubaOS-Switch Access Security Guide for more details on the feature implementation.

TLS

Cipher Suites

By default the switch provides all the supported cipher suites.

When switch is the TLS Client the following are the TLS ciphers to be supported in the evaluated configuration:

1. TLS_RSA_WITH_AES_128_GCM_SHA256
2. TLS_RSA_WITH_AES_256_CBC_SHA256
3. TLS_RSA_WITH_AES_256_CBC_SHA
4. TLS_RSA_WITH_AES_128_CBC_SHA256
5. TLS_RSA_WITH_AES_128_CBC_SHA
6. TLS_RSA_WITH_AES_256_GCM_SHA384
7. TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
8. TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

When switch is the TLS server the following are the TLS ciphers to be supported in the evaluated configuration:

1. TLS_RSA_WITH_AES_128_GCM_SHA256
2. TLS_RSA_WITH_AES_256_CBC_SHA256
3. TLS_RSA_WITH_AES_256_CBC_SHA
4. TLS_RSA_WITH_AES_128_CBC_SHA256
5. TLS_RSA_WITH_AES_128_CBC_SHA
6. TLS_RSA_WITH_AES_256_GCM_SHA384
7. TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
8. TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
9. TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,
10. TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
11. TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,
12. TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA

The following non-required ciphers should be disabled in order to fully comply with the evaluated configuration:

1. TLS_RSA_WITH_3DES_EDE_CBC_SHA
2. TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
3. TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
4. TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
5. TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
6. TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
7. TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
8. TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
9. TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
10. TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
11. TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
12. TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
13. TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
14. TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
15. TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
16. TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
17. TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
18. TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
19. TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
20. TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
21. TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
22. TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
23. TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Issue the following command to disable any cipher suite:

```
Aruba-Switch(config)# tls application all lowest-version tls1.2 disable-  
cipher <Cipher Name>
```

Example

To disable cipher suite - TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA

```
Aruba-Switch(config)# tls application all lowest-version tls1.2 disable-  
cipher ecdh-ecdsa-aes128-sha
```

```
Aruba-Switch(config)# wr mem
```

Enforce Cipher Suites for the TLS connection

Issue the following command to enforce any cipher suites.

```
tls application all lowest-version tls1.2 cipher <Cipher Name>
```

Example

To enforce multiple cipher suites - TLS_RSA_WITH_AES_256_CBC_SHA256 and
TLS_RSA_WITH_AES_256_GCM_SHA384

```
tls application all lowest-version tls1.2 cipher aes256-sha256  
tls application all lowest-version tls1.2 cipher aes256-gcm-sha384  
write mem
```

Minimum Level of Security (minLOS) for TLS

There are two levels of minLOS that can be configured for TLS connections.

- minLOS-128: This security level matches Elliptic Curve P-256.
- minLOS-192: This security level matches Elliptic Curve P-384.

The following command puts the device into strict mode.

```
Aruba (config)# crypto suiteB-MinLoS 128 tls strict
```

MinLOS levels	Strict mode	Non-strict mode

<p>128</p>	<p>Regardless of switch acting as server or client, only the below mentioned ciphers are advertised in strict mode.</p> <ul style="list-style-type: none"> • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 <p>Below mentioned 2 elliptical curves are advertised. Curves: secp256r1, secp384r1. <i>crypto suiteB-MinLoS 128 tls strict</i></p>	<p>Regardless of switch acting as server or client, all 35 ciphers are advertised with the below mentioned ciphers at the top.</p> <ul style="list-style-type: none"> • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 <p>Below mentioned 4 elliptical curves are advertised. Curves: secp256r1,secp384r1,secp521r1,secp224r1 <i>crypto suiteB-MinLoS 128 tls</i></p>
<p>192</p>	<p>Only the below mentioned cipher is advertised in the strict mode. TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384</p> <p>Elliptical curve - secp384r1 is only advertised in the clientHello <i>crypto suiteB-MinLoS 192 tls strict</i></p>	<p>All 35 ciphers are advertised from the switch with the below mentioned cipher at the top. TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384</p> <p>Below mentioned 4 elliptical curves are advertised. Curves: secp256r1,secp384r1,secp521r1,secp224r1 <i>crypto suiteB-MinLoS 192 tls</i></p>

Certificate Revocation Methods

The certification revocation method used is OCSP.

OCSP

OCSP operates on a client server response model. Where, a revocation status is embedded in OCSP response.

When user configures OCSP method, the verification check done at run time, i.e. during TLS connection negotiation, in this case, switch constructs the OCSP request packet and send to the configured OCSP responder URL or OCSP responder URL embed in the certificate. Based on the revocation status, a TLS connection will be allowed or aborted.

Steps to be followed for OCSP configuration are:

1. Configure the revocation check OCSP in delegate mode

```
Aruba-Switch(config)# crypto pki ta-profile <profile_name> revocation-check ocsf delegate
```

2. Configure URL for the OCSP revocation check if the URL to be considered as configured else the the URL will be picked up from the certificate

```
Aruba-Switch(config)# crypto pki ta-profile <profile_name> revocation-  
check oosp delegate url1 <URL1>
```

```
Aruba-Switch(config)# crypto pki ta-profile tal revocation-check oosp  
delegate url1 https://10.1.1.1:8888
```

If chain certificate is used for mutual authentication, then the OCSP URLs can be configured as follows:

```
URL1 : URL of leaf certificate.  
URL2 : URL of the issuer of leaf certificate ( Intermediate-1).  
URL3 : URL of the issuer of intermediate-1 certificate ( Intermediate-  
2).  
URL4 : URL of the Root Certificate.
```

3. Copy the TA profile certificate to the switch.

```
Aruba-Switch(config)# copy sftp ta-certificate tal root@20.1.1.10  
cacert.pem
```

4. Create the CSR on the switch:

```
Aruba-Switch(config)#  
crypto pki create-csr certificate-name cal ta-profile tal usage all  
subject common comm country US state CO locality FO org temp org-unit  
accessories
```

5. Show the details of a Trusted Anchor Profile.

```
Aruba-3810M-48G-PoEP-1-slot# sh crypto pki ta-profile tal detail  
  
Profile Name: tal  
  
Profile Status: Root Certificate Installed  
  
CRL Configured : No  
  
CRL URL1 : Not configured  
  
CRL URL2 : Not configured  
  
CRL Refresh Interval : 24  
  
CRL Enforcement : Strict  
  
CRL Root Certificate Profile :
```

```

OCSP Configured           : Yes
OCSP URL1                 : Not configured
OCSP URL2                 : Not configured
OCSP Enforcement         : Delegate
OCSP Disable Nonce       : No
OCSP Root Certificate Profile:
OCSP Delegate URL1       : https://10.1.1.1:8888
OCSP Delegate URL2       : Not configured
OCSP Delegate URL3       : Not configured
OCSP Delegate URL4       : Not configured

```

Note: If the revocation status of the certificate cannot be determined, the TLS connection will be aborted. In this scenario, the admin should verify OCSP server is running and reachable.

Creation of ECDSA Certificate Request in the Switch

```

Aruba-Switch(config)#crypto pki create-csr certificate-name ecdsaCertificate
ta-profile ta1 key-type ecdsa curve 384 usage all subject

```

```

Enter Common Name (CN) : SwCert
Enter Org Unit (OU) : NTL
Enter Org Name (O) : HPE
Enter Locality (L) : BF
Enter State (ST) : KA
Enter Country (C) : IN
-----BEGIN CERTIFICATE REQUEST-----
MIIBSzcB0wIBADBUMQ8wDQYDVQQDEwZTd0NlcnQxDDAKBgNVBAsTA05UTDEMMAoGA
1UEChMDSFBMFQswCQYDVQQHEwJCRjELMAkGA1UECBMCS0ExCzAJBgNVBAYTAklOMH
YwEAYHkoZiZj0CAQYFK4EEACIDYgAEBEY12WqrlKJh0JtDGbYNehBom+Ui8FNI//I
wIoT1a96cE4+R24LY2LtXHG0dlw6F7CHzoWtwp+LkdzG9drdc8q4cUY8pITBwEfPo
QmbOjg2vEa4XEQ/cvO9QLUEgoXLjoAAwCQYHkoZiZj0EAQNoADB1AjArlVesz3bcC
elREkl6GpRV5xamBZIMuwtVdJn15+7iYH9F0L5+IUhgQPT1LkJT/GkCMQDBVuvNle
fIiw7Rp31ViEDYiZ7th5ZCb4HMnbdmC71JqZaU1blURUL9+Q/4xx/0pEE=
-----END CERTIFICATE REQUEST-----

```

Minimum secure RSA key size.

With minimum secure key feature, the key generation for 1024 bits key will be disabled.

```

Aruba-Switch(config)# crypto enforce secure-rsa

```

Example

```
Aruba-Switch(config)# crypto enforce secure-rsa
**** CAUTION ****
```

Enabling the secure RSA key feature will only allow generation of 2048 bits or higher as 1024 or lower bit keys are deprecated.
Continue (y/n)? y

```
Aruba-Switch(config)# crypto key generate ssh rsa bits 2048
```

```
Aruba-Switch(config)# crypto pki create-csr certificate-name swCert ta-profile
tal key-type rsa key-size 2048
```

Validation of Extended Key Usage Extension for X509v3 certificates

Validate the extended key usage extension OID if present in the certificate during the processing of certificate. Validation are done based on the table.

TABLE 4 - X509V3 VALIDATION

Connection Type	Switch act as Server / Client	Authentication type	Validate For OID
Web connection	Server	Normal	Client (Optional) 1.3.6.1.5.5.7.3.2
Syslog	Client	Mutual authentication	Server 1.3.6.1.5.5.7.3.1
SSH	Server	Normal	Server 1.3.6.1.5.5.7.3.1

User, Password, and Session Management

The default privilege levels on the switch are: “operator” and “manager”. In the evaluated configuration, the user must configure the “operator” and “manager” credentials to prevent unauthenticated access. Manager has full access and the operator has read only access to 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 lower case characters
- 0 through 9 numeric characters
- Special characters: ! @ # \$ % ^ & * ()

- The SPACE character is allowed to form a user name or password pass-phrase. The user name must be in quotes, for example “The little brown fox”. A space is not allowed as part of a user name without the quotes. A password that includes a space or spaces should not have quotes.
- The password length ranges from 8 to 64 characters.

Following need to be followed for strong password configuration:

- The passwords should be combination of the alphanumeric characters with both lower and upper case characters and special characters.
- Does not use known information about yourself (e.g. pets names, your name, kids names or any information available in the public domain);
- Is significantly different from previous passwords (adding a ‘1’ or ‘!’ to the end of the password is not sufficient);
- Does not contain a complete word. (Ex: Password!).

Password complexity feature can be used if additional password functionalities like password expiration, history validation, update interval time, password reconfiguration on first login and upon password expiration, password complexity checks. Please refer to the Security Manual for more details.

Password minimum length

The minimum length of the password should be configured as “8”. The password length can be from 8 to 64 characters.

Command to configure the minimum password:

```
Aruba-Switch(config)#password minimum-length 8
```

User Based Lockout Delay

User based Lockout delay feature will lockout the users based on user name when defined number of unsuccessful authentication attempts has been met. The users are prevented from successfully authenticating until the configured lockout-delay time period has elapsed. This feature locks out users with SSH and does not lock the console session.

Command to lock a user based on username.

```
Aruba-Switch(config)#aaa authentication user-based-lockout
```

Configure the lockout period

```
Aruba-Switch(config)#aaa authentication lockout-delay <seconds>
```

All the unknown users (the users which are not created in the system) will not be locked out even though the maximum number of unsuccessful attempts has been met.

To unlock a user, the command used is:


```
Aruba-Switch(config)#aaa authentication unlock user-name <user-name>
```

To show all the users in locked state

```
Aruba-Switch(config)#show authentication locked-out-users
```

Protecting Credentials

To comply with the evaluated configuration, user name and password information must be saved, encrypted, and hidden. The manager must run the following commands to encrypt user credentials:

```
Aruba-Switch(config)#encrypt-credentials
```

Before beginning encryption, the switch will warn about incompatibility:

```
Aruba-3810M-24G-1-slot(config)# encrypt-credentials

**** CAUTION ****

This will encrypt all passwords and authentication keys.

The encrypted credentials will not be understood by older software versions.
The resulting config file cannot be used by older software versions.
It also may break some of your existing user scripts.

Before proceeding, please save a copy of your current config file, and
associate the current config file with the older software version saved in
flash memory. See "Best Practices for Software Updates" in the Release Notes.

A config file with 'encrypt-credentials' may prevent previous software
versions from booting. It may be necessary to reset the switch to factory
defaults. To prevent this, remove the encrypt-credentials command or use
an older config file.

Save config and continue (y/n)? y
Aruba-3810M-24G-1-slot(config)#
```

FIGURE 14 - WARNING WHEN RUNNING COMMAND "ENCRYPT CREDENTIALS"

Press **[Y]** to begin encryption.

The operator must also run the following command to save credentials and public keys:

```
Aruba-Switch(config)#include-credentials
```

As before, the switch will issue an incompatibility warning:

```
Aruba-3810M-24G-1-slot(config)# include-credentials

**** CAUTION ****

You have invoked the command 'include-credentials'. This action will make
changes to the password and SSH public-key storage.

It will affect *all* stored configurations, which might need to be updated.
Those credentials will no longer be readable by older software revisions.
It also may break some of your existing user scripts. Continue?[y/n] y
```

FIGURE 15 - COMPATIBILITY WARNING WHEN RUNNING COMMAND "INCLUDE-CREDENTIALS"

Press [Y] to continue. The switch will also issue a security warning:

```
**** CAUTION ****

This will insert possibly sensitive information in switch configuration files,
and as a part of some CLI commands output. It is strongly recommended that you
use SFTP rather than TFTP for transfer of the configuration over the network,
and that you use the web configuration interface only with SSL enabled.

Erasing configurations with 'include-credentials' enabled will erase stored
passwords and security credentials. The system will reboot with the factory
default configuration.

Proceed?[y/n] y
```

FIGURE 16 - SECURITY WARNING WHEN RUNNING COMMAND "INCLUDE-CREDENTIALS"

PRESS [Y] TO CONTINUE.

SHA -1 and SHA-256 Password Storage

Passwords can be configured and stored in SHA-1 and SHA-256. Include credentials stores the passwords in SHA1 form and password non-plaintext-sha256 stores the passwords in SHA256 hash. For the passwords to be visible in configuration when hashed using SHA256, Include credentials should be enabled and after enabling include credentials option to configure manager, operator and local user passwords in SHA 256 will become available.

1. To enable/disable password non-plaintext-sha256

```
Aruba-Switch(config)# password non-plaintext-sha256
```

2. To configure user's password input in sha256 format.

```
Aruba-Switch(config)#password manager user-name <username> sha256 "<sha-
text>"
```

Configuring Login Banner

The evaluated configuration requires the display of an administrator-specified advisory notice prior to login. By default, the switch will display the following banner:

```
(C) Copyright 2017 Hewlett Packard Enterprise Development LP

                RESTRICTED RIGHTS LEGEND
Confidential computer software. Valid license from Hewlett Packard Enterprise
Development LP required for possession, use or copying. Consistent with FAR
12.211 and 12.212, Commercial Computer Software, Computer Software
Documentation, and Technical Data for Commercial Items are licensed to the
U.S. Government under vendor's standard commercial license.

We'd like to keep you up to date about:
 * Software feature updates
 * New product announcements
 * Special events
Please register your products now at: www.hpe.com/networking/register
```

FIGURE 17 - DEFAULT LOGIN BANNER

The command to specify a “message of the day” (login) banner:

```
Aruba-Switch(config)#banner motd %
```

The system will prompt for a banner:

```
Enter TEXT message. End with the character `%'
```

Enter the following banner:

```
This is the MOTD banner %
```

The operator must also issue the following command to specify an “exec” (post-login) banner:

```
Aruba-Switch(config)#banner exec %
```

The system will prompt for a banner:

```
Enter TEXT message. End with the character `%'
```

Enter the following banner:

```
This is the post-login banner
%
```

After the banners are set, the switch will display the MOTD banner before beginning the login process.

Example

When connecting over SSH:

```
18:52:54 % ssh admin@10.100.1.247
This is the MOTD banner
```

FIGURE 18 - CONFIGURED MESSAGE OF THE DAY BANNER

Upon successful login, the switch will display the exec banner:

```
This is the post-login banner

Your previous successful login (as manager) was on 2016-01-19 02:42:03
from 10.0.13.122
```

FIGURE 19 - CONFIGURED EXEC BANNER WITH PREVIOUS LOGIN MESSAGE

Configuring Session Timeouts

The evaluated configuration requires the establishment of time limits to automatically disconnect sessions after a given period of inactivity. The Aruba Switch supports inactivity timers for both remote and local (serial) connections. By default, all timers are disabled. The user must establish inactivity timers for both local and remote sessions.

Issue the following commands to set an inactivity timer of 5 minutes for (SSH) and local (serial/USB) sessions:

```
Aruba-Switch(config)#console idle-timeout 300
Aruba-Switch(config)#console idle-timeout serial-usb 300
```

Issue the following command to set inactivity time of 5 minutes for WebUI sessions:

```
Aruba-Switch(config)#web-management idle-timeout 300
```

Sessions idle for longer than 5 minutes will be terminated automatically

Finalizing Configuration

Disabling Services Not Under Evaluation

The evaluated configuration requires the operator to disable the following services not under evaluation:

- Telnet
- Web Management (HTTP)
- DHCP
- REST

The operator must issue the following commands to disable the above services:

```
Aruba-Switch(config)#no telnet-server
Aruba-Switch(config)#no web-management
Aruba-Switch(config)#no dhcp-server enable
Aruba-Switch(config)#no rest-interface
```

Booting to Evaluated Configuration

To save the evaluated configuration, the operator must issue the following command:

```
Aruba-Switch(config)#write mem
```

The above command will commit the evaluated configuration to persistent storage.

Finally the operator must issue the following command to reboot the switch in the evaluated configuration:

```
Aruba-Switch(config)#boot system flash secondary
```

The switch will prompt for confirmation:

```
This will reboot the system from the secondary image.  
Continue (y/n)?
```

Press **[Y]** to reboot. When the switch finishes booting, it will be in the evaluated configuration.

Audit Functionality

The audit Log records operating events in single- or double-line entries and serves as a tool to isolate and troubleshoot problems.

In addition to local audit log storage, the switch supports synchronization of audit logs with a remote audit log server via a secure channel. Events are synchronized with remote log servers whenever new messages are received. If the remote audit server connection is disconnected, the user need to re-establish the session.

NOTE

The audit log is erased if power to the switch is interrupted or if you enter the `boot system` command. The contents of the audit log are not erased if you:

- Reboot the switch by choosing the Reboot Switch option from the menu interface.
 - Enter the reload command from the CLI.
-

Accessing Audit Logs

Use the `show logging` command to display audit logs.

Syntax

```
Aruba-Switch(config)#show logging <a|b|r|s|t|m|p|e|w|i|d|filter|option-  
str|substring ...>
```

The options `a|r|substring` can be used in combination with an event class option.

a	Display all log events, including those from previous boot cycles
b	Display log events as time since boot instead of date/time format
r	Display log events in reverse order (most recent first)
s	Display the active and standby management module log events when operating in nonstop switching mode
t	Display log events in granularity in 10 milliseconds
substring	Instructs the switch to display only those events that match the substring

The remaining event class options are listed in order of severity – lowest severity first. The output of the command is confined to event classes of equal or higher severity. Only one of the options `d|i|w|e|p|m` can be used in the command at a time.

m	Major event class
e	Error event class
p	Performance event class
w	Warning event class
x	Information event class
d	Debug event class
filter	Display log filter configuration and status information
OPTION-STR	Filter events shown

For example, issuing the `show logging` command will produce output similar to the following:

```

Keys:  W=Warning  I=Information
      M=Major    D=Debug  E=Error
---- Reverse event Log listing: Events Since Boot ----
W 03/14/18 13:03:35 05220 activate: Unable to resolve the Activate server
address device.arubanetworks.com.
I 03/14/18 13:03:29 05225 activate: Loading security certificates and
synchronizing time with NTP.
I 03/14/18 12:54:24 03783 dhcp: DHCP server did not offer all the DNS parameters
on Primary VLAN
I 03/14/18 12:54:24 00025 ip: DEFAULT_VLAN: ip address 10.101.115.253/24
configured on vlan 1
I 03/14/18 12:54:24 05177 ip: Setting IP address 10.101.115.1 as default
gateway.
I 03/14/18 12:54:24 00083 dhcp: updating IP address and subnet mask
I 03/14/18 12:54:16 00828 lldp: PVID mismatch on port 1(VID 1)with peer device
port 41(VID 1370)(1)
I 03/14/18 12:54:15 00076 ports: port 1 is now on-line
I 03/14/18 12:54:14 00076 ports: port 47 is now on-line
I 03/14/18 12:54:14 00076 ports: port 46 is now on-line
I 03/14/18 12:54:09 02555 chassis: Co-processor Ready
I 03/14/18 12:54:00 03803 chassis: System Self test completed on 1-48,A
I 03/14/18 12:53:44 05101 amp-server: AMP server configuration is disabled due
to first configuration.
- MORE --, next page: Space, next line: Enter, quit: Control-C

```

FIGURE 20 - SAMPLE LOG

Audit log format

Each Audit Log entry is composed of six or seven fields, depending on whether numbering is turned on or not:

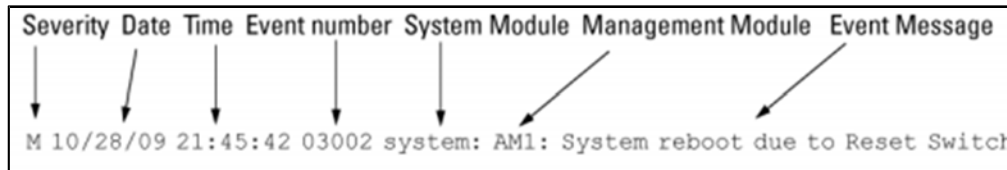


FIGURE 21- AUDIT LOG ENTRY FORMAT

The following table describes each field:

Item	Description
------	-------------

Severity	One of the following codes (from highest to lowest severity): M — (major) indicates that a fatal switch error has occurred. E — (error) indicates that an error condition occurred on the switch. W — (warning) indicates that a switch service has behaved unexpectedly. I — (information) provides information on normal switch operation. D — (debug) is reserved for HPE internal diagnostic information.
Date	The date in the format mm/dd/yy when an entry is recorded in the log.
Time	The time in the format hh:mm:ss when an entry is recorded in the log.
Event number	The number assigned to an event. You can turn event numbering on and off with the <code>[no] log-number</code> command.
System Module	The internal module (such as <code>ports</code> for port manager) that generated a log entry. If VLANs are configured, a VLAN name also appears for an event that is specific to an individual VLAN.
Event Message	A brief description of the operating event

TABLE 5 - AUDIT LOG ENTRY ITEMS

List of Auditable Events (CC Required)

See the Aruba Event Log Message Reference Guide for a full list of Events.

The document link for reference: <https://www.arubanetworks.com/techdocs/AOS-Switch/16.11/Event%20Log%20Message%20Reference%20Guide%20for%20AOS-S%20Switch%2016.11.pdf>

Audit Requirement	Auditable Events	Sample Audit Record Format
NDcPP22e:FAU_GEN.1	Startup and shutdown of the audit functions	Jul 7 2022 14:33:04 192.168.144.162 04331 mgr: syslog: Information logging started on the SYSLOG server tl24-16x.example.com over TLS protocol Jul 7 2022 15:24:08 192.168.144.162 04332 mgr: syslog: Information logging stopped on the SYSLOG server tl24-16x.example.com over TLS protocol
NDcPP22e:FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session.	See FCS_TLSS_EXT.1

<p>NDcPP22e:FCS_SSHS_EXT.1</p>	<p>Failure to establish an SSH session.</p>	<p>Feb 15 2022 06:21:04 192.168.144.162 03345 ssh: User :Login failed for SSH session from 192.168.144.254 due to cipher mismatch.</p> <p>Feb 2 2022 20:00:45 192.168.144.162 05920 ssh: Login failed for SSH session from 192.168.144.254 due to no matching MAC algorithm.</p> <p>Feb 2 2022 20:05:01 192.168.144.162 05918 ssh: Login failed for SSH session from 192.168.144.254 due to no matching key exchange algorithm.</p> <p>Feb 15 2022 06:12:57 192.168.144.162 05919 ssh: Login failed for SSH session from 192.168.144.254 due to no matching host key algorithm.</p>
<p>NDcPP22e:FCS_TLSC_EXT.1</p>	<p>Failure to establish a TLS Session.</p>	<p>Jun 14 2022 13:07:19 192.168.144.162 00469 ssl: User syslogTask:TLS connection failed for SYSLOG session from 192.168.144.254.</p> <p>Aug 29 2022 13:51:46 Aruba-2930F-48G-PoEP-4SFPP-TAA 00469 ssl: User syslogTask:TLS connection failed for SYSLOG session from 192.168.144.254. (6 times in 60 seconds)</p> <p>Aug 29 2022 13:51:46 Aruba-2930F-48G-PoEP-4SFPP-TAA SSL : SSL tSlogTLSConn2:ERR_SSL_BAD_HEADER_VERSION</p> <p>Aug 29 2022 13:58:06 Aruba-2930F-48G-PoEP-4SFPP-TAA 00469 ssl: User syslogTask:TLS connection failed for SYSLOG session from 192.168.144.254. (1 times in 60 seconds)</p> <p>Aug 29 2022 13:58:06 Aruba-2930F-48G-PoEP-4SFPP-TAA SSL : SSL tSlogTLSConn2:ERR_SSL_UNSUPPORTED_CURVE</p> <p>Aug 29 2022 13:59:24 Aruba-2930F-48G-PoEP-4SFPP-TAA 00469 ssl: User syslogTask:TLS connection failed for SYSLOG session from 192.168.144.254. (2 times in 60 seconds)</p> <p>Aug 29 2022 13:59:24 Aruba-2930F-48G-PoEP-4SFPP-TAA SSL : SSL tSlogTLSConn2:ERR_SSL_PROTOCOL_VERSION</p> <p>Aug 29 2022 14:00:47 Aruba-2930F-48G-PoEP-4SFPP-TAA 00469 ssl: User syslogTask:TLS connection failed for SYSLOG session from 192.168.144.254. (1 times in 60 seconds)</p>

		<p>Aug 29 2022 14:00:48 Aruba-2930F-48G-PoEP-4SFPP-TAA SSL : SSL tSlogTLSConn2:ERR_CERT_INVALID_SIGNATURE</p> <p>Aug 29 2022 14:02:06 Aruba-2930F-48G-PoEP-4SFPP-TAA 00469 ssl: User syslogTask:TLS connection failed for SYSLOG session from 192.168.144.254. (1 times in 60 seconds)</p> <p>Aug 29 2022 14:02:08 Aruba-2930F-48G-PoEP-4SFPP-TAA SSL : SSL tSlogTLSConn2:ERR_SSL_PROTOCOL_PROCESS_FINISHED</p> <p>Aug 29 2022 14:03:12 Aruba-2930F-48G-PoEP-4SFPP-TAA 04331 mgr: syslog: Information logging started on the SYSLOG server 192.168.144.254 over TLS protocol</p> <p>Aug 29 2022 14:03:16 Aruba-2930F-48G-PoEP-4SFPP-TAA SSL : SSL tSlogTLSConn2:ERR_SSL_CRYPT_BLOCK_SIZE</p> <p>Aug 29 2022 11:33:09 Aruba-2930F-48G-PoEP-4SFPP-TAA SSL : SSL tSlogTLSConn2:Certificate Public Key does not match supported algorithms. status =</p> <p>Jul 14 2022 10:33:22 Aruba-2930F-48G-PoEP-4SFPP-TAA SSL : SSL tSlogTLSConn1:ERR_CERT_INVALID_EXTENDED_KEYUSAGE</p> <p>Jul 13 2022 16:20:50 192.168.144.162 05928 ssl: TLS connection failed for SYSLOG session from 192.168.144.254 due to bad common name.</p> <p>Jul 13 2022 16:21:48 192.168.144.162 05929 ssl: TLS connection failed for SYSLOG session from 192.168.144.254 due to bad SAN. (1 times in 60 seconds)</p> <p>Aug 10 2022 14:46:33 Aruba-2930F-48G-PoEP-4SFPP-TAA 00469 ssl: User syslogTask:TLS connection failed for SYSLOG session from 192.168.144.254.</p> <p>Aug 10 2022 14:46:33 Aruba-2930F-48G-PoEP-4SFPP-TAA SSL : SSL tSlogTLSConn1:ERR_SSL_PROTOCOL_PROCESS_SERVER_HELLO</p>
--	--	--

<p>NDcPP22e:FCS_TLSS_EXT.1</p>	<p>Failure to establish a TLS Session.</p>	<p>Jul 14 2022 13:18:01 3810M 00469 ssl: User :TLS connection failed for WEB-UI session from 192.168.144.254 due to cipher mismatch.</p> <p>Aug 10 2022 12:51:37 Aruba-2930F-48G-PoEP-4SFPP-TAA SSL : SSL tHttpd:ERR_SSL_PROTOCOL_PROCESS_FINISHED</p> <p>Aug 10 2022 12:51:37 Aruba-2930F-48G-PoEP-4SFPP-TAA 00469 ssl: User :TLS connection failed for WEB-UI session from 192.168.144.254</p> <p>Aug 10 2022 13:03:34 Aruba-2930F-48G-PoEP-4SFPP-TAA SSL : SSL tHttpd:ERR_SSL_PROTOCOL_PROCESS_CLIENT_HELLO</p> <p>Aug 10 2022 13:03:34 Aruba-2930F-48G-PoEP-4SFPP-TAA 00469 ssl: User :TLS connection failed for WEB-UI session from 192.168.144.254.</p>
<p>NDcPP22e:FIA_AFL.1</p>	<p>Unsuccessful login attempt limit is met or exceeded.</p>	<p>Jun 14 2022 13:07:36 192.168.144.162 03369 auth: User 'admin' from 192.168.144.254 is locked out for 60 seconds</p> <p>Jun 14 2022 13:07:36 192.168.144.162 00419 auth: Invalid user name/password on SSH session User 'admin' is trying to login from 192.168.144.254</p>
<p>NDcPP22e:FIA_UAU_EXT.2</p>	<p>All use of identification and authentication mechanism.</p>	<p>Refer to FIA_UIA_EXT.1</p>

<p>NDcPP22e:FIA_UIA_EXT.1</p>	<p>All use of identification and authentication mechanism.</p>	<p>Jun 17 2022 14:14:02 192.168.144.162 00419 auth: Invalid user name/password on CONSOLE session User 'admin' is trying to login from 0.0.0.0</p> <p>Jun 17 2022 14:14:54 192.168.144.162 03362 auth: User 'admin' logged in from 0.0.0.0 to CONSOLE session</p> <p>Jun 14 2022 13:07:36 192.168.144.162 00419 auth: Invalid user name/password on SSH session User 'admin' is trying to login from 192.168.144.254</p> <p>Jun 14 2022 14:23:09 192.168.144.162 03362 auth: User 'admin' logged in from 192.168.144.254 to SSH session</p> <p>Jul 7 2022 12:49:00 192.168.144.162 03343 ssh: User (null) : SSH session aborted due to public-key authentication failure</p> <p>Jul 8 2022 10:10:34 192.168.144.162 03344 ssh: User admin : SSH session established with public-key authentication</p> <p>Jun 14 2022 14:08:02 192.168.144.162 03362 auth: User 'admin' logged in from 192.168.144.253 to WEB_UI session</p> <p>Jun 14 2022 14:07:12 192.168.144.162 00419 auth: Invalid user name/password on WEB-UI session User 'admin' is trying to login from 192.168.144.253</p>
-------------------------------	--	--

<p>NDcPP22e:FIA_X509_EXT.1/Rev</p>	<p>Unsuccessful attempt to validate a certificate.</p>	<p>Jul 7 2022 16:01:40 192.168.144.162 05924 crypto: OCSP signing extension is not enabled for the trusted anchor profile 'syslog'. (1 times in 60 seconds)</p> <p>Jul 7 2022 16:05:56 192.168.144.162 05931 ssl: TLS connection failed for SYSLOG session from 192.168.144.254 due to certificate parse error.</p> <p>Jul 7 2022 16:06:28 192.168.144.162 05930 ssl: TLS connection failed for SYSLOG session from 192.168.144.254 due to decryption failure (corrupted signature).</p> <p>Jul 7 2022 16:06:38 192.168.144.162 05932 ssl: TLS connection failed for SYSLOG session from 192.168.144.254 due to certificate validation failure (bad public key).</p> <p>Aug 29 2022 10:21:30 Aruba-2930F-48G-PoEP-4SFPP-TAA 00469 ssl: User syslogTask:TLS connection failed for SYSLOG session from 192.168.144.254.</p> <p>Aug 29 2022 10:21:31 Aruba-2930F-48G-PoEP-4SFPP-TAA SSL : SSL tSlogTLSConn2:ERR_CERT_EXPIRED</p> <p>Aug 29 2022 11:16:50 Aruba-2930F-48G-PoEP-4SFPP-TAA 00469 ssl: User syslogTask:TLS connection failed for SYSLOG session from 192.168.144.254.</p> <p>Aug 29 2022 11:16:51 Aruba-2930F-48G-PoEP-4SFPP-TAA CRYP: CRYP tSlogTLSConn2:certificate revocation test failed during leaf verify</p> <p>Aug 29 2022 12:41:54 Aruba-2930F-48G-PoEP-4SFPP-TAA 00469 ssl: User syslogTask:TLS connection failed for SYSLOG session from 192.168.144.254. (1 times in 60 seconds)</p> <p>Aug 29 2022 12:42:00 Aruba-2930F-48G-PoEP-4SFPP-TAA CRYP: CRYP tSlogTLSConn2:Unable to find root certificate to validate certificate against.</p>
	<p>Any addition, replacement or removal of trust anchors in the TOE's trust store</p>	<p>Aug 26 2022 15:13:38 Aruba-2930F-48G-PoEP-4SFPP-TAA 03406 crypto: Trust Anchor Profile "2930_1" removed.</p> <p>Aug 26 2022 14:52:19 Aruba-2930F-48G-PoEP-4SFPP-TAA 03405 crypto: Trust Anchor Profile "2930_1" created.</p>
<p>NDcPP22e:FMT_MOF.1/ManualU pdate</p>	<p>Any attempt to initiate a</p>	<p>Refer to FPT_TUD_EXT.1</p>

	manual update.	
NDcPP22e:FMT_SMF.1 *	All management activities of TSF data.	Jul 12 2022 13:41:15 192.168.144.162 notice: Notice-Type='Running Config Change',Event-ID='1362',Config-Method='CLI',Device-Name='Aruba-2930F-48G-PoEP-4SFPP-TAA',User-Name='admin',Remote-IP-Address='0.0.0.0'
NDcPP22e: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 be logged. See also application note on FPT_STM_EXT .1)	Jun 9 2022 13:07:00 192.168.144.162 00178 mgr: Updated time by 18000 seconds. Previous time was Thu Jun 9 08:07:00 2022. Current time is Thu Jun 9 13:07:00 2022
NDcPP22e:FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure).	<p>Aug 16 2022 11:47:40 Aruba-2930F-48G-PoEP-4SFPP-TAA 00163 update: Firmware image contains valid signature.</p> <p>Aug 16 2022 11:47:45 Aruba-2930F-48G-PoEP-4SFPP-TAA 04244 update: User 'root' : Secondary Image updated via SFTP from 192.168.144.254 completed.Firmware version: #012 Before update: WC.16.11.0004 After update : WC.16.11.0007A</p> <p>Aug 17 2022 10:32:18 Aruba-2930F-48G-PoEP-4SFPP-TAA 00161 update: Aborted. Firmware image does not contain a signature.</p> <p>Aug 23 2022 12:08:33 Aruba-2930F-48G-PoEP-4SFPP-TAA 00162 update: Aborted. Firmware image signature is not valid.</p> <p>Aug 26 2022 13:25:33 Aruba-2930F-48G-PoEP-4SFPP-TAA 03311 sftp: User admin: SFTP connection failure while connecting from 192.168.144.254</p>

NDcPP22e:FTA_SSL.3	The termination of a remote session by the session locking mechanism.	<p>Jun 14 2022 14:24:28 192.168.144.162 04242 auth: User 'admin' logout from 192.168.144.254 due to inactivity timer timeout for SSH session</p> <p>Jun 14 2022 13:54:56 192.168.144.162 03387 auth: User 'admin' has been logged out from 192.168.144.253 due to session timeout</p>
NDcPP22e:FTA_SSL.4	The termination of an interactive session.	<p>Feb 2 2022 18:01:02 192.168.144.162 03363 auth: User 'admin' logged out of CONSOLE session from 0.0.0.0</p> <p>Feb 2 2022 17:27:25 192.168.144.162 03363 auth: User 'admin' logged out of SSH session from 192.168.144.254</p> <p>Jun 14 2022 12:32:52 192.168.144.162 03363 auth: User 'admin' logged out of WEB_UI session from 192.168.144.253</p>
NDcPP22e:FTA_SSL_EXT.1	(if 'lock the session' is selected) Any attempts at unlocking of an interactive session. (if 'terminate the session' is selected) The termination of a local session by the session locking mechanism.	<p>Jun 14 2022 14:24:28 192.168.144.162 04242 auth: User 'admin' logout from 192.168.144.254 due to inactivity timer timeout for SSH session</p>
NDcPP22e:FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	<p>Jun 17 2022 14:09:22 192.168.144.162 00468 ssl: User 'syslogTask': logged into SSL/TLS session for SYSLOG from 192.168.144.254</p> <p>Jun 17 2022 14:11:05 192.168.144.162 05937 ssl: SSL/TLS session reconnect for syslog server tl24-16x.example.com because of TCP timeout or session closure.</p> <p>See FCS_TLSC_EXT.1 for failures</p>

NDcPP22e:FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	<p>Feb 2 2022 13:10:27 192.168.144.162 03362 auth: User 'admin' logged in from 192.168.144.254 to SSH session</p> <p>Feb 2 2022 13:11:17 192.168.144.162 03363 auth: User 'admin' logged out of SSH session from 192.168.144.254</p> <p>See FCS_SSHS_EXT.1 for failures</p> <p>Feb 15 2022 00:36:09 192.168.144.162 05933 ssl: SSL/TLS session started for WEB-UI from 192.168.144.253.</p> <p>Jun 9 2022 10:39:20 192.168.144.162 05934 ssl: SSL/TLS session closed for WEB-UI from 192.168.144.254.</p> <p>See FCS_TLSS_EXT.1 for failures</p>
--------------------------	--	--

TABLE 6 - SECURITY FUNCTIONAL REQUIREMENTS AND AUDITABLE EVENTS

Local Command Audit log

The user can configure the local command audit logging to obtain the audit logs of the configuration changes. It does not support direct communication with the external audit log servers like Syslog. When the threshold value (80%) of the buffer is reached, there will be an audit log logged. Upon receiving the threshold audit log, the user is advised to transmit the logs manually which can be used for reference.

Enable Command logging

```
Aruba-Switch(config)# [no] logging command
```

Display Commands logged

```
Aruba-Switch(config)# show logging command
```

To display all command logs, including those from previous boot cycles, specify '-a' at the end

To display the command logs in reverse order (most recent first), specify '-r' at the end

Example:

```
Aruba-Switch(config)# show logging command
```

```
Keys:   W=Warning   I=Information
        M=Major     D=Debug   E=Error
```



```

---- Command Log listing: Events Since Boot ----
I 12/10/17 21:05:06 03440 system: ST1-CMDR: User:'user1':The command:'ip ssh'
is executed.
I 12/10/17 21:06:25 03440 system: ST1-CMDR: User:'user1':The command:'logging
command' is executed.
---- Bottom of Command Log : Events Listed = 3 ----

```

Clear command log

Remove all the entries from the command log.

```
Aruba-Switch(config)# clear logging command
```

More information on Local Audit logging can be obtained in the Security Access Guide.

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. Firmware integrity checks are performed during the reboot.

The switch will perform the following tests:

The following power up self-tests are performed:

- AES Encrypt and Decrypt KATs
- CTR DRBG KATs (DRBG Health Tests as specified in SP800-90A Section 11.3 are performed)
- HMAC-SHA1 KAT
- RSA Known Answer Tests (Separate KAT for signing; Separate KAT for verification)
- SHA1/256/512 KATs
- Triple-DES Encrypt and Decrypt KATs

Test	Purpose
RNG KAT ¹	Validate correct operation of Random Number Generator
SHA1 KAT ¹	Validate correct operation of SHA1 cryptographic algorithm
SHA256 KAT ¹	Validate correct operation of SHA256 cryptographic algorithm
SHA512 KAT ¹	Validate correct operation of SHA512 cryptographic algorithm
HMAC_SHA1 KAT ¹	Validate correct operation of HMAC_SHA1 cryptographic algorithm

3DES KAT ¹	Validate correct operation of 3DES cryptographic algorithm
AES KAT ¹	Validate correct operation of AES cryptographic algorithm
DSA2 PCT ²	Validate correct operation of DSA2 cryptographic algorithm
RSA KAT ¹	Validate correct operation of RSA cryptographic algorithm

TABLE 7 - SELF TESTS

In the event of a test failure, the switch will crash with a message similar to the following:

```
Software exception at cryptoInit.c:267 -- in 'swInitTask', task ID =
0xaa43980
```

```
-> Crypto powerup selftests failed.
```

```
Callstack: 0x001de608 0x001e03b0 0x001def60 0x011e6208 0x0004e568
0x0004fe50 0x013e4074 0x013ea5f8 0x016eedec
```

The admin can try rebooting to see if the issue is solved, if not, can upgrade to different image. If both these options do not solve the issue, the admin should call the support to get it resolved.

1. Known Answer Test. 2. Pairwise Consistency Test

4 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 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)
- 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>