AirWave 8.2.11.1

Switch Configuration Guide

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett-Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett-Packard Enterprise Company
Attn: General Counsel
6280 America Center Drive
San Jose, CA 95002
USA

Please specify the product and version for which you are requesting source code.

You may also request a copy of this source code free of charge at: http://hpe.com/software/opensource.

Contacting Support

Main Site	arubanetworks.com
Support Site	asp.arubanetworks.com
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephone	arubanetworks.com/support-services/contact-support/
Software Licensing Site	lms.arubanetworks.com
End-of-life Information	arubanetworks.com/support-services/end-of-life/
Security Incident Response Team (SIRT)	Site: arubanetworks.com/support-services/security-bulletins/ Email: aruba-sirt@hpe.com

This chapter provides the following information to help you get started using AirWave for switch configuration:

The following sections of the AirWave Switch Configuration Guide have been updated for this release. For a full list of new features and updates in AirWave 8.2.11.1, including updates to other documents, refer to the *AirWave 8.2.11.1 Release Notes*.

Table 1: *What's New in This Version of the Switch Config Guide*

Update	Description
Changes to how the server pushes configurations to Aruba switches.	This document is updated to include procedures to configure Aruba switches running firmware versions 16.01-16.04, as well as switches running firmware version 16.05 and later.

Requirements and Restrictions

AirWave supports switch configuration for:

- Mobility Access Switches running ArubaOS (AOS) 7.2.0.0 or higher
- Switches running AOS 16.01 or higher.

You will need AirWave 7.7.0 or higher installed and operational on the network.

NOTE

AirWave supports a variety of ArubaOS firmware versions. However, unsupported profiles or fields that exist in an older version will not be configured on switch running that version.

NOTE

Switch configuration is not supported in global groups or the Master Console.

Minimum Switch Configuration

In order for AirWave to communicate with the switch, you must have configured the following switch settings using the QuickStart wizard:

- System name
- Management VLAN
- Interface IP
- Management interface VLAN subnet mask
- Management interface subnet mask
- IP default gateway
- Country code
- Time zone
- Time
- Date

- Admin login and password
- Enable password

For information about configuring these switch settings, refer to the *ArubaOS User Guide* for your specific Mobility Access Switch version.

Navigation Basics

When you click in the AirWave WebUI and select a component from the navigation sidebar, AirWave will display monitoring and management pages to the right.

The following WebUI pages support switch configuration:

- "Devices > List Page" on page 9
- "Devices > Manage Page" on page 10
- "Devices > Monitor Page" on page 11
- "Devices > Device Configuration Page" on page 12
- "Groups > Switch Config" on page 13

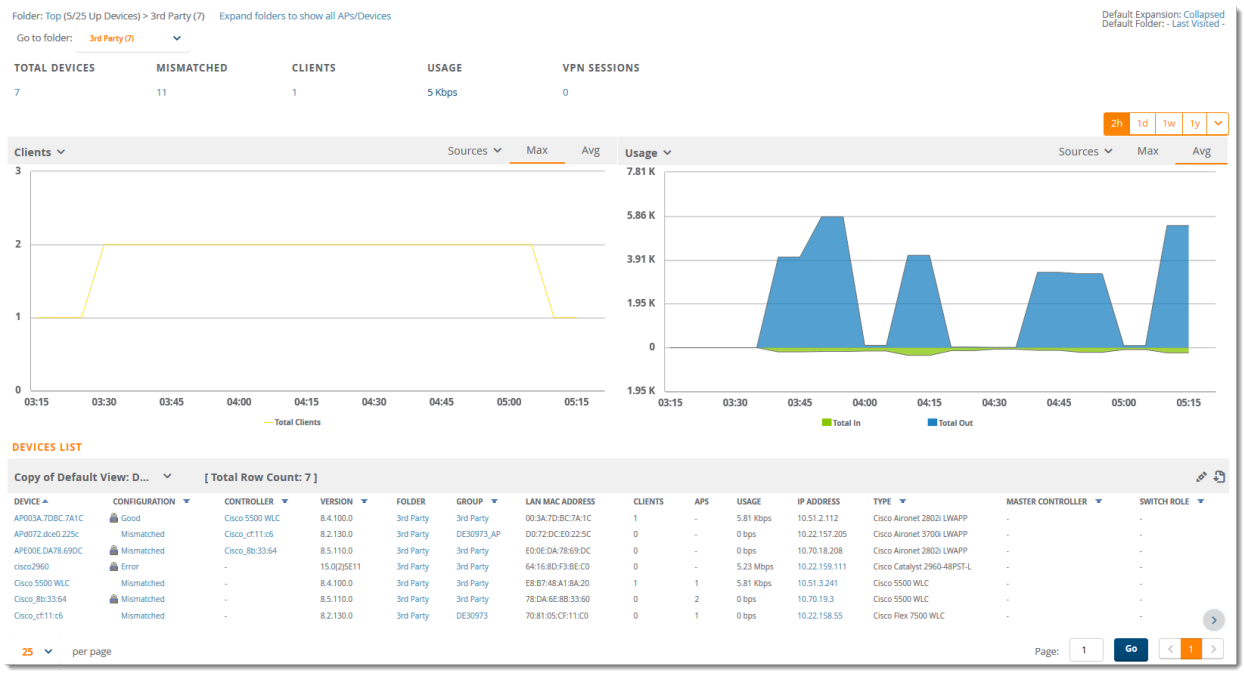
The Switch Config page is hidden from view if global configuration is enabled.

For information about using AirWave for switch monitoring, see the *AirWave 8.2.11.1 User Guide*

Devices > List Page

This page displays all devices that AirWave monitors, including wireless and wired devices. From the List page, you can click  at the top right corner of the Devices List to do device-level tasks such as rebooting, re-provisioning, changing Aruba group membership, and updating thin AP settings.

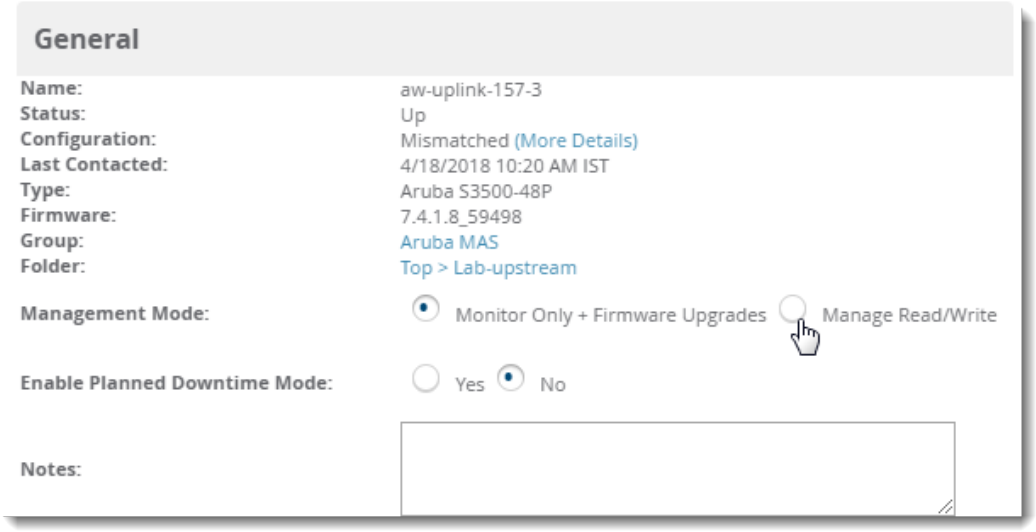
Figure 1: *Devices > List Page*



Devices > Manage Page

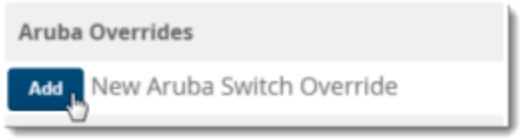
You can configure device-level settings on the Manage page for a switch, including the management mode that determines whether AirWave will push device configurations to the switch.

Figure 2: *Changing the Management Mode for a Switch*



From the Manage page, you can also add a switch override for multiple profiles, or a setting per profile, instead of creating a new profile that differs by only one setting.

Figure 3: *Adding a Switch Override*



NOTE

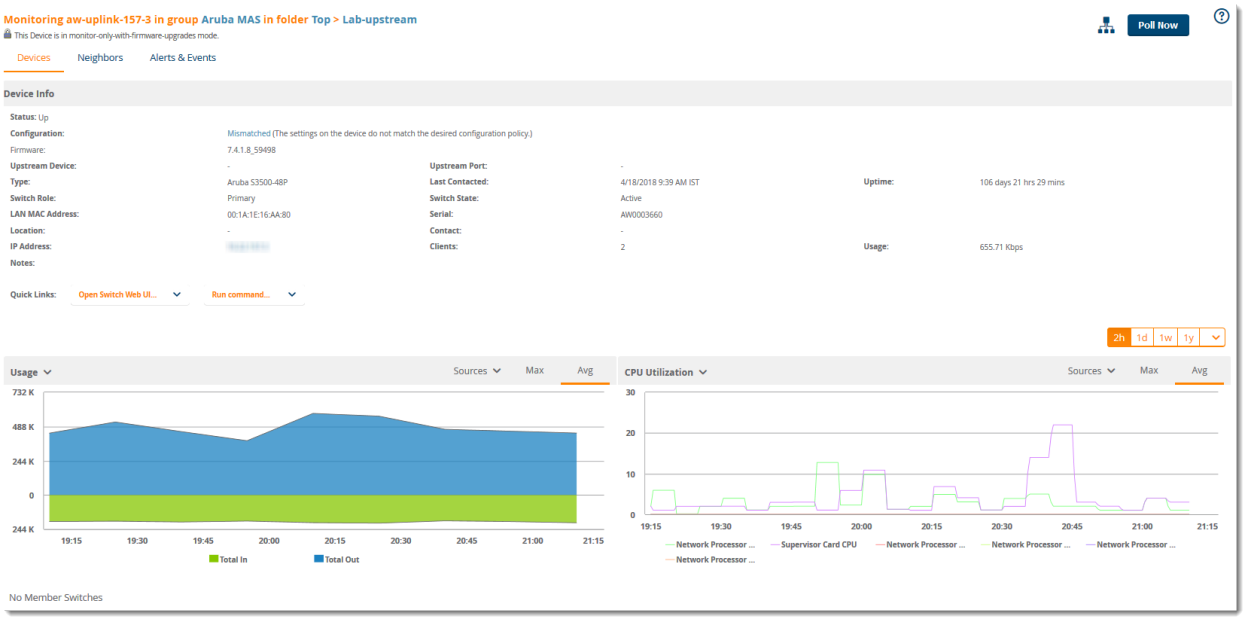
You must log in as the admin user to access the Manage page.

Devices > Monitor Page

Used in conjunction with the **Manage** page, the **Monitor** page enables you to review switch information, such as the following:

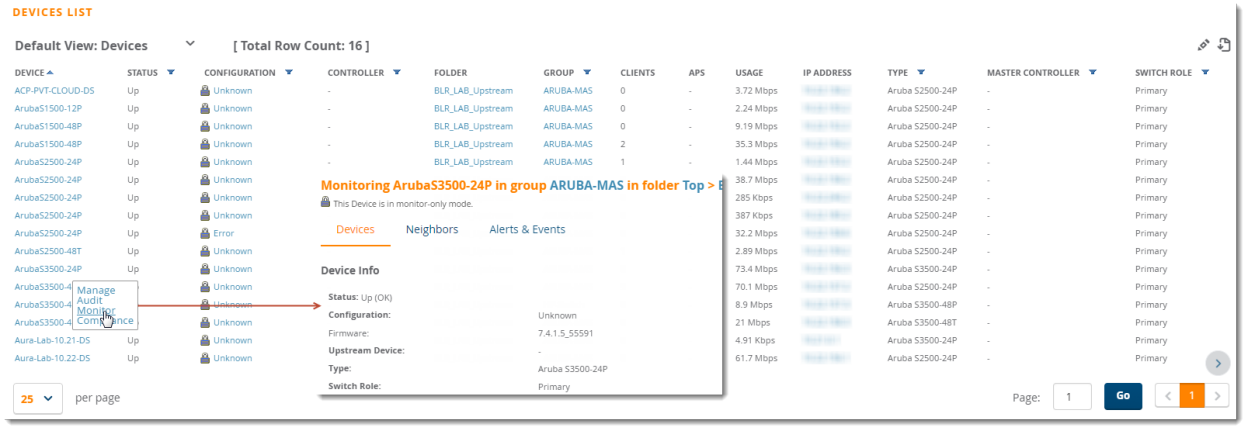
- Status
- Usage, CPU utilization, memory utilization, and clients graphs
- Alert summaries and device events
- Audit Log
- Switch role, state, and stack membership

Figure 4: *Devices > Monitor Page*



To access the monitoring page, navigate to **Devices > List** and select a device from the list. Or, you can hover the pointer over a device and click **Monitor** from the shortcut menu.

Figure 5: *Opening the Monitoring Page for a Device*



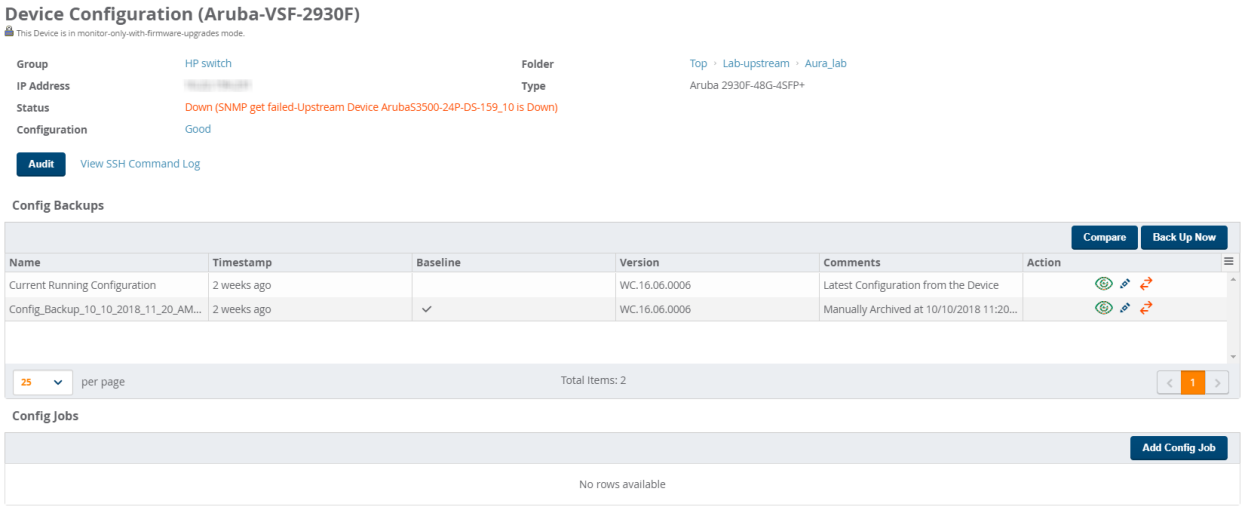
For additional information, refer to "Pushing Device Configurations to Mobility Access Switches" on page 1.

Devices > Device Configuration Page

AirWave makes it easier to troubleshoot switch problems with the **Devices > Device Configuration** page (see Figure 6).

To access the Device Configuration page, navigate to **Devices > List**, right-click the device in the Devices List, and then select **Config** from the shortcut menu. Or you can navigate to **Devices > Config**.

Figure 6: *Device Configuration Page*



The main components of the Device Configuration page include:

- Device Configuration summary. You can view information about the device group and folder the switch belongs to, details, configuration status, and configuration template. Click **Configuration** to compare configurations, the **device name** to access the group template, and **Audit** to run a configuration audit on the switch.
- Config Backups table. Each switch will have an active baseline configuration.

  From the table, you can locate the current running configuration, or a configuration backup and then:

  - Click to view the switch configuration.
  - Click to change the name of the configuration, add comments, or make the selected configuration backup the baseline.
  - Click to restore from the backup.

- Click **Compare** to compare the device configuration against its own configuration or a second switch configuration.
- Click **Back Up Now** to back up a running configuration job.

- Config Jobs. You can click **Add Config Job** at the bottom of the Device Config page to open a pop-up window, where you can select config snippets to run a configuration command on a switch.

Groups > Switch Config

If **Use Global Aruba Configuration** in **AMP Setup > General > Device Configuration** is set to **No**, the **Groups > Switch Config** page becomes available.

You can configure switching profiles on the Switch Config page. Each of the profiles is explained in "Mobility Access Switch Reference" on page 49.

Switch Configuration Tasks

Here are some of the switch configuration tasks you can do:

- Access switch information for rebooting and re-provisioning. For more information, see "Devices > List Page" on page 9.
- Push device configurations to the switch. For more information, see "Devices > Manage Page" on page 10 and "Scheduling Configuration Changes" on page 1.
- Monitor and review switch settings. For more information about the switch settings, see "Devices > Monitor Page" on page 11.
- Run a configuration audit, compare configuration backups, and restore from a configuration backup. For information about these switch management features, see "Devices > Device Configuration Page" on page 12.
- Change the way AirWave runs the audit configuration. For more information, see "Changing the Audit Configuration Setting" on page 14.
- Restore the running configuration from a backup. For more information, see "Restoring a Configuration without a System Reboot" on page 14.
- Configure switching profiles for the Aruba Mobility Access Switch. For information about switching profiles, see "Mobility Access Switch Reference" on page 49.

Scheduling Configuration Changes

You can schedule deployment of Mobility Access Switch Configuration edits to minimize impact on network performance. For example, configuration changes can be accumulated over time by using **Save and Apply** for devices in **Monitor Only** mode, then pushing all configuration changes at one time by putting devices in **Manage** mode. Refer to "Pushing Device Configurations to Mobility Access Switches" on page 1.

If your switches are already in **Manage Read/Write** mode, you can schedule the application of a single set of changes when clicking **Save and Apply**; just enter the date/time under **Scheduling Options** and click **Schedule**.

AirWave pushes configuration settings defined in the AirWave WebUI out to the Aruba Mobility Access Switches as a set of CLI commands using Secure Shell (SSH). A switch reboot is not required.

Auditing and Reviewing Configurations

AirWave supports auditing or reviewing in these ways:

1. You can review the ArubaOS running configuration file. This is configuration information that AirWave reads from the device.

2. You can use the **Devices > Device Configuration** page for device-specific auditing.
3. Once you review the configuration audit, navigate to **Devices > Device Configuration**.
4. Click **Import** to import the switch's current settings into the AirWave group's desired settings.

Changing the Audit Configuration Setting

You might want to change the way AirWave runs the audit configuration if you want to compare a configuration using a template instead of a baseline configuration. By default, AirWave runs the configuration audit for a newly created group using a baseline configuration.

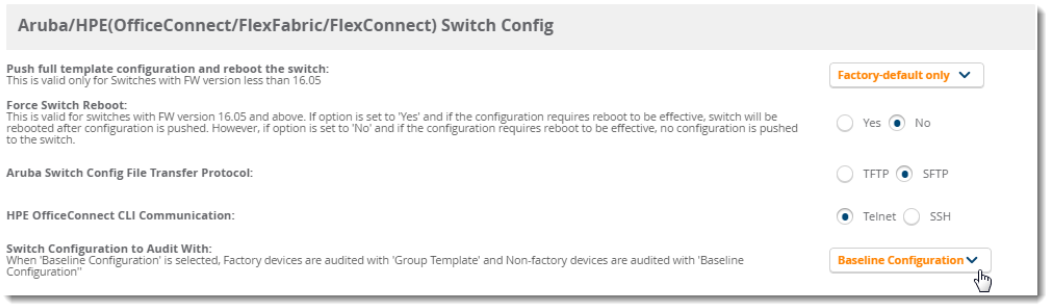
NOTE

When you set the audit configuration method to baseline configuration, AirWave will audit non-factory devices using the baseline configuration and non-default devices using the group template.

To change the audit configuration setting:

1. Navigate to **Groups > List**.
2. Select a group of Aruba switches, then navigate to **Groups > Basic**.
3. Scroll down to the Aruba/HPE OfficeConnect Switch Config section.
4. Select **Baseline Configuration**.

Figure 7: *Changing the Configuration Management Setting*



Restoring a Configuration without a System Reboot

Starting from AirWave 8.2.6, AirWave allows you to restore a configuration as the running configuration without rebooting the system using the `cfg-restore` command. This command supports both TFTP and SFTP protocols.

Only Aruba switches running ArubaOS-Switch 16.05 or later support this feature.

About Factory Default Devices

AirWave considers a switch to be factory default if:

- Only VLAN 1 exists on the switch
- VLAN 1 is using DHCP
- IPv6 is not enabled on VLAN 1

NOTE

When the switch is part of a HPE Virtual Switching Framework (VSF) stack, AirWave supports config restore with the following limitations: you can't use the `cfg-restore` command to remove physical devices, stack members, modules, or flex modules, or to provision stack members, modules, or flex modules. Config changes which cause stack members to renumber aren't supported.

NOTE

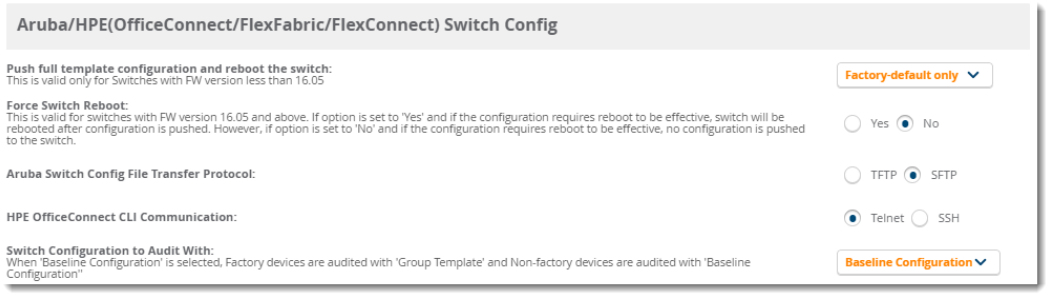
A factory default switch running ArubaOS-Switch 16.05 or later with its device state set to "Factory" will reboot on pushing the golden config from AirWave for the first time, independent of the "Force Switch Reboot" option on the **Group > Basic** page.

Enabling Config Restore Without a Reboot

To enable config restore without a reboot:

1. Navigate to **Groups > List**.
2. Select a group of Aruba switches, then go to **Groups > Basic**.
3. Scroll down to the Aruba/HPE Switch Config section.
4. Select **No** to disable the **Force Switch Reboot** option.

Figure 8: *Disabling the Force Switch Reboot Option*



5. Click **Save and Apply**, then click **Apply Changes Now** to save your settings.

Editing the Group Template

If you are editing the template to create new SNMPv3 users, add those lines below the SNMPv3 engineid line to create the user successfully with user defined credentials. Provide the SNPv3 user in double quotes in the template to match with the running config.

For example, type:

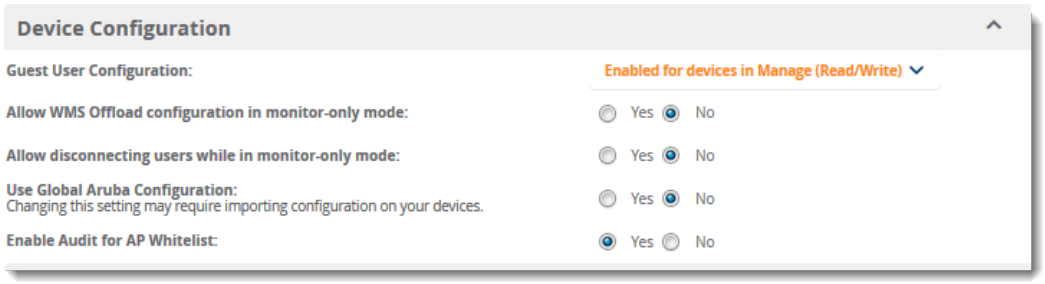
```
snmpv3 engineid "%snmpv3_engineid%"
snmpv3 enable
snmpv3 user “suser” auth md5 AirWave123 priv des AirWave123
snmpv3 group managerpriv user "suser" sec-model ver3
```

Disable Global Configuration

By default, global configuration is enabled. If you want to push a device configuration to the Aruba/HPE switch in AirWave, you must disable global configuration and include the switch in a device group. When these conditions are met, the **Switch Config** page becomes available.

To disable the **Use Global Aruba Configuration** option:

1. Go to **AMP Setup > General**.
2. Click **Device Configuration** to access the configuration options.
3. Select **No** to disable the **Use Global Aruba Configuration** option.

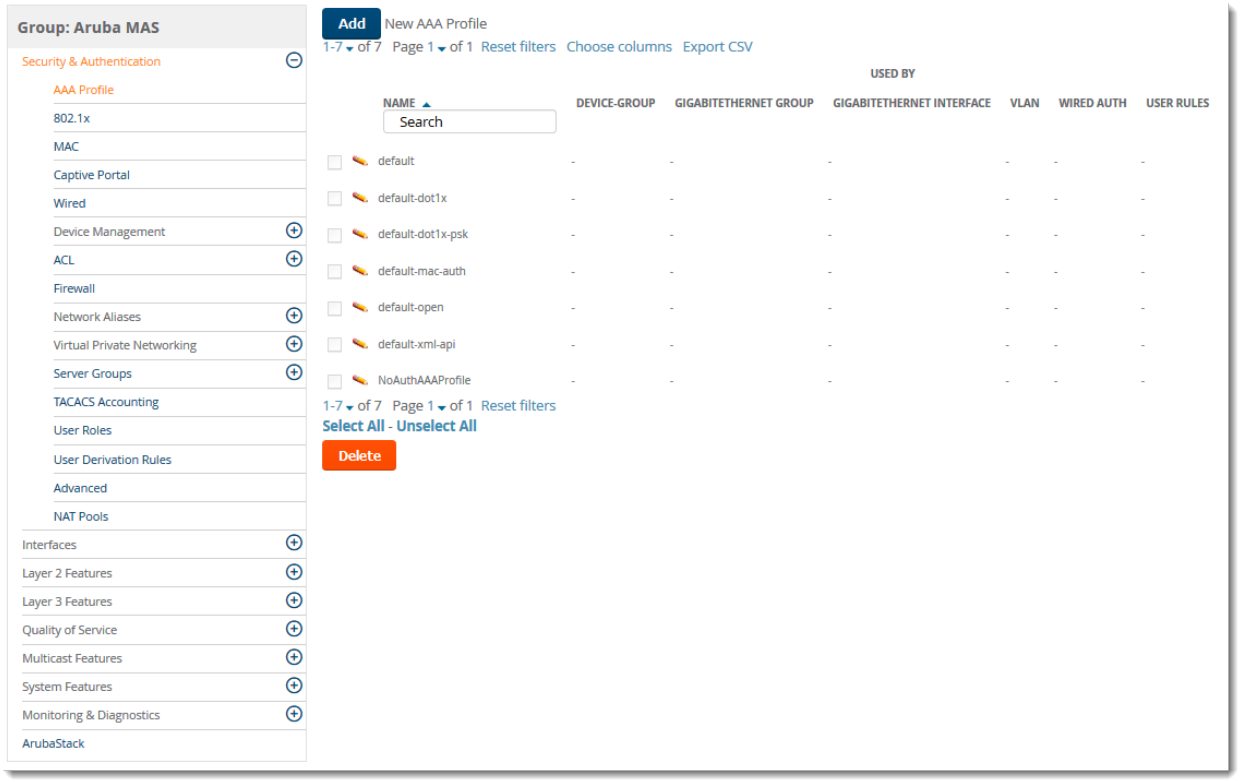


4. Click **Save**.

5. To confirm your changes, navigate to **Groups > List**, then select the group that contains the Aruba/HPE switch from the list of device groups. The **Switch Config** page becomes available in the navigation sidebar.

Figure 9 shows an example S**witch Config** page for a group called **Aruba MAS**.

Figure 9: *Switch Config Page for a Group of Mobility Access Switches*



Configuring IPv6 Monitoring

If using IPv6 for Aruba/HPE switches, then you need to configure AirWave for IPv6 addresses on the switch. AirWave supports only full config, config jobs, and ZTP for IPv6 addresses.

To configure IPv6 monitoring:

1. Go to **AMP Setup > Network**.
2. Select Yes for the IPv6 Enabled option.
3. Enter the IPv6 addresses.

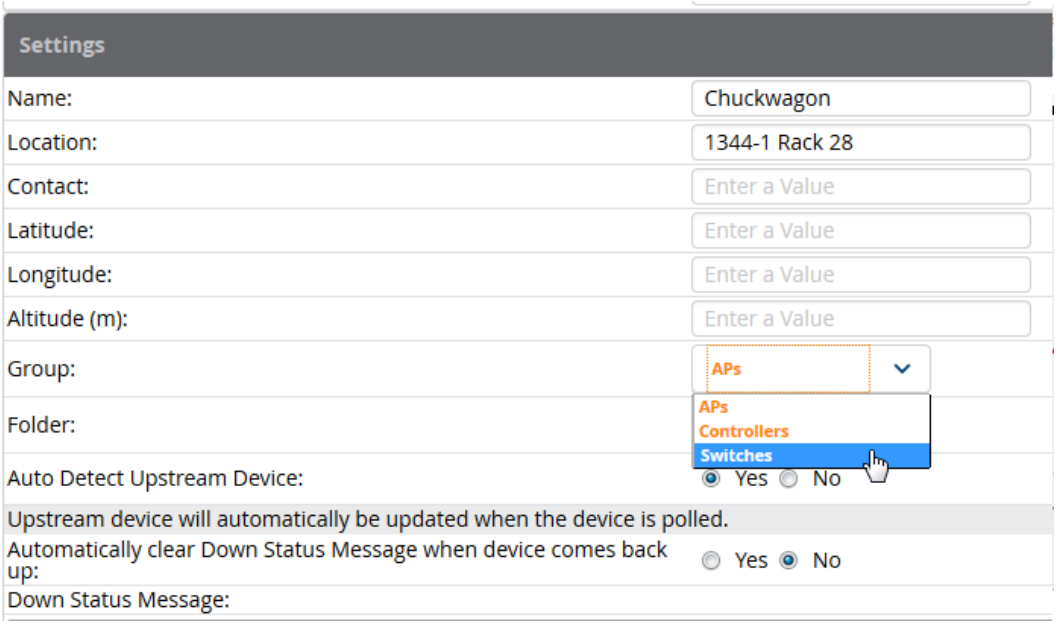
Moving Switches to a New Group

AirWave 8.2.11.1 does not allow Aruba/HPE switches and controllers to reside in the same group.

You can move the switches from one group to another group using the following method:

1. Navigate to **Devices** page and click on the **List** tab.
2. Click on the Mobility Access Switch that you want to move from one group to another group.
3. Click on the **Manage** tab.
4. From the **Group** drop-down under **Settings**, select the group name to which you want to move the switch.
5. Click **Save and Apply**.

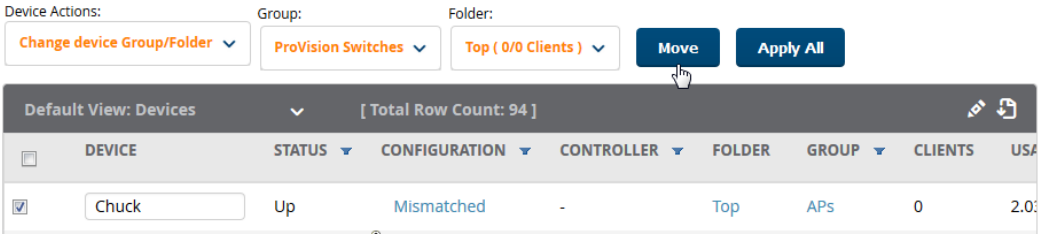
Figure 10: *Moving Switch to New Group - AP/Devices > Manage*



You can also move switches between groups using the following alternate, method:

1. Navigate to **Devices** > **List**.
2. Click the **Modify Devices** ( ) icon in the titlebar of the devices list table.
3. From the devices list, select the checkbox next to the switches that you want to move.
4. Select the group to which you want to move the selected devices from the **Group** drop-down.
5. Click **Move**.

Figure 11: *Moving Switch to New Group - AP/Devices > Manage*



Importing Profiles for Switch Configuration

Please perform the following steps to import switching profiles.

1. Navigate to the **Groups** page and select the group that includes your switches. Be sure that this group does not also include controllers. If it does, then the switches should first be moved to a separate group.
2. On the **Monitor** page, click on **Modify Devices**.
3. Select your existing switches. Be sure that the configuration status is not "Mismatched." Refer to the *AirWave8.2 Getting Started Guide* for information on how to resolve mismatches.
4. Click the **Import Settings** button. This import will enable the Switch Config page and populates the page with existing profiles.

Auditing Your Device Configuration

You can compare a configuration template with the actual configuration running on a device and view any mismatched settings on the Audit page.

The Device Configuration page is available under the following conditions:

- For all devices in a group, full configuration is enabled.
- For ZTP devices with default-factory configurations, config job is enabled.

To view the audit:

1. Go to **Devices > List**.
2. Hold the pointer over a device in the list and select **Audit** from the shortcut menu. Any mismatched settings on the device appear in the **Current Device Configuration** and **Desired Configuration** columns.

Monitoring Your Aruba Switches

You can monitor devices using show commands on some models of Aruba switches. For more information about switch monitoring, see the *AirWave 8.2.9 User Guide*.

To run a command:

1. Navigate to **Devices > List**, or **Groups > List**, then select a switch from the list to monitor.
2. Do one of the following to run a command;

- From the monitoring page for ArubaOS-CX or MAS Switches, select a show command from the **Run command** quick link (see Figure 12).
- From the monitoring page for an ArubaOS-Switch, click the **Troubleshooting** tab and click the Command field to select one or more commands from the drop-down list (see Figure 13).

Figure 12: *Show Commands on a MAS Switch*

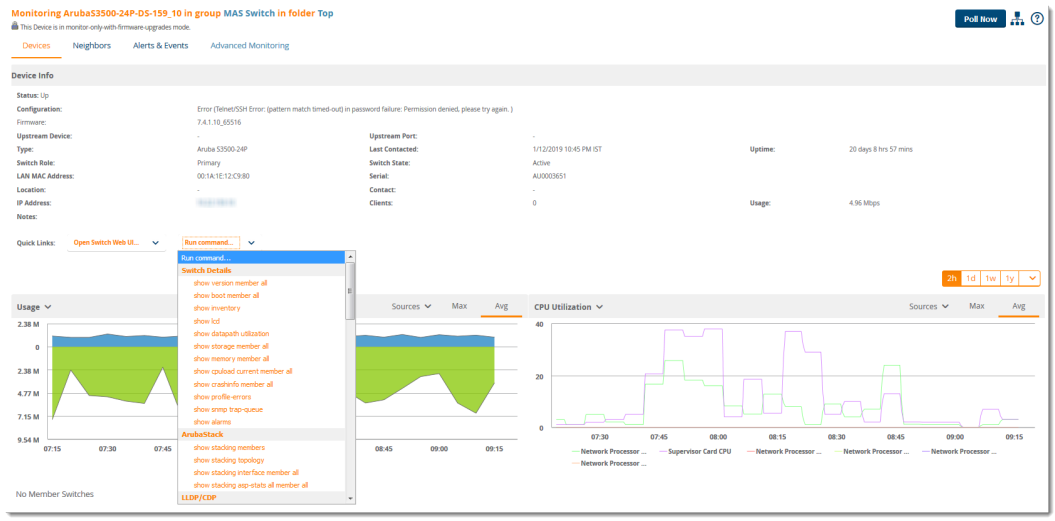
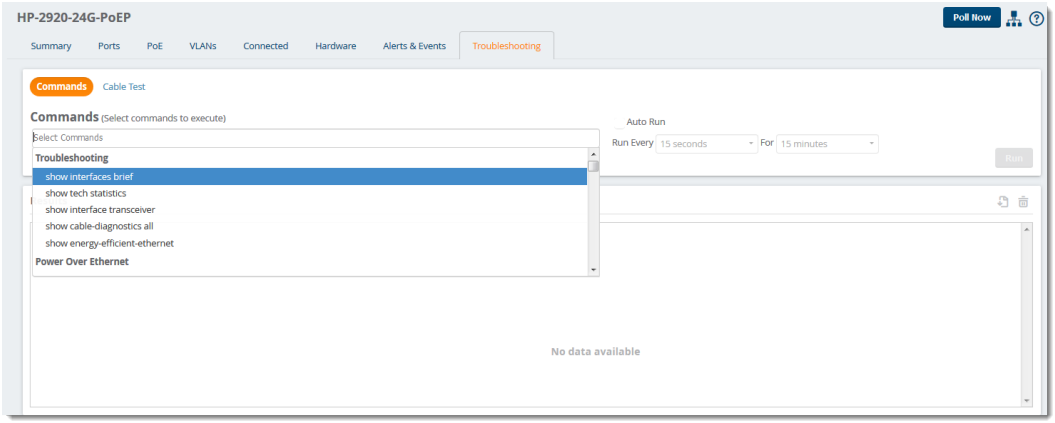


Figure 13: *Show Commands on an ArubaOS-Switch*



For complete information about the output of each command, refer to the documentation for the switch.

This chapter describes the initial setup required in order to use AirWave for the monitoring and configuration of Mobility Access Switches and Aruba Switches. You can access switch configuration features through the AirWave WebUI, although switch configuration and deployment are primarily done through the switch management interfaces (CLI or WebUI).

The first steps include configuring user roles and add discovered switches to AirWave, as described in the following sections:

- "User Roles" on page 1
- "Adding Devices into AirWave" on page 23

Creating User Roles for Switch Configuration

AirWave comes with a default admin user. The admin user can create users and assign them one or more user roles. If the user is logged in to AirWave when assigned a new role, in order to get their new privilege, the user must log out and log in again.

For more information about specific user roles and security profiles required for switch configuration, see "Security and Authentication" on page 49 and "Security and Authentication > User Roles" on page 61.

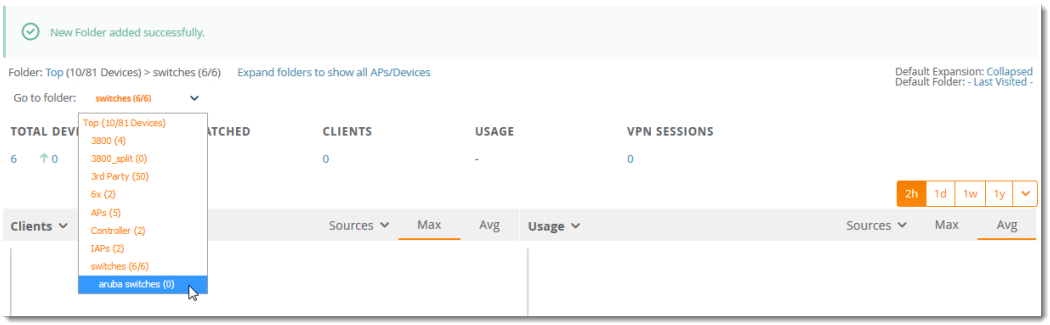
To create a user role for switch configuration:

1. Log in to AirWave as the admin user.
2. Create a AirWave device folder:
   a. Navigate to **APs/Device > List**, scroll to the bottom of the page. Or, you can go to **Users > Connected**.
   b. Click the blue **Add New Folder** link.
   c. Enter a folder name.

Figure 14: *Adding a Folder Named Aruba Switches*

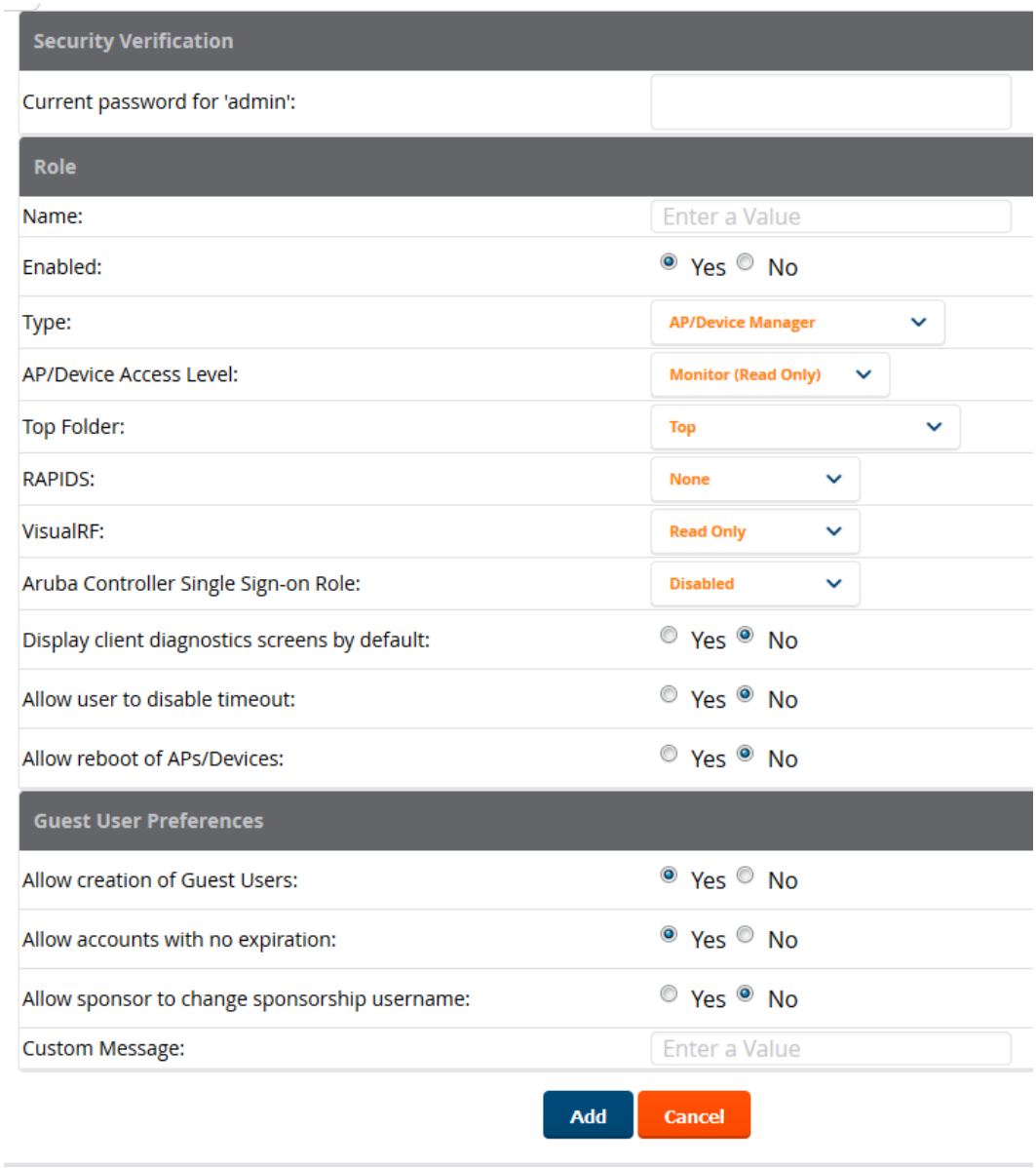
   d. Click **Add**. AirWave displays the **Devices > List** page.
   e. From the **Go to folder** drop-down list at the top left corner of the page, select the newly created folder.

Figure 15: *Selecting the New Created Folder*



3. Navigate to **Device Setup > Add** to select switches and add them to the folder. For information, see "Adding Discovered Devices to a Group or Folder" on page 26
4. Create, or edit, a user role and assign privileges that support switch configuration. At least one user must have administrative privileges. Additional users might require more restriction to sensitive information, such as SSIDs or security-related data:
   a. Navigate to the **AMP Setup > Roles** page, and click **Add New Role** to create a new role with appropriate rights, or click the **pencil** (manage) icon next to an existing role to adjust rights as required. The Role page appears, illustrated in Figure 16.

Figure 16: *AMP Setup > Roles > Add/Edit Role Page Illustration*



b. At a minimum, define the following settings:
   - **Type**—Specify the type of user. Important consideration should be given to whether the user is an administrative user with universal access, or an AP/Device manager to specialize in device administration, or additional users with differing rights and access.
   - **AP/Device Access Level**—Define the access level that this user is to have in support of Aruba controllers, devices, and general Aruba Configuration operations.
   - **Top Folder**—Specify the folder created earlier in this procedure, or specify the Top folder for an administrative user.

c. Click **Add** to complete the role creation, or click **Save** to retain changes to an existing role. The **AMP Setup** page now displays the new or revised role.

5. Add, or edit, users who will have access to folder-level access to switch configurations:
   a. Navigate to the **AMP Setup > User** page.
   b. Click **Add New User**, or click the **pencil** (manage) icon next to an existing user to edit that user.

c. Select the user role created with the prior step, and complete the remainder of this page as per standard AirWave configuration. Refer to the *AirWave 8.2.11.1 User Guide* as required.

6. Review the newly created user roles, folder permissions, and device associations.
7. Add or discover devices for the device folder defined during step 1 of this procedure.

Adding Devices into AirWave

If AirWave doesn't discover devices automatically, there are two methods of adding devices to AirWave. One is where you manually select your device type and model from the Add page. The other is where you bulk import devices from a CSV file.

Adding Devices Manually

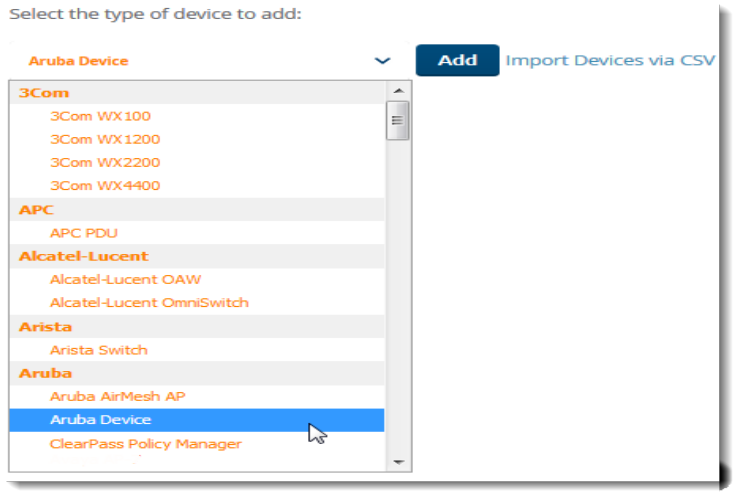
If AirWave doesn't discover devices automatically, you can manually add devices. When you add a Cisco or Aruba device, AirWave adds the make and model into its database. When you add a universal device, AirWave gets only basic monitoring information. If you don't provide SNMP credentials for the device, AirWave will monitor upstream switches, RADIUS servers, and other devices in the wired network using ICMP monitoring. Once you have added a universal device, you can view a list of its interfaces by navigating to **Devices > Manage**.

By selecting the **pencil** icon next to an interface, you can assign it to be non-monitored or monitored as Interface 1 or 2. AirWave collects this information and displays it on the **Devices > Monitor** page in the **Interface** section. AirWave supports MIB-II interfaces and polls in/out byte counts for up to two interfaces. AirWave also monitors sysUptime.

To add a device into AirWave:

1. Log in to the AirWave with the following credentials:
   - Username: admin
   - Password: *admin password*.
2. Navigate to **Devices > New**, then click **Add**.
3. From the **Device Setup > Add** page, select the device from the drop-down menu.

Figure 17: *Selecting the Device*



4. Select **Add**.
5. From the Add page, enter the device communications settings and location settings. The configuration options on this page vary depending on the device. See Table 2 for information about each setting.

NOTE

When adding an Aruba device, be sure to add controllers and switches to separate groups.

6. At the bottom of the page, set the device management mode to **Monitor Only** or **Management read/write**.

If you select **Manage read/write**, AirWave overwrites existing device settings with the **Groups** settings. Place newly discovered devices in **Monitor read/only** mode to enable auditing of actual settings instead of Group Policy settings. For more information, see "Management Modes" on page 1.

7. Select **Add** to finish adding the device to the network.

Table 2 describes the settings on the Add Page.

Table 2: *Device Communication and Location Fields and Default Values*

Setting	Default	Description
Name	None	User-configurable name for the AP (maximum of 20 characters).
IP Address	None	IP address of the device (required). AirWave supports IPv4 and IPv6 addresses.
SNMP Port	161	The port AirWave uses to communicate with the AP using SNMP.
SSH Port	22	For devices that support SSH, specify the SSH port number.
Community String (Confirm)	Taken from **Device Setup > Communication**	Community string used to communicate with the AP. **NOTE:** The **Community String** should have RW (Read-Write) capability. New, out-of-the-box Cisco devices typically have SNMP disabled and a blank user name and password combination for HTTP and Telnet. Cisco supports multiple community strings per AP.
SNMPv3 Username	Taken from **Device Setup > Communication**	User name of the SNMP v3 user on the controller. If you are going to manage configuration for the device, this field provides a read-write user account (SNMP, HTTP, and Telnet) within the Cisco Security System for access to existing APs. AirWave initially uses this user name and password combination to control the Cisco AP. AirWave creates a user-specified account with which to manage the AP if the **User Creation Options** are set to **Create** and user specified as User.
Auth Password	Taken from **Device Setup > Communication**	SNMPv3 authentication password. **NOTE:** SNMPv3 supports three security levels: (1) no authentication and no encryption, (2) authentication and no encryption, and (3) authentication and encryption. AirWave currently only supports authentication and encryption.
Privacy Password (Confirm)	Taken from **Device Setup > Communication**	SNMPv3 privacy password. **NOTE:** SNMPv3 supports three security levels: (1) no authentication and no encryption, (2) authentication and no encryption, and (3) authentication and encryption. AirWave currently only supports authentication and encryption.

Table 2: *Device Communication and Location Fields and Default Values (Continued)*

Setting	Default	Description
SNMPv3 Auth Protocol	Taken from **Device Setup > Communication**	Specifies the SNMPv3 auth protocol, either MD5 or SHA-1.
SNMPv3 Privacy Protocol	Taken from **Device Setup > Communication**	Specifies the SNMPv3 Privacy protocol as either DES or AES. This option is not available for all devices.
Telnet/SSH Username	Taken from **Device Setup > Communication**	Telnet user name for existing Cisco IOS APs. AirWave uses the Telnet user name/password combination to manage the AP and to enable SNMP if desired. **NOTE:** New, out-of-the-box Cisco IOS-based APs typically have SNMP disabled with a default telnet user name of **Cisco** and default password of **Cisco**. This value is required for management of any existing Cisco IOS-based APs.
Telnet/SSH Password (Confirm)	Taken from **Device Setup > Communication**	Telnet password for existing Cisco IOS APs. AirWave uses the Telnet user name/password combination to manage the AP and to enable SNMP if desired. **NOTE:** New, out-of-the-box Cisco IOS-based APs typically have SNMP disabled with a default telnet user name of **Cisco** and default password of **Cisco**. This value is required for management of any existing Cisco IOS-based APs.
enable Password (Confirm)	Taken from **Device Setup > Communication**	Password that allows AirWave to enter **enable** mode on the device.

Adding Devices from a CSV File

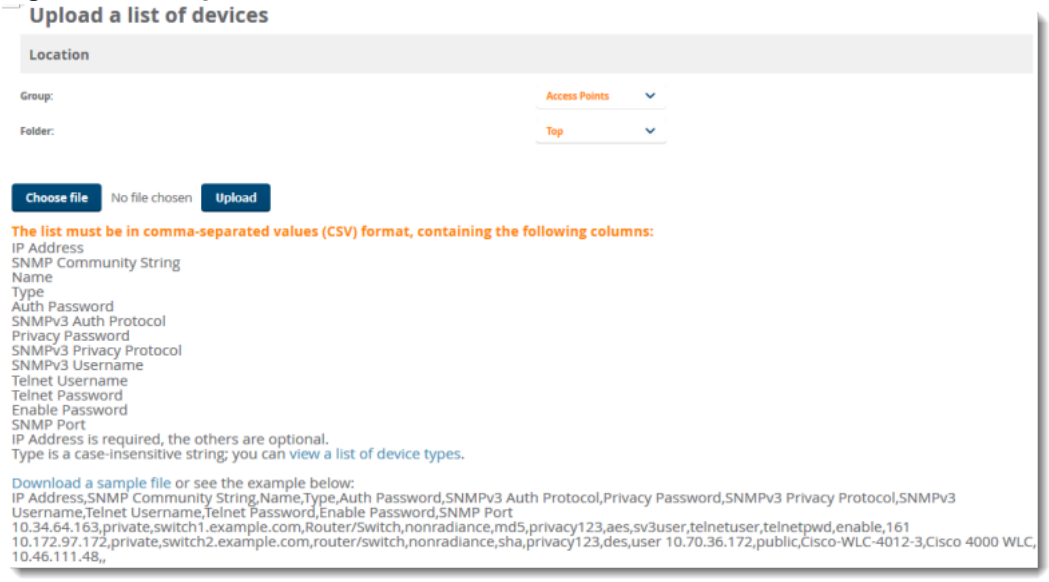
You can use a CSV file to bulk add devices to AirWave. If you specify the vendor name, AirWave automatically determines the correct type while bringing up the device. If your CSV file includes make and model information, AirWave will add the information provided in the CSV file as it did before. AirWave will not override what you have specified in this CSV file in any way.

Use the example provided on the bottom of the page, or click the blue "Download a sample CSV file" link to save the sample as a CSV file and edit the contents with an external application.

To import a CSV file:

1. From the **Device Setup > Add** page, click the blue **Import Devices via CSV** link. The **Upload a list of devices** page displays. See Figure 18.

Figure 18: *Adding Devices from CSV File*



2. Select a group and folder into which to import the list of devices.
3. Click **Choose File** to select the CSV file on your computer.
4. Click **Upload** to add the devices from the list into AirWave.

Adding Discovered Devices to a Group or Folder

When you add devices to AirWave and then put them into groups, AirWave supports group-level monitoring of those devices. You can use folders to manage settings for multiple devices.

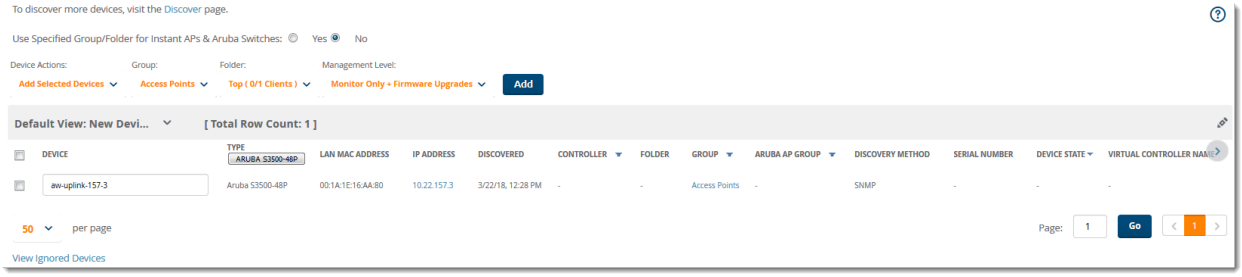
NOTE

Devices cannot be added to a Global Group because groups designated as "Global Groups" cannot contain access points.

To add the discovered device to a group or folder:

1. Navigate to **Devices > New** to make your device selections from the New Devices list. If you specified a different location while defining a scan set, AirWave displays new devices here.

Figure 19: *Adding the Switch to a Group or Folder*



2. Select the **Add Selected Devices** option, and the group and folder you want to add the devices to using the drop-down menus. For ZTP devices, you can add only one device at a time to a device group.
3. Select the management mode:
   - **Monitor Only + Firmware Upgrades**. AirWave will update the firmware, compare the current configuration with the policy, and display any discrepancies on the **Devices > Audit** page. AirWave will not make configuration changes.

- **Manage Read/Write**. AirWave will compare the device's current configuration settings with the group configuration settings and automatically update the device's configuration to match the group policy.

You should put devices into **Monitory Only + Firmware Upgrades** mode when adding them to a newly established device group to avoid overwriting important existing configuration settings.

4. Click **Add**. For non-factory, ZTP devices, AirWave will prompt you for the community string, Telnet/SSH user name and password, and the enable password in order to import the device configuration immediately after the device is added to the group
5. Navigate to **Devices > List** page to verify that the devices have been assigned to the correct folder.

About ZTP Devices

Aruba Activate enables zero touch provisioning (ZTP) of Mobility Access Switches by associating the devices to the configuration master (the AirWave server) from which they can retrieve their configurations. When the Mobility Access Switch connects to the AirWave server, AirWave will either assign the provisioned device to a specified group if at least one device exists in the group with the same shared secret. If the provisioned device doesn't have the same shared secret and group, AirWave will place the device on the New Devices list.

For more information about the basic provisioning workflow and provisioning rules, see the *Aruba Activate User Guide*.

Golden Configuration

The first device that is added to an AirWave group manually through the New Devices List becomes the "golden" configuration for all subsequent devices added to the group. Ensure the stability of this configuration before pushing it to subsequent devices in the group.

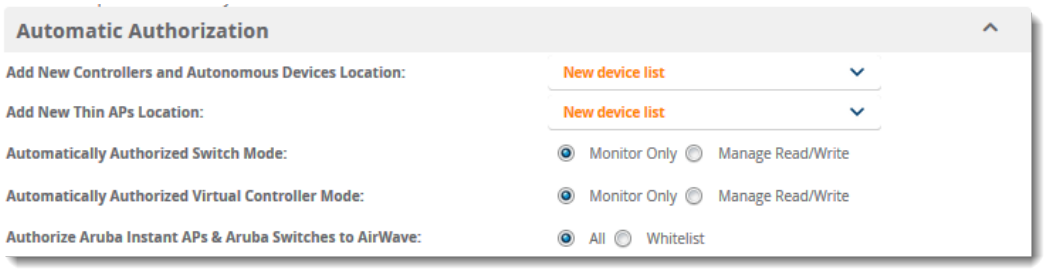
When adding this first device to AirWave, you must log in as an Admin user or provide the admin password in the device's Management profile. This is required in order to change the admin password of the factory default switch so that the configuration can be written and pushed to AirWave.

Automatically Authorized Switch Mode Option

You can configure AirWave to automatically set the management mode for newly added devices to **Monitor Only** or **Manage Read/Write**.

To enable this feature, go to **AMP Setup > General**.

Figure 20: *Automatic Authorization setting in AMP Setup > General*



The first device added to AirWave and whose configuration is imported will display with a "Good" configuration state regardless of the **Automatically Authorized Switch Mode** setting.

After a Mobility Access Switch appears as an associated device on the AirWave server, future configuration changes on the device must be made through AirWave. A message will appear on the AirWave UI to indicate a mismatch in configuration, if you attempt to make configuration changes directly on a switch that is managed by AirWave.

You can push configuration changes to a Mobility Access Switch after initial device configuration immediately to devices that are in Manage Read/Write mode, or store incremental changes to devices that are in Monitor Only mode and push the changes later. This chapter describes both methods.

For a complete reference on all Configuration pages, field descriptions, and additional procedures, refer to "Mobility Access Switch Reference" on page 49.

Push Configurations Immediately

In order for AirWave to push a configuration to a device, the device must be in **Manage Read/Write** mode.

To push device configuration changes immediately:

1. From the **Switch Config** pages, make the device changes.
2. Click **Save and Apply**. AirWave pushes the configuration changes to the device.

Store Configuration Changes to Push Later

You can push several configuration changes to the switch while it is in **Monitor Only** mode, and then change the management mode to **Manage Read/Write** when you are ready to push an entire set of device configurations.

To push multiple device configurations at once to the switch:

1. From the **Switch Config** pages, make all device changes, then click **Save and Apply** each time you complete a device-level change.
2. Review the entire set of mismatched devices on the **Devices > Mismatched** page.
3. Navigate to the **Devices > Device Configuration** page to review recent configuration changes for the device.
4. After verifying that all mismatched device configurations are correct, click **Modify Devices** link on the **Groups > Monitor** page to put the device into **Manage Read/Write** mode and push the pending device configurations to the switch.
5. Change the management mode back to **Monitor Only**.

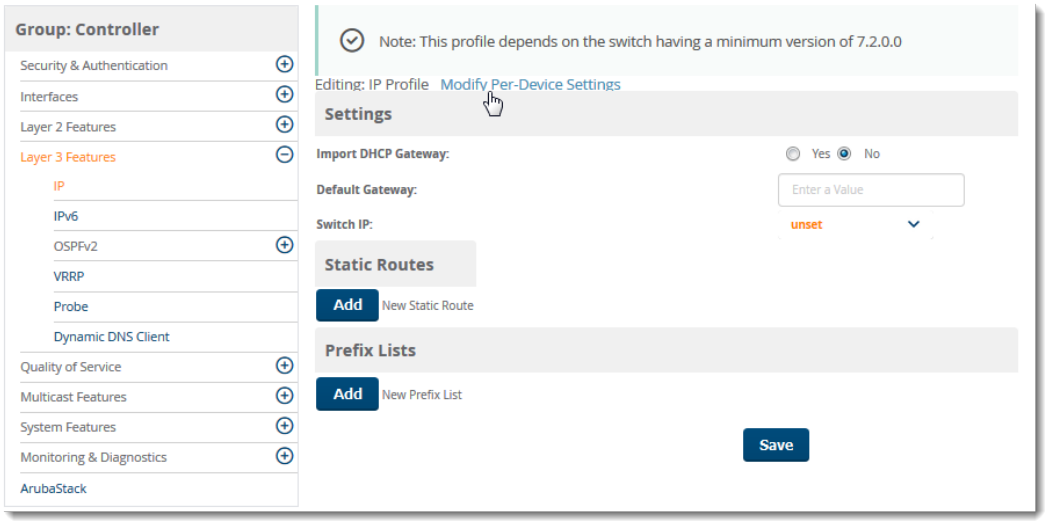
Modify Device Settings

You can bulk edit device settings for switches in a group.

To bulk edit device settings for switches:

1. Navigate to **Groups > List**, then select the group of switches.
2. Go to **Groups > Switch Config**.
3. From **Layer 3 Features** menu, select **IP** to open the Editing IP Profile page.
4. Click the **Modify Per-Device Settings** link. The Editing IP Profile window opens with a list of approved devices.

Figure 21: *Accessing the Editing IP Profile Window*



5. Enter the settings to be pushed from the AirWave server to each device.

Figure 22 shows an example of the Editing IP Profile window.

Figure 22: *Bulk Editing Switch Profiles*

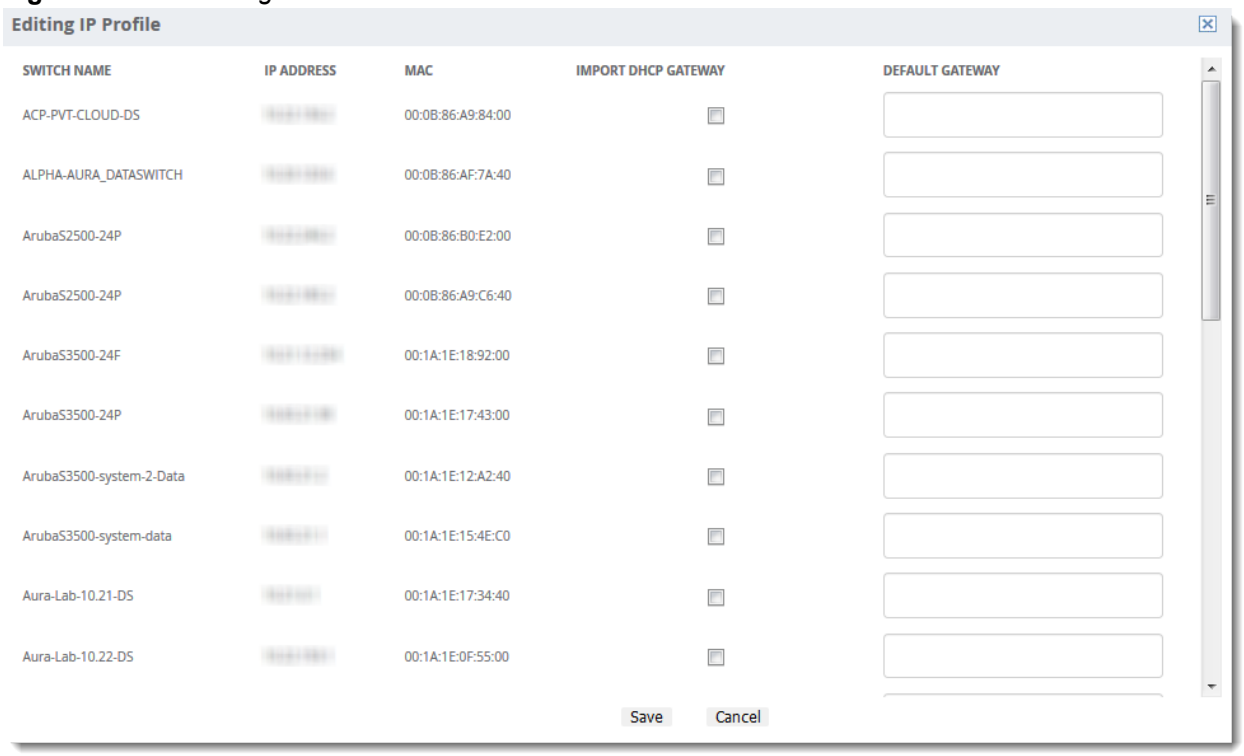


Table 3 lists the switch profiles and fields that AirWave supports.

Table 3: *Profiles supported for Per Device Settings*

Supported Profiles	Supported Fields
Layer 2 Features->Routed VLAN Interfaces	• VLAN Interface ID, IP Address, • IP Netmask, • Secondary IP Address, • Secondary IP Netmask
Layer 3 Features->IP	• Default Gateway
Interface->Loopback	• IP Address
Interfaces->GigabitEthernet Group	• Interfaces
Security & Authentication->Virtual Private Networking->Site-Site VPN->Site-Site IKE Shared Secrets	• IKE Shared Secret, • IP Address, • Subnet Mask
Security & Authentication->Virtual Private Networking->IPSEC->IPSEC Map	• Source Network Address, • Source Network Mask, • Local FQDN ID for Aggressive Mode • Peer Gateway IP Address
System Features->DHCP->Server	• DHCP Server Pool IP Address
System Features->DHCP->Server->Default Router Addresses	• Default Router Address

AirWave lets you push configurations to Aruba switches using zero touch provisioning (ZTP) and configuration templates.

NOTE

AirWave 8.2.0.x-.8.2.2.x included support for a delta configuration push, where AirWave would compare a device configuration to an AirWave template, and push CLI commands to resolve any differences. This feature has been replaced in AirWave 8.2.3 or later with snippets and variables.

Provisioning Devices with Zero Touch Provisioning (ZTP)

Zero Touch Provisioning (ZTP) for Aruba switches can be delivered through AirWave via a DHCP server.

To use ZTP, you need to:

- "Configure the DHCP Server" on page 31
- "Manually Provision the First Device with a Golden Configuration" on page 33

All subsequent devices that join the network will be automatically provisioned with the golden configuration.

NOTE

Some Aruba switches support commands that allow you to view current AirWave settings or manually configure that switch to associate to anAirWave server via the switch command-line interface. For details on these switch commands, including **amp-server** and **show amp**, refer to the documentation for that switch.

NOTE

You must enable TLS 1.0 and TLS 1.1 if you are doing ZTP with AirWave with switch firmware 16.01 and 16.02. Go to **AMP Setup > General > Additional AMP services** and set the "Disable TLS 1.0 and TLS 1.1" option to “No".

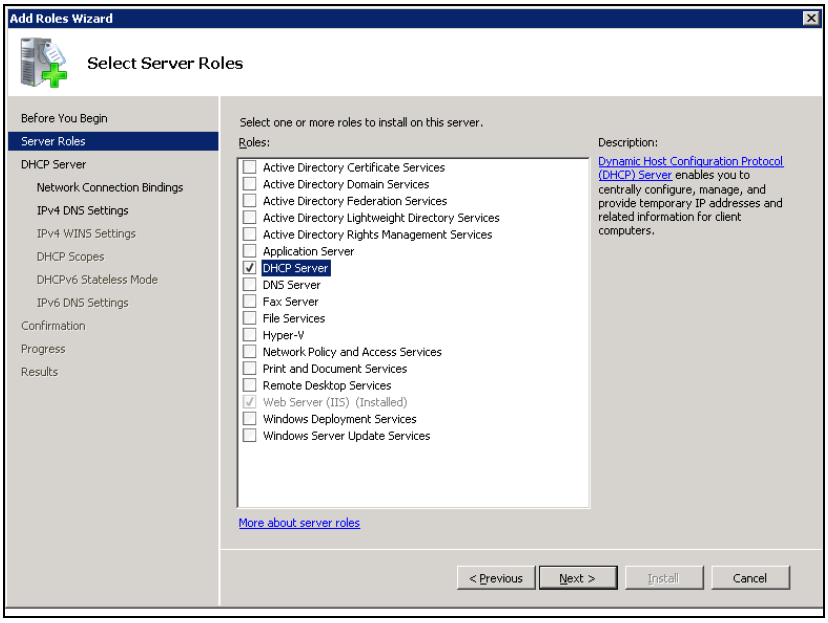
Configure the DHCP Server

The DHCP discovery message must include a NTP server address (Option 42), DHCP vendor-specific information (Option 43), and DHCP vendor class identifier (Option 60).

To configure these options on your Windows-based DHCP server:

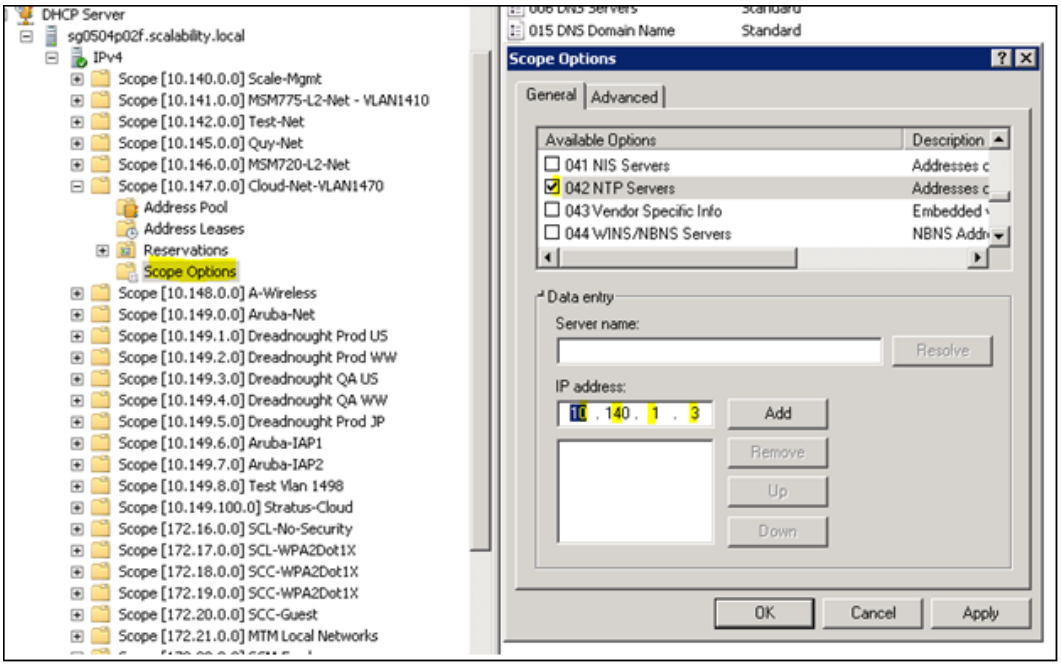
1. Add a DHCP server role.
2. From the Add Roles Wizard window, select **Server Roles** > **DHCP Server**, as shown in Figure 23.

Figure 23: *Add a DHCP Server Role*



3. Click **Next**.
4. From the Server Manager window, select **Roles > DHCP Server > the desired domain DHCP Server > IPv4** and then right-click **Scope Options** and select **Configure Option**.
5. Select **042 NTP Servers** and type the IP address of the NTP Server. For example, type 10.140.1.3 as shown in Figure 24.

Figure 24: *Configure Option 42*

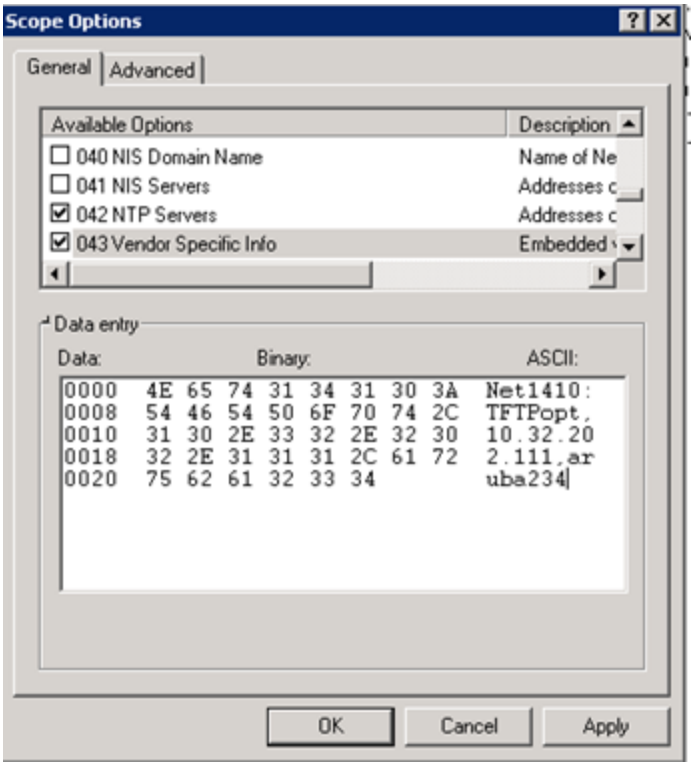


6. Click **Add**.
7. Right click **Scope Options** again and select **Configure Options**.
8. Select **043 Vendor Specific Info** and type the following AirWave configuration parameters in the **ASCII** field:

   `<Group>:<Topfolder>:<folder1>,<AMP IP>,<shared secret>`

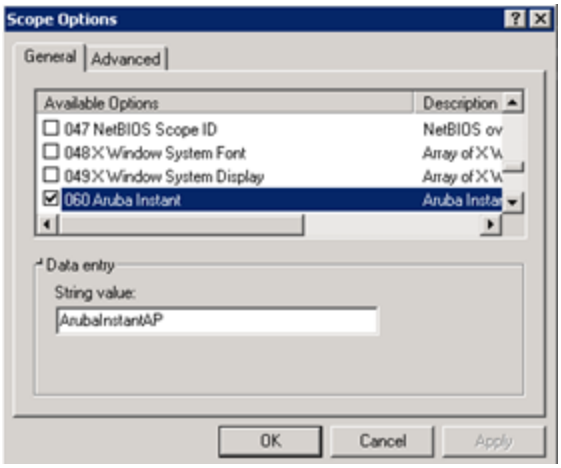
   For example, type **Net1410;TFTPopt:10.32.202.111,aruba234**, as shown in Figure 25.

Figure 25: *Configure Option 43*



9. Click **OK**.
10. Right click **Scope Options** again and select **Configure Options**.
11. Select option **060** and type **ArubaInstantAP** in the **String Value** field, as shown in Figure 26.

Figure 26: *Configure Option 60*



12. Click **OK**.

Manually Provision the First Device with a Golden Configuration

To configure the first device with a golden configuration :

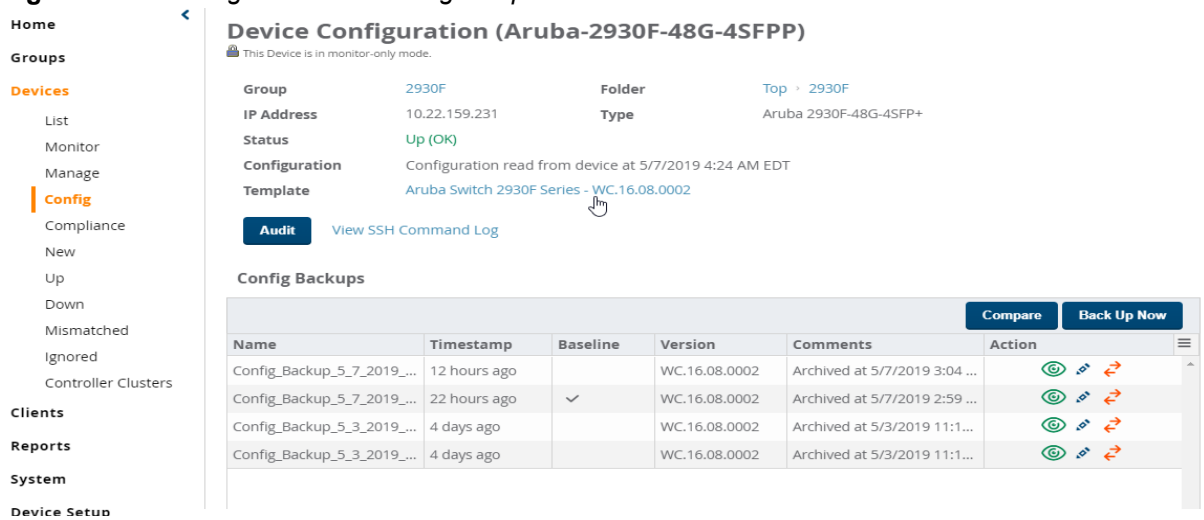
1. Add the first device to create the initial configuration, also called the golden configuration. You can do this by using DHCP, or by running the following command on the switch: `amp-server ip <ip_addr> group <group_name> folder <folder_name> secret <shared_secret>`
2. When the device status is 'Up" on AirWave, go to **Devices > Manage > Device Communication**, enter the Telnet/SSH user name and password, then confirm the password.

NOTE

Before proceeding, verify that your configuration is in a good state.

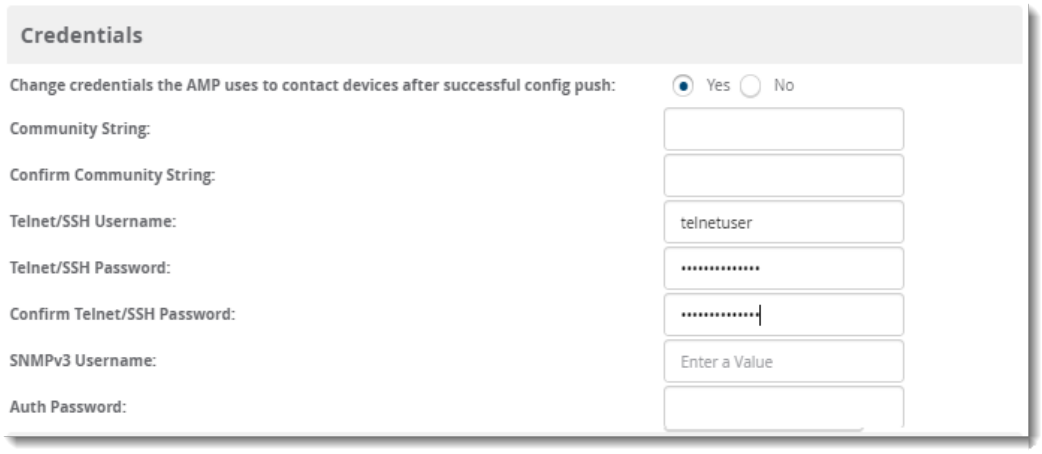
3. Navigate to the **Devices > List page**.
4. Right-click the device in the **Devices List** table, then select the blue **Config** link to open **Devices > Device Configuration** page for that device.
5. Click the blue **Template** link to open the Golden Config template (see Figure 27) . AirWave redirects you to the **Groups > Templates** page.

Figure 27: *Selecting the Golden Config Template*



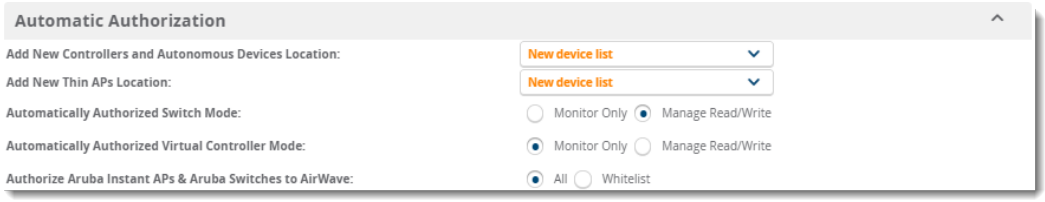
6. Scroll down to the **Credentials** section, then set the **Change credentials AMP uses to contact devices after successful config push** option to **Yes**.
7. In the credential fields that become available, you can enter a new Telnet/SSH user name and password to change the credentials AirWave uses to contact the devices (see Figure 28).

Figure 28: *Changing the Telnet/SSH Credentials*



8. Click **Save** to apply the changes.
9. Go to **AMP Setup> General**, then scroll down to the **Automatic Authorization** section and set the **Automatically Authorized Switch Mode** option to **Manage Read/Write** (see Figure 29).

Figure 29: *Enabling the Automatic Authorized Switch Mode Option*



10. Click **Save** to apply the changes. When switches with a factory-default configuration become active on the network, match the group, and have the shared secret key, the AirWave server automatically authorizes switch provisioning. The devices reboot and come online with their configuration in a good state.

Configuring Devices with Templates

AirWave can push a complete set of configuration changes to Aruba switches, and to Aruba/HPE Switches that are in factory-default state, using configuration templates. The configuration push occurs only when the management mode for all the devices in the group are set to **Manage Read/Write**.

Configuring Devices running FirmWare Version 16.01-16.04

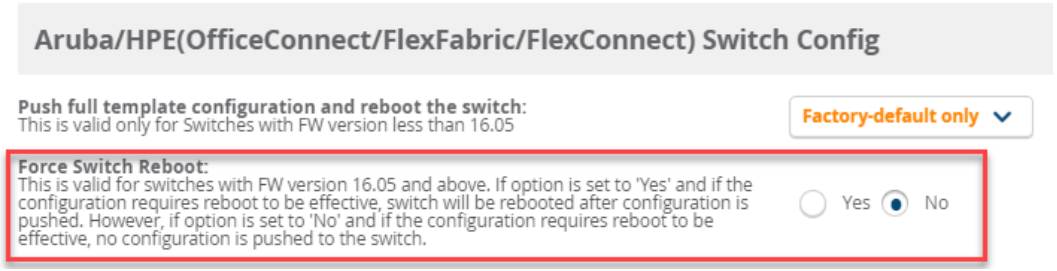
If you are doing a configuration push from AirWave to Aruba/HPE switches with firmware version less than 16.05, you must enable full template configuration. Go to **Group > List**, select a switch group, select **Basic** from the navigation menu, and set the **Push full template configuration** option to **Factory-default only**. (see Figure 30). This setting allows AirWave to push a full template configuration to new factory-default devices only, while the **yes** option will also push a full configuration and require a reboot for existing devices with non-factory-default settings.

Figure 30: *Full Template Configuration Option*

Configuring Devices running Firmware Version 16.05 or Later

If the **Force Switch Reboot** setting on the **Group > List** page is set to **Yes**, when a configuration requiring a reboot is pushed to a switch running firmware 16.05 or later, the configuration update is pushed using the **copy** command, and the switch will reboot after the config update. If the configuration change does *not* require a reboot, the configuration will not be pushed.

Figure 31: *Force Switch Reboot Option*



Alternatively, if the if the **Force Switch Reboot** setting is set to **No**, AirWave will not push a configuration update to an existing switch if that update that requires a reboot, and the switch will appear in a mismatched

state. If the configuration update does *not* require a reboot, the behavior of the AirWave server depends upon the version of AirWave.

- With the **Force Switch Reboot** setting set to **No**, AirWave 8.2.11.0 and earlier releases will still push a configuration update that does not require a reboot to an existing switch.
- With the **Force Switch Reboot** setting set to **No**, AirWave 8.2.11.1 and later releases will not push any configuration to an existing switch, regardless of whether that configuration change would require a reboot.

Note that all versions of AirWave will push a configuration to a factory-default device and allow that device to reboot, regardless of the **Force Reboot Setting**, which is not enforced for factory-default devices.

Auditing and Updating a Switch Configuration

You can choose to audit and update the configurations of groups of devices using either the **Baseline Config** option, or the **Group Template** option. When you select the **Baseline Configuration** option, the configuration template for the group is pushed to factory-default devices, and devices with non-factory-default settings are set to the baseline config. For more information on setting the **Baseline Config** or **Group Template** options, see "Changing the Audit Configuration Setting" on page 14. For details on creating a baseline config, see "Devices > Device Configuration Page" on page 12.

Table 4: *Group Configuration Options*

Audit Setting	Factory-Default Devices	Devices with Non-Factory Settings
Group Templates	The group template assigned to the device is pushed to the device.	The group template assigned to the device is pushed to the device
Baseline Config	The group template assigned to the device is pushed to the device	If a baseine configuration has been defined , it is pushed to the device. Otherwise, the current device configuration is defined as the new baseline config.

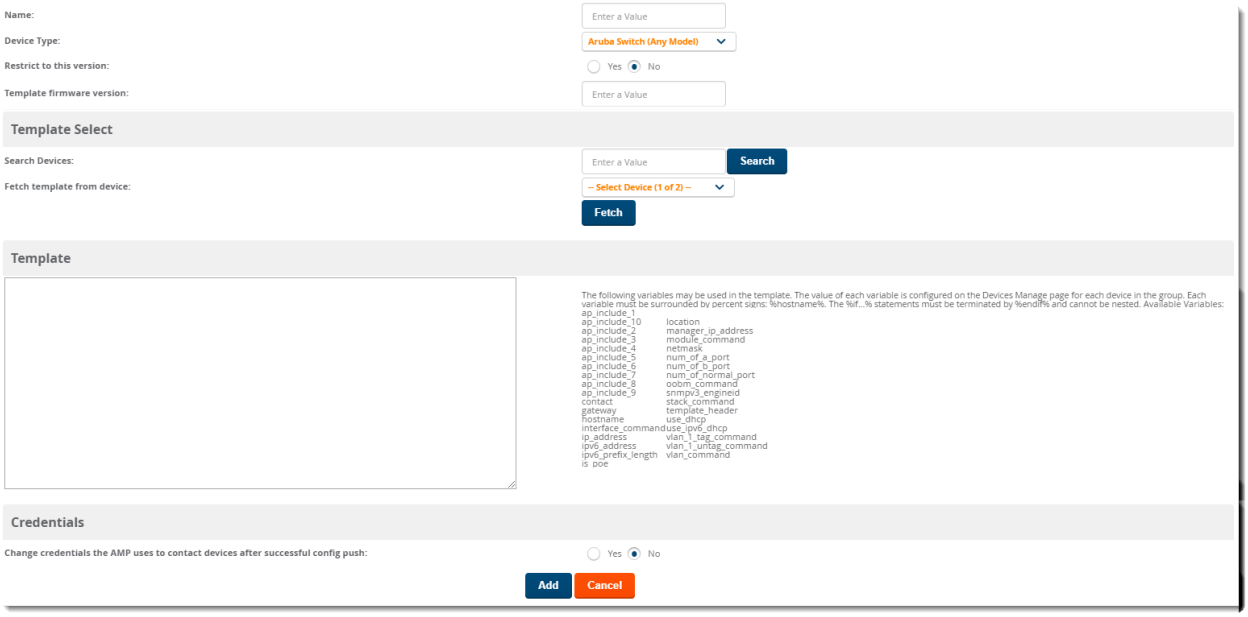
Creating Configuration Templates

You can quickly build a configuration template by using a template and modifying it.

To create a configuration template:

1. Go to the **Groups > List**, and select a device group.
2. From the AirWave navigation pane, select **Templates**.
3. In the Templates page, click **Add** (see Figure 32).

Figure 32: *Adding a Template for a Group of Aruba Switches*



4. Enter a name for the template.
5. Select the device type.
6. Enter the firmware version.
7. If you want to search for a device to fetch a template, enter a device name and click **Search**. If AirWave finds matching devices, the Fetch template from device drop-down automatically lists them.
8. Select a device from the drop-down and click **Fetch**. AirWave retrieves the configuration from the template and applies the configuration to the new template.
9. Check the **Template** field, confirming the order of the command lines and variables used in the template.
10. Modify the **Template** field, as needed, then click **Add**.

Adding Dynamic Variables to Group Templates

While creating or modifying a configuration template, you can add variables defined at the device or configuration level.

Follow these steps to configure default values for dynamic variables and add them to group templates:

1. Go to the **Groups > List**, and select a switch group.
2. From the navigation bar, click **Templates**, then scroll down the **Groups Templates Config** page to the **Template Variables** section.
3. Click **Add**, then enter the variable name and default value. The variable value can include more than one line of text. You can't use spaces, periods, or non-alphanumeric characters. . If you want to create additional variables, repeat this step for each variable.
4. Click **Save**.

Figure 33: *Adding Dynamic Template Variables*

Adding Dynamic Variables from Group Templates on the Device Manage Page

When you create a group template using dynamic variables, you can use the same dynamic variables to manage the configuration for a single device.

Follow these steps to add dynamic variables at the device-level:

1. Go to the **Device > List**, and select a device.
2. From the navigation bar, click **Manage**, then scroll down the Manage page for the device to the **Dynamic Variables** section.
3. Click **Add**, then enter the variable name and default value. The variable value can include more than one line of text. You can't use spaces, periods, or non-alphanumeric characters. . If you want to create additional variables, repeat this step for each variable.
4. Click **Save and Apply**.

Example Device-Level Variables

In the following example, **hostname**, **gateway**,and **snmpv3_engineid** are variables defined at the device level for each device receiving the template.

```
hostname "%hostname%"
include-credentials
ip default-gateway %gateway%
snmp-server community "public" unrestricted
snmp-server host 10.22.156.101 community "public"
snmpv3 engineid "%snmpv3_engineid%"
```

Example Conditional Statement

AirWave also supports conditional statements inside a template. The following example uses **use_dhcp** as a variable in an *if* statement, which allows the **ip address dhcp-bootp** command to be applied only to devices where the **use_dhcp** parameter is set to **1**.

```
%if use_dhcp=1%
ip address dhcp-bootp
%endif%
```

NOTE

For more information on adding variables to a configuration template, refer to the **Modify or Add Template Variables** section of the **AirWave API Guide**.

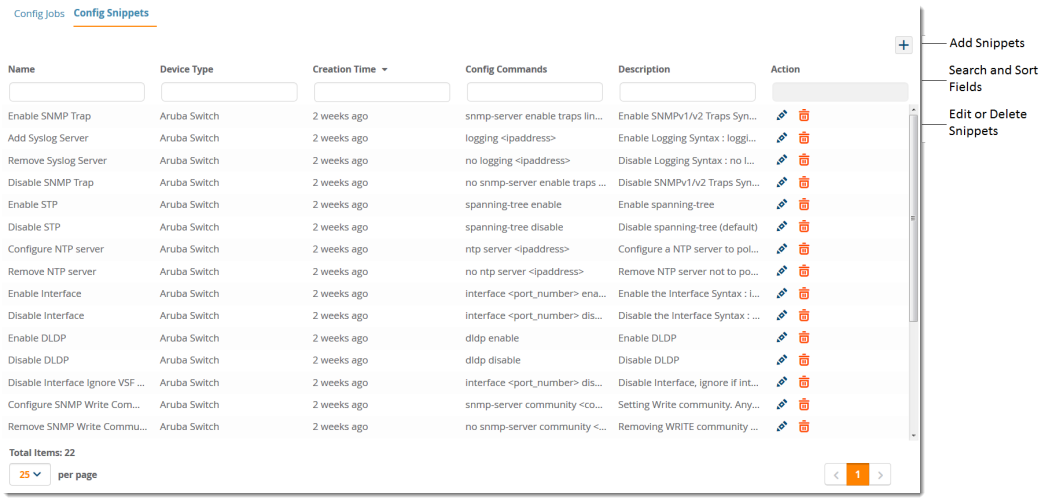
Using Snippets

You can use snippets in your config and audit jobs, or create your own snippets in a few steps. You can also use predefined snippets to build config jobs even quicker. These snippets appear in the **Snippets** tab, as shown in Figure 34. AirWave pushes the snippet to a device in monitor-only mode without the need to change the management mode of the device.

NOTE

Localization isn't available for the Snippets tab. Buttons, menus, and tabs display in English.

Figure 34: *Snippets Tab*



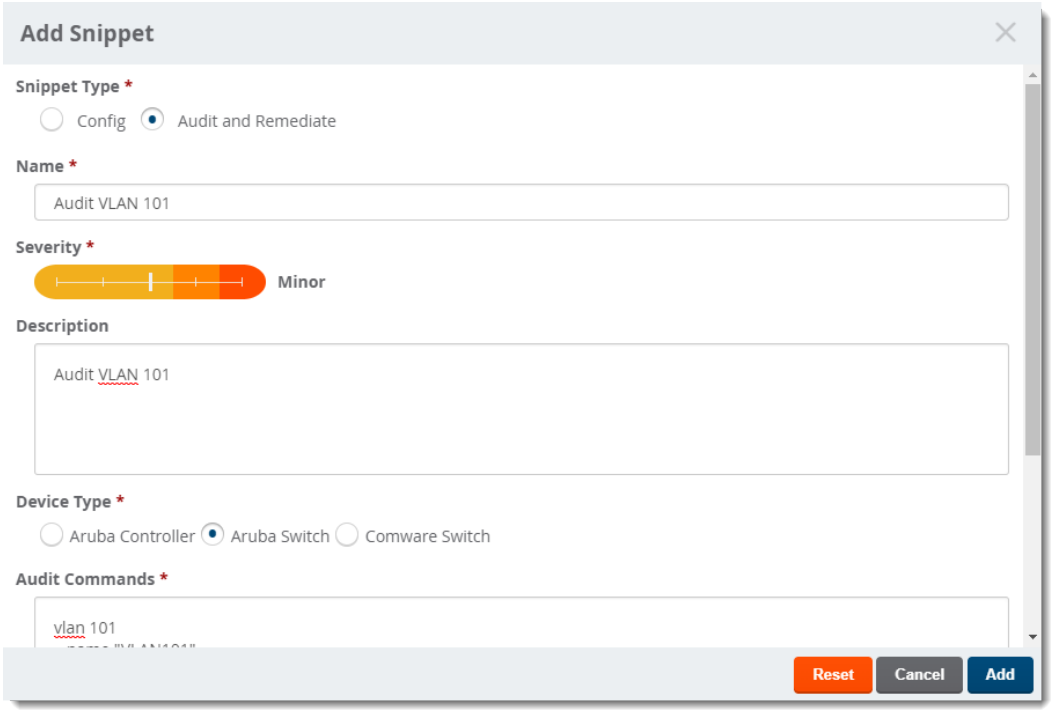
Create Snippets

In the Add Snippets page, you can choose from "Config" or "Audit and Remediate" snippet types. You can also use `show running config` commands on your switch CLI and copy the command syntax to the snippet.

1. Navigate to **Groups > Config & Audit Jobs**, then click the **Snippets** tab.
2. In the Add Snippets page, click + at the top right.
3. By default, AirWave selects **Config**. If you want to create a snippet for an audit job, select **Audit and Remediate**.
4. Enter the snippet name.
5. For snippets used in audit and remediate jobs, you can add a severity level against a device by moving the slider left or right.
6. Add a meaningful description about the snippet, if you want.
7. Select the device type for the snippet.
8. Enter one command per line, building your snippet in the order you would configure the device.
9. Click **Add**.

Figure 35 shows an example of a snippet used to audit a VLAN configuration with a severity level set to minor.

Figure 35: *Adding an Audit and Remediate Snippet*



Edit and Delete Snippets

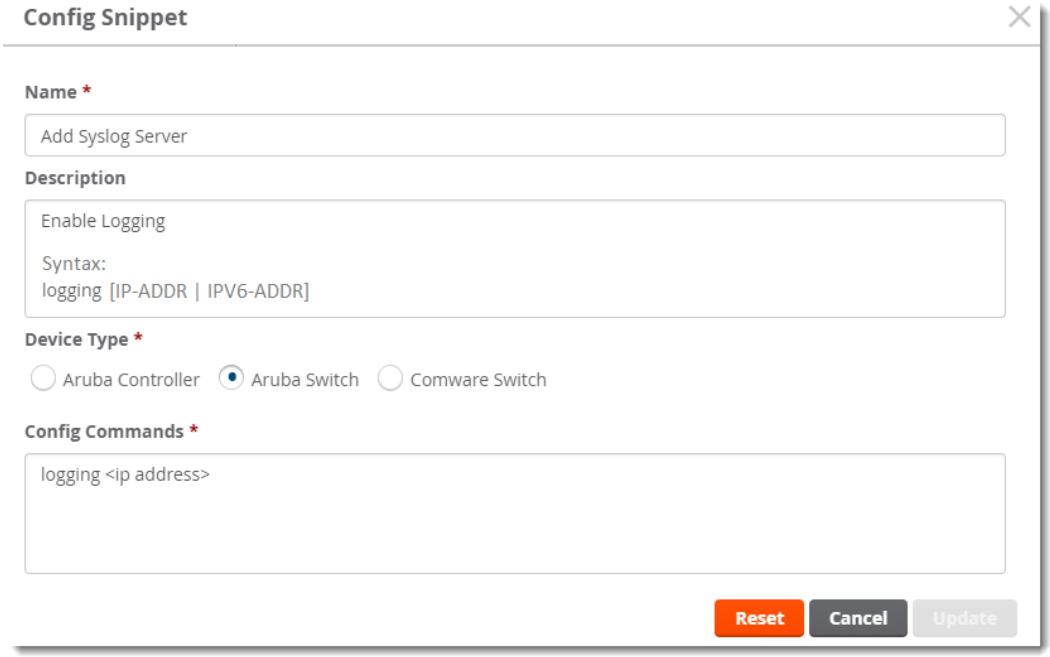
You can edit a predefined snippet (or any snippet), adding the values that you need. Later, while creating a config job, you can use a predefined config snippets like a user-defined config snippets.

Follow these steps to edit or delete a snippet:

1. Go to **Groups > Config & Audit Jobs**, then click the **Snippets** tab.
2. Locate a snippet, then click to edit the snippet. Or, click to delete the snippet. Proceed to the next step to edit the snippet.
3. In the Snippet window, enter the correct syntax in the Config Commands field.

   For example, replace <ipaddress> with the IP address of the syslog server you want to add, as shown in Figure 36.

Figure 36: *Editing the Add Syslog Server Snippet*



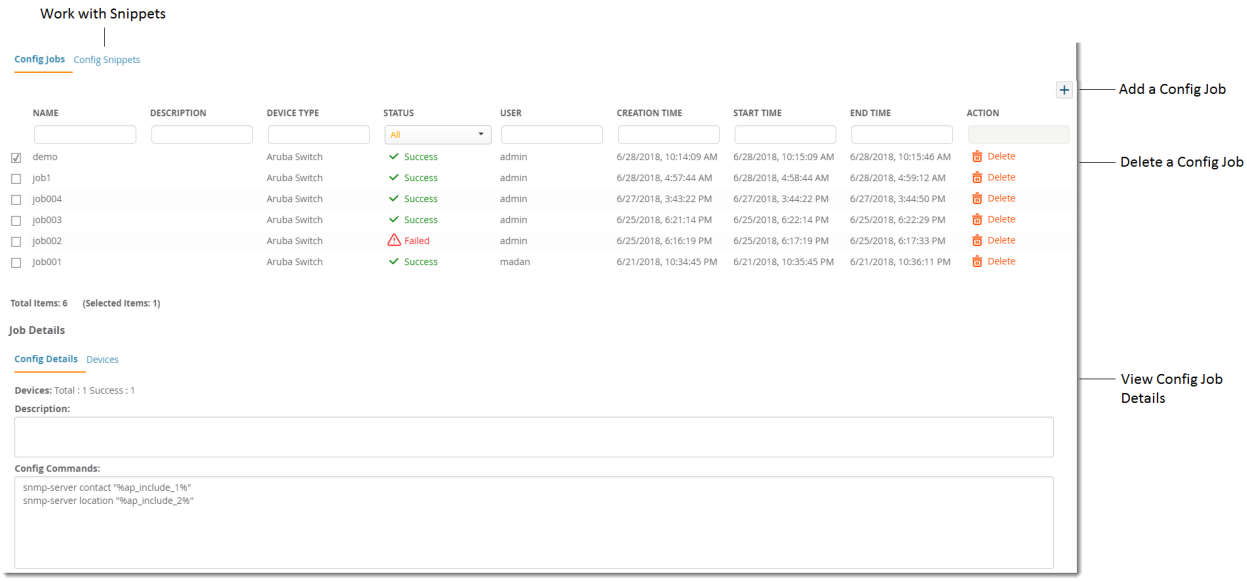
4. Click **Update**.

Device Configuration and Auditing Jobs

From the **Groups > Config & Audit Job** page, you can push a configuration to a device or group of devices using a template, audit the configuration, and remediate the configuration for non compliant devices.

Figure 37 shows what you can do from the Config & Audit Job page.

Figure 37: *Config & Audit Jobs Page*



NOTE

Config jobs are not recommended for groups that contain factory-default devices.

The **Jobs** table displays information about config, audit, and remediation jobs for the selected group of Aruba switches.

Table 5: *Jobs Table Information*

Column	Description
Name	Name of the job.
Device Type	Type of device.
Status	The job can be in several states. • **Scheduled**: The config or audit job will run in the future. • **Running**: The config or audit job is in progress. • **Success**: The config job completed successfully on all devices. • **Failed**: The job failed to run on one or more devices. • **Compliant**: The audit or remediate job completed and all devices are compliant. • **Non Compliant**: The audit or remediate job completed and the configuration on one or more devices is non compliant. **NOTE:** Hover your mouse over the **Status** column to view detailed status and device counts.
Creation Time	Timestamp showing the date and time of the job creation.
Start Time	Timestamp that shows when the job started.
End Time	Time of job completion for all devices
Action	Click to delete the job.

Create a Config Job

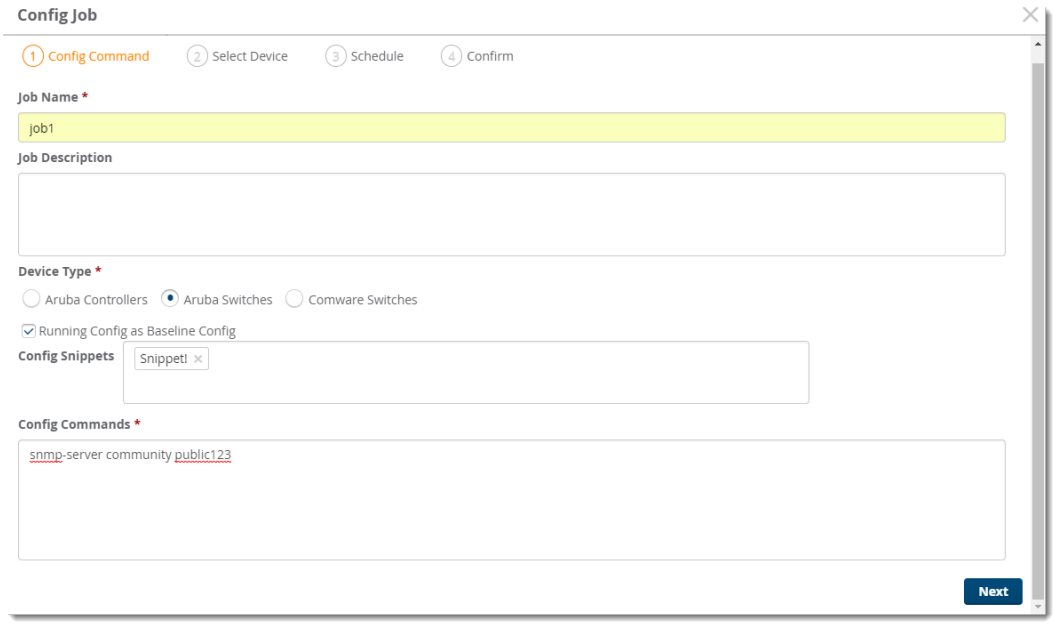
You can create a config job with the options of scheduling the job or saving the configuration as a baseline.

To create, run, or schedule a config job:

1. Navigate to **Groups > Config & Audit Jobs**, then click + to add a config job.
2. In the **Job** window, enter a name for the config job. If you want, enter a description.
3. Select the type of device: Aruba controllers, Aruba switches, or Comware switches.
4. If you want to set this config job as the baseline, check the "Running Config as Baseline Configuration" option.
5. Select one or more config snippets from the drop-down. Or, enter the config command manually one per line.

Figure 38 shows a config job to push a CLI command using a snippet to the Aruba switch.

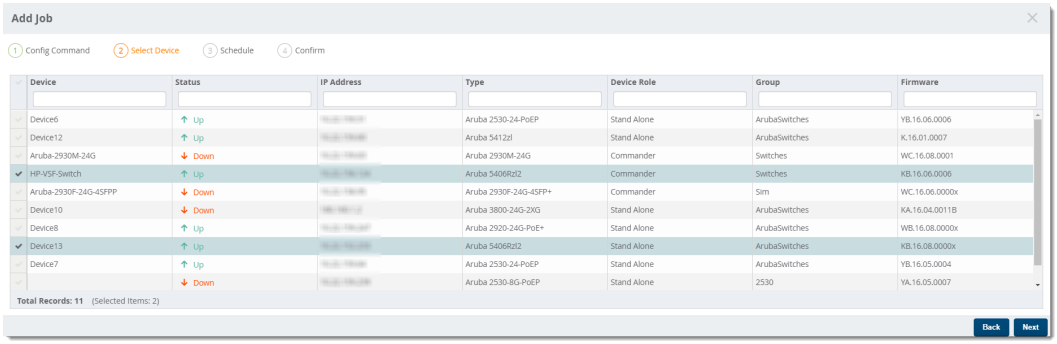
Figure 38: *Adding a Config Job Called job1*



6. Click **Next**.
7. In the **Select Device** tab, select the devices and click **Next**.

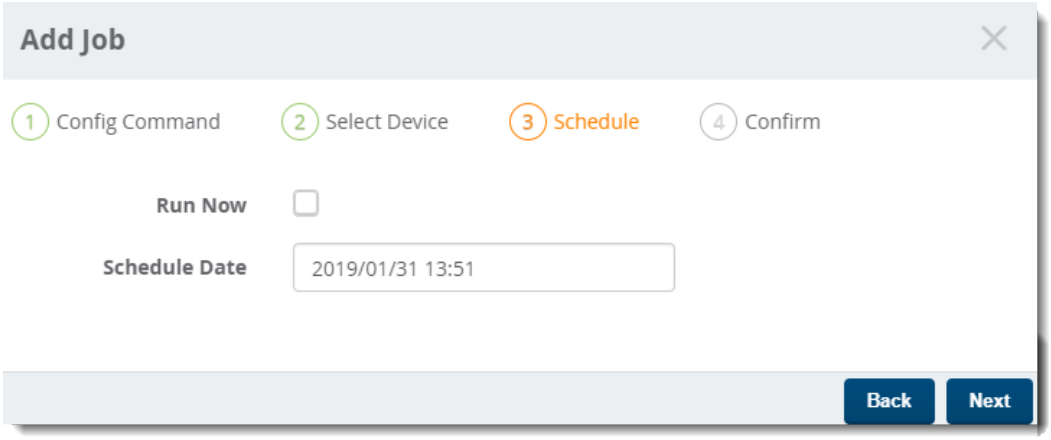
Figure 39 shows that down devices are excluded.

Figure 39: *Selecting Devices for the Config Job*



8. Click **Next**.
9. In the Schedule tab, click **Next** to run the job now. Or, deselect **Run Now** and click the Schedule Date field to select a date using the calendar tool.

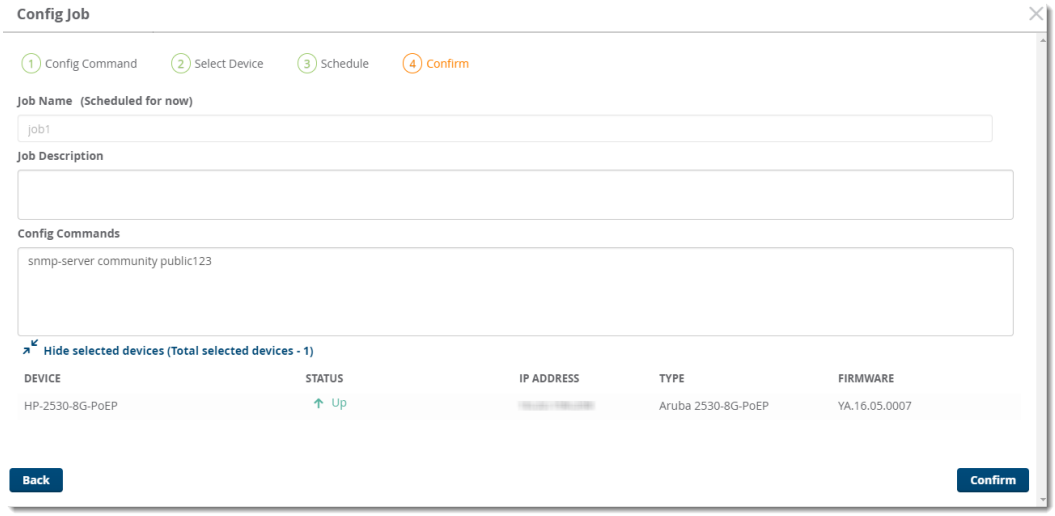
Figure 40: *Scheduling the Config Job*



10.Click **Next**.

11.In the **Confirm** tab, review the config job.

Figure 41: *Reviewing the Config Job Settings*

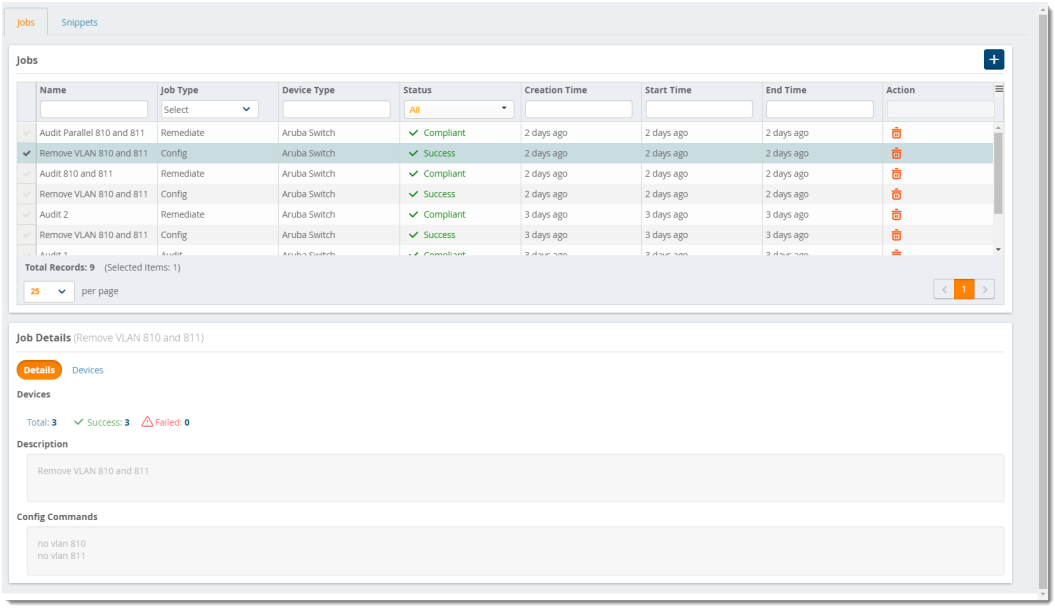


12.Click **Confirm**.

View Config Job Details

When you select a job from the Jobs page, details for the specific job display at the bottom of the page. You can see from the colored status in Figure 42 how many config jobs completed successfully or failed on the devices .

Figure 42: *Job Details*



View Diff Logs and Config Logs for the Config Job

You can view status for each device that received the config push. Information on the Devices tab includes: device name, status, IP address, job start and end time, and type of device.

Actions you can take:

- Click to view side-by-side windows that highlight the differences between previous and current configurations.
- Click to view the switch config log.

Revert or Delete a Job

To revert jobs that failed or delete job that you don't want to keep:

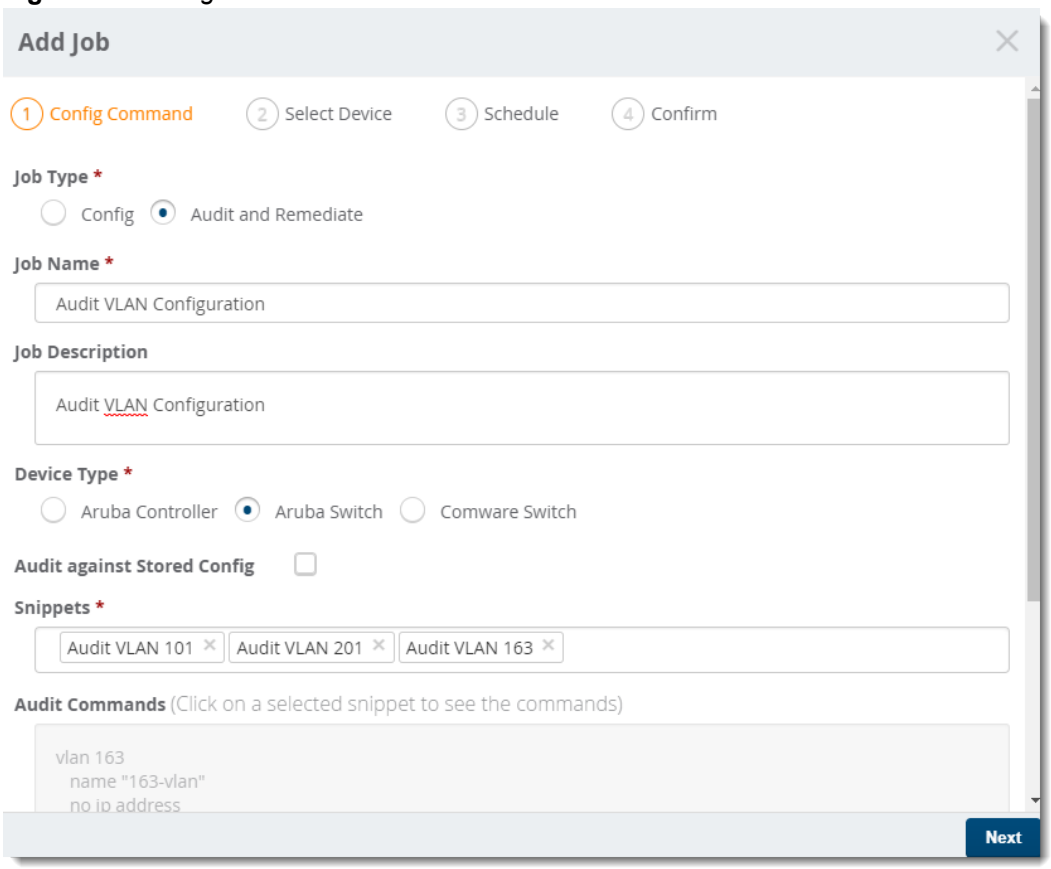
1. From the **Jobs** page, select the config job.
2. Click **Revert** in the **Action** column if you want to reset the device to its previous configuration. Or, click and remove the job.

Create an Audit Job

To run an audit job using a snippet:

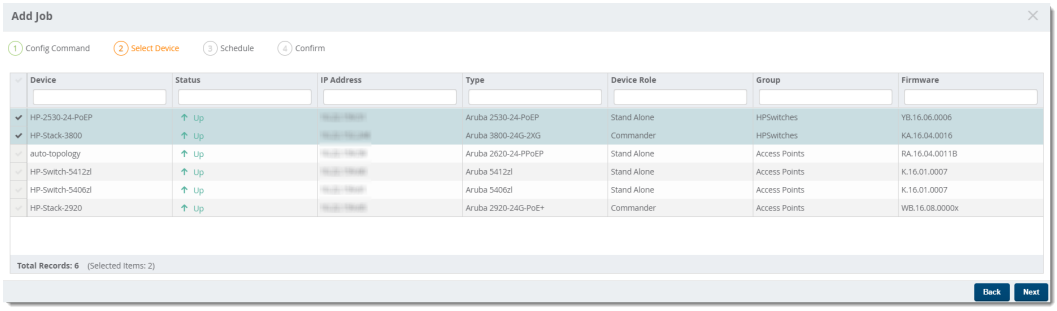
1. Navigate to **Groups > Config & Audit Jobs**, then click + to add a config job.
2. In the **Add Job** window, enter a name for the audit job.
3. If you want, enter a description.
4. Select the type of device: Aruba controllers, Aruba switches, or Comware switches.
5. Select one or more audit snippets from the drop-down.

Figure 43: *Adding an Audit Job*



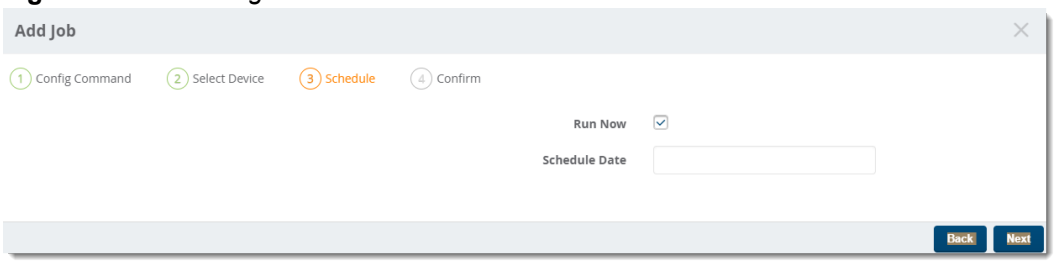
6. Click **Next**.
7. In the **Select Device** tab, select the devices and click **Next**. Figure 39 shows 2 devices selected for the audit job.

Figure 44: *Selecting Devices for the Audit Job*



8. Click **Next**.
9. In the **Schedule** tab, click **Next** to run the job now. Or, deselect **Run Now** and click the Schedule Date field to select a date using the calendar tool.

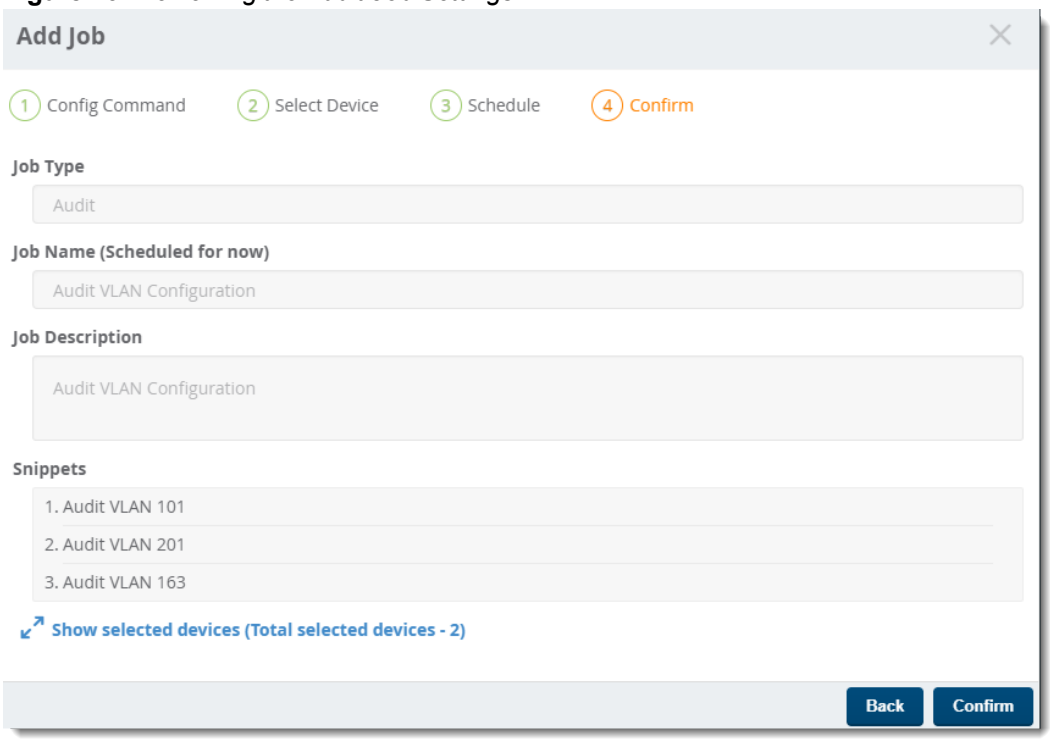
Figure 45: *Scheduling the Audit Job*



10.Click **Next**.

11.In the **Confirm** tab, review the audit job. Click the blue **Show selected devices** link to view device details.

Figure 46: *Reviewing the Audit Job Settings*



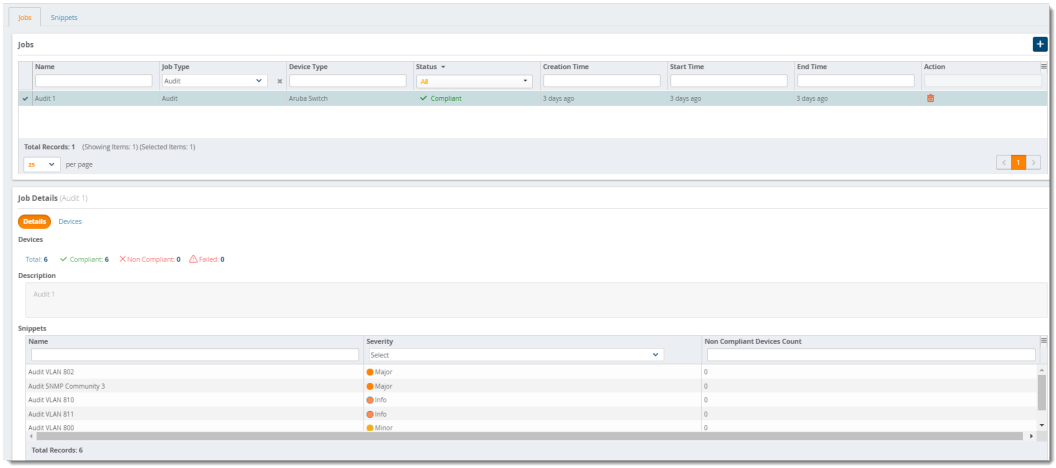
12.Click **Confirm** to create the audit job.

View Audit Job Details

You can view audit job details, including status and device count, by mousing over the job status in the Jobs table. Jobs progress from scheduled to running, and results are compliant, non compliant, or failed.

When you select an audit job from the Jobs table, non compliant device counts and audit snippets that have failed on the devices are also shown in the Job Details section at the bottom of the page . The example in Figure 47 shows that all the audited device configurations were compliant.

Figure 47: *Viewing Audit Job Details*



Remediate Non Compliant Devices

AirWave reports non compliant device counts in the Snippets table at the bottom of the page.

To remediate non compliant devices:

1. Locate the non compliant job in the Jobs table, then click to open the Remediate Job window.
2. In the Remediate Job window, choose **Run Now** or **Schedule**.
3. Click **Remediate**. AirWave returns you to the Job page, where you can see the job type has changed to "Remediate" and the jobs status progresses from scheduled to running.
4. After the remediation job completes, the job status changes to "Compliant" in the Job table.
5. In the Job Details at the bottom of the page, click the **Devices** tab, then click to view side-by-side windows that highlight the configuration change, or click to view the configuration in the telnet log.

Overview

This appendix describes the pages and inter-dependencies of Aruba Mobility Access Switch configuration profiles. It is recommended that you refer to the *ArubaOS User Guide* and the *ArubaOS CLI Guide* when you configure switch profiles inAirWave.

The default values of profile parameters or functions may differ slightly between ArubaOS releases.

To access the pages described in this section, select a switch group from the **Groups** page in the AirWave WebUI, then navigate to **Groups > Switch Config**.

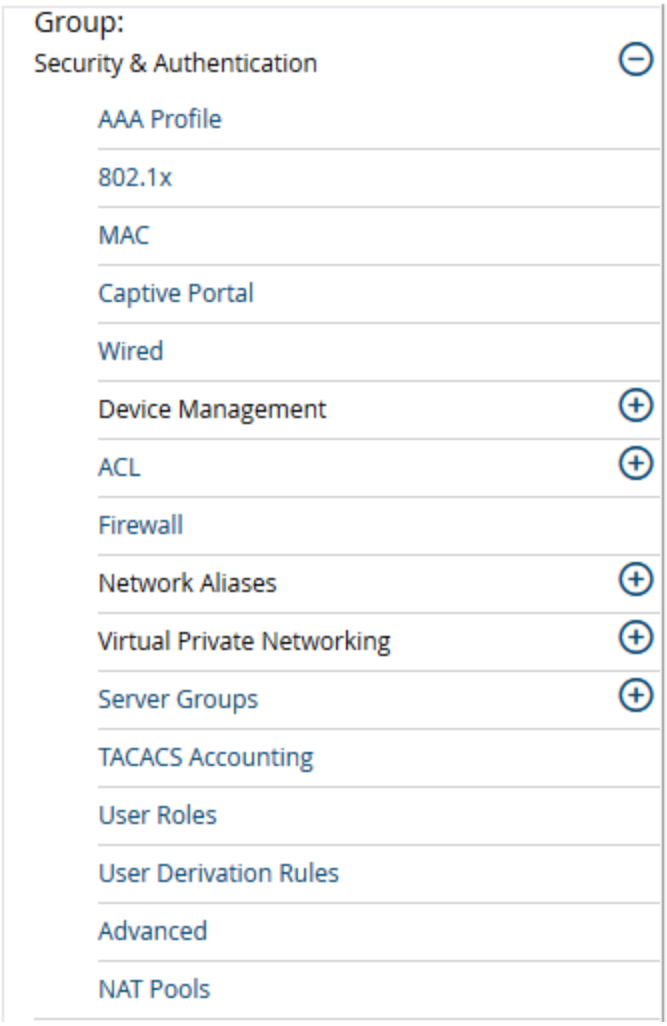
This section describes Switch Configuration components with the following organization and topics:

Security and Authentication

Switch Configuration supports user roles, policies, server groups, and additional security parameters with profiles that define security and authentication settings for the WLAN users, including the role for unauthenticated users and the different roles that should be assigned to users authenticated via 802.1X, MAC, or SIP authentication.

To view and configure Security and Authentication profiles, click the **Security & Authentication** profile heading in the navigation pane (see Figure 48).

Figure 48: *Switch Config > Security & Authentication navigation*



AAA Profile

Perform these steps to configure a AAA profile.

1. Select **Security & Authentication > AAA Profile** in the navigation pane.
2. Click the **Add** button to create a profile. Click the **pencil** icon next to an existing profile to change the settings.
3. Configure or edit the settings for the profile.
4. Select **Add** to save a new profile. Click **Save** to save the changes to an edited profile.

Refer to

- Refer to the AAA Authentication chapter in the *ArubaOS User Guide* for more information about AAA profiles.
- Refer to the "**aaa profile**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

802.1X Authentication Profile

The 802.1X authentication process has three components:

- The *supplicant*, or *client*, is the device attempting to gain access to the network. You can configure the Aruba user-centric network to support 802.1X authentication for wired users as well as wireless users.

- The *authenticator* is the gatekeeper to the network and permits or denies access to the supplicants. The ArubaMobility Access Switch acts as the authenticator, relaying information between the authentication server and supplicant.
- The *authentication server* provides a database of information required for authentication and informs the authenticator to deny or permit access to the supplicant.

The 802.1X authentication server is typically an EAP-compliant Remote Access Dial-In User Service (RADIUS) server that can authenticate either users (through passwords or certificates) or the client computer. The EAP type must be consistent between the authentication server and supplicant and is transparent to the switch.

An example of an 802.1X authentication server is the Internet Authentication Service (IAS) in Windows (go to http://technet2.microsoft.com/windowsserver/en/technologies/ias.mspx.)

In Aruba user-centric networks, you can terminate the 802.1X authentication on the switch. The switch passes user authentication to its internal database or to a backend non-802.1X server. This feature, also called AAA FastConnect, is useful for deployments where an 802.1X EAP-compliant RADIUS server is not available or is not required for authentication.

Perform these steps to configure an 802.1X Auth profile.

1. Select **Security & Authentication > 802.1X Auth** in the navigation pane.
2. Click **Add** to create an 802.1X Auth profile. To edit a profile, click the **pencil** icon next to the profile name.
3. Configure the settings for 802.1X authentication.
4. Select **Add** or **Save**. The name of the new or edited 802.1X Auth profile appears on the **802.1X** page.

Refer to

- Refer to the 802.1X Authentication chapter in the *ArubaOS User Guide* for more information about AAA profiles.

- Refer to the "**aaa authentication dot1x**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

MAC-based Authentication

This section explains how to configure MAC-based authentication.

Prerequisites

Before configuring MAC-based authentication, you must complete the following tasks.

- Select the user role that will be assigned as the default role for the MAC-based authenticated clients. You configure the default user role for MAC-based authentication in the AAA profile.
  - **Tip:** If derivation rules exist, or if the client configuration in the internal database has a role assignment, these values take precedence over the default user role.
- Select the authentication server group that the controller uses to validate the clients. The internal database can be used to configure the clients for MAC-based authentication.

1. Select **Security & Authentication > MAC** in the navigation pane.
2. Click **Add** to create a MAC authentication profile, or click the **pencil** icon next to an existing profile to edit.
3. Configure the settings for MAC authentication.
4. Select **Add** or **Save**.

The name of the new or edited 802.1X Auth profile appears on the **802.1X** page.

- Refer to the MAC-Based Authentication chapter in the *ArubaOS User Guide* for more information about AAA profiles.

- Refer to the "**aaa authentication mac**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Captive Portal Authentication Profile

Configure a Captive Portal profile for guest users where no authentication is required, or for registered users who must be authenticated against an external authentication server or the MAS internal user database.

The Captive Portal Authentication profile specifies the Captive Portal Profile login page and other configurable parameters. The initial user role configuration must include the applicable Captive Portal authentication profile instance. Therefore, you must modify the guest-logon user role configuration to include the guestnet Captive Portal Authentication profile.

Perform these steps to configure a Captive Portal Authentication profile.

1. Select **Security & Authentication > Captive Portal** page.
2. Click the **Add** button to create a profile. Click the pencil icon next to an existing profile to change the settings.
3. Configure or edit the settings for the profile.
4. Select **Add** to save a new profile. Click **Save** to save the changes to an edited profile.

Refer to

- Refer to the *Captive Portal* chapter in the *ArubaOS User Guide* for more information about Captive Portal profiles.

- Refer to the "**aaa authentication captive-portal**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Wired Authentication Profile

The Wired Authentication Profile references a profile used for wired authentication.

Perform these steps to configure a Wired Authentication profile.

1. Select **Security & Authentication > Wired** page.
2. Click the **Add** button to create a profile. Click the pencil icon next to an existing profile to change the settings.
3. Configure or edit the settings for the profile.
4. Select **Add** to save a new profile. Click **Save** to save the changes to an edited profile.

Refer to

- Refer to the AAA Authentication chapter in the *ArubaOS User Guide* for more information about wired authentication.

- Refer to the "**aaa authentication wired**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Device Management

Users who need to access the switch to monitor, manage, or configure the Aruba user-centric network can be authenticated with RADIUS, TACACS+, or LDAP servers or the internal database. The **Device Management** page provides links to the following configurable options:

- External Authentication
- Local Authentication
- Password Policy
- Enable Password

External Authentication

Perform these steps to configure a Management authentication profile.

1. Select **Security & Authentication > Device Management > External Authentication** in the Switch Config navigation pane.
2. Complete the settings as described in Table 6:

Table 6: *Security & Authentication > Management Auth Profile Settings*

Field	Default	Description
Referenced Profiles		
Server Group		Select the AAA authentication server group. Select the pencil icon to edit an existing server group or click the add (**+**) icon to create a new server group.
Other Settings		
Default Role	root	The role to be associated with this authentication profile: • **guest-provisioning**: Allows the user to create guest accounts. • **location-api-mgmt**: Permits access to location API information. You can log in, however, you cannot use any commands. • **network-operations**: Permits access to Monitoring, Reports, and Events pages in the WebUI. You can log in; however, you can only use a subset of commands to monitor the controller. • **no-access**: Indicates that no access is available. • **read-only**: Permits access to monitoring pages only. • **root**: Permits access to all management functions on the controller.
Enable	No	When enabled, this setting activates the authentication server.
Mschapv2	No	When enabled, MSCHAPv2 (Microsoft Challenge Authentication Protocol version 2) will be used for authentication. Refer to RFC 2759 for more information about MSCHAPv2.

3. Select **Save**.

Local Authentication

Perform these steps to configure local user authentication settings:

1. Select **Security & Authentication > Device Management > Local Authentication** in the Switch Config navigation pane.
2. You can choose to enable or disable local user authentication. By default, local authentication is enabled.
3. Select the **Add** button to create a new management local user, or click the pencil icon next to an existing user to edit.
4. Configure the credentials and role for the management local user.
5. Select **Add** or **Save**. The added or edited management local user appears on the **Local Authentication** page.

Password Policy

Go to **Security & Authentication > Device Management > Password Policy** to open the **Management Password Policy** page. You can take the following actions on the page.

- Enable or Disable Password Policy

- Define the minimum password length requirements (the range is 6-32 characters)
- Define the minimum number of the following password characters (range is 0-10 characters)
  - Upper Case Characters
  - Lower Case Characters
  - Digits
  - Special Characters
- Allow or deny the use of the user name or reverse of user name in the password
- Set the maximum number of failed attempts in a 3 minute window to lockout a user (range is 0-10 attempts).
- Set the time duration to lockout the user upon crossing the lockout threshold (range is 1-1440 minutes).
- Set the maximum consecutive character repeats (range is 0-10 characters)

Enable Password

Go to **Security & Authentication > Device Management > Enable Policy** to open the Management Enable page. You can take the following actions on the page:

- Enable or disable Bypass
- Enable Secret
- Confirm Enable Secret

ACL

The **Security & Authentication > ACL** page under Switch Config displays all currently configured policies, including the policy name and the user role that use this policy.

Perform these steps to configure a new Policy/Access Control List.

1. Select **Security & Authentication > ACL** page.
2. Select the **Add** button to create a new policy, or click the **pencil** icon next to an existing policy to edit.
3. Configure the settings for the ACL.
4. Select **Add** or **Save**. The added or edited ACL appears on the **ACL** page.

Refer to

- Refer to the Roles and Policies chapter in the *ArubaOS User Guide* for more information about Access Control Lists.
- Refer to the "`ip access-list`" commands in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Time Range

A time range profile establishes the boundaries by which users and guest users are to be supported on the network. This is a security and access-related profile, and multiple time range profiles can be configured to enable absolute or periodic access.

The **Security & Authentication > ACL > Time Range** page displays all configured time ranges that are currently available, time range profile type, the policy that uses time range profiles, and the controller in which each profile is visible.

To create a new time range profile, click the **Add New Time Range** button, or click the pencil icon next to an existing time range profile to adjust settings.

Refer to

- Refer to the Access Control List chapter in the *ArubaOS User Guide* for more information Time Ranges that are used with policy.

- Refer to the "**time-range**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Firewall

Firewalls are used to examine network traffic and enforce policies based on instructions contained within the Firewall's Ruleset. You can configure the global firewall parameters in the **Security & Authentication > Firewall** page.

1. Navigate to the **Security & Authentication > Firewall** page.
2. Enter the global firewall settings.
3. Select **Save** to save the settings.

Refer to

- Refer to the *Global Firewall Policies* section under the *Roles and Policies* chapter in the *ArubaOS User Guide* for more information on setting global firewall parameters.
- Refer to the "`firewall`" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Network Aliases

The **Network Aliases** page under **Security & Authentication** provides links to the following configurable options:

- Destinations
- Services

Destinations

The **Security & Authentication > Network Aliases > Destinations** page lists the destination name, protocol, and port currently configured, along with the policy and switch that use a configured destination.

To edit an existing destination, click the pencil icon. To create a new destination to be referenced by a security policy, click the **Add New Net Destination** button.

Refer to

- Refer to the Roles and Policies chapter in the *ArubaOS User Guide* for more information about network destination aliases.

- Refer to the "**netdestination**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Services

The **Security & Authentication > Network Aliases > Services** page displays all Netservice profiles that are available for reference by Security policies. This page displays Netservice profile names, the protocol associated with it, the policy that uses this Netservice profile, and the folder.

To edit an existing network service, click the pencil icon. To create a new network service to be referenced by a security policy, click the **Add New Netservice** button.

Refer to

- Refer to the Roles and Policies chapter in the *ArubaOS User Guide* for more information about network aliases.
- Refer to the "**netservice**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Virtual Private Networking

Wireless networks can use virtual private network (VPN) connections to further secure wireless data from attackers. The **VPN** page provides links to the following configurable options:

- Site-Site VPN
- IKE Policy
- IPSEC

Site-Site VPN

Site-to-site VPNs allow networks (for example, a branch office network) to connect to other networks (for example, a corporate network). Unlike a remote access VPN, hosts in a site-to-site VPN do not run VPN client software. All traffic for the other network is sent and received through a VPN gateway which encapsulates and encrypts the traffic.

Perform these steps to configure a site-site VPN:

1. Navigate to **Security & Authentication > Virtual Private Networking > Site-Site VPN** page.
2. Provide the site-site IKE settings.
3. Click **Add** to add a new site-site IKE shared secret or click the pencil icon next an existing IKE shared secret to edit.
4. Click **Save**.

Refer to

- Refer to the *Virtual Private Networks* chapter in the *ArubaOS User Guide* for more information.
- Refer to the "`crypto-local`", commands in the *ArubaOS CLI Guide* for information about the options that are available on this form.

IKE Policy

An IKE policy defines what level of authentication or encryption protection IKE uses during phase 1 negotiations. VPN uses either RSA signature mode or preshared keys to authenticate phase 1 negotiations. The IKE policy also identifies which remote key server will use this policy.

Perform the following tasks to define an IKE policy or make changes to an existing one.

1. Navigate to **Security & Authentication > Virtual Private Networks > IKE > IKE Policy** page.
2. Click **Add** to create a new IKE policy or click the pencil icon next to an existing policy to edit.
3. Provide the IKE policy settings.
4. Click **Save**.

Refer to

- Refer to the *Virtual Private Networks* chapter in the *ArubaOS User Guide* for more information.
- Refer to the "`crypto isakmp policy`", command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Site to Site IKE

Site to Site IKE feature lets you configure Site to Site IKE on an Arubacontroller.

Perform the following tasks to configure Site to Site IKE:

1. Navigate to **Controller Config > Advanced Services > VPN Services > Site to Site IKE** page.
2. Configure the Site to Site IKE settings:
   - Configure IKE DPD
   - Permit Invalid certificates for Site-Site VPN
   - Disable aggressive mode
   - XAuth: Enable IKE XAuth for VPN clients, use no form of command to disable XAuth for Certificate-based VPN clients
   - server-certificate Configure a single IKE Server Certificate for all VPN Clients
   - Configure a single IKE Server Certificate for all
   - Configure IKE CA Certificates for VPN Clients
     - ca-certificate
     - server-certificate
3. Click **Add** to add the Site to Site shared secret.
4. Click **Save**.

Refer to

- Refer to the *Virtual Private Networks* chapter in the *ArubaOS User Guide* for more information.
- Refer to the "`crypto-local isakmp`", command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

IPSEC

The IPSec security profile provides all data required to create an inbound and outbound IPSec policy entry. This IPSEC page provides link to the following configurable options:

- Transform set
- IPSEC Map

Transform Set

You can create or edit transform sets that define a specific encryption and authentication type using the following steps:

1. Navigate to **Security & Authentication > Virtual Private Networks > IPSEC > Transform Set**.
2. Click **Add** to create a new transform set or click the pencil icon next to an existing transform set to edit.
3. Provide the transform set settings.
4. Click **Save**.

Refer to

- Refer to the *Virtual Private Networks* chapter in the *ArubaOS User Guide* for more information.

- Refer to the "`crypto ipsec transform-set`", command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

IPSEC Map

You can create or edit IPSec maps using the following steps:

1. Navigate to **Security & Authentication > Virtual Private Networks > IPSEC > IPSEC Map**.
2. Click **Add** to create a new transform set or click the pencil icon next to an existing IPSec map to edit.
3. Provide the IPSec map settings.
4. Click **Save**.

Refer to

- Refer to the *Virtual Private Networks* chapter in the *ArubaOS User Guide* for more information.
- Refer to the "`crypto-local ipsec-map`", command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Server Groups

The **Server > Server Groups** page displays all server groups currently configured along with the profiles and controllers that are used by each server group:

- AAA
- Captive Portal Auth
- Stateful Kerberos Auth
- Management Auth
- Stateful NTLM Auth
- Stateful 802.1X Auth
- TACACS Accounting
- VIA Auth
- VPN Auth
- WISPr Auth
- Controller

The list of servers in a server group is an ordered list. By default, the first server in the list is always used unless it is unavailable, in which case the next server in the list is used. You can configure the order of servers in the server group. In the WebUI, use the up or down arrows to order the servers (the top server is the first server in the list). In the CLI, use the position parameter to specify the relative order of servers in the list (the lowest value denotes the first server in the list).

The first available server in the list is used for authentication. If the server responds with an authentication failure, there is no further processing for the user or client for which the authentication request failed. You can optionally enable fail-through authentication for the server group so that if the first server in the list returns an authentication deny, the controller attempts authentication with the next server in the ordered list. The controller attempts authentication with each server in the list until either there is a successful authentication or the list of servers in the group is exhausted. This feature is useful in environments where there are multiple, independent authentication servers; users may fail authentication on one server but can be authenticated on another server.

Before enabling fail-through authentication, note the following:

- This feature is not supported for 802.1X authentication with a server group that consists of external EAP compliant RADIUS servers. You can, however, use fail-through authentication when the 802.1X authentication is terminated on the controller (AAA FastConnect).

- Enabling this feature for a large server group list may cause excess processing load on the controller. Best practices are to use server selection based on domain matching whenever possible.
- Certain servers, such as the RSA RADIUS server, lock out the controller if there are multiple authentication failures. Therefore you should not enable fail-through authentication with these servers.

When fail-through authentication is enabled, users that fail authentication on the first server in the server list should be authenticated with the second server.

Supported Servers

ArubaOS supports the following external authentication servers:

- LDAP (Lightweight Directory Access Protocol)
- RADIUS (Remote Authentication Dial-In User Service)
- RFC 3576
- TACACS+ (Terminal Access Controller Access Control System)
- XML API

Additionally, you can use the controller's internal database to authenticate users. You create entries in the database for users and their passwords and default role.

The Switch Config **Security & Authentication > Server Groups** feature does not support Windows server groups.

You can create groups of servers for specific types of authentication. For example, you can specify one or more RADIUS servers to be used for 802.1X authentication. The list of servers in a server group is an ordered list. This means that the first server in the list is always used unless it is unavailable, in which case the next server in the list is used. You can configure servers of different types in one group — for example, you can include the internal database as a backup to a RADIUS server.

Server names are unique. You can configure the same server in multiple server groups. You must configure the server before you can add it to a server group.

Adding a New Server Group

The server group is assigned to the server group for 802.1X authentication.

To create a new server group, click the **Add** button, or to edit an existing group, click the pencil icon next to that group. The **Add New Server Group** page appears.

Internal

An internal server group configures the internal database with the user name, password, and role (student, faculty, or sysadmin) for each user. There is a default internal server group that includes the internal database. For the internal server group, configure a server derivation rule that assigns the role to the authenticated client.

Refer to

- Refer to the Authentication Servers chapter in the *ArubaOS User Guide* for more information about internal server groups.

- Refer to the "**local-userdb add**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

LDAP

You can configure Lightweight Directory Access Protocol (LDAP) servers for use by a server group.
The **Security & Authentication > Server Groups > LDAP** page displays current LDAP servers available for

inclusion in server groups. Click **Add** to create a new LDAP server, or click the pencil icon next to an existing LDAP server to edit the configuration.

Refer to

- Refer to the Authentication Servers chapter in the *ArubaOS User Guide* for more information about LDAP servers.
- Refer to the **aaa authentication-server ldap** command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Security and Authentication > Server Groups > RADIUS

You can configure RADIUS servers for use by a server group. The **Security & Authentication > Server Groups > RADIUS** page displays current RADIUS servers available for inclusion in server groups. Click **Add** to create a new RADIUS server, or click the pencil icon next to an existing RADIUS server to edit the configuration.

Refer to

- Refer to the Authentication Servers chapter in the *ArubaOS User Guide* for more information about RADIUS servers.
- Refer to the "**aaa authentication-server radius**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Security and Authentication > Server Groups > TACACS

You can configure TACACS+ servers for use by a server group. The **Security & Authentication> Server Groups > TACACS** page displays current TACACS servers available for inclusion in server groups. Click **Add** to create a new TACACS server, or click the pencil icon next to an existing TACACS server to edit the configuration.

Refer to

- Refer to the Authentication Servers chapter in the *ArubaOS User Guide* for more information about TACACS servers.
- Refer to the **aaa authentication-server tacacs** command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Security > Server Groups > RFC 3576

RFC 3576 servers support dynamic authorization extensions to Remote Authentication Dial-In User Service (RADIUS). Switch Configuration supports RFC 3576 servers that can be referenced by server groups.

To view currently configured RFC 3576 servers and where they are used, navigate to the **Security & Authentication > Server Groups > RFC 3576** page.

Click **Add** to create a new RFC3576 server, or click the pencil icon next to an existing RFC 3756 server to edit the configuration.

Refer to

- Refer to the Authentication Servers chapter in the *ArubaOS User Guide* for more information about RFC 3576 servers.
- Refer to the **aaa rfc-server** command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Security and Authentication > Server Groups > XML API

Switch Configuration supports server groups that can include XML API servers. XML API servers send and accept requests for information. XML API servers process such requests and act on these requests by performing

requested actions. Such a server also compiles necessary reporting data and sends it back to requesting source.

The **Security & Authentication > Server Groups > XMP API** page lists any XML API servers currently available for use by server groups. From this page, click **Add** to create a new XML API server, or click the pencil icon next to an existing XML API server to edit the configuration.

Refer to

- Refer to the Authentication Servers chapter in the *ArubaOS User Guide* for more information about XML API servers.
- Refer to the "**aaa authentication-server xml-api**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Security > TACACS Accounting

TACACS+ accounting allows commands issued on the switch to be reported to TACACS+ servers. You can specify the types of commands that are reported, and these are action, configuration, or show commands. You can have all commands reported as desired. Switch Configuration supports TACACS Accounting servers that can be referenced by server groups.

To view currently configured TACACS Accounting profiles and where they are used, navigate to the **Security > TACACS Accounting** page. Select **Add** to create a new TACACS Accounting profile, or click the pencil icon to edit an existing profile.

Select **Add** to complete the new TACACS Accounting profile, or click **Save** to complete the editing of an existing profile.

Refer to

- Refer to the Authentication Servers chapter in the *ArubaOS User Guide* for more information about TACACS Accounting.
- Refer to the "**aaa tacacs-accounting server-group**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Security and Authentication > User Roles

A client is assigned a user role by one of several methods. A user role assigned by one method may take precedence over a user role assigned by a different method. The methods of assigning user roles are, from lowest to highest precedence:

1. The initial user role for unauthenticated clients is configured in the AAA profile for a virtual AP.
2. The user role can be derived from user attributes upon the client's association with an AP (this is known as a user-derived role). You can configure rules that assign a user role to clients that match a certain set of criteria. For example, you can configure a rule to assign the role VoIP-Phone to any client that has a MAC address that starts with bytes xx:yy:zz. User-derivation rules are executed before client authentication.
3. The user role can be the default user role configured for an authentication method, such as 802.1X or VPN. For each authentication method, you can configure a default role for clients who are successfully authenticated using that method.
4. The user role can be derived from attributes returned by the authentication server and certain client attributes (this is known as a server-derived role). If the client is authenticated via an authentication server, the user role for the client can be based on one or more attributes returned by the server during authentication, or on client attributes such as SSID (even if the attribute is not returned by the server). Server-derivation rules are executed after client authentication.

5. The user role can be derived from Vendor-Specific Attributes (VSA) for RADIUS server authentication. A role derived from an Aruba VSA takes precedence over any other user roles.

In the Aruba user-centric network, the user role of a wireless client determines its privileges, including the priority that every type of traffic to or from the client receives in the wireless network. Thus, QoS for voice applications is configured when you configure firewall roles and policies.

In an Aruba system, you can configure roles for clients that use mostly data traffic, such as laptop computers, and roles for clients that use mostly voice traffic, such as VoIP phones. Although there are different ways for a client to derive a user role, in most cases the clients using data traffic will be assigned a role after they are authenticated through a method such as 802.1X, VPN, or captive portal. The user role for VoIP phones can be derived from the OUI of their MAC addresses or the SSID to which they associate. This user role will typically be configured to have access allowed only for the voice protocol being used (for example, SIP or SVP).

You must install the Policy Enforcement Firewall license in the switch.

This page displays the current user roles in Switch Config and where they are used.

Select **Add** to complete the configuration of the **User Role**, or click **Save** to complete the editing of an existing role. The new role appears on the **Security and Authentication > User Roles** page.

Refer to

- Refer to the Roles and Policies chapter in the *ArubaOS User Guide* for more information about Roles.
- Refer to the "**user-role**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Security and Authentication > User Derivation Rules

The user role is a user derivation profile. User Rules can be derived from attributes from the client's association with an AP. For VoIP phones, you can configure the devices to be placed in their user role based on the SSID or the Organizational Unit Identifier (OUI) of the client's MAC address.

Navigate to the **Security & Authentication > User Derivation Rules** page in the Switch Config navigation pane. This page displays user rules that are currently configured and the AAA profile that references these rules.

To add a new user rule, which is a derivation profile, click the **Add New User Derivation Profile** button. To edit an existing user rule, click the pencil icon next to an existing rule.

Refer to

- Refer to the Roles and Policies chapter in the *ArubaOS User Guide* for more information about User-Derived roles.
- Refer to the "**aaa derivation-rules**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Advanced Authentication

In Advanced Authentication, you can apply timers and DNS query intervals. Follow these steps to configure an Advanced Authentication profile.

1. Select **Security & Authentication > Advanced** in the navigation pane. The details page summarizes the current profiles of this type.
2. Complete the settings as described in Table 7:

Table 7: *Security & Authentication > Advanced Profile Settings*

Field	Default	Description
Authentication Timers		
User Idle Timeout (30-15300 sec)	300 seconds	Maximum period, in seconds, after which a client is considered idle if there is no user traffic from the client. The timeout period is reset if there is a user traffic. After this timeout period has elapsed, the controller sends probe packets to the client; if the client responds to the probe, it is considered active and the User Idle Timeout is reset (an active client that is not initiating new sessions is not removed). If the client does not respond to the probe, it is removed from the system. Range: 30 to 15300 seconds
User Stats Timeout (300-600 sec)	600 sec	Set the timeout value for user stats reporting in seconds. The supported range is 300-600 seconds, or 5-10 minutes, and the default value is 600 seconds. Requires a minimum version of 6.1.0.0.
Poll user stats (60-600)		Specify a the frequency with which user stats are polled. An empty value indicates that polling will not occur.
Dead Time for down Authentication Server (0-60 min)	10 minutes	Maximum period, in minutes, that the controller considers an unresponsive authentication server to be out of service. This timer is only applicable if there are two or more authentication servers configured on the controller. If there is only one authentication server configured, the server is never considered out of service and all requests are sent to the server. If one or more backup servers are configured and a server is unresponsive, it is marked as out of service for the dead time; subsequent requests are sent to the next server on the priority list for the duration of the dead time. If the server is responsive after the dead time has elapsed, it can take over servicing requests from a lower-priority server; if the server continues to be unresponsive, it is marked as down for the dead time. Range: 0–60 minutes
Unauthenticated User Lifetime (0-255 min)	5 minutes	Maximum time, in minutes, unauthenticated clients are allowed to remain logged on. Range: 0–255 minutes
RADIUS Attributes		
Attribute Name	blank	Specify the name for this new Radius attribute.
Attribute Value	blank	Enter an integer value for a the Radius attribute.

Table 7: *Security & Authentication > Advanced Profile Settings (Continued)*

Field	Default	Description
Attribute type	date	Specify one of the following types to be associated with this attribute: • date • integer • ipaddr • string
Vendor Name	blank	Enter the name of the vendor associated with this attribute.
Vendor Id	blank	Enter an integer value for the vendor ID associated with this attribute.

3. Select **Add** or **Save**. The added or edited profile appears on the **Advanced** page.

NAT Pool

In NAT Pool, you can configure a NAT Pool profile to protect private IPs behind the switch.

1. Select **Security & Authentication > NAT Pool** in the navigation pane. The details page summarizes the current profiles of this type.
2. Select **Add** to create a new NAT Pool profile.
3. Complete the settings as described in :

Table 8: *Security & Authentication > NAT Pool Settings*

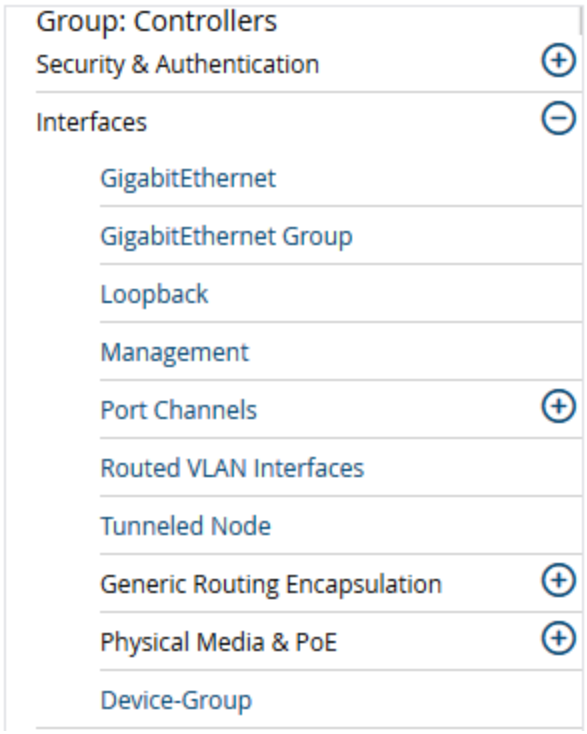
Field	Description
Name	Name of the NAT pool.
Start of Source NAT Range	The starting IP address of the source NAT range.
End of Source NAT Range	The end IP address of the source NAT range.
Destination NAT IP Address	The IP address of the destination NAT.

4. Select **Add**. The added or edited profile appears on the **NAT Pool** page.

Interfaces

Switch Configuration supports a variety of profiles that can be associated with Interfaces. Refer to the **Interfaces** portion of the navigation pane on the **Switch Config** page, as illustrated in Figure 49:

Figure 49: *Interfaces Components in Switch Config*



This section describes the profiles for all Interface components in **Switch Config**.

GigabitEthernet

The Mobility Access Switch supports 24 or 48 port gigabit Ethernet interfaces of 10/100/1000 Mbps speeds.

A network gigabit Ethernet interface is referred by its <slot>/<module>/<port>.

- Slot—The member ID of the stack.
- Module—There are two modules where the first one is the front-panel network module (0), while the other one is the uplink network module (1).
- Port—The individual port number.

For example, interface gigabitethernet 0/0/20 refers to the first stack member (0) on the front-panel network module (0) at port number (20).

NOTE

Mobility Access Switch also supports four 10-Gigabit Ethernet interfaces for stacking and uplink purposes. Refer to the Hardware Installation Guide for more information on the 10-Gigabit Ethernet uplink module.

1. To configure a Gigabit Ethernet interface, navigate to the **Interfaces > GigabitEthernet** page and click **Add New GigabitEthernet Interface**.
2. Specify your settings for the interface.
3. Click **Add** to save the new interface. Additional Gigabit Ethernet Interfaces can then be added and edited from this page.

Refer to

- Refer to the Ethernet Interfaces and PoE chapter in the *ArubaOS User Guide* for more information.
- Refer to the "**interface gigabitethernet**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

GigabitEthernet Group

The Mobility Access Switch can group the interfaces together so that any interface within the group has the same configuration. When you configure an interface that is a member of an interface-group, applying a non-default profile or a parameter to the interface takes precedence over the interface-group configuration. By default, all the interfaces belong to a default interface-group.

When you create non-default interface-groups, the excluded interfaces continue to belong to the default interface-group.

Interface groups and port channels are not the same. Interface groups assign the configuration to individual interfaces, whereas the port channel makes a group of interfaces to work as a single logical interface.

1. To configure a Gigabit Ethernet interface, navigate to the **Interfaces > GigabitEthernet Group** page and click **Add New GigabitEthernet Group**.
2. Specify your settings for the group.
3. Click **Add** to save the new group. Additional Gigabit Ethernet groups can then be added and edited from this page.

You cannot have overlapping ranges of interfaces when you have multiple interface groups. For more information about the scope of an interface and interface group profiles, see the “Scope of the Profiles and Parameters” in the *ArubaOS User Guide*.

Refer to

- Refer to the Ethernet Interfaces and PoE chapter in the *ArubaOS User Guide* for more information.
- Refer to the "**interface-group gigabitethernet**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Loopback

The Mobility Access Switch supports a maximum of 64 (0-63) loopback interfaces. You can also assign a secondary IP address to a loopback interface.

1. To configure a Loopback interface, navigate to the **Interfaces > Loopback** page and click **Add New Loopback**.
2. Specify your settings for the loopback interface.
3. Click **Add** to save the new Loopback Interface. Additional Loopback Interfaces can then be added and edited from this page.

Refer to

- Refer to the Ethernet Interfaces and PoE chapter in the *ArubaOS User Guide* for more information.
- Refer to the "**interface loopback**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Management

The management interface is located above the console port on the rear panel of the Mobility Access Switch. It is labeled as mgmt. The management port is a dedicated interface for out-of-band management purpose. This interface is specifically available for the management of the system and cannot be used as a switching interface. You can configure only the IP address and description for this interface. The management port can be used to access the Mobility Access Switch from any location and configure the system.

1. To configure a Gigabit Ethernet interface, navigate to the **Interfaces > Management** page.
2. Specify your settings for the interface.

3. Click **Save** to save the new interface.

Refer to

- Refer to the Ethernet Interfaces and PoE chapter in the *ArubaOS User Guide* for more information.
- Refer to the "**interface mgmt**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Port Channels

The **Interfaces > Port Channels** page allows you to add new port channels or edit the existing port channel. This page provides links to the following configurable options:

- LACP Global Config
- LACP Interface Config

LACP System Profile

The Link Aggregation Control Protocol (LACP), based on the IEEE 802.3ad standard, provides a standardized means for exchanging information with partner systems to form a dynamic link aggregation group.

After a system profile is configured, this profile can be used for configuring interface-level LACP options, including the port mode. Refer to the "LACP Profile" on page 67 section for more information.

1. To configure an LACP System Profile, navigate to the **Interfaces > Port Channels > LACP > Global Config** page.
2. Enter the LACP Priority value.
3. Select **Save** to save the LACP system profile.

Refer to

- Refer to the Port Channels chapter in the *ArubaOS User Guide* for more information.

- Refer to the "**lacp**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

LACP Profile

LACP profiles can be defined at the Interface level as well as at the Global level. (Refer to "LACP System Profile" on page 67 for information on configuring LACP at the global level.) When configuring an interface LACP profile, you can specify port mode, timeout settings, and priority values.

1. To configure an Interface LACP profile, navigate to the **Interfaces > Port Channels > LACP > Interface Config** page and click **Add New LACP Profile**.
2. Specify values for the profile
3. Click **Add** to save the new profile. Additional LACP profiles can then be added and edited from this page.

Routed VLAN Interfaces

Routed VLAN Interfaces (RVI) are logical interfaces that enable routing and bridging between VLANs. You can route and bridge a protocol on the same interface. The traffic that remains in the bridge group (the bridged traffic) will be bridged among the bridged interfaces, and the traffic that needs to go out to another network (the routed traffic) will be routed internally to the appropriate output routed interface.

There can be an IPv4 address for each VLAN interface. You can also configure IGMP and PIM interface profiles to the VLAN interfaces. A total of 4094 routed VLAN interfaces can be configured in this release. VLAN interface 1 is configured by default.

Important Points to Remember

- The maximum number of VLAN interfaces supported are 4094.
- The Layer 2 VLAN must be configured before configuring the corresponding RVIs.
- The protocol status of a RVI is in up state only when the protocol status of at least one member port in the corresponding VLAN is in up state.

To assign member ports to a VLAN, create a switching profile with the corresponding VLAN, and assign the switching profile to the member interfaces.

Configuring Routed VLAN Interfaces

1. To configure a Routed VLAN interface, navigate to the **Interfaces > Routed Virtual Interfaces** page and click **Add New Routed Virtual Interface**.
2. Specify your settings for the interface.
3. Click **Add** to save the new interface. Additional Routed VLAN Interfaces can then be added and edited from this page.

Refer to

- Refer to the Layer 3 Routing chapter in the *ArubaOS User Guide* for more information.
- Refer to the "**interface vlan**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Tunneled Node Profiles

Tunneled Node (previously known as Mux) provides the ability to tunnel the ingress packets (via GRE) from an interface on the Mobility Access Switch (Tunneled Node port) to an Mobility Controller (Tunneled Node server). You can use the Tunneled Nodes to allow the Mobility Controller to provide centralized security policy, authentication, and access-control.

Refer to the *ArubaOS User Guide* for important information regarding Tunneled Node support, including minimum version requirements, devices that support Tunneled Node, support for backup servers, and more.

1. To configure a Tunneled Node Server profile, navigate to the **Interfaces > Tunneled Node Server** page and click **Add New Tunneled Node Server Profile**. describes the fields that appear on this page.
2. Enter values for the tunneled node.
3. Click **Add** to save the new profile. Additional Tunneled Node Server profiles can then be added and edited from this page.

Refer to

- Refer to the Tunneled Nodes chapter in the *ArubaOS User Guide* for more information about tunneled nodes.
- Refer to the "`interface-profile tunneled-node-profile`" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Generic Routing Encapsulation

Generic Router Encapsulation (GRE) is an Aruba proprietary tunnel across Mobility Access Switches, Aruba controllers, and APs. This page provides links to the following configurable options:

- L2 Tunnel
- L3 Tunnel

L2 Tunnel

L2 GRE tunnel extends VLANs across Mobility Access Switches and Aruba controllers. GRE encapsulates Layer 2 frames with a GRE header and transmits through an IP tunnel over the cloud.

Perform these steps to create or edit an L2 tunnel.

1. Select **Interfaces > GRE > L2 Tunnel** page.
2. Select the **Add** button to create a new Ethernet tunnel, or click the pencil icon next to an existing Ethernet tunnel to edit.
3. Configure the settings for the L2 GRE tunnel.
4. Select **Add** or **Save**. The added or edited tunnel appears on the **L2 Tunnel** page.

Refer to

- Refer to the *Generic Router Encapsulation* chapter in the *ArubaOS User Guide* for more information about L2 GRE Tunnel.
- Refer to the **interface tunnel ethernet** command in the *ArubaOS Command-Line Interface Reference Guide* for information about the options that are available on this form.

L3 Tunnel

L3 GRE tunnel extends VLANs across Mobility Access Switches and Aruba controllers. GRE encapsulates Layer 3 frames with a GRE header and transmits through an IP tunnel over the cloud.

Perform these steps to create or edit an L3 tunnel.

1. Select **Interfaces > GRE > L3 Tunnel** page.
2. Select the **Add** button to create a new IP tunnel, or click the pencil icon next to an existing IP tunnel to edit.
3. Configure the settings for the L3 GRE tunnel.
4. Select **Add** or **Save**. The added or edited tunnel appears on the **L3 Tunnel** page.

Refer to

- Refer to the *Generic Router Encapsulation* chapter in the *ArubaOS User Guide* for more information about L3 GRE Tunnel.
- Refer to the "`interface tunnel ip`" command in the *ArubaOS* CLI Guide for information about the options that are available on this form.

Physical Media and PoE

The **Interfaces > Physical Media & PoE** page provides links to the following configurable options:

- Ethernet Link
- PoE Chassis Management
- PoE Interface Config
- PoE Time Range

Ethernet Link Profiles

You can use the Ethernet link profile to configure gigabit Ethernet switching and uplink ports. The Ethernet interfaces support auto negotiation from 10BaseT to 1000BaseT as per the IEEE 802.3u/z standards. When you enable auto negotiation, the device that is connected to the port is automatically configured to the highest speed supported by the device in the following order (highest to lowest):

- 10000 Mbps full duplex (supported only on the uplink interfaces)
- 1000 Mbps full duplex

- 100 Mbps full duplex
- 100 Mbps half duplex
- 10 Mbps full duplex
- 10 Mbps half duplex

The 1000 Mbps ports (10 gigabit uplink interfaces) cannot scale down to less than 1000 Mbps (1 gigabit speed).

Auto negotiation also supports the pause capabilities, automatic Media Detection Interface (MDI), and Media Detection Interface Crossover (MDIX) cable detection. The devices exchange information using the Fast link Pulse (FLP) bursts. The auto negotiation on the link is performed when you perform any of the following activities:

- Connect the device.
- Power on or reset the device at either end of the link.
- Make a negotiation request.

Ethernet Flow of Control

Ethernet flow control prevents loss of frames by providing a back pressure. When an Ethernet port receives frames faster than it can handle, it sends a PAUSE frame to stop the transmission from the sender for a specific period of time. The PAUSE frame has a destination group address of 01-80-c2-00-00-01.

When flow control frames are received, only pausing the transmit is supported. Sending flow control frames are not supported. This means that the system can only respond to PAUSE frames and cannot generate them. The flow control can be enabled or disabled to respond to incoming PAUSE frames.

Configuring Ethernet Link Profiles

1. To configure an Ethernet Link profile, navigate to the **Interfaces > Physical Media & PoE > Ethernet Link** page and click **Add New Ethernet Link Profile**.
2. Specify values for the profile.
3. Click **Add** to save the new profile. Additional Ethernet Link Profiles can then be added and edited from this page.

Refer to

- Refer to the Ethernet Interfaces and PoE chapter in the *ArubaOS User Guide* for more information about Ethernet link profiles.
- Refer to the "**interface-profile enet-link-profile**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

POE Chassis Management

Power over Ethernet (PoE) as per IEEE 802.3at is a technology for wired Ethernet LANs to carry the electric-power required for the device in the data cables. The IEEE standard defined in IEEE 802.3af allows network equipment (power sourcing equipment) to provide up to 15.4 Watts of power at the output for powered devices (PDs). In addition, the IEEE 802.3at (PoE+) standard provides more power to PDs where up to 30.0 Watts of power on output is delivered on the standard copper cable. The Aruba Mobility Access Switch supports both PoE standards.

Power Management Modes

The Aruba Mobility Access Switch supports three PoE power management modes:

- Static Mode—The power deducted from the total power pool is the maximum power for that interface. This mode ensures that the maximum power specified by you for the interface is always reserved and cannot be shared by other PDs.
- Dynamic Mode—The power allocated from the total power pool for each port is the actual power consumed at that port. You can allocate any unused portion of power to the other PDs. This is the default mode.
- Class-based Mode—The power allocated for each port from the total power pool is the maximum power available for the class of PD connected to that port.

PoE Guard Band

The PoE guard-band can provide protection when there is a sudden spike in the consumed power of powered devices that could potentially impact other PoE enabled ports. When the guard-band is configured, the Aruba Mobility Access Switch reserves a specified amount of power to prevent other PoE enabled ports from powering off and then powering back on again. The default value for guard-band is 11,000 milliwatts (mW). You can specify the guard-band value in increments of 1000 beginning with 1000mW. The maximum guard-band value that you can configure is 30,000mW.

Configuring a PoE Management Profile

1. To configure a PoE Management Profile, navigate to the **Interfaces > Physical Media & PoE > PoE > Chassis Management** page and click **Add New Poe Management Profile**.
2. Specify values for the profile.
3. Click **Add** to save the route. Additional Poe Management Profiles can then be added and edited from this page.

Refer to

- Refer to the Ethernet Interfaces and PoE chapter in the *ArubaOS User Guide* for more information about PoE profiles.
- Refer to the "**poe-management-profile**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

PoE Interface Configuration

PoE Profiles can be configured and then applied to interfaces. Perform the following steps.

1. To configure a PoE Profile, navigate to the **Interfaces > PoE > Interface Config** page and click **Add New PoE Profile**.
2. Specify your settings for the profile.
3. Click **Add** to save the new profile. Additional PoE profiles can then be added and edited from this page.

Refer to

- Refer to the Ethernet Interfaces and PoE chapter in the *ArubaOS User Guide* for more information.
- Refer to the "`interface-profile poe-profile`" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

PoE Time Range

The Mobility Access Switch supports time range for controlling the mode of the PoE power (enable/disable) to the PoE port.

The time range profile is disabled by default in the PoE profile.

The PoE time range can be configured in two modes: absolute and periodic. In absolute mode, the time parameters correspond to a specific time range: start date, start time, end date, and the end time. The PoE port is enabled if the current system time is within this range. In periodic mode, the user can specify start day, start time, end day, and end time. The start day or end day can be daily, weekend, weekday, or any day of the week. The PoE port is enabled if the current day and time falls within the range.

The following are the invalid combinations for start and end values for the time range parameters in the periodic mode:

- start-day: daily, end-day: any other day other than daily
- start-day: weekend, end-day: any other day other than a weekend. (Here weekend refers to Saturday or Sunday)
- start-day: weekday, end-day: any other day other than weekday

Avoid configuring the PoE time-of-day when the connected devices are in the process of being upgraded or when a power loss has rendered the connected device inoperable. In the case of an Aruba wireless Access Point, the PoE time-of-day should not be configured when an AP flash memory upgrade is in progress, as it may result in potential corruption of the flash.

1. To configure a PoE time range, navigate to the **Interfaces > PoE > Time-Range** page and click **Add New PoE Time-Range**.
2. Specify your settings for the time range.
3. Click **Add** to save the new time range. Additional time ranges can then be added and edited from this page.

Refer to

- Refer to the Ethernet Interfaces and PoE chapter in the *ArubaOS User Guide* for more information.
- Refer to the "`time-range-profile`" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Device-Group Profiles

Device group profiles assign a set of ArubaOS profiles to a switch interface, enable and disable access control lists (ACLs), and enable and disable the interface itself. These profiles are only supported by mobility access switches running ArubaOS 7.4.0.0 and later.

Device Group Setting	Description
Interface Trusted Mode	Click Yes to set this interface mode to trusted. When the QoS mode on a port is set to be trusted, the received 802.1P/DSCP is considered trustworthy and the frame is allowed to exit with those values intact.
Interface MTU (64-9216)	Maximum Transmission Unit (MTU) size for the interface.
Interface QOS Profile	A QoS profile assigns specific TC/DP, DSCP, and 802.1p values to the interface.
Interface PoE Profile	a PoE profile assigns max power and priority levels to the interface.
Interface AAA Profile	An AAA profile defines the authentication settings for the interface.

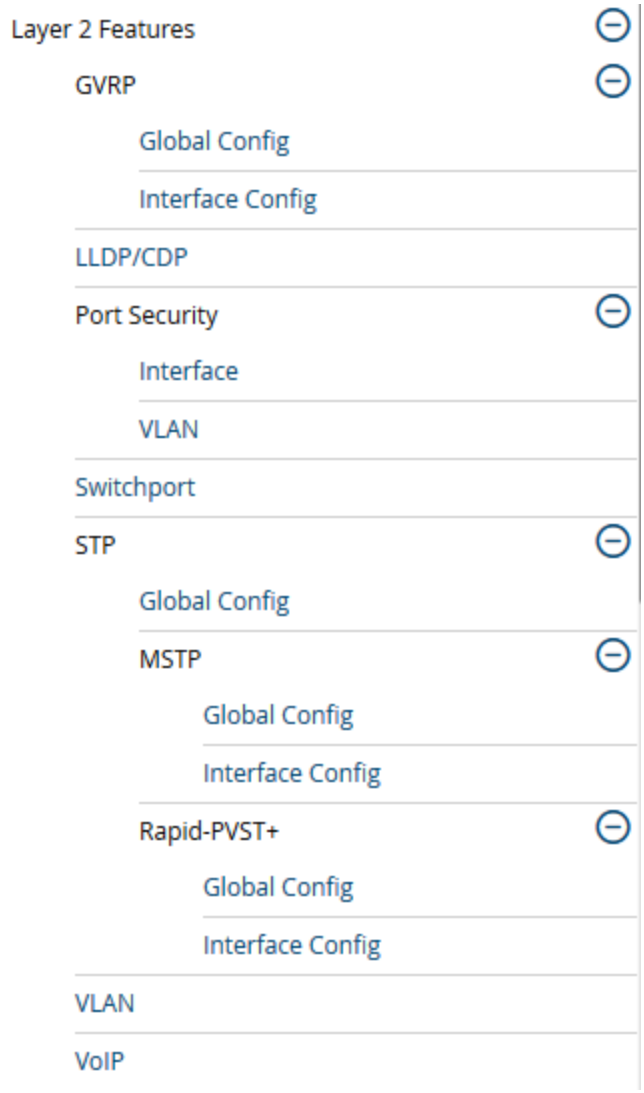
Device Group Setting	Description
Interface Ethernet Link Profile	An Interface Ethernet Link profile configures the gigabit Ethernet switching and uplink ports
Interface GVRP Profile	An Interface GVRP profile enables the switch to register/de-register the dynamic VLAN information received from a GVRP applicant on the network (such as an IAP).
Interface MSTP Profile	MSTP maps a group of Virtual Local Area Networks (VLANs) to a reduced number of spanning tree instances. With the Interface MSTP profile, you can enable BPDUguard, Rootguard, Portfast, and Loopguard options.
Interface PVST Profile	Rapid Per-VLAN Spanning Tree Plus (PVST+) provides for rapid recovery of connectivity following the failure of a device, a device port, or a LAN. Use the PVST profile to enable the loopguard, rootguard, BPDU, and PortFast features on the interface.
Interface LLDP Profile	Use the LLDP profile to enable a simple one-way neighbor discovery protocol with periodic transmissions of LLDP PDUs.
Interface Policer Profile	The Interface Policer profile limits inbound transmission rate of a class of traffic on the basis of user-defined criteria
Interface Switching Profile	The Interface Switching profile asigns VLAN memberships to an interface.
Interface Security Profile:	An Interface Security Profile can be used to restrict the number of MACs allowed on an interface using Router Advertisement Guard, DHCP Trust, Loop Protect, and MAC limits.
Interface Ingress ACL	Select an existing ingress ACL or create an new ingress ACL, and apply it to an interface.
Interface Egress ACL	Select an existing egress ACL or create an new egress ACL, and apply it to an interface.
Interface Session ACL	Select an existing session ACL or create an new session ACL, and apply it to an interface.
Interfaces to Shutdown	Enter the name of an interface a range of interfaces to disable the interface(s).

Layer 2 Features

Switch Configuration supports a variety of profiles that can be associated with Layer 2 protocols. Refer to the **Layer 2 Features** portion of the navigation pane on the **Switch Config** page (see Figure 50). The sections that

follow describe the profiles for all Layer 2 components in **Switch Config**.

Figure 50: *Layer 2 Components in Switch Config*



GVRP

The **Layer 2 Features > GVRP** page provides links to the following configurable options:

- Global GVRP Configuration
- Interface GVRP Profile

Global GVRP Configuration

Configuring GVRP in a Mobility Access Switch enables the switch to register/de-register the dynamic VLAN information received from a GVRP applicant such as an IAP in the network. GVRP support also enables the switch to propagate the registered VLAN information to the neighboring bridges in the network.

1. To configure a Global GVRP Management Profile, navigate to the **Layer 2 Features > GVRP > Global Config** page.

Additional GVRP profiles can be enabled on an interface. Refer to the "Interface GVRP Profiles" on page 75 section for additional information.

2. Specify values for the global configuration.
3. Click **Save** to save the edited GVRP settings.

Refer to

- Refer to the GVRP chapter in the *ArubaOS User Guide* for more information about GVRP.
- Refer to the "**gvrp**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Interface GVRP Profiles

Switch Config allows you to configure an Interface GVRP profile, in which you can specify the GVRP registration mode. In normal registrar mode, the Mobility Access Switch registers and de-registers VLANs to or from its connected switches and IAPs. In forbidden registrar mode, the Mobility Access Switch cannot register nor de-register VLANs to or from its connected switches and IAPs.

1. To configure an Interface GVRP Profile, navigate to the **Layer 2 Features > GVRP > Interface Config** page.

A GVRP profile can also be enabled globally. Refer to the "Global GVRP Configuration" on page 74 section for additional information.

2. Enable or disable GVRP on this interface profile and set the registration mode.
3. Click **Add** to save the new profile. Additional Interface GVRP Profiles can then be added and edited from this page.

Refer to

- Refer to the GVRP chapter in the *ArubaOS User Guide* for more information about GVRP.
- Refer to the "**interface-profile gvrp-profile**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

LLDP Profiles

Link Layer Discovery Protocol (LLDP), defined in the IEEE 802.1AB standard, is a Layer 2 protocol that allows network devices to advertise their identity and capabilities on a LAN. The Mobility Access Switch supports a simple one-way neighbor discovery protocol with periodic transmissions of LLDP PDU.

- LLDP frames are constrained to a local link.
- LLDP frames are TLV (Type-Length-Value) form.
- LLDP Multicast address is 01-80-C2-00-00-0E.

1. To configure an LLDP profile, navigate to the **Layer 2 Features > LLDP** page and click **Add New LLDP Profile**.
2. Specify values for this profile.
3. Click **Add** to save the new profile. Additional LLDP profiles can then be added and edited from this page.

Refer to

- Refer to the Link Layer Discovery Protocols chapter in the *ArubaOS User Guide* for more information about LLDP.

- Refer to the "**interface-profile lldp-profile**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Port Security Profiles

Port Security can be used to restrict the number of MACs allowed on an interface using Router Advertisement Guard, DHCP Trust, Loop Protect, and MAC limits.

The **Layer 2 Features > Port Security** page provides links to the following configurable options:

- Interface
- VLAN

Interface

The interface configuration for the layer 2 features are configured using the port security profile. You can configure the following port security options using the port security profile:

- Router Advertisement Guard
- DHCP trust
- Loop Protect
- MAC Limit

Router Advertisement Guard

The Router Advertisement (RA) Guard functionality analyzes the RAs and filters out RA packets sent by unauthorized devices. The RA guard feature is disabled by default. By enabling, the RA packets received on the interface are dropped and the port can be shutdown based on the interface configuration.

DHCP Trust

The DHCP trust functionality provides support to filter the IPv4 DHCP packets from the unauthorized devices. The following IPv4 DHCP messages are filtered on an interface configured not to trust DHCP.

- DHCP offer messages
- DHCP Ack messages

By default the DHCP packets are trusted on the interface. When the DHCP Trust is disabled, the aforementioned DHCP messages that are received on the interface are dropped.

Loop Protect

The Loop Protect functionality detects the unwanted physical loops in your network. A proprietary protocol data unit (PDU) is used to detect the physical loops in the network. When the system detects a loop, it disables the port that sends the PDU. You can re-enable the port automatically or manually

MAC Limit

The MAC limit feature restricts the maximum number of MACs that can be learned on the interface. When the MAC limit is enabled, it provides support to log the excess MACs or drop the new MAC learning requests or shuts down the port.

Configuring a Port Security Profile

1. To configure a Port Security profile, navigate to the **Layer 2 Features > Port Security** page and click **Add New Port Security Profile**.
2. Specify values for this profile.
3. Click **Add** to save the new profile. Additional Port Security profiles can then be added and edited from this page.

Refer to

- Refer to the Port Security chapter in the *ArubaOS User Guide* for more information about Port Security.
- Refer to the "**interface-profile port-security-profile**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

VLAN

The **Layer 2 Features > Port Security > VLAN** page allows you to add or edit a DHCP Snooping profile which is applied on a VLAN interface.

When DHCP snooping is enabled, the system snoops the DHCP messages to view DHCP lease information to build and maintain the DHCP snooping database. This database contains a list of valid IP address to MAC address bindings.

DHCP snooping helps to build the binding database to support the security features like IP Source Guard (IPSG) and Dynamic ARP Inspection (DAI).

Perform these steps to configure a DHCP Snooping profile.

1. Select **Layer 2 Features > Port Security > VLAN** page.
2. Click the **Add** button to create a profile. Click the pencil icon next to an existing profile to change the settings.
3. Configure or edit the settings for the profile.
4. Select **Add** to save a new profile. Click **Save** to save the changes to an edited profile.

Refer to

- Refer to the *DHCP Snooping* in the *ArubaOS User Guide* for more information about DHCP Snooping.
- Refer to the "**dhcp-snooping-database**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Port Switching (Switchport) Profiles

Switchport profiles are used for assigning VLAN memberships to interfaces.

1. To configure a Port Switching profile, navigate to the **Layer 2 Features > Switchport** page and click **Add New Switchport Profile**. You can set access and trunk settings.
2. To set **access** settings in bulk, select the Switchport Mode **access**.Access settings include:
   - Access VLAN (1-4094)
   - Enable Broadcast Traffic Rate Limit
   - Enable Multicast Traffic Rate Limit
   - Enable Unknown Unicast Rate Limit
   - Max Bandwidth Rate Limit
3. To set trunk settings in bulk, select the Switchport Mode **trunk**. Trunk settings include:
   - Native VLAN (1-4094)
   - Trunk Allowed VLANS
   - Enable Broadcast Traffic Rate Limit
   - Enable Multicast Traffic Rate Limit
   - Enable Unknown Unicast Rate Limit
   - Max Bandwidth Rate Limit
4. Select **Add** to save the new Switchport profile. Additional Switchport profiles can be added and edited from this page.

Refer to

- Refer to the VLANs chapter in the *ArubaOS User Guide* for more information switching profiles.
- Refer to the "`interface-profile switching-profile`" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

STP

The **Layer 2 Features > STP** page provides link to the following configurable options:

- Global Config
- MSTP
- Rapid-PVST+

Spanning Tree Global Config

The spanning tree mode for Aruba Mobility Access Switches defaults to MSTP. Use the Global Config to enable spanning tree operations and to change the spanning tree mode.

1. To change the mode, navigate to the **Layer 2 Features > STP > Global Config** page.
2. Enable or disable STP for this profile, and select the Spanning Tree Operating Mode.
3. Click **Save** to save the setting.

Refer to

- Refer to the MSTP and Rapids PVST chapters in the *ArubaOS User Guide* for more information about Spanning Tree.
- Refer to the "**spanning-tree mode**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

MSTP

MSTP maps a group of Virtual Local Area Networks (VLANs) to a reduced number of spanning tree instances. This allows VLAN bridges to use multiple spanning trees. This protocol enables network traffic from different VLANs to flow through different potential paths within a bridged VLAN. Because most networks do not need more than a few logical topologies, MSTP provides design flexibility as well as better overall network resource utilization.

Layer 2 networks typically use multiple paths and link redundancies to handle node and link failures. By definition, spanning tree uses a subset of the available physical links in its active logical topology to provide complete connectivity between any pair of end hosts.

Interface MSTP Profiles

With the Interface MSTP profile, you can enable BPDUguard, Rootguard, Portfast, and Loopguard options.

BPDUguard

The BPDU guard functionality prevents malicious attacks on edge ports. When the malicious attacker sends a BPDU on the edge port, it triggers unnecessary STP calculation. To avoid this attack, use the BPDU guard on that edge port. The BPDU guard enabled port shuts down as soon as a BPDU is received.

Rootguard

Rootguard provides a way to enforce the root bridge placement in the network. The rootguard feature guarantees that a port will not be selected as Root Port for the CIST or any MSTI. If a bridge receives superior spanning tree BPDUs (Bridge Protocol Data Units) on a rootguard-enabled port, the port is selected as an Alternate Port instead of Root Port and no traffic is forwarded across this port.

By selecting the port as an Alternate Port, the rootguard configuration prevents bridges, external to the region, from becoming the root bridge and influencing the active spanning tree topology.

Portfast

When the link on a bridge port goes up, MSTP runs its algorithm on that port. If the port is connected to a host that does not “speak” MSTP, it takes approximately 30 seconds for the port to transition to the forwarding state. During this time, no user data passes through this bridge port and some user applications may timeout.

Loopguard

Loopguard provides additional protection against Layer 2 forwarding loops (spanning tree loops). A spanning tree loop is created when a spanning tree blocking port, in a redundant topology, erroneously transitions to the forwarding state. This usually happens because one of the ports of a physically redundant topology (not necessarily the spanning tree blocking port) is no longer receiving spanning tree BPDUs.

If loopguard is enabled on a non-designated port receiving BPDUs, then that non-designated port is moved into the spanning tree loop-inconsistent blocking state.

Refer to the *ArubaOS User Guide* for important information regarding MSTP support.

Global MSTP Profiles

1. To configure a Global MSTP profile, navigate to the **Layer 2 Features > STP > MSTP > Global Config** page.
2. Specify values for this profile.
3. Click **Save** to save the profile.

Refer to

- Refer to the MSTP chapter in the *ArubaOS User Guide* for more information about MSTP.
- Refer to the "**mstp** command in the *ArubaOS Command-line Interface Reference Guide* for information about the options that are available on this form.

Configuring an Interface MSTP Profile

1. To configure an Interface MSTP profile, navigate to the **Layer 2 Features > STP > MSTP > Interface Config** page and click **Add New MSTP Port Profile**.
2. Enter values for this profile.
3. Click **Add** to save the new profile. Additional Interface MSTP Profiles can then be added and edited from this page.

Refer to

- Refer to the MSTP chapter in the *ArubaOS User Guide* for more information about MSTP.
- Refer to the "**interface-profile mstp-profile**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Rapid PVST+

Rapid Per-VLAN Spanning Tree Plus (PVST+) provides for rapid recovery of connectivity following the failure of a device, a device port, or a LAN. It also provides rapid convergence for edge ports, new root ports, and ports connected through point-to-point links.

Rapid PVST+ runs a separate spanning tree instance for each Virtual Local Area Network (VLAN). This allows the port to forward some VLANs while blocking other VLANs. PVST+ provides for load balancing of VLANs across multiple ports resulting in optimal usage of network resources.

Convergence occurs rapidly with Rapid PVST+. By default, each designated port in the spanning tree protocol sends out a BPDUs (Bridge Protocol Data Units) every 2 seconds. On a designated port in the topology, if hello

messages are missed three consecutive times, or if the maximum age expires, the port immediately flushes all protocol information from the table. A port considers that it loses connectivity to its direct neighbor designated port when it misses three BPDUs or if the maximum age expires. This rapid aging of the protocol information allows for quick failure detection.

Important Notes

- If your Mobility Access Switch is terminated on a router/switch spanning tree environment running PVST+, your Mobility Access Switch must be in PVST mode.
- Once in Rapid PVST+ mode, a predefined non-editable PVST profile automatically associates all configured VLANs (including default VLAN 1) and PVST+ starts running on all configured VLANs.
- Rapid PVST+ inter-operates seamlessly with IEEE and PVST bridges when the Mobility Access Switch is placed in a network.

Interface PVST Bridge Profiles

Rapid Per-VLAN Spanning Tree Plus (PVST+) provides for rapid recovery of connectivity following the failure of a device, a device port, or a LAN. It provides rapid convergence for edge ports, new root ports, and ports connected through point-to-point links. Interface-based PVST+ Bridge profiles enable you to configure Rapid PVST+ port properties. With the Interface PVST Bridge profile, you can enable PBDUguard, Rootguard, Portfast, and Loopguard options.

BPDUguard

The BPDU guard functionality prevents malicious attacks on edge ports. When the malicious attacker sends a BPDU on the edge port, it triggers unnecessary STP calculation. To avoid this attack, use the BPDU guard on that edge port. The BPDU guard enabled port shuts down as soon as a BPDU is received.

Rootguard

Rootguard provides a way to enforce the root bridge placement in the network. The rootguard feature guarantees that a port will not be selected as Root Port for the CIST or any MSTI. If a bridge receives superior spanning tree BPDUs (Bridge Protocol Data Units) on a rootguard-enabled port, the port is selected as an Alternate Port instead of Root Port and no traffic is forwarded across this port.

By selecting the port as an Alternate Port, the rootguard configuration prevents bridges, external to the region, from becoming the root bridge and influencing the active spanning tree topology.

Portfast

When the link on a bridge port goes up, spanning tree runs its algorithm on that port. If the port is connected to a host that does not communicate with the spanning tree, it takes approximately 30 seconds for the port to transition to the forwarding state. During this time, no user data passes through this bridge port and some user applications may timeout.

Loopguard

Loopguard provides additional protection against Layer 2 forwarding loops (spanning tree loops). A spanning tree loop is created when a spanning tree blocking port, in a redundant topology, erroneously transitions to the forwarding state. This usually happens because one of the ports of a physically redundant topology (not necessarily the spanning tree blocking port) is no longer receiving spanning tree BPDUs.

If loopguard is enabled on a non-designated port receiving BPDUs, then that non-designated port is moved into the spanning tree loop-inconsistent blocking state.

Configuring a Rapid PVST+ Profile

1. To configure a Rapid PVST Profile, navigate to the **Layer 2 Features > STP > Rapid PVST+ > Global Config** page and click **Add New Rapid-PVST+ Profile**.
2. Specify values for this profile

3. Click **Add** to save the profile. Additional Rapid PVST+ Profiles can then be added and edited from this page.

Refer to

- Refer to the Rapid PVST+ chapter in the *ArubaOS User Guide* for more information about Rapid PVST.
- Refer to the "**vlan-profile pvst-profile**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Configuring an Interface PVST Bridge Profile

1. To configure an Interface PVST+ Bridge profile, navigate to the **Layer 2 Features > STP > Rapid PVST+ > Interface Config** page and click **Add New Rapid-PVST Port Profile**.
2. Specify values for this profile.
3. Click **Add** to save the new profile. Additional Interface PVST Bridge profiles can then be added and edited from this page.

Refer to

- Refer to the Rapid PVST+ chapter in the *ArubaOS User Guide* for more information about interface PVST bridge profiles.
- Refer to the "**interface-profile pvst-port-profile**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

VoIP Profiles

The VoIP VLAN feature enables access ports to accept both untagged (data) and tagged (voice) traffic from IP phones connected directly to the Mobility Access Switch and separate these traffic into different VLANs (namely data VLAN and voice VLAN). You can configure a voice VLAN using the voip-profile. The dot1p and DSCP values in the VoIP profile are communicated to the phone using LLDP. VoIP profile does not affect the QoS behavior on the switch. The QoS behavior depends on the QoS configuration on the port.

You can configure VoIP either in static mode or auto-discover mode. By default, VoIP is configured in static mode. When VoIP operates in static mode, the phone is expected to know the Voice VLAN to be used and send the Voice traffic with the Voice VLAN tag. This is achieved, only if the Voice VLAN is configured statically on the phone or propagated to the phone using LLDP-MED. In auto-discover mode, when LLDP-MED or CDP discovers a phone, the switch creates a rule to associate all the traffic originating from the phone to the Voice VLAN. Hence, the Voice VLAN need not be configured statically on the phone. The Voice VLAN can be tagged or untagged depending on the LLDP-MED configuration.

When VoIP is configured in auto-discover mode applies the Voice VLAN only to the first neighbor discovered in an interface. If both LLDP-MED and CDP neighbors are discovered, the preference is always given to the first LLDP-MED neighbor even if a CDP neighbor is already associated.

1. To configure a VoIP profile, navigate to the **Layer 2 Features > VoIP** page and click **Add New VoIP Profile**. Be sure to review the *ArubaOS User Guide* for important limitations and guidelines to consider when creating a VoIP profile.
2. Specify values for this profile.
3. Click **Add** to save the new profile. Additional VoIP profiles can then be added and edited from this page.

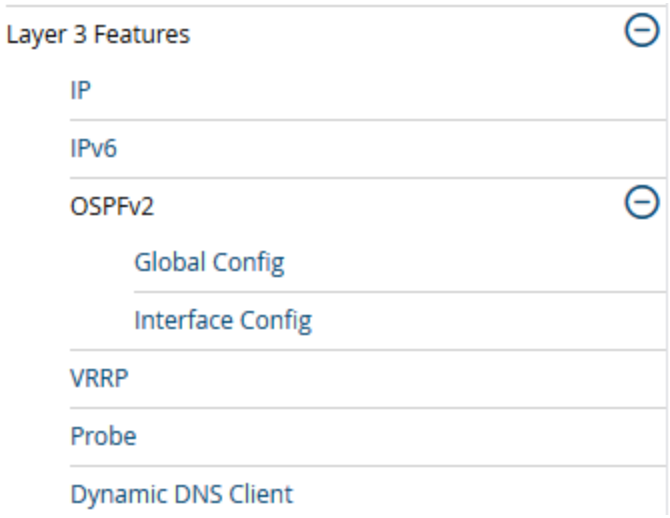
Refer to

- Refer to the VoIP chapter in the *ArubaOS User Guide* for more information about VoIP.
- Refer to the "**interface-profile voip-profile**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Layer 3 Features

Switch Configuration supports a variety of profiles that can be associated with routes and protocols. Refer to the **Layer 3 Features** portion of the navigation pane on the **Switch Config** page (see Figure 51). The sections that follow describe the profiles for all Layer 3 components in **Switch Config**.

Figure 51: *Layer 3 Components in Switch Config*



IP Profile

The Aruba Mobility Access Switch supports static routes configuration. You can configure a default gateway and multiple static routes within the global IP-profile to route packets outside the local network. The static routes are active or added to the routing table only when the next hop is reachable, and can be removed from the static routes list.

Each static route requires a destination, netmask, and nexthop addresses. Equal-Cost Multi-Path (ECMP) is not supported in the current release. This implies that each destination/netmask needs a unique nexthop address. The static routes are inserted in to the FIB, only when the nexthop matches the subnet of any of the RVI interfaces or the management interface. If the nexthop becomes unreachable, the RIB gets purged but the static route is still retained.

Important Points to Remember

- You can have only one default gateway. However, you can have multiple static routes.
- You can have both an IPv4 and an IPv6 default gateway simultaneously.
- Static routes become active only when the nexthop is reachable.
- Nexthops have to be within the local network.
- Each destination/netmask needs a unique nexthop address.
- The nexthop of the default gateway can either be the management interface or a routed VLAN interface.

Default Gateways

A default gateway is a special case of static route where the destination mask and prefix is 0/0. The next hop in a default gateway can be any valid IP address that can be reached through a routing table or the management interface.

1. To configure a static route, navigate to the **Layer 3 Features > IP** page.
2. Specify values for this profile.
3. Click **Save**to save the route.

Refer to

- Refer to the Ethernet Interfaces and PoE chapter in the *ArubaOS User Guide* for more information about IP profiles.
- Refer to the "**ip-profile**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

IPv6 Profile

The IPv6 protocol enables the next generation of large-scale IP networks by supporting addresses that are 128 bits long. This allows 2^{128} possible addresses (versus 2^{32} possible IPv4 addresses).

1. To configure an IPv6 Default Gateway, navigate to the **Layer 3 Features > IPv6** page.
2. Specify the default gateway for this profile.
3. Click **Save** to save the IPv6 default gateway address.

Refer to

- Refer to the IPv6 chapter in the *ArubaOS User Guide* for more information about IPv6.
- Refer to the "**ipv6-profile**" command in the *ArubaOS CLI Guide* for information about configuring IPv6.

OSPFv2

Open Shortest Path First (OSPFv2) is a dynamic interior gateway routing protocol (IGP) based on IETF RFC 2328. The Aruba implementation of OSPFv2 allows the Mobility Access Switch (MAS) to be effectively deployed in a Layer 3 topology.

Key Features Supported by MAS

- All stub area types
- Area border router (ABR)
- OSPF on VLAN and loopback interfaces
- OSPF MD5 authentication
- One OSPF instance
- Redistribute VLANs
- OSPF interface can belong to only one area

LSAs Originated by MAS

With current implementation, the following Link State Advertisement (LSA) types are generated by MAS:

- Type 1 Router LSA
- Type 2 Network LSA
- Type 3 Summary LSA
- Type 4 ASBR Summary LSA

Notes:

- Routes learned from VLAN-based access interfaces are distributed to OSPF as Router LSAs (Type 1).
- MAS can process Type 5 AS External LSA.

OSPFv2 Global Config

Use the OSPFv2 Global Config to configure a global OSPFv2 profile. This profile can then be applied to Routed VLAN interfaces or Loopback Interfaces.

1. To change the mode, navigate to the **Layer 3 Features > OSPFv2 > Global Config** page.
2. Enable or disable OSPF and specify settings for this profile.
3. Click **Save** to save the settings.

Refer to

- Refer to the OSPFv2 chapter in the *ArubaOS User Guide* for more information about OSPF.
- Refer to the "**router ospf**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Interface OSPF Profiles

Aruba's implementation of Open Shortest Path First (OSPFv2) is based on RFC 2328. OSPF profiles can be applied to Layer 3 routed VLAN interfaces and to loopback interfaces.

1. To configure an Interface OSPF profile, navigate to the **Layer 3 Features OSPFv2 > Interface Config** page and click **Add New OSPFv2 Interface Profile**.
2. Specify values for this profile.
3. Click **Add** to save the new profile. Additional Interface OSPF profiles can then be added and edited from this page.

Refer to

- Refer to the OSPFv2 chapter in the *ArubaOS User Guide* for more information about OSPFv2.
- Refer to the "**interface-profile ospf-profile**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

VRRP

Virtual Router Redundancy Protocol (VRRP) enables a group of layer 3 configured Mobility Access Switches to form a single virtual router.

Perform these steps to create or edit a VRRP instance.

1. Select **Layer 3 Features > VRRP** page.
2. Select the **Add** button to create a new VRRP instance, or click the pencil icon next to an existing VRRP instance to edit.
3. Configure the settings for the VRRP instance.
4. Select **Add** or **Save**. The added or edited instance appears on the **VRRP** page.

Refer to

- Refer to the *Virtual Router Redundancy Protocol* chapter in the*ArubaOS User Guide* for more information about VRRP.
- Refer to the "`vrrp`" command in the *ArubaOS* CLI Guide for information about the options that are available on this form.

Quality of Service

A Quality of Service (QoS) profile can be configured to assign specific TC/DP, DSCP, and 802.1p values. This profile can then be applied to an interface profile, a stateless access list, user roles, and policer profiles.

The Aruba Mobility Access Switch supports the following with regards to QoS profiles:

- A QoS profile can be applied to an interface, user role, and traffic flow.
- Eight queues are available per interface in the hardware.
- Eight traffic classes (TC) are available, which map to the corresponding queue (0 – 7).
- A drop-precedence of "low" or "high" for controlling tail-drop.

QoS Profiles can be configured in Trusted or Untrusted modes.

Trusted Mode

When the QoS mode on a port is set to be trusted, the received 802.1p/DSCP is considered trustworthy and the frame is allowed to exit with those values intact. The received DSCP or 802.1p value is used to index predefined QoS profiles to determine traffic class and drop precedence. These QoS profiles cannot be edited at this time.

The Aruba Mobility Access Switch supports the following Trust modes:

- Layer 2 QoS Trust Mode: The port is configured to trust the IEEE 802.1p user priority. This is relevant for 802.1q packets.
- Layer 3 QoS Trust Mode: The port is configured to trust the received DSCP value of the frame.
- Auto (L2+L3) Trust Mode: This mode prioritizes DSCP over 802.1p. If the received frame is IP, the DSCP value is used for indexing the QoS profile. If the received tagged frame is non-IP, then the 802.1p value is used for indexing the QoS profile.

Table 9 below shows DSCP-Queue mapping:

Table 9: *DSCP-Queue Mapping*

DSCP	802.1p	Queue
0-7	0	0
8-15	1	1
16-23	2	2
24-31	3	3
32-39	4	4
40-47	5	5
48-55	6	6
56-63	7	7

Drop Precedence

Drop precedence can be defined as Low or High. The drop precedence is Low for the first 4 values (0-3) and Hi for the last for values (4-7) for each DSCP range. For 802.1p, the drop precedence is defined as Low for all values.

Untrusted Mode

Untrusted Mode is the default for all interfaces where incoming traffic is mapped to TC "0" and then subsequently mapped to egress queue "0."

Profile

- QoS profile can be configured to assign specific TC/DP, DSCP, and 802.1p values.
- The QoS profile can be then applied to:
  - Interface (interface-profile)
  - Stateless access-list
  - User-role
  - Policer profile

Policing

- Limits inbound transmission rate of a class of traffic on the basis of user-defined criteria.
- Policer can be applied to stateless ACL, interface, and user-role.
- 1-rate 3-color policer is supported at FCS.
  - Traffic rate below CIR or burst below CBS limit is considered “conforming” and is allowed to pass through the policer.
  - Traffic rate exceeding CIR, and bursting below EBS limit is considered “exceeding” and is allowed to pass through the policer by default.
  - Traffic rate exceeding CIR, and bursting above EBS limit is considered “violating” and is dropped at the policer by default.

Configuring QoS

1. To configure a QoS Profile, navigate to the **Quality of Service > QoS** page and click **Add New QoS Profile**.
2. Specify values for this profile.
3. Click **Add** to save the profile. Additional QoS Profiles can then be added and edited from this page.

Refer to

- Refer to the Quality of Service chapter in the *ArubaOS User Guide* for more information about QoS.
- Refer to the "**qos-profile**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Configuring Policer

1. To configure a Policer profile, navigate to the **Quality of Service > Policer** page and click **Add New Policer Profile**.
2. Specify values for this profile.
3. Click **Add** to save the profile. Additional Policer profiles can then be added and edited from this page.

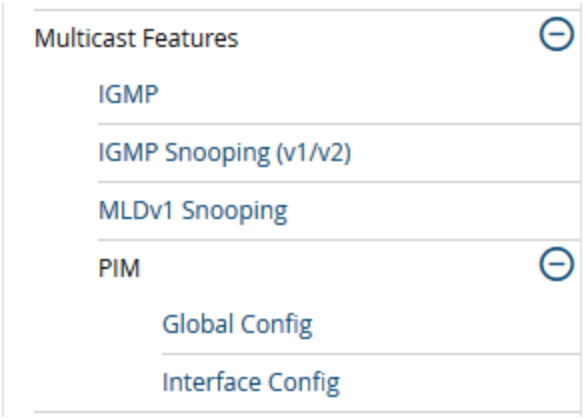
Refer to

- Refer to the Quality of Service chapter in the *ArubaOS User Guide* for more information about Policer profiles.

- Refer to the "**policer-profile**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Multicast Features

Aruba Mobility Access Switches include support for multicast routing protocols including IGMPv1/v2, MLDv1, and PIM-SM.



Interface IGMP Profiles

The Mobility Access Switch supports Internet Group Management Protocol (IGMP) as defined in IETF RFC 1112 (IGMPv1) and RFC 2236 (IGMPv2). IGMP allows hosts and adjacent routers on IP networks to establish multicast group memberships.

1. To configure IGMP Snooping for interfaces, navigate to the **Multicast Features > IGMP** page and click **Add New IGMP Interface Profile**.
2. Enable or disable IGMP for this profile, and specify a query interval value.
3. Click **Add** to save the new profile. Additional IGMP profiles can then be added and edited from this page.

Refer to

- Refer to the IGMP and PIM-SM chapter in the *ArubaOS User Guide* for more information about IGMP and PIM support.

- Refer to the "**interface-profile igmp-profile**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

IGMP Snooping

The Mobility Access Switch supports IGMPv1 and v2 snooping, which prevents multicast flooding on Layer 2 network treating multicast traffic as broadcast traffic. All streams could be flooded to all ports on that VLAN. When multicast flooding occurs, end-hosts that happen to be in the same VLAN would be receiving all the streams only to be discarded without snooping.

When you enable IGMP snooping, the switch becomes IGMP-aware and processes the IGMP control messages as received. You must do this to correctly process all IGMP membership reports and IGMP leave messages. IGMP snooping is handled by the hardware for performance. Multicast routers and multicast receivers associated with each IP multicast group are learned dynamically.

1. To configure IGMP Snooping for interfaces, navigate to the **Multicast Features > IGMP Snooping (v1/v2)** page and click **Add New IGMP Snooping**.
2. Specify values for this profile.

3. Click **Add** to save the new profile. Additional IGMP Snooping Profiles can then be added and edited from this page.

Refer to

- Refer to the IGMP Snooping chapter in the *ArubaOS User Guide* for more information about IGMP Snooping.
- Refer to the "**vlan-profile igmp-snooping-profile**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

MLDv1 Snooping

Multicast Listener Discovery (MLD) is a component of the Internet Protocol Version 6 (IPv6) suite. It is used by IPv6 routers for discovering multicast listeners on a directly attached link. When multicast is supported at the IPv6 level, it often broadcasts at lower levels. So, for example, an Ethernet switch broadcasts multicast traffic on all ports, even if only one host wants to receive it.

To prevent entire Ethernet segments from being flooded, MLD snooping can be implemented on Ethernet switches. The MLD snooping solution is similar to the IGMP snooping solution for IPv4. When MLD snooping is implemented on a switch, it detects all MLD version 1 messages that are exchanged on the link. It also maintains a table that indicates which IPv6 multicast groups should be forwarded for each of the interfaces.

Important Notes

- ArubaOS 7.2.0.0 supports MLDv1 (RFC 2710), so MLDv2 specific packets are not processed.
- MLD snooping prevents multicast flooding on an Ethernet link, but it requires complex processing for each of the interfaces on switches that were not initially designed for this kind of task.
- Unlike IGMP, which uses a separate protocol, MLD is embedded in ICMPv6. MLDv1 is similar to IGMPv2 and MLDv2 is similar to IGMPv3.

Configuring an MLDv1 Snooping Profile

1. To configure an MLD Snooping Profile, navigate to the **Multicast Features > MLDv1 Snooping** page and click **Add New MLDv1 Snooping Profile**.
2. Specify values for this profile.
3. Click **Add** to save the profile. Additional MLD Snooping Profiles can then be added and edited from this page.

Refer to

- Refer to the MLD Snooping chapter in the *ArubaOS User Guide* for more information about MLD Snooping.
- Refer to the "**vlan-profile mld-snooping-profile**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Protocol Independent Multicast

Protocol-Independent Multicast (PIM) is a family of multicast routing protocols for Internet Protocol (IP) networks that provide one-to-many and many-to-many distribution of data over a LAN, WAN or the Internet. It is termed protocol-independent because PIM does not include its own topology discovery mechanism, but instead uses routing information supplied by other traditional routing protocols. There are four variants of PIM. Currently, Switch Config supports PIM Sparse Mode (PIM-SM) only. PIM-SM explicitly builds unidirectional shared trees rooted at a rendezvous point (RP) per group, and optionally creates shortest-path trees per source. PIM-SM is recognized for scaling well for wide-area usage. PIM-SM is useful for routing multicast streams between VLANs, subnets, or local area networks (LANs) in applications such as IPTV.

Configuring a Global PIM Rendezvous Point

1. To configure a Global PIM profile, navigate to the **Multicast Features > PIM > Interface PIM** page and click **Add New Static Rendezvous Point**.
2. Specify the IP address, group address, and mask value.
3. Select **Add** to save the new rendezvous point. Additional Rendezvous Points can then be added and edited from this page.

Refer to

- Refer to the IGMP and PIM-SM chapter in the *ArubaOS User Guide* for more information about PIM profiles.
- Refer to the "**router-pim**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Configuring an Interface PIM Profile

1. To configure an Interface PIM profile, navigate to the **Multicast Features > PIM > Interface PIM** page and click **Add New PIM Interface Profile**.
2. Specify values for this profile.
3. Select **Add** to save the new profile. Additional Interface PIM profiles can then be added and edited from this page.

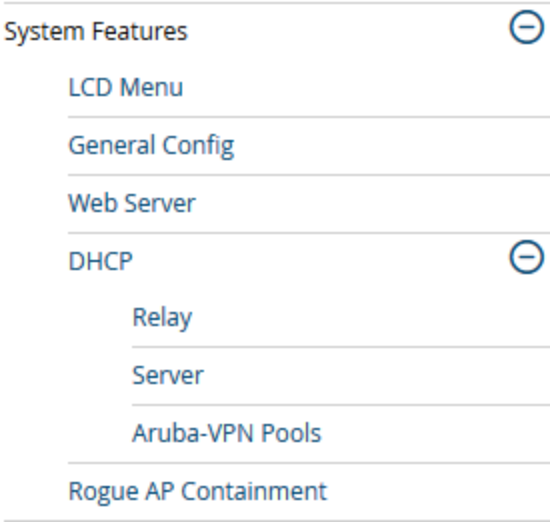
Refer to

- Refer to the IGMP and PIM-SM chapter in the *ArubaOS User Guide* for more information about PIM profiles.
- Refer to the "**interface-profile pim-profile**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

System Features

Switch Configuration supports a variety of profiles that can be associated with DHCP. Refer to the **System Features** portion of the navigation on the **Switch Config** page (see).

Figure 52: *System Features*



LCD Menu

In addition to displaying current status, LCD panel supports a user-interactive maintenance mode. You can configure the following settings under the LCD menu options for a standalone switch or an ArubaStack:

- ArubaOS software image upgrade
- Configuration file upload
- Erase configuration (write erase all)
- Factory default setting (restore factory-default stacking)
- Media (external USB) eject
- System reboot (reload)
- System Halt (halt)
- GUI Quick Setup

Select the **System Features > LCD Menu** page to enable or disable the various LCD menu options and select **Save**.

- Refer to the *System Basics* chapter in the *ArubaOS User Guide* for more information about LCD menu options.
- Refer to the "`lcd-menu`" command in the *ArubaOS Command Line Interface Reference Guide* for information about the options that are available on this form.

General Config

The General Config component is used for local configuration of switching devices. Locally configured settings are not pushed to local switches by the master controller.

Select the **System Features > General Config** page to specify whether to enable DHCP services. Table 10 describes the fields for this page.

Table 10: *System Features > General Config fields*

Field	Default	Description
NTP Settings		
NTP Authentication	No	Enable or disable Network Time Protocol (NTP) authentication.
NTP Server	N/A	Optionally add an NTP server by specifying an IP address, Iburst mode and Authentication key.
NTP Identification Keys	N/A	Click **Add** to add new NTP identification keys.
NTP Trusted Keys	N/A	Click **Add** to add new NTP Trusted keys.
Time Zone		
Name	PST	Specify the time zone name.
Hour Offset from GMT (-23-23)	-8	Specify the hour offset from GMT.
Minute Offset from GMT (0-59)	0	Specify the minute offset from GMT

Table 10: *System Features > General Config fields (Continued)*

Field	Default	Description
Summer Time Zone		
Adjust Clock in Summer	No	Enable the clock to automatically adjust in summer.
Domain Settings		
Enable IP Domain Name System Hostname Translation	Yes	Enable or disable DNS hostname translation.
Domain Name	N/A	Specify a domain name.
Domain Name Servers	N/A	Click **Add** to add a new Domain name server.

Select **Save** when you are finished.

Web Server

The Web server component is used for configuring the default Web SSH management profile.

Select the **System Features > Web Server** page to specify the web server settings and selecting certificates for the devices in the group. Table 11 describes the fields for this page.

Table 11: *System Features > General Config fields*

Field	Default	Description
Settings		
Web UI User/Password Authentication	Yes	Specify whether to enable the DHCP service for the group.
Web UI Certificate Authentication	No	Enable or disable UI certificate authentication.
Web Server Certificate	Default	Select the web server certificate from the drop-down.
Web UI Idle Timeout (30-3600 sec)	900	Configure the UI session timeout between 30 to 3600 seconds.
Captive Portal Certificate	Default	Select the certificate to be used for Captive Portal.
Cipher	high	Set the cipher encryption level to low, medium, or high.
Maximum Supported Concurrent Clients (25-400)	25	Set the maximum number of clients between 25 and 400 that can connect simultaneously.
SSL Protocol	Yes	Enable or disable SSL protocol.

Table 11: *System Features > General Config fields (Continued)*

Field	Default	Description
TLS Protocol	Yes	Enable or disable TLS protocol.
Certificates		
Select the Certificates to apply to devices in this Group	N/A	Select an available certificate, or use the + sign to add additional certificates.

Select **Save** when you are finished.

DHCP

You can enable or disable DHCP service by navigating to **System Features > DHCP** page. This page provides links to the following configurable options:

- Relay
- Server

DHCP Relay Profile

DHCP-Relay is supported with DHCP Option 82. DHCP Option 82 allows a DHCP relay agent to insert circuit specific information into a request that is being forwarded to a DHCP server.

Clients on subnets that are not directly connected to a DHCP server must go through a "relay agent." If DHCP relay is not enabled on the VLAN on which the request is received, but a pool is configured for that subnet, the IP is assigned from the internal DHCP server.

DHCP relay is enabled when a DHCP relay profile is attached to a VLAN interface. At this point, the relay agent receives the DHCP broadcast packets from the client and unicasts them to one or more of the DHCP servers that are configured on the VLAN interface. The relay agent stores its own IP address in the Gateway IP Address (GIADDR) field of the DHCP packet. The DHCP server uses the GIADDR to determine the subnet on which the relay agent received the broadcast and allocates an IP address on that subnet. When the DHCP server replies to the client, the reply is unicasted to the GIADDR. The relay agent then retransmits the response on the local network.

DHCP Option 82 works by setting two sub-options:

- Circuit ID: The circuit ID includes information specific to the circuit on which the request arrives. Circuit identifier parameters can be interface name, VLAN ID, or both.
- Remote ID: The remote ID carries information relating to the remote host end of the circuit. Remote identifier parameters can be the MAC address or the hostname of the relay agent.

DHCP Relay Option 82 can be configured using a DHCP Relay profile.

Configuring a DHCP Relay Profile

1. You can configure a DHCP Relay profile by selecting the **Add New DHCP Relay Profile** button on the **DHCP > Relay** page of Switch Config.
2. Specify values for the new profile.
3. Select **Add** to create the DHCP Relay profile.

Refer to

- Refer to the DHCP Server & DHCP Relay chapter in the *ArubaOS User Guide* for more information about DHCP Relay profiles.

- Refer to the **interface-profile dhcp-relay-profile** command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

DHCP Server Profile

Dynamic Host Configuration Protocol (DHCP) automates network-parameter assignment to network devices from one or more DHCP servers. When a DHCP-configured client connects to a network, the DHCP client sends a broadcast query requesting necessary information from a DHCP server. The DHCP server manages a pool of IP addresses and information about client configuration parameters such as default gateway, domain name, servers, etc.

On receiving a valid request, the server assigns the computer an IP address, a lease (length of time the allocation is valid), and other IP configuration parameters, such as the subnet mask and the default gateway. The query is typically initiated immediately after booting, and must complete before the client can initiate IP-based communication with other hosts. During initialization, network clients try to dynamically obtain their IP addresses. In small networks, where all the systems are in the same IP subnet, the client and the server can communicate directly.

Configuring a DHCP Server Profile

1. You can configure a DHCP Relay profile by selecting the **Add New DHCP Server Profile** button on the **DHCP > Server** page of Switch Config.
2. Specify values for the new profile.
3. Select **Add** to create the DHCP Server profile.

Refer to

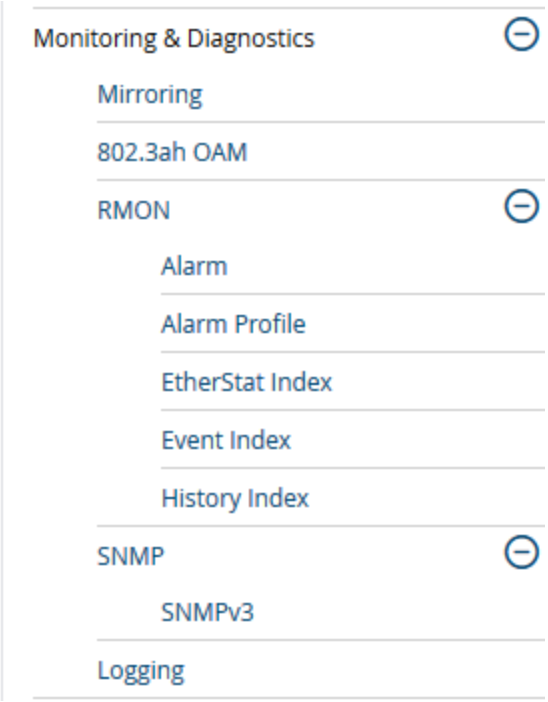
- Refer to the DHCP Server & DHCP Relay chapter in the *ArubaOS User Guide* for more information about DHCP Server profiles.

- Refer to the "**interface-profile dhcp-server-profile**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Monitoring and Diagnostics

Switch Configuration supports a variety of profiles that can be associated with Monitoring and Diagnostics features on your switch. Refer to the **Monitoring & Diagnostics** portion of the navigation pane on the **Switch Config** page, (see). The sections that follow describe the profiles for all Monitoring and Diagnostics components in **Switch Config**.

Figure 53: *Monitoring & Diagnostics Components in Switch Config*



Mirroring Profiles

Switch Config supports port mirroring, which can be used to send copies of all or sampled packets seen on specific port(s) or port-channel to a destination. Port mirroring can also be used for appliances such as sniffers that monitor network traffic for further analysis.

The Mirroring profile allows you to specify a destination port. A single port can be the destination interface. (Port-channels and VLANs cannot be a destination.) Normal traffic forwarding will not be performed on the destination port; only the mirrored packets can be received on the destination port. A destination port cannot be a port mirroring source port at the same time. The destination port does not participate in any Layer 2 protocol, including Spanning-tree. Switching profiles, such as access or trunk profiles, cannot be applied on the destination port.

1. To configure a Mirroring profile, navigate to the **Monitoring & Diagnostics > Mirroring** page and click **Add New Mirroring Profile**.
2. Specify the Destination GigabitEthernet Interface and the port mirroring ratio.
3. Select **Add** to save the new profile. Additional Mirroring profiles can then be added and edited from this page.

Refer to

- Refer to the Port Mirroring chapter in the *ArubaOS User Guide* for more information about Mirroring profiles.
- Refer to the "**interface-profile mirroring-profile**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

802.3ah OAM Profiles

Operations, Administration, and Maintenance (OAM) refers to the tools and utilities to install, monitor, and troubleshoot a network. OAM tools report layer-2 network behavior, which can help network administrators monitor and troubleshoot a network without sending technicians into the field to diagnose problems on location. OAM provides mechanisms to monitor link operations and health and to improve fault isolation.

The MAS OAM feature supports the following Link Fault Management options:

- Discovery – An OAM-enabled local interface discovers a remote interface enabled with OAM and notifies each other of their own capabilities. After discovery, both sides send OAM PDUs periodically to monitor the link.
- Remote fault detection – Detection and handling of faulty links, such as those not receiving an OAM PDU from the other peer within the configured time-out or an OAM PDU with a “link-fault” flag.
- Remote loopback – Link segment testing is controlled remotely using test frames. Usually remote loopback is used during installation or for troubleshooting.

1. To configure and OAM profile, navigate to the **Monitoring & Diagnostics > OAM** page and click **Add New OAM Profile**.
2. Specify values for this profile.
3. Select **Add** to save the new profile. Additional OAM profiles can then be added and edited from this page.

Refer to

- Refer to the Operations, Administration, and Maintenance chapter in the *ArubaOS User Guide* for more information about OAM profiles.

- Refer to the "**interface-profile oam--profile**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Remote Monitoring (RMON)

Remote Monitoring (RMON) provides standard information that a network administrator can use to monitor, analyze, and troubleshoot a group of distributed local area networks (LANs). Monitoring devices (commonly called "probes") contain RMON software agents that collect information and analyze packets. These probes act as servers and the Network Management applications that communicate with them act as clients. While both agent configuration and data collection use SNMP, RMON is designed to operate differently than other SNMP-based systems:

- Probes have more responsibility for data collection and processing, which reduces SNMP traffic and the processing load of the clients.
- Information is only transmitted to the management application when required, instead of continuous polling.

ArubaOS supports the following RMON groups:

- Ethernet statistics
- History control
- Ethernet history
- Alarm
- Event Index

Enabling RMON

Perform the following steps to enable RMON.

1. Navigate to the **Monitoring & Diagnostics > RMON** page.
2. Select **Yes** for the Enable RMON Service option.
3. Click the **Save** button.

Configuring an Alarm

1. To configure an Alarm entry, navigate to the **Monitoring & Diagnostics > RMON > Alarm** page and click **Add New Alarm**.
2. Specify values for this Alarm entry.
3. Click **Add** to save the new Alarm entry. Additional Alarms can then be added and edited from this page.

Refer to

- Refer to the Remote Monitoring (RMON) chapter in the *ArubaOS User Guide* for more information about Alarms.
- Refer to the "**rmon alarm**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Alarm Profile

Create an alarm profile and associate that profile with an alarm entry.

1. To configure an Alarm Profile, navigate to the **Monitoring & Diagnostics > RMON > Alarm Profile** page and click **Add New Alarm Profile**.
2. Specify values for this Alarm profile.
3. Click **Add** to save the new Alarm profile. Additional Alarms profiles can then be added and edited from this page.

Refer to

- Refer to the Remote Monitoring (RMON) chapter in the *ArubaOS User Guide* for more information about Alarms.
- Refer to the "**rmon alarm-profile**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Ethernet Statistics Index

Perform the following steps to configure Ethernet statistics collection on an interface.

1. To configure an Alarm entry, navigate to the **Monitoring & Diagnostics > RMON > EtherStat Index** page and click **Add New EtherStat Index**.
2. Specify values for this entry.
3. Click **Add** to save the new Ethernet Statistics entry. Additional Ethernet Statistic entries can then be added and edited from this page.

Refer to

- Refer to the Remote Monitoring (RMON) chapter in the *ArubaOS User Guide* for more information about Ethernet Statistics.
- Refer to the "**rmon etherstat**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Event Index

An Event Index specifies the action to take when an alarm triggers an event.

1. To configure an Event Index, navigate to the **Monitoring & Diagnostics > RMON > Event Index** page and click **Add New Event Index**.
2. Specify values for this entry.
3. Click **Add** to save the new Event Index entry. Additional Event Index entries can then be added and edited from this page.

Refer to

- Refer to the Remote Monitoring (RMON) chapter in the *ArubaOS User Guide* for more information about Event Index entries.

- Refer to the "**rmon event**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

History Index

1. To configure a History Index, navigate to the **Monitoring & Diagnostics > RMON > History Index** page and click **Add New History Index**.
2. Specify values for this entry.
3. Click **Add** to save the new History Index entry. Additional History Index entries can then be added and edited from this page.

Refer to

- Refer to the Remote Monitoring (RMON) chapter in the *ArubaOS User Guide* for more information about History Index entries.
- Refer to the "**rmon history**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

SNMP Management Profile

SNMP Management profile settings for switch devices are managed locally. Management profiles for the AP are managed by group or global configuration on the **Monitoring & Diagnostics > SNMP** page. Navigate to this page to create or edit SNMP Management profile settings.

If you push configuration to a switch without having imported the contents of this profile, it will stop responding to AirWave, because the default profile has no community strings in it.

Refer to

- Refer to the MIB and SNMP chapter in the *ArubaOS User Guide* for more information about SNMP management settings.
- Refer to the "`snmp-server`" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

SNMPv3 User

1. To configure an SNMv3 user on the switch, navigate to the **Monitoring & Diagnostics > SNMP > SNMPv3 User** page and click **Add New SNMPv3 User**.
2. Enter a name for the user and specify the authentication method.
3. Select **Add** to save the new user. Additional SNMPv3 users can then be added and edited from this page.

Refer to

- Refer to the MIB and SNMP chapter in the *ArubaOS User Guide* for more information about SNMPv3 Users.
- Refer to the "**snmp-server**" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

Logging

Select the **Monitoring & Diagnostics > Logging** page to enable and specify logging levels. For each category or subcategory of message, you can set the logging level or severity level. The following table describes the different logging levels and their description:

Table 12: *Logging levels*

Logging Level	Description
Emergency	System is unusable
Alerts	Immediate action is needed
Critical	Any critical conditions
Errors	Error Conditions
Warning	Warning messages
Notifications	Normal but signification conditions
Informational	Messages of general interest to system users
Debug	Messages containing information useful for debugging

Table 12 describes the fields for this page.

Table 13: *Logging fields*

Field	Description
Logging facility	Select the logging facility from the drop-down.
Logging Servers	Click **Add** to add new logging servers.
Network Logging Levels	Set the logging levels for the Network related messages.
Security Logging Levels	Set the logging levels for the Security related messages.
System Logging Levels	Set the logging levels for the System related messages.
User Logging Levels	Set the logging levels for the User related messages.

Select **Save** when you are finished.

ArubaStack

An ArubaStack is a set of interconnected Aruba Mobility Access Switches that use stacking ports to form an ArubaStack. A stacking port is a physical port configured to run the stacking protocol. In factory default settings for Aruba Mobility Access Switches, uplink ports 2 and 3 are pre-provisioned to be stacking ports. Once a port is provisioned for stacking, it is no longer available to be managed as a network port. A stacking port can only be connected to other Aruba Mobility Access Switches running the Aruba Stacking Protocol (ASP).

1. To configure an ArubaStack, navigate to the **Switch Config > ArubaStack** page.
2. Specify values for the ArubaStack.
3. Click **Save** to save the settings.

Refer to

- Refer to the ArubaStack chapter in the *ArubaOS User Guide* for more information.
- Refer to the "`stack-profile`" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.