Aruba Instant in AirWave 8.2.11.0

Deployment 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	support.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

Aruba Instant (Instant) is a system of access points in a Layer 2 subnet. The IAPs are controlled by a single IAP that serves a dual role as an IAP and primary Virtual Controller (VC), eliminating the need for dedicated controller hardware. This system can be deployed through a simplified setup process appropriate for smaller organizations, or for multiple geographically dispersed locations without an on-site administrator.

Only the first IAP/Virtual Controller you add to the network must be configured; the subsequent IAPs will all inherit the necessary configuration information from the Virtual Controller. Aruba Instant continually monitors the network to determine the IAP that should function as the Virtual Controller at any time, and the Virtual Controller will move from IAP to IAP as necessary without impacting network performance. The Virtual Controller technology in Aruba Instant is capable of IAP auto discovery, 802.1X authentication, role-based and device-based policy enforcement, rogue detection, and RF management.

Using Instant with AirWave

AirWave can be used to provision and manage a multi-site deployment of Aruba Instant networks. For example, if you have 100 retail offices that require Instant to provide WLAN connectivity at each office, AirWave can be used to provision all the 100 offices from a central site. AirWave also provides the administrator with the ability to monitor these geographically dispersed Instant networks using an AirWave server (depending on the scalability recommendations for AirWave).

With a distributed deployment where multiple locations have a Virtual Controller and IAPs, AirWave serves as a centralized management console. AirWave provides all functionality for normal WLAN deployments, including long-term trend reporting, PCI compliance, configuration auditing, role-based administration, location services, RF visualization, and many other features.

Refer to the *AirWave Supported Infrastructure Devices Guide* for an up-to-date list of the Instant firmware versions and functions supported by AirWave.

Instant Integration into AirWave

Unlike other WLAN management products, AirWave eliminates the need to configure and troubleshoot individual APs or dispatch IT personnel on-site. With AirWave, IT can centrally configure, monitor, and troubleshoot Aruba Instant WLANs, upload new software images, track devices, generate reports, and perform other vital management tasks, all from a remote location. Integrating Instant systems into AirWave is unique from the setup of any other device class due to the following considerations:

- **Discovery:** AirWave does not discover Instant devices via scanning (SNMP or HTTP) the network. Each Instant deployment will automatically check-in to the AirWave configured within the IAP's user interface. The first Virtual Controller for an organization will automatically appear as a new device in AirWave. Subsequent IAPs are discovered via the Virtual Controller, just like standard controller/thin AP deployments.
- **Auto-provisioning:** The first authorized Virtual Controller requires manual authorization into AirWave via shared secret to ensure security. Along with the shared secret, the Virtual Controller sends an Organization String which automatically initializes and organizes the IAPs in AirWave. Unlike the traditional infrastructure of a physical controller and thin APs, Instant automates many tedious steps of developing a complex hierarchical structure of folders, config groups, templates, admin users, and admin roles for Instant.
- **Communication via HTTPS:** Because Instant devices may be deployed behind NAT-enabled firewalls, Virtual Controllers push data to AirWave via HTTPS. AirWave initiates no connections to Instant devices via SNMP, TFTP, SSH, and the like. This enables quick remote setup without having to modify firewall rules.
- **Virtual controller listed as separate device:** The Virtual Controller is listed as an additional device, even though it is part of the existing set of IAPs. If you have 10 physical IAPs, AirWave will list 10 Instant IAPs and

one Instant Virtual Controller. An asterisk icon (*) beside the device name indicates that a device is acting as a Virtual Controller. You can also identify the IAP acting as the Virtual Controller by the identical LAN MAC addresses on the **Devices > List** page, Device Inventory reports, and any other AirWave pages that list your network devices.

A device that is added as a Virtual Controller does not count as a license for AirWave.

Refer to the IAP product data sheet for full operational and regulatory specifications, hardware capabilities, antenna plots, and radio details.

Secure Access to AirWave

By default, virtual controllers use a pre-shared key to authenticate to AirWave. To enable support for a different security method, navigate to **AMP Setup>General>Aruba Instant Options**, and select **PSK**, **PSK and Certificate** or **Certificate only**. If you select a security method that supports certificate authentication, you can view the currently valid certificate using the **View Certificate** link in **AMP Setup>General>Aruba Instant Options**, or click **Change** to upload a new certificate file.

A Virtual Controller or Instant AP can authenticate to the AirWave server using a pre-shared key, or using two-way certificate-based authentication using an SSL certificate sent from AirWave to the Instant device.

The Certificate-based authentication feature requires you upload the a certificate from a supported certificate authority to the AirWave server, as the default AirWave certificate will not be recognized by the Instant AP, and will cause the SSL handshake to fail. Certificate authentication also requires that the **AMP IP address** information configured on the Instant AP is a domain name, and not an IP address.

AirWave supports the following trusted certificate authorities:

- **Chain 1**: Trusted Root CA: C=SE, O=AddTrust AB, OU=AddTrust External TTP Network, CN=AddTrust External CA Root Intermediate CA: C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO High-Assurance Secure Server CA
- **Chain 2**: Trusted Root CA: C=US, O=GeoTrust Inc., CN=GeoTrust Global CA Intermediate CA: Subject: C=US, O=Google Inc, CN=Google Internet Authority G2
- **Chain 3**: Trusted Root CA: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 2006 VeriSign, Inc. - For authorized use only, CN=VeriSign Class 3 Public Primary Certification Authority - G5 Intermediate CA: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=Terms of use at https://www.verisign.com/rpa (c)10, CN=VeriSign Class 3 Secure Server CA - G3
- **Root C**A: Trusted Root CA: C=US, O=Equifax, OU=Equifax Secure Certificate Authority

Virtual Controllers push data to AirWave via HTTPS. If your enterprise has a security policy that restricts the use of port 443 for inbound communication, you can change the port AirWave uses to communicate with Instant devices on the **AMP Setup>General>Aruba Instant Options.**

Intrusion Detection System

AirWave automatically detects rogue IAPs irrespective of their location in the network. It prevents authorized IAPs from being detected as rogue IAPs, and tracks and correlates the IDS events to provide a comprehensive picture of your network's security.

Instant Firmware Management

There are several ways to manage firmware updates in AirWave:

- Load the firmware image onto AirWave, and then launch an upgrade from AirWave. For a cluster of Instant APs, AirWave pushes the firmware image to the virtual controller, and the virtual controller pushes the firmware to the rest of its Instant APs.

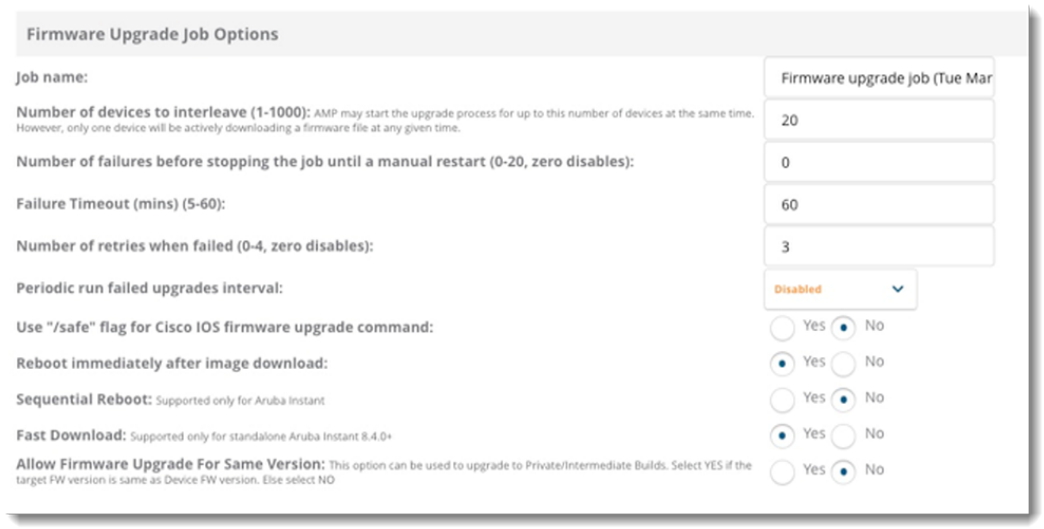
- Perform a rolling upgrade of the Instant firmware on standalone APs. When you enable the **Sequential Reboot** option on the **Groups > Firmware** page, the **Fast Download** option is automatically enabled. First, APs download the firmware image from the AirWave server. APs which have completed the download share, or seed, the firmware image with the remaining APs. After all APs have successfully downloaded the firmware image, AirWave sequentially reboots APs in the same RF zone.

Go to **Groups > Firmware** to configure the firmware upgrade job options (see Figure 1).

NOTE

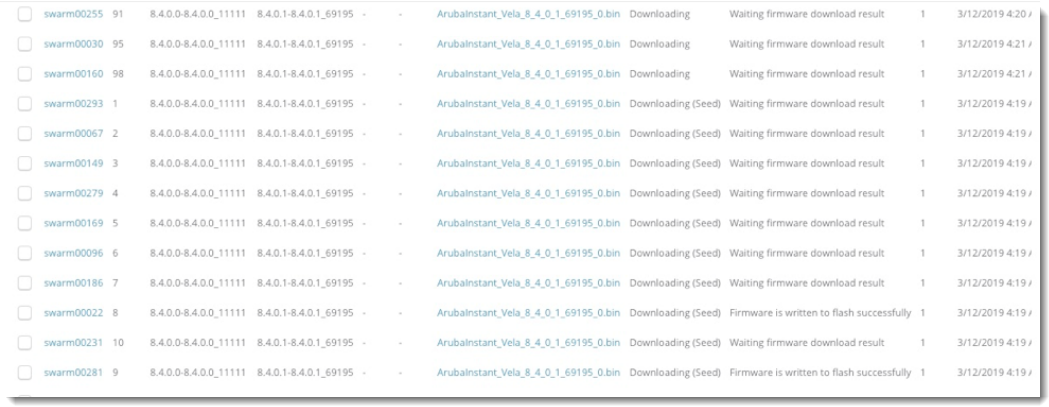
AirWave supports rolling upgrades for Instant APs running Instant 8.4.0.0 or later.

Figure 1: *Firmware Upgrade Job Options for IAPs*



To view the upgrade progress, go to **System > Firmware Upgrade Jobs**. In Figure 2, the upgrade status, "Downloading" indicates that the IAP is downloading the image from the AirWave server while "Downloading (Seed)" indicates that the IAP is downloading the image from another IAP.

Figure 2: *Firmware Upgrade Jobs Status*



For the complete list of products that have reached the end of life milestone and are not supported, refer to http://www.arubanetworks.com/support-services/end-of-life/ .

Table 1 lists the Instant firmware versions and functions supported by AirWave.

Table 1: *Supported Aruba Instant Firmware Versions and Functions*

Instant Version	Support for	
	Template Config	Instant GUI Config
Instant 8.6.0.4	AirWave 8.2.11.0	AirWave 8.2.11.0
Instant 8.6.0.0	AirWave 8.2.10.1	AirWave 8.2.10.1
Instant 8.5.0.2	AirWave 8.2.10.0	AirWave 8.2.10.0
Instant 8.5.0.0	AirWave 8.2.9.1	AirWave 8.2.9.1
Instant 8.5.0.0	AirWave 8.2.9.0	AirWave 8.2.9.0
Instant 8.4.0.1	AirWave 8.2.8.2	AirWave 8.2.8.2
Instant 8.4.0.0	AirWave 8.2.8.1	AirWave 8.2.8.1
Instant 8.3.0.0	AirWave 8.2.7.1	AirWave 8.2.7.1
Instant 8.3.0.0	AirWave 8.2.6.1	AirWave 8.2.6.1
Instant 6.5.4.0	AirWave 8.2.5.1	AirWave 8.2.5.1
Instant 6.5.4.0	AirWave 8.2.5.0	AirWave 8.2.5.0
Instant 6.5.3.0	AirWave 8.2.4.1	AirWave 8.2.4.1
Instant 6.5.2.0	AirWave 8.2.4.0	AirWave 8.2.4.0
Instant 4.3.1.0	AirWave 8.2.3.1	AirWave 8.2.3.1
Instant 4.3.0.0	AirWave 8.2.3.0	AirWave 8.2.3.0
Instant 4.2.4.0	AirWave 8.2.1.0	AirWave 8.2.2.0
Instant 4.2.3.0	AirWave 8.2.0.0	AirWave 8.2.2.0

Starting with 6.4.3.x-4.2, Instant software does not support IAP-92 and IAP-93.

AirWave Pages with Instant-Specific Features

You can configure Instant features on the following pages:

- **Devices > New**

  From the **Devices > New** page, the admin user can mouse over the value in the **Type** column to display the device's shared secret with AirWave.
- **Devices > Manage**

  From the **Devices > Manage** page, you can configure general device properties, settings, maintenance windows, and configure dynamic variables for a device.
- **Devices > List**

On the **Devices > List** page, ✱ beside a device name indicates that the device is acting as a Virtual Controller. You can also identify the IAP acting as the Virtual Controller by the identical LAN MAC addresses on the **Devices > List** page, device inventory reports, and any other AirWave pages that list your network devices. AirWave lists the Virtual Controller as an additional device, even though it is part of the existing set of IAPs.

- **Clients > Client Detail**

  After IAPs are serving clients, the IAPs can use user-agent strings to extract operating systems and device descriptions of its clients, and then populate the **Device Description** and **Device OS** fields in the **Clients > Client Detail** page.

- **Devices > Config**

  From the **Devices > Config** page,you can click the blue template link to access the configuration template and then fetch an Aruba Instant configuration. You can also click **Configuration** to compare configurations, the **device name** to access the group template, and **Audit** to run a configuration audit on the IAP.

- **Devices > Monitor > Radio Statistics**

  The **Radio Statistics** page for Aruba Instant devices displays Clients, Usage, Radio Channel, Radio Noise, Radio Power, Radio Errors, and Channel Utilization.

- **Groups > Instant Config**

  The **Groups > Instant Config** page becomes available after you go to the **Groups > Basic** page and turn on the **Enable Instant GUI Config** option. This feature allows you to use AirWave as a management console with the same UI as the IAP device.

- **RAPIDS**

  Instant supports mitigation and IDS event notification. All rogue devices are reported and stored in AirWavefor evaluation based on high-level rule sets.

- **Reports**

  Instant Virtual Controllers appear as a separate device in the Device Inventory Report and most other reports that list devices.

AirWave does not provide a Device Uptime report for Aruba Instant devices.

In order to configure and manage an group of Instant APs via AirWave, the Instant AP acting as the Virtual Controller for the Instant AP cluster must be able to contact and authenticate to the AirWave server. This can be done in any of the following ways

- Manual Configuration via the Instant AP Interface.
- Automatic Zero-Touch provisioning via DHCP or Activate.

Automatic zero-touch provisioning (ZTP) is the most efficient provisioning method for a multi-site Instant deployment. However, Aruba recommends you manually deploy one or more Instant devices on your network and verify that the devices are working as expected before you launch a larger-scale automatic provisioning deployment.

For each remote location, an on-site installer is required to physically mount the IAPs, connect them to the Aruba Instant SSID, configure the WLAN, and configure the names of the IAPs. The installer must then enter information into the IAP Virtual Controller that allows that device to communicate with AirWave. The configuration on the first Instant Virtual Controller that is added to AirWave acts as the 'golden' configuration that is used as a template to provision other Instant Virtual Controllers at other locations as the locations are brought online. It is recommended that the 'golden' configuration is validated and pre-tested in a non-production environment prior to applying it to a production network.

Users have the option to add additional devices into managed mode automatically by setting the **Automatically Authorized Virtual Controller Mode** option to **Manage Read/Write** on the **AMP Setup > General** page. Refer to the *AirWave 8.2.11.0 User Guide* for more information. It is also important to note that any changes that are made to the template variables will have to be manually applied to each deployed device.

Before you Begin

Before you start your initial Instant deployment via AirWave, you should define an AirWave organization string for your Instant network, and identify which authentication method(s) the Virtual Controller will use to associate with AirWave. If you choose the hwhitelist authentication option, use the procedures in this section of the document to define your device whitelists.

Create your Organization Strings

The organization string is a list of colon-separated strings that define the group and folder the Instant Virtual Controller is placed into after it authenticates to the AirWave server. When an Instant Virtual Controller is added to AirWave, the device is authorized based on its organization string.

The format of the organization string is **<org_name>:<subfolder1>:<subfolder2>...** and so on, up to 31 characters. The **<org_name>** parameter, the top-level string, is generally the name of your organization.

When you add an Instant Virtual Controller using an organization string, AirWave will automatically create the an AirWave role, group and folder, (if not already present) based upon the organization name in the organization string.

- AirWave Role *<org_name> Admin*. This role gives access to the *<org_name>* folder.
- The configuration group *<org_name>*. AirWave groups are primarily for configuration. Instant devices will automatically be placed into the configuration group defined by their organizational string, where they will receive the configuration settings and firmware version associated with that group.

- The folders *<org_name>[:<subfolder1>:<subfolder2>...]*. AirWave folders are hierarchical and are used to control which AirWave users have access to which devices. All folders, including those created by an organization string, are located under the Top folder in AirWave

Example: Simple Organization String

This a simple organization string: US

A device with an organization string of "US" will placed in an AirWave group that is called "US" and in a folder that is called "US." The folder is one level beneath the top folder. In addition, a user and a role are created that grants access to devices in the "US" folder.

Example: More Complex Organization String

This is a more complex organization string: US:California:Sunnyvale

A device with an organization string of "US:California:Sunnyvale" will be placed in an AirWave group that is called "US" and that is in a folder that is called "US" that mirrors a geographical structure with Sunnyvale beneath California.

Select your Authentication Methods

When the AirWave administrator manually authorizes the first Instant Virtual Controller for an organization, AirWave uses that Virtual Controller's shared key or authentication certificate to authenticate other Virtual Controllers on the network. Once individual Virtual Controllers successfully complete authentication, they can also be validated against a predefined whitelist before they appear in the **Devices > New** list.

Users have the option to add additional devices into managed mode automatically by setting the **Automatically Authorized Virtual Controller Mode** option to **Manage Read/Write** on the **AMP Setup > General** page. Refer to the *AirWave 8.2.11.0 User Guide* for more information. It is also important to note that any changes that are made to the template variables will have to be manually applied to each deployed device.

Shared Key Authentication

The AirWave administrator can use a shared key to manually authorize the first Instant Virtual Controller for an organization, or to automatically authenticate additional Virtual Controllers via automatic Zero-Touch provisioning. Any string is acceptable, but this string must be the same for all devices in your organization.

The AirWave administrator sends the shared secret key, organization string and the AirWave IP address to an on-site installer, who enters this information into the Virtual Controller. When that device authenticates to the AirWave AirWave server, it appears in the **Devices > New** list, and must be manually authorized by an AirWave administrator. After the Instant device has been validated, other Instant devices using that shared key will automatically authenticate to the AirWave server, and appear in the **Devices > New** list.

Always ensure the protection of your organization's shared secret. Knowledge of this shared secret, the organization string, and communication protocol could allow a rogue device to masquerade as a Aruba Instant device.

Certificate Authentication

The Instant Virtual Controller can authenticate to the AirWave server with two-way certificate-based authentication, using an SSL certificate sent from AirWave to the Instant device. Instant Virtual Controllers push data to AirWave via HTTPS. If your enterprise has a security policy that restricts the use of port 443 for inbound communication, you can change the port AirWave uses to communicate with Instant devices.

To enable certificate authentication for Instant Virtual Controllers authorizing to an AirWave server:

1. Navigate **to the AMP Setup > General > Aruba Instant Options** section of the AirWave WebUI.
2. Click the **Security method for adding new Virtual Controllers** drop-down list, and select **PSK and Certificate** or **Certificate Only**.

3. Click **Change**. The WebUI displays the Upload SSL certificate section of the **AMP Setup > General** page.
4. Click **Browse** to browse to and select a certificate file. The file must be PEM format containing both a valid private key and certificate.
5. Click **Upload**.

Whitelist Authentication

You can use an Instant whitelist to specify the Instant Virtual Controllers that are allowed to access the AirWave server after those devices complete pre-shared key or certificate authentication. For more information on Instant whitelists, see "Zero-Touch Provisioning using a Whitelist" on page 17.

Setting up Instant Manually

To manually configure an Aruba Instant Virtual Controller to contact and authenticate to your AirWave server and then download the proper configuration, you must enter the following information into the WebUI of each IAP/VC:

- AirWave IP address: IP address of the AirWave server.
- Organization string: This settings defines the device group to which the Virtual Controller will be associated.

You must also configure at least one of the following authentication methods.

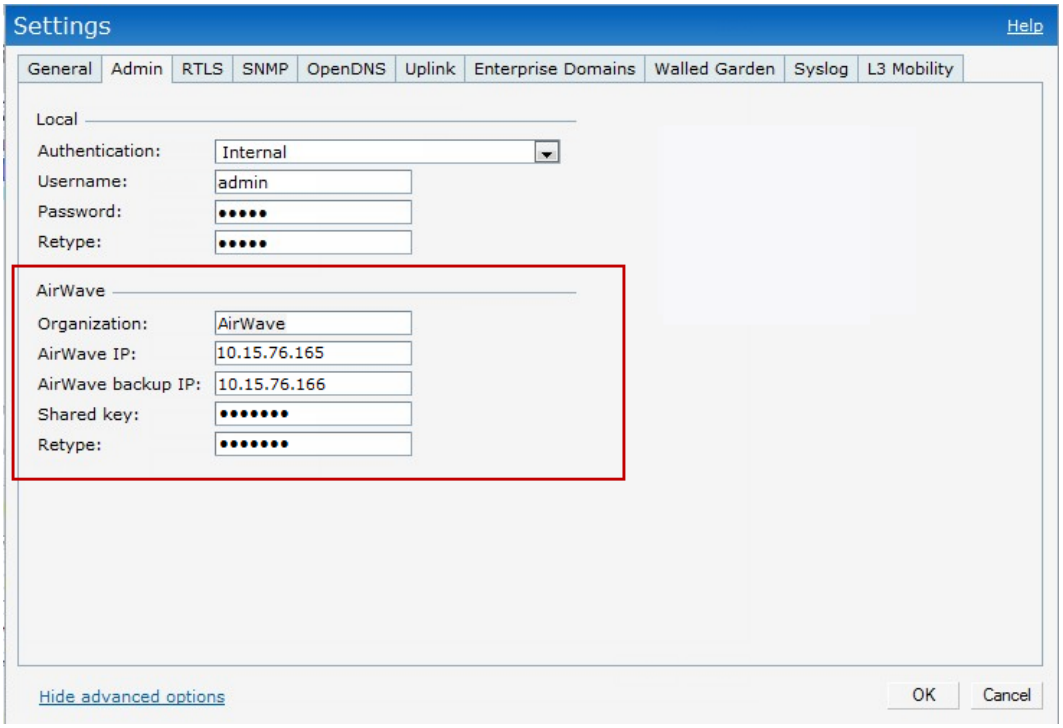
- Pre-Shared Key (PSK) authentication: Enter a shared authentication key to associate your Virtual Controller to the AirWave server.
- Certificate authentication: Upload a certificate onto your and AirWave server to allow your Virtual Controller to authenticate to AirWave using certificates.

Entering the Organization String and AirWave IP

For the initial Instant Virtual Controller installed in each location, the on-site installer must log into that device's web interface via the Aruba Instant configuration SSID, then perform the following steps to configure that device to authenticate to the AirWave server.

1. Log into your Virtual Controller.
2. Click on either **Set up Now** at the bottom of the UI or on the **Settings** tab in the top right corner. This opens the **Settings** menu.
3. Locate the AirWave section on the **Admin** tab.

Figure 3: *Aruba Instant > Settings page*

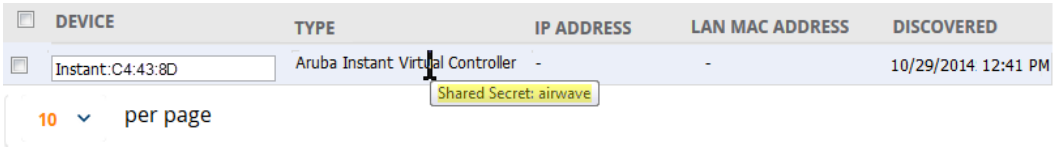


4. Enter the organization string, the AirWave IP address, and the shared key.
5. Click **OK** when you are finished.

Verifying the Shared Secret

After an initial Instant Virtual Controller contacts and authenticates to the AirWave server, that Instant device appears in the **Devices > New** page. The admin user can mouse over the value inthe **Type** column to verify the device's shared secret with AirWave, as shown in Figure 4.

Figure 4: *Mouse over the Type column to view the Shared Secret*



If the incoming shared secret matches the one you created, select **Add**, then **Save and Apply** in the confirmation page.

If you defined an organization string when you configured the device to contact AirWave, you do not have to select any group or golder from the drop-down menus on the **Devices > New** page. An Instant Virtual Controller will automatically be added into the group or folder specified by its organization string, and will ignore any attempts to manually override its group or folder when the device is first added to AirWave. If you have any Virtual Controllers with no organization specified the first time they communicate with AirWave then they will be placed in the Folder/Group drop-box values you have selected.

Assigning a Configuration and Firmware Version to the Device

After the Instant Virtual Controller has contacted and authenticated to the AirWave server and is associated to the group and folder defined by its organization string, you must determine whether the Instant devices in these

groups will be managed using template-based configuration or using Instant Config. Refer to the following sections for information on configuring your Instant Virtual Controllers using either of these two methods.

- Using Template Configuration on page 20
- Using Instant GUI Config on page 28

Devices will revert to Monitor Only mode when you change group configuration from Instant Config to Template based.

Automatic Zero-Touch Provisioning

Instant devices can use an AP whitelist or DHCP options 60 and 43 for automatic zero-touch provisioning (ZTP). If you use Aruba Activate to manage your devices, you can assign your devices to folders within Activate and then apply provisioning rules to the folder. Refer to the following sections of this document for more information:

- "Zero-Touch Provisioning via DHCP" on page 16
- "Zero-Touch Provisioning using a Whitelist" on page 17
- "Zero-Touch Provisioning via Activate" on page 19

Zero-Touch Provisioning via DHCP

The Aruba Instant Virtual Controller initiates a DHCP request with the DHCP option 60 string 'Aruba Instant.' If the DHCP server is configured to recognize this option 60 string, it will return an option 43 string containing the organization, AirWave IP, and pre-shared key (Organization is optional). The three pieces of information should be specified using comma separators without any spaces. For example,

```
option 43 text "TME-Instant,10.169.240.8,aruba123"
```

The AirWave information in the option 43 will be used to connect to AirWave, if AirWave is not otherwise configured manually on the Virtual Controller.

The organization string can be hierarchical and define sub-folders for different stores. This supports an architecture that is required to manage multiple branches or stores where individual stores can be managed by local administrators.

DHCP server options:

```
ip dhcp pool IAP-Pool
 default-router 10.169.241.1
 option 60 text "ArubaInstantAP"
 option 43 text "CompanyName :Store1,10.169.240.8,aruba123"
 network 10.169.241.0 255.255.255.0
 authoritative
!
ip dhcp pool IAP-Pool2
 default-router 10.169.242.1
 option 60 text "ArubaInstantAP"
 option 43 text "CompanyName:Store2,10.169.240.8,aruba123"
 network 10.169.242.0 255.255.255.0
 authoritative
```

In the example configuration shown above, the following group and folder structure is created on AirWave:

- A group called CompanyName is created.
- A top-level folder called CompanyName is created.
- Two sub-folders called Store1 and Store2 are created which will contain the IAPs.

Zero-Touch Provisioning using a Whitelist

The Instant whitelist database is a list of the Instant Virtual Controllers that are allowed to access the AirWave server after those devices complete pre-shared key or certificate authentication. This Instant whitelist must be manually configured using the AirWave UI or imported into AirWave in comma-separated values (CSV) format before you deploy the devices on the list.

Whitelist files can include the following data columns. Each entry must include the **name** field, and must also contain either a **serial number** or a **LAN MAC address**.

- Name
- LAN MAC Address
- Serial Number
- Virtual Controller Name
- Group Name
- Folder Name
- Timezone
- CHAP Secret
- PPPoE Service Name
- PPPoE User Name
- PPPoE Password
- Radius Servers
- RF Band Selection
- Location
- Syslog Server
- Control Plane VLAN
- VLAN Number
- Gateway
- Netmask
- Modem PIN
- Notes
- custom_variable_1...custom_variable_10
- Modify authorized device
- Sync dynamic variables
- dynamic_variables

An example of a whitelist entry using this format is as follows:

```
Name,LAN MAC Address,Serial Number,Virtual Controller Name,Group Name,Folder Name IAP_Canada_
1,ff:c7:c8:c4:21:ff,BD0086086,Canada-Office,Canada,Vancouver:Downtown IAP_US_
1,F0:0B:86:CF:93:FF,BE0542245,US-Office,US,San Fancisco:CenterTown:HillTop
```

When this feature is enabled and an Instant Virtual Controller attempts to connect to AirWave, AirWave checks the MAC address or serial number of the device against this whitelist, and authorizes the device if it's MAC address or serial number matches a whitelist entry. Once authorized, that Virtual Controller appears in the **Devices > New** page, where it can be assigned to an AirWave group and folder.

There are four methods to create an Instant Whitelist. You can create a whitelist using the AirWave WebUI, import a whitelist in CSV format using the AirWave WebUI, upload a whitelist via an AirWave API, or configure whitelist Entries using a script in the AirWave command-line interface. These options are described in the sections below.

Creating Whitelists via the AirWave WebUI

To enable whitelist authentication and manually add Instant Virtual Controllers to a whitelist via the AirWave WebUI:

1. Navigate to **AMP Setup >General**
2. Expand the **Automatic Authorization** section
3. In the **Authorize ArubaInstant APs & Aruba Switches to AirWave** section, select **Whitelist.**
4. Click **Save**.
5. Next, navigate to **Devices > New**.
6. Click the **Instant AP & Aruba Switch Whitelist** drop-down list, and select **Add aInstant AP or an Aruba Switch to the Whitelist**.

7. Enter whitelist information for the Instant Virtual Controller. Each whitelist entry must have an Instant AP name and either a serial number or a MAC address.
8. In the **Group** and **Folder** fields, specify the group and folder to which the device will be assigned
9. Click **Add**. You are prompted to confirm changes. Click **Apply Changes Now**, or specify a time that the device should be added to the whitelist.

Importing a Whitelist in CSV Format

To import a whitelist in Comma-Separated Value (CSV) format to the AirWave server:

1. Navigate to **Devices > New**.
2. Click the **Instant AP & Aruba Switch Whitelist** drop-down list, and select **Import Instant AP or an Aruba Switch Whitelist from CSV**.
1. Navigate to **Device Setup > Add**.
2. In the **Select the type of device to add** field, select **Aruba Device**.
3. Click the **Import Devices via CSV** link.
4. The **Upload a list of devices** page opens. This page describes the required fields and format for the whitelist file.
5. Click **Choose File,** browse to and select the CSV file, then click **Upload**.

Uploading a Whitelist via an AirWave API

Software developers can use the AirWave API to upload a whitelist in CSV format.

- **URL**: https://<airwave_server_address>/api/ap_whitelist_upload
- **Location of whitelist in CSV format**: /var/www/html/static/sample/import_whitelist_sample.csv

Table 2: *Whitelist API Parameters*

Parameter	Description
csv	Whitelist document in proper Instant whitelist CSV format.
append_whitelist	Specify one of the following update options: • **0**: Replace the whole whitelist with the current content. All the items not in current content will get removed. • **1**: Update the whitelist with the current content. All the items not in current content will remain the same.

Example URL:

https://<airwave_server_ip>/api/ap_whitelist_upload? append_whitelist=1&csv=<csv_file>

Example POST:

```
Name,LAN MAC Address,Serial Number,Virtual Controller Name,Group Name,Folder Name,custom_
variable_1,custom_variable_9
IAP_Canada_1,ff:c7:c8:c4:21:ff,BD0086086,Canada-Office,Canada,Vancouver:Downtown,abc,456
IAP_US_1,F0:0B:86:CF:93:FF,BE0542245,US-Office,US,San Fancisco:CenterTown:HillTop,cde,789
```

Example Successful Result:

```
Device (Name:IAP_Canada_1, LAN MAC:ff:c7:c8:c4:21:ff, Serial Number:BD0086086): created/updated
successfully
Device (Name:IAP_US_1, LAN MAC:F0:0B:86:CF:93:FF, Serial Number:BE0542245): created/updated
successfully
2 devices created or updated.
```

Uploading a Whitelist via a Script

AirWave includes a built-in script that can be used to configure whitelist entries. The script is located at

```
usr/local/airwave/bin/import_whitelist.pl
```

This script can either be run from the AirWave server or another unix machine (like Linux or Mac) that has Perl installed.

If you run the whitelist update script on another machine, be sure to edit the Perl path in the first line of the example script below.

Usage:

```
/usr/local/airwave/bin/import_whitelist.pl --amp <ip/host> --usr <username> --passwd <password>
--file <file> [--update <update>]
```

This script supports the following parameters:

Table 3: *Whitelist Script Parameters*

Parameter	Description
--amp <ip/host>	AirWave server ip address or hostname
--usr <username>	User name of the AirWave user uploading the whitelist file.
--passwd <password>	Password for the AirWave user uploading the whitelist file.
--file <file>	Name of the CSV file that contains the whitelist.
--update <update>	Specify one of the following update options: • 0: Replace the outdated whitelist with content from a newer file. All the items not included in the newer file will get removed. • 1: Update the whitelist with the additional content from a newer file. Any items not in the current content file will remain the same.

Zero-Touch Provisioning via Activate

Refer to the documentation that accompanies Aruba Activate for detailed information on provisioning Instant devices.

If you are using Aruba Activate to set up your devices, the devices will automatically move to the appropriate group if you enable the **Autoconfigure New Virtual Controllers** option in the **Groups > Instant Config >AirWave > AirWave Settings** section of the AirWave WebUI. If your Instant device groups use template-based configuration, all device settings for that group must be managed via templates. However, if you enable AirWave Instant Config for the group, then you can use the AirWave Instant Config WebUI to configure the devices in that group. Note that autoconfiguration will wipe out any existing configuration on the device, including the factory default settings. The device will be configured based only on the group policy.

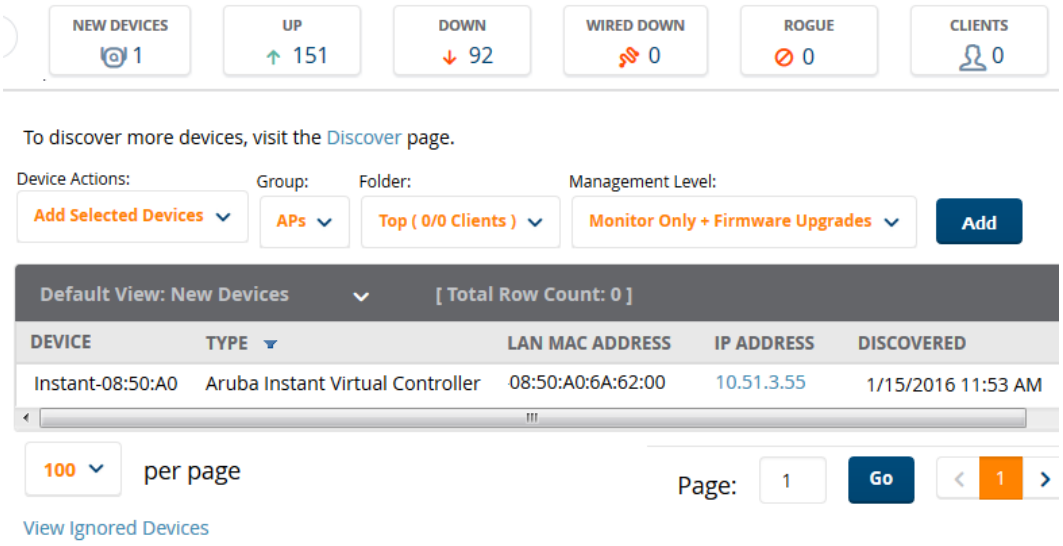
Template configuration allows you manage IAP devices with minimal administrative intervention by applying a group-based template configuration to all Instant AP Virtual Controllers that are added to the group.

Additional information about creating templates for Aruba Instant is available in the *AirWave 8.2.11.0 User Guide*.

Manually Confirm the First Instant Device

After the first Instant Virtual Controller receives the AirWave server information from the DHCP server, or after AirWave server information is manually configured, the Virtual Controller appears as a new device in AirWave. This Virtual Controller is added in **Monitor Only** mode.

Figure 5: *A new Instant device in AirWave*



1. Click **Add** to add the device. A group and folder do not have to be selected. The Virtual Controller will automatically get added to the new group created by AirWave to match the device's organization string.
2. Select **Apply Changes Now** to add the Virtual Controller to its group.

Updating the Instant Template

The configuration on the first Instant Virtual Controller added to AirWave becomes the default "golden configuration" for that device group. AirWave automatically creates a template based on configuration of this initial device, then uses the template to provision other Virtual Controllers added to the group. After adding the first Virtual Controller to AirWave, you can view and, if necessary, edit this configuration before you add other Virtual Controllers.

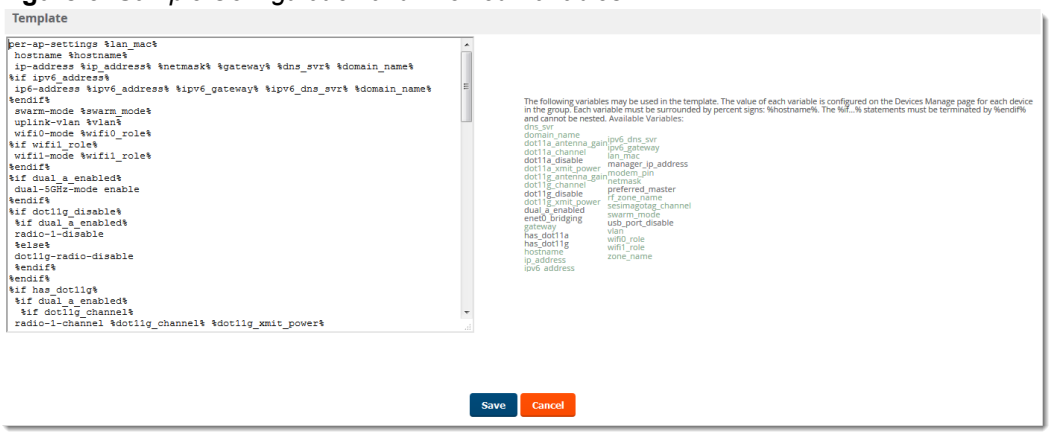
Aruba recommends that you validate and test this default configuration in a non-production environment prior to applying it to a production network. Any changes that are made to this configuration will be applied to other Instant devices in that group.

You can configure a group of Instant devices using the configuration template or the Instant GUI Configuration (IGC) feature. AirWave will not display the **Groups > Templates** pages if you enable the Instant GUI Config feature for that group.

To view or edit the Instant template:

1. Navigate to **Groups > List** and select the group that contains your initial Instant device.
2. From the **Groups** table, select the name of the group. The navigation menu on the left side of the web page updates to display additional navigation options, including the **Groups > Template** option.
3. Navigate to **Groups > Template**.
4. Locate the template and click to edit the Instant template.

Figure 6: *Sample Configuration and Allowed Variables*



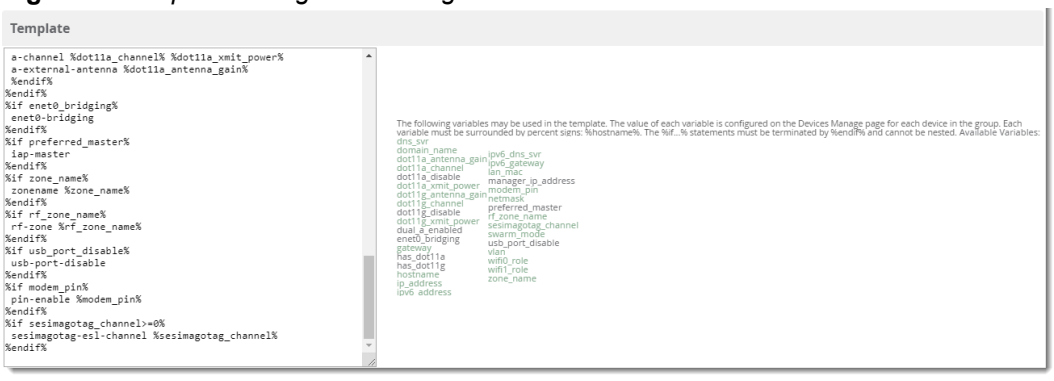
The **Allowed Variables** section at the right of the template editor displays the set of variables that you can added to the template. Refer to the *AirWave 8.2.11.0 User Guide* for information about using templates and variables.

Template Configuration for SES-imagotag Electronic Shelf Labels

For Instant APs (IAPs) running Instant 8.5.0.0 or later, AirWave now supports ESL profiles used to configure an Electronic Shelf Label (ESL) label by SES-imagotag. From the **Groups > Template** page, you can use variables, or import ESL settings from an Instant AP, to configure the static channel number of the ESL radio and the ESL server ip address.

Figure 7 shows the **sesimagotag-esl-channel** variable used in the configuration template.

Figure 7: *Template Configuration using Variables*



For more information about the SES-imagotag ESL System, see the *ArubaOS8.5.0.0 User Guide*.

Adding Additional Instant APs to AirWave

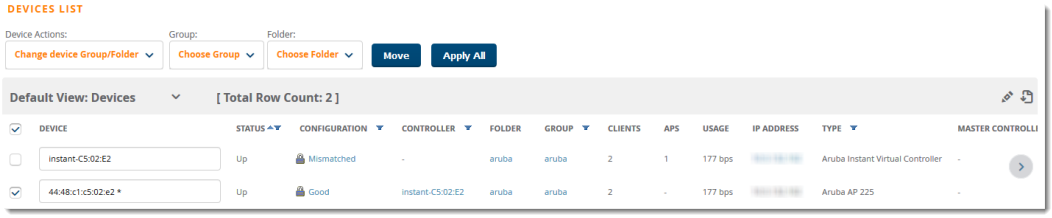
There are several ways to add Instant devices to AirWave: monitor-only mode,automatic provisioning, and bulk provisioning with a CSV file.

Adding Devices in Monitor-Only Mode

As a best practice for using Instant in AirWave, change the mode for new devices to **Monitor Only**. This ensures that AirWave doesn't overwrite the configuration for the new devices.

1. Navigate to **Devices > List** page.
2. Filter the devices by the folder name using the Folder drop down menu on the top portion of the page.
3. Scroll down to the Devices List, then click  to open the Modify Devices tool.
4. Select all devices.
5. From the **Device Actions** drop-down list, select **Management Level**.
6. Click **Monitor Only + Firmware Upgrades**.
7. Click **Apply All**, or schedule the change for later.

Figure 8: *Changing the mode to Monitor Only + Firmware Upgrades*

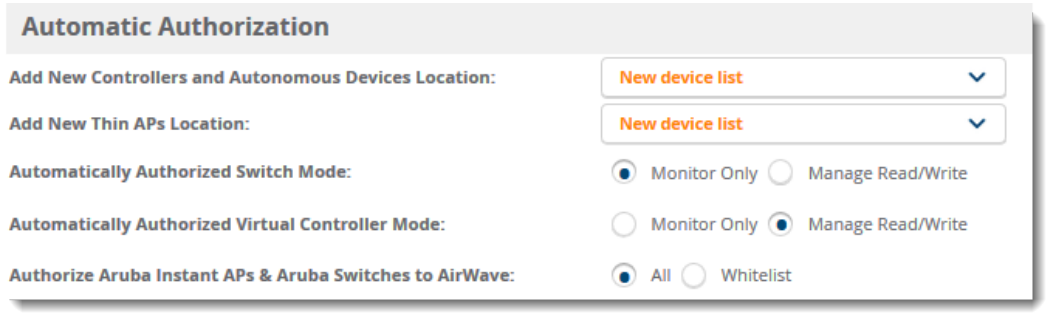


Adding Devices with Automatic Provisioning

To allow new Virtual Controllers to automatically update to their assigned group configuration:

1. Navigate to **AMP Setup > General**.
2. In the Automatic Authorization section, select **Manage Read/Write** for the "Automatically Authorized Virtual Controller Mode" option, as shown inFigure 9.

Figure 9: *Turning on the Automatic Provisioning Mode*



3. Click **Save**.

When the second Instant Virtual Controller contacts AirWave using the same shared key as the first Virtual Controller , that device is automatically placed into the group described in its organization string, and provisioned with the golden configuration for that group.

If you have allowed AirWave to add Virtual Controllers in **Manage Read/Write** mode, there is no need for manual intervention to provision these new Instant networks. When provisioning is complete, the status of the device will change from **Verifying** to **Good**.

Adding Multiple Devices from a File

You can add devices in bulk from a file to AirWave. Here you also have the option of specifying vendor name only, and AirWave will automatically determine the correct type while bringing up the device. If the .csv file includes make and model information, AirWave will add the information provided in the file. It will not override what you have specified in this file in any way.

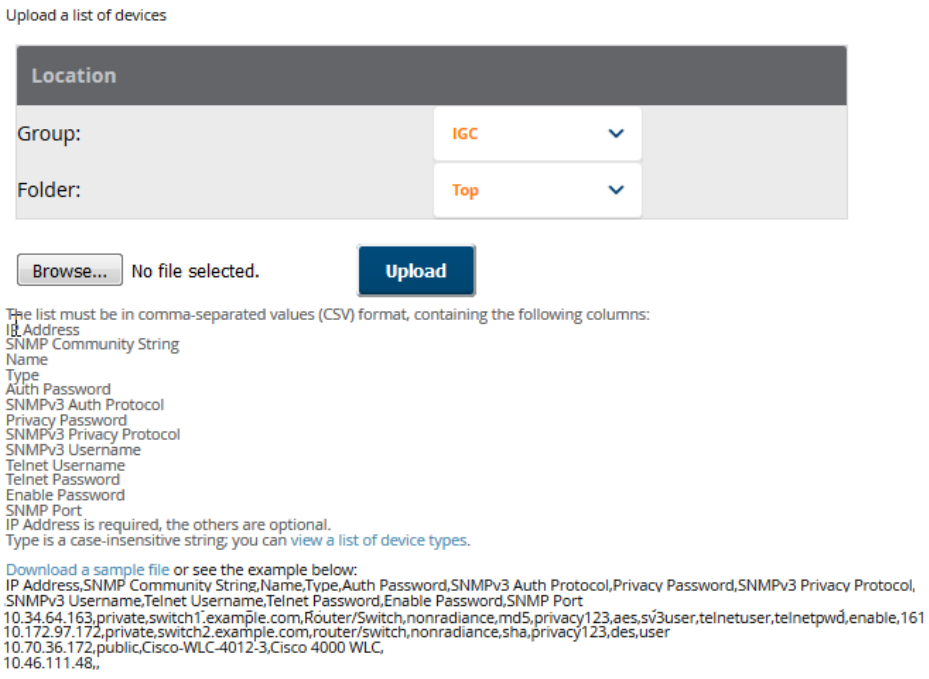
The CSV list must contain the following columns:

- IP Address
- SNMP community string
- Name
- Type
- Authentication password
- SNMPv3 auth protocol
- Privacy password
- SNMPv3 privacy protocol
- SNMPv3 user name
- Telnet user name
- Telnet password
- Enable password
- SNMP port

You can download and customize a file.

1. To import a CSV file, go to the **Device Setup > Add** page.
2. Click the **Import Devices via CSV** link. The **Upload a list of devices** page displays. See Figure 10.

Figure 10: *Device Setup > Add > Import Devices via CSV Page Illustration*



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

5. Click **Upload** to add the list of devices to AirWave.

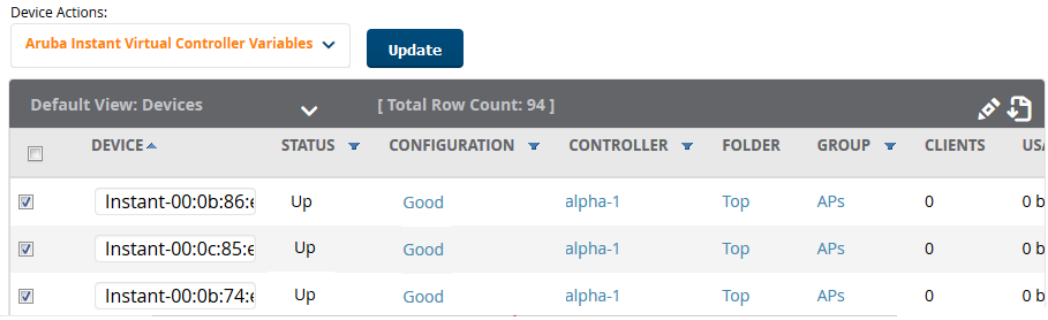
Editing Variables

AirWave includes support for editing variables on virtual controllers that have different values. Some common variables include Name, LAN IP Address, Syslog Server, Timezone, Radius Servers, and RF Band Selection. AirWave also supports additional generic variables that you can customize (such as adding a new WLAN). The defaults for all VC variables can be changed from the Template page.

Perform the following steps to begin editing variables on virtual controllers.

1. On the **Devices > List** page, click  in the device list table header, and then select the check box beside the virtual controllers that you want to edit.

Figure 11: *Select the VCs to update*



2. Click the **Device Actions** drop-down list and select the **Aruba Virtual Controller Variables** option.
3. Click **Update**. The opens the **Variable Edit** page.

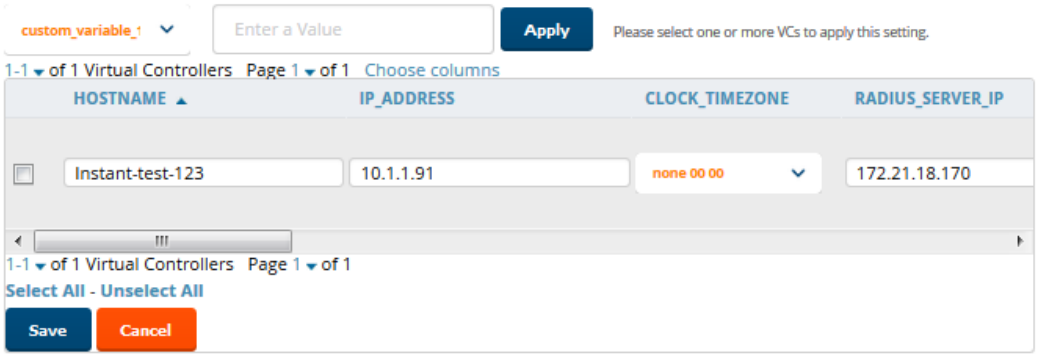
Refer to the following sections for information on using the **Variable Edit** page:

- "Editing Individual Virtual Controller Values" on page 24
- "Bulk Editing of Multiple Virtual Controllers" on page 25
- "Using Custom Variables" on page 25
- "Applying Changes" on page 26

Editing Individual Virtual Controller Values

After you click **Update** in the Modify Devices form, the Variable Edit screen displays. This screen includes two sections. The lower section includes editable fields. Enter values or select options directly in these fields.

Figure 12: *Change the Individual VC Names*



Bulk Editing of Multiple Virtual Controllers

The upper section of the **Variable Edit** page includes a drop down menu of variables that can be used to apply bulk changes to all VCs that you select in the lower section.

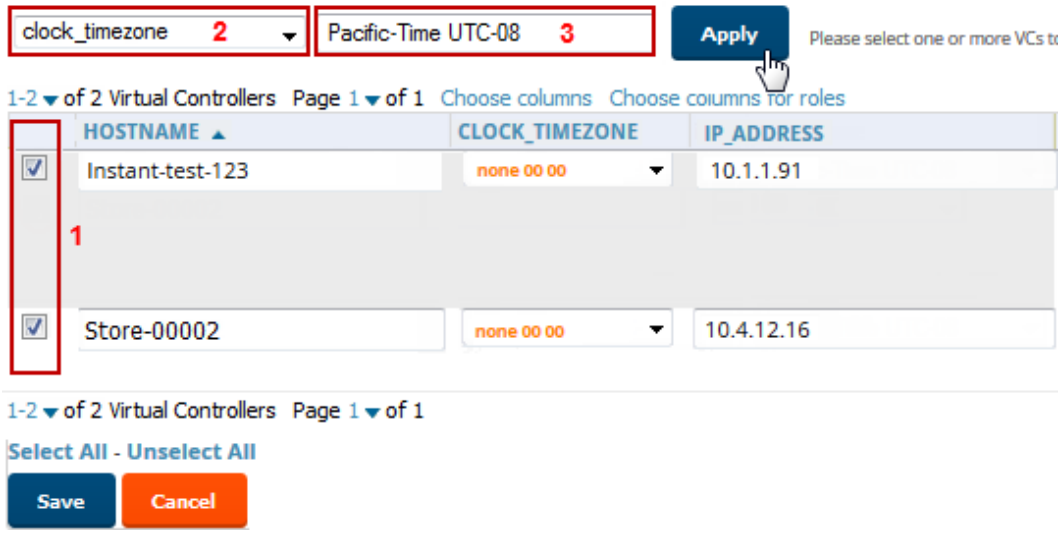
Perform the following steps to apply bulk edits.

1. In the edit screen, select the check box beside the virtual controller(s) that will be edited. (See Figure 13.)
2. Select the variable that you want to change from the drop down list in the upper section.
3. Enter or select the new value. In the example below, clock_timezone is changed to Pacific time for both VCs.
4. Click **Apply** when you are finished making each change. The selected virtual controllers will display the updated information. Follow these same steps for each variable that you want to edit.

NOTE

The **Apply** button remains disabled until a virtual controller is selected (via its check box).

Figure 13: *Change the Timezone variable*



Using Custom Variables

The Variable Edit page includes additional generic fields, labeled as **custom_variable_1** through **custom_variable_10**. The custom_variable_1 field can be used to add multiple lines of text rather than a single entry (as indicated by the larger note field on the UI.) This is useful, for example, if you want to add a new

WLAN configuration to a Virtual Controller. Other variables can be used to enter additional, single support commands.

The process for creating custom variables is the same as that used in editing available variables. To create a custom variable on a single Virtual Controller, use the horizontal scroll bar (if necessary) to locate the variable you want to edit, and type directly into that field. To add the same custom variable to all virtual controllers, select the check box beside the Virtual Controllers you want to edit, select the variable from the drop-down menu at the top of the edit page, enter the variable information, and then click **Apply**.

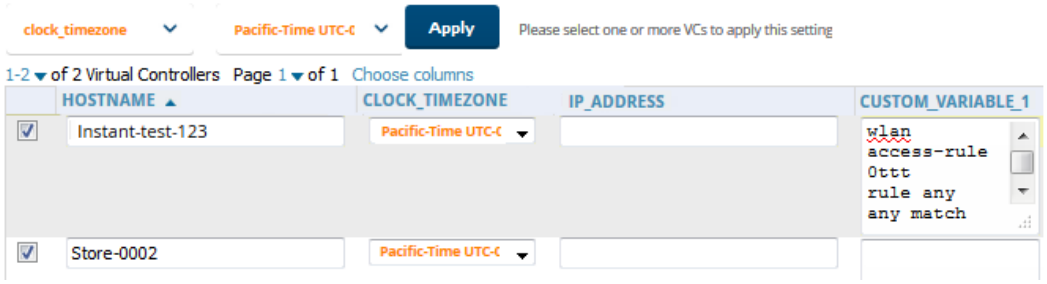
NOTE

Your template must support or contain the commands and/or configuration that you add using the custom variables in order for any changes to be pushed to your devices.

In the image below, a new WLAN config is added to Store-00001 with the following configuration:

```
wlan access-rule 0ttt
rule any any match any any any permit
wlan ssid-profile 0ttt
type employee
essid 0ttt
wpa-passphrase 8d072cdea5bcec1eaae3cb597975951fbd7d7124120e3217
opmode wpa2-psk-aes
max-authentication-failures 0
rf-band all
captive-portal disable
dtim-period 1
inactivity-timeout 1000
broadcast-filter none
dmo-channel-utilization-threshold 90
```

Figure 14: *Entering a custom variable (cropped)*



Applying Changes

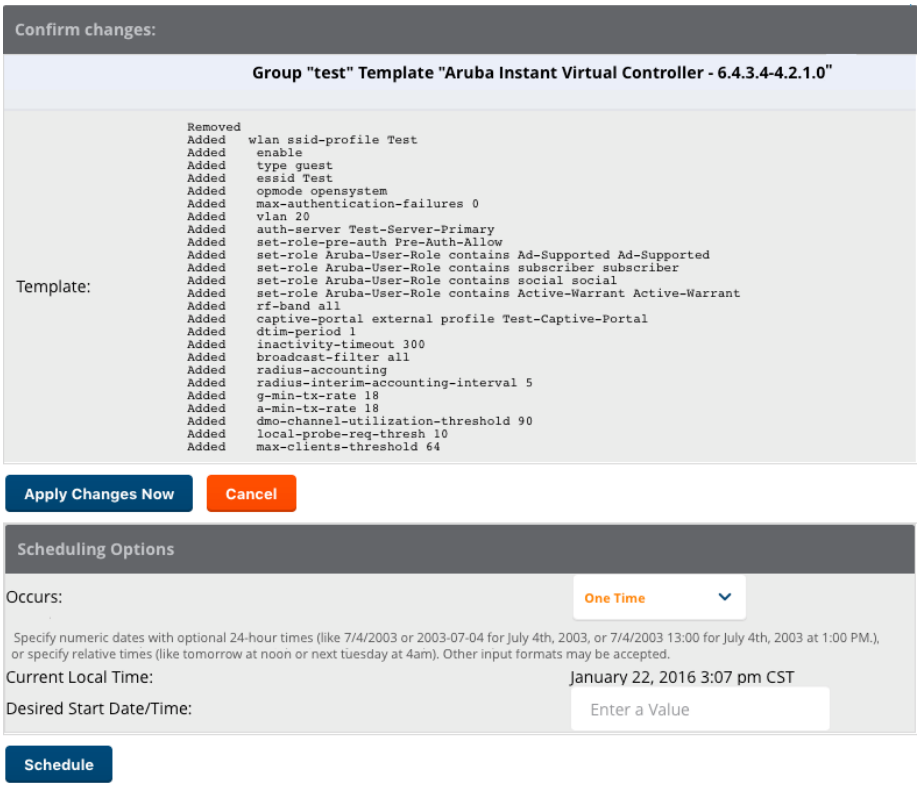
Select **Save** when you are done updating variables.

NOTE

All changes will be lost if you do not click **Save**.

The **Confirm Changes** page opens, displaying your recent edits. At this point, you can apply changes immediately, you can schedule to apply the changes at a later time, or you can cancel.

Figure 15: *Confirm Changes page*



Selecting **Cancel** returns you to the Variable Edit page, where your latest edits will still be visible. Click **Cancel** again to return to the **Devices > List** page with no changes saved or applied.

Instant GUI Config (also called IGC or Instant Config) provides an alternate method for configuring and managing devices running Instant 3.2 to Instant 8.5.0.0.x. If Instant Virtual Controllers are added to a group, this feature is available when you select **Enable Instant GUI Config** option on the **Groups > Basic** page. When this feature is enabled, the **Groups > Templates**, **Devices > Manage**, and **Devices > Device Configuration** pages are unavailable. Instead, all IAP management is performed from the **Instant Config** pages in AirWave.

Instant Config is fully compatible with devices running Instant version 3.2 to 8.5.0.0. Instant devices running different firmware versions cannot reside in the same group. Each group can only include devices with the same firmware version.

Refer to the following sections for more information:

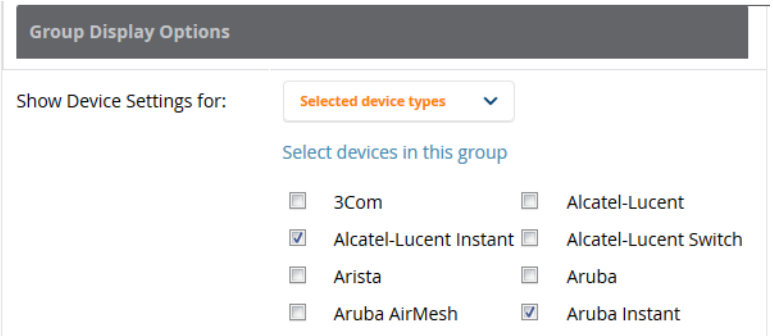
- "Enabling Instant GUI Config" on page 28
- "Importing Devices for Instant GUI Config" on page 29
- "The Instant GUI Config WebUI" on page 30
- "Where to Get Additional Information" on page 38

Enabling Instant GUI Config

The **Groups > Instant Config** pages are hidden by default. Perform the following steps to enable this feature and allow the AirWave WebUI to display the **Groups > Instant Config** pages.

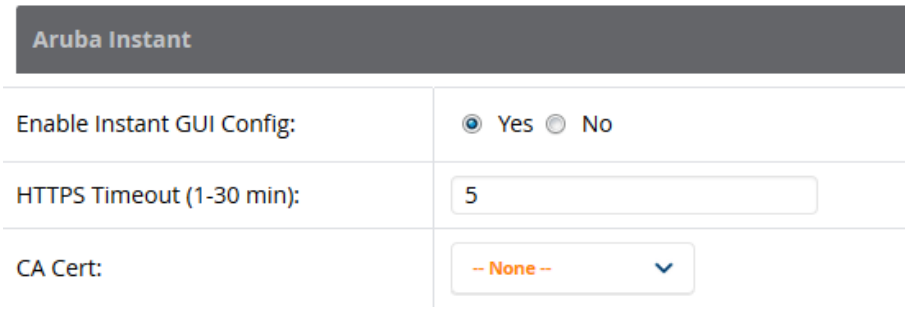
1. Navigate to **Groups > List**.
2. Select the group on which you want to enable this feature.
   - To enable this feature on a new group, click **Add**, name the new group, then click **Add** again.
   - To enable this feature on an existing group, select the name of the group from the **Groups** table.
3. Navigate to **Groups > Basic**, and scroll down to the **Group Display Options** section.
4. Ensure that the **Show Device Settings for** option includes Instant devices. Instant GUI Config is only available for groups that include Instant devices. The example **Group Display Options** settings in the figure below allow the AirWave WebUI to display device settings for Alcatel-Lucent and Aruba Instant devices.

Figure 16: *Include Instant devices*



5. Click **Save and Apply**. You are directed to the **Groups > Monitor** page.
6. Navigate back to the **Groups > Basic** page.
7. In the Aruba Instant section, select **Yes** for the **Enable Instant GUI Config** option.
8. Click **Save and Apply**.

Figure 17: *Enable Instant Config*



Importing Devices for Instant GUI Config

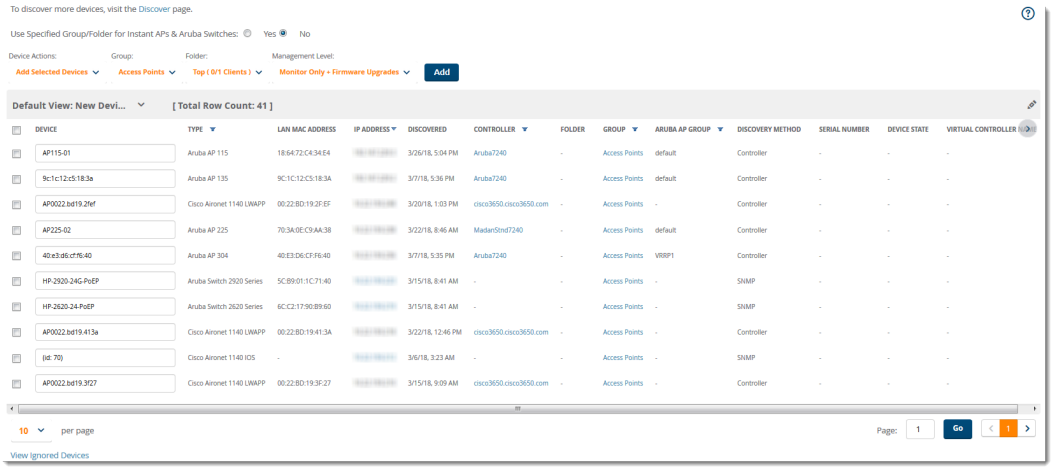
Once you have set up an Instant GUI Config group, devices that are added to this group can be managed using Instant GUI Config.

NOTE

When importing Instant devices in bulk to a new group, AirWave selects the first device added to that group as the "golden" configuration. The configuration will be pushed to other Instant Virtual Controllers added to the group. As a recommended best practice, select a Virtual Controller with a configuration that can be used as the golden configuration for other devices, and add it to the group before adding any others.

1. Click the **New Devices** statistics icon in the top header to open the **Devices > New** page and view information about the newly discovered devices (see Figure 18).

Figure 18: *List of Discovered Devices*



2. Select the check box beside the Instant device(s) you want to add to the Instant Virtual Controller group.
3. Use the **Group** and **Folder** drop-down lists to select the groups and folder to which the devices will be added. The default group appears at the top of the Group list.
4. Click **Add**.
5. Go to the **Devices > List** page, select the folder that contains the newly added devices, and verify that the devices have been properly assigned.

NOTE

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

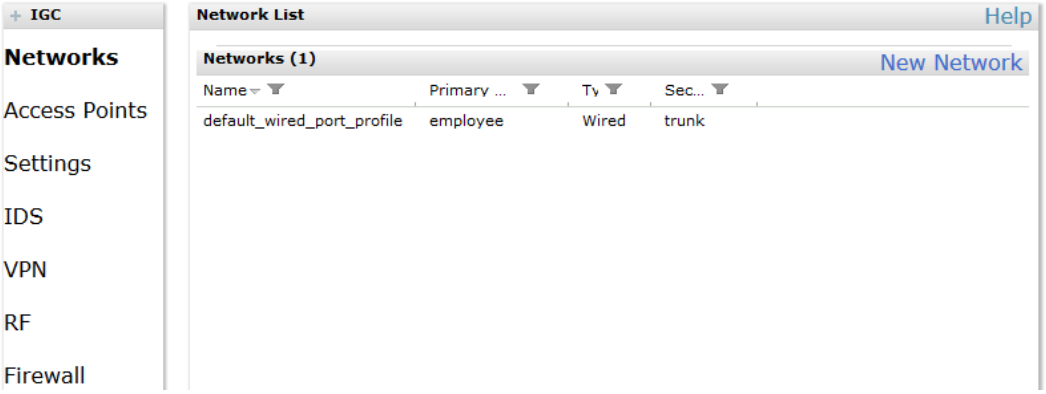
The Instant GUI Config WebUI

The **Groups > Instant Config** page of the AirWave WebUI allows network administrators to configure Instant Virtual Controllers remotely through AirWave. The flow of pages within the Instant GUI Config UI closely resemble the pages available in Aruba Instant.

NOTE

For more information on the Instant settings configurable via the AirWave, WebUI, refer to the *Aruba Instant User Guide*.

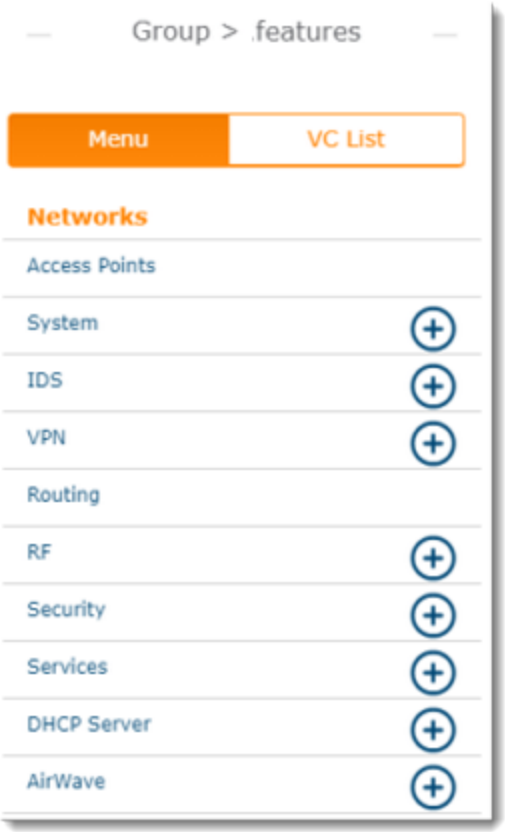
Figure 19: *Groups > Instant Config*



Group Configuration

The **Groups > Instant Config** page provides an expandable menu of the available Instant group configuration settings, as shown in Figure 20. When you configure group settings, AirWave applies the changes to all devices in the group. Click the **VC List** tab to view and modify individual devices within the group.

Figure 20: *Group Menu*



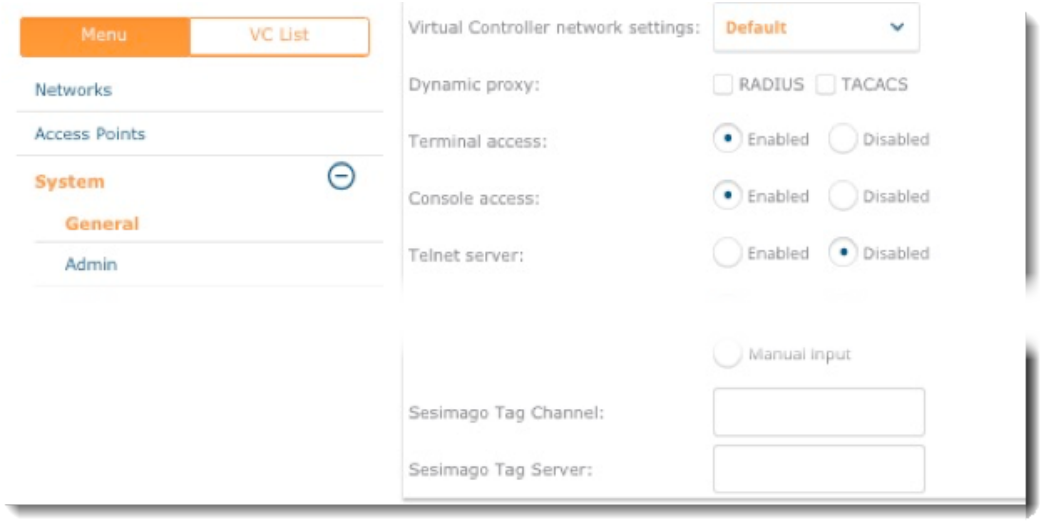
System Configuration

For Instant APs (IAPs) running Instant 8.5.0.0 or later, AirWave supports ESL profiles used to configure an Electronic Shelf Label (ESL) label by SES-imagotag. You can configure ESL Settings using Instant GUI Config (IGC) for the devices in a group.

To configure ESL settings:

1. Go to **Groups > Instant Config**, then click the VC List tab.
2. Select the devices you want to configure from the list of access points, then click **Bulk Edit**. Or, click the blue name link to open the configuration page for the device.
3. Enter the communication channel number for the "Sesimago Tag Channel" option and the IPv4 address for the "Sesimago Tag Server" option (see Figure 21).
4. Click **Apply**.

Figure 21: *Group Configuration using the IGC*



DHCP Server Configuration

The DHCP Servers page allows you to configure various DHCP modes, including a centralized DHCP scope for L2 and L3 clients. For more information about DHCP scopes, see the *Aruba Instant User Guide*.

To configure a centralized scope:

1. Go to **Groups > Instant Config**, then click **DHCP** or ⊕ to open the **DHCP Servers** page.
2. Enter a name for the DHCP profile.
3. Choose one of the following types:
   - **Centralized, L2 Clients**. In this mode, the VC bridges the DHCP traffic to the controller over the VPN or GRE tunnel. The IP address is obtained from the DHCP server behind the controller serving the VLAN or GRE of the client.
   - **Centralized, L3 Clients**. In this mode, the VC acts as a DHCP relay agent that forwards the DHCP traffic to the DHCP server located either in the corporate or local network. The centralized, L3 VLAN IP is used as the source IP, and the IP address is obtained from the DHCP server.
4. Enter the VLAN ID. Or, disable the **Split tunnel** option to enter a comma-separated VLAN range.
5. If the **DHCP relay** option is enabled, enter the IP addresses of the DHCP server.
6. For centralized, L3 clients, enter the DHCP subnet gateway IP address and the subnet mask of the gateway IP address.
7. Optionally, add a **DHCP Option 82** to the DHCP traffic forwarded to the controller. Select **Alcatel** to enable the **DHCP Option 82**.

   The format for the Option 82 string, which is specific to Alcatel and can't be altered, consists of the following:
   - Remote Circuit ID; X AP-MAC; SSID; SSID-Type
   - Remote Agent; X IDUE-MAC

AirWave Configuration

The **AirWave** configuration menu on this page contains a number options that allow AirWave to automatically make changes to the following settings on any virtual controller connected to the AirWave server.

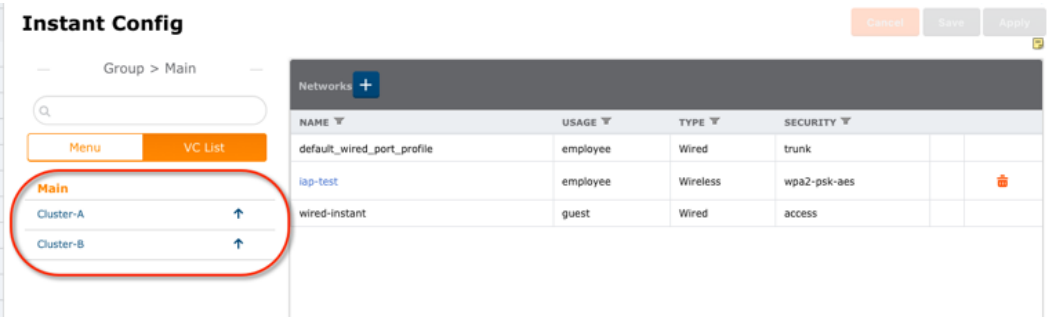
- **Auto-configure Virtual Controller** - Selecting **Yes** allows AirWave to automatically push configuration to new virtual controllers when the are added to the group.

- **Allow Configuration of Country Code**: Selecting **Yes** allows you to manually configure the country code for the group under **IGC > Settings > General > Country Code**. When No is selected, the previously described field is grayed-out. This is set to **No** by default.
- **Allow configuration of AirWave Settings**: Selecting **Yes** allows you manually configure the AirWave field under **IGC > Settings > Admin**. When **No** is selected, the previously described field is grayed-out and AirWave pushes this information to each virtual controller in the group. This is set to **No** be default.
- **Policy Version** and **Copy policy from group**: These options cannot be executed at the same time.
  - **Policy Version**: This displays the current policy version, and when selected, allows you to select another from the drop-down menu.
  - **Copy policy from group**: When selected, this option allows you to copy the policy from another group.

Virtual Controller Configuration

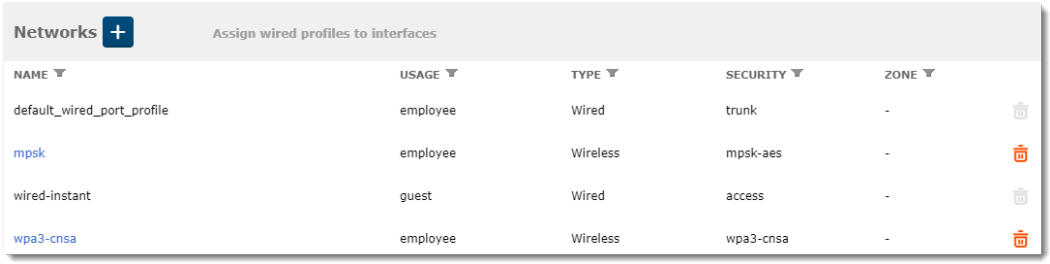
From the **Groups > Instant Config** page, click the **VC List** tab and select a device from this list to change settings for individual devices. Afteryou have selected a Virtual Controller from the list, the Groups > Instant Config page allows you to configure settings for the networks available on each device, such as authentication mode, access point radio settings, and VPN settings. You can also add and delete wired and wireless networks. Any configuration changes made when Instant Config is in device focus applies only to the selected device.

Figure 22: *e Focus*



Network Configuration

The **Networks** page is where you configure settings for the networks available on each device, such as the authentication mode, access point radio settings, and VPN settings. From this page, you can also add and delete wired and wireless networks.



MPSK and WPA3-CNSA Configuration

1. Click + to add a network.
2. Enter the network name, or SSID, then click **Next**.
3. In the Security tab, select one of the following **Key management** options:
   - **MPSK-AES**. Personal security settings for employee and voice users.
   - **WPA3-CNSA**. Enterprise security settings for the employee and voice network SSID profiles

Figure 23: *Configuring the MPSK Security Settings*

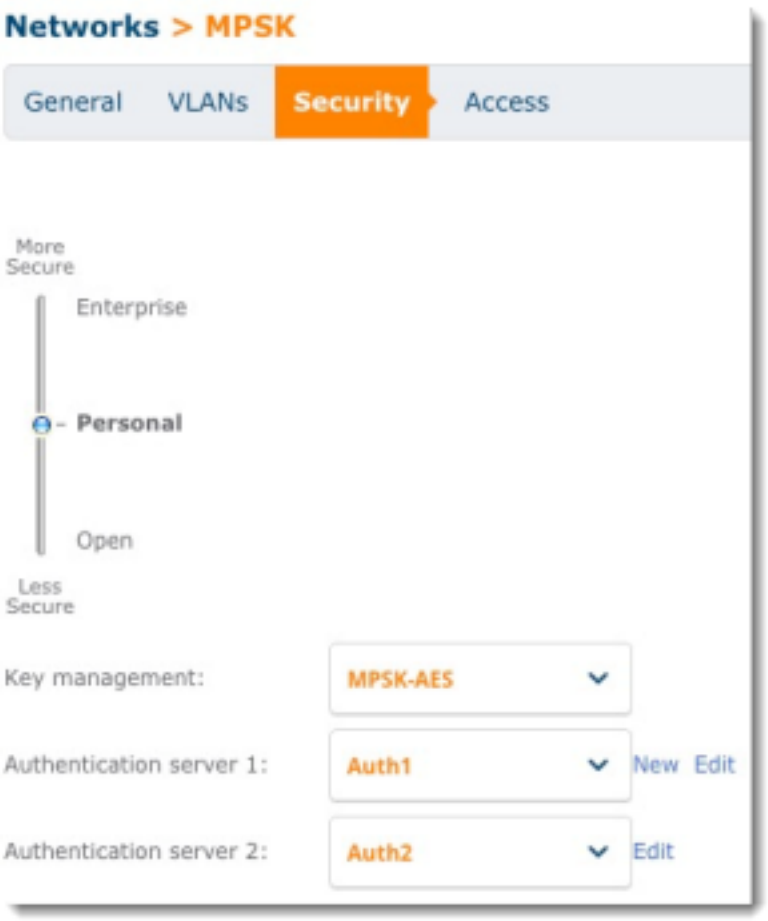
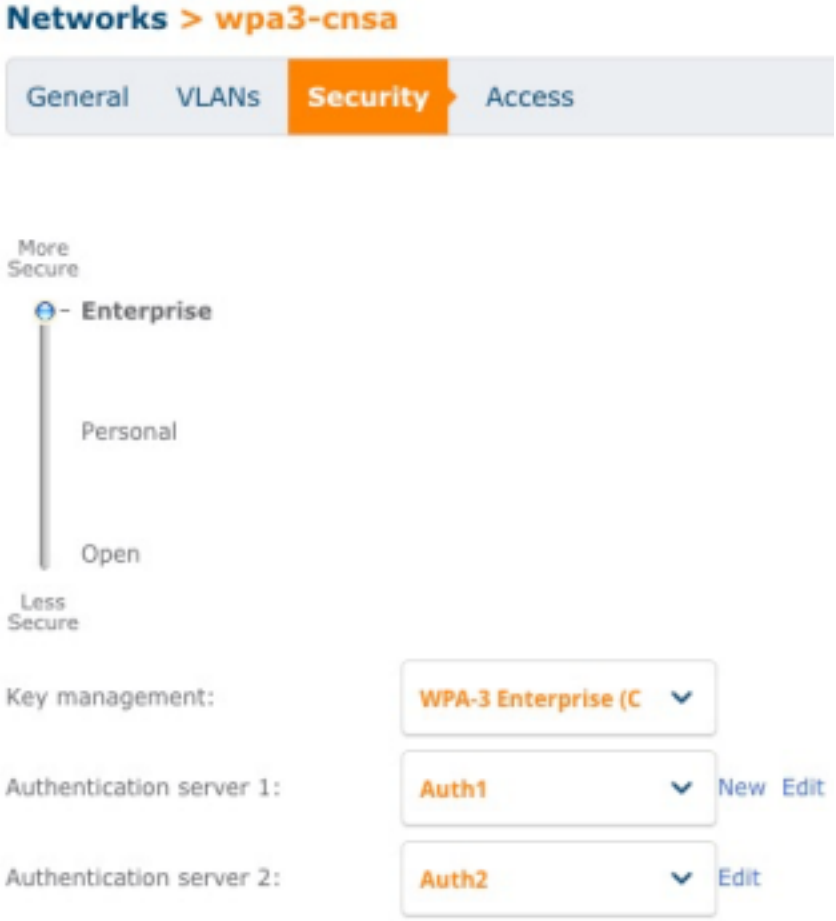

Networks > MPSK
General
VLANs
Security
Access
More Secure
Enterprise
Personal
Open
Less Secure
Key management:
MPSK-AES
Authentication server 1:
Auth1
New
Edit
Authentication server 2:
Auth2
Edit

Figure 24: *Configuring the WPA3-CNSA Security Settings*



4. Select the authentication server.
5. Enter the RADIUS re-authentication interval in minutes.
6. Click **Apply**. AirWave updates the **Network** page with the network profile.

AirWave Settings

The **AirWave** menu in IGC provides options to view configuration history, configuration mismatches, and AP events, as well as, settings that dictate how AirWave interacts with IAP groups and virtual controllers.

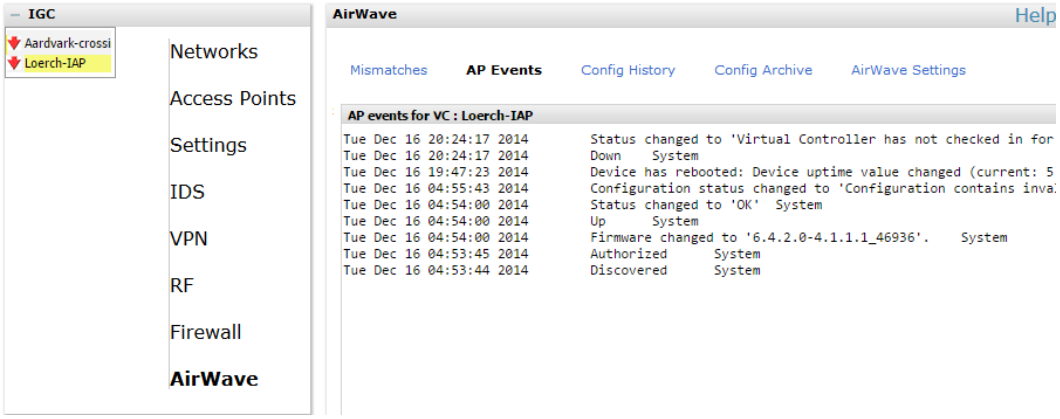
Mismatches

The **Mismatches** page displays the configuration mismatches for the selected virtual controller. For more information about resolving mismatches through the Instant Config, see "Resolving Mismatches when Instant Config is Enabled" on page 41.

AP Events

The **AP Events** page provides a list of events pertaining to the selected virtual controller since being discovered by AirWave.

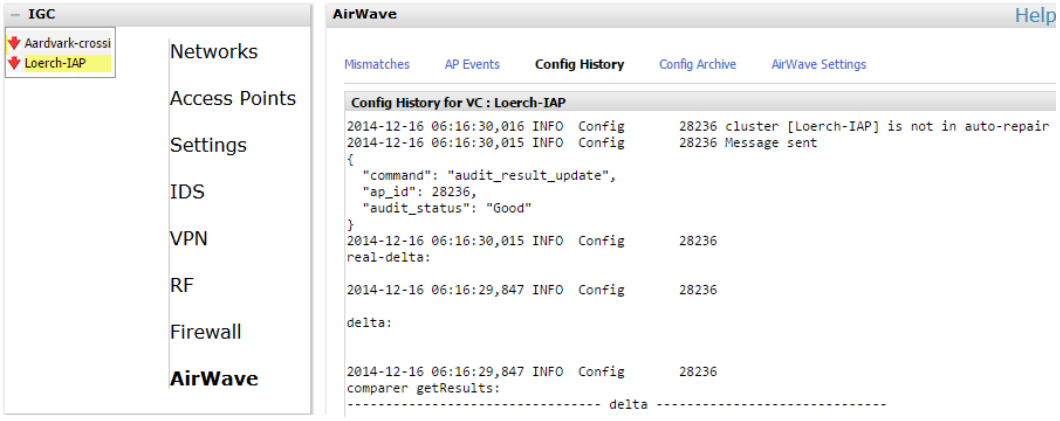
Figure 25: *AirWave > AP Events*



Config History

Config History displays the current and previous configurations on the selected virtual controller as well the delta between the two configurations.

Figure 26: *AirWave > Config History*



Config Archive

The Config Archive page displays the current running configuration on the selected virtual controller. Additionally, you can run an audit on the selected virtual controller's configuration.

Clicking on the caret displays drop-down list of all audited configurations. By selecting two configurations and clicking **Delta**, you can view the difference between any two configurations.

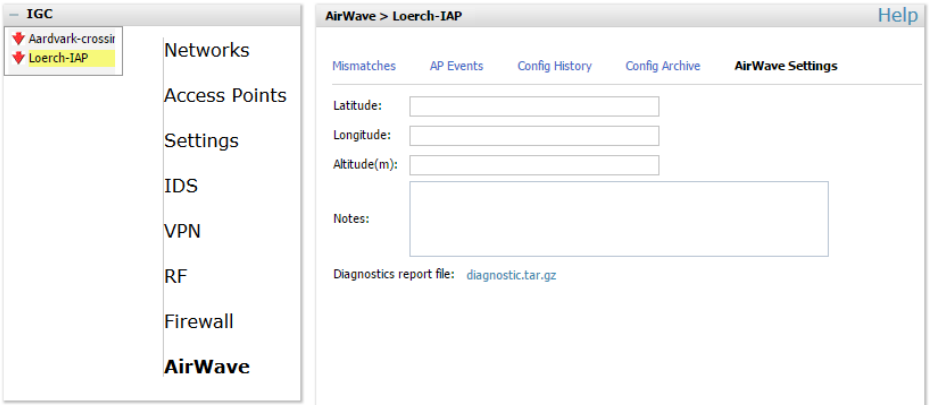
AirWave Settings

The AirWave Setting page changes depending on whether or not a virtual controller is specified.

With A Virtual Controller Specified

This page allows you to enter and save the latitude, longitude, altitude in meters, and any notes about the specified virtual controller.

Figure 27: *AirWave Settings (VC Selected)*

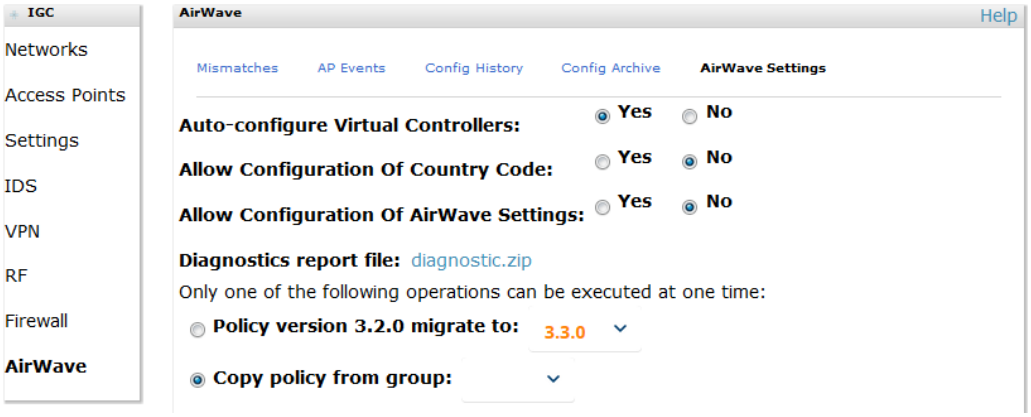


Without A Virtual Controller Specified

This page contains a number options that allow AirWave to automatically make changes to certain settings on any virtual controller connected to the AirWave server.

- **Auto-configure Virtual Controller** - Selecting **Yes** allows AirWave to automatically push configuration to new virtual controllers when the are added to the group.
- **Allow Configuration of Country Code**: Selecting **Yes** allows you to manually configure the country code for the group under **IGC > Settings > General > Country Code**. When No is selected, the previously described field is grayed-out. This is set to **No** by default.
- **Allow configuration of AirWave Settings**: Selecting **Yes** allows you manually configure the AirWave field under **IGC > Settings > Admin**. When **No** is selected, the previously described field is grayed-out and AirWave pushes this information to each virtual controller in the group. This is set to **No** be default.
- **Policy Version** and **Copy policy from group**: These options cannot be executed at the same time.
  - **Policy Version**: This displays the current policy version, and when selected, allows you to select another from the drop-down menu.
  - **Copy policy from group**: When selected, this option allows you to copy the policy from another group.

Figure 28: *AirWave Settings (No VC Selected)*



Where to Get Additional Information

Click the Help link (Help) in the upper-right portion of the page open the Instant Configuration User Guide, or refer to the following documents for additional information.

- *Aruba Instant 8.5.0.0 User Guide*

- *AirWave 8.2.11.0 Release Notes*

The following additional tasks can be completed in AirWave. These include configuration and monitoring tasks.

Resolving Mismatches

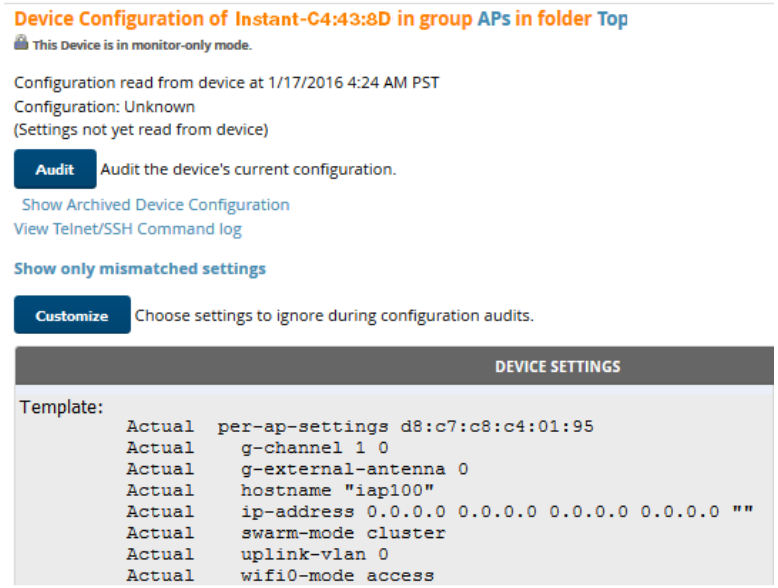
After adding a device, the new device will appear in AirWave as two devices: the first is the Virtual Controller for that Instant network, and the second is the access point itself. In some cases, the Instant device shows up as having Mismatched configuration. This occurs when the AirWave information was received from Instant via the DHCP server (i.e, was not manually configured). The method for resolving mismatches varies based on whether Instant Config is enabled.

Resolving Mismatches when Instant Config is Disabled

When Instant Config is disabled, configuration for IAP devices is done via the Instant UI. In this case, AirWave is used to monitor the devices, and when necessary, to update the Instant template and variables within the template.

Clicking on the mismatched device opens the audit page of the device, showing the reason for the mismatch. The configuration shows the desired configuration versus the current Instant configuration. As shown in the following image, the AirWave IP address, shared secret, and organization string has to be provisioned on the Instant device.

Figure 29: *Devices > Audit page*



Perform the following steps to resolve the mismatch.

1. Navigate to the **AP/Devices > Manage** page for that Instant device.

NOTE

The **Devices > Manage** page is not available when Instant Config is enabled.

2. Change the **Management Mode** option to **Manage Read/Write**.
3. Click on **Save and Apply** at the bottom on the page.
4. When the **Confirm changes** page opens, click on **Apply Changes Now** for the changes take effect.

Upon completion, the configuration will be synced to the Instant network. The status of the device will initially display as 'Verifying' during this process. The status will change to 'Good' after the provisioning is successful.

NOTE

This is the same process for any configuration change sync that is done in future.

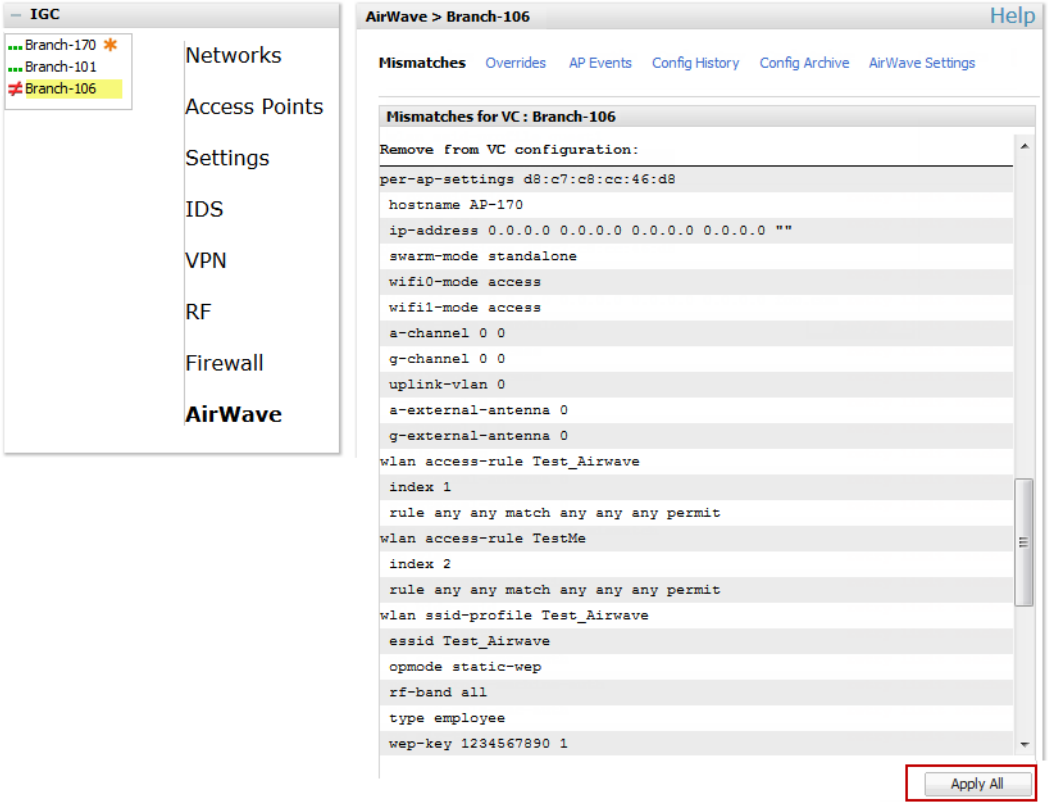
Resolving Mismatches when Instant Config is Enabled

In Instant Config, mismatches are indicated with a red, unequal symbol (≠) beside the device name. Click on the device name, then navigate to **AirWave > Mismatches** to view the details for mismatch. Click **Apply All** at the bottom of the page to resolve the mismatches.

NOTE

The **Apply All** button resolves all mismatches. You cannot select individual mismatches to resolve.

Figure 30: *Viewing mismatches in Instant Config*

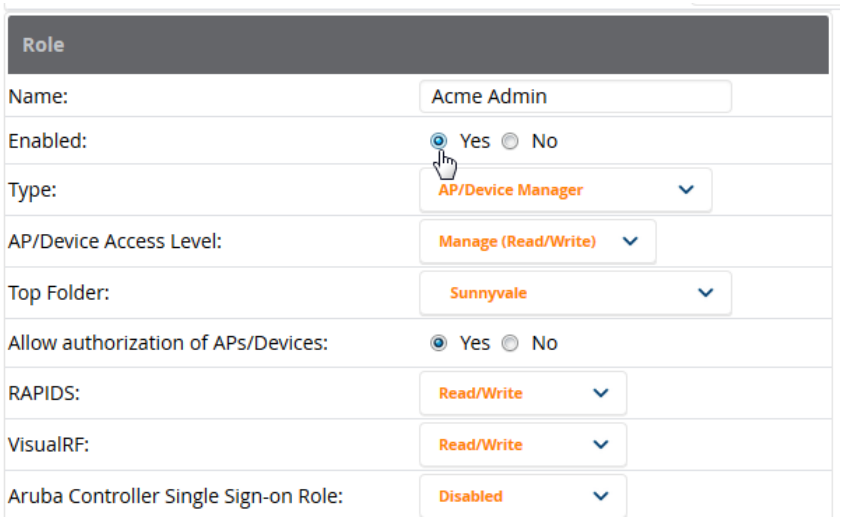


Enabling the IAP Role

As shown previously, new IAP devices can be added to AirWave automatically. In some cases, after a device is added, the Admin may want to enable store-specific access. In this case, the Admin might enable a specific IAP role.

1. Enable the newly created Admin User Role in **AMP Setup > Roles**, as shown in Figure 31.

Figure 31: *Enable Admin User Roles in* ***AMP Setup > Roles***



2. In **Groups > Template** for the newly created group, verify the first Virtual Controller's auto-created template.

NOTE

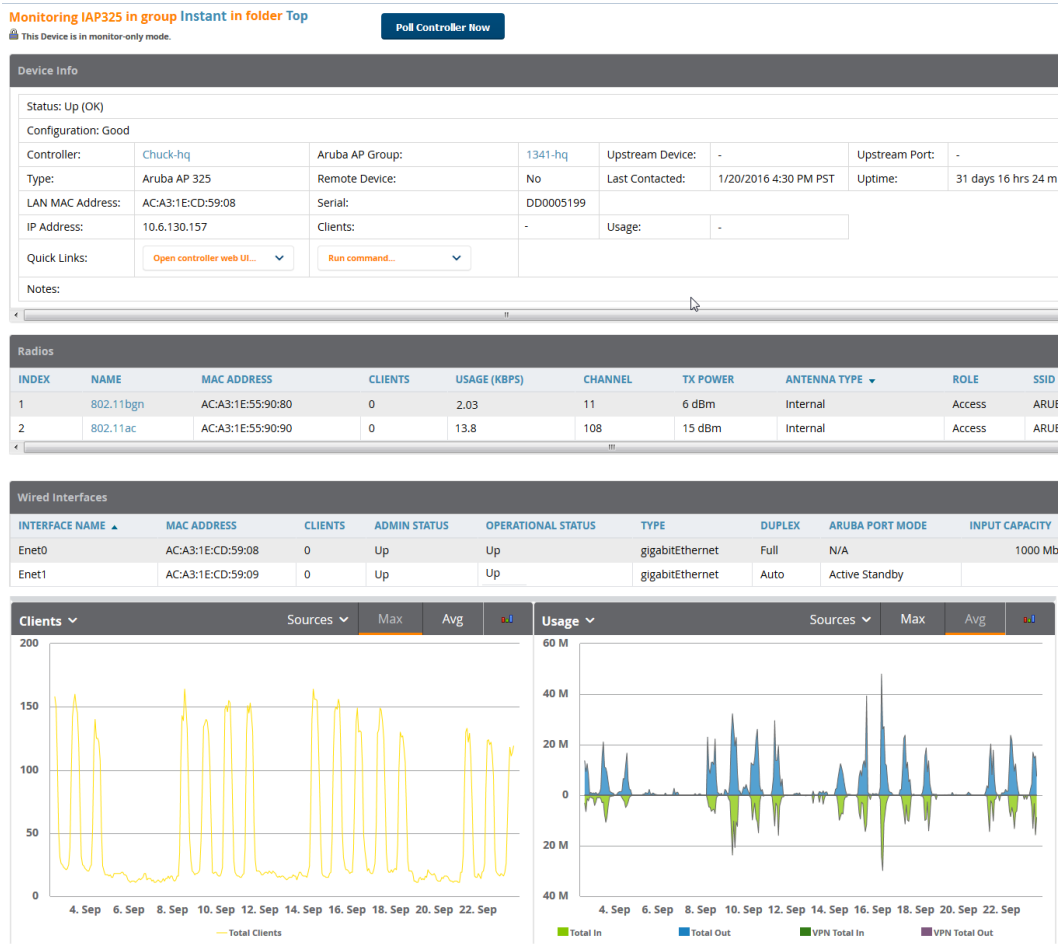
The auto-created template is most useful if the first Virtual Controller for the top-level Organization String is fully configured on-site *before* it is pointed at AirWave in the Virtual Controller's UI.

3. Evaluate, approve, or ignore incoming Virtual Controllers with a different top level Organization String and/or Shared Secret in the **Devices > New** list. Subsequent IAP are auto-authorized if they have an Organization/Shared Secret key that matches the Shared Secret key of any existing authorized Virtual Controller in the top-level Organization String.
4. Set the initial Virtual Controller to **Manage Read/Write** mode and push the good configuration to the subsequent IAPs.
5. Set up AirWave users to have access to specific folders, if desired.

Monitoring Devices

Use the **Devices > Monitor** page to monitor your Instant devices. AirWave provides you with detailed information for your virtual controller, APs, and radios. This information includes spectrum interferers, rogue clients, and channel utilization. The image below shows an example of radio statistics.

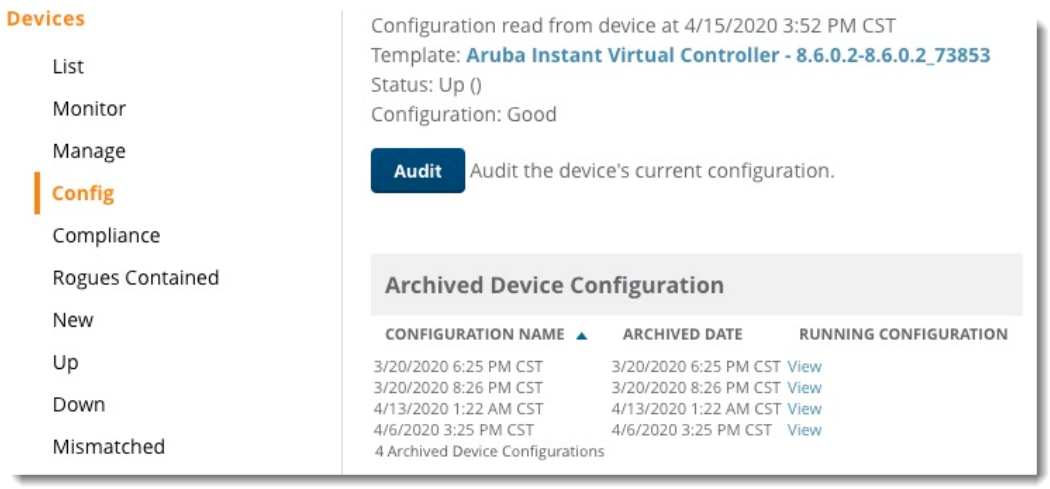
Figure 32: *Monitoring Radios*



Running Config Backups

When a configuration change is made from the WebUI or CLI, AirWave runs a backup and archives the device configuration on the **Devices > Config** page. You can use the device configuration for audits and data recovery.

Figure 33: *Archived Device Configuration for Instant APs*



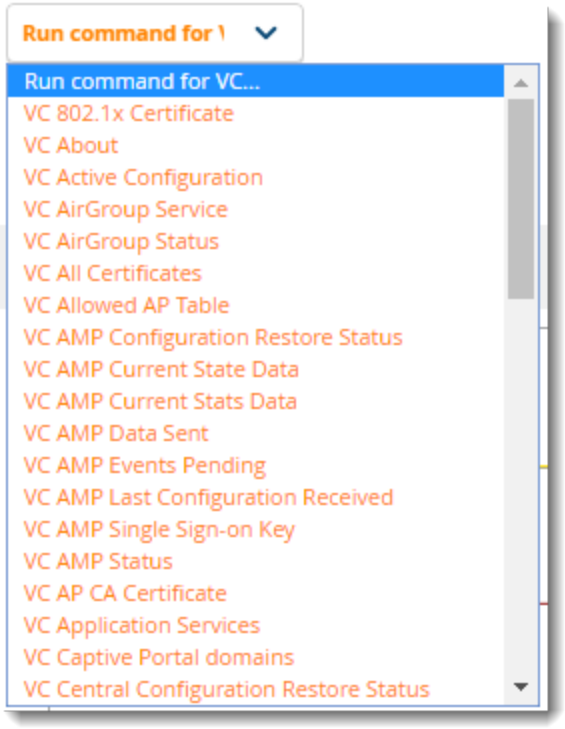
Running Commands

If your Instant devices are running Instant 3.2 or later, you can run a command from **Devices > Monitor** page for the virtual controller or AP. On the virtual controller, you can also run commands for all APs as well as for the current virtual controller.

NOTE

When you first run a command, the results can take up to a minute to appear. For subsequent commands, the results will appear after one or two seconds.

Figure 34: *Selecting a Command for a VC*



This section describes some best practices to follow when using AirWave to monitor and configure Instant devices. It also includes some known issues to take into consideration when using AirWave. This list is inclusive of the AirWave release notes and Instant release notes.

Best Practices

- Keep Instant devices in Monitor Only mode to audit the device and to ensure that configurations are not automatically pushed. This practice is consistent with the rest of AirWave.
- Be sure that the default configuration is validated and has been pre-tested in a non-production environment prior to applying it to a production network. Any changes that are made to this configuration will follow the same process each time and will be applied to other Instant networks.
- If you modify an IAP device's configuration through the Instant user interface, we recommend that you put the device in Manage Mode, and then use the **Import Settings** button from the **Devices > Manage** page. When using this method instead of Instant Config, you can import settings and update the template from a single page. Import the settings and then wait approximately a minute. If you find that you need to also update the template, the **Devices > Manage** page for the Virtual Controller provides a link to quickly access the template.

Known Issues with the Instant Integration with AirWave

- If the Organization String configured on the Instant device is different than what is statically written in the template, AirWave will overwrite the configured Organization String to match the template.
- The Instant primary device sends an update message to AirWave every minute. If the send fails, then the device will continue to send a state message every two seconds. If the send fails 25 times, then Instant will determine that AirWave is down.