

Aruba Instant in AirWave 8.2



Copyright Information

© Copyright 2016 Hewlett Packard Enterprise Development LP

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
3000 Hanover Street
Palo Alto, CA 94304
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 dl-gplquery@arubanetworks.com.

| | |
|---|-----------|
| About this Document | 6 |
| Overview of Aruba Instant | 6 |
| Instant Management with AirWave | 6 |
| AirWave Security Options | 6 |
| Intrusion Detection System | 7 |
| Managing the Firmware Image | 7 |
| Task 1: Uploading the Firmware to AirWave | 7 |
| Task 2: Configuring Automatic Firmware Updates | 7 |
| Using Instant with AirWave | 8 |
| Secure Access to AirWave | 9 |
| AirWave Pages with Instant-Specific Features | 9 |
| Supported Firmware | 9 |
| Setting up Aruba Instant | 12 |
| Overview | 12 |
| Setting up Instant Manually | 12 |
| Creating your Organization String | 12 |
| Authenticating to the AirWave Server | 13 |
| Shared Key Authentication | 13 |
| Whitelist Authentication | 13 |
| Entering the Organization String and AirWave Information into the IAP | 14 |
| Setting up Instant Automatically | 15 |
| Verifying the Shared Secret | 16 |
| Completing the Setup | 16 |
| Using Template Configuration | 18 |
| Adding the First Instant Device to AirWave | 18 |
| Updating the Instant Template | 18 |
| Adding Additional Instant APs to AirWave | 19 |
| Adding Multiple Devices from a File | 20 |
| Changing the Mode to Monitor Only for New Instant Devices | 21 |
| Editing Variables | 22 |
| Editing Individual Virtual Controller Values | 22 |
| Bulk Editing of Multiple Virtual Controllers | 23 |
| Using Custom Variables | 23 |
| Applying Changes | 24 |
| Using Instant Config | 26 |
| Enabling Instant Config | 26 |
| Buttons and Icons in Instant Config | 27 |
| Importing Devices for Instant Config | 28 |
| Add Newly Discovered Devices to a Group | 28 |
| The Instant Config UI | 29 |
| Group Focus | 29 |
| Virtual Controller Focus | 30 |
| Network Focus | 30 |
| Instant Config > AirWave | 31 |
| Mismatches | 31 |

| | |
|--|-----------|
| AP Events | 31 |
| Config History | 31 |
| Config Archive | 32 |
| AirWave Settings | 32 |
| Where to Get Additional Information | 33 |
| Other Available Tasks | 34 |
| Resolving Mismatches | 34 |
| Resolving Mismatches when Instant Config is Disabled | 34 |
| Resolving Mismatches when Instant Config is Enabled | 35 |
| Enabling the IAP Role | 36 |
| Monitoring Devices | 36 |
| Run Commands | 37 |
| Best Practices and Known Issues | 40 |
| Best Practices | 40 |
| Known Issues with the Instant Integration with AirWave | 40 |

This document describes the Aruba Instant access point and Virtual Controller system as well as the procedure to integrate this system with AirWave. This section contains the following points:

- "Overview of Aruba Instant" on page 6
- "Instant Management with AirWave" on page 6
- "Using Instant with AirWave" on page 8
- "AirWave Pages with Instant-Specific Features" on page 9
- "Supported Firmware" on page 9

Overview of Aruba Instant

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 Adaptive Radio Management (ARM).

Instant Management with 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.

AirWave Security Options

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 CA:** Trusted Root CA: C=US, O=Equifax, OU=Equifax Secure Certificate Authority

By default, AirWave supports only pre-shared key authentication. To enable support for certificate authentication with a failthrough to pre-shared key authentication or certificate authentication only, navigate to **AMP Setup>General>Aruba Instant Options**, and select the option **PSK and Certificate** or **Certificate only**. If you enable certificate authentication, you can view the current AirWave certificate using the **View Certificate** link on that page, or click **Change** to upload a new certificate file to the AirWave server.

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.

Managing the Firmware Image

AirWave pushes firmware to the Aruba Instant Virtual Controller, and the Virtual Controller pushes the firmware to the rest of its IAPs. When using AirWave to manage IAPs, you can upgrade the firmware by loading the firmware onto AirWave, and then scheduling an upgrade from AirWave.

If you have a mixed deployment with multiple Instant products, you can upload firmware for each of the device types.



If you are using Aruba Activate to set up your devices, then firmware updates will be available from the Activate server. Refer to the documentation that accompanies Aruba Activate for more information.

To manage the firmware image, complete the following tasks in this order:

- [Task 1: Uploading the Firmware to AirWave on page 7](#)
- [Task 2: Configuring Automatic Firmware Updates on page 7](#)

Task 1: Uploading the Firmware to AirWave

The first task in preparing for a firmware upgrade is loading the software image to AirWave. To add an Instant software image to AirWave, complete the following steps.

1. Download the Instant firmware from the Aruba support site.
2. In the AirWave UI, navigate to **Device Setup > Upload Firmware & Files**.
3. Click the **Add** button next to **New Firmware File**.
4. Specify **Aruba Device (Any Model)** from the **Type** drop-down list.
5. Check the **Upload firmware files (and use built-in firmware file server)** radio button.
6. The **Server Protocol** field is not required for Instant, but setting it to **HTTPS** in the drop-down menu is recommended to avoid confusion.
7. Click the **Choose File** button and locate the firmware file you downloaded in Step 1.
8. Click **Add** to complete the upload.

Task 2: Configuring Automatic Firmware Updates

To configure an AirWave group for automatic upgrades as new devices are added, complete the following steps:

1. Navigate to the **Groups** tab and select your Instant group from the list.

2. On the group's page, click the **Firmware** tab.
3. Check the **Yes** radio button next **Enforce Group Firmware Version**.
4. Select the version of Instant from the **ArubaInstant Virtual Controller** drop-down menu.
5. (Optional) To allow the downgrade of new device, the **Yes** radio button next to **Allow Downgrade of Devices**.
6. Click **Save** to complete the configuration or **Save and Upgrade Devices** to complete the configuration and immediately upgrade devices in the selected group.

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.

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 **APs/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.

AirWave Pages with Instant-Specific Features

The following is a summary of AirWave pages affected by Aruba Instant support:

- **APs/Devices > New:** When an Aruba Instant device appears in the **APs/Devices > New** page, an admin user can mouse over the value on the Type column to display the device's Shared Secret with AirWave.
- **APs/Devices > List:** The Virtual Controller is listed as an additional device, even though it is part of the existing set of IAPs. An asterisk icon (*) 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 **APs/Devices > List** page, Device Inventory reports, and any other AirWave pages that list your network devices.
- **Clients > Client Detail:** Once 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 **Clients > Client Detail**.
- **APs/Devices > Audit:** Aruba Instant configuration fetching can be performed in **APs/Devices > Audit**. When template configuration is used to manage devices, the running configuration is stored on the IAP and verified by the template.
- **APs/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:** This feature is available if **Enable Instant GUI Config** is enabled on the **Groups > Basic** page. This feature allows you to use AirWave as a management console with the same UI as the IAP device.
- **RAPIDS:** Because Instant does not support mitigation or high-level rogue reporting, it does not synchronize classification. All rogue devices are reported and stored in AirWave for evaluation based on high-level rule sets. Instant currently does not match wireless BSSIDs to local MAC addresses within an IAP's ARP table, and does not currently support IDS event notification.
- **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.

Supported Firmware

AirWave supports Aruba IAPs running Instant 6.4.3.0-4.2 and prior versions, including the management of configuration settings and software upgrades. The following table shows when each new version of Instant was initially supported in AirWave.

Table 1: *Instant support in AirWave*

| Instant Version | Support Introduced | Support for Instant Config |
|-----------------|----------------------------|----------------------------------|
| 6.4.3.x-4.2.0.0 | AirWave 8.1/ AirWave 8.0.9 | Yes |
| 6.4.2.3-4.1.2.0 | AirWave 8.1/ AirWave 8.0.9 | Yes |
| 6.4.2.0-4.1.1.0 | AirWave 8.0.4 | Yes |
| 6.4.0.0-4.1.0.0 | AirWave 8.0 | Yes, introduced in AirWave 8.0.4 |
| 6.3.1.0-4.0.0.0 | AirWave 8.0 and 7.7.10 | Yes |
| 6.2.1.0-3.4.0.0 | AirWave 7.7.2 | Yes |
| 6.2.0.0-3.3.0.0 | AirWave 7.6.4 | Yes |
| 6.2.0.0-3.2.0.0 | AirWave 7.6.1 | Yes |
| 6.1.3.4-3.1.0.0 | AirWave 7.5.6 | No |
| 6.1.3.1-3.0.0.0 | AirWave 7.5.0 | No |

Overview

You can set up Aruba Instant in one of the following ways:

- Manually. See ["Setting up Instant Manually" on page 12](#).
- Automatically (through DHCP). See ["Setting up Instant Automatically" on page 15](#).
- Using Aruba Activate. Refer to the documentation that accompanies Aruba Activate for detailed information.



If you are using Aruba Activate to set up your devices, the devices will automatically move to the appropriate group if "Autoconfigure New Virtual Controllers" is enabled. If the group is template based, then the device will be configured via templates. If Instant Config is enabled on the group, then Instant Config will be used to configure the devices. In addition, autoconfiguration will wipe out any existing configuration on the device, including the factory defaults. The device will be configured based on the group policy.

The automatic setup is most suited for a multi-site Instant deployment. Both options are summarized here, but refer to the Aruba Instant documentation for more information on setting up the hardware and configuring the network.

For each remote location, an on-site installer is required to physically mount the IAPs, connect to the Aruba Instant SSID, configure the WLAN, configure the names of the IAPs, and enter the information in the first IAP's user interface that will enable communication with AirWave. The first Instant network that is added to AirWave includes the 'golden' configuration that is used as a template to provision other Instant networks 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 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.

Setting up Instant Manually

When setting up Aruba Instant manually, you will be requested to provide an Organization string, the AirWave IP address, and a Shared Key. The steps to create this information are described in the following sections:

- ["Creating your Organization String" on page 12](#)
- ["Authenticating to the AirWave Server" on page 13](#)
- ["Entering the Organization String and AirWave Information into the IAP" on page 14](#)

Creating your Organization String

The Organization String is a set of colon-separated strings created by the AirWave administrator to accurately represent the deployment of each Aruba Instant system. This string is entered into the Aruba Instant UI by the on-site installer.

The format of the Organization String is Org:subfolder1:subfolder2... and so on, up to 31 characters long. Org, the top-level string, is generally the name of your organization and is used to automatically generate the following (if not already present) in AirWave:

- AirWave Role: Org Admin (initially disabled)
- AirWave User: Org Admin (assigned to the role Org Admin)

- Folder: Org (under the Top folder in AirWave)
- Configuration Group: Org

Additional strings in the Organization String are used to create a hierarchy of subfolders under the folder named Org:

- subfolder1 would be a folder under the Org folder
- subfolder2 would be a folder under subfolder1

To create your Organization String, consider the plan of how your Aruba Instant IAPs are to be physically distributed. As a best practice, the Organization String should mirror your company's geographical or internal reporting structure. For example, if you plan to deploy Aruba Instant in four stores in two different cities for Acme Corporation, your Organization Strings might look like these:

- Acme:New York:Times Square Store
- Acme:New York:Queens Store
- Acme:San Francisco:Sunset Store
- Acme:San Francisco:SOMA Store

Authenticating to the AirWave Server

When the AirWave administrator manually authorizes the first Virtual Controller for an organization, AirWave uses the Virtual Controller's shared key or authentication certificate to authenticate other Instant devices on the network. Once individual Instant access points successfully completed authentication, they can also be validated against a predefined whitelist before they appear in the **APs/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 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 Virtual Controller for an organization. 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 the on-site installer setting up the Virtual Controller and other Instant devices on the network. The AirWave administrator then manually authorizes the Virtual Controller shared secret key when it appears in the **APs/Devices > New** list. After the VC has been validated, other Instant devices using that shared key will automatically to the AirWave server, and appear in the **APs/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 an Aruba Instant device.

Whitelist Authentication

The Instant whitelist database is a list of the Instant APs that are allowed to access the AirWave server after completing pre-shared key or certificate authentication. The Instant AP whitelist can be manually configured using the AirWave UI, or imported into AirWave in comma-separated values (CSV) format.

Whitelist files can include the following data columns. The **Name** field is mandatory, and each entry 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
- custom_variable_1...custom_variable_10

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 Francisco:CenterTown:HillTop
```

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

To enable whitelist authentication and add Instant APs to a whitelist:

1. Navigate to **AMP Setup>General**
2. In the **Automatic Authorization** section, select **Whitelist**.
3. Click **Add devices to Whitelist**.
4. Click **Add an Instant AP to the Whitelist**.
5. Enter whitelist information for the Instant AP. Each whitelist entry must have an Instant AP name and either a serial number or a MAC address.
6. 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.

To import a whitelist file to the AirWave server:

1. Navigate to **AMP Setup>General>Automatic Authorization**
2. Click **Add devices to Whitelist**.
3. Click **Import Instant AP Whitelist from CSV**. The **Upload Options** page opens. This page describes the required fields and format for the whitelist file.
4. Select one of the following upload modes.
 - Update: Add new information to the existing whitelist database
 - Replace: Delete the existing whitelist database, and replace it with the new file.
5. Click **Browse** to select the CSV file, then click **Upload**.

Entering the Organization String and AirWave Information into the IAP

For the initial IAP/Virtual Controller set up in each location, the on-site installer logs in to the first IAP's web interface via the Aruba Instant configuration SSID, and navigates to **Settings > AirWave**. The installer then enters the correct Organization String, the AirWave IP address, and the Shared Secret key, as shown in [Figure 1](#). Perform the following steps to set up AirWave in Instant.

1. Log into your IAP.
2. Click on either the **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 1: *Aruba Instant > Settings page*

Settings [Help](#)

General Admin RTLS SNMP OpenDNS Uplink Enterprise Domains Walled Garden Syslog L3 Mobility

Local

Authentication: Internal

Username: admin

Password: •••••

Retype: •••••

AirWave

Organization: AirWave

AirWave IP: 10.15.76.165

AirWave backup IP: 10.15.76.166

Shared key: ••••••••

Retype: ••••••••

[Hide advanced options](#) OK Cancel

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

Setting up Instant Automatically

Instant can be configured automatically using DHCP options 60 and 43.

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

Verifying the Shared Secret

After the role is enabled, the Aruba Instant device will appear in the **APs/Devices > New** page, the admin user should mouse over the value under the **Type** column to verify the device's Shared Secret with AirWave, as shown in [Figure 2](#).

Figure 2: Mouse over the Type column to view the Shared Secret

| DEVICE | TYPE | IP ADDRESS | LAN MAC ADDRESS | DISCOVERED |
|---|----------------------------------|------------|-----------------|---------------------|
| <input type="checkbox"/> Instant:C4:43:8D | Aruba Instant Virtual Controller | - | - | 10/29/2014 12:41 PM |

10 per page

Shared Secret: airwave

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



With an Organization specified, you do not have to select any Group or Folder from the drop-down menus on the **APs/Devices > New** page. In fact, if you do change the Group/Folder drop-down menus, all Organization-specified Virtual Controllers will ignore these values and will use the folder/group values from the Organization String instead. If you select **Add** for some non-Aruba Instant devices as well as some Organization-specified Virtual Controllers, the drop-down menus will apply to the non-IAPs but not the Virtual Controllers. 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.

Completing the Setup

After the setup is completed, determine whether the devices in your groups will be managed using template-based configuration or using Instant Config, and then refer to the following sections.

- [Using Template Configuration on page 18](#)
- [Using Instant Config on page 26](#)



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

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



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.

Additional information about creating templates for Aruba Instant is available in the *AirWave 8.2 User Guide*.

Adding the First Instant Device to AirWave

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

Figure 3: A new Instant device in AirWave

The screenshot shows the AirWave interface with a top navigation bar containing status cards for NEW DEVICES (1), UP (151), DOWN (92), WIRED DOWN (0), ROGUE (0), and CLIENTS (0). Below this is a message: "To discover more devices, visit the [Discover](#) page." The main section has filters for Device Actions (Add Selected Devices), Group (APs), Folder (Top (0/0 Clients)), and Management Level (Monitor Only + Firmware Upgrades), followed by an Add button. A table titled "Default View: New Devices" shows a single device: Instant-08:50:A0, Aruba Instant Virtual Controller, with LAN MAC ADDRESS 08:50:A0:6A:62:00, IP ADDRESS 10.51.3.55, and DISCOVERED 1/15/2016 11:53 AM. The table has a row count of 0. Below the table is a pagination control showing 100 per page, Page 1, and a Go button.

| DEVICE | TYPE | LAN MAC ADDRESS | IP ADDRESS | DISCOVERED |
|------------------|----------------------------------|-------------------|------------|--------------------|
| Instant-08:50:A0 | Aruba Instant Virtual Controller | 08:50:A0:6A:62:00 | 10.51.3.55 | 1/15/2016 11:53 AM |

1. Click **Add** to add the device. A Group and Folder do not have to be selected. The Instant device will automatically get added to the new group that was created.
2. Select **Apply Changes Now** to add the Instant device to the group.

Updating the Instant Template

As stated previously, the first Instant network that is added to AirWave automatically includes the default configuration that is used as the template to provision other Instant networks. You can view and, if necessary, edit this template directly on the **Groups > Templates** configuration page.



The **Groups > Templates** page is not available if Instant Config is enabled.



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.

Figure 4: *The Instant template editor*

```
Template
per-ap-settings %lan_mac%
hostname %hostname%
ip-address %ip_address% %netmask% %gateway% %dns_svr%
swarm-mode %swarm_mode%
uplink-vlan %vlan%
wifi0-mode %wifi0_role%
%if wifi1_role%
wifi1-mode %wifi1_role%
%endif%
%if dot11g_disable%
dot11g-radio-disable
%endif%
%if has_dot11g%
g-channel %dot11g_channel% %dot11g_xmit_power%
g-external-antenna %dot11g_antenna_gain%
%endif%
%if dot11a_disable%
dot11a-radio-disable
%endif%
%if has_dot11a%
a-channel %dot11a_channel% %dot11a_xmit_power%
a-external-antenna %dot11a_antenna_gain%
%endif%
%if enet0 bridging%
enet0-bridging
```

If you want to add additional variables to the template, the Allowed Variables section just to the right of the Instant template editor shows you the set of variables that can be added.

Figure 5: *Sample Allowed Variables*

The following variables may be used in the template. The value of each variable is configured on the APs/Devices Manage page for each device in the group. Each variable must be surrounded by percent signs: %hostname%. The %if...% statements must be terminated by %endif% and cannot be nested.

Available Variables:

| | |
|---------------------|--------------------|
| dns_svr | ip_address |
| domain_name | lan_mac |
| dot11a_antenna_gain | manager_ip_address |
| dot11a_channel | modem_pin |
| dot11a_disable | netmask |
| dot11a_xmit_power | preferred_master |
| dot11g_antenna_gain | swarm_mode |
| dot11g_channel | usb_port_disable |
| dot11g_disable | vlan |
| dot11g_xmit_power | wifi0_role |
| enet0_bridging | wifi1_role |
| gateway | zone_name |
| has_dot11a | |
| has_dot11g | |
| hostname | |

Refer to the *AirWave 8.2 User Guide* for detailed information about templates and variables.

Adding Additional Instant APs to AirWave

After the first Instant device has been provisioned and set up in AirWave, additional Instant networks in other locations can be added and provisioned automatically. To do this, set the **Automatically Authorized Virtual Controller Mode** option to **Manage Read/Write** on the **AMP Setup > General** page.

Figure 6: *Setting devices to Manage Read/Write mode*

| Automatic Authorization | |
|--|---|
| Add New Controllers and Autonomous Devices Location: | New device list ▼ |
| Add New Thin APs Location: | New device list ▼ |
| Automatically Authorized Switch Mode: | <input checked="" type="radio"/> Monitor Only + Firmware Upgrades <input type="radio"/> Manage Read/Write |
| Automatically Authorized Virtual Controller Mode: | <input type="radio"/> Monitor Only + Firmware Upgrades <input checked="" type="radio"/> Manage Read/Write |

When the second Instant contacts AirWave using the DHCP server options as described previously, and that second Instant device has the same Shared key, it shows up on AirWave. Because the devices are in **Manage Read/Write** mode, there is no need for manual intervention to provision these new Instant networks. The new networks will automatically be placed into the same group (if this is the desired configuration), but a new folder will be created to contain these devices.



Keep Aruba 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.

The golden template configuration from the first Instant network is used to provision the second Instant network in the new folder. 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
- Auth Password
- SNMPv3 Auth Protocol
- Privacy Password
- SNMPv3 Privacy Protocol
- SNMPv3 Username
- Telnet Username
- 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 7](#).

Figure 7: Device Setup > Add > Import Devices via CSV Page Illustration

Upload a list of devices

| Location | |
|----------|--------------------|
| Group: | IGC ▼ |
| Folder: | Top ▼ |

No file selected.

The list must be in comma-separated values (CSV) format, containing the following columns:
IP Address
SNMP Community String
Name
Type
Auth Password
SNMPv3 Auth Protocol
Privacy Password
SNMPv3 Privacy Protocol
SNMPv3 Username
Telnet Username
Telnet Password
Enable Password
SNMP Port
IP Address is required, the others are optional.
Type is a case-insensitive string; you can [view a list of device types](#).

[Download a sample file](#) or see the example below:
IP Address,SNMP Community String,Name,Type,Auth Password,SNMPv3 Auth Protocol,Privacy Password,SNMPv3 Privacy Protocol,SNMPv3 Username,Telnet Username,Telnet Password,Enable Password,SNMP Port
10.34.64.163,private,switch1.example.com,Router/Switch,nonradiance,md5,privacy123,aes,sv3user,telnetuser,telnetpwd,enable,161
10.172.97.172,private,switch2.example.com,router/switch,nonradiance,sha,privacy123,des,user
10.70.36.172,public,Cisco-WLC-4012-3,Cisco 4000 WLC,
10.46.111.48,,

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.

Changing the Mode to Monitor Only for New Instant Devices

A best practice for using Instant in AirWave is to change the mode for new devices to Monitor Only. This ensures that the configuration for the new devices does not get unintentionally overwritten and is a consistent behavior and practice throughout AirWave.

1. Navigate to **AP/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. Select the **Modify Devices** (pencil) icon, and select all devices.
4. Click the **Device Actions** drop-down list and select **Management Level**.
5. Select **Monitor Only + Firmware Upgrades**.
6. You can apply the changes immediately or schedule the change to be applied later.

Figure 8: *Changing the mode to Monitor Only*

Device Actions:

Management Level

Monitor Only + Firmware Upgrades

Manage Read/Write

Default View: Devices

[Total Row Count: 75]

| | DEVICE | STATUS | CONFIGURATION | CONTROLLER | FOLDER | GROUP | CLIENTS | USAG |
|-------------------------------------|-------------|--------|---------------|------------|--------|-------|---------|-------|
| <input checked="" type="checkbox"/> | 1344-1-AL01 | Up | Good | alpha-1 | Top | APs | 0 | 0 bps |
| <input checked="" type="checkbox"/> | 1344-1-AL52 | Up | Good | alpha-1 | Top | APs | 0 | 0 bps |
| <input checked="" type="checkbox"/> | 1344-1-AL54 | Up | Good | alpha-1 | Top | APs | 0 | 0 bps |

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 **APs/Devices > List** page, select **Modify Devices** (wrench icon), and then select the check box beside the virtual controllers that you want to edit.

Figure 9: *Select the VCs to update*

Device Actions:

Aruba Instant Virtual Controller Variables

Update

Default View: Devices

[Total Row Count: 94]

| | DEVICE | STATUS | CONFIGURATION | CONTROLLER | FOLDER | GROUP | CLIENTS | US |
|-------------------------------------|---------------------------------|--------|---------------|------------|--------|-------|---------|-----|
| <input checked="" type="checkbox"/> | Instant-00:0b:86:e1:00:00:00:00 | Up | Good | alpha-1 | Top | APs | 0 | 0 b |
| <input checked="" type="checkbox"/> | Instant-00:0c:85:e1:00:00:00:00 | Up | Good | alpha-1 | Top | APs | 0 | 0 b |
| <input checked="" type="checkbox"/> | Instant-00:0b:74:e1:00:00:00:00 | Up | Good | alpha-1 | Top | APs | 0 | 0 b |

2. Click the **Update** button next to the Aruba Instant Virtual Controller Variables field. This 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 22](#)
- ["Bulk Editing of Multiple Virtual Controllers" on page 23](#)
- ["Using Custom Variables" on page 23](#)
- ["Applying Changes" on page 24](#)

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 10: Change the Individual VC Names

custom_variable_1 ▾ Enter a Value Apply Please select one or more VCs to apply this setting.

1-1 ▾ of 1 Virtual Controllers Page 1 ▾ of 1 Choose columns

| | HOSTNAME ▴ | IP_ADDRESS | CLOCK_TIMEZONE | RADIUS_SERVER_IP |
|--------------------------|------------------|------------|----------------|------------------|
| <input type="checkbox"/> | Instant-test-123 | 10.1.1.91 | none 00 00 ▾ | 172.21.18.170 |

1-1 ▾ of 1 Virtual Controllers Page 1 ▾ of 1

Select All - Unselect All

Save Cancel

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 11.](#))
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.



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

Figure 11: Change the Timezone variable

clock_timezone 2 ▾ Pacific-Time UTC-08 3 Apply Please select one or more VCs to

1-2 ▾ of 2 Virtual Controllers Page 1 ▾ of 1 Choose columns Choose columns for roles

| | HOSTNAME ▴ | CLOCK_TIMEZONE | IP_ADDRESS |
|-------------------------------------|------------------|----------------|------------|
| <input checked="" type="checkbox"/> | Instant-test-123 | none 00 00 ▾ | 10.1.1.91 |
| <input checked="" type="checkbox"/> | Store-00002 | none 00 00 ▾ | 10.4.12.16 |

1-2 ▾ of 2 Virtual Controllers Page 1 ▾ of 1

Select All - Unselect All

Save Cancel

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 VC. 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 VC, 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 VCs 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**.



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 permit
wlan ssid-profile 0ttt
type employee
ssid 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 12: Entering a custom variable (cropped)

| HOSTNAME | CLOCK_TIMEZONE | IP_ADDRESS | CUSTOM_VARIABLE_1 |
|--|--------------------|------------|--|
| <input checked="" type="checkbox"/> Instant-test-123 | Pacific-Time UTC-8 | | wlan access-rule 0ttt rule any any match |
| <input checked="" type="checkbox"/> Store-0002 | Pacific-Time UTC-8 | | |

Applying Changes

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



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.

Confirm changes:

Group "test" Template "Aruba Instant Virtual Controller - 6.4.3.4-4.2.1.0"

Removed

Added wlan ssid-profile Test

Added enable

Added type guest

Added essid Test

Added opmode opensystem

Added max-authentication-failures 0

Added vlan 20

Added auth-server Test-Server-Primary

Added set-role-pre-auth Pre-Auth-Allow

Added set-role Aruba-User-Role contains Ad-Supported Ad-Supported

Added set-role Aruba-User-Role contains subscriber subscriber

Added set-role Aruba-User-Role contains social social

Added set-role Aruba-User-Role contains Active-Warrant Active-Warrant

Added rf-band all

Added captive-portal external profile Test-Captive-Portal

Added dtim-period 1

Added inactivity-timeout 300

Added broadcast-filter all

Added radius-accounting

Added radius-interim-accounting-interval 5

Added g-min-tx-rate 18

Added a-min-tx-rate 18

Added dmo-channel-utilization-threshold 90

Added local-probe-reg-thresh 10

Added max-clients-threshold 64

Template:

Removed

Added wlan ssid-profile Test

Added enable

Added type guest

Added essid Test

Added opmode opensystem

Added max-authentication-failures 0

Added vlan 20

Added auth-server Test-Server-Primary

Added set-role-pre-auth Pre-Auth-Allow

Added set-role Aruba-User-Role contains Ad-Supported Ad-Supported

Added set-role Aruba-User-Role contains subscriber subscriber

Added set-role Aruba-User-Role contains social social

Added set-role Aruba-User-Role contains Active-Warrant Active-Warrant

Added rf-band all

Added captive-portal external profile Test-Captive-Portal

Added dtim-period 1

Added inactivity-timeout 300

Added broadcast-filter all

Added radius-accounting

Added radius-interim-accounting-interval 5

Added g-min-tx-rate 18

Added a-min-tx-rate 18

Added dmo-channel-utilization-threshold 90

Added local-probe-reg-thresh 10

Added max-clients-threshold 64

Apply Changes Now

Cancel

Scheduling Options

Occurs:

One Time

Specify numeric dates with optional 24-hour times (like 7/4/2003 or 2003-07-04 for July 4th, 2003, or 7/4/2003 13:00 for July 4th, 2003 at 1:00 PM.), or specify relative times (like tomorrow at noon or next tuesday at 4am). Other input formats may be accepted.

Current Local Time:

January 22, 2016 3:07 pm CST

Desired Start Date/Time:

Enter a Value

Schedule

Instant Config provides an alternate method for configuring and managing devices running Instant 3.2 to Instant 4.2. After Instant devices 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**, **APs/Devices > Manage**, and **APs/Devices > Audit** 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 4.2. 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 Config" on page 26
- "Importing Devices for Instant Config" on page 28
- "The Instant Config UI" on page 29
- "Where to Get Additional Information" on page 33

Enabling Instant Config

The **Groups > Instant Config** pages are not available by default. Perform the following steps to enable this feature.

1. On the **Groups > List** page, click **Add**.
2. Name the group, and click **Add**.
3. On the **Groups > Basic** page, scroll down to the Group Display Options section. Ensure that the **Show Device Settings** for option includes Instant devices. Instant Config is only available for groups that include Instant devices. The following image specifies to include only selected Instant devices.

Figure 14: *Include Instant devices*

The screenshot shows the "Group Display Options" section of the AirWave GUI. It features a "Show Device Settings for:" label followed by a dropdown menu currently set to "Selected device types". Below this is a link "Select devices in this group". Underneath, there is a grid of checkboxes for various device types. The checked items are "Alcatel-Lucent Instant" and "Aruba Instant".

| Select devices in this group | |
|--|---|
| <input type="checkbox"/> 3Com | <input type="checkbox"/> Alcatel-Lucent |
| <input checked="" type="checkbox"/> Alcatel-Lucent Instant | <input type="checkbox"/> Alcatel-Lucent Switch |
| <input type="checkbox"/> Arista | <input type="checkbox"/> Aruba |
| <input type="checkbox"/> Aruba AirMesh | <input checked="" type="checkbox"/> Aruba Instant |

4. Save and apply changes. Upon completion, you are directed to the **Groups > Monitor** page. Navigate back to the **Groups > Basic** page.
5. In the Aruba Instant section, specify **Yes** for the **Enable Instant GUI Config** option.
6. Click **Save and Apply**.

Figure 15: Enable Instant Config

Aruba Instant

| | |
|----------------------------|---|
| Enable Instant GUI Config: | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| HTTPS Timeout (1-30 min): | <input type="text" value="5"/> |
| CA Cert: | <div>-- None --</div> |

Buttons and Icons in Instant Config

Table 2 describes the buttons and icons that are available on the Instant Config pages.

Table 2: Instant Config Buttons and Icons

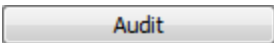

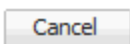










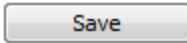
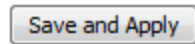

| Function | Image | Description |
|------------------------------------|---|--|
| Audit |  | On the AirWave > Config Archive page for a device, select this to audit a device's configuration. |
| Auditing or applying configuration |  | Indicates that the device is undergoing an audit or that a new configuration is being applied. |
| Cancel |  | Cancels the current edit or task. |
| Delete |  | Deletes a network. |
| Down |  | Indicates a device is down. |
| Employee Usage |  | Indicates the network is used for Employee data. |
| Filter (Funnel icon) |  | Filters a list by values of the selected column. To reset all filters in all columns, click the Reset filters link at the bottom of the table. |
| Guest Usage |  | Indicates that the network is used for Guest data. This is normally used when captive portal is enforced. |
| Mismatched |  | Indicates a mismatched device configuration. |

Table 2: *Instant Config Buttons and Icons (Continued)*

| Function | Image | Description |
|--------------|---|---|
| Multi-Edit |  | Used with text entry fields to perform an edit across multiple devices. This option is only available when the Instant Config focus is the Group. It is not available when viewing devices or networks. |
| Note |  | Drag a note from the menu bar onto the configuration page. Notes that are placed on configuration pages can be used to indicate why you changed an option or setting. |
| Override |  | Indicates that an override exists. Navigate to the AirWave > Overrides page for the selected device to view the override(s). |
| Policy Error |  | Indicates that AirWave is unable to push or compare configurations because the policy version does not match the firmware version. |
| Save |  | Saves the information on the current page in the AirWave database. |
| Save & Apply |  | Saves changes to AirWave's database and applies all changes. NOTE: Instant Config does not currently allow users to apply individual edits. After you click Save and Apply , changes made on other pages that have not been canceled will also be applied. |
| Voice Usage |  | Indicates that the network is used for voice traffic. This is normally used when all traffic must be prioritized. |

Importing Devices for Instant Config

The section "[Enabling Instant Config](#)" on [page 26](#) describes how to set up an Instant Config group. Devices that are added to this group can be managed using Instant Config.



When importing Instant devices in bulk to a new group, AirWave randomly selects the first device that it encounters and uses that device as the "golden" configuration. The configuration is used across all other Instant networks. As a recommended best practice, select a device that can be used as the golden configuration, and add it to the group before adding any others. New devices that are added after the golden configuration device will include the configuration from that golden device.

Add Newly Discovered Devices to a Group

1. Select the **New Devices** link in the header to launch the **APs/Devices > New** page where information about all newly discovered devices is displayed ([Figure 16](#)). You might launch a different page if you specified a different location while defining a scan set.

The information on this page includes the related controller (when known/applicable), the device type (including vendor and model), the LAN MAC Address, the IP address, and the date/time of discovery. See [Figure 16](#).

Figure 16: *APs/Devices > New Page*

To discover more devices, visit the [Discover](#) page.

Add Selected Devices ▾ Group: Access Points ▾ Folder: Top (0 Clients) ▾ Management Level: Monitor Only + Firmware Upgrades ▾ [Add](#)

Default View: New Devices:Configuration ▾

| <input type="checkbox"/> | DEVICE | TYPE ▴▾ | LAN MAC ADDRESS | IP ADDRESS | DISCOVERED |
|--------------------------|--------------------------|-----------------|-------------------|-------------|------------------|
| <input type="checkbox"/> | corvina-dev-1 | Aruba S3500-24P | 00:00:00:00:00:00 | 10.51.3.205 | 7/23/14, 9:32 AM |
| <input type="checkbox"/> | Aruba-S3500-25SP-1stFlr3 | Aruba S3500-24T | 00:0B:86:6A:62:00 | 10.51.3.55 | 7/23/14, 9:32 AM |
| <input type="checkbox"/> | ArubaS3500-48P | Aruba S3500-48P | 00:0B:86:6C:1E:00 | 10.51.3.57 | 7/23/14, 9:32 AM |

2. Select the check box beside the device or devices that you want to add.
3. Use the drop-down lists to select the **Group** and **Folder** to which the devices will be added. The default group appears at the top of the Group list.
4. Select **Add** when you are done. At this point, you can go to the **APs/Devices > List** page and select the folder that contains the newly added devices. This enables you to verify that the devices have been properly assigned.



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

The Instant Config UI

The **Groups > Instant Config** feature allows network administrators to configure Instant access points on the network remotely through AirWave. The flow of pages within the Instant Config UI closely resemble the pages available in Aruba Instant.



When performing Instant configurations within AirWave, be sure to have a copy of the *Aruba Instant User Guide* available.

Figure 17: *Groups > Instant Config*

+ IGC

Networks

Access Points

Settings

IDS

VPN

RF

Firewall

Network List [Help](#)

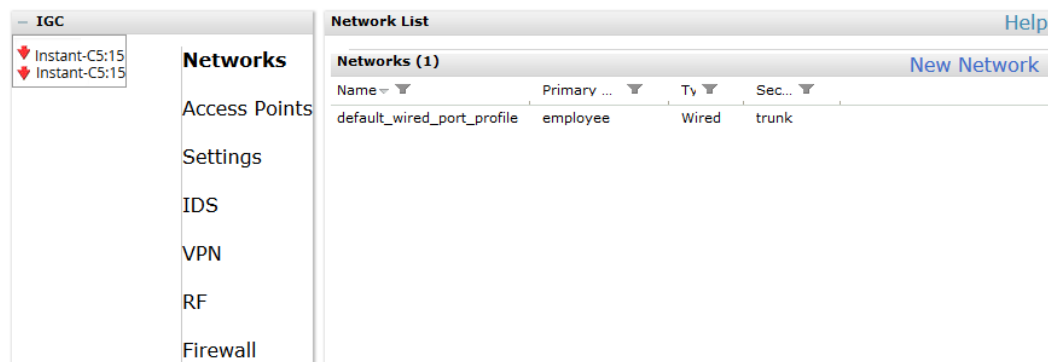
Networks (1) [New Network](#)

| Name ▾ ▾ | Primary ... ▾ | Ty ▾ | Sec... ▾ |
|----------------------------|---------------|-------|----------|
| default_wired_port_profile | employee | Wired | trunk |

Group Focus

The Instant Config page opens in the Group focus. [Figure 18](#) shows a group named "IGC." Click the group name to view the available devices.

Figure 18: Group Focus



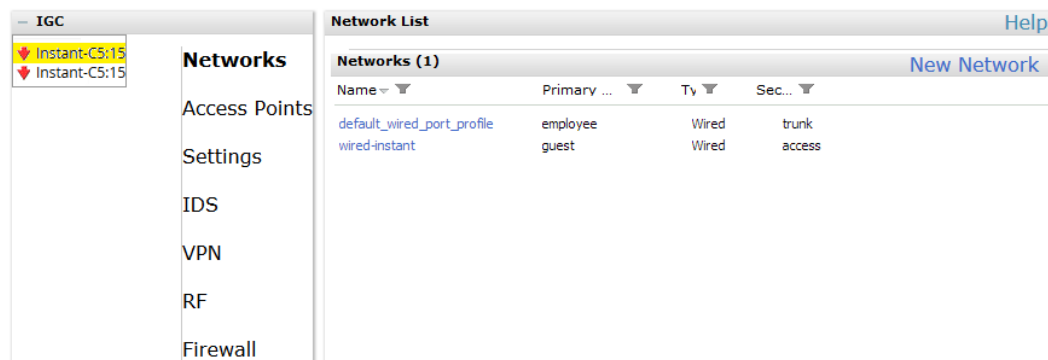
Group focus is used to changes settings and apply those changes to all devices within the group.

Virtual Controller Focus

Virtual Controller focus is used to change settings for selected devices. From this page, you can add and configure wired and wireless networks. Select a device from the Group list to change to Device focus. Navigation at the top of the page indicates the currently selected device. The selected device is also highlighted in the list of Devices.

In [Figure 19](#), the Instant-C5:15:F6 device is selected. You can see that the device currently has two networks configured.

Figure 19: Device Focus

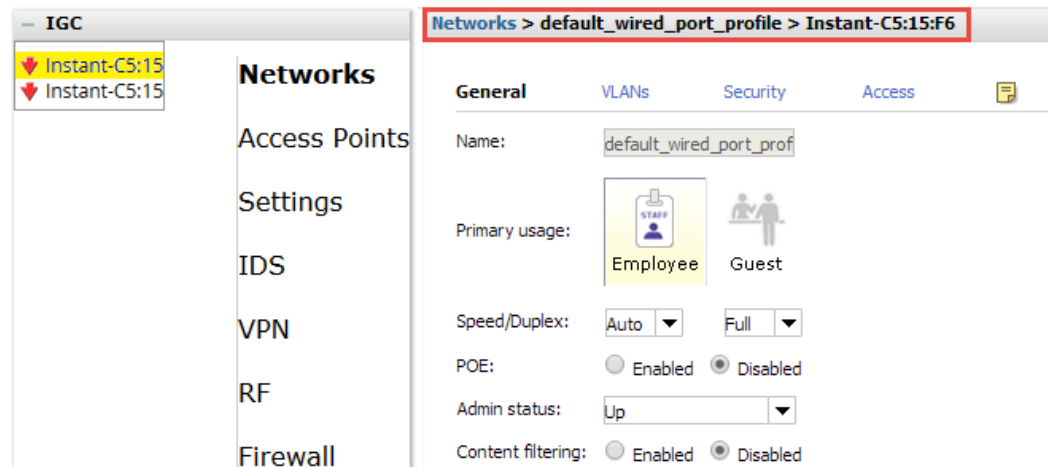


Network Focus

Network focus is used to configure settings for the networks available on each device, for example, the authentication mode, access point radio settings, VPN settings, etc. From this page, you can also add and delete wired and wireless networks.

[Figure 20](#) shows the General settings for the "default_wired_port_profile" network on the Instant-C5:15:F6 device.

Figure 20: Network Focus



Instant Config > AirWave

The IGC's AirWave menu 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.

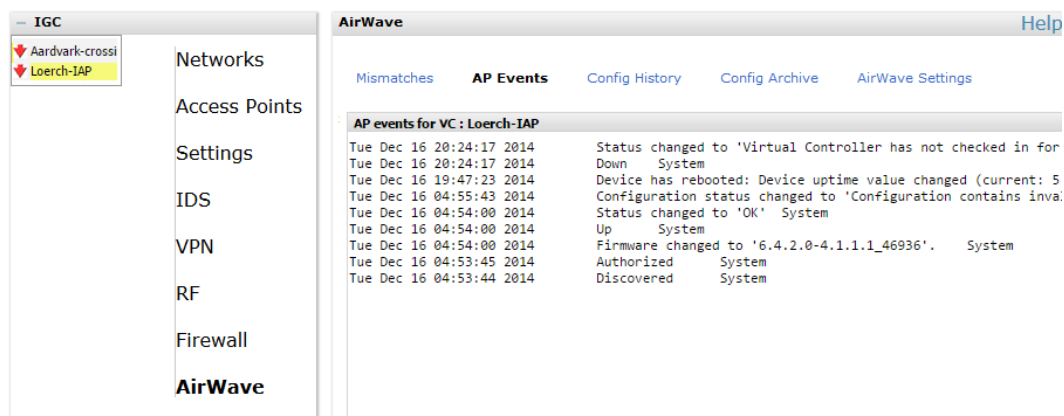
Mismatches

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 35.

AP Events

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

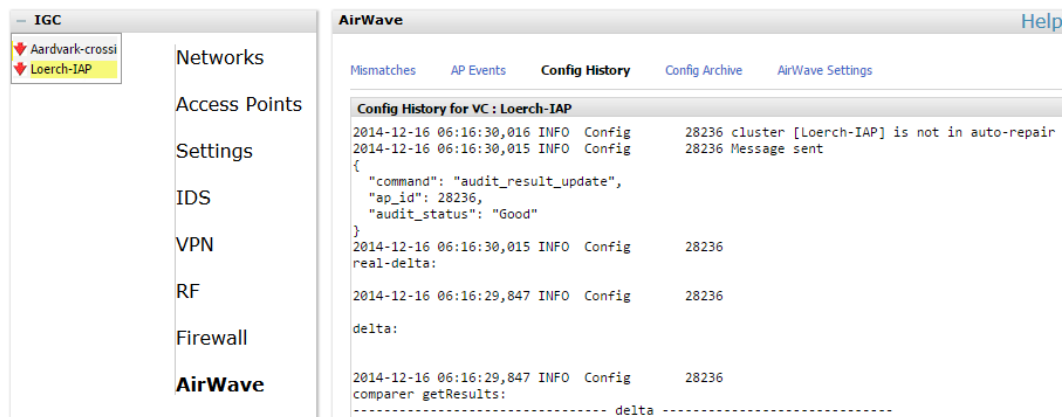
Figure 21: AirWave > AP Events



Config History

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

Figure 22: 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.

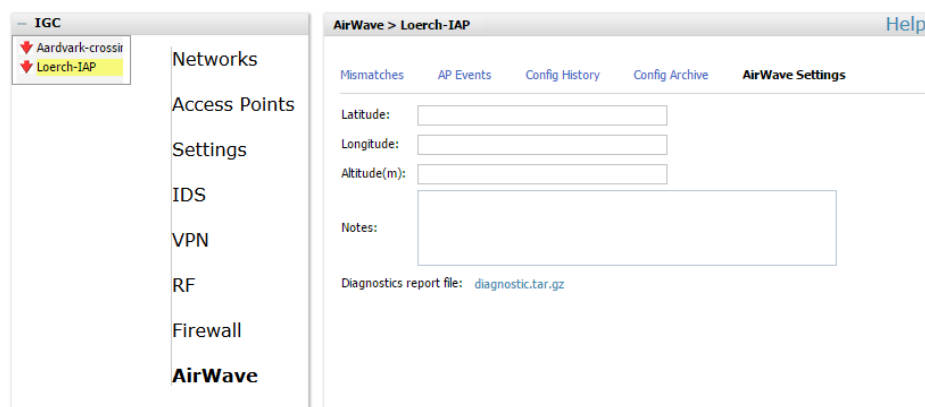
AirWave Settings

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 23: AirWave Settings (VC Selected)



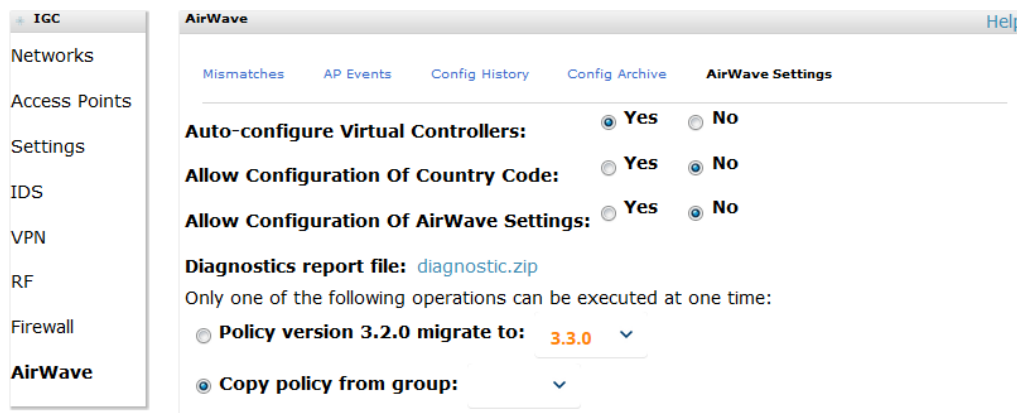
Without A Virtual Controller Specified

This page contains a number of 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 they 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 descibed 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 24: 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 6.4.3.0-4.2 User Guide*
- *Aruba Instant 6.4.3.0-4.2 User Guide*
- *Aruba Instant 6.4.3.0-4.2 User Guide*
- *AirWave 8.2 Release Notes*

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

- ["Resolving Mismatches" on page 34](#)
- ["Enabling the IAP Role" on page 36](#)
- ["Monitoring Devices" on page 36](#)
- ["Run Commands" on page 37](#)

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" on page 34](#)
- ["Resolving Mismatches when Instant Config is Enabled" on page 35](#)

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 25: *APs/Devices > Audit page*

Device Configuration of Instant-C4:43:8D in group APs in folder Top

This Device is in monitor-only mode.

Configuration read from device at 1/17/2016 4:24 AM PST
Configuration: Unknown
(Settings not yet read from device)

Audit Audit the device's current configuration.

[Show Archived Device Configuration](#)

[View Telnet/SSH Command log](#)

[Show only mismatched settings](#)

Customize Choose settings to ignore during configuration audits.

| DEVICE SETTINGS | |
|-----------------|---|
| Template: | |
| Actual | per-ap-settings d8:c7:c8:c4:01:95 |
| Actual | g-channel 1 0 |
| Actual | g-external-antenna 0 |
| Actual | hostname "iap100" |
| Actual | ip-address 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 "" |
| Actual | swarm-mode cluster |
| Actual | uplink-vlan 0 |
| Actual | wifi0-mode access |

Perform the following steps to resolve the mismatch.

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



The **APs/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.



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.



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

Figure 26: Viewing mismatches in Instant Config

The screenshot shows the AirWave web interface. On the left is a sidebar with a navigation menu including 'Networks', 'Access Points', 'Settings', 'IDS', 'VPN', 'RF', 'Firewall', and 'AirWave'. The 'AirWave' option is selected. The main content area is titled 'AirWave > Branch-106' and has a 'Help' link. Below the title are tabs for 'Mismatches', 'Overrides', 'AP Events', 'Config History', 'Config Archive', and 'AirWave Settings'. The 'Mismatches' tab is active, showing a list of configuration items for 'VC: Branch-106'. The list includes items like 'per-ap-settings', 'hostname', 'ip-address', 'swarm-mode', 'wifi0-mode', 'wifil-mode', 'a-channel', 'g-channel', 'uplink-vlan', 'a-external-antenna', 'g-external-antenna', 'wlan access-rule', and 'wlan ssid-profile'. Each item has a value next to it. At the bottom right of the list is a red box containing the text 'Apply All'.

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 27](#).

Figure 27: Enable Admin User Roles in **AMP Setup > Roles**

| Role | |
|---------------------------------------|---|
| Name: | Acme Admin |
| Enabled: | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| Type: | AP/Device Manager |
| AP/Device Access Level: | Manage (Read/Write) |
| Top Folder: | Sunnyvale |
| Allow authorization of APs/Devices: | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| RAPIDS: | Read/Write |
| VisualRF: | Read/Write |
| Aruba Controller Single Sign-on Role: | Disabled |

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



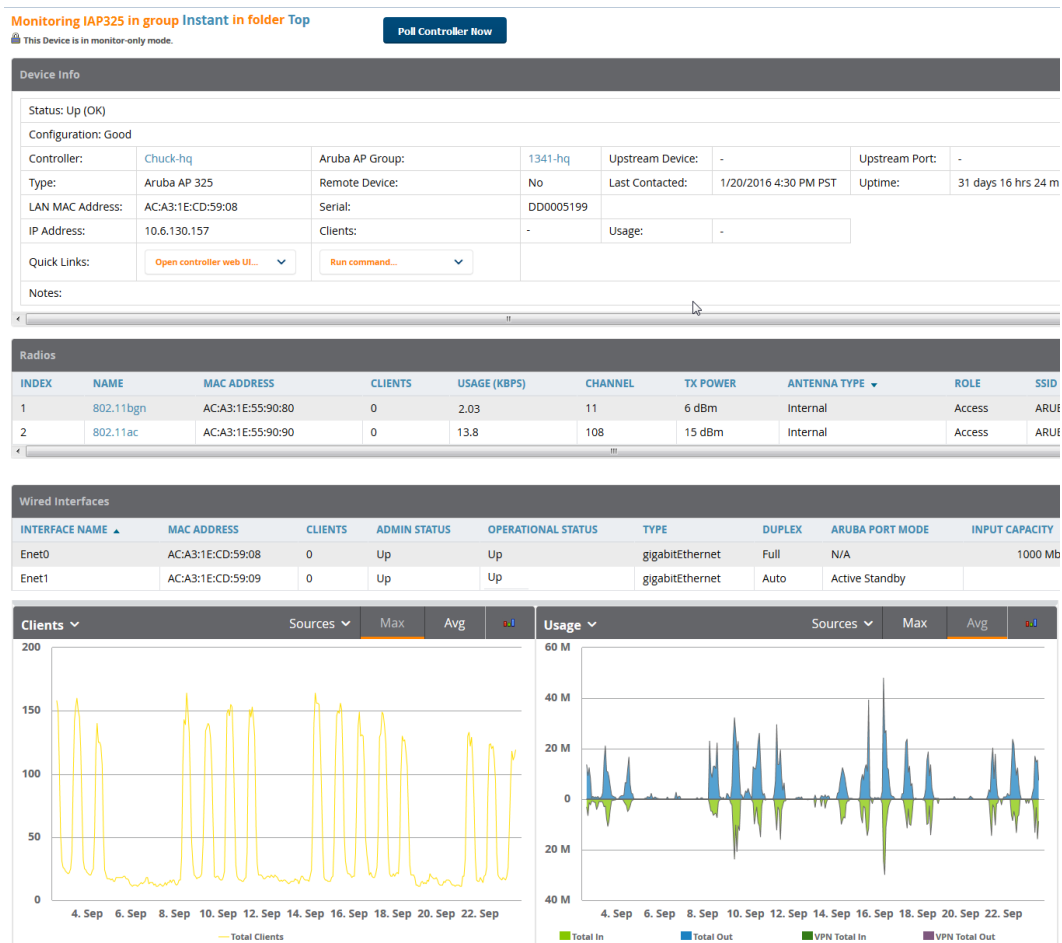
The auto-created template is most useful if the first Virtual Controller for the top-level Organization String is fully configured on-site *before* it is pointed at AirWave in the Virtual Controller's UI.

3. Evaluate, approve, or ignore incoming Virtual Controllers with a different top level Organization String and/or Shared Secret in the **APs/Devices > New** list. Subsequent IAPs 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 **APs/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 28: Monitoring Radios



Run Commands

If you are running a minimum of IAP 3.2, the AirWave **APs/Devices > Monitor** page provides a set of quick links that allow you to specify a command you can run from the virtual controller or from the AP. On the virtual controller, you also have option to run commands for all APs as well as for the current virtual controller.



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 29: Run Commands

Monitoring test vc in group test in folder Top > regression

Device Info

Status: Up (OK)

Configuration: Verifying

| | | | | | | | |
|------------------|----------------------------------|------------------|-----------------------|----------|--------------|--------|---|
| Firmware: | 6.4.3.4-4.2.1.0_52654 | Upstream Port: | - | | | | |
| Upstream Device: | - | Controller Role: | - | | | | |
| Type: | Aruba Instant Virtual Controller | Last Contacted: | 1/22/2016 3:16 PM CST | Uptime: | 3 hrs 0 mins | | |
| LAN MAC Address: | - | Location: | "sys location" | | | | |
| IP Address: | 10.65.1.218 | APs: | 1 | Clients: | 0 | Usage: | - |
| VPN Sessions: | 0 | VPN Usage: | - | | | | |

Run command for VC...

VC 802.1x Certificate

VC About

VC Active Configuration

VC AirGroup Service

VC AirGroup Status

VC Allowed AP Table

VC AMP Current State Data

VC AMP Current Stats Data

VC AMP Data Sent

VC AMP Events Pending

VC AMP Last Configuration Received

VC AMP Single Sign-on Key

VC Application Services

VC Auth-Survivability Cache

VC Client List

VC DHCP Option 43 Received

VC Global Alerts

VC Global Statistics

VC IDS AP List

VC IDS Client List

VC Internal RADIUS Server Configuration

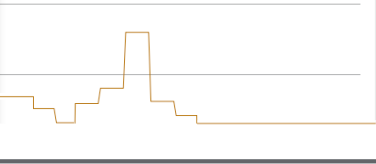
Run command for all

Sources

Max

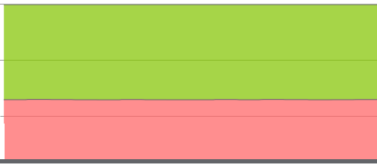
Avg

all



Memory Utilization

Sources



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 **APs/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 **APs/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.