

Aruba Instant in AirWave 7.6

Deployment Guide

About this Document

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

- ["Overview of Aruba Instant" on page 1](#)
- ["Using Aruba Instant with AirWave" on page 1](#)
- ["Setting up Aruba Instant" on page 2](#)
- ["Remaining Manual Admin Tasks in AirWave" on page 5](#)
- ["Adding Additional Instant APs to AirWave" on page 6](#)
- ["Changing the Mode to Monitor Only for New Instant Devices" on page 7](#)
- ["AMP Pages with Instant-Specific Features " on page 8](#)
- ["Other Available Features" on page 8](#)
- ["Optional Tasks" on page 13](#)
- ["Best Practices" on page 15](#)
- ["Known Issues with the Aruba Instant Integration with AirWave" on page 16](#)

Overview of Aruba Instant

Aruba Instant is a system of access points (IAP-92AP, IAP-93, IAP-105, AP-130, AP-134, and AP-135) per Layer 2 subnet. Instant IAPs are controlled by a single IAP that serves a dual role as a primary Virtual Controller, 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- and device-based policy enforcement, rogue detection, and Adaptive Radio Management (ARM).

Using Aruba Instant with AirWave

AirWave can be used to provision and manage a multi-site deployment of 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 and also give the administrator 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 each have an Aruba Instant Virtual Controller and IAPs, AirWave serves as a centralized management console. AMP 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 Aruba Instant systems into AMP is unique from the setup of any other device class due to the following considerations:

- **Discovery:** AMP does not discover Aruba Instant devices via scanning (SNMP or HTTP) the network. Each Aruba Instant deployment will automatically check-in to the AMP configured within the IAP's user interface. The first Virtual Controller for an organization will automatically appear as a new device in AMP. 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 AMP 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 AMP. Unlike the traditional infrastructure of a physical controller and thin APs, Aruba Instant automates many tedious steps of developing a complex hierarchical structure of folders, config groups, templates, admin users, and admin roles for Aruba Instant.
- **Communication via HTTPS:** Because Aruba Instant devices may be deployed behind NAT-enabled firewalls, Virtual Controllers push data to AMP via HTTPS. AMP initiates no connections to Aruba 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, AMP will list 10 Aruba Instant IAPs and one Aruba Instant Virtual Controller. You can identify the IAP acting as the Virtual Controller by their identical LAN MAC addresses in **APs/Devices > List** pages, Device Inventory reports, and any other AMP 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 *Aruba Instant Data Sheet* for full operational and regulatory specifications, hardware capabilities, antenna plots, and radio details.

Setting up Aruba Instant

You can set up Aruba Instant in one of three ways:

- Manually. See ["Setting up Aruba Instant Manually" on page 3](#).
- Automatically (through DHCP). See ["Setting up Aruba Instant Automatically" on page 4](#).
- Using Aruba Activate. Refer to the documentation that accompanies Aruba Activate for detailed information.

The automatic setup is most suited for a multi-site Instant deployment. Both options are summarized here, but refer to the *Aruba Instant Quick Start Guide*, the *Aruba Instant Professional Installation Guide*, the *IAP-105 Wireless Access Point Installation Guide*, and the *IAP-92 and IAP-93 Wireless Access Point Installation Guide* 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 AMP.

An AMP administrator sends an Organization String and Shared Secret key along with AMP's IP address to the on-site installer. The AMP admin later validates the first Virtual Controller's Organization String and its Shared Secret when it appears in the **APs/Devices > New** list. The administrator also enables user roles to administer the Aruba Instant systems, makes any other changes in AMP as necessary.



The first Instant network that is added to AMP 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 7.6 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 Aruba Instant Manually

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

Creating your Organization String

The Organization String is a set of colon-separated strings created by the AMP 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 AMP:

- AMP Role: Org Admin (initially disabled)
- AMP User: Org Admin (assigned to the role Org Admin)
- Folder: Org (under the Top folder in AMP)
- 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

The Shared Key

The Shared key is used by the administrator to manually authorize the first Virtual Controller for an organization that appears in the **APs/Devices > New** page in AMP. Any string is acceptable, but this string must be the same for all devices in your organization.



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.

At this point, the admin in our example should send the Organization String, Shared Secret key, and AMP IP address to the on-site installers setting up Aruba Instant hardware inside the storefronts.

Entering the Organization String and AMP 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 AMP IP address, and the Shared Secret key, as shown in [Figure 1](#). Perform the following steps to set up AMP 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.

Figure 1 *Aruba Instant > Settings page.*

The screenshot shows the 'Settings' window with the 'Admin' tab selected. The 'Local' section has 'Authentication' set to 'Internal', 'Username' as 'admin', and 'Password' and 'Retype' fields with masked characters. The 'AirWave' section has empty fields for 'Organization', 'AirWave IP', 'AirWave backup IP', 'Shared key', and 'Retype'. At the bottom, there is a 'Hide advanced options' link and 'OK' and 'Cancel' buttons.

3. Locate the AirWave section on the **Admin** tab.
4. Enter the Organization string, the AirWave IP address, and the Shared key.
5. Click **OK** when you are finished.

Setting up Aruba Instant Automatically

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

The Aruba Instant Virtual Controller initiates DHCP request with the DHCP option 60 string 'ArubaInstant.' If the DHCP server is configured to recognize this option 60 string, it will return an option 43 string containing the organization, AMP 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 AMP information in the option 43 will be used to connect to AMP, if AMP 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-Pool1
  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 AMP:

- 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.

Remaining Manual Admin Tasks in AirWave

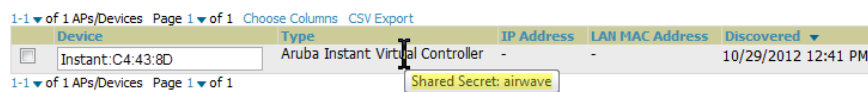
Once the setup is complete, what remains is to verify the shared secret and add the device.

- "Verifying the Shared Secret " on page 5
- "Adding the First Instant Device to AirWave" on page 5

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 AMP, as shown in [Figure 2](#).

Figure 2 Mouse over the Aruba Instant Type column to view the Shared Secret



Device	Type	IP Address	LAN MAC Address	Discovered
Instant-C4:43:8D	Aruba Instant Virtual Controller	-	-	10/29/2012 12:41 PM

Shared Secret: airwave

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

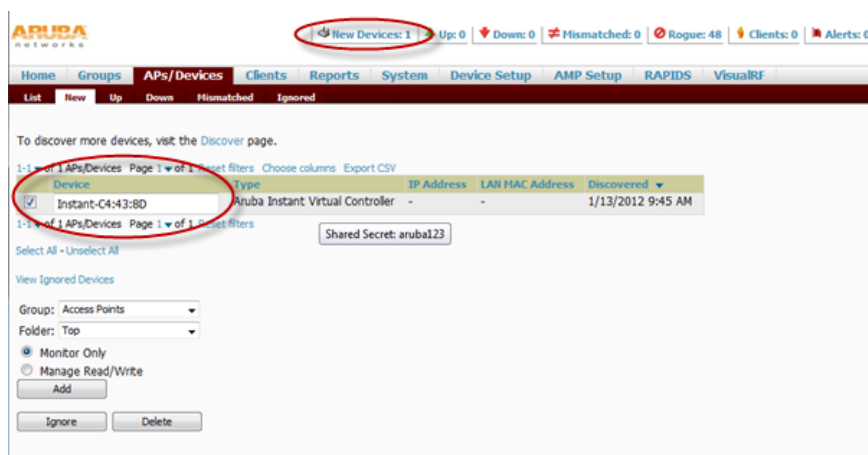
With an Organization specified, you do not have to select any Group or Folder from the drop-down menus on the **APs/Devices > New** page. In fact, if you do change the Group/Folder drop-down menus, all Organization-specified Virtual Controllers will ignore these values and will use the folder/group values 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.



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 appear as a new device in AirWave. As shown, this virtual controller is added in **Monitor Only** mode.

Figure 3 A new Instant device in AirWave



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.

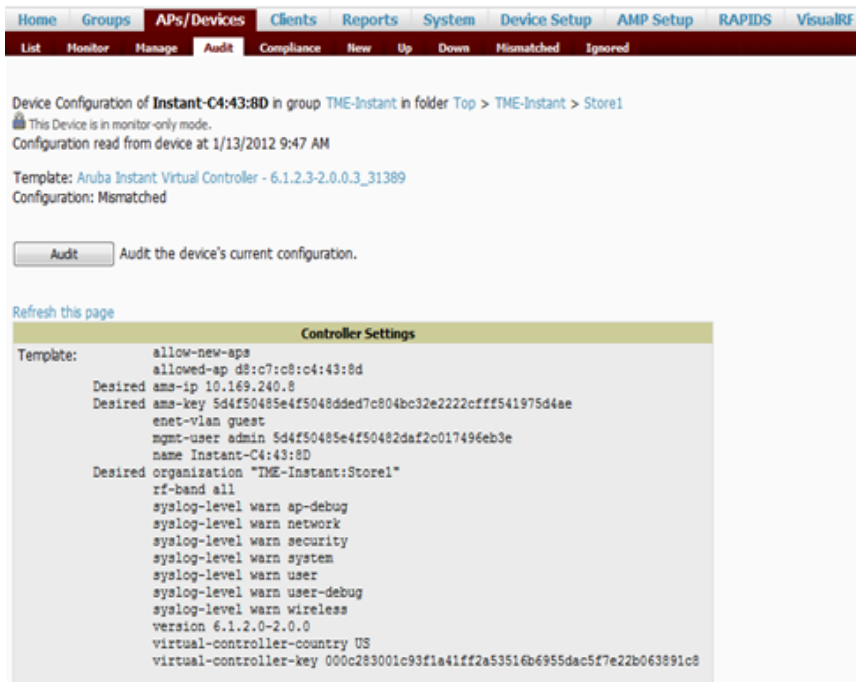
2. Select **Apply Changes Now** to add the Instant device to the group.

Resolving Mismatches

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).

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 4 *Audit page*



Perform the following steps to resolve the mismatch.

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

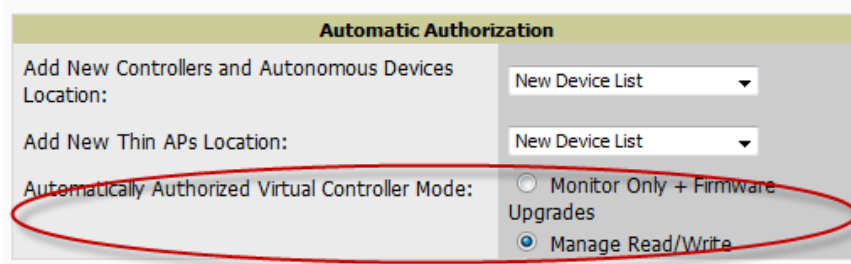


This is the same process for any configuration change sync that is done in future.

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 5 Setting devices to Manage Read/Write mode

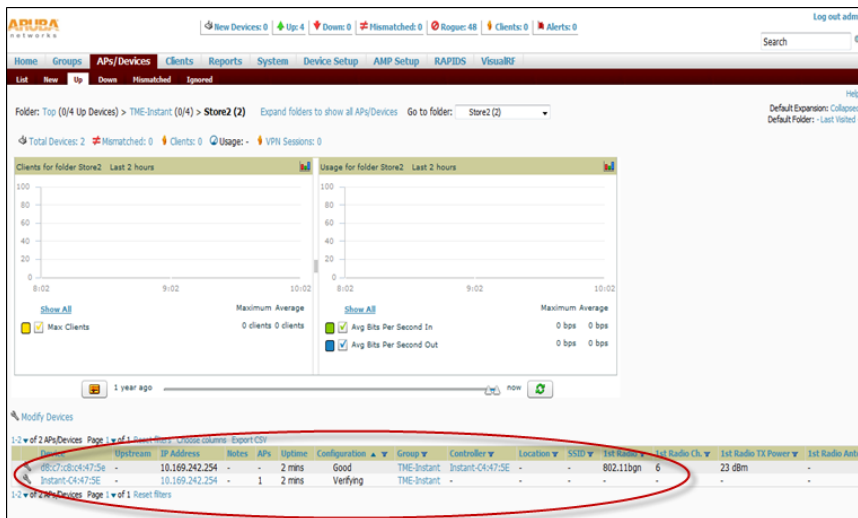


When the second Instant contacts AirWave using the DHCP server options as described previously, and that second Instant device has the same Shared key, it shows up on AirWave as shown below. Because the devices are in **Manage Read/Write** mode, there is no need for manual intervention to provision these 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 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.

Figure 6 Adding an additional Instant device to 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**.

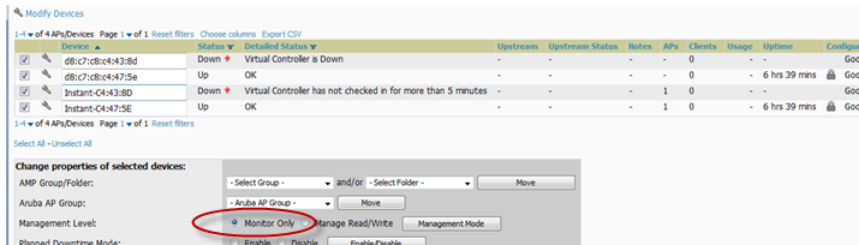
Changing the Mode to Monitor Only for New Instant Devices

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** (wrench) icon, and select all devices.
4. Select the **Monitor Only** radio button.

- Click the **Management Mode** button. This opens the Confirm Changes page. You can apply the changes now or schedule the change to be applied later.

Figure 7 Changing the mode to Monitor Only



AMP Pages with Instant-Specific Features

The following is a summary of AMP 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 AMP.
- APs/Devices > List:** The Virtual Controller is listed as an additional device, even though it is part of the existing set of IAPs. You can identify the IAP acting as the Virtual Controller by their identical LAN MAC addresses.
- 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**. 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 CPU Utilization, Channel Utilization, Bandwidth, Power, and MAC/Phy Error statistics.
- RAPIDS:** Because Aruba Instant does not support mitigation or high-level rogue reporting, it does not synchronize classification. All rogue devices are reported and stored in the AMP for evaluation based on high-level rule sets. Aruba 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:** Aruba Instant Virtual Controllers appear as a separate device in the Device Inventory Report and most other reports that list devices.



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

Other Available Features

Additional Instant features that are supported in AirWave include an editor for common variables, monitoring features, CLI commands, and firmware image management.

- "Editing Variables " on page 9
- "Monitoring Features" on page 12
- "Running Commands" on page 12
- "Firmware Image Management" on page 13
- "Intrusion Detection System" on page 13

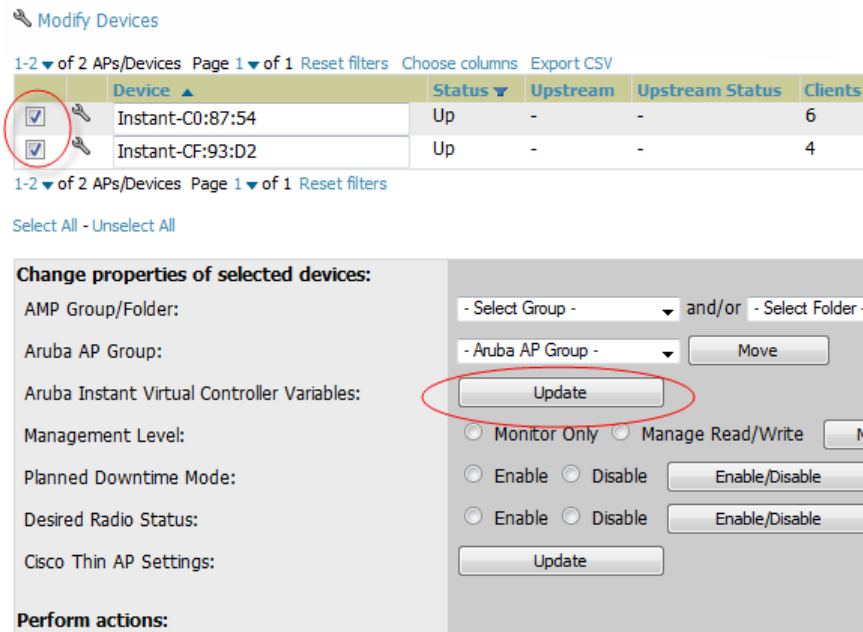
Editing Variables

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 8 *Select the VCs to update*



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 9
- "Bulk Editing on Multiple Virtual Controllers" on page 10
- "Using Custom Variables" on page 11
- "Applying Changes" on page 11

Editing Individual Virtual Controller Values

After you click **Update**, the Variable Edit screen that displays includes two sections. The lower section includes editable fields. Enter values or select options directly in these fields to make changes on individual controllers. In the example below, the VC names are changed from Instant-C0:87:54 and Instant-CF:93:D2 to Store-00001 and Store-00002 respectively.

Figure 9 *Change the Individual VC Names*

The screenshot shows the 'Variable Edit' page with a dark red header containing tabs: List, New, Up, Down, Mismatched, and Ignored. Below the header, a dropdown menu is set to 'custom_variable_10', followed by an empty text input field and a disabled 'Apply' button. A message 'Please select one or more' is visible. Below this, a table lists two virtual controllers. The table has columns for 'hostname', 'clock_timezone', and 'ip_address'. The first row shows 'Store-00001' with 'none 00 00' for the clock_timezone. The second row shows 'Store-00002' with 'none 00 00' for the clock_timezone. At the bottom, there are 'Save' and 'Cancel' buttons.

hostname	clock_timezone	ip_address
Store-00001	none 00 00	
Store-00002	none 00 00	

Bulk Editing on 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 9](#).)
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 10 *Change the Timezone variable*

The screenshot shows the 'Variable Edit' page with the 'List' tab selected. The dropdown menu is set to 'clock_timezone', the text input field contains 'Pacific-Time UTC-08', and the 'Apply' button is now enabled. A red box highlights the 'Apply' button and the text input field. Below the header, a table lists two virtual controllers. The table has columns for 'hostname', 'clock_timezone', and 'ip_address'. The first row shows 'Store-00001' with 'none 00 00' for the clock_timezone. The second row shows 'Store-00002' with 'none 00 00' for the clock_timezone. A red box highlights the check boxes in the first column of the table, with a red '1' next to it. At the bottom, there are 'Save' and 'Cancel' buttons.

hostname	clock_timezone	ip_address
<input checked="" type="checkbox"/> Store-00001	none 00 00	
<input checked="" type="checkbox"/> Store-00002	none 00 00	

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 8d072cdea5bcecleaae3cb597975951fbd7d7124120e3217
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 11 *Entering a custom variable (cropped)*

hostname	clock_timezone	ip_address	custom_variable_1
<input checked="" type="checkbox"/> Store-0001	Pacific-Time UTC-08		wlan access-rule 0ttt rule any any match any any permit
<input checked="" type="checkbox"/> Store-0002	Pacific-Time UTC-08		

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.

Figure 12 *Confirm Changes page*

Confirm changes:

Controller "Instant-C0:87:54"

Extra Device Commands #1 (empty string)

➔

wlan access-rule 0ttt
rule any any match any 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

Name

Instant-C0:87:54

➔

Store-00001

Timezone

none 00 00

➔

Pacific-Time UTC-08

Controller "Instant-CF:93:D2"

Name

Instant-CF:93:D2

➔

Store-00002

Timezone

none 00 00

➔

Pacific-Time UTC-08

Apply Changes Now

Cancel

Scheduling Options

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:

November 14, 2012 6:21 am CST

Desired Start Date/Time:

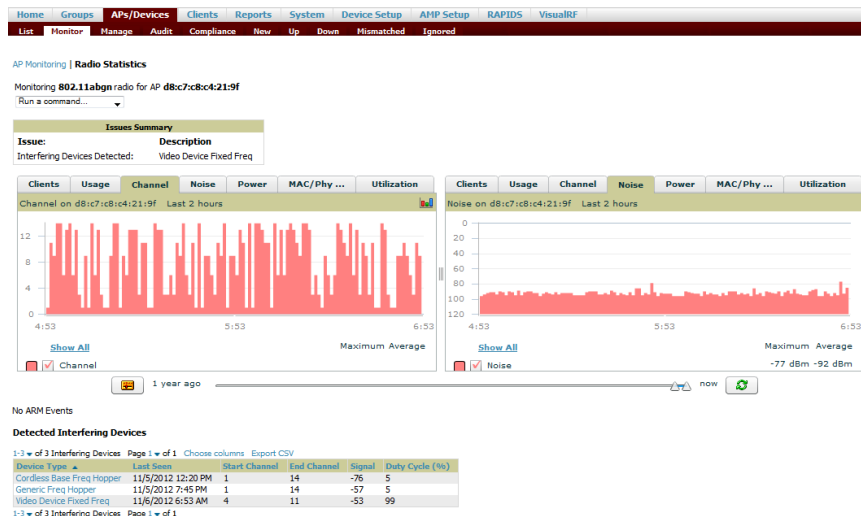
Schedule

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

Monitoring Features

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 13 *Monitoring Radios*



Running Commands

If you are running IAP 3.2, then AirWave provides a set of commands that you can run from the virtual controller and 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 14 *Running Commands*

Monitoring **Instant-C4:21:9F** in group **junyei** in folder **Top > junyei**
This Device is in monitor-only-with-firmware-upgrades mode.

Device Info	
Status:	Up (OK)
Configuration:	Mismatched (The settings on the device do not match the desired configuration)
Firmware:	6.1.3.4-3.1.0.0-arm_0
Upstream Device:	-
Upstream Port:	-
Controller Role:	-
Type:	Aruba Instant Virtual Controller
Last Contacted:	10/1/2012 2:
LAN MAC Address:	-
IP Address:	192.168.1.102
APs:	2

Run a command for virtual controller... Run a command for all APs

- show 1xcert
- show about
- show running-config
- show allowed-aps
- show app-services
- show alert global
- show stats global
- show users
- show radius-attributes
- show radius-servers support
- show configuration
- show snmp-configuration
- show ap debug airwave-config-received
- show ap debug airwave-events-pending
- show ap debug airwave-data-sent
- show ap debug airwave-state
- show ap debug airwave-stats
- show dhcpc-opts
- show opendns support

Usage on

Maximum Average

0 clients 0 clients

Firmware Image Management

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, AirWave allows you to upload firmware for each of the device types.

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.

Optional Tasks

Additional optional tasks include enabling an IAP role for location-specific access and updating the Instant template.

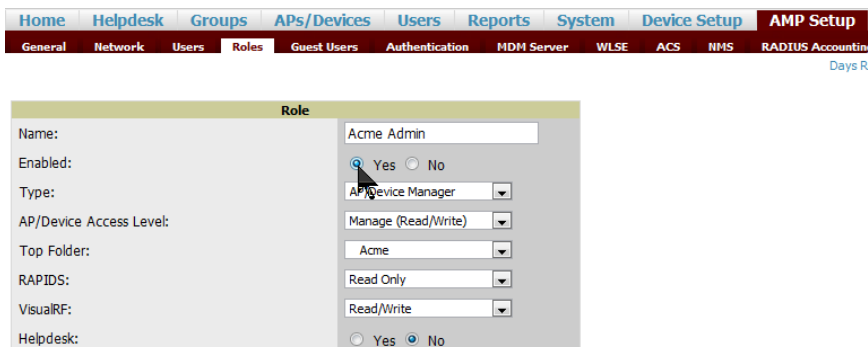
- "Enabling the IAP Role" on page 14
- "Updating the Instant Template" on page 14

Enabling the IAP Role

As shown previously, new IAP devices can be added to AMP 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 15](#).

Figure 15 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.



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 AMP 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.

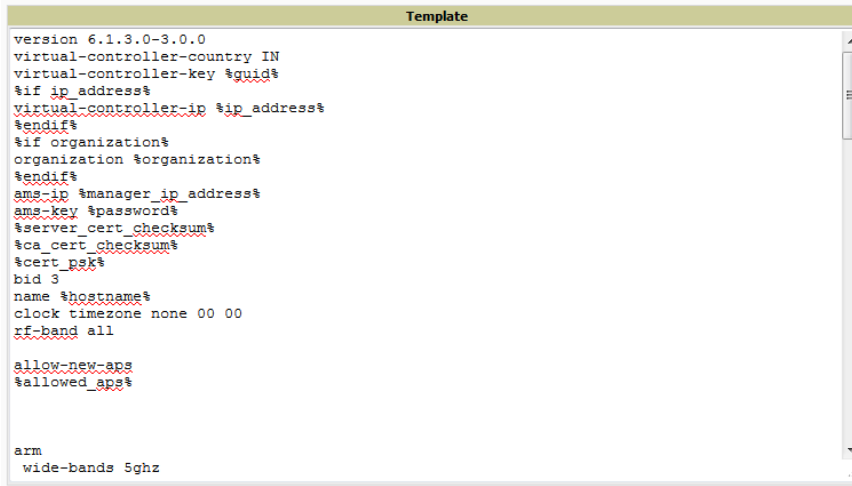
Updating the Instant Template

As stated previously, the first Instant network that is added to AMP 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.



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 16 *The Instant template editor*



```
version 6.1.3.0-3.0.0
virtual-controller-country IN
virtual-controller-key %guid%
%if ip_address%
virtual-controller-ip %ip_address%
%endif%
%if organization%
organization %organization%
%endif%
ams-ip %manager_ip_address%
ams-key %password%
%server_cert_checksum%
%ca_cert_checksum%
%cert_psk%
bid 3
name %hostname%
clock timezone none 00 00
rf-band all

allow-new-aps
%allowed_aps%

arm
wide-bands 5ghz
```

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 17 *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:

allowed_aps	guid
ams_identity	hostname
ca_cert_checksum	ip_address
cert_psk	ip_address_a
clock_timezone	ip_address_a_b
custom_variable_1	ip_address_a_b_c
custom_variable_10	manager_ip_address
custom_variable_2	organization
custom_variable_3	password
custom_variable_4	radius_server_ip
custom_variable_5	rf_band
custom_variable_6	server_cert_checksum
custom_variable_7	syslog_server
custom_variable_8	
custom_variable_9	

Refer to the *AirWave 7.6 User Guide* for detailed information about templates and variables.

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 a 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. With this method, 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 VC provides a link to quickly access the Template.

Known Issues with the Aruba Instant Integration with AirWave

- If the Organization String configured on the Aruba 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.