Aruba Instant in AirWave 7.5

Deployment Guide

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

Overview of Aruba Instant

Aruba Instant is a system of access points (IAP-92, IAP-93, or IAP-105) per Layer 2 subnet. Aruba 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 which IAP 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 AMP

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 two ways:

- Manually. See Setting up Aruba Instant Manually
- Automatically (through DHCP). See Setting up Aruba Instant Automatically

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 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.

NOTE

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.

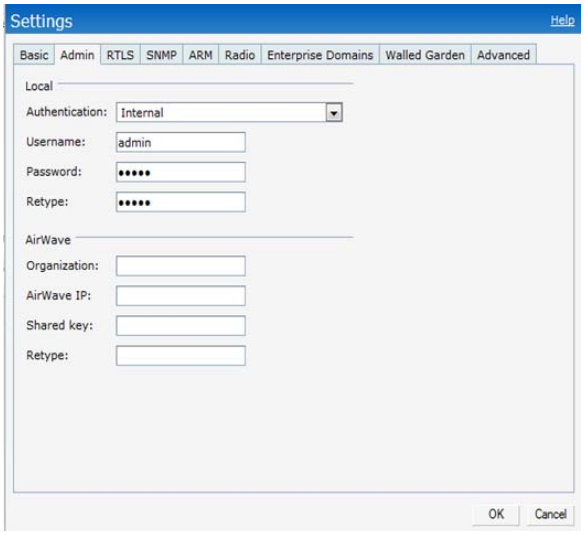
At this point, the admin in our example should send the Organization String, Shared Secret key, and AMP IP address to the on-site installers setting up Aruba Instant hardware inside the storefronts.

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.
4. 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.*



5. Locate the AirWave section on the **Admin** tab.
6. Enter the Origanization string, the AirWave IP address, and the Shared key.
7. 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-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 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.

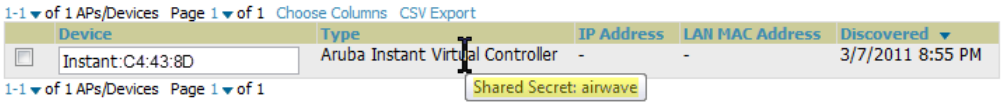
Remaining Manual Admin Tasks in AirWave

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

Verifying the Shared Secret

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 *Mouseover the Aruba Instant Type to Indicate Shared Secret*



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

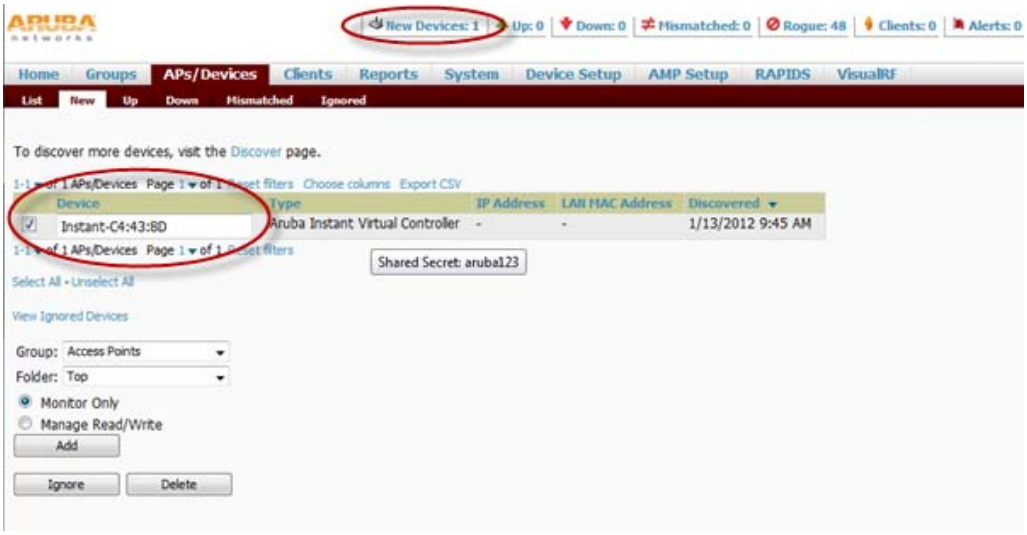
NOTE

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*



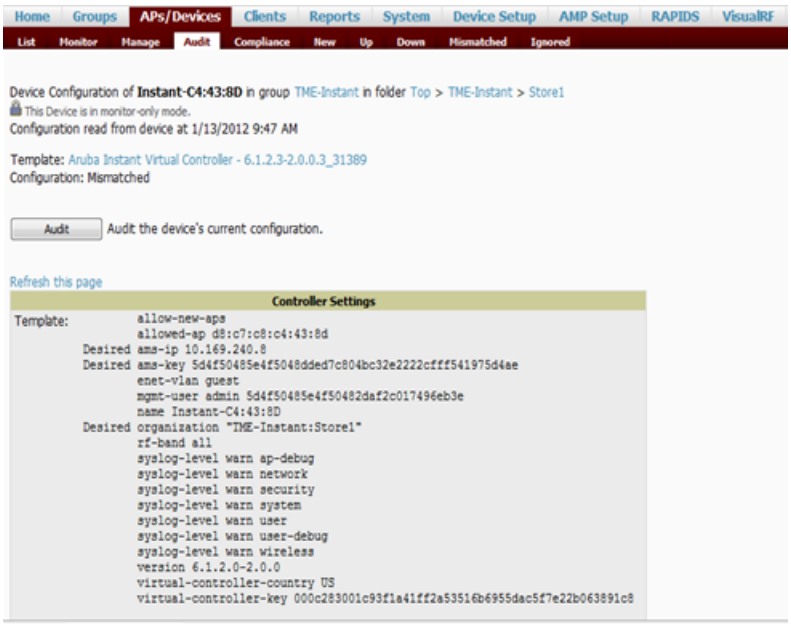
1. Click **Add** to add the device. A Group and Folder do not have to be selected. The Instant device will automatically get added to the new group that was created.
8. Select **Apply Changes Now** to add the Instant device to the group.

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

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

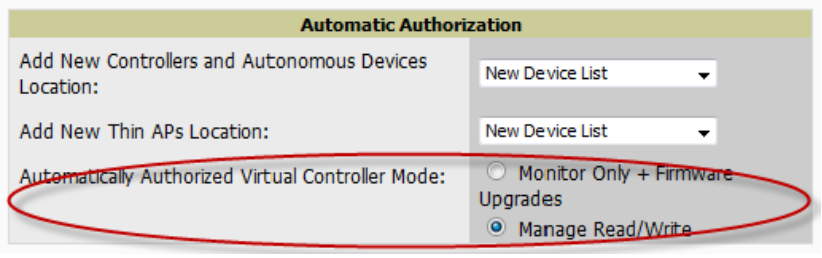

NOTE

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

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*



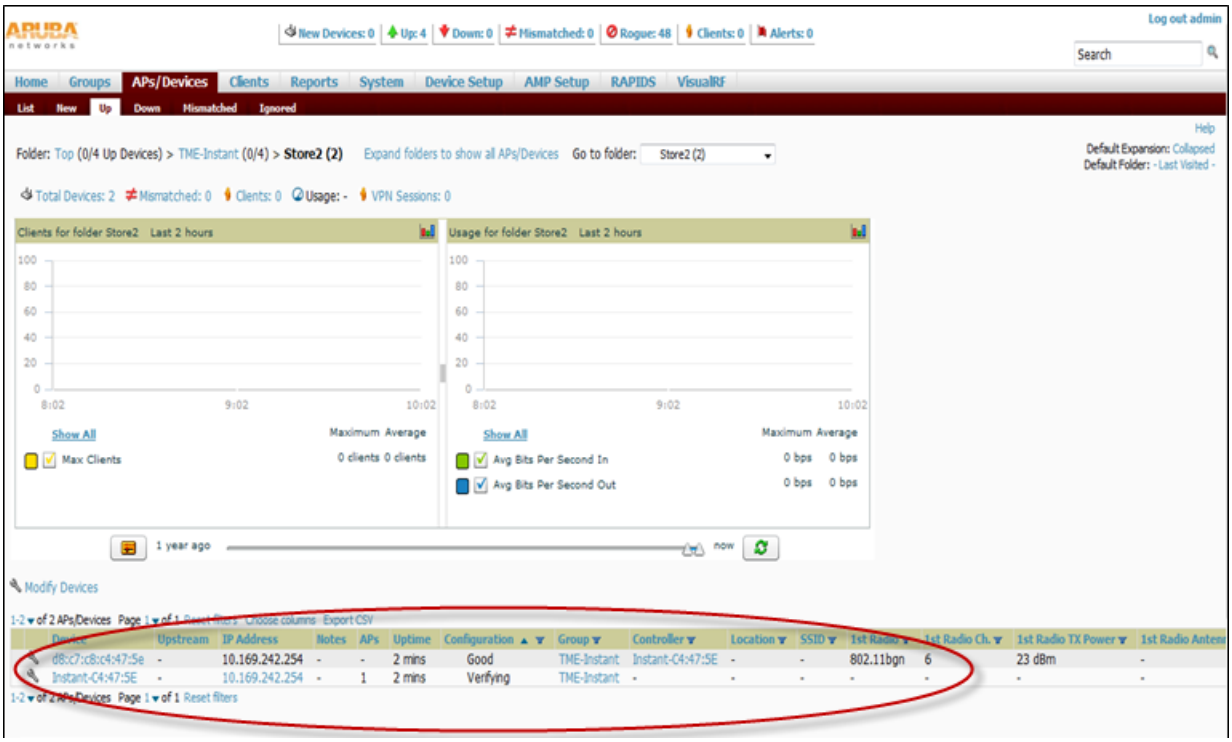
When the second Instant contacts AirWave using the DHCP server options as described previously, and that second Instant device has the same Shared key, it shows up on AirWave as shown below. Because the devices are in **Manage Read/Write** mode, there is no need for manual intervention to provision these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

NOTE

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*



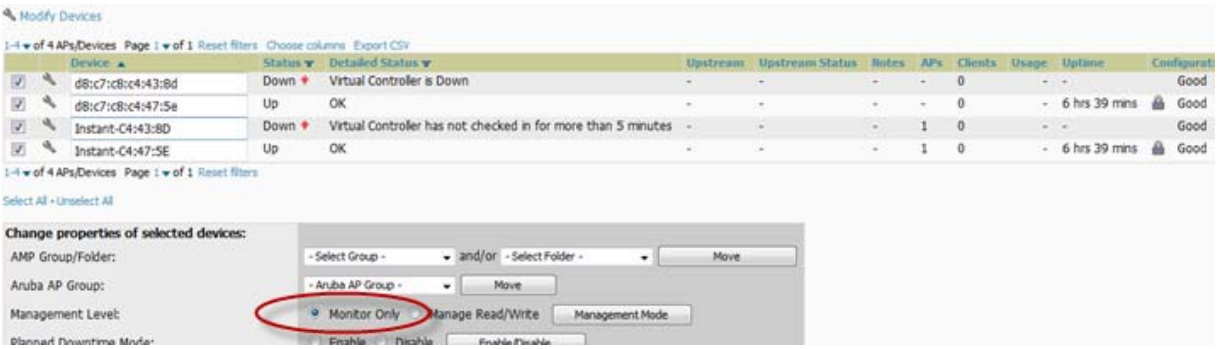
The golden template configuration from the first Instant network is used to provision the second Instant network in the new folder. When provisioning is complete, the status of the device will change from **Verifying** to **Good**.

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.
12. Filter by the folder name.
13. Select all devices and put them into monitor mode.
14. Click **Save** at the bottom of the page.

Figure 7 *Changing the mode 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.

Optional Tasks

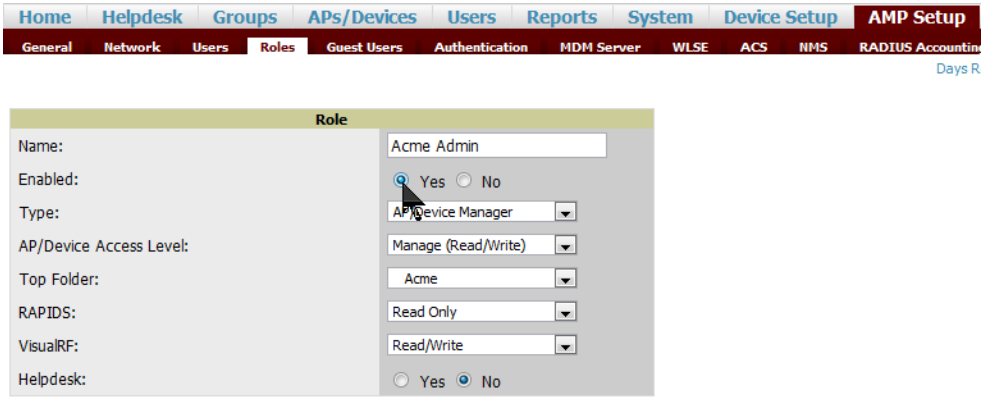
Additional optional tasks including enabling an IAP role for location-specific access and updating the Instant template.

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 8.

Figure 8 *Enable Admin User Roles in* ***AMP Setup > Roles***



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

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

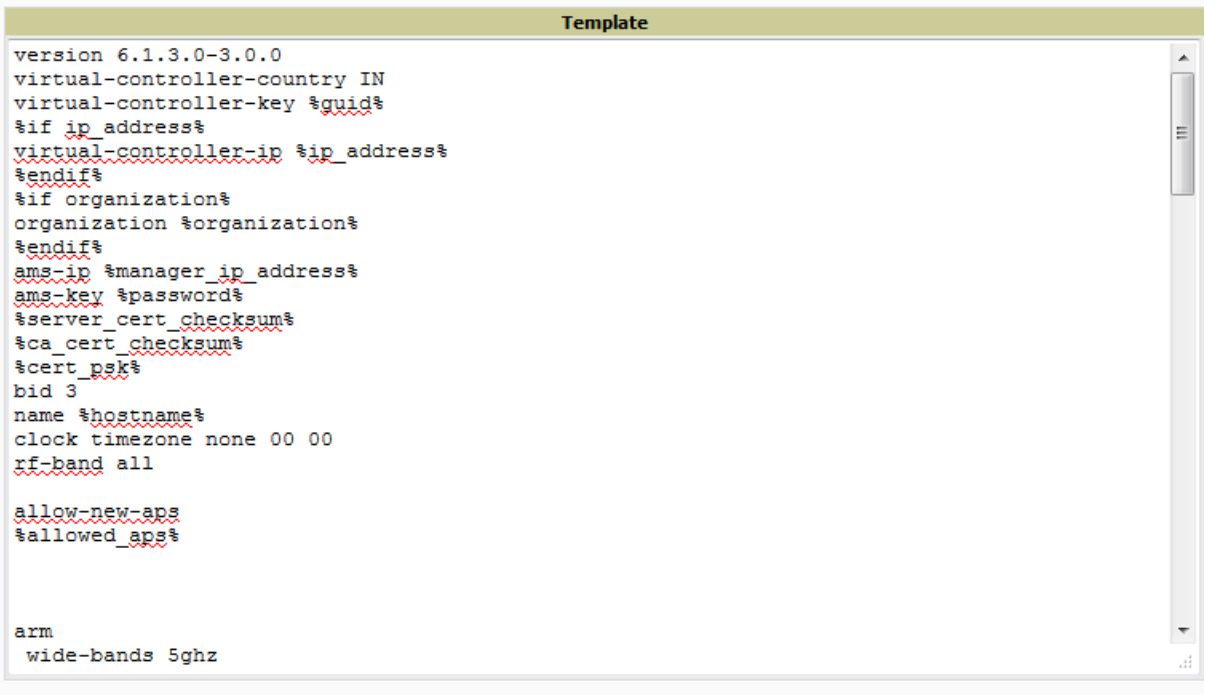
16. Evaluate, approve, or ignore incoming Virtual Controllers with a different top level Organization String and/or Shared Secret in the **APs/Devices > New** list. Subsequent IAPs are auto-authorized if they have an Organization/Shared Secret key that matches the Shared Secret key of any existing authorized Virtual Controller in the top-level Organization String.
17. Set the initial Virtual Controller to **Manage Read/Write** mode and push the good configuration to the subsequent IAPs.
18. 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.

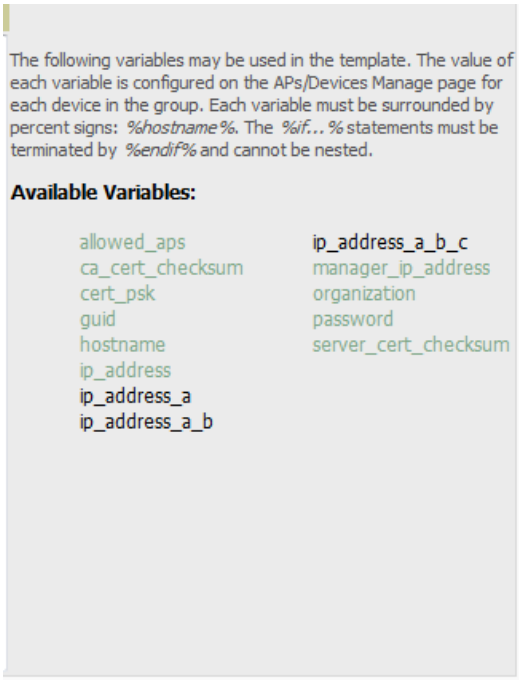
Be sure that the default configuration is validated and has been pre-tested in a non-production environment prior to applying it to a production network. Any changes that are made to this configuration will follow the same process each time and will be applied to other Instant networks.

Figure 9 *The Instant template editor*



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 10 *Allowed variables*



Other Available Features

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.

Known Issues of 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.