OmniVista 3600 Air Manager 8.2.14.1

Alcatel·Lucent

Enterprise

Deployment Guide

Contents

Alcatel-Lucent Instant (Instant) is a system of access points in a Layer 2 subnet. The OAW-IAPs are controlled by a single OAW-IAP that serves a dual role as an OAW-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 OAW-IAP/Virtual Controller you add to the network must be configured; the subsequent OAW-IAPs will all inherit the necessary configuration information from the Virtual Controller. Alcatel-Lucent Instant continually monitors the network to determine the OAW-IAP that should function as the Virtual Controller at any time, and the Virtual Controller will move from OAW-IAP to OAW-IAP as necessary without impacting network performance. The Virtual Controller technology in Alcatel-Lucent Instant is capable of OAW-IAP auto discovery, 802.1X authentication, role-based and device-based policy enforcement, rogue detection, and RF management.

Using Instant with OV3600

OV3600 can be used to provision and manage a multi-site deployment of Alcatel-Lucent Instant networks. For example, if you have 100 retail offices that require Instant to provide WLAN connectivity at each office, OV3600 can be used to provision all the 100 offices from a central site. OV3600 also provides the administrator with the ability to monitor these geographically dispersed Instant networks using an OV3600 server (depending on the scalability recommendations for OV3600).

With a distributed deployment where multiple locations have a Virtual Controller and OAW-IAPs, OV3600 serves as a centralized management console. OV3600 provides all functionality for normal WLAN deployments, including long-term trend reporting, PCI compliance, configuration auditing, role-based administration, location services, RF visualization, and many other features.

Refer to the *OV3600 Supported Infrastructure Devices Guide* for an up-to-date list of the Instant firmware versions and functions supported by OV3600.

Instant Integration into OV3600

Unlike other WLAN management products, OV3600 eliminates the need to configure and troubleshoot individual APs or dispatch IT personnel on-site. With OV3600, IT can centrally configure, monitor, and troubleshoot Alcatel-Lucent Instant WLANs, upload new software images, track devices, generate reports, and perform other vital management tasks, all from a remote location. Integrating Instant systems into OV3600 is unique from the setup of any other device class due to the following considerations:

- **Discovery:** OV3600 does not discover Instant devices via scanning (SNMP or HTTP) the network. Each Instant deployment will automatically check-in to the OV3600 configured within the IAP's user interface. The first Virtual Controller for an organization will automatically appear as a new device in OV3600. 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 OV3600 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 OV3600. 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 OV3600 via HTTPS. OV3600 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, OV3600 will list 10 Instant IAPs and one Instant Virtual Controller. An asterisk icon (*) beside the device name indicates that a device is acting as a Virtual Controller. You can also identify the IAP acting as the Virtual Controller by the identical LAN MAC addresses on the **Devices > List** page, Device Inventory reports, and any other OV3600 pages that list your network devices.

> **NOTE**
> A device that is added as a Virtual Controller does not count as a license for OV3600.

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

Secure Access to OV3600

By default, virtual controllers use a pre-shared key to authenticate to OV3600. To enable support for a different security method, navigate to **OV3600 Setup>General>Alcatel-Lucent 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 **OV3600 Setup>General>Alcatel-LucentInstant Options**, or click **Change** to upload a new certificate file.

A Virtual Controller or Instant AP can authenticate to the OV3600 server using a pre-shared key, or using two-way certificate-based authentication using an SSL certificate sent from OV3600 to the Instant device.

The Certificate-based authentication feature requires you upload the a certificate from a supported certificate authority to the OV3600 server, as the default OV3600 certificate will not be recognized by the Instant AP, and will cause the SSL handshake to fail. Certificate authentication also requires that the **OV3600 IP address** information configured on the Instant AP is a domain name, and not an IP address.

OV3600 supports the following trusted certificate authorities:

■ **Chain 1**: Trusted Root CA: C=SE, O=AddTrust AB, OU=AddTrust External TTP Network, CN=AddTrust External CA Root Intermediate CA: C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO High-Assurance Secure Server CA

■ **Chain 2**: Trusted Root CA: C=US, O=GeoTrust Inc., CN=GeoTrust Global CA Intermediate CA: Subject: C=US, O=Google Inc, CN=Google Internet Authority G2

■ **Chain 3**: Trusted Root CA: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 2006 VeriSign, Inc. - For authorized use only, CN=VeriSign Class 3 Public Primary Certification Authority - G5 Intermediate CA: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=Terms of use at https://www.verisign.com/rpa (c)10, CN=VeriSign Class 3 Secure Server CA - G3

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

Virtual Controllers push data to OV3600 via HTTPS. If your enterprise has a security policy that restricts the use of port 443 for inbound communication, you can change the port OV3600 uses to communicate with Instant devices on the **OV3600 Setup>General>Alcatel-Lucent Instant Options.**

Intrusion Detection System

OV3600 automatically detects rogue IAPs irrespective of their location in the network. It prevents authorized IAPs from being detected as rogue IAPs, and tracks and correlates the IDS events to provide a comprehensive picture of your network's security.

Instant Firmware Management

There are several ways to manage firmware updates in OV3600:

- Load the firmware image onto OV3600, and then launch an upgrade from OV3600. For a cluster of Instant APs, OV3600 pushes the firmware image to the virtual controller, and the virtual controller pushes the firmware to the rest of its Instant APs.

- Perform a rolling upgrade of the Instant firmware on standalone APs. When you enable the **Sequential Reboot** option on the **Groups > Firmware** page, the **Fast Download** option is automatically enabled. First, APs download the firmware image from the OV3600 server. APs which have completed the download share, or seed, the firmware image with the remaining APs. After all APs have successfully downloaded the firmware image, AirWave sequentially reboots APs in the same RF zone.

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

> **NOTE**
>
> OV3600 supports rolling upgrades for Instant APs running Instant 8.4.0.0 or later.

Figure 1 *Firmware Upgrade Job Options for OAW-IAPs*

To view the upgrade progress, go to **System > Firmware Upgrade Jobs**. In Figure 2, the upgrade status, "Downloading" indicates that the OAW-IAP is downloading the image from the OV3600 server while "Downloading (Seed)" indicates that the OAW-IAP is downloading the image from another IAP.

Figure 2 *Firmware Upgrade Jobs Status*

☐	swarm00255	91	8.4.0.0-8.4.0.0_11111	8.4.0.1-8.4.0.1_69195	-	ArubaInstant_Vela_8_4_0_1_69195_0.bin	Downloading	Waiting firmware download result	1	3/12/2019 4:20 /
☐	swarm00030	95	8.4.0.0-8.4.0.0_11111	8.4.0.1-8.4.0.1_69195	-	ArubaInstant_Vela_8_4_0_1_69195_0.bin	Downloading	Waiting firmware download result	1	3/12/2019 4:21 /
☐	swarm00160	98	8.4.0.0-8.4.0.0_11111	8.4.0.1-8.4.0.1_69195	-	ArubaInstant_Vela_8_4_0_1_69195_0.bin	Downloading	Waiting firmware download result	1	3/12/2019 4:21 /
☐	swarm00293	1	8.4.0.0-8.4.0.0_11111	8.4.0.1-8.4.0.1_69195	-	ArubaInstant_Vela_8_4_0_1_69195_0.bin	Downloading (Seed)	Waiting firmware download result	1	3/12/2019 4:19 /
☐	swarm00067	2	8.4.0.0-8.4.0.0_11111	8.4.0.1-8.4.0.1_69195	-	ArubaInstant_Vela_8_4_0_1_69195_0.bin	Downloading (Seed)	Waiting firmware download result	1	3/12/2019 4:19 /
☐	swarm00149	3	8.4.0.0-8.4.0.0_11111	8.4.0.1-8.4.0.1_69195	-	ArubaInstant_Vela_8_4_0_1_69195_0.bin	Downloading (Seed)	Waiting firmware download result	1	3/12/2019 4:19 /
☐	swarm00279	4	8.4.0.0-8.4.0.0_11111	8.4.0.1-8.4.0.1_69195	-	ArubaInstant_Vela_8_4_0_1_69195_0.bin	Downloading (Seed)	Waiting firmware download result	1	3/12/2019 4:19 /
☐	swarm00169	5	8.4.0.0-8.4.0.0_11111	8.4.0.1-8.4.0.1_69195	-	ArubaInstant_Vela_8_4_0_1_69195_0.bin	Downloading (Seed)	Waiting firmware download result	1	3/12/2019 4:19 /
☐	swarm00096	6	8.4.0.0-8.4.0.0_11111	8.4.0.1-8.4.0.1_69195	-	ArubaInstant_Vela_8_4_0_1_69195_0.bin	Downloading (Seed)	Waiting firmware download result	1	3/12/2019 4:19 /
☐	swarm00186	7	8.4.0.0-8.4.0.0_11111	8.4.0.1-8.4.0.1_69195	-	ArubaInstant_Vela_8_4_0_1_69195_0.bin	Downloading (Seed)	Waiting firmware download result	1	3/12/2019 4:19 /
☐	swarm00022	8	8.4.0.0-8.4.0.0_11111	8.4.0.1-8.4.0.1_69195	-	ArubaInstant_Vela_8_4_0_1_69195_0.bin	Downloading (Seed)	Firmware is written to flash successfully	1	3/12/2019 4:19 /
☐	swarm00231	10	8.4.0.0-8.4.0.0_11111	8.4.0.1-8.4.0.1_69195	-	ArubaInstant_Vela_8_4_0_1_69195_0.bin	Downloading (Seed)	Waiting firmware download result	1	3/12/2019 4:19 /
☐	swarm00281	9	8.4.0.0-8.4.0.0_11111	8.4.0.1-8.4.0.1_69195	-	ArubaInstant_Vela_8_4_0_1_69195_0.bin	Downloading (Seed)	Firmware is written to flash successfully	1	3/12/2019 4:19 /

OV3600 Pages with Instant-Specific Features

You can configure Instant features on the following pages:

- **Devices > New**

  From the **Devices > New** page, the admin user can mouse over the value in the **Type** column to display the device's shared secret with OV3600.

- **Devices > Manage**

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

- **Devices > List**

  On the **Devices > List** page, beside a device name indicates that the device is acting as a Virtual Controller. You can also identify the IAP acting as the Virtual Controller by the identical LAN MAC addresses on the **Devices > List** page, device inventory reports, and any other OV3600 pages that list your network devices. OV3600 lists the Virtual Controller as an additional device, even though it is part of the existing set of OAW-IAPs.

- **Clients > Client Detail**

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

- **Devices > Config**

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

- **Devices > Monitor > Radio Statistics**

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

- **Groups > Instant Config**

  The **Groups > Instant Config** page becomes available after you go to the **Groups > Basic** page and turn on the **Enable Instant GUI Config** option. This feature allows you to use OV3600 as a management console with the same UI as the OAW-IAP device.

- **RAPIDS**

  Instant supports mitigation and IDS event notification. All rogue devices are reported and stored in OV3600 for evaluation based on high-level rule sets.

- **Reports**

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

  > **NOTE**
  >
  > OV3600 does not provide a Device Uptime report for Alcatel-Lucent Instant devices.

In order to configure and manage an group of Instant APs via OV3600, the Instant AP acting as the Virtual Controller for the Instant AP cluster must be able to contact and authenticate to the OV3600 server. This can be done in any of the following ways

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

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

For each remote location, an on-site installer is required to physically mount the OAW-IAPs, connect them to the Alcatel-Lucent Instant SSID, configure the WLAN, and configure the names of the OAW-IAPs. The installer must then enter information into the OAW-IAP Virtual Controller that allows that device to communicate with OV3600. The configuration on the first Instant Virtual Controller that is added to OV3600 acts as the 'golden' configuration that is used as a template to provision other Instant Virtual Controllers at other locations as the locations are brought online. It is recommended that the 'golden' configuration is validated and pre-tested in a non-production environment prior to applying it to a production network.

> Users have the option to add additional devices into managed mode automatically by setting the **Automatically Authorized Virtual Controller Mode** option to **Manage Read/Write** on the **OV3600 Setup > General** page. Refer to the *OmniVista 3600 Air Manager 8.2.14.1 User Guide* for more information. It is also important to note that any changes that are made to the template variables will have to be manually applied to each deployed device.

Before you Begin

Before you start your initial Instant deployment via OV3600, you should define an OV3600 organization string for your Instant network, and identify which authentication method(s) the Virtual Controller will use to associate with OV3600. If you choose the hwhitelist authentication option, use the procedures in this section of the document to define your device whitelists.

Create your Organization Strings

The organization string is a list of colon-separated strings that define the group and folder the Instant Virtual switch is placed into after it authenticates to the OV3600 server. When an Instant Virtual Controller is added to AirWave, the device is authorized based on its organization string.

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

When you add an Instant Virtual Controller using an organization string, OV3600 will automatically create the an OV3600 role, group and folder, (if not already present) based upon the organization name in the organization string.

- OV3600 Role *<org_name> Admin.* This role gives access to the *<org_name>* folder.

- The configuration group *<org_name>.* OV3600 groups are primarily for configuration. Instant devices will automatically be placed into the configuration group defined by their organizational string, where they will receive the configuration settings and firmware version associated with that group.

- The folders *<org_name>[:<subfolder1>:<subfolder2>...].* OV3600 folders are hierarchical and are used to control which OV3600 users have access to which devices. All folders, including those created by an organization string, are located under the Top folder in OV3600

Example: Simple Organization String

This a simple organization string: US

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

Example: More Complex Organization String

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

A device with an organization string of "US:California:Sunnyvale" will be placed in an OmniVista 3600 Air Manager group that is called "US" and that is in a folder that is called "US" that mirrors a geographical structure with Sunnyvale beneath California.

Select your Authentication Methods

When the OV3600 administrator manually authorizes the first Instant Virtual Controller for an organization, OmniVista 3600 Air Manager uses that Virtual Controller's shared key or authentication certificate to authenticate other Virtual Controllers on the network. Once individual Virtual Controllers successfully complete authentication, they can also be validated against a predefined whitelist before they appear in the **Devices > New** list.

NOTE

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 **OV3600 Setup > General** page. Refer to the *OmniVista 3600 Air Manager 8.2.14.1 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 OV3600 administrator can use a shared key to manually authorize the first Instant Virtual Controller for an organization, or to automatically authenticate additional Virtual Controllers via automatic Zero-Touch provisioning. Any string is acceptable, but this string must be the same for all devices in your organization.

The OV3600 administrator sends the shared secret key, organization string and the OV3600 IP address to an on-site installer, who enters this information into the Virtual Controller. When that device authenticates to the OV3600 OV3600 server, it appears in the **Devices > New** list, and must be manually authorized by an OV3600 administrator. After the Instant device has been validated, other Instant devices using that shared key will automatically authenticate to the OV3600 server, and appear in the **Devices > New** list.

> **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 Alcatel-Lucent Instant device.

Certificate Authentication

The Instant Virtual Controller can authenticate to the OV3600 server with two-way certificate-based authentication, using an SSL certificate sent from OV3600 to the Instant device. Instant Virtual Controllers push data to OV3600 via HTTPS. If your enterprise has a security policy that restricts the use of port 443 for inbound communication, you can change the port OV3600 uses to communicate with Instant devices.

To enable certificate authentication for Instant Virtual Controllers authorizing to an OV3600 server:

1. Navigate **to the OV3600 Setup > General > Alcatel-Lucent Instant Options** section of the OV3600 WebUI.

2. Click the **Security method for adding new Virtual Controllers** drop-down list, and select **PSK and Certificate** or **Certificate Only**.

3. Click **Change**. The WebUI displays the Upload SSL certificate section of the **OV3600 Setup > General** page.

4. Click **Browse** to browse to and select a certificate file. The file must be PEM format containing both a valid private key and certificate.

5. Click **Upload**.

Whitelist Authentication

You can use an Instant whitelist to specify the Instant Virtual Controllers that are allowed to access the OV3600 server after those devices complete pre-shared key or certificate authentication. For more information on Instant whitelists, see Zero-Touch Provisioning using a Allowlist.

Setting up Instant Manually

To manually configure an Alcatel-Lucent Instant Virtual Controller to contact and authenticate to your OV3600 server and then download the proper configuration, you must enter the following information into the WebUI of each OAW-IAP/VC:

- OV3600 IP address: IP address of the OV3600 server.

- Organization string: This settings defines the device group to which the Virtual Controller will be associated.

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

- Pre-Shared Key (PSK) authentication: Enter a shared authentication key to associate your Virtual Controller to the OV3600 server.

- Certificate authentication: Upload a certificate onto your and OV3600 server to allow your Virtual Controller to authenticate to OV3600 using certificates.

Entering the Organization String and OV3600 IP

For the initial Instant Virtual Controller installed in each location, the on-site installer must log into that device's web interface via the Alcatel-Lucent Instant configuration SSID, then perform the following steps to configure that device to authenticate to the OV3600 server.

1. Log into your Virtual Controller.

2. Click on either **Set up Now** at the bottom of the UI or on the **Settings** tab in the top right corner. This opens the **Settings** menu.

3. Locate the OmniVista 3600 Air Manager section on the **Admin** tab.

   Figure 3 *Alcatel-Lucent Instant > Settings page*

4. Enter the organization string, the OV3600 IP address, and the shared key.

5. Click **OK** when you are finished.

Verifying the Shared Secret

After an initial Instant Virtual Controller contacts and authenticates to the OV3600 server, that Instant device appears in the **Devices > New** page. The admin user can mouse over the value in the **Type** column to verify the device's shared secret with OV3600, as shown in Figure 4.

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

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

If you defined an organization string when you configured the device to contact OV3600, you do not have to select any group or golder from the drop-down menus on the **Devices > New** page. An Instant Virtual Controller will automatically be added into the group or folder specified by its organization string, and will ignore any attempts to manually override its group or folder when the device is first added to OV3600. If you have any Virtual Controllers with no organization specified the first time they communicate with OV3600 then they will be placed in the Folder/Group drop-box values you have selected.

Assigning a Configuration and Firmware Version to the Device

After the Instant Virtual Controller has contacted and authenticated to the OV3600 server and is associated to the group and folder defined by its organization string, you must determine whether the Instant devices in these groups will be managed using template-based configuration or using Instant Config. Refer to the following sections for information on configuring your Instant Virtual switches using either of these two methods.

- Using Template Configuration on page 23
- Using Instant GUI Config on page 31

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

Creating your Organization String

The Organization String is a set of colon-separated strings created by the OV3600 administrator to accurately represent the deployment of each Alcatel-Lucent Instant system. This string is entered into the Alcatel-Lucent 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 organizational configuration (if not already present) in OV3600:

- OV3600 Role: <Org> Admin (initially disabled)
- OV3600 User: <Org> Admin (assigned to the role Org Admin)
- Folder: <Org> (under the Top folder in OV3600)
- 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 Alcatel-Lucent Instant OAW-IAP 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 Alcatel-Lucent Instant in four stores in two different cities for Acme Corporation, your Organization Strings might look like these:

- CompanyName:New York:Times Square Store
- CompanyName:New York:Queens Store

- CompanyName:San Francisco:Sunset Store
- CompanyName:San Francisco:SOMA Store

Authenticating to the OV3600 Server

When the OV3600 administrator manually authorizes the first Virtual Controller for an organization, OmniVista 3600 Air Manager 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 **Devices > New** list.

> **NOTE**
>
> 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 **OV3600 Setup > General** page. Refer to the *OmniVista 3600 Air Manager 8.2.14.1 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 OV3600 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 OV3600 administrator sends the shared secret key, Organization String and the OV3600 IP address to the on-site installer setting up the Virtual Controller and other Instant devices on the network. The OV3600 administrator then manually authorizes the Virtual Controller shared secret key when it appears in the **Devices > New** list. After the VC has been validated, other Instant devices using that shared key will automatically to the OV3600 server, and appear in the **Devices > New** list.

> **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 Alcatel-Lucent Instant device.

Whitelist Authentication

The Instant whitelist database is a list of the Instant APs that are allowed to access the OV3600 server after completing pre-shared key or certificate authentication. The Instant AP whitelist can be manually configured using the OV3600 UI, or imported into OV3600 in comma-separated values (CSV) format.

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

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

- Radius Servers
- RF Band Selection

- dynamic_variables

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

```
Name,LAN MAC Address,Serial Number,Virtual Controller Name,Group Name,Folder Name IAP_
Canada_1,ff:c7:c8:c4:21:ff,BD0086086,Canada-Office,Canada,Vancouver:Downtown IAP_US_
1,F0:0B:86:CF:93:FF,BE0542245,US-Office,US,San Fancisco:CenterTown:HillTop
```

When this feature is enabled and an Instant AP attempts to connect to OV3600, OV3600 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 **Devices > New** page, where it can be assigned to an OmniVista 3600 Air Manager group and folder.

To enable whitelist authentication and manually add Instant APs to a whitelist via the OV3600 WebUI:

1. Navigate to **OV3600 Setup > General**

2. Expand the **Automatic Authorization** section

3. In the **Authorize Alcatel-Lucent Instant APs & Aruba Switches to OV3600** section, select **Whitelist.**

4. Click **Save**.

5. Next, navigate to **Devices > New**.

6. Click the **Instant AP & Aruba Switch Whitelist drop-down list, and select Add an Instant AP or an Aruba Switch to the Whitelist.**

7. 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.

8. In the **Group** and **Folder** fields, specify the group and folder to which the device will be assigned

9. Click **Add**. You are prompted to confirm changes. Click **Apply Changes Now**, or specify a time that the device should be added to the whitelist.

To import a whitelist in Comma-Separated Value (CSV) format to the OV3600 server:

1. Navigate to **Devices > New**.

2. Click the **Instant AP & Aruba Switch Whitelist** drop-down list, and select **Import Instant AP or an Aruba Switch Whitelist from CSV**.

1. Navigate to **Device Setup > Add**.

2. In the **Select the type of device to add** field, select **Alcatel-Lucent Device**.

3. Click the **Import Devices via CSV** link.

4. The **Upload a list of devices** page opens. This page describes the required fields and format for the whitelist file.

5. Click **Choose File,** browse to and select the CSV file, then click **Upload**.

Entering the Organization String and OV3600 Information into the OAW-IAP

For the initial OAW-IAP or Virtual Controller installed in each location, the on-site installer must log into that device's web interface via the Alcatel-Lucent Instant configuration SSID, then perform the following steps to set up OV3600 in Instant.

1. Log into your OAW-IAP.

2. Click on either **Set up Now** at the bottom of the UI or on the **Settings** tab in the top right corner. This opens the **Settings** menu.

3. Locate the OmniVista 3600 Air Manager section on the **Admin** tab.

Figure 5 *Alcatel-Lucent Instant > Settings page*

4. Enter the Organization string, the OV3600 IP address, and the Shared key.

5. Click **OK** when you are finished.

Automatic Zero-Touch Provisioning

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

- Zero-Touch Provisioning via DHCP
- Zero-Touch Provisioning using a Allowlist

Zero-Touch Provisioning via DHCP

The Alcatel-Lucent Instant Virtual Controller initiates a DHCP request with the DHCP option 60 string 'Alcatel-Lucent Instant.' If the DHCP server is configured to recognize this option 60 string, it will return an option 43 string containing the organization, OV3600 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,alcatellucent123"
```

The OV3600 information in the option 43 will be used to connect to OV3600, if OV3600 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 "AlcatellucentInstantAP"
 option 43 text "CompanyName :Store1,10.169.240.8,alcatellucent123"
 network 10.169.241.0 255.255.255.0
 authoritative
!
ip dhcp pool IAP-Pool2
 default-router 10.169.242.1
 option 60 text "AlcatellucentInstantAP"
 option 43 text "CompanyName:Store2,10.169.240.8,alcatellucent123"
 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 OV3600:

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

Zero-Touch Provisioning using a Allowlist

The Instant allowlist database is a list of the Instant Virtual Controllers that are allowed to access the OV3600 server after those devices complete pre-shared key or certificate authentication. This Instant allowlist must be manually configured using the OV3600 UI or imported into OV3600 in comma-separated values (CSV) format before you deploy the devices on the list.

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

- Name
- LAN MAC Address
- Serial Number
- Virtual Controller Name
- Group Name
- Folder Name
- Timezone
- CHAP Secret
- PPPoE Service Name
- PPPoE User Name
- PPPoE Password
- Radius Servers
- RF Band Selection

- Location
- Syslog Server
- Control Plane VLAN
- VLAN Number
- Gateway
- Netmask
- Modem PIN
- Notes
- custom_variable_1...custom_variable_10
- Modify authorized device
- Sync dynamic variables
- dynamic_variables

An example of a allowlist entry using this format is as follows:
```
Name,LAN MAC Address,Serial Number,Virtual Controller Name,Group Name,Folder Name IAP_
Canada_1,ff:c7:c8:c4:21:ff,BD0086086,Canada-Office,Canada,Vancouver:Downtown IAP_US_
1,F0:0B:86:CF:93:FF,BE0542245,US-Office,US,San Fancisco:CenterTown:HillTop
```

When this feature is enabled and an Instant Virtual Controller attempts to connect to OV3600, OV3600 checks the MAC address or serial number of the device against this allowlist, and authorizes the device if it's MAC address or serial number matches a allowlist entry. Once authorized, that Virtual Controller appears in the **Devices > New** page, where it can be assigned to an OmniVista 3600 Air Manager group and folder.

There are four methods to create an Instant allowlist. You can create a allowlist using the OV3600 WebUI, import a allowlist in CSV format using the OV3600 WebUI, upload a allowlist via an OV3600 API, or configure allowlist Entries using a script in the OV3600 command-line interface. These options are described in the sections below.

Creating Allowlists via the OV3600 WebUI

To enable Allowlist authentication and manually add Instant Virtual Controllers to a allowlist via the OV3600 WebUI:

1. Navigate to **OV3600 Setup >General**

2. Expand the **Automatic Authorization** section

3. In the **Authorize Alcatel-Lucent Instant APs & Aruba Switches to OV3600** section, select **Allowlist.**

4. Click **Save**.

5. Next, navigate to **Devices > New**.

6. Click the **Instant AP & Aruba Switch Allowlist** drop-down list, and select **Add an Instant AP or an Aruba Switch to the Allowlist**.

7. Enter allowlist information for the Instant Virtual Controller. Each allowlist entry must have an Instant AP name and either a serial number or a MAC address.

8. In the **Group** and **Folder** fields, specify the group and folder to which the device will be assigned

9. Click **Add**. You are prompted to confirm changes. Click **Apply Changes Now**, or specify a time that the device should be added to the allowlist.

Importing a Allowlist in CSV Format

To import a Allowlist in Comma-Separated Value (CSV) format to the OV3600 server:

1. Navigate to **Devices > New**.

2. Click the **Instant AP & Aruba Switch Allowlist** drop-down list, and select **Import Instant AP or an Aruba Switch Allowlist from CSV**.

3. Navigate to **Device Setup > Add**.

4. In the **Select the type of device to add** field, select **Alcatel-Lucent Device**.

5. Click the **Import Devices via CSV** link.

6. The **Upload a list of devices** page opens. This page describes the required fields and format for the allowlist file.

7. Click **Choose File,** browse to and select the CSV file, then click **Upload**.

Uploading a Allowlist via an OV3600 API

Software developers can use the OV3600 API to upload a allowlist in CSV format.

- **URL**: https://<airwave_server_address>/api/ap_allowlist_upload

- **Location of allowlist in CSV format**: /var/www/html/static/sample/import_allowlist_sample.csv

Table 1: Allowlist API Parameters

Parameter	Description
csv	Allowlist document in proper Instant Allowlist CSV format.

Parameter	Description
append_allowlist	Specify one of the following update options: ■ **0**: Replace the whole allowlist with the current content. All the items not in current content will get removed. ■ **1**: Update the allowlist with the current content. All the items not in current content will remain the same.

Example URL:

https://<ov3600_server_ip>/api/ap_allowlist_upload?append_allowlist=1&csv=<csv_file>

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

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

Uploading a Allowlist via a Script

OV3600 includes a built-in script that can be used to configure allowlist entries. The script is located at `usr/local/airwave/bin/import_allowlist.pl`

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

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

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

This script supports the following parameters:

Table 2: allowlist Script Parameters

Parameter	Description
--amp <ip/host>	OV3600 server ip address or hostname
--usr <username>	User name of the OV3600 user uploading the allowlist file.
--passwd <password>	Password for the OV3600 user uploading the allowlist file.
--file <file>	Name of the CSV file that contains the allowlist.
--update <update>	Specify one of the following update options: ■ 0: Replace the outdated allowlist with content from a newer file. All the items not included in the newer file will get removed. ■ 1: Update the allowlist with the additional content from a newer file. Any items not in the current content file will remain the same.

Verifying the Shared Secret

After an initial Instant Virtual Controller contacts and authenticates to the OV3600 server, that Instant device appears in the **Devices > New** page. The admin user should mouse over the value under the **Type** column to verify the device's Shared Secret with OV3600, as shown in Figure 6.

Figure 6 *Mouse over the Type column to view the Shared Secret*

	DEVICE	TYPE	IP ADDRESS	LAN MAC ADDRESS	DISCOVERED
☐	Instant:C4:43:8D	Aruba Instant Virtual Controller	-	-	10/29/2014 12:41 PM

Shared Secret: airwave

10 ∨ per page

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

NOTE

If you defined an organization string when you configured the device to contact OV3600, you do not have to select any group or golder from the drop-down menus on the **Devices > New** page. These Instant devices will automatically be added into the group or folder specified by their organization string, and will ignore any attempts to manually override their group or folder when the device is first added to OV3600. If you have any Virtual Controllers with no organization specified the first time they communicate with OV3600 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 23
- Using Instant GUI Config on page 31

NOTE

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

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

Additional information about creating templates for Alcatel-Lucent Instant is available in the *OmniVista 3600 Air Manager 8.2.14.1 User Guide*.

Manually Confirm the First Instant Device

After the first Instant Virtual Controller receives the OV3600 server information from the DHCP server, or after OV3600 server information is manually configured, the Virtual Controller appears as a new device in OV3600. This Virtual Controller is added in **Monitor Only** mode.

Figure 7 *A new Instant device in OV3600*
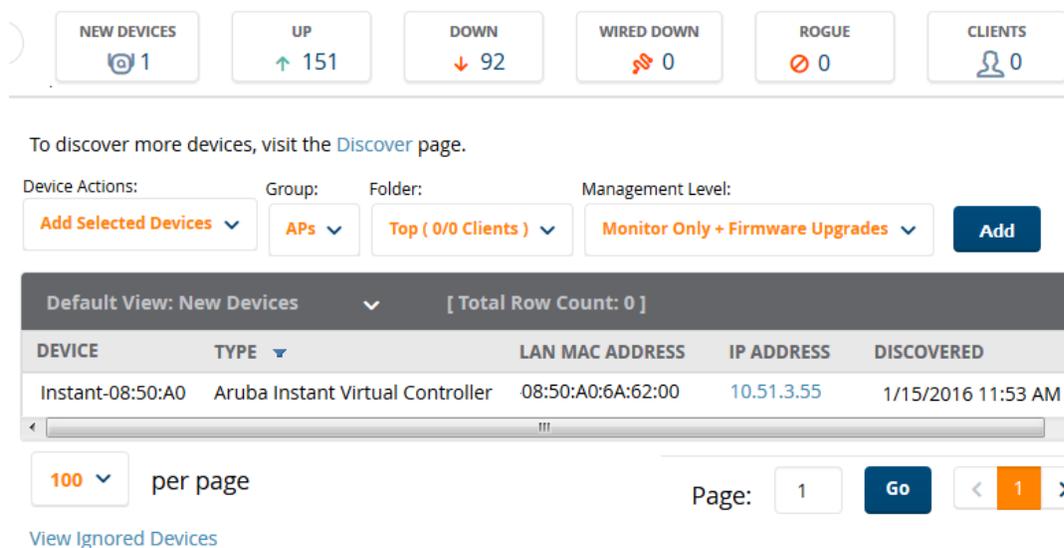
1. Click **Add** to add the device. A group and folder do not have to be selected. The Virtual Controller will automatically get added to the new group created by OV3600 to match the device's organization string.

2. Select **Apply Changes Now** to add the Virtual Controller to its group.

Updating the Instant Template

The configuration on the first Instant Virtual Controller added to OV3600 becomes the default "golden configuration" for that device group. OV3600 automatically creates a template based on configuration of this initial device, then uses the template to provision other Virtual Controllers added to the group. After adding the first Virtual Controller to OV3600, you can view and, if necessary, edit this configuration before you add other Virtual Controllers.

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

You can configure a group of Instant devices using the configuration template or the Instant GUI Configuration (IGC) feature. OV3600 will not display the **Groups > Templates** pages if you enable the Instant GUI Config feature for that group.

To view or edit the Instant template:

1. Navigate to **Groups > List** and select the group that contains your initial Instant device.

2. From the **Groups** table, select the name of the group. The navigation menu on the left side of the web page updates to display additional navigation options, including the **Groups > Template** option.

3. Navigate to **Groups > Template**.

4. Locate the template and click 🖊 to edit the Instant template.

Figure 8 *Sample Configuration and Allowed Variables*

The **Allowed Variables** section at the right of the template editor displays the set of variables that you can added to the template. Refer to the *OmniVista 3600 Air Manager 8.2.14.1 User Guide* for information about using templates and variables.

Template Configuration for SES-imagotag Electronic Shelf Labels

For Instant APs (IAPs) running Instant 8.8.0.0 or later, OV3600 now supports ESL profiles used to configure an Electronic Shelf Label (ESL) label by SES-imagotag. From the **Groups > Template** page, you can use variables, or import ESL settings from an Instant AP, to configure the static channel number of the ESL radio and the ESL server ip address.

Figure 9 shows the sesimagotag-esl-channel variable used in the configuration template.

Figure 9 *Template Configuration using Variables*

For more information about the SES-imagotag ESL System, see the *Alcatel-Lucent AOS-W8.8.0.0 User Guide*.

Adding Additional Instant APs to OV3600

There are several ways to add Instant devices to OV3600: monitor-only mode,automatic provisioning, and bulk provisioning with a CSV file.

Adding Devices in Monitor-Only Mode

As a best practice for using Instant in OV3600, change the mode for new devices to **Monitor Only**. This ensures that OV3600 doesn't overwrite the configuration for the new devices.

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

Figure 10 *Changing the mode to Monitor Only + Firmware Upgrades*
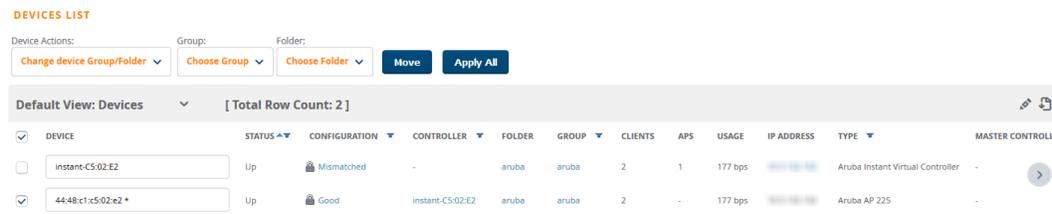
Adding Devices with Automatic Provisioning

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

1. Navigate to **OV3600 Setup > General**.
2. In the Automatic Authorization section, select **Manage Read/Write** for the "Automatically Authorized Virtual Controller Mode" option, as shown inFigure 11.

Figure 11 *Turning on the Automatic Provisioning Mode*

3. Click **Save**.

When the second Instant Virtual Controller contacts OV3600 using the same shared key as the first Virtual Controller , that device is automatically placed into the group described in its organization string, and provisioned with the golden configuration for that group.

If you have allowed OV3600 to add Virtual Controllers in **Manage Read/Write** mode, there is no need for manual intervention to provision these new Instant networks. When provisioning is complete, the status of the device will change from **Verifying** to **Good**.

Editing Variables

OmniVista 3600 Air Manager 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. OmniVista 3600 Air Manager also supports additional generic variables that you can customize (such as adding a new WLAN). The defaults for all VC variables can be changed from the Template page.

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

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

Figure 12 *Select the VCs to update*

2. Click the **Device Actions** drop-down list and select the **Alcatel-Lucent Virtual Controller Variables** option.

3. Click **Update**. The opens the **Variable Edit** page.

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

- [Editing Individual Virtual Controller Values](#)
- [Bulk Editing of Multiple Virtual Controllers](#)
- [Using Custom Variables](#)
- [Applying Changes](#)

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 13 *Change the Individual VC Names*

Bulk Editing of Multiple Virtual Controllers

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

Perform the following steps to apply bulk edits.

1. In the edit screen, select the check box beside the virtual controller(s) that will be edited. (See Figure 14.)
2. Select the variable that you want to change from the drop down list in the upper section.
3. Enter or select the new value. In the example below, clock_timezone is changed to Pacific time for both VCs.
4. Click **Apply** when you are finished making each change. The selected virtual controllers will display the updated information. Follow these same steps for each variable that you want to edit.

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

Figure 14 *Change the Timezone variable*

Using Custom Variables

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

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

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

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

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

Figure 15 *Entering a custom variable (cropped)*

Applying Changes

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

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

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

Figure 16 *Confirm Changes page*

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

Instant GUI Config (also called IGC or Instant Config) provides an alternate method for configuring and managing devices running Instant 3.2 to Instant 8.10.0.0. If Instant Virtual Controllers are added to a group, this feature is available when you select **Enable Instant GUI Config** option on the **Groups > Basic** page. When this feature is enabled, the **Groups > Templates**, **Devices > Manage**, and **Devices > Device Configuration** pages are unavailable. Instead, all OAW-IAP management is performed from the **Instant Config** pages in OV3600.

> **NOTE**
> - Instant Config is fully compatible with devices running Instant version 3.2 to 8.10.0.0. Instant devices running different firmware versions cannot reside in the same group. Each group can only include devices with the same firmware version.
>
> - OV3600 8.2.13.1 introduces support for a new device, AP-635. AP-635 runs on ArubaOS 8.9.0.0. AP-635 supports 2.4 GHz, 5 GHz, and 6 GHz radios. The 6 GHz radio supports channel range from 1 to 233 and the supported channel widths are 20MHz, 40MHz, 80MHz, and 160MHz.

Refer to the following sections for more information:

- Enabling Instant GUI Config
- Importing Devices for Instant GUI Config
- The Instant GUI Config WebUI
- Where to Get Additional Information

Enabling Instant GUI Config

The **Groups > Instant Config** pages are hidden by default. Perform the following steps to enable this feature and allow the OV3600 WebUI to display the **Groups > Instant Config** pages.

1. Navigate to **Groups > List**.
2. Select the group on which you want to enable this feature.
   - To enable this feature on a new group, click **Add**, name the new group, then click **Add** again.
   - To enable this feature on an existing group, select the name of the group from the **Groups** table.
3. Navigate to **Groups > Basic**, and scroll down to the **Group Display Options** section.
4. Ensure that the **Show Device Settings for** option includes Instant devices. Instant GUI Config is only available for groups that include Instant devices. The example **Group Display Options** settings in the figure below allow the OV3600 WebUI to display device settings for Alcatel-Lucent and Aruba Instant devices.

Figure 17 *Include Instant devices*

Group Display Options

Show Device Settings for: Selected device types ▾

                                                     Select devices in this group
                                                     Select All - Unselect All
                                                     ☐ 3Com
                                                     ☐ Alcatel-Lucent
                                                     ☑ Alcatel-Lucent Instant
                                                     ☐ Alcatel-Lucent Switch
                                                     ☐ Arista
                                                     ☐ Aruba
                                                     ☐ Aruba AirMesh
                                                     ☑ Aruba Instant
                                                     ☐ Aruba MAS
                                                     ☐ ArubaOS Switch
                                                     ☐ ArubaOS-CX Switch

5. Click **Save and Apply**. You are directed to the **Groups > Monitor** page.

6. Navigate back to the **Groups > Basic** page.

7. In the Aruba/Alcatel-Lucent Instant section, select **Yes** for the **Enable Instant GUI Config** option.

8. Click **Save and Apply**.

Figure 18 *Enable Instant Config*

Aruba/Alcatel-Lucent Instant

Enable Instant GUI Config:	⦿ Yes ◯ No
HTTPS Timeout (1-30 min):	5
CA Cert:	-- None -- ▾

Buttons and Icons in Instant Config

Table 3 describes the buttons and icons that are available on the Instant Config pages.

Table 3: Instant Config Buttons and Icons

Function	Image	Description
Audit	Audit	On the **OV3600 > 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.
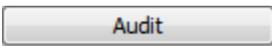
Table 3: Instant Config Buttons and Icons (Continued)

Function	Image	Description
Cancel	Cancel	Cancels the current edit or task.
Delete	☒	Deletes a network.
Down	✖	Indicates a device is down.
Employee Usage	Employee	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	Guest	Indicates that the network is used for Guest data. This is normally used when captive portal is enforced.
Mismatched	≠	Indicates a mismatched device configuration.
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 **OV3600 > Overrides** page for the selected device to view the override(s).
Policy Error	!	Indicates that OV3600 is unable to push or compare configurations because the policy version does not match the firmware version.
Save	Save	Saves the information on the current page in the OV3600 database.
Save & Apply	Save and Apply	Saves changes to OV3600'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.

Table 3: *Instant Config Buttons and Icons (Continued)*

Function	Image	Description
Voice Usage	*(Voice icon)*	Indicates that the network is used for voice traffic. This is normally used when all traffic must be prioritized.

Importing Devices for Instant GUI Config

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

> **NOTE**
>
> When importing Instant devices in bulk to a new group, OV3600 selects the first device added to that group as the "golden" configuration. The configuration will be pushed to other Instant Virtual Controllers added to the group. As a recommended best practice, select a Virtual switch with a configuration that can be used as the golden configuration for other devices, and add it to the group before adding any others.

1. Click the **New Devices** statistics icon in the top header to open the **Devices > New** page and view information about the newly discovered devices (see Figure 19).

Figure 19 *List of Discovered Devices*

2. Select the check box beside the Instant device(s) you want to add to the Instant Virtual Controller group.

3. Use the **Group** and **Folder** drop-down lists to select the groups and folder to which the devices will be added. The default group appears at the top of the Group list.

4. Click **Add**.

5. Go to the **Devices > List** page, select the folder that contains the newly added devices, and verify that the devices have been properly assigned.

> **N O T E**
>
> Devices cannot be added to a Global Group because groups designated as "Global Groups" cannot contain access points.

Add Newly Discovered Devices to a Group

1. Select the **New Devices** link in the header to launch the **Devices > New** page where information about all newly discovered devices is displayed Figure 20). 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 switch (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 20.

    Figure 20 *Devices > New Page*

    To discover more devices, visit the Discover page.

    Use Specified Group/Folder for Instant APs & Aruba Switches: ◯ Yes ⦿ No

Device Actions:	Group:	Folder:	Management Level:	
Add Selected Devices ⌄	Access Points ⌄	Top (1/1 Clients) ⌄	Monitor Only + Firmware Upgrades ⌄	**Add**

    Default View: New Devi... ⌄   [Total Row Count: 62]

	DEVICE	TYPE ▼	LAN MAC ADDRESS	IP ADDRESS	DISCOVERED
☐	RAP-315-Yilydia-home	AP 315	70:3A:0E:C0:78:D6		7/23/19, 5:03 AM
☐	RAP-305-Zhouqiang-home	AP 305	40:E3:D6:CF:F4:C0		7/25/19, 5:16 AM
☐	RAP-205-cxwang-home	AP 205	B4:5D:50:CA:99:A8		8/5/19, 8:24 AM
☐	RAP-325-Zhenleiwang-home	AP 325	80:8D:B7:CD:FF:82		8/9/19, 12:51 AM
☐	84:d4:7e:c5:28:7c	AP 315	84:D4:7E:C5:28:7C		9/11/19, 5:44 AM
☐	F25-d0:15:a6:c3:a9:d2	AP 50	D0:15:A6:C3:A9:D2		9/16/19, 12:20 AM

To discover more devices, visit the Discover page.

Use Specified Group/Folder for Instant APs & Aruba Switches: ○ Yes ⦿ No

Device Actions:	Group:	Folder:	Management Level:	
Add Selected Devices ⌄	Access Points ⌄	Top (1/1 Clients) ⌄	Monitor Only + Firmware Upgrades ⌄	Add

Default View: New Devi... ⌄   [Total Row Count: 62]

☐	DEVICE	TYPE ▼	LAN MAC ADDRESS	IP ADDRESS	DISCOVERED
☐	RAP-315-Yilydia-home	AP 315	70:3A:0E:C0:78:D6		7/23/19, 5:03 AM
☐	RAP-305-Zhouqiang-home	AP 305	40:E3:D6:CF:F4:C0		7/25/19, 5:16 AM
☐	RAP-205-cxwang-home	AP 205	B4:5D:50:CA:99:A8		8/5/19, 8:24 AM
☐	RAP-325-Zhenleiwang-home	AP 325	80:8D:B7:CD:FF:82		8/9/19, 12:51 AM
☐	84:d4:7e:c5:28:7c	AP 315	84:D4:7E:C5:28:7C		9/11/19, 5:44 AM
☐	F25-d0:15:a6:c3:a9:d2	AP 50	D0:15:A6:C3:A9:D2		9/16/19, 12:20 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 **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.

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

The Instant GUI Config WebUI

The **Groups > Instant Config** page of the OV3600 WebUI allows network administrators to configure Instant Virtual Controllers remotely through OV3600. The flow of pages within the Instant GUI Config UI closely resemble the pages available in Alcatel-Lucent Instant.

> **NOTE**
> For more information on the Instant settings configurable via the OV3600, WebUI, refer to the latest *Alcatel-Lucent Instant User Guide*.

Figure 21 *Groups > Instant Config*
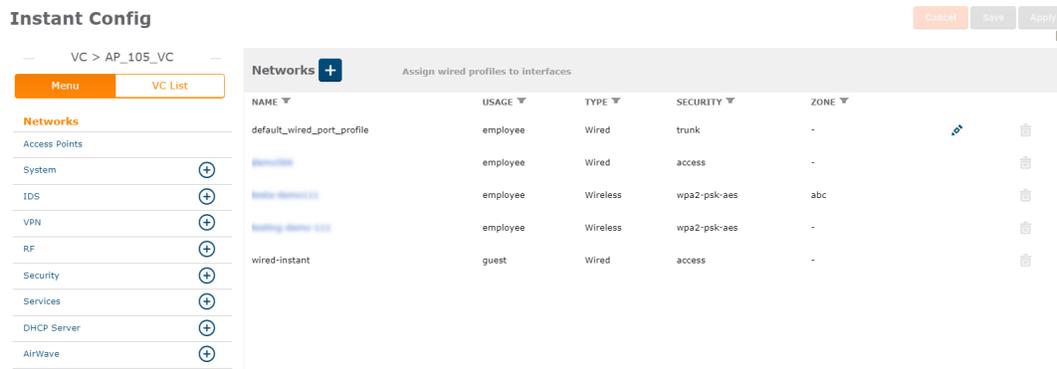
Group Configuration

The **Groups > Instant Config** page provides an expandable menu of the available Instant group configuration settings, as shown in . When you configure group settings, OV3600 applies the changes to all devices in the group. Click the **VC List** tab to view and modify individual devices within the group.

Figure 22 *Group Menu*
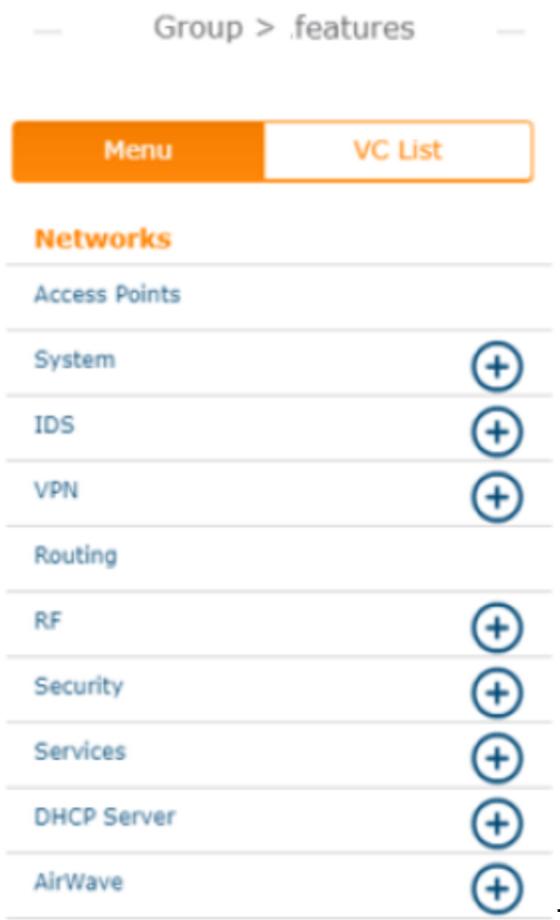
System Configuration

For Instant APs (IAPs) running Instant 8.5.0.0 or later, OV3600 supports ESL profiles used to configure an Electronic Shelf Label (ESL) label by SES-imagotag. You can configure ESL Settings using Instant GUI Config (IGC) for the devices in a group.

To configure ESL settings, complete the following steps:

1. Go to **Groups > Instant Config**, then click the **VC List** tab.

2. Select the devices you want to configure from the list of access points, then click **Bulk Edit**. Or, click the blue name link to open the configuration page for the device.

3. Enter the communication channel number for the "Sesimago Tag Channel" option and the IPv4 address for the "Sesimago Tag Server" option (see Figure 23).

4. Click **Apply**.

Figure 23 *Group Configuration using the IGC*
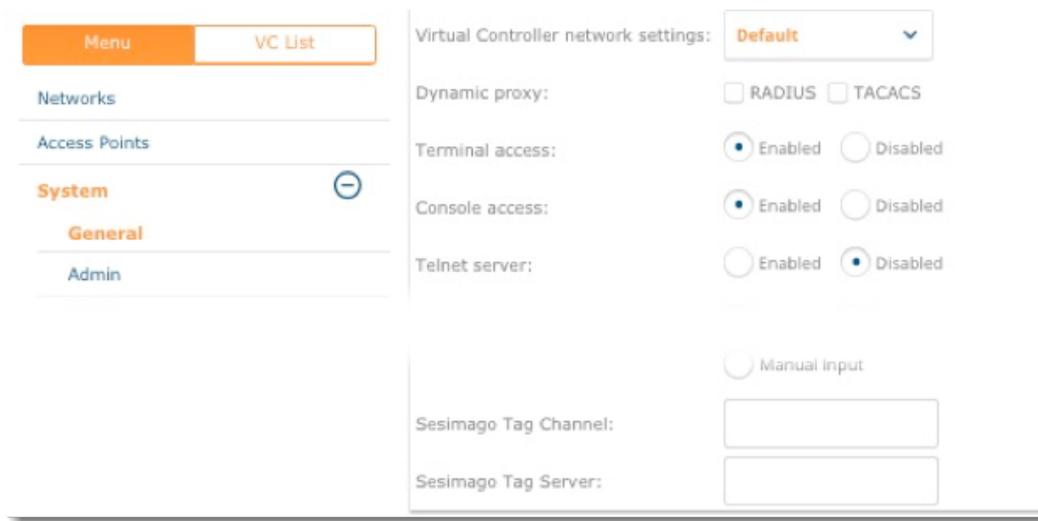
Configuring GPS for Cellular Uplink Profiles

To configure GPS for cellular uplink profiles, complete the following steps:

1. Go to **Groups > List** and select the group.

2. Click **Instant Config**.

3. Click the **System** accordion.

4. Click **Uplink**.

   The **Uplink** page is displayed.

5. In **Cellular GPS/Modem GPS**, click **Enabled** to configure GPS for cellular uplink profiles.

6. Click **Save**.

NOTE

To configure GPS for cellular uplink profiles, ensure that the modem is connected to the Instant Access Point (IAP).

In OV3600, the Aruba USB LTE Modem is automatically applied as the primary uplink when the Ethernet uplink fails. To maintain connectivity with OV3600 when the cellular uplink is automatically applied as the primary uplink, ensure that OV3600 is configured with a public IP address or IAP is configured with a VPN.

DHCP Configuration

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

To configure a centralized scope, complete the following steps:

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

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

Enabling MU-MIMO uplink for 6 GHz Radio Bands

The **RF** > **Radio** page allows you to configure the MU-MIMO uplink for 6 GHz radio bands. It allows multiple clients connected to the Instant AP (IAP) to send acknowledgment responses simultaneously resulting in improved network throughput and efficiency.

To configure the MU-MIMO uplink, complete the following steps:

1. Go to **Groups > List** and select the group.
2. Click **Instant Config**.
3. Click the **RF** accordion.
4. Click **Radios**.

   The **Radios** page is displayed.
5. Click **6 GHz band**.
6. In the **New 6 GHz band** window, click **Enabled** to enable the MU-MIMO uplink.
7. Click **Save**.

> **NOTE**
>
> The **6 GHz band** is applicable only for AP-655.

OV3600 Configuration

The **AirWave** configuration menu on this page contains a number options that allow OV3600 to automatically make changes to the following settings on any virtual controller connected to the OV3600 server.

- **Auto-configure Virtual Controller**—Selecting **Yes** allows OV3600 to automatically push configuration to new virtual controllers when the are added to the group.

- **Allow Configuration of Country Code**—Selecting **Yes** allows you to manually configure the country code for the group under **IGC > Settings > General > Country Code**. When No is selected, the previously described field is grayed-out. This is set to **No** by default.

- **Allow configuration of OV3600 Settings**—Selecting **Yes** allows you manually configure the OV3600 field under **IGC > Settings > Admin**. When **No** is selected, the previously described field is grayed-out and OV3600 pushes this information to each virtual controller in the group. This is set to **No** be default.

- **Policy Version** and **Copy policy from group**—These options cannot be executed at the same time.
  - **Policy Version**—This displays the current policy version, and when selected, allows you to select another from the drop-down menu.
  - **Copy policy from group**—When selected, this option allows you to copy the policy from another group.

Virtual Controller Configuration

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

Figure 24 *e Focus*
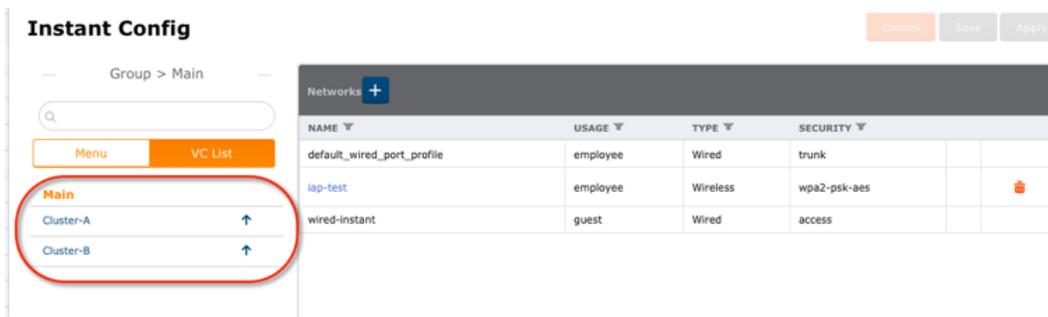
Network Configuration

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

Default Wired Port Profile

If the wired clients are to be supported on the Instant APs, configure wired port profiles and assign these profiles to the ports of an Instant AP. The wired ports of an Instant AP allow third-party devices such as VoIP phones or printers (which support only wired port connections) to connect to the wireless network.

A default wired port profile allows you to connect the Instant APs to the uplink ports of a switch. Airwave now allows you to edit the settings of a default wired port profile.

To edit a default wired port profile, complete the following steps:

1. Go to **Groups > List** and select the group.

2. Click **Instant Config**.

3. In the **Networks** pane, click the icon to edit the default wired port profile.

4. Edit any profile setting.

5. Click **Apply** for the changes to take effect.

> **NOTE** Airwave supports editing of the default wired port profile in IGC from Airwave 8.2.13.1 version onwards. Airwave does not allow you to either delete or edit the name of the default wired port profile.

Multi Pre-Shared Key

Multi Pre-Shared Key (MPSK) is an enhancement to WPA2-Personal that allows device-specific and group-specific passphrases. This offers enhanced security and deployment flexibility for headless and IoT devices over traditional per-SSID, static passphrases.

For information on configuring an SSID profile, see *Configuring SSIDs and VLANs for Device Groups* chapter in latest **OV3600 User Guide.**

Configuring an MPSK Local Profile

MPSK Local allows the user to configure 24 PSKs per SSID locally on the device. These local PSKs would serve as an extension of the base MPSK functionality.

To configure an MPSK Local profile, complete the following steps:

1. Go to **Groups > List** and select the group.

2. Click **Instant Config**.

3. Click **Security** tab.

4. Click **MPSK Local** accordion.

5. In the **MPSK Local** window, click **+** and enter a name for the MPSK Local profile.

6. To create an MPSK Local passphrase, click **+** and enter the following information in the **MPSK Local Passphrase** window, and then click **OK**.

a. Name—Enter a name.

b. Passphrase—Enter a passphrase.

c. Retype Passphrase—Retype the passphrase to confirm.

d. Role—Select a user role from the drop-down list.

7. In the **MPSK Local Passphrase** window, select an MPSK Local passphrase name, and then click **OK**.

8. Click **Save**.

> **NOTE** Each MPSK local profile must have a distinct passphrase. The passphrase must be between 8 to 16 characters.

Enabling an MPSK Local for Wireless Networks

To enable MPSK Local for wireless networks, complete the following steps:

1. Go to **Groups > List** and select the group.

2. Click **Instant Config**.

3. Click **Networks** tab.

4. Click **+ New Network** to create a new SSID. To modify an existing SSID, click on a wireless SSID from the **Wireless SSIDs** list.

5. Click the **Security** tab.

6. Select **Personal** from the **Security Level**. The authentication options applicable to the personal network are displayed.

7. From the **Key Management** drop-down list, select the **MPSK Local** option.

8. From the **MPSK Local** drop-down list, select an MPSK Local profile.

9. Click **Save**.

> **NOTE**
>
> MPSK Local feature is supported in IGC from OmniVista 3600 Air Manager 8.2.14.1 version onwards, and the device firmware version 8.7.0 or later. You cannot select an MPSK Local profile in IGC from the MPSK Local drop-down list if the device firmware version is less than 8.7.0.

Editing an MPSK Local Profile

To edit an MPSK Local profile, complete the following steps:

1. Go to **Groups > List** and select the group.

2. Click **Instant Config**.

3. Click **Security** tab.

4. Click **MPSK Local** accordion.

5. In the **MPSK Local** table, select an MPSK Local profile that you want to edit, and then click the edit icon.

6. In the **MPSK Local Passphrase** table, click **+** and enter the following information to add a new MPSK Local passphrase, and then click **OK**.

a. Name—Enter a name.

b. Retype Passphrase—Retype the passphrase to confirm.

c. Role—Select a user role from the drop-down list.

d. Passphrase—Enter a passphrase.

7. Click **OK**.

8. Click **Save**.

Deleting an MPSK Local Profile

To delete an MPSK Local profile, complete the following steps:

1. Go to **Groups > List** and select the group.

2. Click **Instant Config**.

3. Click **Security** tab.

4. Click **MPSK Local** accordion.

5. In the **MPSK Local** table, select an MPSK Local profile that you want to delete, and then click the delete icon.

6. Click **Save**.

MPSK and WPA3-CNSA Configuration

1. Click + to add a network.

2. Enter the network name, or SSID, then click **Next**.

3. In the Security tab, select one of the following **Key management** options:
    - **MPSK-AES**. Personal security settings for employee and voice users.
    - **WPA3 Enterprise (CNSA)**. Enterprise security settings for the employee and voice network SSID profiles

4. Select the authentication server.

5. Enter the RADIUS re-authentication interval in minutes.

6. Click **Apply**. OV3600 updates the **Network** page with the network profile.

Intelligent Power Monitoring

The Intelligent Power Monitoring (IPM) feature actively measures the power utilization of an AP and dynamically adapts to the power resources. IPM allows you to define the features that must be disabled to save power, allowing the APs to operate at a lower power consumption without hampering the performance of the related features. This feature constantly monitors the AP power consumption and adjusts the power saving IPM features within the power budget.

IPM dynamically limits the power requirement of an AP as per the available power resources. IPM applies a sequence of power reduction steps as defined by the priority definition until the AP functions within the power budget. This happens dynamically as IPM constantly monitors the AP power consumption and applies the next power reduction step in the priority list, if the AP exceeds the power threshold. To manage this prioritization, you can create IPM policies to define a set of power reduction steps and associate them with a priority. The IPM policies, when applied to the AP, are based on IPM priorities, where the IPM policy can be configured to disable or reduce certain features in a specific sequence to reduce the AP power consumption below the power budget. IPM priority settings are defined by integer values, where the lower values have the highest priority and are implemented first.

> **NOTE**
> The Intelligent Power Monitoring feature is supported in IGC from Airwave 8.2.13.1 version onwards, and the device firmware version 6.5.3 or later.

To configure Intelligent Power Monitoring, complete the following steps:

1. Go to **Groups > List** and select the group.

2. Click **Instant Config**.

3. Click the **System** accordion.

4. Click **IPM**.

5. Select the **IPM Activation** check-box to enable IPM.

6. Click the **+** icon in the **IPM Power Reduction Steps With Priorities** pane.
    The **IPM Power Reduction Steps With Priorities** window is displayed.

7. In the **IPM Step Priority** field, enter a value from 1 to 16 to define IPM priority.

8. From the **IPM Step** drop-down list, select a setting as described in the following table:

Table 4: *Intelligent Power Monitoring Step Parameters*

Parameters	Description	Validated From
cpu_throttle_25	Reduces CPU frequency to 25% of normal.	6.5.3.0
cpu_throttle_50	Reduces CPU frequency to 50% of normal.	6.5.3.0
cpu_throttle_75	Reduces CPU frequency to 75% of normal.	6.5.3.0
disable_alt_eth	Disables the second Ethernet port.	6.5.3.0
disable_pse	Disables Power Sourcing Equipment (PSE).	6.5.3.0—8.7.1.0
disable_usb	Disables USB.	6.5.3.0
radio_2ghz_chain_1x1	Reduces 2 GHz chains to 1x1.	6.5.3.0
radio_2ghz_chain_2x2	Reduces 2 GHz chains to 2x2.	6.5.3.0
radio_2ghz_chain_3x2	Reduces 2 GHz chains to 3x3.	6.5.3.0
radio_2ghz_power_3dB	Reduces 2 GHz radio power by 3 dB from the maximum value.	6.5.3.0
radio_2ghz_power_6dB	Reduces 2 GHz radio power by 6 dB from the maximum value.	6.5.3.0
radio_5ghz_chain_1x1	Reduces 5 GHz chains to 1x1.	6.5.3.0
radio_5ghz_chain_2x2	Reduces 5 GHz chains to 2x2.	6.5.3.0
radio_5ghz_chain_3x3	Reduces 5 GHz chains to 3x3.	6.5.3.0
radio_5ghz_power_3dB	Reduces 5 GHz radio power by 3 dB from the maximum value.	6.5.3.0
radio_5ghz_power_6dB	Reduces 5 GHz radio power by 6 dB from the maximum value.	6.5.3.0
disable_pse1	Disables Power Sourcing Equipment 1 (PSE1).	8.8.0.0
disable_pse2	Disables Power Sourcing Equipment 2 (PSE2).	8.8.0.0
radio_6ghz_chain_1x1	Reduces 6 GHz chains to 1x1.	8.9.0.0
radio_6ghz_chain_2x2	Reduces 6 GHz chains to 2x2.	8.9.0.0
radio_6ghz_chain_3x3	Reduces 6 GHz chains to 3x3.	8.9.0.0
radio_6ghz_power_3dB	Reduces 6 GHz radio power by 3 dB from the maximum value.	8.9.0.0
radio_6ghz_power_6dB	Reduces 6 GHz radio power by 6 dB from the maximum value.	8.9.0.0

9.

10. Click **OK**.

    The **IPM Power Reduction Steps With Priorities** table in the **IPM** section lists all the IPM settings.

11. Click **Apply** for the changes to take effect.

OV3600 Settings

The **OV3600** menu in IGC provides options to view configuration history, configuration mismatches, and AP events, as well as, settings that dictate how OV3600 interacts with OAW-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.

AP Events

The **AP Events** page provides a list of events pertaining to the selected virtual controller since being discovered by OV3600.

Figure 25 *OV3600 > AP Events*
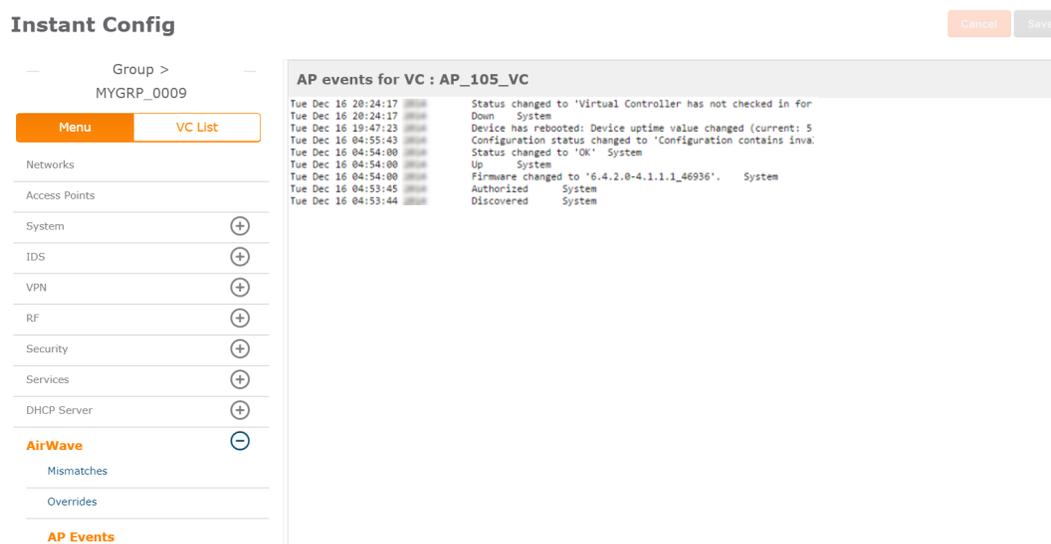
Config History

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

Figure 26 *OV3600 > 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 OV3600 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.

Alcatel-Lucent Instant in OV3600 8.2.14.1 | Deployment Guide

Figure 27 *OV3600 Settings (VC Selected)*

Without A Virtual Controller Specified

This page contains a number options that allow OV3600 to automatically make changes to certain settings on any virtual controller connected to the OV3600 server.

■ **Auto-configure Virtual Controller** - Selecting **Yes** allows OV3600 to automatically push configuration to new virtual controllers when the are added to the group.

■ **Allow Configuration of Country Code**: Selecting **Yes** allows you to manually configure the country code for the group under **IGC > Settings > General > Country Code**. When No is selected, the previously described field is grayed-out. This is set to **No** by default.

■ **Allow configuration of OV3600 Settings**: Selecting **Yes** allows you manually configure the OV3600 field under **IGC > Settings > Admin**. When **No** is selected, the previously described field is grayed-out and OV3600 pushes this information to each virtual controller in the group. This is set to **No** be default.

■ **Hashed Management Password (Enable only)**: Starting from Instant version 4.3, you can enforce hashing of management user's passwords. A hashed password is more secure than an encrypted password the reason being, encrypted password can be decrypted back but hashed password cannot be reversed back to original text. Selecting **Yes** allows you to enable the **Hashed Management Password (Enable only)** and cannot see the management password in plain text. Selecting **No** allows you to see the management password in plain text in running configuration using *show running-configuration no-encrypt*.

- **Policy Version** and **Copy policy from group**: These options cannot be executed at the same time.
  - **Policy Version**: This displays the current policy version, and when selected, allows you to select another from the drop-down menu.
  - **Copy policy from group**: When selected, this option allows you to copy the policy from another group.

Figure 28 *OV3600 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.

- *Alcatel-Lucent Instant 8.10.0.0 User Guide*
- *OV3600 8.2.14.1 Release Notes*

The following additional tasks can be completed in OV3600. These include configuration and monitoring tasks.

- Resolving Mismatches
- Enabling the OAW-IAP Role
- Monitoring Devices
- Running Config Backups
- Running Commands

Resolving Mismatches

After adding a device, the new device will appear in OV3600 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 OV3600 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
- Resolving Mismatches when Instant Config is Enabled

Resolving Mismatches when Instant Config is Disabled

When Instant Config is disabled, configuration for OAW-IAP devices is done via the Instant UI. In this case, OV3600 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 OV3600 IP address, shared secret, and organization string has to be provisioned on the Instant device.

Figure 29 *Devices > Audit page*

Perform the following steps to resolve the mismatch.

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

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

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

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

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

Resolving Mismatches when Instant Config is Enabled

In Instant Config, mismatches are indicated with a red, unequal symbol (≠) beside the device name. Click on the device name, then navigate to **OV3600 > Mismatches** to view the details for mismatch. Click **Apply All** at the bottom of the page to resolve the mismatches.

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

Figure 30 *Viewing mismatches in Instant Config*
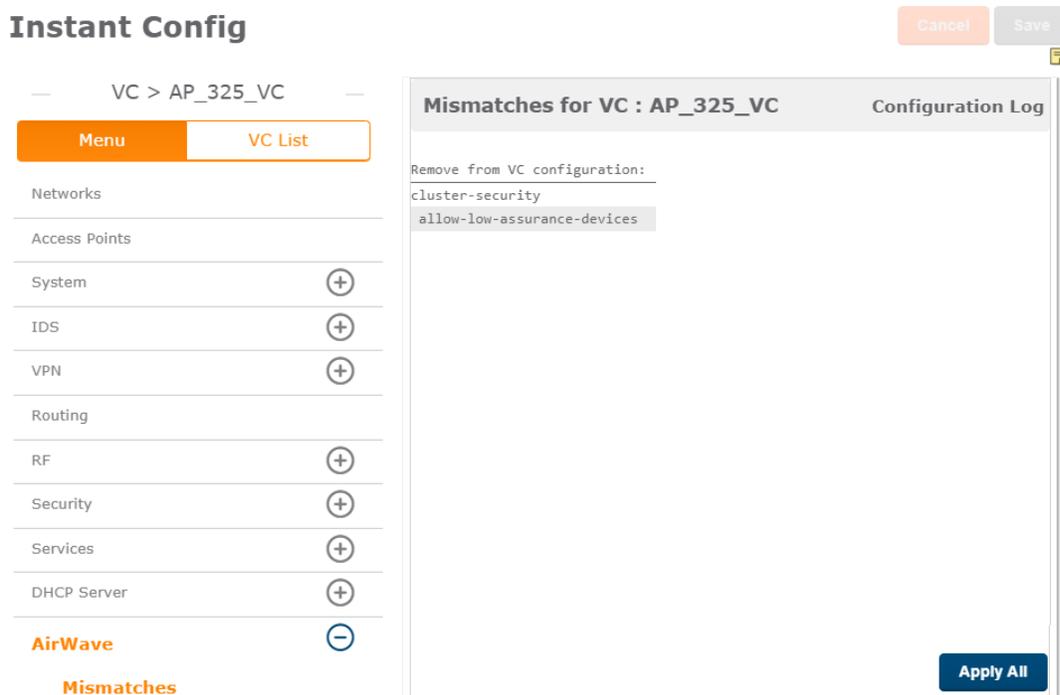
Enabling the OAW-IAP Role

As shown previously, new OAW-IAP devices can be added to OV3600 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 OAW-IAP role.

1. Enable the newly created Admin User Role in **OV3600 Setup > Roles**, as shown in Figure 31.

Figure 31 *Enable Admin User Roles in OV3600 Setup > Roles*

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

> **NOTE**
> The auto-created template is most useful if the first Virtual Controller for the top-level Organization String is fully configured on-site *before* it is pointed at OV3600 in the Virtual Controller's UI.

3. Evaluate, approve, or ignore incoming Virtual Controllers with a different top level Organization String and/or Shared Secret in the **Devices > New** list. Subsequent OAW-IAP are auto-authorized if they have an Organization/Shared Secret key that matches the Shared Secret key of any existing authorized Virtual Controller in the top-level Organization String.

4. Set the initial Virtual Controller to **Manage Read/Write** mode and push the good configuration to the subsequent OAW-IAPs.

5. Set up OV3600 users to have access to specific folders, if desired.

Monitoring Devices

Use the **Devices > Monitor** page to monitor your Instant devices. OV3600 provides you with detailed information for your virtual controller, APs, and radios. This information includes spectrum interferers, rogue clients, and channel utilization. The image below shows an example of radio statistics.
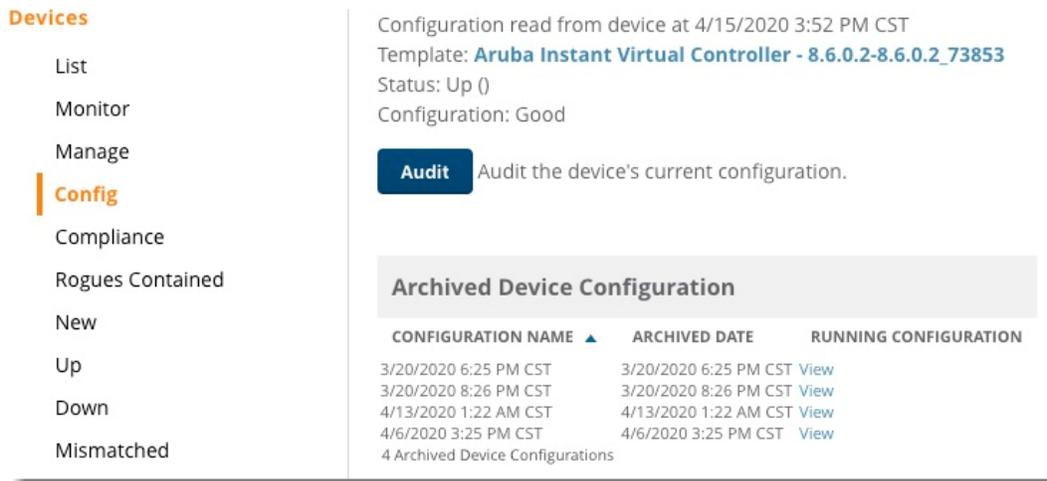
Figure 32 *Monitoring Radios*
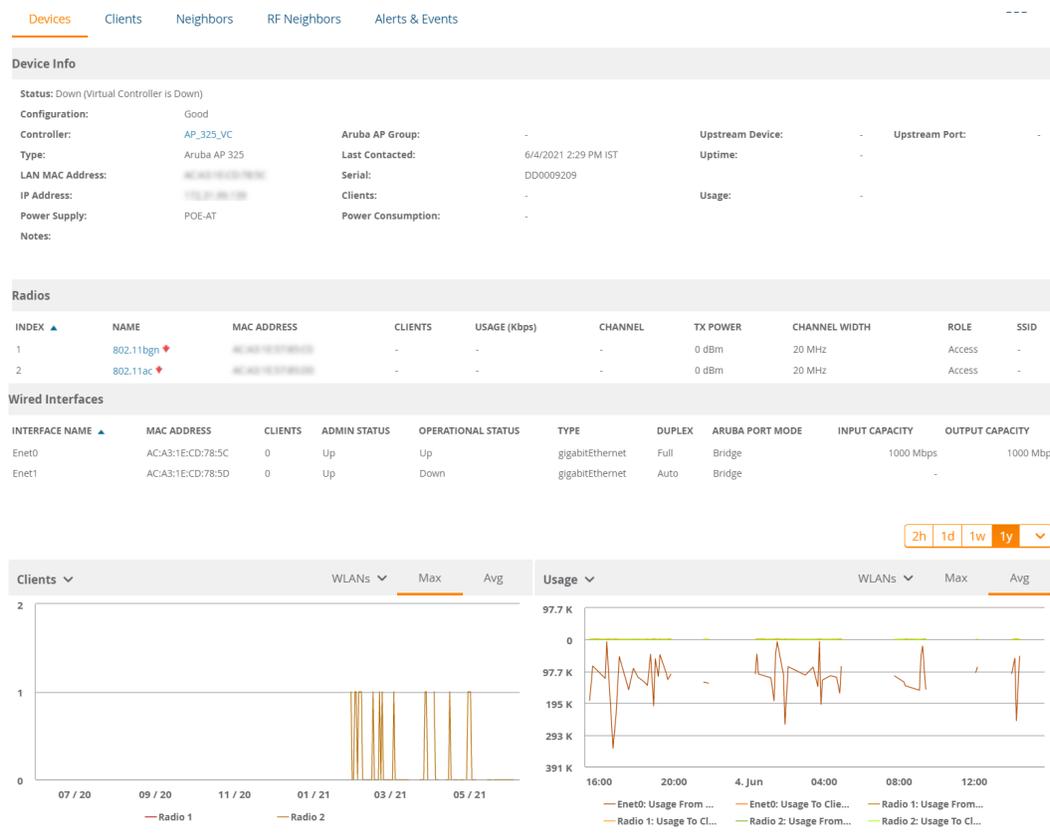
Running Config Backups

When a configuration change is made from the WebUI or CLI, OV3600 runs a backup and archives the device configuration on the **Devices > Config** page. You can use the device configuration for audits and data recovery.

**Figure 33** *Archived Device Configuration for Instant APs*

Running Commands

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

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

Figure 34 *Selecting a Command for a VC*
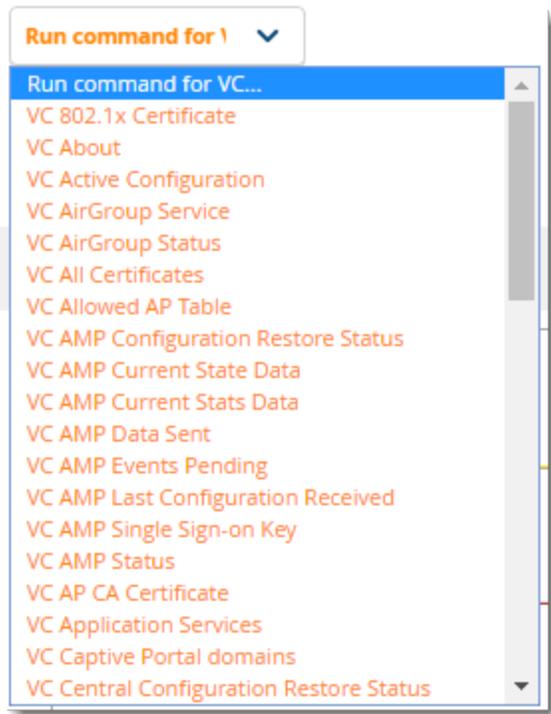
This section describes some best practices to follow when using OV3600 to monitor and configure Instant devices. It also includes some known issues to take into consideration when using OV3600. This list is inclusive of the OV3600 release notes and Instant release notes.

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 OV3600.
- 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 OAW-IAP device's configuration through the Instant user interface, we recommend that you put the device in Manage Mode, and then use the **Import Settings** button from the **Devices > Manage** page. When using this method instead of Instant Config, you can import settings and update the template from a single page. Import the settings and then wait approximately a minute. If you find that you need to also update the template, the **Devices > Manage** page for the Virtual Controller provides a link to quickly access the template.

Known Issues with the Instant Integration with OV3600

- If the Organization String configured on the Instant device is different than what is statically written in the template, OV3600 will overwrite the configured Organization String to match the template.
- The Instant primary device sends an update message to OV3600 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 OV3600 is down.