Aruba Central

aruba

a Hewlett Packard
Enterprise company

User Guide

Copyright Information

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett-Packard Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett-Packard Company

Attn: General Counsel

3000 Hanover Street

Palo Alto, CA 94304

USA

Please specify the product and version for which you are requesting source code. You may also request a copy of this source code free of charge at dl-gplquery@arubanetworks.com.

Chapter 1
About this Guide

This user guide describes the features supported by Aruba Central and provides detailed instructions to set up and configure devices such as IAPs and Switches.

Intended Audience

This guide is intended for system administrators who configure and monitor their wireless network using Central.

Related Documents

In addition to this document, the Central product documentation includes the following documents:

- *Aruba Central Getting Started Guide*
- *Aruba Central Online Help*
- *Aruba Central Release Notes*

Conventions

The following conventions are used throughout this guide to emphasize important concepts:

Table 1: *Typographical Conventions*

Type Style	Description
Italics	This style is used to emphasize important terms and to mark the titles of books.
`System items`	This fixed-width font depicts the following: ● Sample screen output ● System prompts

The following informational icons are used throughout this guide:

NOTE

Indicates helpful suggestions, pertinent information, and important things to remember.

CAUTION

Indicates a risk of damage to your hardware or loss of data.

WARNING

Indicates a risk of personal injury or death.

Contacting Support

Table 2: *Contact Information*

Main Site	arubanetworks.com
Support Site	support.arubanetworks.com
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephone	arubanetworks.com/support-services/contact-support/
Software Licensing Site	licensing.arubanetworks.com
End-of-life Information	arubanetworks.com/support-services/end-of-life/
Security Incident Response Team (SIRT)	Site: arubanetworks.com/support-services/security-bulletins/ Email: sirt@arubanetworks.com

Chapter 2
Aruba Central Overview

Aruba Central is a cloud-based platform that enables you to manage your Aruba wireless network. Designed as a software-as-a-service (SAAS) subscription, Central provides a standard web-based interface that allows you to configure and monitor multiple Aruba Wi-Fi networks from anywhere, provided you have an Internet connection.

Central offers the following key features:

- Streamlined management of devices
- Dashboard view of network and client health
- Easy grouping of devices
- Centralized configuration and firmware updates
- Guest Wi-Fi access configuration
- Reporting
- Remote troubleshooting and client information
- API gateway to manage APIs

Supported Devices

Central supports the following Access Points (APs) and Switch platforms.

Supported IAPs

The current release of Central supports the following IAP platforms:

- IAP-324/325
- IAP-277
- IAP-228
- IAP-205H
- IAP-103 Series
- IAP-114/115
- IAP-204/205
- IAP-214/215
- IAP-274/275
- IAP-224/225
- RAP-3WN/3WNP
- RAP-108/109
- RAP-155/155P
- IAP-175P/175AC
- IAP-134/135
- IAP-104/105
- IAP-92/93

Supported IAP Versions

The current release of Central supports only the following IAP firmware versions:

- 6.4.2.0-4.1.1.9 or later
- 6.4.2.3-4.1.2.3
- 6.4.3.1-4.2.0.3
- 6.4.3.4-4.2.1.0
- 6.4.4.3-4.2.2.0
- 6.4.4.4-4.2.3.0
- 6.4.4.4-4.2.3.1
- 6.4.4.4-4.2.3.2
- 6.4.4.6-4.2.4.0

Supported Switches

The following sections list the Switch models supported in Central.

New Switch Platforms

- Aruba 2920 Switch Series
- Aruba 2930F Switch Series

Supported Firmware Versions

Central supports the following firmware versions on Aruba switches:

- Aruba 2920 Switch Series—WB.16.02.0010 or later
- Aruba 2930F Switch Series—WC.16.02.0010 or later

Legacy Aruba Switch Platforms

Central also supports the following legacy Switch models:

- S1500-12P
- S1200-24P
- S2500-24P
- S3500-24T

Supported Firmware Versions

The following ArubaOS software versions are supported on the legacy Switch platforms:

- 7.3.2.6
- 7.4.0.3
- 7.4.1.4

Subscription and Licenses

Central feature availability is based on the following license terms:

- If you have purchased only the IAP license, only the information related to the IAPs and IAP configuration pages are available in the Central UI.
- If you have purchased only the Switch license, only the information related to the Switches and the Switch configuration pages are available in the Central UI.

- If you have purchased both the IAP and the Switch licenses, both the IAP and Switch configuration pages are available in the Central UI.

For more information on obtaining and activating your subscriptions, see *Aruba Central Getting Started Guide*.

Accessing Central UI

You can access Central using a standard web browser from a remote management console or workstation and launch it using any of the following browsers:

Table 3: *Browser Compatibility Matrix*

Browser Versions	Operating System
Google Chrome 39.0.2171.65 or later	Windows and Mac OS
Mozilla FireFox 34.0.5 or later	Windows and Mac OS
Internet Explorer 11	Windows
Internet Explorer 10	Windows
Safari 8	Mac OS
Safari 7	Mac OS
Safari 5.1.7	Windows

NOTE

To view the Central UI, ensure that JavaScript is enabled on the web browser.

Setting up Customer Accounts

Central offers a 90-day evaluation license for customers who want to try the Aruba cloud solution for managing their Wi-Fi networks. When you create an account with Central, an evaluation license is automatically assigned, unless you have a paid subscription. To obtain license keys, contact the Aruba IT team.

Signing up for Aruba Central

To sign up as a customer for Central:

1. Go to http://www.arubanetworks.com/products/sme/eval/.
2. Enter your email address and click **Continue**.

- If you are signing up for Central for the first time, the registration page is displayed. Complete the registration process (see step 3 through step 8).
- If you are an existing customer and your email address is already in the Central database, and you have verified your email address, the Central login page is displayed.
- If your email address already exists in the Central database and you have not verified your email address, click **Resend Verification Email** and verify your email address by clicking the **Activate Your Account** link.
- If you are an existing Aruba customer with SSO login credentials and you are signing up for Central for the first time:
  - Validate your account by providing your SSO password. On successful authentication, the registration page is displayed. Complete the registration process to gain access to Central (see step 3 through step 8).
  - If you have forgotten your SSO password, click **Forgot Password** and complete the steps to retrieve your password.
  - To sign up again, click **Try Signing up again** and complete the steps to sign up for an Central account.

3. On the Registration page, enter first name, last name, and address details. If you are a new user, enter the password. For registered users and those with SSO login credentials, the **Password** field is disabled.
4. If you have Aruba Activate user credentials, select **I have an Aruba Activate account** check box and enter your user name and password for the Activate account.

NOTE

You can use your Aruba Activate account to manually import devices into Central. However, Central allows each user account to import devices using Aruba Activate account only once.

5. Select the **I agree to the Terms and Conditions** check box.
6. Click **Sign Up**. On successfully completing the registration, a verification email is sent to your email address.
7. Access your email account and click the **Activate Your Account** link. If the email verification is successful, the **Log in to Aruba Central** button is displayed.
8. Click **Log in to Aruba Central** and provide your registered user name and password. If an account has multiple customers configured , the accounts selection page is displayed.
9. Select an account to access the Central dashboard.

NOTE

When you sign up for Aruba Central, a user account on Aruba Centraland Aruba Activate is created.

Binding Devices to Your License

After you successfully log in to Central, a welcome message is displayed in the Central UI. To bind devices to your license, click **Manage Your License**. The **Device Management** pane is displayed. To view the subscription key details before binding devices, click **Subscription Keys**.

Central supports zero touch provisioning of the devices. It automatically retrieves the devices associated with your license and Central subscription. However, if the retrieval of devices is not complete or successful due to process errors, you can manually add the devices.

Central allows you to import devices using your Aruba Activate user credentials, the MAC address and cloud activation key of a device, or the MAC address and Serial Number of a device. You can specify the method for importing devices when adding a device.

For users with the evaluation subscription, the devices are not automatically synchronized. Therefore, the users must manually add the devices.

NOTE

The evaluation subscription key allows you to add only five IAP devices and two Aruba Switches.

For IAPs that dynamically form a cluster, the users must add the master IAP from the **Device Management** page every time a slave IAP joins the cluster, so that the slave IAP details are synchronized.

To manually add a device:

1. In the **Device Management** page, click **Add Devices**. The **Manually Add Devices** window opens. Select one of the following device addition options:

Table 4: *Adding Devices*

Device Addition Option	Description
Aruba Activate Credentials	To retrieve all devices associated to an Activate user account: 1. Select **Aruba Activate Credentials** from the **Add devices using** drop-down list. 2. Enter the username and password of the Activate user account. 3. Click **Next**. The Activate account details and the total number of devices associated with this account are displayed. 4. To add all devices, click **Add <Number> Devices** button. The devices associated with the Activate account are retrieved and added to the list of devices displayed on the **Device Management** page. **NOTE:** You can use this option only once. After the devices are added, Central does not allow you to modify or re-import the devices using your Aruba Activate credentials.
Bulk addition of devices based on cloud activation key	To retrieve multiple devices from a single purchase order by providing the cloud activation key: 1. Note the Cloud Activation Key and MAC address of the device. To obtain these details: ● For IAPs, execute the **show about** command at the IAP CLI or click **Maintenance** >**About** in the IAP UI. ● For legacy Switches, execute the **show inventory | include HW** and **show version** commands on the Switch CLI. ● For the other ArubaSwitches, to view the MAC address and the serial number, run the **sh system | in Base** and **sh system | in Serial** commands at the CLI. You can also view the cloud activation key in the **Maintenance** > **About** tab of the switch UI. The activation key is enabled only if the Switch has access to the Internet. 2. Select **Cloud Activation Key** from the **Add devices using** drop-down list. 3. Enter the **MAC address** and **Cloud Activation Key** of the device. 4. Click **Next**. Central retrieves all devices that belong to the same purchase order and displays the list. A list of blocked devices is displayed if any of the device belongs to another customer account or is used by other services. As Central does not allow you to add blocked devices, you may have to release the blocked devices from another customer account. 5. To continue adding devices, click **Add <x> Devices**. 6. To restart the device addition procedure, click **Start Again**.
Adding up to 32 devices	To manually add devices by using the serial number and MAC address of the device: 1. Select **Device List (Up to 32 Devices)** from the **Add device using** drop-down list. 2. Enter the MAC address and serial number of the device. 3. Click **Next**. The list of available devices is displayed. 4. Click **Add <x> Devices**. **NOTE:** Central allows you to add up to 32 devices.

5. To assign a license to the device, select the device and click **Assign License(s)**.

NOTE

The provisioning of the legacy Aruba Switch fails when the provisioning process is interrupted during the initial booting and if the switch has a static IP address with no DNS server configured.

During Zero Touch Provisioning, the ArubaSwitches can join Central only if they are running the factory default configuration, and have a valid IP address and DNS settings from a DHCP server.

Adding User Accounts

To add user accounts to your license, complete the following steps:

1. Click **Maintenance > User Management**.
2. On the **User Management** pane, click **Add User**. The **Create User** window is displayed.

3. Enter the email address of the user in the **Username** text box.

4. From the **User Scope** drop-down list, select the group to which you want to assign the user.

5. Select the user access level that you want to assign to the user from the **Access Level** drop-down list.

Central supports following types of users:

- **Admin**—The Admin users have full access to all the groups and have special rights to create or update user details, groups, and to provision devices.
- **Read/Write**—The users with read/write privileges can access the groups or devices assigned by the Admin user. The users with Read/Write privileges can perform operations that can change the behavior of devices or groups such as modifying the configuration of a device, deleting a device and so on.
- **Read only**—The users with read-only privileges can access the groups or devices assigned by the Admin user and view details of the groups and devices.
- **Guest operator**—The guest operators have access to guest management operations only. These users can add guest users and configure splash page profiles.

NOTE

A user cannot have different access rights for different groups.

6. Click **Save**. When the user account is successfully created:

- New users will receive a welcome email with the registration link. Complete the registration steps described in step 7 through step 11.
- Users with an existing Central account will receive an email invite with a link to the Central portal. Click the link to access the Central UI.

NOTE

If the user has not received the registration email, click **Resend Invite Email** in the **User Management** pane to resend the invite.

7. To register, click **Register Your Account** link. The **Sign up with Aruba Central** page is displayed.

8. Enter the password, , first name, last name, and address details.

9. Select a country and state.

10. Select the **I agree to the Terms and Conditions** check box.

11. Click **Sign Up**. On successful completion of registration, the user account is created.

12. Log in to Central with the registered credentials.

You can also enable two-factor authentication for the users associated with a specific customer account. For more information on two-factor authentication, see Two-Factor Authentication on page 150.

Creating Additional Customer Accounts

If you want to manage Wi-Fi networks in multiple regions, you can create additional customer accounts. Central allows you to create up to five customer accounts.

To create an additional customer account:

1. Click the **Settings** icon next to your user name on the main pane. Click **Switch Customer**. The customer account selection page is displayed.

2. Click the + icon to add a new account. The **Sign up with Aruba Central** page is displayed.

3. Enter your address, and select the country and state.

4. Enter the city and ZIP code details.

5. Select the **I agree to the Terms and Conditions** check box.

6. Click **Sign Up**. The customer account is added.

7. Repeat the procedure to add another customer account.

To log in with a different customer account, click **Switch Customer** and click the account that you want to access.

This chapter describes the following topics:

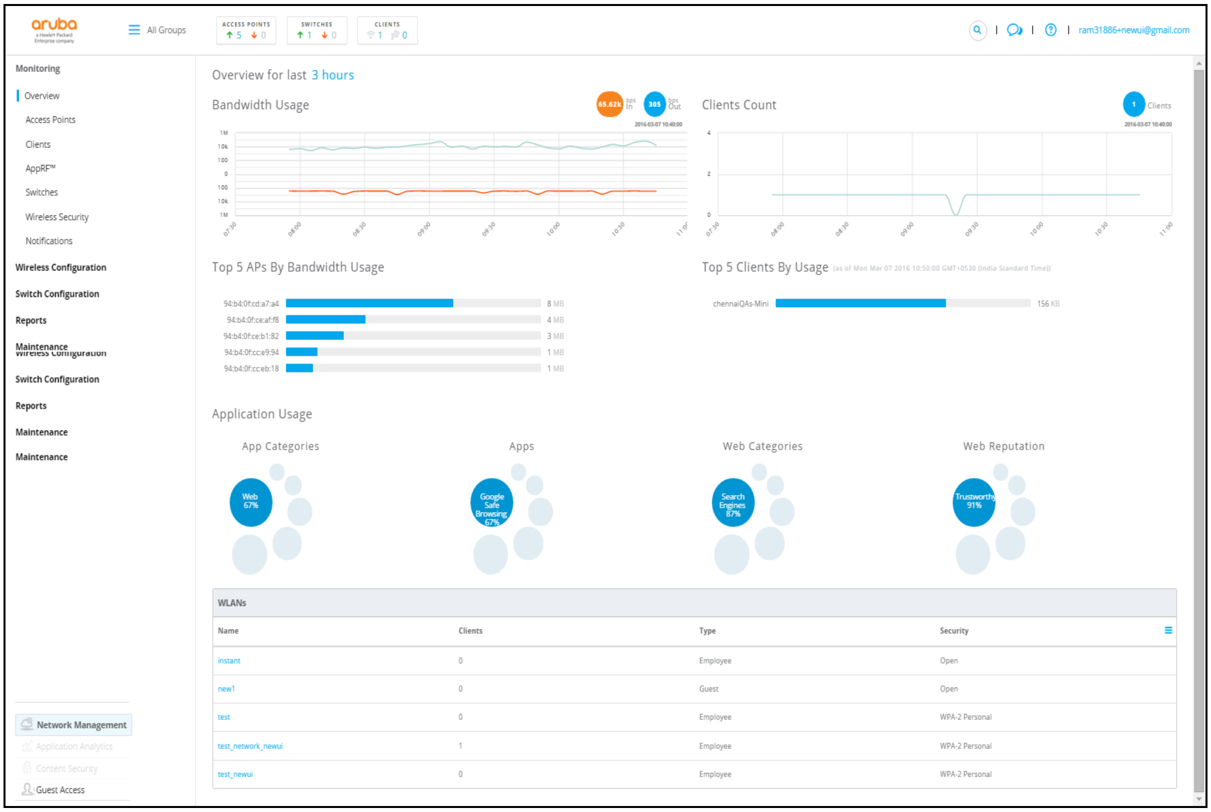
- Main Window
- Header Pane
- Left Navigation Pane
- Data Pane
- Other UI Elements and Functions

Main Window

After you log in to Central, the Central main window displays monitoring dashboard.

Central Main Window shows the Central main window.

Figure 1 *Central Main Window*



WLANs

Name	Clients	Type	Security
instant	0	Employee	Open
new1	0	Guest	Open
test	0	Employee	WPA-2 Personal
test_network_newui	1	Employee	WPA-2 Personal
test_newui	0	Employee	WPA-2 Personal

The main window consists of the following elements:

- Header Pane
- Left Navigation Pane
- Data Pane
- Other UI Elements and Functions

Header Pane

The header area of the main window displays the following information:

- Company Logo—On clicking the logo, the monitoring dashboard is displayed.
- Group selection—The group settings icon allows you to perform the following actions:
  - To view the existing groups, click Groups icon.
  - To add a new group or to manage devices in the existing, click the edit icon next to **All Groups**.
  - Search for devices based on all the labels.
  - View unprovisioned devices.

For more information on groups, see Managing Groups on page 27.

- The number and of APs, switches, and clients.
  - **Access Points**—Displays the **Access Points** page on clicking the arrows. Click the up arrow to view the APs that are up and down arrow to view the APs that are down.
  - **Switches**—Displays the **Switches** page when on clicking the arrows. Click the up arrow to view the switches that are up and down arrow to view the switches that are down.
  - **Clients**—Displays the **Clients** page on clicking the wired and wireless icons.
- The Search icon—On clicking the search icon, a **Search** box opens. The search box allows administrators to search devices, clients , or a specific network. When you enter a text string in the search box, the search function suggests matching keywords and automatically completes the search text entry.
- The Callout icon—Displays the following options:
  - **Documentation**—Lists latest versions of Central user documentation, including the User Guide, Getting Started Guide, and What's New documents.
  - **Support**—Directs you to the Aruba support community site for troubleshooting support.
- The Help icon—Click the **Help** icon to view a short description or definition of the selected terms and fields in a pane or dialog box. To view the online help:

  a. Click the **(?)** at the top right corner of Central main window. The data pane items are displayed in green color.

  b. Move your cursor over a data pane item to view the help text.

  c. To disable the help mode, click **(?)** again.
- A drop-down menu for managing user and customer accounts. This menu includes the following commands:
  - **Switch Customer**—Allows you to switch to another customer account. For more information, see Creating Additional Customer Accounts on page 19.
  - **Change Password**—Allows you to change the password of account.
  - **User Settings**—Displays the date, time and timezone. The administrators can also set a language preference and a timeout value for inactive user sessions.

NOTE

The Central UI is available in English, French, and Spanish. You can now set your language preference through the **User Settings** menu from the drop-down list on the header pane. Central saves your language preference setting and displays the UI in the language set by you.

  - **Managed Service Mode**—Enables Managed Service mode and switches the interface to the Managed Service Portal. For more information on the Managed Service portal, see *Aruba Central Managed Service Portal User Guide*.
  - **Logout**—Allows you to log out of your Aruba Central account.

Left Navigation Pane

The top left navigation pane consists of the function tabs. The contents on the top left navigation pane change dynamically based on the menu option selected in the **Aruba Central Apps** area at the bottom left pane.

For example, clicking on **Network Management** from the **Aruba Central Apps** area displays the function tabs for network monitoring, device configuration, and management. Similarly, clicking on **Guest Access** or **Present Analytics** displays the menu options for guest network configuration and presence analysis respectively.

The **Aruba Central Apps** area also displays the **General** option. Clicking on **General** displays menu options such as Labels for label assignment and management.

By default, each tab appears in a compressed view. Click the tabs to expand or collapse the tab view.

Network Management

The following menu options are displayed on clicking **Network Management** from the bottom left pane:

- Monitoring
- Configuration
- Reports
- Maintenance

Monitoring

The following menu options are available:

- **Overview**—Displays the profile, status, activity, and diagnostics details such as total number of devices and clients, number of devices that are down, and throughput to and from the client.
- **Access Points**—Provides details of the IAPs connected to Central.
- **Clients** — Provides details of the clients associated with the IAP.
- **AppRF™**—Provides a summary of client traffic to applications, application categories, websites category, and website reputation score.
- **Switches**—Provides details of the Switches connected to Central.
- **Wireless Security**—The Wireless Intrusion Detection System (WIDS) monitors the presence of unauthorized IAPs and clients.
- **Notifications**—Displays the unacknowledged notifications count at the top right corner of the Central UI.

Configuration

The **Configuration** tab allows you to configure the devices attached to a specific group or default group. It consists of the following menu options:

- **Access Points**—The **Access Points** menu allows you to configure APs, wireless or wired network profiles, Radio Frequency (RF) settings, security settings, Dynamic Host Control Protocol (DHCP) profiles, services, and system parameters.
- **Switch - MAS**—The **Switch-MAS** menu allows you to configure legacy Aruba switches such as Mobility Access Switches. You can also add or modify VLANs, ports, the DHCP, and system parameters for these switches.
- **Switch - Aruba**—The **Switch-Aruba** menu allows you to configure new Aruba switches. You can also add or modify VLANs, ports, and system parameters for these switches.

Reports

The **Reports** tab allows you to generate reports such as network summary, security, PCI compliance, client inventory, infra inventory, and client usage reports. You can also export reports and send the reports to an email account.

Maintenance

The **Maintenance** tab allows you to maintain the network and configure user credentials. It also allows you to:

- View the current firmware version of the devices and provides options to upgrade to the latest firmware version.
- View the license information such as license name, start and end dates, license capacity, and the options to add or remove the Central software license.
- View and manage devices and attach licenses to devices.
- View and manage users associated with a customer account.
- View audit trail for the events pertaining to device allocation, configuration, and firmware upgrade status.
- Run troubleshooting commands on AP devices.
- View APIs and manage OAuth tokens.

Guest Access

The following menu options are displayed on clicking **Guest Access** from the bottom left pane:

- **Splash Page**—Allows you to configure splash page profiles for guest network profiles.
- **Visitors**—Allows you create guest user accounts and assign these users to a guest SSID.

Presence Analytics

The **Presence Analytics** application provides a real-time and historical view of the user traffic patterns in public venues and enterprise environments. The application includes the following menu options:

- **Monitoring**—The Monitoring dashboard displays the following information:
  - **Presence**—Displays graphs with traffic patterns for the passer by, visitor, engaged and dwelling users.
  - **Insights**—Provides detailed statistics of user traffic patterns.
- **Settings**—Allows administrators to set RSSI thresholds to determine user engagement and classify user traffic patterns.

Label Management

The **Label Management** tab allows you to create and manage labels for devices. The labels can use used to tag devices to a location, to specific owners, or departments.

Data Pane

Displays detailed information of the tabs and data for the selected menu commands.

Other UI Elements and Functions

Central UI also includes the following UI features:

- Labels
- Variables
- Groups
- Other UI Elements and Functions

Labels

Labels are tags that can be used to filter devices for monitoring and reporting purposes. A device can have multiple labels. For example, consider an IAP labeled as **Building 25** and **Lobby**. These tags identify the location of the IAP within the enterprise campus and the building. The IAPs in other buildings can also be tagged as **Lobby** to enable all the IAPs in the lobbies of all these buildings in the campus. To filter and monitor

IAPs in the lobbies of all the campus buildings, you can tag all the IAPs in a lobby with the label **Lobby**. Labels can also be used to determine the ownership, departments, and functions of the devices.

For information on creating and assigning labels, see Labels on page 173.

Filtering Devices Assigned to a Label

To filter devices based on a specific label:

1. Ensure that **All Groups** is selected.

> The label filter cannot be applied at the individual group level. The applied filters are cleared when you move from all groups to another group.

2. Under **Enter Label to Filter** on, enter the label based on which you want to filter the devices.
3. Click **Apply Search**. The data for the devices associated to the selected label is shown in the monitoring dashboard pages.

Variables

Variables are device parameters that can be configured. Variables cannot inherit their values from the default group. These user-defined parameters are specific to a device, for example, Virtual Controller name, IP address, and VLAN.

Groups

A group consists of devices provisioned in the network. You can create multiple groups and attach devices to these groups. Central defines a group as a subset of the devices on the wireless LAN, ranging in size from one device to hundreds of devices that share some common configuration settings. For example, if one or several VCs are grouped together with a cluster of IAPs, you can configure the IAPs associated with each VC as a single unit from the Central UI. These configuration parameters are assigned with the same default value. You can quickly configure a number of IAPs using a group. The group configuration is shared across all devices. For more information on groups, see Managing Groups on page 27.

Overrides

The devices in a group share the same configuration settings. The configuration changes applied at the group level takes precedence. However, the configuration changes applied at the device levels can be preserved as well. For more information on overrides, see Managing Overrides on page 28.

This chapter describes the following topics:

Firewall Ports for Device Communication

Most of the communication between devices on the remote site and Central server in the cloud is carried out through HTTPS (TCP 443). However, you may need to configure the following ports:

- TCP port 443 for configuration and management of devices.
- TCP port 80 for image upgrade.
- UDP port 123 for NTP server to configure timezone when factory default IAP comes up.
- TCP port 2083 for RADIUS authentication for guest management. If 2083 port is blocked, the HTTPS protocol is used.

Initial Configuration of Devices

The devices can join Central with either factory default configuration or the configuration previously set by the AP administrator.

If a device joins Central with the factory default configuration, the device is moved to the default group or a pre-assigned group if any. To assign the devices to an existing group, complete the following steps:

1. Go to **Device Management** page.
2. Select the device to assign to a group.
3. Click **Assign Group**.

If the device joins Central with non-default configuration, the device is automatically assigned to an unprovisioned group. The devices in the unprovisioned group have independent configuration and do not share the common configuration settings.

If the device is in an unprovisioned group, the administrators can perform the following actions:

- Create a new group for the device and apply the existing configuration of the device to the group.
- Move the device to an existing group and apply the group configuration to the device.

If a new IAP cluster joins Central:

- If the new IAP cluster was previously a part of an existing cluster in the network, the device is assigned to the cluster group to which it belonged earlier.
- If the new IAP cluster was not associated with any existing cluster groups on Central, the device is moved to the unprovisioned group.

Importing Existing Configuration from a Device

When a pre-configured device is included in Central, it is initially listed under unprovisioned group.

To import configuration from the device:

1. Go to https://portal.central.arubanetworks.com and log in with your user credentials.
2. Ensure that the device is connected to the wired network.
3. Click a device. **The Import New Group** and **Overwrite Existing Config** options are displayed.
4. To create a new group, click **Import to New Group** tab and then click **Save**.

To overwrite an existing configuration, click **Overwrite Existing Config**.

5. Click **Save**. Central deletes the existing configuration and applies the group configuration.

Pending Configuration

If an IAP configuration is not synchronized with the Central configuration, a pending configuration icon is displayed. This implies that there are some pending configurations, which are not applied to the Virtual Controller.

Click the **Pending Configuration** icon to view the configurations that are not synchronized and click **Resolve**. The entire configuration is re-applied to the Virtual Controller.

Managing Groups

Central allows some configuration settings to be managed efficiently at the group level, while others are managed at an individual device level. Central defines a group as a subset of the devices on the wireless LAN, ranging in size from one device to hundreds of devices that share some common configuration settings. When a group is configured, all devices within a group share the same basic configuration settings.

Creating a Group

To create a group, complete the following steps:

1. Click the icon next to **All Groups** on the left pane.
2. Click **(+)** to create a new group. The **Create New Group** pane appears.
3. Enter a name for the group in **Enter Group Name**.
4. Select the device that you want to assign to the new group, for example virtual controller or switch.
5. Click **Next**.
6. Enter the default device password for the newly created group in the **Password** text box.
7. To reconfirm the password, re-enter the default device password in the **Retype Password** text box.
8. Click **Save**.

Editing a Group

To edit or delete a group, complete the following steps:

1. Click the icon next to **All Groups** in the left pane.
2. Select the group to modify or delete, and then click **Actions**.
3. To create a clone of an existing group, click **Actions** > **Clone**.
   a. Enter the name of the group in the **Enter Group Name** text box.
   b. Click **Save**.
4. To delete a group, select the group to delete and click **Actions** > **Delete**.
5. To move a device from one group to an another group:
   a. Select a group from **Groups**.
   b. Select the device to move.
   c. Click **Move**.

d. Select the group to which you want to assign the device.

e. Click **Save**.

Managing Overrides

Devices in Central can be configured at the group level as they share the same basic configuration settings. However, you can also apply configuration changes at device level. If the device configuration differs from the configuration applied at the group level, an **Override** icon is displayed for this device. For example, the configuration changes to AAA server, SNMP read-only/read-write community string, syslog server, and SSID or network profiles at the device can be marked as overrides. . When a device has overrides and its configuration is modified at the group level, the overrides are automatically preserved. You can also resolve the overrides and remove the configuration changes applied at the device level.

To resolve overrides, complete the following steps:

1. Click the Override icon displayed next to the device. The **Overrides** window is displayed.
2. Click **Resolve all Overrides** to resolve configuration differences.

Modifying AP Administrator Credentials

To change AP administrator password:

1. Select **Configuration > Access Points > System**. The system configuration pane is displayed.
2. Click **Administrator** under **Local**, provide a new password that you would like the administrator users to use.
3. Click **OK**.

Chapter 6
Monitoring

The **Monitoring** tab displays the monitoring dashboard for Central. The tab includes the following:

- Overview
- Access Points
- AppRF
- Switches
- Clients
- Wireless Security
- Notifications

Overview

The **Overview** pane displays a summary of the bandwidth usage, client count, type of clients, application usage, WLAN network details of the selected group. By default, the graphs are plotted for a time range of 3 hours. To view the graphs for a different time range, click the **3 Hours** link.

Table 5: *Overview Pane*

Data Pane Item	Description
Time Range Panel (3 Hours link)	Allows you to select a time range for the graphs displayed on the Overview pane. You can choose to view graphs for a time period of 3 hours, 1 day, 1 week, 1 month and 3 months.
Bandwidth Usage Graph	Displays the aggregate incoming and outgoing data traffic of all clients in the selected group.
Clients count	Displays the total number of clients connected to an IAP over a specific duration.
TOP APs By Bandwidth Usage	Displays the list of top IAPs that utilize the maximum bandwidth in the network.

Data Pane Item	Description
Application Usage	If Deep Packet Inspection is enabled, the Application Usage graphs display the applications, application categories, and web categories accessed by the clients in the network. The Web Reputation graph displays the web reputation score for the websites accessed by the clients connected to the network.
TOP Clients By Usage	Displays a list of clients connected to the currently available SSIDs that utilize the maximum bandwidth in the network. The **Top Clients by Usage** table displays data only for the clients that are connected to the network for a total duration of two or more hours.
WLANs	Displays the list of SSIDs configured. The WLANs table displays the SSID details such the name, type, security settings, and the clients connected on the network. To expand or collapse the column view, click the column settings icon next to the last column in the table.

Access Points

The **Access Points** pane displays a summary of the number of the APs that are up or down, bandwidth and application usage graphs for the APs in the selected group.

The **Access Points** pane consists of the following tabs:

- **Usage**—Clicking on the **Usage** tab displays the graphs for all APs in the group.
- **List**—Clicking on the **List** tab displays a list of APs in the group. To view the details of an AP, click the AP entry in the **Access Points** table.

The **Access Points** pane displays the following information:

Table 6: *Access Points Pane*

Data Pane Content	Description
Time Range	By default, the graphs are plotted for a time range of 3 hours. To view the graphs for a different time range, click the **3 Hours** link. You can choose to view graphs for a time period of 3 hours, 1 day, 1 week, 1 month and 3 months.
Up and Down Status Indicators	Displays the total number of APs in the Up and Down status. To view the APs that are up or down, click the numbers below the status indicators.
Bandwidth Usage	Displays the aggregate incoming and outgoing data traffic of all APs over a specific duration.
Client Count	Displays the number of clients connected to an AP over a specific time period.

Data Pane Content	Description
Bandwidth Usage per Network	Displays the aggregate incoming and outgoing traffic for all access points per SSID over a specific duration.
Client Count per Network	Displays the number of clients connected to an access point as per SSID over a specified time period.
Top N	Displays a list of APs with maximum bandwidth usage.
List view—Access Points table	The **Access Points** table displays the following information: ● Name—Name of the AP ● Location—Location of the AP ● Group—Group to which the AP belongs ● Status—Status of the AP ● Clients—Clients connected to the AP ● IP Address—IP address of the AP ● Mode—AP Radio mode such as access or monitor ● Type—Type of AP device ● 2.4 GHz—Channels assigned under the 2.4 GHz band ● 5.0 GHz—Channels assigned under the 5 GHz band ● Virtual Controller—Name of the Virtual controller (VC) ● Uptime—Time since which the AP is operational. ● Labels—Labels associated with the AP. You can also add a new label to the AP by clicking on the edit icon. ● The Search box—The Search text box that allows you to specify a criteria for searching devices. Central supports single column search. It filters the search results and sorts the list of devices based on the search string specified from a single column. To expand or collapse the column view, click the column settings icon next to the last column of the table.

AP Details

On clicking the **List** tab displays a list of APs in the group. To view the details of an AP, click the AP entry in the **Access Points** table. The following details of the selected AP are displayed.

Table 7: *Access Points Details Page*

Parameter	Description
Time Range	By default, the graphs are plotted for a time range of 3 hours. To view the graphs for a different time range, click the **3 Hours** link. You can choose to view graphs for a time period of 3 hours, 1 day, 1 week, 1 month and 3 months. However, the application usage graphs display data for a time period of 3 hours or 1 day only.
Device Stat us	Displays the current status of the AP.
Network	Displays the number of network profiles configured on the AP.
Uptime	Displays the time since which the AP is operational.
Alerts	Displays the alerts generated for the AP.
CPU Utilization	Displays the percentage of processing resources utilized on the AP.
Memory Utilization	Displays the percentage of memory utilized on the AP.
Usage Graphs	Displays the following graphs: ● Bandwidth Usage—Displays the aggregate incoming and outgoing data traffic of the AP over a specific duration. The UI provides aggregate, 2,4 GHz, and 5 GHz options to view graphs with aggregate data , for 2.4 or 5 GHz radios only. ● Client Count—Displays the total number of clients connected to an AP over a specific duration. **NOTE:** The UI provides aggregate, 2,4 GHz, and 5 GHz options to view the Bandwidth Usage and Client Count graphs with aggregate data, or for 2.4 or 5 GHz radios only. ● Application Usage graphs: ● Apps—Displays the applications used by the clients connected to the AP. ● App Categories—Displays the application categories that are accessed by the clients connected to the AP. ● Web Categories—Displays the web categories accessed by the clients connected to the AP. ● Web Reputation—Displays the Web reputation score for the websites accessed by the clients connected to the AP.
RF Health Graphs	Displays the following graphs: ● RF Channel Utilization—Shows channel utilization statistics. ● Noise Floors—Shows the noise floor detected in the network to which the AP belongs ● Error/Retries/Drop statistics—Shows the number of connection errors, retries and drops.

Parameter	Description
	● Neighboring Clients—The number of clients in the AP neighborhood.
Interface	Displays the wired and wireless network interface details. ● The wired interface details include Ethernet ports, link type, and duplex mode. ● The wireless interface details include type of radio, status of the AP, the number of clients connected to the AP, SSIDs configured on the AP, channels and power settings configured on the AP, type of the AP antenna, and the radio mode in which the AP operates.
Clients	Displays the details and type of the clients connected to the AP.
Alerts and Event Log	Displays the alerts generated for the AP and the list of events associated with the AP.
Info	Displays general information about the AP: ● AP Name—Name of the AP ● Serial Number—Serial number of the AP ● MAC Address—MAC address of the AP ● IP Address—IP address of the AP ● Mode—The radio mode in which the AP operates. ● Mesh Role—Role of the mesh AP. ● VC Name—Name of VC to which the AP is connected. ● AP Model Type—AP model ● Firmware Version—Firmware version running on the AP ● Group Name—Group to which the AP belongs ● Country Code—Country code in which the AP operates.
Map	Displays the geographical location of the IAP.
Actions drop-down	Displays the following menu options: ● Delete AP—Deletes an inactive AP. ● Reboot AP—Reboots the AP. ● Console—Opens the remote console for a CLI session through SSH. Remote console access is supported only on VCs. ● Troubleshoot—Allows administrators and users with read-write permissions to run troubleshooting or diagnostics commands AP without logging in to the AP. For more information on troubleshooting APs, see Troubleshooting Devices on page 154.
Labels	Allows you to edit labels associated with the AP. You can also add new labels to the AP.

Clients

The **Clients** pane displays the total number of clients, bandwidth usage, and the application usage by the clients connected to the wired and wireless networks.

Table 8: *Clients Pane*

Data Pane Content	Description
Time Range	By default, the graphs on the **Clients** pane are plotted for a time range of 3 hours. To view the graphs for a different time range, click the **3 Hours** link. You can choose to view graphs for a time period of 3 hours, 1 day, 1 week, 1 month and 3 months.
Total	Displays the total number of clients.
Wired	Displays the total number of clients connected to the wired network.
Wireless	Displays the total number of clients connected to wireless network.
Usage	Displays the following graphs: ● Bandwidth Usage graph—Displays the incoming and outgoing throughput traffic for all the clients during a specific time range. The graph will not show any data for the clients that are connected to the network for less than two hours. ● Application Usage graphs: ● Apps—Displays the applications used by the clients. ● App Categories—Displays the application categories that are accessed by the clients. ● Web Categories—Displays the web categories accessed by the clients. ● Web Reputation—Displays the Web reputation score for the websites accessed by the clients.

Data Pane Content	Description
Distribution	Displays the type of client device connected to the wireless network.
Top Clients By Usage	Displays a list of clients connected to the currently available SSIDs that utilize the maximum bandwidth in the network. The **Top Clients by Usage** table displays data only for the clients that are connected to the network for a total duration of two or more hours.
List view—Clients table	The **Clients** table displays the following information: ● MAC Address—MAC address of the client ● IP Address—address of the client ● User name—User name of the client ● Hostname—Host name of the client ● Device type—Type of client device ● Connected To—The AP to which the client is connected ● SSID—The SSID to which the client is connected ● Connection—The AP radio to which the client is assigned ● Labels—Labels associated with the client To expand or collapse the column view, click the column settings icon next to the last column of the table.

NOTE

Central does not provide details of the wired clients under the **Monitoring > Clients** page if the ports are trusted. The Switch details are provided only if the ports are untrusted.

Client Details

To view the details of a client, click a client from the **Clients** table on the **Monitoring > Clients >List** page.

Table 9: *Client Details*

Data Pane Content	Description
Time Range panel	By default, the graphs on the **Clients** pane are plotted for a time range of 3 hours. To view the graphs for a different time range, click the **3 Hours** link. You can choose to view graphs for a time period of 3 hours, 1 day, 1 week, 1 month and 3 months. However, the application usage graphs display data for a time period of 3 hours or 1 day only.
Current AP	Displays the AP to which the client is currently connected.
SSID	Displays the SSID to which the client is connected.
Role	Displays the user role assigned to the client.
OS	Displays the OS running on the client device.
Alerts	Displays alerts generated for the client.
Usage Graphs	Displays the following graphs: ● Bandwidth Usage graph—Displays the incoming and outgoing throughput traffic for the client during a specific time range. ● Application Usage graphs: ● Apps—Displays the applications used by the client. ● App Categories—Displays the application categories that are accessed by the client. ● Web Categories—Displays the web categories accessed by the client. ● Web Reputation—Displays the Web reputation score for the websites accessed by the client.
RF Health	Displays the following RF health statistics: ● Signal—Indicates signal strength of the client device in dB as measured by the AP ● Speed—Indicates the connection speed of the client. ● SNR—Indicates the signal-to-Noise Ratio of the client device. ● Channel/Band—Displays the channel and the radio band to which the client is assigned.
Mobility Trail	Displays the time stamp and details of the IAP and client association.
Alert and Event Log	Displays the alerts and events generated for the client.

AppRF

The AppRF pane displays the traffic summary for IAPs and client devices. The AppRF graphs are based on Deep Packet Inspection (DPI) application and Web Policy Enforcement service, which provides application traffic summary for the client devices associated with an IAP.

For more information, see Application Visibility on page 125.

Switches

The **Switches** page displays the status and location of the Switches.

Table 10: *Switches Pane*

Data Pane Content	Description
Time Range	By default, the graphs on the **Switches** pane are plotted for a time range of 3 hours. To view the graphs for a different time range, click the **3 Hours** link. You can choose to view graphs for a time period of 3 hours, 1 day, 1 week, 1 month and 3 months.
Usage	Displays the following graphs: ● Throughput—Indicates aggregate client data traffic detected on the switches. ● Client—Indicates the number of clients connected to the switch.
Top N	Displays a list of Switches with maximum usage.
List view—Switches table	Displays a list of Switchess provisioned under the selected group. The **Switches** table provides the following information: ● Name—Name of the Switch ● Location—Location of the Switch ● Group—Group under which the Switch is provisioned. ● Status—Operational status of the Switch ● Clients—Number of clients connected to the Switch. ● IP Address—IP address of the Switch ● Avg Usage—Average usage of the Switch. ● Uptime—Time since which the Switches are operational. ● Labels—Labels associated with the AP. You can also add a new label to the AP by clicking on the edit icon. ● Uplink Ports—Uplink ports configured on the Switch. To manually assign a port, click the edit icon. ● Search—The Search text box that allows you to specify a criteria for searching devices. Central supports single column search. It filters the search results and sorts the list of devices based on the search string specified from a single column. To expand or collapse the column view, click the column settings icon next to the last column of the table.
Map	Displays the geographical location of the Switch.

Switch Details

To view the details of the Switch, select **Monitoring > Switches > List** pane and click the Switch for which you want to view the details. The **Switch Details** pane is displayed.

Table 11: *Switch Details Pane*

Data Pane Content	Description
Status	Indicates the operational status of the Switch.
Uptime	Indicates the time since which the Switches are operational.
Graphs	Displays the following graphs: ● Throughput—Indicates the aggregate client data traffic detected on the Switches. ● Connected Clients—Indicates the number of clients connected to the Switch.
Ports	Displays the following details of the Switch ports: ● Port#—Port number ● Oper Stat—Operational status of the Switch ● PoE—PoE status of the port ● Type—Type of Switch port. ● Mode—Operational mode of the port ● Tx Usage—Client data transmission details. ● Rx Usage—Data traffic received from the clients connected to the port. ● Trusted—Indicates if the port is a trusted port.
Uplink	Displays the Uplink Stats graph. The graph displays the uplink statistics for the inbound and outbound data traffic.
Info	Displays the following details for the Switch: ● Hostname—Host name of the switch ● Switch Model Type—Indicates the switch model ● Firmware Version—Firmware version of the Switch ● Public IP— The public IP address of the Switch ● Serial Number—Serial number of the Switch. ● Group Name—Name of the group to which Switch belongs ● Fan Speed—Fan speed of the switch. The fan speed for legacy Aruba switches is indicated in Rotations per Minute (RPM). For the other switches, the Fan Speed field shows **Ok** to indicate that the fan speed is fine. ● Management IP— Management IP address of the Switch ● MAC address—MAC address of the switch ● PoE Consumption— PoE power drawn from the Switch in watts (W).

Data Pane Content	Description
Alerts and Event Log	Displays the list of events and alerts associated with the Switch.
Map	Displays the geographical location of the Switch.
Actions	Displays the following menu options: ● Delete Switch—Deletes the Switch. ● Reboot Switch—Reboots the Switch. ● Console—Opens the remote console for a CLI session through SSH. For the Aruba 2920 and Aruba 2930F Switch Series, the remote console access is enabled only when the user credentials are configured on the **Configuration** > **Switch - Aruba** > **System** page. ● Manage Access—This menu option is available only for the legacy Aruba Switches such as Mobility Access Switches. This menu command allows you to set the access mode for Switch operation. Before a Switch is connected to Central, the switch is in **Monitored** mode. In the monitored mode, the Switch has the configurations that can be modified only through the switch console. When a Switch is connected to Central for the first time, the switch is in the managed mode. When Switch access is changed to managed mode, you can configure the Switch features only through Central. ● Labels—Allows you to edit labels associated with the Switch. You can also add new labels to the Switch. **NOTE:** If a switch is in the monitored mode, the configuration changes at the group or device level will not be applied to the switch. When any configuration is modified at the group or device level for the switches in the monitored mode, the **Configuration cannot be pushed to device as device is monitoring mode** message is displayed.

NOTE

To reboot the Switch from Central, click **Reboot Switch** in the **Monitoring** > **Switches** > **Switch Details** pane.

Wireless Security

The **Wireless Security** pane provides a summary of the rogue IAPs, interfering IAPs, and the total number of wireless attacks detected on an AP and client devices at a given duration.

Table 12: *WIDS Pane*

Data Pane Content	Description
Time Range	By default, the graphs are plotted for a time range of 3 hours. To view the graphs for a different time range, click the **3 Hours** link. You can choose to view graphs for a time period of 3 hours, 1 day, and 1 week.
Rogue APs	Indicates the total number of rogue APs detected in the network.
Infrastructure Attacks	Indicates the number of infrastructure attacks detected in the network
Client Attacks	Indicates the number of client attacks detected in the network.
Rogues	Displays a graph showing the top 5 rogue APs detected in the network.
Interferences	Displays a graph showing the top 5 interferences detected in the network.
Intrusion Detection	Displays graphs showing the top 5 infrastructure, client, and intrusion detection attacks.
WIDS Events	Displays a list of the WIDS events. The WIDS event table includes the following columns: ● Date/Time ● Level ● Description ● Type ● Detecting AP ● Virtual Controller ● Radio ● Station MAC

Notifications

The **Notifications** pane displays all types of notification alerts that are detected and unacknowledged by Central.

NOTE

The UI also shows the alerts and pending actions such as importing a device, setting country code of IAPs and so on in the bottom pane of the UI. Click the links to complete the required action.

Table 13: *Notifications Pane*

Data Pane Content	Description
Notifications	Displays all types of notification alerts.
Search box	Allows to search for notifications and define a filter criteria to display notifications in the table.
Acknowledge All	Acknowledges all the notifications at once.

Setting Notification Alerts

To configure a notification alert, complete the following steps:

1. Go to **Monitoring > Notifications**.
2. On the **Notifications**page, click the **> Settings** icon.
3. Select a notification type from the **Type**drop-down list.
4. Select an event type from the **Event** drop-down list.
5. Select a group type from the **Group** drop-down list.
6. To receive email notifications, select the **Email** check box and enter the email address.
7. Click **Save**.

Chapter 7
Configuring Access Points

This chapter describes the following topics:

Configuring System Parameters for IAP Network

To configure system parameters:

1. Select **Configuration > Access Points** > **System**. The **System** details are displayed.
2. Click **General** and configure the following parameters:

Table 14: *System Parameters*

Data Pane Item	Description
Name	To change the name of an IAP: 1. Click **Edit Values**. The **Edit VC Name** pane is displayed. 2. Click the edit icon. 3. Modify the name. 4. Click **Save**.
Virtual Controller IP	You can specify a single static IP address to manage a multi-AP Central network. This IP address is automatically provisioned on a shadow interface on the IAP that takes the role of a VC. The AP sends three Address Resolution Protocol (ARP) messages with the static IP address and its MAC address to update the network ARP cache. To configure the VC name and IP address: 1. Click **Edit Values** next to **Virtual Controller IP**. The **Edit IP Address** pane is displayed. 2. Click the edit icon. 3. Enter the IP address in **IP Addresses**. 4. Click **Save**.
Timezone	To configure a timezone, select a timezone from the **Timezone** drop-down list.

Table 14: *System Parameters*

Data Pane Item	Description
	If the selected timezone supports DST, the UI displays the "The selected country observes Daylight Savings Time" message.
Preferred Band	Assign a preferred band by selecting an appropriate option from the **Preferred Band** drop-down list. **NOTE:** Reboot the IAP after modifying the radio profile for changes to take effect.
NTP Server	To facilitate communication between various elements in a network, time synchronization between the elements and across the network is critical. Time synchronization allows you to: ● Trace and track security gaps, network usage, and troubleshoot network issues. ● Validate certificates. ● Map an event on one network element to a corresponding event on another. ● Maintain accurate time for billing services and similar. The Network Time Protocol (NTP) helps obtain the precise time from a server and regulate the local time in each network element. Connectivity to a valid NTP server is required to synchronize the IAP clock to set the correct time. If NTP server is not configured in the IAP network, an IAP reboot may lead to variation in time data. By default, the IAP tries to connect to **pool.ntp.org** to synchronize time. The NTP server can also be provisioned through the DHCP option 42. If the NTP server is configured, it takes precedence over the DHCP option 42 provisioned value. The NTP server provisioned through the DHCP option 42 is used if no server is configured. The default server **pool.ntp.org** is used if no NTP server is configured or provisioned through DHCP option 42. To configure an NTP server, enter the IP address or the URL (domain name) of the NTP server. and reboot the AP to apply the configuration changes.
Virtual Controller Netmask Virtual Controller Gateway Virtual Controller VLAN	**NOTE:** The IP configured for the VC can be in the same subnet as IAP or can be in a different subnet. Ensure that you configure the VC VLAN, gateway, and subnet mask details only if the VC IP is in a different subnet. **NOTE:** Ensure that VC VLAN is not the same as native VLAN of the IAP.
Dynamic CPU Utilization	IAPs perform various functions such as wired and wireless client connectivity and traffic flows, wireless security, network management, and location tracking. If an AP is overloaded, prioritize the platform resources across different functions. Typically, the IAPs manage resources automatically in real time. However, under special circumstances, if dynamic resource management needs to be enforced or disabled altogether, the dynamic CPU management feature settings can be modified. To configure dynamic CPU management, select any of the following options from **Dynamic CPU Utilization**. ● **Automatic**—When selected, the CPU management is enabled or disabled automatically during run-time. This decision is based on real time load calculations taking into account all different functions that the CPU needs to perform. This is the default and recommended option.

Table 14: *System Parameters*

Data Pane Item	Description
	● **Always Disabled in all APs**— When selected, this setting disables CPU management on all APs, typically for small networks. This setting protects user experience. ● **Always Enabled in all APs**—When selected, the client and network management functions are protected. This setting helps in large networks with high client density.
Auto Join Mode	When set to **ON**, IAPs can automatically discover the VC and join the network. The **Auto Join Mode** feature is enabled by default. If the auto join mode feature is disabled, a **New** link is displayed in the **Access Points** tab. Click this link to add IAPs to the network. If this feature is disabled, the inactive IAPs are displayed in red.
Terminal Access	When set to **ON**, the users can access the IAP CLI through SSH.
Telnet Server	When set to **ON**, the users can start a Telnet session with the IAP CLI.
LED Display	Enables LED display for all IAPs in a cluster when the LEDs are set to ON. **NOTE:** The LED display is always enabled during the IAP reboot.
Extended SSID	**Extended SSID** is enabled by default in the factory default settings of IAPs. This disables mesh in the factory default settings.
Deny Inter-user Bridging	If you have security and traffic management policies defined in upstream devices, you can disable bridging traffic between two clients connected to the same AP on the same VLAN. When inter-user bridging is denied, the clients can connect to the Internet but cannot communicate with each other, and the bridging traffic between the clients is sent to the upstream device to make the forwarding decision. To disable inter-user bridging, select **ON**.
Deny Local Routing	If you have security and traffic management policies defined in upstream devices, you can disable routing traffic between two clients connected to the same IAP on different VLANs. When local routing is disabled, the clients can connect to the Internet but cannot communicate with each other, and the routing traffic between the clients is sent to the upstream device to make the forwarding decision. To disable local routing, select **ON**.
Dynamic RADIUS Proxy	When set to **ON**, the virtual controller network will use the IP Address of the virtual controller for communication with external RADIUS servers. You must set the virtual controller IP Address as a NAS client in the RADIUS server if **Dynamic RADIUS proxy** is enabled.
MAS Integratio n	To enable LLDP protocol for Switch integration. With this protocol, IAPs can instruct the Switch to turn off ports where rogue access points are connected, as well as take actions such as increasing PoE priority and automatically configuring VLANs on ports where IAPs are connected.

Configuring AP Settings

This section describes the procedures for configuring settings that are specific to an IAP in the cluster.

To customize IAP parameters, complete the following steps:

1. Click **Configuration**.
2. Select a group and then click **Access Points**. The **Access Points** page is displayed.
3. Click the IAP that you want to customize.
4. Click **Edit**. The **Edit** pane for modifying the IAP details is displayed.
5. Configure the parameters described in Table 15 as required and then click **Save Settings**.

Table 15: *Access Points Configuration*

UI	Parameters	Description
Basic Info	Name	Configures a name for the IAP. You can specify a character string of up to 32 ASCII characters.
	AP Zone	Configures the IAP zone. When a zone is configured for an IAP and if the same zone details are configured on an SSID, the SSID can be broadcast only by the IAPs in that specific zone. Only one zone can be configured on an SSID. An IAP can belong to only one zone at any point in time.
	Preferred Master	Provisions the IAP as a master IAP.
	IP Address for Access Point	Allows IP to get an IP address from the DHCP server. By default, the IAPs obtain IP address from a DHCP server. The users can also assign a static IP address to the IAP. To specify a static IP address for the IAP, complete the following steps: 1. Enter the new IP address for the IAP in the **IP Address** text box. 2. Enter the subnet mask of the network in the **Netmask** text box. 3. Enter the IP address of the default gateway in the **Default Gateway** text box. 4. Enter the IP address of the Domain Name System (DNS) server in the **DNS Server** text box. 5. Enter the domain name in the **Domain Name** text box.
RADIO	Mode	Select any of the following options: ● Access—In the **Access** mode, the IAP serves clients, while also monitoring for rogue IAPs in the background. ● Monitor—In the **Monitor** mode, the IAP acts as a dedicated monitor, scanning all channels for rogue IAPs and clients. ● Spectrum Monitor—In the **Spectrum Monitor** mode, the IAP functions as a dedicated full-spectrum RF monitor, scanning all channels to detect interference, whether from the neighboring IAPs or from non-Wi-Fi devices such as microwaves and cordless phones. **NOTE:** In the **Monitor** and **Spectrum Monitor** modes, the IAPs do not provide access services to clients.

UI	Parameters	Description
		You can configure a radio profile on an IAP either manually or by using the Adaptive Radio Management (ARM) feature. ARM is enabled on Central by default. It automatically assigns appropriate channel and power settings for the IAPs.
Uplink	Uplink Management VLAN	The uplink traffic on IAP is carried out through a management VLAN. However, you can configure a non-native VLAN as an uplink management VLAN. After an IAP is provisioned with the uplink management VLAN, all management traffic sent from the IAP is tagged to the management VLAN. To configure a non-native uplink VLAN, click **Uplink** and specify the VLAN in **Uplink Management VLAN**.
	Eth0 Bridging	Select **Enable** from **Eth0 Bridging** if you want to convert the Eth0 uplink port to a downlink port.

6. Click **Save Settings** and reboot the IAP.

Configuring External Antenna

If your IAP has external antenna connectors, you need to configure the transmit power of the system. The configuration must ensure that the system's Equivalent Isotropically Radiated Power (EIRP) is in compliance with the limit specified by the regulatory authority of the country in which the IAP is deployed. You can also measure or calculate additional attenuation between the device and antenna before configuring the antenna gain. To know if your IAP device supports external antenna connectors, see the *Installation Guide* that is shipped along with the IAP device.

EIRP and Antenna Gain

The following formula can be used to calculate the EIRP limit related RF power based on selected antennas (antenna gain) and feeder (Coaxial Cable loss):

EIRP = Tx RF Power (dBm)+GA (dB) - FL (dB)

The following table describes this formula:

Table 16: *Formula Variable Definitions*

Formula Element	Description
EIRP	Limit specific for each country of deployment
Tx RF Power	RF power measured at RF connector of the unit
GA	Antenna gain
FL	Feeder loss

Configuring Antenna Gain

To configure antenna gain for IAPs with external connectors, complete the following steps:

1. Select **Configuration > Access Points > Basic Info** and select the access point to configure and then click **Edit**.
2. Select **Radio** and select **External Antenna** to configure the antenna gain value. This option is available only for access points that support external antennas.
3. Enter the antenna gain values in dBm for the 2.4 GHz and 5 GHz bands.
4. Click **Save Settings**.

Adding an IAP

To add an IAP to Central, assign an IP address and a license.

After an IAP is connected to the network and if the **Auto Join Mode** feature is enabled, the IAP inherits the configuration from the VC and is listed in the **Access Points** tab.

Removing an IAP from the Network

To remove an IAP from the network:

1. In the **Maintenance** tab, select the IAP to remove. The **Unassign** button is displayed in the bottom of the page.
2. Click **Unassign** to confirm the deletion.

Configuring Networks

This section describes the following procedures:

- Configuring a WLAN SSID Profile for Employee and Voice Networks on page 47
- Configuring Captive Portal Profiles for Guest Access on page 54
- Configuring Ethernet Profiles on page 61
- Editing a Network Profile on page 64
- Deleting a Network Profile on page 64

Configuring a WLAN SSID Profile for Employee and Voice Networks

NOTE

You can configure up to six wireless networks. By enabling Extended SSID (**Configuration > Access Points > System > General**), you can create up to **16** networks.

Configuring WLAN Settings

To configure WLAN settings, complete the following steps:

1. Click **Configuration**.
2. Select a group and then click **Networks**. The **Networks** page is displayed.
3. To create a new SSID profile, click the + icon. The **Create a New Network** pane is displayed.
4. Under **Basic Settings**, configure the following parameters:
   a. From the **Type** list, select **Wireless**.
   b. Enter a name that is used to identify the network in the **Name (SSID)** box.
   c. Based on the type of network profile, select any of the following options under **Primary Usage**:
   - **Employee**—An Employee network is a classic Wi-Fi network. This network type is used by the employees in an organization and it supports passphrase-based or 802.1X-based authentication methods. Employees can access the protected data of an enterprise through the employee network

after successful authentication. The employee network is selected by default during a network profile configuration.

- **Voice**—The Voice network type allows you to configure a network profile for devices that provide only voice services such as handsets or applications that require voice traffic prioritization.
- **Guest**—The Guest wireless network is created for guests, visitors, contractors, and any non-employee users who use the enterprise Wi-Fi network. The VC assigns the IP address for the guest clients. Captive portal or passphrase-based authentication methods can be set for this wireless network. Typically, a guest network is an unencrypted network. However, you can specify the encryption settings when configuring a guest network.

NOTE

When a client is associated to the voice network, all data traffic is marked and placed into the high priority queue in QoS (Quality of Service).

5. Configure the following SSID parameters as required.

Table 17: *WLAN Configuration Parameters*

Parameter	Description
Broadcast Filtering	Select any of the following values: ● **All**—The IAP drops all broadcast and multicast frames except DHCP and ARP, IGMP group queries, and IPv6 neighbor discovery protocols. ● **ARP**—The IAP drops broadcast and multicast frames except DHCP and ARP, IGMP group queries, and IPv6 neighbor discovery protocols. Additionally, it converts ARP requests to unicast and sends frames directly to the associated clients. ● **Disabled**—All broadcast and multicast traffic is forwarded to the wireless interfaces.
DTIM Interval	The **DTIM Interval** indicates the Delivery Traffic Indication Message (DTIM) period in beacons, which can be configured for every WLAN SSID profile. The DTIM interval determines how often the IAP delivers the buffered broadcast and multicast frames to the associated clients in the power save mode. The default value is 1, which means the client checks for buffered data on the IAP at every beacon. You can also configure a higher DTIM value for power saving.
Multicast Transmission Optimization	Select **Enabled** if you want the IAP to select the optimal rate for sending broadcast and multicast frames based on the lowest of unicast rates across all associated clients. When this option is enabled, multicast traffic can be sent up to a rate of 24 Mbps. The default rate for sending frames for 2.4 GHz is 1 Mbps and that for 5 GHz is 6 Mbps. This option is disabled by default.
Dynamic Multicast Optimization	Select **Enabled** to allow IAP to convert multicast streams into unicast streams over the wireless link. Enabling Dynamic Multicast Optimization (DMO) enhances the quality and reliability of streaming video, while preserving the bandwidth available to the nonvideo clients. **NOTE:** When you enable DMO on multicast SSID profiles, ensure that the DMO feature is enabled on all SSIDs configured in the same VLAN.
DMO Channel Utilization Threshold	Specify a value to set a threshold for DMO channel utilization. With DMO, the IAP converts multicast streams into unicast streams as long as the channel utilization does not exceed this threshold. The default value is 90% and the maximum threshold value is 100%. When the threshold is reached or exceeds the maximum value, the IAP sends multicast traffic over the wireless link.
Transmission Rates	Specify the following parameters: ● **2.4 GHz**—If the 2.4 GHz band is configured on the IAP, specify the minimum and

Parameter	Description
	maximum transmission rates. The default value for minimum transmission rate is 1 Mbps and maximum transmission rate is 54 Mbps. - **5 GHz** —If the 5 GHz band is configured on the IAP, specify the minimum and maximum transmission rates. The default value for minimum transmission rate is 6 Mbps and maximum transmission rate is 54 Mbps.
Zone	Specify the zone for the SSID. When the zone parameter is configured in the SSID profile and if the same zone is defined on the IAP, the SSID is broadcast by that IAP. - If an SSID belongs to a zone, all IAPs in this zone can broadcast this SSID. - If no IAP belongs to the zone configured on the SSID, the SSID is not broadcast. - If an SSID does not belong to any zone, all IAPs can broadcast this SSID.
Time Range	Click **Edit**. Select a time range profile from the list and a status to apply and then click **Save**.
Bandwidth Limits	Under **Bandwidth Limits**: - **Airtime** —Select this to specify an aggregate amount of airtime that all clients in this network can use for sending and receiving data. Specify the airtime percentage. - **Each Radio**—Select this to specify an aggregate amount of throughput that each radio is allowed to provide for the connected clients.
WMM	Configure the following options for Wi-Fi Multimedia (WMM) traffic management. WMM supports voice, video, best effort, and background access categories. You can allocate a higher bandwidth for voice and video traffic than other types of traffic based on the network profile. Specify a percentage value for the following parameters: - **Background WMM Share**—Allocates bandwidth for background traffic such as file downloads or print jobs. - **BEST Effort WMM Share**—Allocates bandwidth or best effort traffic such as traffic from legacy devices or traffic from applications or devices that do not support QoS. - **Video WMM Share** —Allocates bandwidth for video traffic generated from video streaming. - **Voice WMM Share**—Allocates bandwidth for voice traffic generated from the incoming and outgoing voice communication. In a non-WMM or hybrid environment, where some clients are not WMM-capable, you can allocate higher values for **Best Effort WMM** share and **Voice WMM Share** to allocate a higher bandwidth to clients transmitting best effort and voice traffic.
Content Filteri ng	Select **Enabled** to route all DNS requests for the non-corporate domains to OpenDNS on this network.
Band	Select a value to specify the band at which the network transmits radio signals. You can set the band to **2.4 GHz**, **5 GHz**, or **All**. The **All** option is selected by default.
Inactivity Timeout	Specify an interval for session timeout. If a client session is inactive for the specified duration, the session expires and the users are required to log in again. You can specify a value within the range of 60–3600 seconds. The default value is 1000 seconds.
Hide SSID	Select this check box if you do not want the SSID (network name) to be visible to users.

Parameter	Description
Disable SSID	Select this check box if you want to disable the SSID. When selected, the SSID will be disabled, but will not be removed from the network. By default, all SSIDs are enabled.
Can be used without uplink	Select this check box if you do not want the SSID profile to use uplink.
Max Clients Threshold	Specify the maximum number of clients that can be configured for each BSSID on a WLAN. You can specify a value within the range of 0– 255. The default value is 64.
Local Probe Request Threshold	Specify a threshold value to limit the number of incoming probe requests. When a client sends a broadcast probe request frame to search for all available SSIDs, this option controls system response for this network profile and ignores probe requests if required. You can specify a Received Signal Strength Indication (RSSI) value within range of 0–100 dB.

6. Click **Next** to configure VLAN settings.

Configuring VLAN Settings

To configure VLAN settings for an SSID, complete the following steps:

1. In the **VLAN**tab, select any of the following options for **Client IP Assignment**:

- **Virtual Controller Assigned** —On selecting this option, the client obtains the IP address from the VC. The VC creates a private subnet and VLAN on the IAP for the wireless clients. The network address translation for all client traffic that goes out of this interface is carried out at the source. This setup eliminates the need for complex VLAN and IP address management for a multi-site wireless network. For more information on DHCP scopes and server configuration, see Configuring DHCP and Client IP Assignment Modes on page 97.
- **Network Assigned**—Select this option to obtain the IP address from the network.

2. If **Network Assigned** is selected, specify any of the following options for the **Client VLAN Assignment**.

- **Default**—On selecting this option, the client obtains the IP address in the same subnet as the IAPs. By default, the client VLAN is assigned to the native VLAN on the wired network.
- **Static** —On selecting this option, you need to specify a single VLAN, a comma separated list of VLANS, or a range of VLANs for all clients on this network. If a large number of clients need to be in the same subnet, you can select this option to configure VLAN pooling. VLAN pooling allows random assignment of VLANs from a pool of VLANs to each client connecting to the SSID.
- **Dynamic**—On selecting this option, you can assign the VLANs dynamically from a DHCP server. To create VLAN assignment rules:

a. Click **New** to assign the user to a VLAN. The **New VLAN Assignment Rule** pane is displayed.

b. Enter the following information:

- **Attribute** —Select an attribute returned by the RADIUS server during authentication.
- **Operator**—Select an operator for matching the string.
- **String**—Enter the string to match.
- **VLAN**—Enter the VLAN to be assigned.

3. Click **Next** to configure security settings for the employee network.

Configuring Security Settings

To configure security settings for an employee or voice network, complete the following steps:

1. In **Security**, specify any of the following for **Security Level**:

- **Enterprise**—On selecting **Enterprise** security level, the authentication options applicable to the enterprise network are displayed.
- **Personal**—On selecting **Personal** security level, the authentication options applicable to the personalized network are displayed.
- **Open**—On selecting **Open** security level, the authentication options applicable to an open network are displayed:

The default security setting for a network profile is **Personal**.

2. Based on the security level specified, specify the following parameters:

Table 18: *WLAN Security Settings*

Data pane item	Description
Key Management	For **Enterprise** security level, select any of the following options from **Key Management**: ● WPA-2 Enterprise ● Both (WPA-2 & WPA) ● WPA Enterprise ● Dynamic WEP with 802.1X—If you do not want to use a session key from the RADIUS Server to derive pairwise unicast keys, set **Session Key for LEAP** to **Enabled**. This is required for old printers that use dynamic WEP through Lightweight Extensible Authentication Protocol (LEAP) authentication. The **Session Key for LEAP** feature is **Disabled** by default. **NOTE:** When **WPA-2 Enterprise** and **Both (WPA2-WPA)** encryption types are selected and if 802.1x authentication method is configured, the **Opportunistic Key Caching** (OKC) is enabled by default. If OKC is enabled, a cached Pairwise Master Key (PMK) is used when the client roams to a new AP. This allows faster roaming of clients without the need for a complete 802.1x authentication. OKC roaming can be configured only for the **Enterprise** security level.
	For **Personal** security level, select an encryption key from **Key Management**. For WPA-2 Personal, WPA Personal, and Both (WPA-2&WPA) keys, specify the following parameters: ● **Passphrase Format**: Select a passphrase format. The options are available are 8-63 alphanumeric characters and 64 hexadecimal characters. ● Enter a passphrase in **Passphrase** and reconfirm. For **Static WEP**, specify the following parameters: ● Select an appropriate value for **WEP Key Size** from the WEP key size. You can specify 64-bit or 128-bit. ● Select an appropriate value for Tx key from **Tx Key**. ● Enter an appropriate **WEP Key** and reconfirm.
Fast Roaming	Enable the following fast roaming features as per your requirement: ● **802.11r**—To enable 802.11r roaming, select **802.11r**. Selecting this enables fast BSS transition. The fast BSS transition mechanism minimizes the delay when a client transitions from one BSS to another within the same cluster. ● **802.11k**—To enable 802.11k roaming on the, select **802.11k**. The 802.11k protocol enables IAPs and clients to dynamically measure the available radio resources. When 802.11k is enabled, IAPs and clients send neighbor reports, beacon reports, and link

Data pane item	Description
	measurement reports to each other. ● **802.11v**—To enable 802.11v based BSS transition, select **802.11v**. 802.11v standard defines mechanisms for wireless network management enhancements and BSS transition management. It allows the client devices to exchange information about the network topology and RF environment. The BSS transition management mechanism enables an AP to request a voice client to transition to a specific AP, or suggest a set of preferred APs to a voice client, due to network load balancing or BSS termination. It also helps the voice client identify the best AP to transition to as they roam.
Termination	To terminate the EAP portion of 802.1X authentication on the IAP instead of the RADIUS Server, set **Termination** to **Enabled**. Enabling **Termination** can reduce network traffic to the external RADIUS Server by terminating the authorization protocol on the IAP. By default, for 802.1X authorization, the client conducts an EAP exchange with the RADIUS Server, and the IAP acts as a relay for this exchange. When **Termination**is enabled, the IAP acts as an authentication server and terminates the outer layers of the EAP and relays only the innermost layer to the external RADIUS Server. **NOTE:** If you are using LDAP for authentication, ensure that AP termination is configured to support EAP.
Authentication Server 1 and Authentication Server 2	Select an authentication server from **Authentication Server** or select **New** to create a new server. For information on configuring external servers, see Configuring External Servers for Authentication on page 80. To use an internal server, select **Internal server** and add the clients that are required to authenticate with the internal RADIUS Server. Click **Users** to add the users. If an external server is selected, you can also configure another authentication server.
Load Balancing	Set this to **Enabled** if you are using two RADIUS authentication servers, to balance the load across these servers. For more information on the dynamic load balancing mechanism, see Dynamic Load Balancing between Authentication Servers on page 80.
Reauth Interval	Specify a value for **Reauth Interval**. When set to a value greater than zero, APs periodically reauthenticate all associated and authenticated clients. If the re-authentication interval is configured: ● On an SSID performing L2 authentication (MAC or 802.1X authentication): When re-authentication fails, the clients are disconnected. If the SSID is performing only MAC authentication and has a pre-authentication role assigned to the client, the client will get a post-authentication role only after a successful re-authentication. If re-authentication fails, the client retains the pre-authentication role. ● On an SSID performing both L2 and L3 authentication (MAC with captive portal authentication): When re-authentication succeeds, the client retains the role that is already assigned. If re-authentication fails, a pre-authentication role is assigned to the client. ● On an SSID performing only L3 authentication (captive portal authentication): When re-authentication succeeds, a pre-authentication role is assigned to the client that is in a post-authentication role. Due to this, the clients are required to go through captive portal to regain access.
Blacklisting	To enable blacklisting of the clients with a specific number of authentication failures, select **Enabled** from **Blacklisting** and specify a value for **Max Authentication Failures**. The users who fail to authenticate the number of times specified in **Max Authentication Failures** field are dynamically blacklisted.

Data pane item	Description
Accounting	To enable accounting, select **Enabled** from **Accounting**. On setting this option to **Enabled**, APs post accounting information to the RADIUS server at the specified **Accounting Interval**.
Authentication Survivability	To enable authentication survivability, set **Authentication Survivability** to **Enabled**. Specify a value in hours for **Cache Timeout** to set the duration after which the authenticated credentials in the cache expires. When the cache expires, the clients are required to authenticate again. You can specify a value within range of 1 to 99 hours and the default value is 24 hours.
MAC Authentication	To enable MAC address based authentication for **Personal** and **Open** security levels, set **MAC Authentication** to **Enabled**. For **Enterprise** security level, the following options are available: ● **Perform MAC Authentication Before 802.1X** — Select this to use 802.1X authentication only when the MAC authentication is successful. ● **MAC Authentication Fail-Thru** — On selecting this, the 802.1X authentication is attempted when the MAC authentication fails.
Delimiter Character	Specify a character (for example, colon or dash) as a delimiter for the MAC address string. When configured, the IAP uses the delimiter in the MAC authentication request. For example, if you specify the colon as a delimiter, MAC addresses in the xx:xx:xx:xx:xx:xx format are used. If the delimiter is not specified, the MAC address in the xxxxxxxxxxxx format is used. This option is available only when MAC authentication is enabled.
Uppercase Support	Set to **Enabled** to allow the IAP to use uppercase letters in MAC address string for MAC authentication. This option is available only if MAC authentication is enabled.

3. Click **Next** to configure access rules.

Configuring Access Rules

You can configure up to 64 access rules for a wireless network profile. To configure access rules for an employee or voice network, complete the following steps:

1. In **Access Rules**, select any of the following types of access control:

- **Unrestricted** —Select this to set unrestricted access to the network.
- **Network-based** —Select **Network-based** to set common rules for all users in a network. The **Allow any to all destinations** access rule is enabled by default. This rule allows traffic to all destinations. To define an access rule:

    c. Click (**+**) icon.

    d. Select appropriate options in the **New Rule** pane.

    e. Click **OK**.

- **Role based** —Select **Role based** to enable access based on user roles. For role-based access control:
    - Create a user role if required.
    - Create access rules for a specific user role. You can also configure an access rule to enforce Captive portal authentication for an SSID that is configured to use 802.1X authentication method. For more information, see Configuring Captive Portal Roles for an SSID on page 59.
    - Create a role assignment rule.

2. Click **Finish**.

Configuring Captive Portal Profiles for Guest Access

Central supports the Captive portal authentication method in which a web page is presented to the guest users, when they try to access the Internet in hotels, conference centers or Wi-Fi hotspots. The web page also prompts the guest users to authenticate or accept the usage policy and terms. Captive portals are used at Wi-Fi hotspots and can be used to control wired access as well.

The Central Captive portal solution consists of the following:

- The captive portal web login page hosted by an internal or external server.
- The RADIUS authentication or user authentication against internal database of the AP.
- The SSID broadcast by the IAP.

With Central, administrators can create a wired or WLAN guest network based on captive portal authentication for guests, visitors, contractors, and any non-employee users who can use the enterprise Wi-Fi network. Administrators can also create guest accounts and customize the captive portal page with organization-specific logo, terms, and usage policy. With captive portal authentication and guest profiles, the devices associating with the guest SSID are assigned an initial role and are assigned IP addresses. When a guest user tries to access a URL through HTTP or HTTPS, the captive portal web page prompts the user to authenticate with a user name and password.

Splash Page Profiles

Central supports the following types of splash page profiles:

- **Internal Captive portal**— Select this splash page to use an internal server for hosting the captive portal service. Internal captive portal supports the following types of authentication:
  - **Internal Authenticated** — When **Internal Authenticated** is enabled, a guest user who is pre-provisioned in the user database has to provide the authentication details.
  - **Internal Acknowledged**—When **Internal Acknowledged** is enabled, a guest user has to accept the terms and conditions to access the Internet.
- **External Captive portal**— Select this splash page to use an external portal on the cloud or on a server outside the enterprise network for authentication.
- **Cloud Guest**—Select this splash page to use the cloud guest profile configured through the **Guest Management** tab.

Selecting **None** disables the captive portal authentication.

Configuring Captive Portal Profiles for Guest Network

For information on how to create and assign a captive portal profile, see the following sections:

- Configuring a WLAN SSID for Guest Access on page 54
- Configuring Internal Captive Portal for Guest Network on page 55
- Configuring External Captive Portal for a Guest Network on page 57
- Configuring Guest Logon Role and Access Rules for Guest Users on page 58
- Configuring Captive Portal Roles for an SSID on page 59

Configuring a WLAN SSID for Guest Access

To create an SSID for guest access, complete the following steps:

1. Click **Configuration**.
2. Select a group and then click **Networks**. The **Networks** page is displayed.
3. To create a new SSID profile, click the + icon. The **Create a New Network** pane is displayed.
4. Under **Basic Settings**, configure the following parameters:

a. From the **Type** list, select **Wireless**.

b. Enter a name that is used to identify the network in the **Name (SSID)** box.

c. Select the **Primary Usage** as **Guest**.

5. If configuring a wireless guest profile, set the required WLAN configuration parameters described in Table 17.

6. Click **Next** to configure VLAN settings. The VLAN details are displayed.

7. Select any of the following options for **Client IP Assignment**:

- **Virtual Controller Assigned**—On selecting this option, the client obtains the IP address from the VC. The VC creates a private subnet and VLAN on the IAP for the wireless clients. The NAT for all client traffic that goes out of this interface is carried out at the source. This setup eliminates the need for complex VLAN and IP address management for a multi-site wireless network. For more information on DHCP scopes and server configuration, see Configuring DHCP and Client IP Assignment Modes on page 97.
- **Network Assigned**—Select this option to obtain the IP address from the network.

8. If the **Network Assigned** is selected, specify any of the following options for the **Client VLAN Assignment**.

- **Default**— On selecting this option, the client obtains the IP address in the same subnet as the IAPs. By default, the client VLAN is assigned to the native VLAN on the wired network.
- **Static**— On selecting this option, you need to specify a single VLAN, a comma separated list of VLANS, or a range of VLANs for all clients on this network. Select this option for configuring VLAN pooling.
- **Dynamic**— On selecting this option, you can assign the VLANs dynamically from a DHCP server. To create VLAN assignment rules:

  a. Click **New** to assign the user to a VLAN. The **New VLAN Assignment Rule** data pane is displayed.

  b. Enter the following information:

  - **ATTRIBUTE**— Select an attribute returned by the RADIUS server during authentication.
  - **OPERATOR**— Select an operator for matching the string.
  - **STRING**— Enter the string to match.
  - **VLAN**— Enter the VLAN to be assigned.

9. Click **Next** to configure internal or external captive portal profiles.

Configuring Internal Captive Portal for Guest Network

To configure internal captive portal profile:

1. In the **Security** tab, assign values for the configuration parameters:

Table 19: *Internal Captive Portal Configuration Parameters*

Parameter	Description
Splash Page Type	Select any of the following: - **Internal - Authenticated**—When **Internal Authenticated** is enabled, the guest users are required to authenticate in the captive portal page to access the Internet. The guest users who are required to authenticate must already be added to the user database. - **Internal - Acknowledged**— When **Internal Acknowledged** is enabled, the guest users are required to accept the terms and conditions to access the Internet.
MAC Authentication	Select **Enabled** to enable the MAC authentication.
Captive-portal proxy server	If you want to configure a captive portal proxy server or global proxy server to match your browser configuration, enter the IP address and port number in the **Captive-portal proxy server IP** and **Captive Portal Proxy Server Port** fields.
Authentication Server 1 Authentication Server 2	Select any one of the following: - A server from the list of servers if the server is already configured. - **Internal Server** to authenticate user credentials at run time. - Select **New** for configuring a new external RADIUS server for authentication.
Load Balancing	Select **Enabled** to enable load balancing if two authentication servers are used.
Reauth Interval	Select a value to allow the APs to periodically re-authenticate all associated and authenticated clients.
Blacklisting	If you are configuring a wireless network profile, select **Enabled** to enable blacklisting of the clients with a specific number of authentication failures. This is applicable for WLAN SSIDs only.
Accounting Mode	Select an accounting mode for posting accounting information at the specified **Accounting interval**. When the accounting mode is set to **Authentication**, the accounting starts only after client authentication is successful and stops when the client logs out of the network. If the accounting mode is set to **Association**, the accounting starts when the client associates to the network successfully and stops when the client disconnects. This is applicable for WLAN SSIDs only.

Table 19: *Internal Captive Portal Configuration Parameters*

Parameter	Description
Disable If Uplink Type Is	To exclude uplink, select an uplink type.
Encryption	Select **Enabled** and configure the following encryption parameters: ● **Key Management**—Specify an encryption and authentication key ● **Passphrase format**—Specify a passphrase format. ● **Passphrase**—Enter a passphrase and retype to confirm.
Splash Page Design	Under **Splash Page Visuals**, use the editor to specify text and colors for the initial page that is displayed to the users connecting to the network. The initial page asks for user credentials or email, depending on the splash page type (Internal - Authenticated or Internal -Acknowledged) for which you are customizing the splash page design. Perform the following steps to customize the splash page design. ● To change the color of the splash page, click the Splash page rectangle and select the required color from the **Background Color** palette. ● To change the welcome text, click the first square box in the splash page, enter the required text in the **Welcome Text**box, and click **OK**. Ensure that the welcome text does not exceed 127 characters. ● To change the policy text, click the second square in the splash page, enter the required text in the **Policy Text** box, and click **OK**. Ensure that the policy text does not exceed 255 characters. ● To upload a custom logo, click **Upload**, browse the image file, and click **upload image**. Ensure that the image file size does not exceed 16 KB. ● To redirect users to another URL, specify a URL in **Redirect URL**. ● To preview the captive portal page, click **Preview** splash page. **NOTE:** You can customize the captive portal page using double-byte characters. Traditional Chinese, Simplified Chinese, and Korean are a few languages that use double-byte characters. Click on the banner, term, or policy in the **Splash Page Visuals** to modify the text in the red box. These fields accept double-byte characters or a combination of English and double-byte characters.

2. Click **Next**.

Configuring External Captive Portal for a Guest Network

You can configure external captive portal profiles and associate these profiles to a user role or SSID. You can create a set of captive portal profiles in the **Security > External Captive Portal** data pane and associate these profiles with an SSID or a wired profile. You can also create a new captive portal profile under the **Security** tab of the WLAN wizard or a Wired Network pane. You can configure up to eight external captive portal profiles.

When the captive portal profile is associated to an SSID, it is used before user authentication. If the profile is associated to a role, it is used only after the user authentication. When a captive portal profile is applied to an SSID or wired profile, the users connecting to the SSID or wired network are assigned a role with the captive portal rule. The guest user role allows only DNS and DHCP traffic between the client and network, and directs all HTTP or HTTPS requests to the captive portal unless explicitly permitted.

To configure an external captive portal profile, complete the following steps:

1. Select **Configuration > Access Points > Security**> **External Captive Portal**.
2. Click **New**. The **New** pop-up pane is displayed.
3. Specify values for the following parameters:

Table 20: *External Captive Portal Profile Configuration Parameters*

Data Pane Item	Description
Name	Enter a name for the profile.
Type	Select any one of the following types of authentication: ● **Radius Authentication**—Select this option to enable user authentication against a RADIUS server. ● **Authentication Text**—Select this option to specify an authentication text. The specified text will be returned by the external server after a successful user authentication.
IP or Hostname	Enter the IP address or the host name of the external splash page server.
URL	Enter the URL of the external captive portal server.
Port	Enter the port number that is used for communicating with the external Captive portal server.
Use HTTPS	Select this to enforce clients to use HTTPS to communicate with the captive portal server. This option is available only if RADIUS Authentication is selected.
Captive Portal Failure	This field allows you to configure Internet access for the guest users when the external captive portal server is not available. Select **Deny Internet** to prevent guest users from using the network, or **Allow Internet** to access the network.
Automatic URL Whitelisting	On enabling this for the external captive portal authentication, the URLs that are allowed for the unauthenticated users to access are automatically whitelisted.
Auth Text	If the **External Authentication splash** page is selected, specify the authentication text that is returned by the external server after successful authentication. This option is available only if Authentication Text is selected.
Redirect URL	Specify a redirect URL if you want to redirect the users to another URL.

4. Click **Save**.
5. If you want to configure a captive portal proxy server or a global proxy server to match your browser configuration, enter the IP address and port number in the **Captive-portal proxy server IP** and **Captive Portal Proxy Server Port** fields.
6. Specify encryption settings if required.
7. To exclude uplink, select an uplink type.
8. Click **Next** and then click **Finish**.

Configuring Guest Logon Role and Access Rules for Guest Users

To configure access rules for a guest network:

1. Select **Configuration** > **Access Points** > **Networks** and then click **Create New**. The **Create a New Network** pane is displayed.
2. For **Type**, select **Wireless**.
3. Enter a name that is used to identify the network in the **Name (SSID)** box.
4. Select **Guest** under **Primary Usage** and click **Next**.

5. In the **Access** tab, select any of the following types of access control:

- **Unrestricted** — Select this to set unrestricted access to the network.
- **Network Based** — Select **Network Based** to set common rules for all users in a network. By default, **Allow any to all destinations** access rule is enabled. This rule allows traffic to all destinations. To define an access rule:

    c. Click **(+)** icon and select appropriate options for **Rule Type**, **Service**, **Action**, **Destination**, and **Options** fields.

    d. Click **Save**.

- **Role Based** — Select **Role Based** to enable access based on user roles. For role-based access control:

  1. Create a user role:

     a. Click **New** in **Role** pane.

     b. Enter a name for the new role and click **OK**.

  2. Create access rules for a specific user role:

     a. Click **(+)** icon and select appropriate options for **RuleType**, **Service**, **Action**, **Destination**, and **Options** fields.

     b. Click **Save**.

  3. Create a role assignment rule.

     a. Under **Role Assignment Rule**, click **New**. The **New Role Assignment Rule** pane is displayed.

     b. Select appropriate options in **Attribute**, **Operator**, **String**, and **Role** fields.

     c. Click **Save**.

6. Click **Finish**.

Configuring Captive Portal Roles for an SSID

You can configure an access rule to enforce captive portal authentication for SSIDs with 802.1X authentication enabled. You can configure rules to provide access to an external captive portal, internal captive portal, so that some of the clients using this SSID can derive the captive portal role.

The following conditions apply to the 802.1X and captive portal authentication configuration:

- If captive portal settings are not configured for a user role, the captive portal settings configured for an SSID are applied to the client's profile.
- If captive portal settings are not configured for a SSID, the captive portal settings configured for a user role are applied to the client's profile.
- If captive portal settings are configured for both SSID and user role, the captive portal settings configured for a user role are applied to the profile of the client.

To create a captive portal role for the **Internal-acknowledged** and **External Authentication Text** splash page types:

1. Select an SSID profile from **Configuration > Access Points > Networks**, and click **Edit.**
2. Click **Access**, select **Role based**, and select an existing role or create a new one.
3. Click (**+ Add Rule**). The **Add Rules** data pane is displayed.
4. In the **Add Rules** data pane, specify the following parameters.

Table 21: *Access Rule Configuration Parameters*

Data pane item	Description
Rule Type	Select **Captive Portal** from the drop down.
Splash Page Type	Select a splash page type.
Internal	If **Internal** is selected as splash page type: ● Under **Splash Page Visuals**, use the editor to specify text and colors for the initial page that will be displayed to users connecting to the network. The initial page asks for user credentials or email, depending on the splash page type configured ● To change the welcome text, enter the required text in **Welcome Text**, and click **Save**. Ensure that the welcome text does not exceed 127 characters. ● To change the policy text, enter the required text in **Policy Text**, and click **Save**. Ensure that the policy text does not exceed 255 characters. ● To change the color of the splash page, click the box corresponding to **Body Background Color** and select the required color from the palette. ● To redirect the guest users, specify the URL in **Redirect URL**. ● To preview the captive portal page, click **Preview Splash Page**.
External	If **External** is selected, perform the following steps: ● Select a profile from **Captive Portal Profile**. ● If you want to edit the profile, click **Edit** and update the following parameters: ● **Type** — Select either **RADIUS Authentication** (to enable user authentication against a RADIUS server) or **Authentication Text** (to specify the authentication text to returned by the external server after a successful user authentication). ● **IP OR Hostname**— Enter the IP address or the hostname of the external splash page server. ● **URL**— Enter the URL for the external splash page server. ● **Port** — Enter the port number for communicating with the external splash page server. ● **Captive Portal Failure** —This field allows you to configure Internet access for the guest clients when the external captive portal server is not available. Select **Deny Internet** to prevent clients from using the network, or **Allow Internet** to allow the guest clients to access Internet when the external captive portal server is not available. ● **Automatic URL Whitelisting**— Select **Enabled** or **Disabled** to enable or disable automatic whitelisting of URLs. On selecting this for the external captive portal authentication, the URLs allowed for the unauthenticated users to access are automatically whitelisted. The automatic URL whitelisting is disabled by default. ● **Auth TEXT**— Indicates the authentication text returned by the external server after a successful user authentication. ● **Redirect URL**— Specify a redirect URL to redirect the users to another URL.

5. Click **Save**. The enforce captive portal rule is created and listed as an access rule.

6. Click **Save Settings.**

The client can connect to this SSID after authenticating with user name and password. After the user logs in successfully, the captive portal role is assigned to the client.

Disabling Captive Portal Authentication

To disable captive portal authentication, perform the following steps:

1. Select **Configuration** > **Access Points** > **Networks**.
2. Select the network profile for which captive portal needs to be disabled and then click **Edit**. The **Networks > Configuration <profile-name>** pane is displayed.
3. Select **Security** and select **None** from **Splash Page Type**.
4. Click **Save Settings.**

Configuring Walled Garden Access

Administrators can also control the resources that the guest users can access and the amount of bandwidth or air time they can use at any given time. When an external Captive portal is used, administrators can configure a walled garden, which determines access to the URLs requested by the guest users. For example, In a hotel environment, the unauthenticated users are allowed to access a designated login page (for example, a hotel website) and all its contents. Users who do not sign up for the Internet service can view only the *allowed* websites (typically hotel property websites).

Administrators can allow or block access to specific URLs by creating a whitelist and blacklist. When users attempt to access other Websites, which are not in the whitelist of the walled garden profile, users are redirected to the login page. If the requested URL is on the blacklist, it is blocked. If it appears on neither list, the request is redirected to the external Captive portal.

To create a walled garden access.

1. Select **Configuration** > **Access Points** > **Security** > **Walled Garden**. The Walled Garden details are displayed.
2. Click **Blacklist:n Whitelist:n.** The **Walled Garden** data pane is displayed**.**
3. To allow users to access a specific domain, click **New** and enter the domain name or URL in the **Whitelist** data pane. This allows access to a domain while the user remains unauthenticated. Specify a POSIX regular expression (regex(7)). For example:

- yahoo.com matches various domains such as news.yahoo.com, travel.yahoo.com and finance.yahoo.com
- www.apple.com/library/test is a subset of www.apple.com site corresponding to path /library/test/*
- favicon.ico allows access to /favicon.ico from all domains.

4. To deny users access to a domain, click **New** and enter the domain name or URL in the **Blacklist** data pane. This prevents the unauthenticated users from viewing specific websites. When a URL specified in the blacklist is accessed by an unauthenticated user, IAP sends an HTTP 403 response to the client with a simple error message.

   If the requested URL does not appear on the blacklist or whitelist list, the request is redirected to the external captive portal.
5. Select the domain name/URL and click **Edit** to modify or click **Delete** to remove the entry from the list.
6. Click **OK** to apply the changes.

Configuring Ethernet Profiles

The Ethernet ports allow third-party devices such as VoIP phones or printers (which support only wired connections) to connect to the wireless network. You can also configure an Access Control List (ACL) for additional security on the Ethernet downlink.

To configure wired settings, complete the following steps:

1. Click **Configuration**.
2. Select a group and then click **Networks**. The **Networks** page is displayed.
3. To create a new SSID profile, click the + icon. The **Create a New Network** pane is displayed.
4. Enter a name that is used to identify the network in the **Name (SSID)** box.
5. From the **Type** list, select **Wired** and configure the following parameters:

   a. **Speed/Duplex**Ensure that appropriate values are selected for **Speed/Duplex**. Contact your network administrator if you need to assign speed and duplex parameters.

   b. **PoE**—Set **PoE** to **Enabled** to enable Power over Ethernet.

   c. **Admin Status**—Ensure that an appropriate value is selected. The **Admin Status** indicates if the port is up or down.

   d. **Content Filtering**— To ensure that all DNS requests to non-corporate domains on this wired network are sent to OpenDNS, select **Enabled** for **Content Filtering**.

   e. **Uplink**—Select **Enabled** to configure uplink on this wired profile. If **Uplink** is set to **Enabled** and this network profile is assigned to a specific port, the port will be enabled as Uplink port.

   f. **Spanning Tree**—Select the **Spanning Tree** check box to enable Spanning Tree Protocol (STP) on the wired profile. STP ensures that there are no loops in any bridged Ethernet network and operates on all downlink ports, regardless of forwarding mode. STP will not operate on the uplink port and is supported only on IAPs with three or more ports. By default Spanning Tree is disabled on wired profiles.
6. Click **Next**. The **VLANs** pane details are displayed.
7. On the VLANs pane, configure VLANs for the wired network:

   a. **Mode**—Specify any of the following modes:

   - **Access**—Select this mode to allow the port to carry a single VLAN specified as the native VLAN.
   - **Trunk**—Select this mode to allow the port to carry packets for multiple VLANs specified as allowed VLANs.

   b. Specify any of the following values for **Client IP Assignment**:

   - **Virtual Controller Assigned**: Select this option to allow the Virtual Controller to assign IP addresses to the wired clients. When the Virtual Controller assignment is used, the source IP address is translated for all client traffic that goes through this interface. The Virtual Controller can also assign a guest VLAN to a wired client.
   - **Network Assigned**: Select this option to allow the clients to receive an IP address from the network to which the Virtual Controller is connected. On selecting this option, the **New** button to create a VLAN is displayed. Create a new VLAN if required.

   c. If the **Trunk** mode is selected:

   - Specify the **Allowed VLAN**, enter a list of comma separated digits or ranges 1,2,5 or 1-4, or all. The Allowed VLAN refers to the VLANs carried by the port in Access mode.
   - If the **Client IP Assignment** is set to **Network Assigned**, specify a value for **Native VLAN**. A VLAN that does not have a VLAN ID tag in the frames is referred to as Native VLAN. You can specify a value within the range of 1-4093.

   d. If the **Access** mode is selected:

   - If the **Client IP Assignment** is set to **Virtual Controller Assigned**, proceed to step 6.
   - If the **Client IP Assignment** is set to **Network Assigned**, specify a value for **Access VLAN** to indicate the VLAN carried by the port in the **Access** mode.
8. Click **Next**. The **Security** pane details are displayed.

9. On the **Security** pane, select the security options as per your requirement:

- **MAC Authentication**—To enable MAC authentication, select **Enabled**. The MAC authentication is disabled by default.
- **802.1X Authentication**—To enable 802.1X authentication, select **Enabled**.
- **MAC Authentication Fail-Through**—To enable authentication fail-thru, select **Enabled**. When this feature is enabled, 802.1X authentication is attempted when MAC authentication fails. The **MAC Authentication Fail-Through** check box is displayed only when both **MAC Authentication** and **802.1X Authentication** are **Enabled**.
- Select any of the following options for **Authentication Server 1**:
  - **New**—On selecting this option, an external RADIUS server must be configured to authenticate the users. For information on configuring an external server, see Configuring External Servers for Authentication on page 80.
  - **Internal Server**— If an internal server is selected, add the clients that are required to authenticate with the internal RADIUS server. Click the **Users** link to add the users.
- **Reauth Interval**—Specify the interval at which all associated and authenticated clients must be reauthenticated.
- **Load Balancing**— Set this to **Enabled** if you are using two RADIUS authentication servers, so that the load across the two RADIUS servers is balanced. For more information on the dynamic load balancing mechanism, see Dynamic Load Balancing between Authentication Servers on page 80.

10. Click **Next**. The **Access** pane is displayed.

11. On the **Access** pane, configure the access rule parameters.

a. Select any of the following types of access control:

- **Role-based**— Allows the users to obtain access based on the roles assigned to them.
- **Unrestricted**— Allows the users to obtain unrestricted access on the port.
- **Network-based**— Allows the users to be authenticated based on access rules specified for a network.

b. If the **Role-based** access control is selected:

- Under **Role**, select an existing role for which you want to apply the access rules, or click **New** and add the required role. To add a new access rule, click **Add Rule** under **Access Rules For Selected Roles**.

NOTE

The default role with the same name as the network is automatically defined for each network. The default roles cannot be modified or deleted.

- Configure role assignment rules. To add a new role assignment rule, click **New** under **Role Assignment Rules**. Under **New Role Assignment Rule**:

a. select an attribute.

b. Specify an operator condition.

c. Select a role.

d. Click **Save**.

12. Click **Next**. The **Network Assignment** pane is displayed.

13. On the **Network Assignment** pane, assign wired profiles to Ethernet ports:

e. Select a profile from the **0/0** drop down list.

f. Select the profile from the **0/1** drop down list.

g. If the IAP supports Enet2, Enet3 and Enet4 ports, assign profiles to these ports by selecting a profile from the **0/2**, **0/3**, and **0/4** drop-down list respectively.

14. Click **Finish**.

Editing a Network Profile

To edit a network profile, complete the following steps:

1. Click **Configuration**.
2. Select a group and then click **Networks**.
3. Select the network that you want to edit.
4. Click the **Edit** icon under **Actions** column. The network details are displayed.
5. Modify the profile.
6. Click **Save Settings** to save the changes.

Deleting a Network Profile

To delete a network profile, complete the following steps:

1. Click **Configuration**.
2. Select a group and then click **Networks**.
3. Select the network that you want to delete.
4. Click the **Delete** icon under **Actions** column. A delete confirmation pane is displayed.
5. Click **OK**.

Configuring Time Based Services

Central allows you to configure the availability of a WLAN SSID at a particular time of the day. You can now create a time range profile and assign it to a WLAN SSID, so that you can enable or disable access to the SSID and thus control user access to the network during a specific time period.

Before you configure time based services, ensure that the NTP server connection is active.

Creating a Time Range Profile

To create a time range profile, complete the following steps:

1. Click **Configuration**.
2. Select a group and click **Access Points** > **System** on the left pane. The System page opens.
3. Click **Time Based Services**.
4. Click **+** under Time Range Profiles. The **New Profile** window for creating time range profiles opens. Configure the parameters listed in the following table:

Table 22: *Time Range Profile Configuration Parameters*

Parameter	Description
Name	Specify a name for the time range profile.
Type	Select the type of time range profile. ● **Periodic**— When configured, the state of the SSID changes based on the time range configured in the profile. ● **Absolute**—When configured, the state of the SSID changes during a specific date / day and time.
Period Type	For periodic time range profiles, specify a periodic interval (day / weekday / weekend / daily) at which the time range profile must be applied.
Start Day and **End Day**	For absolute time range profiles, specify the start day and end day to configure a specific time period during which the time range profile is applied.
Start Time	Select the start time for the time range profile in the hh:mm format.
End Time	Choose the end time for the time range profile in hh:mm format.

Associating a Time Range Profile to an SSID

To apply a time range profile to an SSID, complete the following steps:

1. Click **Configuration** > **Networks**.
2. Click the edit icon next to the SSID to which you want to apply the time range profile.
3. Click **Advanced Settings**.
4. Under **Time Range**, click **Edit**. Select a time range profile from the list and select a value from the **Status** drop-down list.

- When a time range profile is enabled on SSID, the SSID is made available to the users for the configured time range. For example, if the specified time range is 12:00 to 13:00, the SSID becomes available only between 12 PM to 1 PM on a given day.
- If a time range is disabled, the SSID becomes unavailable for the configured time range. For example, if configured time-range is 14:00 to 17:00, the SSID is made unavailable from 2 PM to 5 PM on a given day.

5. Click **Save**.

For more information on time range configuration, see the *Aruba Instant User Guide*.

Configuring ARM and RF Parameters

This section provides the following information:

- ARM Overview on page 66
- Configuring ARM Features on page 66
- Configuring Radio Parameters on page 69

ARM Overview

ARM is a radio frequency management technology that optimizes WLAN performance even in the networks with highest traffic by dynamically and intelligently choosing the best 802.11 channel and transmitting power for each IAP in its current RF environment. ARM works with all standard clients, across all operating systems, while remaining in compliance with the IEEE 802.11 standards. It does not require any proprietary client software to achieve its performance goals. ARM ensures low-latency roaming, consistently high performance, and maximum client compatibility in a multi-channel environment. By ensuring the fair distribution of available Wi-Fi bandwidth to mobile devices, ARM ensures that data, voice, and video applications have sufficient network resources at all times. ARM allows mixed 802.11a, b, g, n, and ac client types to inter operate at the highest performance levels.

When ARM is enabled, an IAP dynamically scans all 802.11 channels within its 802.11 regulatory domain at regular intervals and sends reports on network (WLAN) coverage, interference, and intrusion detection to the Virtual Controller. ARM computes coverage and interference metrics for each valid channel, chooses the best performing channel, and transmit power settings for each IAP RF environment. Each IAP gathers other metrics on its ARM-assigned channel to provide a snapshot of the current RF health state.

IAPs support the following ARM features:

- Channel or Power Assignment—Assigns channel and power settings for all the IAPs in the network according to changes in the RF environment.
- Voice Aware Scanning—Improves voice quality by preventing an IAP from scanning for other channels in the RF spectrum during a voice call and by allowing an IAP to resume scanning when there are no active voice calls.
- Load Aware Scanning—Dynamically adjusts the scanning behavior to maintain uninterrupted data transfer on resource intensive systems when the network traffic exceeds a predefined threshold.
- Bandsteering—Assigns the dual-band capable clients to the 5 GHz band on dual-band IAPs thereby reducing co-channel interference and increasing the available bandwidth for dual-band clients.
- Client Match—Continually monitors the RF neighborhood of the client to support the ongoing band steering and load balancing of channels, and enhanced IAP reassignment for roaming mobile clients.

NOTE

When Client Match is enabled on 802.11n capable IAPs, the Client Match feature overrides any settings configured for the legacy band steering, station hand-off assist or load balancing features. The 802.11ac capable IAPs do not support the legacy band steering, station hand off or load balancing settings, so these IAPs must be managed using Client Match.

- Airtime Fairness—Provides equal access to all clients on the wireless medium, regardless of client type, capability, or operating system to deliver uniform performance to all clients.

For more information on ARM features supported by the APs, see the *Aruba Instant User Guide*.

Configuring ARM Features

To configure ARM features such as band steering, and airtime fairness mode and Client Match, complete the following steps:

1. Click **Configuration** >**Access Points**> **RF** > **ARM**. The ARM details are displayed.
2. Click **Client Control**.
3. For **Band Steering Mode**, configure the following parameters:

Table 23: *Band Steering Mode Configuration Parameters*

Data pane item	Description
Prefer 5 GHz	Enables band steering in the 5 GHz mode. On selecting this, the IAP steers the client to the 5 GHz band (if the client is 5 GHz capable), but allows the client connection on the 2.4 GHz band if the client persistently attempts for 2.4 GHz association.
Force 5 GHz	Enforces 5 GHz band steering mode on the IAPs.
Balance Bands	Allows the IAP to balance the clients across the two radios to best utilize the available 2.4 GHz bandwidth. This feature takes into account the fact that the 5 GHz band has more channels than the 2.4 GHz band, and that the 5 GHz channels operate in 40 MHz, while the 2.5 GHz band operates in 20 MHz.
Disable	Allows the clients to select the band to use.

4. For **Airtime Fairness Mode**, specify any of the following values:

Table 24: *Airtime Fairness Mode Configuration Parameters*

Data Pane Item	Description
Default Access	Allows access based on client requests. When **Air Time Fairness** is set to default access, per user, and per SSID bandwidth limits are not enforced.
Fair Access	Allocates air time evenly across all the clients.
Preferred Access	Sets a preference where 802.11n clients are assigned more air time than 802.11a/11g. The 802.11a/11g clients get more airtime than 802.11b. The ratio is 16:4:1.

5. For Client Match, configure the following parameters:

Table 25: *Additional ARM Configuration Parameters*

Data Pane Item	Description
Client Match	Enables the Client Match feature on APs. When enabled, client count is balanced among all the channels in the same band. When Client Match is enabled, ensure that scanning is enabled. **NOTE:** When the Client Match is disabled, channels can be changed even when the clients are active on a BSSID.
CM Calculating Interval	Configures a value for the calculating interval of Client Match. The interval is specified in seconds and the default value is 30 seconds. You can specify a value within the range of 10-600.
CM Neighbor Matching%	Configures the calculating interval of Client Match. This number takes into account the least similarity percentage to be considered as in the same virtual RF neighborhood of Client Match. You can specify a percentage value within the range of 20-100. The default value is 75%.
CM Threshold	Configures a Client Match threshold value. This number takes acceptance client count difference among all the channels of Client Match. When the client load on an AP reaches or exceeds the threshold in comparison, Client Match is enabled on that AP. You can specify a value within range of 1-20. The default value is 2.
SLB Mode	Enables the **SLB Mode** to determine the balancing strategy for Client Match. The following options are available: ● Channel ● Radio ● Channel + Radio

6. Click **Access Point Control**, and configure the following parameters:

Table 26: *AP Control Configuration Parameters*

Data pane item	Description
Customize Valid Channels	Allows you to select a custom list of valid 20 MHz and 40 MHz channels for 2.4 GHz and 5 GHz bands. By default, the AP uses valid channels as defined by the Country Code (regulatory domain). On selecting **Customize Valid Channels**, a list of valid channels for both 2.4.GHz and 5 GHz are displayed. The valid channel customization feature is disabled by default. The valid channels automatically show in the **static channel assignment** data pane.
Minimum Transmit Power	Allows you to configure a minimum transmission power within a range of 3 to 33 dBm in 3 dBm increments. If the minimum transmission EIRP setting configured on an AP is not supported by the AP model, this value is reduced to the highest supported power setting. The default value for minimum transmit power is 18 dBm.
Maximum Transmit Power	Allows you to configure the maximum transmission power within a range of 3 to 33 dBm in 3 dBm increments. If the maximum transmission EIRP configured on an AP is not supported by the local regulatory requirements or AP model, the value is reduced to the highest supported power setting. s
Client Aware	Allows ARM to control channel assignments for the IAPs with active clients. When the Client Match mode is set to **Disabled**, an IAP may change to a more optimal channel, which disrupts current client traffic. The **Client Aware** option is **Enabled** by default.
Scanning	Allows the IAP to dynamically scan all 802.11 channels within its 802.11 regulatory domain at regular intervals. This scanning report includes WLAN coverage, interference, and intrusion detection data. **NOTE:** For Client Match configuration, ensure that scanning is enabled.
Wide Channel Bands	Allows the administrators to configure 40 MHz channels in the 2.4 GHz and 5.0 GHz bands. 40 MHz channels are two 20 MHz adjacent channels that are bonded together. The 40 MHz channel effectively doubles the frequency bandwidth available for data transmission. For high performance, you can select 5 GHz. If the AP density is low, enable in the 2.4 GHz band.
80 MHz Support	Enables or disables the use of 80 MHz channels on APs. This feature allows ARM to assign 80 MHz channels on APs with 5 GHz radios, which support a very high throughput. This setting is enabled by default. **NOTE:** Only the APs that support 802.11ac can be configured with 80 MHz channels.

7. Click **Save Settings**.

Configuring Radio Parameters

To configure RF parameters for the 2.4 GHz and 5 GHz radio bands on an IAP, complete the following steps:

1. Select **Configuration**>**Access Points** > **RF** >**Radio**. The Radio details are displayed.
2. Under 2.4 GHz, 5 GHz, or both, configure the following parameters.

Table 27: *Radio Configuration Parameters*

Data pane item	Description
Legacy Only	When set to **ON**, the IAP runs the radio in the non-802.11n mode. This option is set to **OFF** by default.
802.11d / 802.11h	When set to **ON**, the radios advertise their 802.11d (Country Information) and 802.11h (Transmit Power Control) capabilities. This option is set to **OFF** by default.
Beacon Interval	Configures the beacon period for the IAP in milliseconds. This indicates how often the 802.11 beacon management frames are transmitted by the AP. You can specify a value within the range of 60–500. The default value is 100 milliseconds.
Interference Immunity Level	Configures the immunity level to improve performance in high-interference environments. The default immunity level is 2. ● **Level 0** — No ANI adaptation. ● **Level 1** — Noise immunity only. This level enables power-based packet detection by controlling the amount of power increase that makes a radio aware that it has received a packet. ● **Level 2** — Noise and spur immunity. This level also controls the detection of OFDM packets, and is the default setting for the Noise Immunity feature. ● **Level 3** — Level 2 settings and weak OFDM immunity. This level minimizes false detects on the radio due to interference, but may also reduce radio sensitivity. This level is recommended for environments with a high-level of interference related to 2.4 GHz appliances such as cordless phones. ● **Level 4** — Level 3 settings, and FIR immunity. At this level, the AP adjusts its sensitivity to in-band power, which can improve performance in environments with high and constant levels of noise interference. ● **Level 5** — The AP completely disables PHY error reporting, improving performance by eliminating the time the IAP spends on PHY processing. **NOTE:** Increasing the immunity level makes the AP lose a small amount of range.
Channel Switch Announcement Count	Configures the number of channel switching announcements to be sent before switching to a new channel. This allows the associated clients to recover gracefully from a channel change.

Data pane item	Description
Background Spectrum Monitoring	When set to **ON**, the APs in the access mode continue with their normal access service to clients, while performing additional function of monitoring RF interference (from both neighboring APs and non Wi-Fi sources such as, microwaves and cordless phones) on the channel they are currently serving the clients.
Customize ARM Power Range	Configures a minimum (Min Power) and maximum (Max Power) power range value for the 2.4 GHz and 5GHz band frequencies. The default value is 3 dBm. Unlike the configuration in the ARM profile, the transmit power of all radios in the Radio profile do not share the same configuration.
Very high throughput	When set to **ON**, the very high throughput (VHT) is enabled on the 802.11ac devices for the 5GHz radio band. If VHT is enabled for the 5 GHz radio profile on an IAP, it is automatically enabled for all SSIDs configured on an IAP. By default, VHT is enabled on all SSIDs. **NOTE:** If you want the 802.11ac IAPs to function as 802.11n IAPs, clear this check box to disable VHT on these devices.

3. Click **Save Settings**.

Configuring IDS Parameters

Central supports the Intrusion Detection System (IDS) feature that monitors the network for the presence of unauthorized IAPs and clients. It also logs information about the unauthorized IAPs and clients, and generates reports based on the logged information.

Rogue APs

The IDS feature in the Central network enables you to detect rogue APs, interfering APs, and other devices that can potentially disrupt network operations. A rogue AP is an unauthorized AP plugged into the wired side of the network. An interfering AP is an AP seen in the RF environment, but it is not connected to the wired network. While the interfering AP can potentially cause RF interference, it is not considered a direct security threat, because it is not connected to the wired network. However, an interfering AP may be reclassified as a rogue AP.

The built-in IDS scans for APs that are not controlled by the VC. These are listed and classified as either Interfering or Rogue, depending on whether they are on a foreign network or your network.

Configuring Wireless Intrusion Detection and Protection Policies

You can configure the following options:

- **Infrastructure Detection Policies** — Specifies the policy for detecting wireless attacks on APs.
- **Client Detection Policies** — Specifies the policy for detecting wireless attacks on clients.
- **Infrastructure Protection Policies** — Specifies the policy for protecting APs from wireless attacks.
- **Client Protection Policies** — Specifies the policy for protecting clients from wireless attacks.
- **Containment Methods** — Prevents unauthorized stations from connecting to your Central network.

Each of these options contains several default levels that enable different sets of policies. An administrator can customize enable or disable these options accordingly. The detection levels can be configured using the **IDS** pane. The following levels of detection can be configured in the WIP Detection page:

- **Off**
- **Low**

- **Medium**
- **High**

The following table describes the detection policies enabled in the Infrastructure Detection **Custom settings** field.

Table 28: *Infrastructure Detection Policies*

Detection level	Detection policy
Off	Rogue Classification
Low	● Detect AP Spoofing ● Detect Windows Bridge ● IDS Signature — Deauthentication Broadcast ● IDS Signature — Deassociation Broadcast
Medium	● Detect Adhoc networks using VALID SSID — Valid SSID list is auto-configured based on AP configuration ● Detect Malformed Frame — Large Duration
High	● Detect AP Impersonation ● Detect Adhoc Networks ● Detect Valid SSID Misuse ● Detect Wireless Bridge ● Detect 802.11 40MHz intolerance settings ● Detect Active 802.11n Greenfield Mode ● Detect AP Flood Attack ● Detect Client Flood Attack ● Detect Bad WEP ● Detect CTS Rate Anomaly ● Detect RTS Rate Anomaly ● Detect Invalid Address Combination ● Detect Malformed Frame — HT IE ● Detect Malformed Frame — Association Request ● Detect Malformed Frame — Auth ● Detect Overflow IE ● Detect Overflow EAPOL Key ● Detect Beacon Wrong Channel ● Detect devices with invalid MAC OUI

The following table describes the detection policies enabled in the Client Detection **Custom settings** field.

Table 29: *Client Detection Policies*

Detection level	Detection policy
Off	All detection policies are disabled.
Low	• Detect Valid Station Misassociation
Medium	• Detect Disconnect Station Attack • Detect Omerta Attack • Detect FATA-Jack Attack • Detect Block ACK DOS • Detect Hotspotter Attack • Detect unencrypted Valid Client • Detect Power Save DOS Attack
High	• Detect EAP Rate Anomaly • Detect Rate Anomaly • Detect Chop Chop Attack • Detect TKIP Replay Attack • IDS Signature — Air Jack • IDS Signature — ASLEAP

The following levels of detection can be configured in the WIP Protection page:

- **Off**
- **Low**
- **High**

The following table describes the protection policies that are enabled in the Infrastructure Protection **Custom settings** field.

Table 30: *Infrastructure Protection Policies*

Protection level	Protection policy
Off	All protection policies are disabled
Low	• Protect SSID — Valid SSID list is auto derived from AP configuration • Rogue Containment
High	• Protect from Adhoc Networks • Protect AP Impersonation

The following table describes the detection policies that are enabled in the Client Protection **Custom settings** field.

Table 31: *Client Protection Policies*

Protection level	Protection policy
Off	All protection policies are disabled
Low	Protect Valid Station
High	Protect Windows Bridge

Containment Methods

You can enable wired and wireless containment measures to prevent unauthorized stations from connecting to your Central network.

Central supports the following types of containment mechanisms:

- Wired containment — When enabled, IAPs generate ARP packets on the wired network to contain wireless attacks.
- Wireless containment — When enabled, the system attempts to disconnect all clients that are connected or attempting to connect to the identified AP.
  - None — Disables all the containment mechanisms.
  - Deauthenticate only — With deauthentication containment, the AP or client is contained by disrupting the client association on the wireless interface.
  - Tarpit containment — With tarpit containment, the AP is contained by luring clients that are attempting to associate with it to a tarpit. The tarpit can be on the same channel or a different channel as the AP being contained.

NOTE

The Federal Communications Commission (FCC) and some third parties have alleged that under certain circumstances, the use of containment functionality violates 47 U.S.C. §333. Before using any containment functionality, ensure that your intended use is allowed under the applicable rules, regulations, and policies. Aruba is not liable for any claims, sanctions, or other direct, indirect, special, consequential or incidental damages related to your use of containment functionality.

Configuring Authentication and Security Parameters

This section provides the following information:

- Supported Authentication Methods on page 75
- Supported Authentication Servers on page 78
- Configuring External Servers for Authentication on page 80
- Configuring Authentication Parameters for IAP Management Users on page 82
- Configuring Users for Internal Database of an IAP on page 83
- Configuring Roles and Policies for User Access Control on page 84
- Configuring ALG Protocols on page 91
- Blacklisting Clients on page 91

Supported Authentication Methods

Authentication is a process of identifying a user through a valid username and password. Clients can also be authenticated based on their MAC addresses.

The authentication methods supported by the IAPs managed through Central are described in the following sections.

802.1X Authentication

802.1X is a method for authenticating the identity of a user before providing network access to the user. The Central network supports internal RADIUS server and external RADIUS server for 802.1X authentication. For authentication purpose, the wireless client can associate to a network access server (NAS) or RADIUS client such as a wireless IAP. The wireless client can pass data traffic only after successful 802.1X authentication.

NOTE

The NAS acts as a gateway to guard access to a protected resource. A client connecting to the wireless network first connects to the NAS.

Configuring 802.1X Authentication for a Network Profile

To configure 802.1X authentication for a wireless network profile, complete the following steps:

1. Select **Configuration** > **Access Points** > **Networks**, select an existing profile for which you want to enable 802.1X authentication, and click **Edit**.
2. In **Edit <profile-name>**, ensure that all required WLAN and VLAN attributes are defined, and then click the **Security** tab.
3. Under **Security**, for the **Enterprise** security level, select the preferred option from **Key Management**.
4. To terminate the EAP portion of 802.1X authentication on the IAP instead of the RADIUS server, set **Termination** to **Enabled**.

   For 802.1X authorization, by default, the client conducts an EAP exchange with the RADIUS server, and the AP acts as a relay for this exchange. When **Termination** is enabled, the IAP itself acts as an authentication server, terminates the outer layers of the EAP protocol, and only relays the innermost layer to the external RADIUS server.
5. Specify the type of authentication server to use.
6. Click **Save Settings**.

MAC Authentication

Media Access Control (MAC) authentication is used for authenticating devices based on their physical MAC addresses. MAC authentication requires that the MAC address of a machine matches a manually defined list of addresses. This authentication method is not recommended for scalable networks and the networks that require stringent security settings.

MAC authentication can be used alone or it can be combined with other forms of authentication such as WEP authentication.

Configuring MAC Authentication for a Network Profile

To configure MAC authentication for a wireless profile, complete the following steps:

1. Select **Configuration > Network**, select an existing profile for which you want to enable MAC authentication and click **Edit**.
2. In the **Edit <profile-name>,** ensure that all required WLAN and VLAN attributes are defined, and then click the **Security** tab**.**
3. In **Security**, for **MAC Authentication**, select **Enabled** for **Personal** or **Open** security level.
4. Specify the type of authentication server to use.
5. Click **Save Settings**.

MAC Authentication with 802.1X Authentication

The administrators can enable MAC authentication for 802.1X authentication. MAC authentication shares all the authentication server configurations with 802.1X authentication. If a wireless or wired client connects to the network, MAC authentication is performed first. If MAC authentication fails, 802.1X authentication does not trigger. If MAC authentication is successful, 802.1X authentication is attempted. If 802.1X authentication is successful, the client is assigned an 802.1X authentication role. If 802.1X authentication fails, the client is assigned a **deny-all** role or **mac-auth-only** role.

You can also configure the following authentication parameters for MAC+802.1X authentication:

- MAC authentication only role—Allows you to create a **mac-auth-only** role to allow role-based access rules when MAC authentication is enabled for 802.1X authentication. The **mac-auth-only** role is assigned to a client when the MAC authentication is successful and 802.1X authentication fails. If 802.1X authentication is successful, the **mac-auth-only** role is overwritten by the final role. The **mac-auth-only** role is primarily used for wired clients.
- L2 authentication fall-through—Allows you to enable the **l2-authentication-fallthrough** mode. When this option is enabled, the 802.1X authentication is allowed even if the MAC authentication fails. If this option is disabled, 802.1X authentication is not allowed. The **l2-authentication-fallthrough** mode is disabled by default.

Configuring MAC Authentication with 802.1X Authentication

To configure MAC authentication with 802.1X authentication for wireless network profile, configure the following parameters:

1. Select **Configuration > Network**, select an existing profile for which you want to enable MAC and 802.1X authentication and click **Edit**.
2. Click **Security**.
3. Select **Perform MAC Authentication Before 802.1X** to use 802.1X authentication only when the MAC authentication is successful.
4. Select **MAC Authentication Fail Through** to use 802.1X authentication even when the MAC authentication fails.
5. Click **Save Settings**.

Captive Portal Authentication

Captive portal authentication is used for authenticating guest users. For more information, see Configuring Captive Portal Profiles for Guest Network on page 54.

MAC Authentication with Captive Portal Authentication

The following conditions apply to a network profile with MAC authentication and Captive Portal authentication enabled:

- If the captive portal splash page type is **Internal-Authenticated** or **External-RADIUS Server**, MAC authentication reuses the server configurations.
- If the captive portal splash page type is **Internal-Acknowledged** or **External-Authentication Text** and MAC authentication is enabled, a server configuration page is displayed.
- If the captive portal splash page type is **none**, MAC authentication is disabled.

The MAC authentication with captive portal authentication supports the **mac-auth-only** role.

Configuring MAC Authentication with Captive Portal Authentication

To configure the MAC authentication with captive portal authentication for a network profile, complete the following steps:

1. Select an existing wireless profile for which you want to enable MAC with captive portal authentication. Depending on the network profile selected, the **Edit <WLAN-Profile>** data pane is displayed.
2. In **Access**, specify the following parameters for a network with **Role Based** rules:
   a. Select **Enforce Machine Authentication** when MAC authentication is enabled for captive portal. If the MAC authentication fails, the captive portal authentication role is assigned to the client.
   b. For wireless network profile, select **Enforce MAC Auth Only Role** when MAC authentication is enabled for captive portal. After successful MAC authentication, the **MAC auth only** role is assigned to the client.
3. Click **Next** and then click **Save Settings**.

802.1X Authentication with Captive Portal Authentication

This authentication method allows you to configure different Captive portal settings for clients on the same SSID. For example, you can configure an 802.1X SSID and create a role for captive portal access, so that some of the clients using the SSID derive the captive portal role. You can configure rules to indicate access to external or internal Captive portal, or none.

For more information on configuring Captive portal roles for an SSID with 802.1X authentication, see Configuring Captive Portal Roles for an SSID on page 59.

WISPr Authentication

Wireless Internet Service Provider roaming (WISPr) authentication allows a smart client to authenticate on the network when they roam between wireless Internet service providers, even if the wireless hotspot uses an Internet Service Provider (ISP) with whom the client may not have an account.

If a hotspot is configured to use WISPr authentication in a specific ISP and a client attempts to access the Internet at that hotspot, the WISPr AAA server configured for the ISP authenticates the client directly and allows the client to access the network. If the client only has an account with a *partner* ISP, the WISPr AAA server forwards the client's credentials to the partner ISP's WISPr AAA server for authentication. When the client is authenticated on the partner ISP, it is also authenticated on your hotspot's own ISP as per their service agreements. The IAP assigns the default WISPr user role to the client when your ISP sends an authentication message to the IAP.

IAPs support the following smart clients:

- iPass
- Boingo

These smart clients enable client authentication and roaming between hotspots by embedding iPass Generic Interface Specification (GIS) *redirect*, *authentication*, and *logoff* messages within HTML messages that are sent to the IAP.

Configuring WISPr Authentication

To configure WISPr authentication, complete the following steps:

1. Click **Configuration**> **System.**
2. Select **WISPr**. The **WISPr** details are displayed. Configure the following parameters:

- **ISO Country Code**—The ISO Country Code for the WISPr Location ID.
- **E.164 Area Code**—The E.164 Area Code for the WISPr Location ID.
- **Operator Name**—The operator name of the hotspot.
- **E.164 Country Code**—The E.164 Country Code for the WISPr Location ID.
- **SSID/Zone**—The SSID/Zone for the WISPr Location ID.
- **Location Name**—Name of the hotspot location. If no name is defined, the name of the IAP, to which the user is associated, is used.

3. Click **Save Settings** to apply the changes.

The WISPr RADIUS attributes and configuration parameters are specific to the RADIUS server used by your ISP for the WISPr authentication. Contact your ISP to determine these values. You can find a list of ISO and ITU country and area codes at the ISO and ITU websites (www.iso.org and http://www.itu.int).

NOTE

A Boingo smart client uses a NAS identifier in the format <CarrierID>_<VenueID> for location identification. To support Boingo clients, ensure that you configure the NAS identifier parameter in the RADIUS server profile for the WISPr server.

Walled Garden

On the Internet, a walled garden typically controls access to web content and services. The Walled garden access is required when an external captive portal is used. For example, a hotel environment where the unauthenticated users are allowed to navigate to a designated login page (for example, a hotel website) and all its contents.

The users who do not sign up for the Internet service can view the allowed websites (typically hotel property websites). The website names must be DNS-based and support the option to define wildcards. When a user attempts to navigate to other websites that are not in the whitelist of the walled garden profile, the user is redirected to the login page. IAP supports Walled Garden only for the HTTP requests. For example, if you add yahoo.com in Walled Garden whitelist and the client sends an HTTPS request (https://yahoo.com), the requested page is not displayed and the users are redirected to the captive portal login page.

In addition, a blacklisted walled garden profile can also be configured to explicitly block the unauthenticated users from accessing some websites.

Configuring Walled Garden Access

To configure walled garden access, complete the following steps:

1. Click the **Configuration**> **Security** > **Walled Garden**.

2. To allow access to a specific set of websites, create a whitelist, click + and add the domain names. This allows access to a domain while the user remains unauthenticated. Specify a POSIX regular expression (regex(7)). For example:

- yahoo.com matches various domains such as news.yahoo.com, travel.yahoo.com and finance.yahoo.com
- www.apple.com/library/test is a subset of www.apple.com site corresponding to path /library/test/*
- favicon.ico allows access to /favicon.ico from all domains.

3. To deny users access to a domain, click + under Blacklist, and enter the domain name in the window. This prevents the unauthenticated users from viewing specific websites. When a URL specified in the blacklist is accessed by an unauthenticated user, IAP sends an HTTP 403 response to the client with an error message.

4. Click **OK**.

Supported Authentication Servers

Based on the security requirements, you can configure internal or external Remote Authentication Dial In User Service (RADIUS) servers. This section describes the types of authentication servers and authentication termination, that can be configured for a network profile:

External RADIUS Server

In the external RADIUS server, the IP address of the VC is configured as the NAS IP address. Central RADIUS is implemented on the VC, and this eliminates the need to configure multiple NAS clients for every IAP on the RADIUS server for client authentication. Central RADIUS dynamically forwards all the authentication requests from a NAS to a remote RADIUS server. The RADIUS server responds to the authentication request with an

Access-Accept or **Access-Reject** message, and users are allowed or denied access to the network depending on the response from the RADIUS server.

When you enable an external RADIUS server for the network, the client on the IAP sends a RADIUS packet to the local IP address. The external RADIUS server then responds to the RADIUS packet.

Central supports the following external authentication servers:

- RADIUS
- LDAP

To use an LDAP server for user authentication, configure the LDAP server on the VC, and configure user IDs and passwords.

To use a RADIUS server for user authentication, configure the RADIUS server on the VC.

RADIUS Server Authentication with VSA

An external RADIUS server authenticates network users and returns to the IAP the Vendor-Specific Attribute (VSA) that contains the name of the network role for the user. The authenticated user is placed into the management role specified by the VSA.

Internal RADIUS Server

Each IAP has an instance of free RADIUS server operating locally. When you enable the internal RADIUS server option for the network, the client on the IAP sends a RADIUS packet to the local IP address. The internal RADIUS server listens and replies to the RADIUS packet.

The following authentication methods are supported in the Central network:

- EAP-TLS — The Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) method supports the termination of EAP-TLS security using the internal RADIUS server. The EAP-TLS requires both server and Certification Authority (CA) certificates installed on the IAP. The client certificate is verified on the VC (the client certificate must be signed by a known CA), before the username is verified on the authentication server.
- EAP-TTLS (MSCHAPv2) — The Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS) method uses server-side certificates to set up authentication between clients and servers. However, the actual authentication is performed using passwords.
- EAP-PEAP (MSCHAPv2) — The Extensible Authentication Protocol-Protected Extensible Authentication Protocol (EAP-PEAP) is an 802.1X authentication method that uses server-side public key certificates to authenticate clients with server. The PEAP authentication creates an encrypted SSL / TLS tunnel between the client and the authentication server. Exchange of information is encrypted and stored in the tunnel ensuring the user credentials are kept secure.
- LEAP— Lightweight Extensible Authentication Protocol (LEAP) uses dynamic Wired Equivalent Privacy (WEP) keys for authentication between the client and authentication server.

To use the internal database of an AP for user authentication, add the names and passwords of the users to be authenticated.

NOTE

Aruba does not recommend the use of LEAP authentication because it does not provide any resistance to network attacks.

Authentication Termination on IAP

Central allows EAP termination for PEAP-Generic Token Card (PEAP-GTC) and Protected Extensible Authentication Protocol-Microsoft Challenge Authentication Protocol version 2 (PEAP-MSCHAPv2). PEAP-GTC termination allows authorization against an LDAP server and external RADIUS server while PEAP-MSCHAPv2 allows authorization against an external RADIUS server.

This allows the users to run PEAP-GTC termination with their username and password to a local Microsoft Active Directory server with LDAP authentication.

- EAP-GTC— This EAP method permits the transfer of unencrypted usernames and passwords from client to server. The EAP-GTC is mainly used for one-time token cards such as SecureID and the use of LDAP or RADIUS as the user authentication server. You can also enable caching of user credentials on the IAP to an external authentication server for user data backup.
- EAP-MSCHAPv2— This EAP method is widely supported by Microsoft clients. A RADIUS server must be used as the back-end authentication server.

Dynamic Load Balancing between Authentication Servers

You can configure two authentication servers to serve as a primary and backup RADIUS server and enable load balancing between these servers. Load balancing of authentication servers ensures that the authentication load is split across multiple authentication servers and enables the IAPs to perform load balancing of authentication requests destined to authentication servers such as RADIUS or LDAP.

The load balancing in IAP is performed based on the outstanding authentication sessions. If there are no outstanding sessions and if the rate of authentication is low, only primary server will be used. The secondary is used only if there are outstanding authentication sessions on the primary server. With this, the load balance can be performed across asymmetric capacity RADIUS servers without the need to obtain inputs about the server capabilities from the administrators.

Configuring External Servers for Authentication

You can configure an external RADIUS server, TACACS or LDAP server for user authentication. To configure a server, complete the following steps:

1. Select **Configuration > Access Points > Security > Authentication Servers**.
2. To create a new server, click **New**. A pane for specifying details for the new server is displayed.
3. Configure any of the following types of server:

Type of Server	Parameters
RADIUS	Configure the following parameters: ● Name—Name of the external RADIUS server. ● IP Address— IP address of the external RADIUS server. ● Auth Port—Authorization port number of the external RADIUS server. The default port number is 1812. ● Accounting Port—The accounting port number used for sending accounting records to the RADIUS server. The default port number is 1813. ● Shared Key and Retype Shared Key—Shared key for communicating with the external RADIUS server. ● Timeout—The timeout duration for one RADIUS request. The IAP retries sending the request several times (as configured in the **Retry count**) before the user is disconnected. For example, if the **Timeout** is 5 seconds, **Retry counter** is 3, user is disconnected after 20 seconds. The default value is 5 seconds. ● Retry Count—The maximum number of authentication requests that can be sent to the server group by the IAP. You can specify a value within the range of 1–5. The default value is 3 requests. ● RFC 3576—To allow the APs to process RFC 3576-compliant CoA and disconnect messages from the RADIUS server, select **Enabled**. Disconnect messages terminate the user session immediately, whereas the CoA messages modify session authorization attributes such as data filters. ● NAS IP Address—Enter the VC IP address. The NAS IP address is the VC IP address that is sent in data packets. ● NAS Identifier—Use this to configure strings for RADIUS attribute 32, NAS Identifier, to be sent with RADIUS requests to the RADIUS server. ● Dead Time—Specify a dead time for authentication server in minutes. When two or more authentication servers are configured on the IAP and a server is unavailable, the dead time configuration determines the duration for which the authentication server is available if the server is marked as unavailable. ● Dynamic RADIUS Proxy Parameters—If Dynamic RADIUS Proxy is enabled under **Configuration > Access Points** > **System**, specify the following dynamic RADIUS proxy parameters: ● DRP IP—IP address to be used as source IP for RADIUS packets. ● DRP MASK—Subnet mask of the DRP IP address. ● DRP VLAN—VLAN in which the RADIUS packets are sent. ● DRP GATEWAY—Gateway IP address of the DRP VLAN.
LDAP	Configure the following parameters: ● Name—Name of the LDAP server ● IP Address—IP address of the LDAP server ● Auth Port—Authorization port number of the LDAP server. The default port number is 389. ● Admin-DN—A distinguished name for the admin user with read and search privileges across all the entries in the LDAP database (the admin user need not have write privileges, but the admin user must be able to search the database, and read attributes of other users in the database). ● Admin Password and Retype Admin Password—Password for the admin user. ● Base-DN— Distinguished name for the node that contains the entire user database.

Type of Server	Parameters
	● Filter—The filter to apply when searching for a user in the LDAP database. The default filter string is **(objectclass=*)** ● Key Attribute— The attribute to use as a key while searching for the LDAP server. For Active Directory, the value is **sAMAccountName**. ● Timeout—Timeout interval within a range of 1–30 seconds for one RADIUS request. The default value is 5. ● Retry Count—The maximum number of authentication requests that can be sent to the server group. You can specify a value within the range of 1–5. The default value is 3.
TACACS	Configure the following parameters: ● Name—Name of the server. ● Shared Key and Retype Key—The secret key to authenticate communication between the TACACS client and server. ● Auth Port—The TCP IP port used by the server. The default port number is 49. ● Timeout—A number between 1 and 30 seconds to indicate the timeout period for TACACS+ requests. The default value is 20 seconds. ● IP Address—IP address of the server. ● Retry Count—The maximum number of authentication attempts to be allowed. The default value is 3.
CoA	Configure the following parameters: ● Name—Name of the server. ● IP Address—IP address of the server. ● BONJOUR Support CoA Port—A port number for sending Bonjour support CoA on a different port than on the standard CoA port. The default value is 5999. ● Shared Key and Retype Key—A shared key for communicating with the external RADIUS server.

4. Click **Save Server**.

To assign the authentication server to a network profile, select the newly added server when configuring security settings for a wireless or wired network profile.

NOTE

You can also add an external RADIUS server by selecting New for Authentication Server when configuring a WLAN or wired profile.

Configuring Authentication Parameters for IAP Management Users

You can configure RADIUS or TACACS authentication servers to authenticate and authorize the management users of an IAP. The authentication servers determine if the user has access to administrative interface. The privilege level for different types of management users is defined on the RADIUS or TACACS server. The IAPs map the management users to the corresponding privilege level and provide access to the users based on the attributes returned by the RADIUS or TACACS server.

To configure authentication parameters for local admin, read-only, and guest management administrator account settings.

1. Click **Configuration > Access Points** > **System** > **Administrator**. The **Administrator** tab details are displayed.

Table 32: *Configuration Parameters For The IAP Users*

Type of the User	Authentication Options	Steps to Follow
Client Control	Internal	Select **Internal** if you want to specify a single set of user credentials. If using an internal authentication server: 1. Enter a **Username** and **Password**. 2. Retype the password to confirm.
	Authentication server	Select the RADIUS or TACACS authentication servers. You can also create a new server by selecting **New** from the **Authentication server** drop-down list.
	Authentication server w/ fallback to internal	Select **Authentication server w/ fallback to internal** option if you want to use both internal and external servers. When enabled, the authentication switches to **Internal** if there is no response from the RADIUS server (RADIUS server timeout). To use this option, select the authentication servers and configure the user credentials (**username** and **password**)for internal server based authentication.
	Load Balancing	If two servers are configured, the users can use them in the primary or backup mode, or load balancing mode. To enable load balancing, select **Enabled** from the **Load balancing** drop-down list. For more information on load balancing, see Dynamic Load Balancing between Authentication Servers on page 80.
View Only		To configure a user account with the read-only privileges: 1. Specify a **Username** and **Password**. 2. Retype the password to confirm.
Guest Registration Only		To configure a guest user account with the read-only privileges: 1. Specify the **Username** and **Password**. 2. Retype the password to confirm.

3. Click **Save Settings**.

Configuring Users for Internal Database of an IAP

The Central user database consists of a list of guest and employee users. The addition of a user involves specifying a login credentials for a user. The login credentials for these users are provided outside the Central system.

A guest user can be a visitor who is temporarily using the enterprise network to access the Internet. However, if you do not want to allow access to the internal network and the Intranet, you can segregate the guest traffic from the enterprise traffic by creating a guest WLAN and specifying the required authentication, encryption, and access rules.

An employee user is the employee who is using the enterprise network for official tasks. You can create Employee WLANs, specify the required authentication, encryption and access rules and allow the employees to use the enterprise network.

NOTE

The user database is also used when an IAP is configured as an internal RADIUS server.

The local user database of APs can support up to 512 user entries except IAP-9x. IAP-9x supports only 256 user entries. If there are already 512 users, IAP-9x will not be able to join the cluster.

In the Central UI

To configure users:

1. Click the **Security** at the top right corner of Central main window.
2. Click **Users for Internal Server**.
3. Enter the username in the **Username** text box.
4. Enter the password in the **Password** text box and reconfirm.
5. Select a type of network from the **Type** drop-down list.
6. Click **Add** and click **OK.** The users are listed in the **Users** list.
7. To edit user settings:
   a. Select the user to modify under **Users**
   b. Click **Edit** to modify user settings.
   c. Click **OK**.
8. To delete a user:
   a. In the **Users** section, select the username to delete
   b. Click **Delete**.
   c. Click **OK**.
9. To delete all or multiple users at a time:
   a. Select the usernames that you want to delete
   b. Click **Delete All**.
   c. Click **OK**.

NOTE

Deleting a user only removes the user record from the user database, and will not disconnect the online user associated with the username.

Configuring Roles and Policies for User Access Control

This section provides the following information:

- Firewall and ACL Rules on page 84
- Configuring Access Rules for Network Services on page 85
- Configuring User Roles on page 87
- Configuring Derivation Rules on page 88
- Managing Inbound Traffic on page 90

Firewall and ACL Rules

The Central firewall provides identity-based controls to enforce application-layer security, prioritization, traffic forwarding, and network performance policies for wired and wireless networks. Using the Central firewall, you can enforce network access policies that define access to the network, areas of the network that users may access, and the performance thresholds of various applications.

Central supports a role-based stateful firewall. Central firewall recognizes flows in a network and keeps track of the state of sessions. The Central firewall manages packets according to the first rule that matches packet. The firewall logs on the IAPs are generated as syslog messages. The Central firewall also supports the Application Layer Gateway (ALG) functions such as SIP, Vocera, Alcatel NOE, and Cisco Skinny protocols.

ACL Rules

You can use Access Control List (ACL) rules to either permit or deny data packets passing through the IAP. You can also limit packets or bandwidth available to a set of user roles by defining access rules. By adding custom rules, you can block or allow access based on the service or application, source or destination IP addresses.

You can create access rules to allow or block data packets that match the criteria defined in an access rule. You can create rules for either inbound traffic or outbound traffic. Inbound rules explicitly allow or block the inbound network traffic that matches the criteria in the rule. Outbound rules explicitly allow or block the network traffic that matches the criteria in the rule. For example, you can configure a rule to explicitly block outbound traffic to an IP address through the firewall.

The IAP clients are associated with user roles, which determine the client's network privileges and the frequency at which clients re-authenticate. Central supports the following types of ACLs:

- ACLs that permit or deny traffic based on the source IP address of the packet.
- ACLs that permit or deny traffic based on source or destination IP address, or source or destination port number.

NOTE

You can configure up to 64 access control rules for a firewall policy.

Configuring Network Address Translation Rules

Network Address Translation (NAT) is the process of modifying network address information when packets pass through a routing device. The routing device acts as an agent between the public (the Internet) and private (local network), which allows translation of private network IP addresses to a public address space.

Central supports the NAT mechanism to allow a routing device to use the translation tables to map the private addresses into a single IP address and packets are sent from this address, so that they appear to originate from the routing device. Similarly, if the packets are sent to the private IP address, the destination address is translated as per the information stored in the translation tables of the routing device.

Configuring Access Rules for Network Services

This section describes the procedure for configuring ACLs to control access to network services. For information on:

- Configuring access rules based on application and application categories, see Configuring ACL Rules for Application and Application Categories on page 130.
- Configuring access rules based on web categories and web reputation, see Configuring Web Policy Enforcement on page 131.

To configure access rules, complete the following steps:

1. Select **Configuration > Access Points > Security**, and then click **Roles**. The **Roles** pane is displayed.

   You can also configure access rules for a wired or wireless network profile in the **Configuration > Access Points** > **Networks** > **Create a New Network** > **Access** pane.

2. Select a network profile for which you to assign the ACL rules.

3. Under **Access Rules For Selected Roles**, click **+ Add Rule** to add a new rule. The new rule window is displayed.

4. In the new rule window, specify the following parameters:

Table 33: *Access Rule Configuration Parameters*

Data Pane Item	Description
Rule Type	Select a rule type from the list, for example **Access Control**.
Service	Select a service from the list of available services. You can allow or deny access to any or all of the following services based on your requirement: ● **any**—Access is allowed or denied to all services. ● **custom**—Available options are TCP, UDP, and Other. If you select the TCP or UDP options, enter appropriate port numbers. If you select the Other option, enter the appropriate ID. **NOTE:** If TCP and UDP uses the same port, ensure that you configure separate access rules to permit or deny access.
Action	Select any of following attributes: ● Select **Allow** to allow access users based on the access rule. ● Select **Deny** to deny access to users based on the access rule. ● Select **Destination-NAT** to allow changes to destination IP address. ● Select **Source-NAT** to allow changes to the source IP address.
Destination	Select a destination option. You can allow or deny access to any the following destinations based on your requirements. ● **To all destinations** — Access is allowed or denied to all destinations. ● **To a particular server** — Access is allowed or denied to a particular server. After selecting this option, specify the IP address of the destination server. ● **Except to a particular server** — Access is allowed or denied to servers other than the specified server. After selecting this option, specify the IP address of the destination server. ● **To a network** — Access is allowed or denied to a network. After selecting this option, specify the IP address and netmask for the destination network. ● **Except to a network** — Access is allowed or denied to networks other than the specified network. After selecting this option, specify the IP address and netmask of the destination network. ● **To a Domain Name** — Access is allowed or denied to the specified domains. After selecting this option, specify the domain name in the **Domain Name** text box.
Log	Select **Log** to create a log entry when this rule is triggered. The Central firewall supports firewall based logging. Firewall logs on the IAPs are generated as security logs.
Blacklist	Select **Blacklist** to blacklist the client when this rule is triggered. The blacklisting lasts for the duration specified as **Auth failure blacklist time** on the **BLACKLISTING** tab of the **Security** window. For more information, see Blacklisting Clients on page 91.
Classify Media	Select **Classify Media** to prioritize video and voice traffic. When enabled, a packet inspection is performed on all non-NAT traffic and the traffic is marked as follows:

Table 33: *Access Rule Configuration Parameters*

Data Pane Item	Description
	- Video: Priority 5 (Critical) - Voice: Priority 6 (Internetwork Control)
Disable Scanning	Select **Disable Scanning** to disable ARM scanning when this rule is triggered. The selection of the **Disable Scanning** applies only if ARM scanning is enabled. For more information, see Configuring Radio Parameters on page 69.
DSCP Tag	Select **DSCP Tag**to specify a DSCP value to prioritize traffic when this rule is triggered. Specify a value within the range of 0 to 63.
802.1 priority	Select **802.1 priority** to specify an 802.1 priority. Specify a value between 0 and 7.

5. Click **Save**.

Configuring User Roles

Every client in the Central network is associated with a user role, which determines the client's network privileges, the frequency of re-authentication, and the applicable bandwidth contracts. The user role configuration on an IAP involves the following procedures:

- Creating a User Role on page 87
- Assigning Bandwidth Contracts to User Roles on page 87

Creating a User Role

To create a user role, complete the following steps:

1. Select **Configuration > Access Points > Security**. The **Security** pane is displayed.
2. Click **Roles**. The **Roles** pane contents are displayed.
3. Under **Roles**, click **New**.
4. Enter a name for the new role and click **OK**.

NOTE

You can also create a user role when configuring wireless profile. For more information, see Configuring Access Rules on page 53.

Assigning Bandwidth Contracts to User Roles

The administrators can manage bandwidth utilization by assigning maximum bandwidth rates, or bandwidth contracts to user roles. The administrator can assign a bandwidth contract configured in Kbps to upstream (client to the IAP) or downstream (IAP to clients) traffic for a user role. The bandwidth contract will not be applicable to the user traffic on the bridged out (same subnet) destinations. For example, if clients are connected to an SSID, you can restrict the upstream bandwidth rate allowed for each user to 512 Kbps.

By default, all users that belong to the same role share a configured bandwidth rate for upstream or downstream traffic. The assigned bandwidth will be served and shared among all the users. You can also assign bandwidth per user to provide every user a specific bandwidth within a range of 1 to 65535 Kbps. If there is no bandwidth contract specified for a traffic direction, unlimited bandwidth is allowed.

To assign bandwidth contracts to a user role,

1. Select **Configuration > Access Points > Security**. The **Security** pane contents are displayed.

2. Click **Roles**. The **Roles** pane contents are displayed.

3. Create a new role or select an existing role.

4. Under **Access Rues For Selected Roles**, click **(+)**.

5. Select **Bandwidth Contract** under **Rule-Type**.

6. Specify the downstream and upstream rates in Kbps. If the assignment is specific for each user, select **Peruser**.

7. Click **Save**.

8. Associate the user role to a WLAN SSID or wired profile.

You can also create a user role and assign bandwidth contracts while Configuring an SSID.

Configuring Derivation Rules

Central allows you to configure role and VLAN derivation-rules. You can configure these rules to assign a user role or VLAN to the clients connecting to an SSID or a wired profile. For more information on derivation rules, see *Aruba Instant User Guide*.

Creating a Role Derivation Rule

You can configure rules for determining the role that is assigned for each authenticated client.

NOTE

When creating more than one role assignment rule, the first matching rule in the rule list is applied.

To create a role assignment rule:

1. Select **Configuration > Access Points > Networks > Create New** to create a new network profile.

2. Under **Access**, select **Role Based**.

3. Under **Role Assignment Rules**, click **New**. In **New Role Assignment Rule**, define a match method by which the string in *Operand* is matched with the attribute value returned by the authentication server.

4. Select the attribute from the **Attribute** list that the rule it matches against. The list of supported attributes includes RADIUS attributes, dhcp-option, dot1x-authentication-type, mac-address, and mac-address-and-dhcp-options. For information on a list of RADIUS attributes, see RADIUS Server Authentication with VSA on page 79.

5. Select the operator from the **Operator** list. The following types of operators are supported:

- **contains**— The rule is applied only if the attribute value contains the string specified in *Operand*.
- **Is the role**— The rule is applied if the attribute value is the role.
- **equals**— The rule is applied only if the attribute value is equal to the string specified in *Operand*.
- **not-equals**— The rule is applied only if the attribute value is not equal to the string specified in *Operand*.
- **starts-with**— The rule is applied only if the attribute value starts with the string specified in *Operand*.
- **ends-with**— The rule is applied only if the attribute value ends with string specified in *Operand*.
- **matches-regular-expression**— The rule is applied only if the attribute value matches the regular expression pattern specified in *Operand*. This operator is available only if the **mac-address-and-dhcp-options** attribute is selected in the **Attribute** list. The **mac-address-and-dhcp-options** attribute and **matches-regular-expression** are applicable only for WLAN clients.

6. Enter the string to match in the **String** box.

7. Select the appropriate role from the **Role** list.

8. Click **Save**.

Configuring VLAN Derivation Rules

The users are assigned to a VLAN based on the attributes returned by the RADIUS server after users authenticate.

To configure VLAN derivation rules for an SSID profile:

1. Select **Configuration > Access Points > Networks**, and then click **Create New**. The **Create A New Network** pane is displayed.
2. For **Type**, select **Wireless**.
3. Enter a name that is used to identify the network in the **Name (SSID)** box.
4. Based on the type of network profile, select any of the following options under **Primary Usage**:

- **Employee**
- **Voice**
- **Guest**

5. Click **Next** to configure VLAN settings.
6. Select **Dynamic** under **Client VLAN Assignment**.
7. Click **New** to create a VLAN assignment rule. The **New VLAN Assignment Rule** window is displayed. In this window, you can define a match method by which the string in *Operand* is matched with the attribute values returned by the authentication server.
8. Select an attribute from the **Attribute** list.
9. Select an operator from the **Operator** list. The following types of operators are supported:

- **contains**— The rule is applied only if the attribute value contains the string specified in *Operand*.
- **equals**— The rule is applied only if the attribute value is equal to the string specified in *Operand*.
- **not-equals** — The rule is applied only if the attribute value is not equal to the string specified in *Operand*.
- **starts-with** — The rule is applied only if the attribute value starts with the string specified in *Operand*.
- **ends-with** — The rule is applied only if the attribute value ends with string specified in *Operand*.
- **matches-regular-expression** — The rule is applied only if the attribute value matches the regular expression pattern specified in *Operand*. This operator is available only if the **mac-address-and-dhcp-options** attribute is selected in the **Attribute** list. The **mac-address-and-dhcp-options** attribute and **matches-regular-expression** are applicable only for the WLAN clients.

10. Enter the string to match in the **String** field.
11. Select the appropriate VLAN ID from **VLAN**.
12. Ensure that all other required parameters are configured.
13. Click **Save** to apply the changes.

Configuring a User Role for VLAN Derivation

This section describes the following procedures:

- Creating a User VLAN Role on page 89
- Assigning User VLAN Roles to a Network Profile on page 90

Creating a User VLAN Role

To configure a user role for VLAN derivation:

1. Select **Configuration > Access Points > Security**.
2. Click **Roles**. The **Roles** pane contents are displayed.
3. Under **Role**, click **New**.

4. Enter a name for the new role and click **OK**.
5. Under **Access Rules For Selected Roles**, click **(+)**.
6. Select the **Rule Type** as **VLAN Assignment**.
7. Enter the ID of the VLAN in the **VLAN ID** box.
8. Click **Save**.

Assigning User VLAN Roles to a Network Profile

To assign a user VLAN role:

1. Select **Configuration > Access Points > Networks > Create New > Access**.
2. Select **Role Based**.
3. Click **New** under the **Role Assignment Rules** and configure the following parameters:
   a. Select an attribute from the **Attribute** list.
   b. Select an operator from the **Operator** list.
   c. Enter the string in the **String** box.
   d. Select the role to be assigned from the **Role** box.
   e. Click **Save.**

Configuring Firewall Settings for Protection from ARP Attacks

To configure firewall settings, complete the following steps:

1. Select **Configuration > Access Points > Security**.
2. Click **Firewall Settings**. The **Firewall Settings** pane contents are displayed.
3. Set the following options to **Enabled**:

- **Drop Bad ARP**—Drops the fake ARP packets.
- **Fix Malformed DHCP**—Fixes the malformed DHCP packets.
- **ARP poison check**—Triggers an alert on ARP poisoning caused by the rogue APs.

4. Click **Save Settings.**

Managing Inbound Traffic

Central supports an enhanced inbound firewall by allowing the configuration of management subnets and restricting corporate access through an uplink switch.

To allow flexibility in firewall configuration, Central supports the following features:

- Configurable management subnets
- Restricted corporate access

Configuring Management Subnets

You can configure subnets to ensure that the IAP management is carried out only from these subnets. When the management subnets are configured, Telnet, SSH, and UI access is restricted to these subnets only.

To configure management subnets, complete the following steps:

1. Select **Configuration > Access Points > Security >Firewall Settings**. The **Firewall Settings** pane contents are displayed.
2. To add a new management subnet, perform the following actions:

- Enter the subnet address in **Subnet**.
- Enter the subnet mask in **Mask.**
- Click **Add**.

3. To add multiple subnets, repeat step 2.

4. Click **Save Settings**.

Configuring Restricted Access to Corporate Network

You can configure restricted corporate access to block unauthorized users from accessing the corporate network. When restricted corporate access is enabled, corporate access is blocked from the uplink port of master IAP, including clients connected to a slave IAP.

To configure restricted corporate access, complete the following steps:

1. Select **Configuration > Access Points > Security >Firewall Settings**. The **Firewall Settings** pane contents are displayed.
2. Select **Enabled** from the **Restrict Corporate Access**.
3. Click **Save Settings**.

Disabling Auto Topology Rules

If the firewalls rules are configured, the **Auto Topology Rules** are enabled by default. When the inbound firewall settings are enabled:

- Access Control Entities (ACEs) must be configured to block auto topology messages, as there is no default rule at the top of predefined ACLs.
- ACEs must be configured to override the guest VLAN auto-expanded ACEs. In other words, the user defined ACEs take higher precedence over guest VLAN ACEs.

To disable the auto topology rules, set the **Auto Topology Rules** to **OFF**.

Configuring ALG Protocols

To configure protocols for ALG:

1. Select **Configuration > Access Points > Security**.
2. Click **Firewall Settings**. The **Firewall Settings** pane contents are displayed.
3. Under **Application Layer Gateway (ALG) Algorithms**, select **Enabled** against the corresponding protocol to enable SIP, VOCERA, ALCATEL NOE, and CISCO SKINNY protocols.
4. Click **Save Settings.**

NOTE

When the protocols for the ALG are **Disabled** the changes do not take effect until the existing user sessions have expired. Reboot the IAP and the client, or wait a few minutes for changes to take effect.

Blacklisting Clients

The client blacklisting denies connection to the blacklisted clients. When a client is blacklisted, it is not allowed to associate with an IAP in the network. If a client is connected to the network when it is blacklisted, a deauthentication message is sent to force client disconnection.

Blacklisting Clients Manually

Manual blacklisting adds the MAC address of a client to the blacklist. These clients are added into a permanent blacklist. These clients are not allowed to connect to the network unless they are removed from the blacklist.

To add a client to the blacklist manually:

1. Select **Configuration** > **Access Points** > **Security** > **Blacklisting**.
2. Click **New** and enter the MAC address of the client to be blacklisted in **Enter A New MAC Address**.

3. Click **Ok**. The **Blacklisted Since** field displays the time at which the current blacklisting has started for the client.

To delete a client from the manual blacklist, select the MAC Address of the client under the **Manual Blacklisting**, and then click **Delete**.

Blacklisting Clients Dynamically

The clients can be blacklisted dynamically when they exceed the authentication failure threshold or when a blacklisting rule is triggered as part of the authentication process.

When a client takes time to authenticate and exceeds the configured failure threshold, it is automatically blacklisted by an IAP.

In session firewall based blacklisting, an Access Control List (ACL) rule automates blacklisting. When the ACL rule is triggered, it sends out blacklist information and the client is blacklisted.

To configure the blacklisting duration:

1. Select **Configuration > Access Points** > **Security** > **Blacklisting**.
2. Under **Dynamic Blacklisting**:
   a. For **Auth Failure Blacklist Time**, enter the duration after which the clients that exceed the authentication failure threshold must be blacklisted.
   b. For **PEF Rule Blacklised Time**, enter the duration after which the clients can be blacklisted due to an ACL rule trigger.

NOTE

You can configure a maximum number of authentication failures by the clients, after which a client must be blacklisted. For more information on configuring maximum authentication failure attempts, see Configuring Security Settings on page 50.

Configuring VPN Networks

This section describes the following VPN configuration procedures:

- Understanding VPN Features on page 92
- Configuring VPN Tunnels on page 93
- Configuring Routing Profiles on page 96

Understanding VPN Features

As IAPs use a Virtual Controller architecture, the IAP network does not require a physical controller to provide the configured WLAN services. However, a physical controller is required for terminating Virtual Private Networks (VPN) tunnels from the IAP networks at branch locations or data centers, where the Aruba controller acts as a VPN concentrator.

When the VPN is configured, the IAP acting as the Virtual Controller creates a VPN tunnel to Aruba mobility controller in your corporate office. The controller acts as a VPN end-point and does not supply the IAP with any configuration.

The VPN features are recommended for:

- Enterprises with many branches that do not have a dedicated VPN connection to the corporate office.
- Branch offices that require multiple APs.
- Individuals working from home, connecting to the VPN.

Supported VPN Protocols

IAPs support the following VPN protocols for remote access:

Table 34: *VPN Protocols*

VPN Protocol	Description
Aruba IPsec	IPsec is a protocol suite that secures IP communications by authenticating and encrypting each IP packet of a communication session. You can configure an IPsec tunnel to ensure that to ensure that the data flow between the networks is encrypted. However, you can configure a split-tunnel to encrypt only the corporate traffic. When IPsec is configured, ensure that you add the IAP MAC addresses to the whitelist database stored on the controlleror an external server. IPsec supports Local, L2, and L3 modes of IAP-VPN operations. **NOTE:** The IAPs support IPsec only with Aruba Controllers.
Layer-2 (L2) GRE	Generic Routing Encapsulation (GRE) is a tunnel protocol for encapsulating multicast, broadcast, and L2 packets between a GRE-capable device and an end-point. IAPs support the configuration of L2 GRE (Ethernet over GRE) tunnel with an ArubaController to encapsulate the packets sent and received by the IAP. You can use the GRE configuration for L2 deployments when there is no encryption requirement between the IAP and controller for client traffic. IAPs support two types of GRE configuration: ● **Manual GRE**—The manual GRE configuration sends unencrypted client traffic with an additional GRE header and does not support failover. When manual GRE is configured on the IAP, ensure that the GRE tunnel settings are enabled on the controller. ● **Aruba GRE**—With Aruba GRE, no configuration on the controller is required except for adding the IAP MAC addresses to the whitelist database stored on the controller or an external server. Aruba GRE reduces manual configuration when **Per-AP tunnel** configuration is required and supports failover between two GRE end-points. **NOTE:** IAPs support manual and Aruba GRE configuration only for L2 mode of operations. Aruba GRE configuration is supported only with Aruba Controllerss.
L2TP	The Layer 2 Tunneling Protocol version 3 (L2TPv3) feature allows IAP to act as L2TP Access Concentrator (LAC) and tunnel all wireless clients L2 traffic from AP to L2TP Network Server (LNS). In a centralized L2 model, the VLAN on the corporate side are extended to remote branch sites. Wireless clients associated with IAP gets the IP address from the DHCP server running on LNS. For this, AP has to transparently allow DHCP transactions through the L2TPv3 tunnel.

Configuring VPN Tunnels

IAP supports the configuration of tunneling protocols such as Generic Routing Encapsulation (GRE), IPsec, and L2TPv3. This section describes the procedure for configuring VPN host settings on an IAP to enable communication with a controller in a remote location:

- Configuring IPSec Tunnel on page 93
- Enabling Automatic Configuration of GRE Tunnel on page 94
- Configuring GRE Tunnel Manually on page 95
- Configuring an L2TPv3 Tunnel on page 96

Configuring IPSec Tunnel

An IPsec tunnel is configured to ensure that the data flow between the networks is encrypted. When configured, the IPSec tunnel to the controller secures corporate data. You can configure an IPSec tunnel from

Virtual Controller using Central.

To configure a tunnel using the IPSec Protocol, complete the following steps:

1. Click the **Configuration > Access Points** > **VPN** link in Central.
2. Click **Controller**. Select **Aruba IPSec** from the **Protocol** drop-down list.
3. Enter the IP address or fully qualified domain name (FQDN) for the main VPN/IPSec endpoint in the **Primary host** field.
4. Enter the IP address or FQDN for the backup VPN/IPSec endpoint in the **Backup host** field. This entry is optional. When you specify the primary and backup host details, the other fields are displayed.
5. Specify the following parameters.

   a. To allow the VPN tunnel to switch back to the primary host when it becomes available again, select **Enabled** from the **Preemption** drop-down list. This step is optional.

   b. If **Preemption** is enabled, specify a value in seconds for **Hold time**. When preemption is enabled and the primary host comes up, the VPN tunnel switches to the primary host after the specified hold-time. The default value for **Hold time** is 600 seconds.

   c. To allow the IAP to create a backup VPN tunnel to the controller along with the primary tunnel, and maintain both the primary and backup tunnels separately, select **Enabled** from the **Fast failover** drop-down list. When fast failover is enabled and if the primary tunnel fails, the IAP can switch the data stream to the backup tunnel. This reduces the total failover time to less than one minute.

   d. Specify a value in seconds for **Secs between test packets**. Based on the configured frequency, the IAP can verify if an active VPN connection is available. The default value is 5 seconds, which means that the IAP sends one packet to the controller every 5 seconds.

   e. Enter a value for **Max allowed test packet loss**, to define a number for lost packets, after which the IAP can determine that the VPN connection is unavailable. The default value is 2.

   f. To disconnect all wired and wireless users when the system switches during VPN tunnel transition from primary to backup and backup to primary, set **Reconnect user on failover** to **Enabled**.

   g. To configure an interval for which wired and wireless users are disconnected during a VPN tunnel switch, specify a value in seconds for **Reconnect time on failover** within a range of 30—900 seconds. By default, the reconnection duration is set to 60 seconds. The **Reconnect time on failover** field is displayed only when **Reconnect user on failover** is enabled.
6. When the IPsec tunnel configuration is completed, the packets that are sent from and received by an IAP are encrypted.

Enabling Automatic Configuration of GRE Tunnel

You can configure an IAP to automatically set up a GRE tunnel from the IAP to controller by using Central.

1. Click the **Configuration > Access Points** > **VPN**.
2. Click **Controller**. Select **Aruba GRE** from the **Protocol** drop-down list.
3. Enter the IP address or FQDN for the main VPN/IPSec endpoint in the **Primary host** field.
4. Enter the IP address or FQDN for the backup VPN/IPSec endpoint in the **Backup host** field. This entry is optional. When you enter the primary host IP address and backup host IP address, other fields are displayed.
5. Specify the following parameters. A sample configuration is shown in .

   a. To allow the VPN tunnel to switch back to the primary host when it becomes available again, select **Enabled** from the **Preemption** drop-down list. This step is optional.

   b. If **Preemption** is enabled, specify a value in seconds for **Hold time**. When preemption is enabled and the primary host comes up, the VPN tunnel switches to the primary host after the specified hold time. The default value for **Hold time** is 600 seconds.

c. To allow the IAP to create a backup VPN tunnel to the controller along with the primary tunnel, and maintain both the primary and backup tunnels separately, select **Enabled** or **Disabled** from the **Fast failover** drop-down list. If the primary tunnel fails, the IAP can switch the data stream to the backup tunnel. This reduces the total failover time to less than one minute.

d. To disconnect all wired and wireless users when the system switches during VPN tunnel transition from primary to backup and backup to primary, set **Reconnect user on failover** to **Enabled**.

e. To configure an interval for which wired and wireless users are disconnected during a VPN tunnel switch, specify a value in seconds for **Reconnect time on failover** within the range of 30—900 seconds. By default, the reconnection duration is set to 60 seconds.

f. Specify a value in seconds for **Secs between test packets**. Based on the configured frequency, the IAP can verify if an active VPN connection is available. The default value is 5 seconds, which means that the IAP sends one packet to the controller every 5 seconds.

g. Enter a value for **Max allowed test packet loss**, to define a number for lost packets, after which the IAP can determine that the VPN connection is unavailable. The default value is 2.

h. Select **Enabled** or **Disabled** from the **Per-AP tunnel** drop-down list. The administrator can enable this option to create a GRE tunnel from each IAP to the VPN/GRE Endpoint rather than the tunnels created just from the master IAP. When enabled, the traffic to the corporate network is sent through a Layer-2 GRE tunnel from the IAP itself and need not be forwarded through the master IAP.

6. Click **Next** to continue.

Configuring GRE Tunnel Manually

You can also manually configure a GRE tunnel by configuring the GRE tunnel parameters on the IAP and controller. This procedure describes the steps involved in the manual configuration of a GRE tunnel from Virtual Controller by using Central.

During the manual GRE setup, you can either use the Virtual Controller IP or the IAP IP to create the GRE tunnel at the controller side depending upon the following IAP settings:

- If a Virtual Controller IP is configured and if Per-AP tunnel is disabled, the Virtual Controller IP is used to create the GRE tunnel.
- If a Virtual Controller IP is not configured or if Per-AP tunnel is enabled, the IAP IP is used to create the GRE tunnel.

To configure the GRE tunnel manually, complete the following steps:

1. Click the **Configuration > Access Points** > **VPN**.
2. Click **Controller**. Select **Manual GRE** from the **Protocol** drop-down list.
3. Specify the following parameters.

a. Enter an IP address or the FQDN for the main VPN/GRE endpoint.

b. Enter a value for the GRE type parameter.

c. Select **Enabled** or **Disabled** from the **Per-AP tunnel** drop-down list. The administrator can enable this option to create a GRE tunnel from each IAP to the VPN/GRE Endpoint rather than the tunnels created just from the master IAP. When enabled, the traffic to the corporate network is sent through a Layer-2 GRE tunnel from the IAP itself and need not be forwarded through the master IAP.

NOTE

By default, the **Per-AP tunnel** option is disabled.

4. When the GRE tunnel configuration is completed on both the IAP and Controller, the packets sent from and received by an IAP are encapsulated, but not encrypted.

Configuring an L2TPv3 Tunnel

The Layer 2 Tunneling Protocol version 3 (L2TPv3) feature allows IAP to act as L2TP Access Concentrator (LAC) and tunnel all wireless clients L2 traffic from AP to L2TP Network Server (LNS). In a centralized L2 model, the VLAN on the corporate side are extended to remote branch sites. Wireless clients associated with IAP gets the IP address from the DHCP server running on LNS. For this, AP has to transparently allow DHCP transactions through the L2TPv3 tunnel.

To configure an L2TPv3 tunnel by using Central, complete the following steps:

1. Click the **Configuration > Access Points** > **VPN**.
2. Click **Controller**.
3. Select **L2TPv3** from the Protocol drop-down list.
4. Perform the following actions to configure the tunnel profile:
   a. Click **New** and enter the profile name to be used for tunnel creation.
   b. Enter the primary server IP address.
   c. Enter the remote end backup tunnel IP address. This is an optional field and is required only when backup server is configured.
   d. Enter the remote end UDP port number. The default value is 1701.
   e. Enter the interval at which the hello packets are sent through the tunnel. The default value is 60 seconds.
   f. Select the message digest as MD5 or SHA used for message authentication.
   g. Enter a shared key for the message digest. This key should match with the tunnel end point shared key.
   h. If required, select the failover mode as Primary or Backup (when the backup server is available).
   i. Specify a value for the tunnel MTU value if required. The default value is 1460.
   j. Click **Save**.
5. Perform the following actions to configure the session profile:
   a. Enter the session name to be used for session creation.
   b. Enter the tunnel profile name where the session will be associated.
   c. Configure the tunnel IP address with the corresponding network mask and VLAN ID. This is required to reach an AP from a corporate network. For example, SNMP polling.
   d. Select the cookie length and enter a cookie value corresponding to the length. By default, the cookie length is not set.
   e. Click **Save**.

Configuring Routing Profiles

Central can terminate a single VPN connection on Aruba mobility controller. The routing profile defines the corporate subnets which need to be tunneled through IPSec.

You can configure routing profiles to specify a policy based on routing into the VPN tunnel using Central.

1. Click **Configuration > Access Points** > **VPN**.

1. Click **Routing**.
2. Click **New**. The route parameters to configure are displayed.
3. Update the following parameters:

- **Destination**— Specify the destination network that is reachable through the VPN tunnel. This defines the IP or subnet that must reach through the IPsec tunnel. Traffic to the IP or subnet defined here will be forwarded through the IPsec tunnel.

- **Netmask**— Specify the subnet mask to the destination defined for **Destination**.
- **Gateway**— Specify the gateway to which traffic must be routed. This IP address must be the controller IP address on which the VPN connection is terminated. If you have a primary and backup host, configure two routes with the same destination and netmask, but ensure that the gateway is the primary controller IP for one route and the backup controller IP for the second route.

4. Click **OK**.
5. Click **Finish**.

Configuring DHCP and Client IP Assignment Modes

This section provides the following information:

- Configuring DHCP Scopes on page 97
- Configuring DHCP Server for Client IP Assignment on page 102

Configuring DHCP Scopes

The VC supports different modes of DHCP address assignment. With each DHCP address assignment mode, various client traffic forwarding modes are associated.

Configuring Distributed DHCP Scopes

Central allows you to configure the DHCP address assignment for the branches connected to the corporate network through VPN. You can configure the range of DHCP IP addresses used in the branches and the number of client addresses allowed per branch. You can also specify the IP addresses that must be excluded from those assigned to clients, so that they are assigned statically.

Central supports the following distributed DHCP scopes:

- **Distributed, L2** — In this mode, the VC acts as the DHCP server, but the default gateway is in the data center. Based on the number of clients specified for each branch, the range of IP addresses is divided. Based on the IP address range and client count configuration, the DHCP server in the VC controls a scope that is a subset of the complete IP Address range for the subnet distributed across all the branches. This DHCP Assignment mode is used with the L2 forwarding mode.
- **Distributed, L3** — In this mode, the VC acts as the DHCP server and the default gateway. Based on the number of clients specified for each branch, the range of IP addresses is divided. Based on the IP address range and client count configuration, the DHCP server in the VC is configured with a unique subnet and a corresponding scope.

To configure distributed DHCP scopes such as Distributed, L2 or Distributed,L3.

1. Select **Configuration > Access Points** > **DHCP**.
2. To configure a distributed DHCP mode, click **New** under **Distributed DHCP Scopes**. The **New DHCP Scope** pane is displayed.
3. Based on the type of distributed DHCP scope, configure the following parameters:

Table 35: *Distributed DHCP Scope Configuration Parameters*

Data pane item	Description
Name	Enter a name for the DHCP scope.
Type	Select any of the following options: - **Distributed, L2**— On selecting **Distributed, L2**, the VC acts as the DHCP Server but the default gateway is in the data center. Traffic is bridged into VPN tunnel. - **Distributed, L3**— On selecting **Distributed, L3**, the VC acts as both DHCP Server and default gateway. Traffic is routed into the VPN tunnel.
VLAN	Specify a VLAN ID. To use this subnet, ensure that the VLAN ID specified here is assigned to an SSID profile.
Netmask	If **Distributed, L2** is selected for type of DHCP scope, specify the subnet mask. The subnet mask and the network determine the size of subnet.
Default Router	If **Distributed, L2** is selected for type of DHCP scope, specify the IP address of the default router.
DNS Server	If required, specify the IP address of a DNS server.
Domain Name	If required, specify the domain name.
Lease Time	Specify a lease time for the client in minutes.
IP Address Range	Specify a range of IP addresses to use. To add another range, click the + icon. You can specify up to four different ranges of IP addresses. - For Distributed, L2 mode, ensure that all IP ranges are in the same subnet as the default router. On specifying the IP address ranges, a subnet validation is performed to ensure that the specified ranges of IP address are in the same subnet as the default router and subnet mask. The configured IP range is divided into blocks based on the configured client count. - For Distributed, L3 mode, you can configure any discontiguous IP ranges. The configured IP range is divided into multiple IP subnets that are sufficient to accommodate the configured client count. **NOTE:** You can allocate multiple branch IDs (BID) per subnet. The IAP generates a subnet name from the DHCP IP configuration, which the controller can use as a subnet identifier. If static subnets are configured in each branch, all of them are assigned the with BID 0, which is mapped directly to the configured static subnet.
Option	Specify the type and a value for the DHCP option. You can configure the organization-specific DHCP options supported by the DHCP server. For example, 176, 242, 161, and so on. To add multiple DHCP options, click the + icon. You can add up to eight DHCP options.

4. Click **Next**.

5. Specify the number of clients to use per branch. The client count configured for a branch determines the use of IP addresses from the IP address range defined for a DHCP scope. For example, if 20 IP addresses are available in an IP address range configured for a DHCP scope and a client count of 9 is configured, only a few IP addresses (in this example, 9) from this range will be used and allocated to a branch. The IAP does

not allow the administrators to assign the remaining IP addresses to another branch, although a lower value is configured for the client count.

6. Click **Next**. The **Static IP** tab is displayed. Specify the number of first and last IP addresses to reserve in the subnet.
7. Click **Finish**.

Configuring a Centralized DHCP Scope

The centralized DHCP scope supports L2 and L3 clients.

When a centralized DHCP scope is configured:

- The Virtual Controller does not assign an IP address to the client and the DHCP traffic is directly forwarded to the DHCP Server.
- For L2 clients, the Virtual Controller bridges the DHCP traffic to the controller over the VPN/GRE tunnel. The IP address is obtained from the DHCP server behind the controller serving the VLAN/GRE of the client. This DHCP assignment mode also allows you to add the DHCP option 82 to the DHCP traffic forwarded to the controller.
- For L3 clients, the Virtual Controller acts as a DHCP relay agent that forwards the DHCP traffic to the DHCP server located behind the controller in the corporate network and reachable through the IPSec tunnel. The centralized L3 VLAN IP is used as the source IP. The IP address is obtained from the DHCP server.

To configure a centralized DHCP scope:

1. Select **Configuration > Access Points** > **DHCP**.
2. To configure **Centralized** DHCP scopes, click **New** under **Centralized DHCP Scopes**. The **New DHCP Scope** data pane is displayed.
3. Based on type of DHCP scope, configure the following parameters:

Table 36: *DHCP Mode Configuration Parameters*

Data pane item	Description
Name	Enter a name for the DHCP scope.
VLAN	Specify a VLAN ID. To use this subnet, ensure that the VLAN ID specified here is assigned to an SSID profile.
DHCP Relay	Select **Enabled** to allow the IAPs to intercept the broadcast packets and relay DHCP requests.
Helper Address	Enter the IP address of the DHCP server.

Table 36: *DHCP Mode Configuration Parameters*

Data pane item	Description
VLAN IP	Specify the VLAN IP address of the DHCP relay server.
VLAN Mask	Specify the VLAN subnet mask of the DHCP relay server.
Option 82	This option is available only if Centralized is selected. Select **Alcatel** to enable DHCP Option 82 to allow clients to send DHCP packets with the Option 82 string. The Option 82 string is available only in the Alcatel (ALU) format. The ALU format for the Option 82 string consists of the following: Remote Circuit ID; X AP-MAC; SSID; SSID-Type Remote Agent; X IDUE-MAC

4. Click **OK**.

NOTE

The Option 82 is specific to Alcatel and is not configurable in this version of Central.

The following table describes the behavior of the DHCP Relay Agent and Option 82 in the IAP.

Table 37: *DHCP Relay And Option 82*

DHCP relay	Option 82	Behavior
Enabled	Enabled	DHCP packet relayed with the ALU-specific Option 82 string
Enabled	Disabled	DHCP packet relayed without the ALU-specific Option 82 string
Disabled	Enabled	DHCP packet not relayed, but broadcast with the ALU-specific Option 82 string
Disabled	Disabled	DHCP packet not relayed, but broadcast without the ALU-specific Option 82 string

Configuring Local and Local, L3 DHCP Scopes

You can configure Local and Local, L3 DHCP scopes.

- **Local**—In this mode, the VC acts as both the DHCP Server and default gateway. The configured subnet and the corresponding DHCP scope are independent of subnets configured in other IAP clusters. The VC assigns an IP address from a local subnet and forwards traffic to both **corporate** and **non-corporate** destinations. The network address is translated appropriately and the packet is forwarded through the IPSec tunnel or through the uplink. This DHCP assignment mode is used for the NAT forwarding mode.
- **Local, L2**—In this mode, the VC acts as a DHCP server and the gateway is located outside the IAP.

- **Local, L3**—In this mode, the VC acts as a DHCP server and default gateway, and assigns an IP address from the local subnet. The IAP routes the packets sent by clients on its uplink. This DHCP assignment mode is used with the L3 forwarding mode.

To configure a new DHCP scope:

1. Select **Configuration > Access Points >DHCP**. The **DHCP Server** data pane is displayed.
2. Click **Local DHCP Scopes** > **New**. The **New DHCP Scope** pane is displayed.
3. Based on type of DHCP scope, configure the following parameters:

Table 38: *Local DHCP Configuration Parameters*

Data pane item	Description
Name	Enter a name for the DHCP scope.
Type	Select any of the following options: ● **Local**— On selecting **Local**, the DHCP server for local branch network is used for keeping the scope of the subnet local to the IAP. In the NAT mode, the traffic is forwarded through the uplink. ● **Local, L2**—On selecting Local, L2, the VC acts as a DHCP server and a default gateway in the local network is used. ● **Local, L3**—On selecting **Local, L3**, the VC acts as a DHCP server and gateway.
VLAN	Enter the VLAN ID. To use this subnet, ensure that the VLAN ID specified here is assigned to an SSID profile.
Network	Specify the network to use.
Netmask	Specify the subnet mask. The subnet mask and the network determine the size of subnet.
Excluded Address	Specify a range of IP addresses to exclude. You can add up to two exclusion ranges. Based on the size of the subnet and the value configured for **Excluded address**s, the IP addresses either before or after the defined range are excluded.
Default Router	Enter the IP address of the default router.
DNS Server	Enter the IP address of a DNS server.
Domain Na me	Enter the domain name.
Lease Time	Enter a lease time for the client in minutes.
Option	Specify the type and a value for the DHCP option. You can configure the organization-specific DHCP options supported by the DHCP server. To add multiple DHCP options, click the (**+**) icon.

4. Click **OK**.

Configuring DHCP Server for Client IP Assignment

The DHCP server is a built-in server, used for networks in which clients are assigned IP address by the VC. You can customize the DHCP pool subnet and address range to provide simultaneous access to more number of clients. The largest address pool supported is 2048. The default size of the IP address pool is 512.

NOTE

When the DHCP server is configured and if the **Client IP assignment** parameter for an SSID profile is set to **Virtual Controller Assigned**, the Virtual Controller assigns the IP addresses to the WLAN or wired clients. By default, the IAP automatically determines a suitable DHCP pool for **Virtual Controller Assigned** networks.
The IAP typically selects the 172.31.98.0/23 subnet. If the IP address of the IAP is within the 172.31.98.0/23 subnet, the IAP selects the 10.254.98.0/23 subnet. However, this mechanism does not avoid all possible conflicts with the wired network. If your wired network uses either 172.31.98.0/23 or 10.254.98.0/23, and you experience problems with the **Virtual Controller Assigned** networks after upgrading to Aruba Central, manually configure the DHCP pool by following the steps described in this section.

To configure a domain name, DNS server, and DHCP server for client IP assignment.

1. Select **Configuration > Access Points** > **System >DHCP**. The **DHCP** details are displayed.
2. Enter the domain name of the client in **Domain Name**.
3. Enter the IP addresses of the DNS servers in **DNS Server**. To add another DNS server, click the **+** icon.
4. Enter the duration of the DHCP lease in **Lease Time**.
5. Select **Minutes**, **Hours**, or **Days** for the lease time from the list next to **Lease Time**. The default lease time is 0.
6. Enter the network in the **Network** box.
7. Enter the mask in the **Mask** box.

NOTE

To provide simultaneous access to more than 512 clients, use the Network and Mask fields to specify a larger range. While the network (or prefix) is the common part of the address range, the mask (suffix) specifies how long the variable part of the address range is.

8. Click **Save Settings** to apply the changes.

NOTE

When the DHCP server is configured and if the **Client IP assignment** parameter for an SSID profile is set to **Virtual Controller Assigned**, the Virtual Controller assigns the IP addresses to the WLAN or wired clients. By default, the IAP automatically determines a suitable DHCP pool for **Virtual Controller Assigned** networks.
The IAP typically selects the 172.31.98.0/23 subnet. If the IP address of the IAP is within the 172.31.98.0/23 subnet, the IAP selects the 10.254.98.0/23 subnet. However, this mechanism does not avoid all possible conflicts with the wired network. If your wired network uses either 172.31.98.0/23 or 10.254.98.0/23, and you experience problems with the **Virtual Controller Assigned** networks after upgrading to Aruba Central, manually configure the DHCP pool by following the steps described in this section.

Configuring Services

This section provides the following:

- Configuring an IAP for RTLS Support on page 103
- Configuring an IAP for Analytics and Location Engine Support on page 103
- Configuring OpenDNS Credentials on page 104
- CALEA Integration and Lawful Intercept Compliance on page 104
- Configuring an IAP for AirGroup Support on page 106
- Integrating an IAP with Palo Alto Networks Firewall on page 109

- Enabling AppRF™ Service on page 110

Configuring an IAP for RTLS Support

Central supports the real time tracking of devices when integrated with a third-party RTLS such as Aeroscout. With the help of the RTLS, the devices can be monitored in real time or through history.

To configure third-party RTLS such as Aeroscout:

1. Select **Configuration > Access Points > Services > RTLS**.
2. Select **Aeroscout** to send the RFID tag information to an Aeroscout RTLS.
3. Specify the IP address and port number of the Aeroscout server, to which location reports must be sent.
4. Select **Include Unassociated Stations** to send reports on the stations that are not associated to any IAP to the Aeroscout RTLS server.
5. Click **Save Settings**.

To configure third-party RTLS such as Aeroscout:

1. Select the **Aeroscout** check box to send the RFID tag information to an AeroScout RTLS.
2. Specify the IP address and port number of the AeroScout server, to which location reports must be sent.
3. Select the **Include unassociated stations** check box to send reports on the stations that are not associated to any IAP to the Aeroscout RTLS server.
4. Click **OK**.

Configuring an IAP for Analytics and Location Engine Support

The Analytics and Location Engine (ALE) is designed to gather client information from the network, process it and share it through a standard API. The client information gathered by ALE can be used for analyzing a client's Internet behavior for business such as shopping preferences.

ALE includes a location engine that calculates the associated and unassociated device location every 30 seconds by default. For every device on the network, ALE provides the following information through the Northbound API:

- Client user name
- IP address
- MAC address
- Device type
- Application firewall data, showing the destinations and applications used by associated devices.
- Current location
- Historical location

ALE requires the AP placement data to be able to calculate location for the devices in a network.

ALE with Central

Central supports Analytics and Location Engine (ALE). The ALE server acts as a primary interface to all third-party applications and the IAP sends client information and all status information to the ALE server.

To integrate IAP with ALE, the ALE server address must be configured on an IAP. If the ALE sever is configured with a host name, the Virtual Controller performs a mutual certificated-based authentication with ALE server, before sending any information.

Enabling ALE support on an IAP

To configure an IAP for ALE support:

1. Click **Configuration > Access Points** > **Services**. The **Services** pane is displayed.
2. Click **RTLS**.
3. Select **Analytics & Location Engine**.
4. Specify the ALE server name or IP address.
5. Specify the reporting interval within the range of 6–60 seconds. The IAP sends messages to the ALE server at the specified interval. The default interval is 30 seconds.
6. Click **OK**.

Configuring OpenDNS Credentials

Central uses the OpenDNS credentials to provide enterprise-level content filtering.

To configure OpenDNS credentials:

1. Select **Configuration > Access Points** > **Services** > **OpenDNS**. The **OpenDNS** details are displayed.
2. Enter the **Username** and **Password**.
3. Click **Save Settings**.

CALEA Integration and Lawful Intercept Compliance

Lawful Intercept (LI) allows the Law Enforcement Agencies (LEA) to perform an authorized electronic surveillance. Depending on the country of operation, the service providers (SPs) are required to support LI in their respective networks.

In the United States, SPs are required to ensure LI compliance based on Communications Assistance for Law Enforcement Act (CALEA) specifications.

Central supports CALEA integration in a hierarchical and flat topology, mesh IAP network, the wired and wireless networks.

NOTE

Enable this feature only if lawful interception is authorized by a law enforcement agency.

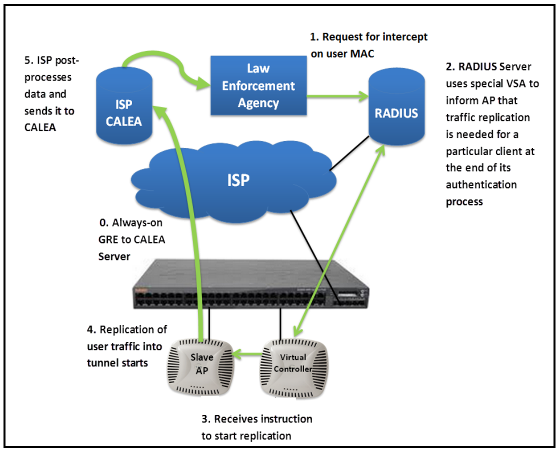
CALEA Server Integration

To support CALEA integration and ensure LI compliance, you can configure the IAPs to replicate a specific or selected client traffic and send it to a remote CALEA server.

Traffic Flow from AP to CALEA Server

You can configure an IAP to send GRE encapsulated packets to the CALEA server and replicate client traffic within the GRE tunnel. Each IAP sends GRE encapsulated packets only for its associated or connected clients. The following figure illustrates the traffic flow from the IAP to the CALEA server.

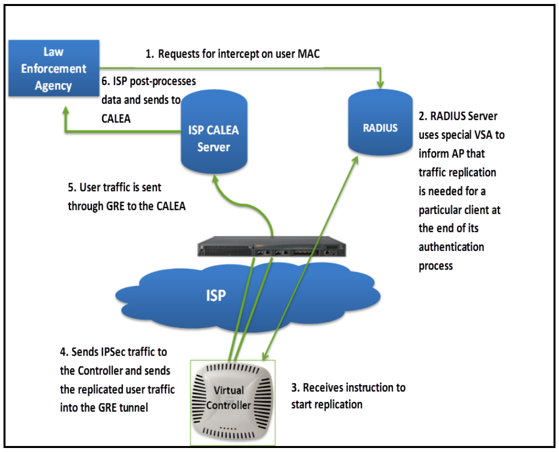
Figure 2 *AP To CALEA Server*


1. Request for intercept on user MAC
5. ISP post-processes data and sends it to CALEA
Law Enforcement Agency
ISP CALEA
RADIUS
2. RADIUS Server uses special VSA to inform AP that traffic replication is needed for a particular client at the end of its authentication process
ISP
0. Always-on GRE to CALEA Server
4. Replication of user traffic into tunnel starts
Slave AP
Virtual Controller
3. Receives instruction to start replication

Traffic Flow from IAP to CALEA Server through VPN

You can also deploy the CALEA server with the controller and configure an additional IPSec tunnel for corporate access. When CALEA server is configured with the controller, the client traffic is replicated by the slave IAP and client data is encapsulated by GRE on slave, and routed to the master IAP. The master IAP sends the IPsec client traffic to the controller. The controller handles the IPSec client traffic while GRE data is routed to the CALEA server. The following figure illustrates the traffic flow from IAP to the CALEA server through VPN.

Figure 3 *AP To CALEA Server Through VPN*


Law Enforcement Agency
1. Requests for intercept on user MAC
6. ISP post-processes data and sends to CALEA
ISP CALEA Server
RADIUS
2. RADIUS Server uses special VSA to inform AP that traffic replication is needed for a particular client at the end of its authentication process
5. User traffic is sent through GRE to the CALEA
ISP
4. Sends IPSec traffic to the Controller and sends the replicated user traffic into the GRE tunnel
Virtual Controller
3. Receives instruction to start replication

Ensure that IPSec tunnel is configured if the client data has to be routed to the ISP or CALEA server through VPN. For more information on configuring IPSec, see Configuring IPSec Tunnel on page 93.

Client Traffic Replication

Client traffic is replicated in the following ways:

- Through RADIUS VSA— In this method, the client traffic is replicated by using the RADIUS VSA to assign clients to a CALEA related user role. To enable role assignment to clients, you need to create a user role and a CALEA access rule, and then assign the CALEA rule to the user role. Whenever a client that is configured to use a CALEA rule connects, a replication role is assigned.
- Through Change of Authorization (CoA)—In this method, a user session can start without replication. When the network administrator triggers a CoA from the RADIUS server, the user session is replicated. The replication is stopped when the user disconnects or by sending a CoA to change the replication role.

As the client information is shared between multiple IAPs in a cluster, the replication rules persist when clients roam within the cluster.

Configuring an IAP for CALEA Integration

To enable CALEA server integration, perform the following steps:

Creating a CALEA Profile

You can create a CALEA profile by using Central.

1. Click **Configuration** > **Services** of the Central main window.
2. Click **CALEA**. The **CALEA** tab details are displayed.
3. Specify the following parameters:

- **IP address**— Specify the IP address of the CALEA server.
- **Encapsulation type**— Specify the encapsulation type. The current release of Central supports GRE only.
- **GRE type**— Specify the GRE type.
- **MTU**— Specify a size for the maximum transmission unit (MTU) within the range of 68—1500. After GRE encapsulation, if packet length exceeds the configured MTU, IP fragmentation occurs. The default MTU size is 1500.

4. Click **OK**.

Creating an Access Rule for CALEA

You can create an access rule for CALEA by using Central.

1. To add the CALEA access rule to an existing profile, select an existing wireless (**Networks** tab > **edit**) or wired (**More** > **Wired** > **Edit**) profile. To add the access rule to a new profile, click **New** under Network tab and create a WLAN profile, or click **More**>**Wired**>**New** and create a wired port profile.
2. In the **Access** tab, select the role for which you want create the access rule.
3. Under **Access Rules**, click **New**. The **New Rule** window is displayed.
4. Select **CALEA**.
5. Click **OK**.
6. Create a role assignment rule if required.
7. Click **Finish**.

Configuring an IAP for AirGroup Support

This section provides the following information:

- AirGroup Overview on page 106
- AirGroup with Central on page 107
- Configuring AirGroup and AirGroup Services on page 108

AirGroup Overview

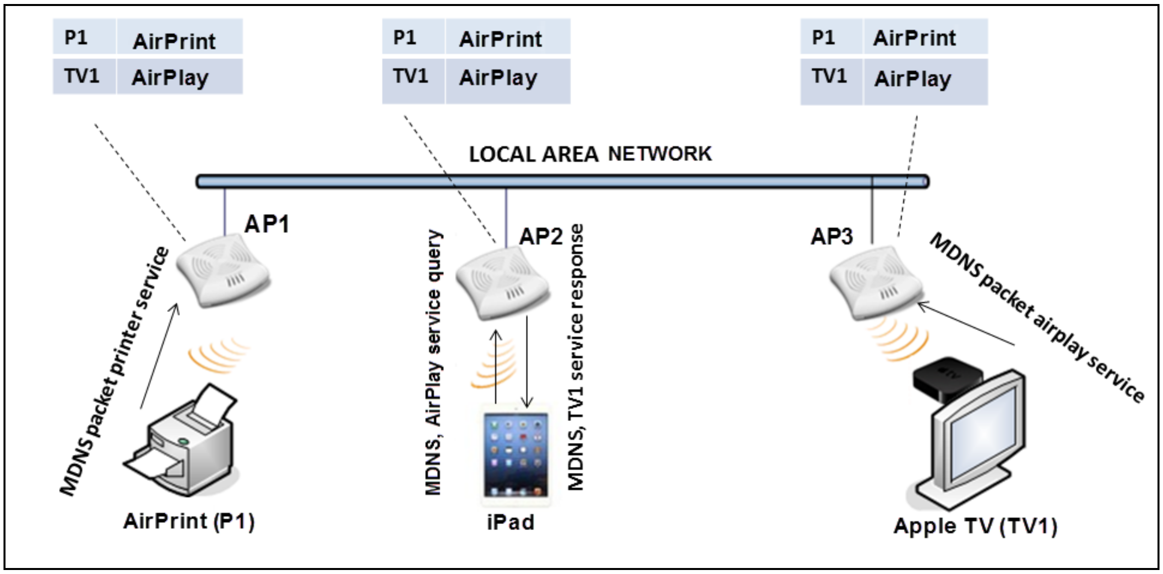
AirGroup is a zero configuration networking protocol that enables service discovery, address assignment, and name resolution for desktop computers, mobile devices, and network services. It is designed for flat, single-subnet IP networks such as wireless networking at home.

Bonjour can be installed on computers running Microsoft Windows and is supported by the new network-capable printers. Bonjour uses multicast DNS (mDNS) to locate devices and the services offered by these devices. The AirGroupsolution supports both wired and wireless devices. Wired devices that support Bonjour services are part of AirGroup when connected to a VLAN that is terminated on the VC.

The distributed AirGroup architecture allows each IAP to handle Bonjour queries and responses without overloading a VC. This results in a scalable AirGroup solution.

AirGroup architecture shows a sample AirGroup architecture. In this scenario, IAP1 discovers the Air Print printer (P1) and IAP3 discovers the Apple TV (TV1). IAP1 advertises information about P1 to the other IAPs on the LAN. Similarly, IAP3 advertises information about TV1 to IAP1 and IAP2. This type of distributed architecture allows any IAP to respond to its connected devices locally. In this example, the iPad obtains a direct response from AP2 about the other Bonjour-enabled services in the network.

Figure 4 *AirGroup Architecture*



AirGroup with Central

AirGroup capabilities are available in Aruba WLANs where Wi-Fi data is transmitted via IAPs. AirGroup is available on anAruba WLAN that is managed by Central.

- The AirGroup administrator assigns the AirGroup operator role to an end user, which authorizes the user to register their device—such as an Apple TV.
- Central maintains information for all mDNS services.
- Central responds to device queries based on contextual data such as user role, username, and location.

AirGroup Solution

In large universities and enterprise networks, it is common for Bonjour-capable devices to connect to the network across VLANs. As a result, user devices such as an iPad on a specific VLAN cannot discover an Apple TV that resides on another VLAN. As the addresses used by the protocol are link-scope multicast addresses, each query or advertisement can only be forwarded on its respective VLAN.

Broadcast and multicast traffic are usually filtered out from a wireless LAN network to preserve airtime and battery life. This inhibits the performance of Bonjour services as they rely on multicast traffic. Aruba addresses this mDNS challenge with AirGroup technology.

AirGroup leverages key elements from portfolio of Aruba including operating system software for Central. AirGroup maintains seamless connectivity between clients and services across VLANs and SSIDs. The mDNS packet traffic is minimized, thereby preserving valuable wired network bandwidth and WLAN airtime.

The following list summarizes the filtering options that are integrated with Central deployment models:

- Allow mDNS to propagate across subnets/VLANs
- Limit multicast mDNS traffic on the network
- VLAN based mDNS service policy enforcement
- User-role based mDNS service policy enforcement

AirGroup also enables context awareness for services across the network:

- AirGroup is aware of personal devices. For example, an Apple TV in a dorm room can be associated with the student who owns it.
- AirGroup is aware of shared resources.For example, an Apple TV in a meeting room or a printer in a supply room that is available to certain users, such as the marketing department. Or, in a classroom, teachers can use AirPlay to wirelessly project a laptop screen onto an HDTV monitor using an Apple TV.
- When configured with Central, AirGroup enables a client to perform a location-based discovery. For example, when a client roams from one Central cluster to another, it can discover devices available in the new cluster to which the client is currently connected.

AirGroup provides the following features:

- Send unicast responses to mDNS queries and reduces mDNS traffic footprint.
- Ensure cross-VLAN visibility and availability of mDNS devices and services.
- Allow or block mDNS services for all users.
- Allow or block mDNS services based on user roles.
- Allow or block mDNS services based on VLANs.

Bonjour supports zero-configuration services. The services are preconfigured and are available as part of the factory default configuration. The administrator can also enable or disable any or all services.

The following services are available for IAP clients:

- AirPlay — Apple AirPlay allows wireless streaming of music, video, and slideshows from your iOS device to Apple TV and other devices that support the AirPlay feature.
- AirPrint — Apple AirPrint allows you to print from an iPad, iPhone, or iPod Touch directly to any AirPrint compatible printer.
- iTunes— The iTunes service is used by iTunes Wi-Fi sync and iTunes home-sharing applications across all Apple devices.
- RemoteMgmt— Use this service for remote login, remote management, and FTP utilities on Apple devices.
- Sharing— Applications such as disk sharing and file sharing, use the service ID that are part of this service on one or more Apple devices.
- Chat— The iChat (Instant Messenger) application on Apple devices uses this service.

Configuring AirGroup and AirGroup Services

To enable AirGroup and its services:

1. Select **Configuration > Access Points > Services > AirGroup**.
2. Select the **AirGroup** check box. The **AirGroup** configuration parameters are displayed.
3. Select **Enable AirGroup Support Across Mobility Domains**to enable Inter cluster mobility.
4. Select required AirGroup services. To allow all services, select **Allow All**.
5. Based on the services configured, you can block any user roles and VLAN from accessing a AirGroup service. The user roles and VLANs marked as disallowed are prevented from accessing the corresponding AirGroup service. You can create a list of disallowed user roles and VLANs for all AirGroup services configured on the IAP. For example, If the AirPlay service is selected, the **Edit** links for the **AirPlay**

Disallowed Roles and **AirPlay Disallowed VLANS** are displayed. Similarly, if sharing service is selected, the **Edit** links for the **Sharing Disallowed Roles** and **Sharing Disallowed VLANS** are displayed.

- To block user roles from accessing a AirGroup service, click the corresponding **Edit** link and select the user roles for which you want to restrict access. By default, an AirGroup service is accessible by all user roles configured in your IAP cluster.
- To select VLANs from allowing access to AirGroup service, click the corresponding **Edit** link and select the VLANs to exclude. By default, the AirGroup services are accessible by users or devices in all VLANs configured in your IAP cluster.

6. To allow the users to use AirGroup services enabled in a guest VLAN, select the **Guest AirGroup Multicast** check box. However, the AirGroup devices are visible in the guest VLAN and AirGroup does not discover or enforce policies in the guest VLAN.
7. Click **Save Settings**.

Integrating an IAP with Palo Alto Networks Firewall

Palo Alto Networks (PAN) next-generation firewall offers contextual security for all users for safe enabling of applications. A simple firewall beyond basic IP address or TCP port numbers only provides a subset of the enhanced security required for enterprises to secure their networks. In the context of businesses using social networking sites, legacy firewalls are not able to differentiate valid authorized users from casual social networking users.

The Palo Alto next-generation firewall is based on user ID, which provides many methods for connecting to sources of identity information and associating them with firewall policy rules. For example, it provides an option to gather user information from Active Directory or LDAP server.

Integration with Central

The functionality provided by the PAN firewall based on user ID requires the collection of information from the network. The IAP maintains the network (such as mapping IP address) and user information for its clients in the network and can provide the required information for the user ID feature on PAN firewall. Before sending the user-ID mapping information to the PAN firewall, the IAP must retrieve an API key that is used for authentication for all APIs.

IAP and PAN firewall integration can be seamless with the XML-API that available with PAN-OS 5.0 or later.

To integrate an IAP with PAN user ID, a global profile is added. This profile can be configured on an IAP with PAN firewall information such as IP address, port, user name, password, firewall enabled or disabled status.

The IAP sends messages to PAN based on the type of authentication and client status:

- After a client completes the authentication and is assigned an IP address, IAP sends the **login** message.
- After a client is disconnected or dissociated from the IAP, the IAP sends a **logout** message.

Configuring IAP for PAN integration

To configure IAP for PAN firewall integration:

1. Select **Configuration > Access Points > Services**. The **Services** pane is displayed.
2. Click **Network Integration**. The PAN firewall configuration options are displayed.
3. Select **Enable** to enable PAN firewall.
4. Specify the **User Name** and **Password**. Ensure that you provide user credentials of the PAN firewall administrator.
5. Enter the PAN firewall **IP Address**.
6. Enter the port number within the range of 1—65535. The default port is 443.
7. Click **Save Settings**.

Enabling AppRF™ Service

To view the AppRF statistics for the clients associated with an IAP, you must enable the AppRF service.

To enable AppRF, complete the following steps:

1. Navigate to **Configuration > Access Points**>**Services**.
2. Click APP RF and then select the **DPI** check box.

Configuring Uplinks

This section provides the following information:

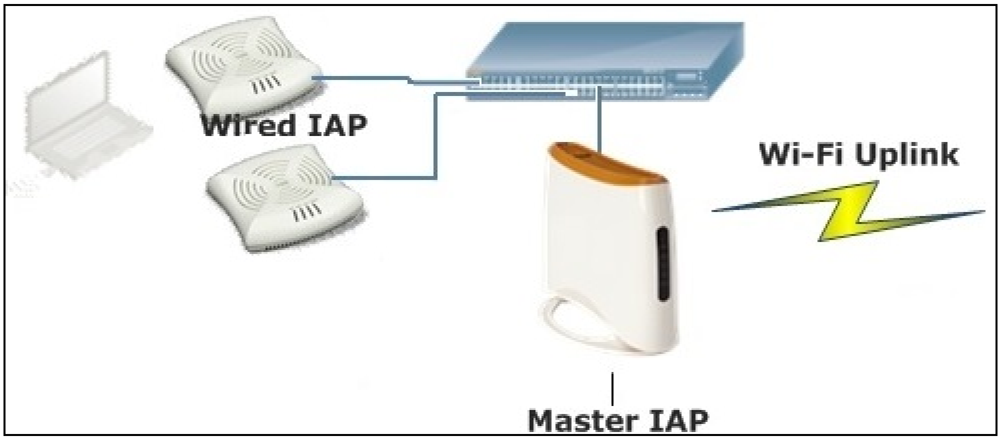
- Uplink Interfaces on page 110
- Uplink Preferences and Switching on page 117

Uplink Interfaces

Central supports 3G and 4G USB modems, and the Wi-Fi uplink to provide access to the corporate network.

Figure 5 illustrates a scenario in which the IAPs join the Virtual Controller as slave IAPs through a wired or mesh Wi-Fi uplink:

Figure 5 *Uplink Types*



The following types of uplinks are supported on Central:

- 3G/4G Uplink
- Wi-Fi uplink
- Ethernet Uplink

3G/4G Uplink

Central supports the use of 3G/4G USB modems to provide the Internet backhaul to Central. The 3G/4G USB modems can be used to extend client connectivity to places where an Ethernet uplink cannot be configured. This enables the RAPs to automatically choose the available network in a specific region.

Types of Modems

Central supports the following three types of 3G modems:

- **True Auto Detect** — Modems of this type can be used only in one country and for a specific ISP. The parameters are configured automatically and hence no configuration is necessary.

- **Auto-detect + ISP/country** — Modems of this type require the user to specify the Country and ISP. The same modem is used for different ISPs with different parameters configured for each of them.
- **No Auto-detect** — Modems of this type are used only if they share the same Device-ID, Country, and ISP details. You need to configure different parameters for each of them. These modems work with Central when the appropriate parameters are configured.

The following table lists the types of supported 3G modems:

Table 39: *List Of Supported 3G Modems*

Modem Type	Supported 3G Modems
True Auto Detect	• USBConnect 881 (Sierra 881U) • Quicksilver (Globetrotter ICON 322) • UM100C (UTstarcom) • Icon 452 • Aircard 250U (Sierra) • USB 598 (Sierra) • U300 (Franklin wireless) • U301 (Franklin wireless) • USB U760 for Virgin (Novatel) • USB U720 (Novatel/Qualcomm) • UM175 (Pantech) • UM150 (Pantech) • UMW190(Pantech) • SXC-1080 (Qualcomm) • Globetrotter ICON 225 • UMG181 • NTT DoCoMo L-05A (LG FOMA L05A) • NTT DoCoMo L-02A • ZTE WCDMA Technologies MSM (MF668?) • Fivespot (ZTE) • c-motech CNU-600 • ZTE AC2736 • SEC-8089 (EpiValley) • Nokia CS-10 • NTT DoCoMo L-08C (LG) • NTT DoCoMo L-02C (LG) • Novatel MC545 • Huawei E220 for Movistar in Spain • Huawei E180 for Movistar in Spain • ZTE-MF820 • Huawei E173s-1 • Sierra 320 • Longcheer WM72 • U600 (3G mode)

Table 39: *List Of Supported 3G Modems*

Modem Type	Supported 3G Modems
Auto-detect + ISP/country	• Sierra USB-306 (HK CLS/1010 (HK)) • Sierra 306/308 (Telstra (Aus)) • Sierra 503 PCIe (Telstra (Aus)) • Sierra 312 (Telstra (Aus)) • Aircard USB 308 (AT&T's Shockwave) • Compass 597(Sierra) (Sprint) • U597 (Sierra) (Verizon) • Tstick C597(Sierra) (Telecom(NZ)) • Ovation U727 (Novatel) (Sprint) • USB U727 (Novatel) (Verizon) • USB U760 (Novatel) (Sprint) • USB U760 (Novatel) (Verizon) • Novatel MiFi 2200 (Verizon Mifi 2200) • Huawei E272, E170, E220 (ATT) • Huawei E169, E180,E220,E272 (Vodafone/SmarTone (HK)) • Huawei E160 (O2(UK)) • Huawei E160 (SFR (France)) • Huawei E220 (NZ and JP) • Huawei E176G (Telstra (Aus)) • Huawei E1553, E176 (3/HUTCH (Aus)) • Huawei K4505 (Vodafone/SmarTone (HK)) • Huawei K4505 (Vodafone (UK)) • ZTE MF656 (Netcom (norway)) • ZTE MF636 (HK CSL/1010) • ZTE MF633/MF636 (Telstra (Aus)) • ZTE MF637 (Orange in Israel) • Huawei E180, E1692,E1762 (Optus (Aus)) • Huawei E1731 (Airtel-3G (India)) • Huawei E3765 (Vodafone (Aus)) • Huawei E3765 (T-Mobile (Germany) • Huawei E1552 (SingTel) • Huawei E1750 (T-Mobile (Germany)) • UGM 1831 (TMobile) • Huawei D33HW (EMOBILE(Japan)) • Huawei GD01 (EMOBILE(Japan))

Table 39: *List Of Supported 3G Modems*

Modem Type	Supported 3G Modems
	- Huawei EC150 (Reliance NetConnect+ (India)) - KDDI DATA07(Huawei) (KDDI (Japan)) - Huawei E353 (China Unicom) - Huawei EC167 (China Telecom) - Huawei E367 (Vodafone (UK)) - Huawei E352s-5 (T-Mobile (Germany))
No auto-detect	- Huawei D41HW - ZTE AC2726

Table 40: *4G Supported Modem*

Modem Type	Supported 4G Modem
True Auto Detect	- Pantech UML290 - Ether-lte

When UML290 runs in auto detect mode, the modem can switch from 4G network to 3G network or vice-versa based on the signal strength. To configure the UML290 for the 3G network only, manually set the USB type to **pantech-3g**. To configure the UML290 for the 4G network only, manually set the 4G USB type to **pantech-lte**.

Configuring Cellular Uplink Profiles

You can configure 3G or 4G uplinks using Central.

1. Click the **System** link at the upper right corner of the Central main window. The **System** window is displayed.
2. In the **System** window, click the **show advanced settings** link. The advanced options are displayed.
3. Click the **Uplink** tab and perform any of the following steps:

- To configure a 3G or 4G uplink automatically, select the **Country** and **ISP**. The parameters are automatically populated.
- To configure a 3G or 4G uplink manually, perform the following steps:

a. Obtain the modem configuration parameters from the local IT administrator or the modem manufacturer.

b. Enter the type of the 3G/4G modem driver type:

- For 3G — Enter the type of 3G modem in the **USB type** text box.
- For 4G — Enter the type of 4G modem in the **4G USB type** text box.

c. Enter the device ID of modem in the **USB dev** text box.

d. Enter the TTY port of the modem in the **USB tty** text box.

e. Enter the parameter to initialize the modem in the **USB init** text box.

f. Enter the parameter to dial the cell tower in the **USB dial** text box.

g. Enter the username used to dial the ISP in the **USB user** text box.

h. Enter the password used to dial the ISP in the **USB password** text box.

i. Enter the parameter used to switch a modem from the storage mode to modem mode in the **USB mode switch** text box.

4. To configure 3G/4G switch network, provide the driver type for the 3G modem in the **USB type** text box and the driver type for 4G modem in the **4G USB type** text box.
5. Click **OK**.
6. Reboot the IAP for changes to affect.

Wi-Fi uplink

The Wi-Fi uplink is supported for all IAP models, except 802.11ac APs. Only the master IAP uses the Wi-Fi uplink. The Wi-Fi allows uplink to open, PSK-CCMP, and PSK-TKIP SSIDs.

- For single radio IAPs, the radio serves wireless clients and Wi-Fi uplink.
- For dual radio IAPs, both radios can be used to serve clients but only one of them can be used for Wi-Fi uplink.

NOTE

When Wi-Fi uplink is in use, the client IP is assigned by the internal DHCP server.

Configuring a Wi-Fi Uplink Profile

The following configuration conditions apply to the Wi-Fi uplink:

- To bind or unbind the Wi-Fi uplink on the 5 GHz band, reboot the IAP.
- If Wi-Fi uplink is used on the 5 GHz band, mesh is disabled. The two links are mutually exclusive.

To provisionan IAP with Wi-Fi Uplink, complete the following steps:

1. If you are configuring a Wi-Fi uplink after restoring factory settings on an IAP, connect the IAP to an Ethernet cable to allow the IAP to get the IP address. Otherwise, go to step 2.
2. Select **Configuration > Access Points > System**. The **System** details are displayed.
3. Select **Uplink** and under **WiFi**, enter the name of the wireless network that is used for Wi-Fi uplink in the **Name (SSID)** box.
4. From **Management**, select the type of key for uplink encryption and authentication. If the uplink wireless router uses mixed encryption, WPA-2 is recommended for Wi-Fi uplink.
5. From **Band**, select the band in which the VC currently operates. The following options are available:
   - 2.4 GHz (default)
   - 5 GHz
6. From **Passphrase Format**, select a **Passphrase format**. The following options are available:
   - 8 - 63 alphanumeric characters
   - 64 hexadecimal characters

NOTE

Ensure that the hexadecimal password string is exactly 64 digits in length.

7. Enter a pre-shared key (PSK) passphrase in **Passphrase** and click **OK**.

Ethernet Uplink

The Ethernet 0 port on an IAP is enabled as an uplink port by default.

Ethernet uplink supports the following:

- PPPoE
- DHCP
- Static IP

You can use PPPoE for your uplink connectivity in a single AP deployment.

Uplink redundancy with the PPPoE link is not supported.

When the Ethernet link is up, it is used as a PPPoE or DHCP uplink. After the PPPoE settings are configured, PPPoE has the highest priority for the uplink connections. The IAP can establish a PPPoE session with a PPPoE server at the ISP and get authenticated using PAP or the CHAP. Depending upon the request from the PPPoE server, either the PAP or the CHAP credentials are used for authentication. After configuring PPPoE, reboot the IAP for the configuration to take effect. The PPPoE connection is dialed after the AP comes up. The PPPoE configuration is checked during IAP boot and if the configuration is correct, Ethernet is used for the uplink connection.

When PPPoE is used, do not configure Dynamic RADIUS Proxy and IP address of the VC. An SSID created with default VLAN is not supported with PPPoE uplink.

You can also configure an alternate Ethernet uplink to enable uplink failover when an Ethernet port fails.

Configuring PPPoE uplink profile

To configure PPPOE settings:

1. Select **Configuration > Access Points >System**. The **System** details are displayed.
2. Select **Uplink**, perform the following steps in the **PPPoE** pane:

   a. Enter the **PPPoE service name** provided by your service provider in **Service Name**.

   b. In the **Chap Secret** and **Retype CHAP Secret** fields, enter the secret key used for CHAP authentication. You can use a maximum of 34 characters for the CHAP secret key.

   c. Enter the user name for the PPPoE connection in the **USER** field.

   d. In the **Password** and **Retype Password** fields, enter a password for the PPPoE connection and confirm it.
3. To set a local interface for the PPPoE uplink connections, select a value from **Local Interface**. The selected DHCP scope is used as a local interface on the PPPoE interface and the Local, L3 DHCP gateway IP address as its local IP address. When configured, the local interface acts as an unnumbered PPPoE interface and and allocated the entire Local, L3 DHCP subnet to the clients.

The options in **Local Interface** are displayed only if a Local, L3 DHCP scope is configured on the IAP.

4. Click **Save Settings**.
5. Reboot the IAP.

Uplink Preferences and Switching

This topic describes the following procedures:

- Enforcing Uplinks on page 118
- Setting an Uplink Priority on page 118
- Enabling Uplink Pre-emption on page 118

Enforcing Uplinks

The following configuration conditions apply to the uplink enforcement:

- When an uplink is enforced, the IAP uses the specified uplink regardless of uplink pre-emption configuration and the current uplink status.
- When an uplink is enforced and multiple Ethernet ports are configured and uplink is enabled on the wired profiles, the IAP tries to find an alternate Ethernet link based on the priority configured.
- When no uplink is enforced and pre-emption is not enabled, and if the current uplink fails, the IAP tries to find an available uplink based on the priority configured.
- When no uplink is enforced and pre-emption is enabled, and if the current uplink fails, the IAP tries to find an available uplink based on the priority configured. If current uplink is active, the IAP periodically tries to use a higher priority uplink and switches to the higher priority uplink even if the current uplink is active.

To enforce a specific uplink on an IAP, complete the following steps:

1. Select **Configuration > Access Points > System >Uplink**. The **Uplink** details are displayed.
2. Under **Management**, select the type of uplink from **Enforce Uplink**. If Ethernet uplink is selected, the **Port** field is displayed.
3. Specify the Ethernet interface port number.
4. Click **OK**. The selected uplink is enforced on the IAP.

Setting an Uplink Priority

To set an uplink priority:

1. Select **Configuration > Access Points > System > Uplink**. The **Uplink** details are displayed.
2. Under **Uplink Priority List**, select the uplink, and increase or decrease the priority. By default, the Eth0 uplink is set as a high priority uplink.
3. Click **OK**. The selected uplink is prioritized over other uplinks.

Enabling Uplink Pre-emption

The following configuration conditions apply to uplink pre-emption:

- Pre-emption can be enabled only when no uplink is enforced.
- When pre-emption is disabled and the current uplink fails, the IAP tries to find an available uplink based on the uplink priority configuration.
- When pre-emption is enabled and if the current uplink is active, the IAP periodically tries to use a higher priority uplink, and switches to a higher priority uplink even if the current uplink is active.

To enable uplink pre-emption:

1. Select **Configuration > Access Points >System >Uplink**. The **Uplink** details are displayed.
2. Under **Management**, ensure that the **Enforce Uplink** is set to None.
3. Set **Pre-Emption** to **ON**.
4. Click **OK**.

Switching Uplinks based on the Internet Availability

You can configure Central to switch uplinks based on the Internet availability.

When the uplink switchover based on Internet availability is enabled, the IAP continuously sends ICMP packets to some well-known Internet servers. If the request is timed out due to a bad uplink connection or uplink interface failure, and the Internet is not reachable from the current uplink, the IAP switches to a different connection.

To configure uplink switching, complete the following steps:

1. Select **Configuration > Access Points > System >Uplink**. The **Uplink** details are displayed.
2. Under **Management**, set **Internet Failover** to **ON**.
3. Specify values for **Failover Internet Packet Send Frequency**, **Failover Internet Packet Lost Count**, and **Internet Check Count**.
4. Click **OK**.

NOTE

When **Internet failover** is enabled, the IAP ignores the VPN status, although uplink switching based on VPN status is enabled.

Mobility and Client Management

This section provides the following information:

- Layer-3 Mobility Overview on page 119
- Configuring L3 Mobility Domain on page 120

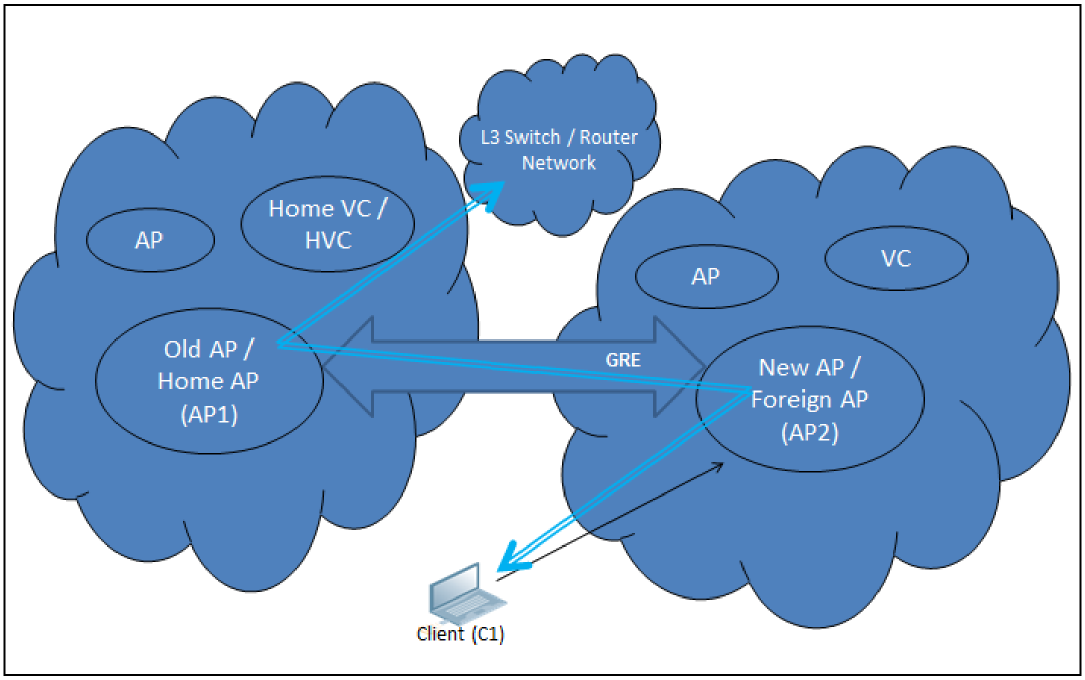
Layer-3 Mobility Overview

IAPs form a single Central network when they are in the same Layer-2 (L2) domain. As the number of clients increase, multiple subnets are required to avoid broadcast overhead. In such a scenario, a client must be allowed to roam away from the Central network to which it first connected (home network) to another network supporting the same WLAN access parameters (foreign network) and continue its existing sessions.

Layer-3 (L3) mobility allows a client to roam without losing its IP address and sessions. If WLAN access parameters are the same across these networks, clients connected to IAPs in a given Central network can roam to IAPs in a foreign Central network and continue their existing sessions using their IP addresses. You can configure a list of Virtual Controller IP addresses across which L3 mobility is supported.

The Aruba Central Layer-3 mobility solution defines a Mobility Domain as a set networks, with the same WLAN access parameters, across which client roaming is supported. The Central network to which the client first connects is called its home network. When the client roams to a foreign network, an IAP in the home network (home IAP) anchors all traffic to or from this client. The IAP to which the client is connected in the foreign network (foreign IAP) tunnels all client traffic to or from the home IAP through a GRE tunnel.

Figure 6 *Traffic Routing*



When a client first connects to Central network, a message is sent to all configured VC IP addresses to see if this is an L3 roamed client. On receiving an acknowledgment from any of the configured VC IP addresses, the client is identified as an L3 roamed client. If the IAP has no GRE tunnel to this home network, a new tunnel is formed to an IAP (home IAP) from the home network of the client.

Each foreign IAP has only one home IAP per Central network to avoid duplication of broadcast traffic. Separate GRE tunnels are created for each foreign IAP / home IAP pair. If a peer IAP is a foreign IAP for one client and a home IAP for another, two separate GRE tunnels are used to handle L3 roaming traffic between these IAPs.

If client subnet discovery fails on association due to some reason, the foreign IAP identifies its subnet when it sends out the first L3 packet. If the subnet is not a local subnet and belongs to another network, the client is treated as an L3 roamed client and all its traffic is forwarded to the home network through a GRE tunnel.

Configuring L3 Mobility Domain

To configure a mobility domain, you have to specify the list of all Central networks that form the mobility domain. To allow clients to roam seamlessly among all the APs, specify the VC IP for each foreign subnet. You may include the local Central or VC IP address, so that the same configuration can be used across all Central networks in the mobility domain.

It is recommended that you configure all client subnets in the mobility domain. When client subnets are configured:

- If a client is from a local subnet, it is identified as a local client. When a local client starts using the IP address, the L3 roaming is terminated.
- If the client is from a foreign subnet, it is identified as a foreign client. When a foreign client starts using the IP address, the L3 roaming is set up.

Home agent load balancing

Home Agent Load Balancing is required in large networks where multiple tunnels might terminate on a single border or lobby AP and overload it. When load balancing is enabled, the VC assigns the home AP for roamed clients by using a round robin policy. With this policy, the load for the APs acting as Home Agents for roamed clients is uniformly distributed across the IAP cluster.

Configuring L3 mobility domain

To configure L3 mobility domain:

1. Select **Configuration > Access Points > System**. The **System** details are displayed.
2. Select **L3 Mobility**. The L3 Mobility details are displayed.
3. From **Home Agent Load Balancing**, select **Enabled**. By default, home agent load balancing is disabled.
4. Click **New** in **Virtual Controller IP Addresses**, add the IP address of a VC that is part of the mobility domain, and click **OK**.
5. Repeat Step 2 to add the IP addresses of all VCs that form the L3 mobility domain.
6. Click **New** in **Subnets** and specify the following:
   a. Enter the client subnet in the **IP Address** box.
   b. Enter the mask in the **Subnet Mask** box.
   c. Enter the VLAN ID in the home network in the **VLAN ID** box.
   d. Enter the home VC IP address for this subnet in the **Virtual Controller IP** box.
7. Click **OK**.

Enterprise Domains

The enterprise domain names list displays the DNS domain names that are valid on the enterprise network. This list is used to determine how client DNS requests are routed. When **Content Filtering** is enabled, the DNS request of the clients is verified and the domain names that do not match the names in the list are sent to the openDNS server.

Configuring Enterprise Domains

To configure an enterprise domain, complete the following steps:

1. Select **Configuration > Access Points > System**, click **Enterprise Domains**. The **Enterprise Domains** details are displayed.
2. Click **New** and enter a name in the **New Domain Name**.
3. Click **Ok**.

To remove a domain, select the domain and click **Delete**.

You can configure an enterprise domain using Central.

4. Select **System** > **General**, click **Enterprise Domains**. The **Enterprise Domain** details are displayed.
5. Click **New** and enter a **New Domain Name**
6. Click **OK** to apply the changes.

To delete a domain, select the domain and click **Delete** to remove the domain name from the list.

SNMP and Logging

This section provides the following information:

- Configuring SNMP on page 122
- Configuring a Syslog Server on page 124
- Configuring TFTP Dump Server on page 124

Configuring SNMP

This section provides the following information:

- SNMP parameters for IAP on page 122
- Configuring Community String for SNMP on page 122
- Configuring SNMP Traps on page 123

SNMP parameters for IAP

Central supports SNMPv1, SNMPv2c, and SNMPv3 for reporting purposes only. An IAP cannot use SNMP to set values in an Aruba system.

You can configure the following parameters for an IAP:

Table 41: *SNMP Parameters*

Parameter	Description
Community Strings for SNMPV1 and SNMPV2	An SNMP Community string is a text string that acts as a password, and is used to authenticate messages sent between the Virtual Controller and the SNMP agent.
If you are using SNMPv3 to obtain values from the IAP, you can configure the following parameters:	
Name	A string representing the name of the user.
Authentication Protocol	An indication of whether messages sent on behalf of this user can be authenticated, and if so, the type of authentication protocol used. This can take one of the two values: ● MD5— HMAC-MD5-96 Digest Authentication Protocol ● SHA: HMAC-SHA-96 Digest Authentication Protocol
Authentication protocol password	If messages sent on behalf of this user can be authenticated, the (private) authentication key for use with the authentication protocol. This is a string password for MD5 or SHA depending on the choice above.
Privacy protocol	An indication of whether messages sent on behalf of this user can be protected from disclosure, and if so, the type of privacy protocol which is used. This takes the value DES (CBC-DES Symmetric Encryption).
Privacy protocol password	If messages sent on behalf of this user can be encrypted/decrypted with DES, the (private) privacy key for use with the privacy protocol.

Configuring Community String for SNMP

This section describes the procedure for configuring SNMPv1, SNMPv2, and SNMPv3 community strings using the Central.

Creating Community strings for SNMPv1 and SNMPv2 using Central

To create community strings for SNMPv1 and SNMPv2:

1. Click the **System** link at the top right corner of the Central main window. The system window is displayed.
2. Click the **Monitoring** tab.
3. Click **New**.
4. Enter the string in the **New Community String** text box.
5. Click **OK**.
6. To delete a community string, select the string, and click **Delete**.

Creating community strings for SNMPv3 using Central

To create community strings for SNMPv3:

1. Click **System** link at the top right corner of the Central main window. The system window is displayed.
2. Click the **Monitoring** tab. The SNMP configuration parameters displayed in the **Monitoring** tab.
3. Click **New** in the **Users for SNMPV3** box. A window for specifying SNMPv3 user information is displayed.
4. Enter the name of the user in the **Name** text box.
5. Select the type of authentication protocol from the **Auth protocol** drop-down list.
6. Enter the authentication password in the **Password** text box and retype the password in the **Retype** text box.
7. Select the type of privacy protocol from the **Privacy protocol** drop-down list.
8. Enter the privacy protocol password in the **Password** text box and retype the password in the **Retype** text box.
9. Click **OK**.
10. To edit the details for a particular user, select the user and click **Edit**.
11. To delete a particular user, select the user and click **Delete**.

Configuring SNMP Traps

Central supports the configuration of external trap receivers. Only the IAP acting as the Virtual Controller generates traps. The OID of the traps is 1.3.6.1.4.1.14823.2.3.3.1.200.2.X.

You can configure SNMP traps using Central.

1. Select **System** > **SNMP**. The **SNMP** window is displayed.
2. Under **SNMP Traps**, enter a name in the **SNMP Engine ID** text box. It indicates the name of the SNMP agent on the access point. The SNMPV3 agent has an engine ID that uniquely identifies the agent in the device and is unique to that internal network.
3. Click **New** and update the following fields:

- **IP Address—** Enter the **IP Address** of the new SNMP Trap receiver.
- **Version**— Select the SNMP version— **v1, v2c, v3** from the drop-down list. The version specifies the format of traps generated by the access point.
- **Community/Username**— Specify the community string for SNMPv1 and SNMPv2c traps and a username for SNMPv3 traps.
- **Port**— Enter the port to which the traps are sent. The default value is 162.
- **Inform**— When enabled, traps are sent as SNMP INFORM messages. It is applicable to SNMPV3 only. The default value is **Yes**.

4. Click **OK** to view the trap receiver information in the **SNMP Trap Receivers** window.

Configuring a Syslog Server

To specify a syslog server for sending syslog messages to the external servers:

1. Select **Configuration > Access Points>System**. The **System** details are displayed.
2. Select the **Logging** tab.
3. In the **Syslog Server** box, enter the IP address of the server to which you want to send system logs.
4. Select the required values to configure Syslog Facility Levels. Syslog facility is an information field associated with a syslog message. It is an application or operating system component that generates a log message. The following facilities are supported by syslog:

- **AP-Debug**—Detailed log about the AP device.
- **Network**— Log about change of network, for example, when a new IAP is added to a network.
- **Security**—Log about network security, for example, when a client connects using wrong password.
- **System**—Log about configuration and system status.
- **User**—Important logs about client.
- **User-Debug**— Detailed log about client.
- **Wireless**— Log about radio.

The following table describes the logging levels in order of severity, from the most severe to the least.

Table 42: *Logging Levels*

Logging level	Description
Emergency	Panic conditions that occur when the system becomes unusable.
Alert	Any condition requiring immediate attention and correction.
Critical	Any critical condition such as a hard drive error.
Error	Error conditions.
Warning	Warning messages.
Notice	Significant events of a non-critical nature. The default value for all syslog facilities.
Information	Messages of general interest to system users.
Debug	Messages containing information useful for debugging.

5. Click **Save Settings**.

Configuring TFTP Dump Server

To configure a TFTP server for storing core dump files:

1. Select **WirelessConfiguration** > **System> Logging**.
2. Enter the IP address of the TFTP server in the **TFTP Dump Server** box.
3. Click **Save Settings**.

This chapter provides the following information:

Deep Packet Inspection with AppRF

AppRF is a custom built Layer 7 firewall capability supported for IAPs managed by Central. It consists of an on-board deep packet inspection and a cloud-based Web Policy Enforcement service that allows creating firewall policies based on types of application.

IAPs with DPI capability analyze data packets to identify applications in use and allow you to create access rules to determine client access to applications, application categories, web categories and website URLs based on security ratings. You can also define traffic shaping policies such as bandwidth control and QoS per application for client roles. For example, you can block bandwidth monopolizing applications on a guest role within an enterprise.

NOTE

The Deep Packet Inspection feature is supported on IAP running 6.4.3.x-4.1.x.x or later releases. The AppRF feature is not supported on IAP-104/105, and IAP-134/135 devices.

Application Visibility

The Central UI includes the **AppRF** option under the **Monitoring** tab. On clicking **AppRF**, a dashboard that provides a summary of client traffic to application and application categories is displayed. You can analyze the client traffic flow using the graphs displayed in the **AppRF** dashboard. To view the graphs on the **AppRF** pane, ensure that the AppRF service is enabled.

NOTE

Application Visibility is supported for IAPs running 6.4.3.1-4.2.0.0 or later release version.

Central supports AppRF monitoring, DPI configuration, and web filtering for IAP-103, RAP-108/109, IAP-114/115, RAP-155, IAP-205, IAP-214/215, IAP-224/225, IAP-274/275, IAP-228, IAP-277, IAP-324/325 devices. The IAP-104/105, IAP-134/135, RAP-3WNP, and IAP-175 devices support only web policy enforcement.

AppRF Dashboard

The **AppRF** dashboard displays application information in the following two tabs:

- **Overview**—The **Overview** tab provides a summary of client traffic to applications, application categories, website categories, and web reputation.
- **Analyze**—The Analyze tab provides a detailed view of client traffic per application, application category, website categories, web reputation, SSID, device type, and user roles.

Both the **AppRF** >**Overview** and **AppRF** > **Analyze** panes include the **Configuration** link. Click the **Configuration** link, to create or modify the DPI ACL rules for applications, application categories, websites, and web categories based on the security score for a specific network profile. For more information on configuring DPI access rules, see Configuring ACL Rules for Application and Application Categories and Configuring Web Policy Enforcement .

You can view the client traffic to **Applications, Application Categories, Website Categories, and Web Reputation** graphs for a specific time frame (3 Hours, 1 Day, 1 Week, 1 Month, 3 Months). By default, the graphs display real-time client traffic data or usage trend in the last three hours.

NOTE

The application (Apps) and Web Categories graphs are also displayed in the **Monitoring > Access Points >** AP details and **Monitoring > Clients >** Client details pages.

AppRF data is updated every 0th minute of every hour. The data population on the AppRF dashboard may be delayed by an hour when compared to the AppRF data displayed in the**Monitoring > Access Points >** AP details and **Monitoring > Clients >** Client details pages.

Overview

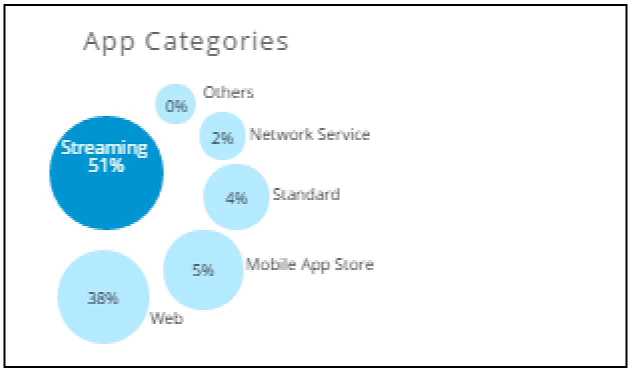
The **Overview** pane include the following sections:

- **Overview**—Presents four different graph areas with data graphs on all client traffic flowing to application (Apps), application category (App Categories), web categories, and website reputation.
- **TOP 5 CLIENTS**—Displays the MAC address and traffic usage in bits per Second (bps) of the top 5 client that use the highest bandwidth. Clicking on a MAC address in the list provides the client details. The AppRF dashboard displays application data only for the clients connected to the network for a total duration of two or more hours.

App Categories Chart

The **App Categories** chart displays details on the client traffic towards the application categories. When the cursor is placed on the chart, the app category and percentage of client traffic flowing to that app category is displayed. The legend below the chart displays the list of application categories to which the client traffic flow is detected. On clicking an app category from legend, the chart hides that app category and displays data for the remaining app categories.

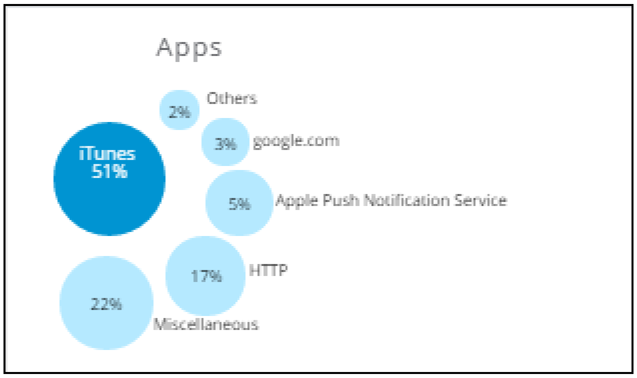
Figure 7 *App Categories Chart With Mouse Hover Text*



Apps Chart

The **Apps** chart displays details on the client traffic flow to specific applications. When the cursor is placed on the chart, the application and percentage of traffic to that application is displayed. The legend below the chart displays the list of applications to which the client traffic flow is detected. On selecting an app from the legend, the chart hides that app and displays data for the remaining apps.

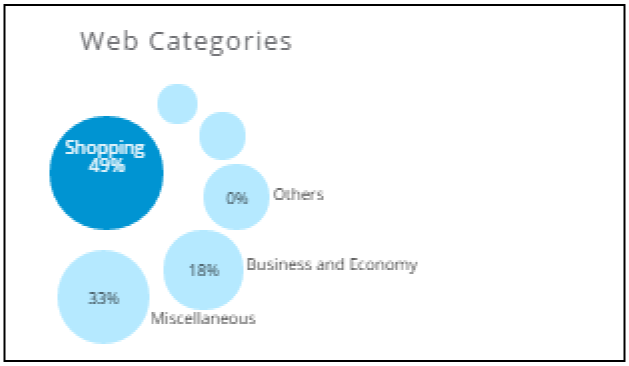
Figure 8 *Apps Chart*



Web Categories Chart

The **Web Categories** chart displays details of the client traffic to web categories. When the cursor is placed on the chart, the web category and percentage of traffic to the web category is displayed. The legend below the chart displays the list of website categories to which the client traffic flow is detected. On selecting a web category from the legend, the chart hides that web category from the chart and displays data for the remaining web categories.

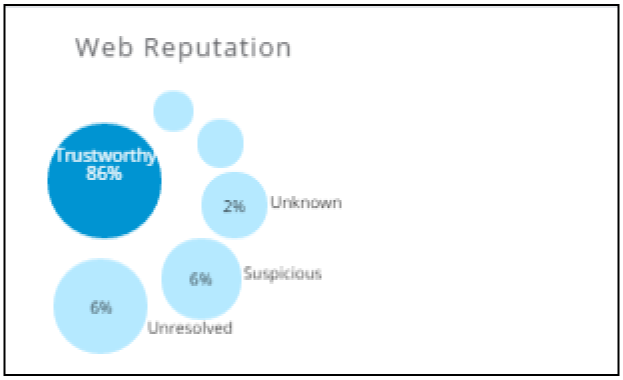
Figure 9 *Web Categories Chart*



Web Reputation Charts

The Web Reputation chart displays details of the client traffic flow to the URLs that are assigned a web reputation score. When the cursor is placed on the chart, the web reputation type and percentage of traffic to the web reputation is displayed. On selecting a web reputation type from the legend, the chart hides the web reputation type and displays data for the remaining web reputation types.

Figure 10 *Web Reputation Chart*



Analyze

The **Analyze** pane allows you to analyze the client traffic to applications, application categories, web categories, web reputation score, SSID, device type, and user roles.

The **Analyze** pane consists of the **App Categories**. **Apps**, **Web Categories**, **Web Reputation**, **SSID**, **Device Type** and **User Roles** widgets.

NOTE

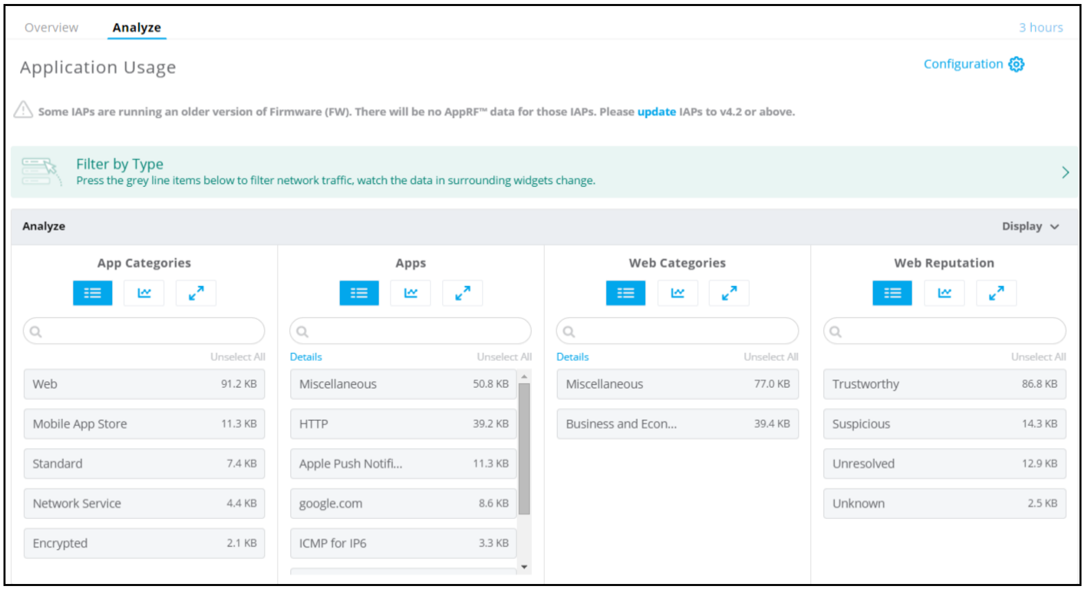
The **SSID**, **Device Type**, and **User Role** widgets are not displayed by default. These can be displayed by selecting them from the **Display** drop-down list.

All widgets provide the following view options:

- **List view**—Displays data usage for applications, application categories, web categories, and web reputation in the list format.
- **Chart view**—Presents the data usage information for applications, application categories, web categories, and web reputation in the graphical format. Place the cursor on the chart provides to view the data usage details.
- **Full screen**—Displays the data in the full screen mode.

The following figure shows the contents of the **Analyze** pane.

Figure 11 *Analyze Tab Dashboard*



Some IAPs are running an older version of Firmware (FW). There will be no AppRF™ data for those IAPs. Please update IAPs to v4.2 or above.

Filter by Type

Press the grey line items below to filter network traffic, watch the data in surrounding widgets change.

App Categories (Unselect All)

Web	91.2 KB
Mobile App Store	11.3 KB
Standard	7.4 KB
Network Service	4.4 KB
Encrypted	2.1 KB

Apps (Details, Unselect All)

Miscellaneous	50.8 KB
HTTP	39.2 KB
Apple Push Notifi...	11.3 KB
google.com	8.6 KB
ICMP for IP6	3.3 KB

Web Categories (Details, Unselect All)

Miscellaneous	77.0 KB
Business and Econ...	39.4 KB

Web Reputation (Unselect All)

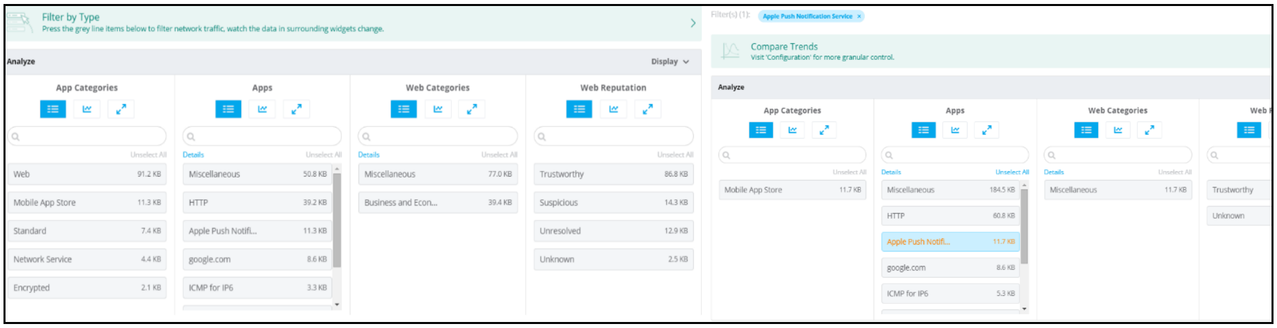
Trustworthy	86.8 KB
Suspicious	14.3 KB
Unresolved	12.9 KB
Unknown	2.5 KB

Filter

To filter the network traffic, ensure that you are in the list view. If you want to add multiple filters from different widgets, do not use the full screen mode. To add filters, click the line items in each widget and notice that the data in surrounding widgets change.

Figure 12 shows the data without filters and data with filters on:

Figure 12 *Data Without Filter And With Filter*



Filter by Type

Press the grey line items below to filter network traffic, watch the data in surrounding widgets change.

Filter(s) (1): Apple Push Notification Service ×

Compare Trends

Visit 'Configuration' for more granular control.

The filtered categories are displayed as filters above widgets. To remove a filter, click the filter or click **X** next to filtered category.

Details—Apps

Clicking on **Details** in the **Apps** widget displays a list of all applications and client traffic to all these applications.

Table 43: *Details—Apps*

Parameter	Description
Category	Name of the application.
Total Usage	The total usage of the application bandwidth.
Usage(%)	Percentage of client traffic to an application.
#SSID	Number of SSIDs through which the clients access an application.

Details—Web Categories

Clicking on **Details** in the **Web Categories** widget displays a table that shows the details of the client traffic to all web categories the last three hours or one day. By default, the details are displayed for the last 3 hours.

Table 44: *Details—Web Categories*

Parameter	Description
Category	Name of the web category.
Total Usage	The total bandwidth used by clients accessing the web category.
Usage(%)	Percentage of clients traffic to the web category.
#SSID	Number of SSIDs used for accessing the web category.

Configuring ACL Rules for Application and Application Categories

This section describes the procedure for configuring access rules based on application and application categories to allow deep packet inspection of client traffic.

For information on configuring access rules based on web categories and web reputation, see Configuring Web Policy Enforcement on page 131.

To configure ACL rules for a user role:

1. Select **Configuration** > **Security** > **Roles**.
2. Select the role for which you want to configure access rules.
3. Under **Access Rules For Selected Roles**, click **(+)** to add a new rule. The new rule window is displayed.
4. Under **Rule Type**, select **Access Control.**
5. To configure access to applications or application categories, select a service category from the following list:

- Application category
- Application

6. Based on the selected service category, configure the following parameters:

Table 45: *Access Rule Configuration Parameters*

Service category	Description
Application Category	Select the application categories to which you want to allow or deny access.
Application	Select the applications to which you want to allow or deny access.
Application Throttling	Application throttling allows you to set a bandwidth limit for an application and application categories. For example, you can limit the bandwidth rate for video streaming applications such as Youtube or Netflix, or assign a low bandwidth to high risk sites. To specify a bandwidth limit: 1. Select the **Application Throttling** check box. 2. Specify the **Downstream** and **Upstream** rates in Kbps.
Action	Select one of the following actions: ● Select **Allow** to allow access users based on the access rule. ● Select **Deny** to deny access to users based on the access rule.
Log	Select this check box if you want a log entry to be created when this rule is triggered. Central supports firewall based logging. Firewall logs on the IAPs are generated as security logs.
Blacklist	Select the **Blacklist** check box to blacklist the client when this rule is triggered. The blacklisting lasts for the duration specified as **Auth failure blacklist time** on the Blacklisting tab of the **Security** window. For more information, see Blacklisting Clients on page 91.
Disable Scanning	Select **Disable scanning** check box to disable ARM scanning when this rule is triggered.

Table 45: *Access Rule Configuration Parameters*

Service category	Description
	The selection of the **Disable scanning** applies only if ARRM scanning is enabled, For more information, see Configuring Radio Parameters on page 69.
DSCP Tag	Select this check box to add a Differentiated Services Code Point (DSCP) tag to the rule. DSCP is an L3 mechanism for classifying and managing network traffic and providing quality of service (QoS) on the network. To assign a higher priority, specify a higher value.
802.1 priority	Select this check box to enable 802.1 priority. 802.1p is an L2 protocol for traffic prioritization to manage quality of service (QoS) on the network. There are eight levels of priority, 0-7. To assign a higher priority, specify a higher value.

3. Click **Save**.

Configuring Web Policy Enforcement

You can configure web policy enforcement on an AP to block certain categories of websites based on your organization specifications by defining ACL rules.

To configure web policy enforcement:

1. Select **Configuration** > **Access Points** > **Security** > **Roles**.
2. Select the role for which you want to configure access rules.
3. Under **Access Rules For Selected Roles**, click **(+)** to add a new rule. The new rule window is displayed.
4. Under **Rule Type**, select **Access Control.**
5. To set an access policy based on web categories:

   a. Under **Service**, select **Web Category**.

   b. Select the categories to which you want to deny or allow access. You can also search for a web category and select the required option.

   c. Under **Action**, select **Allow** or **Deny**.

   d. Click **Save**.
6. To filter access based on the security ratings of the website:

   a. Select **Web Reputation** under **Service**.

   b. Move the slider to select a specific web reputation value to deny access to websites with a reputation value lower than or equal to the configured value or to permit access to websites with a reputation value higher than or equal to the configured value. The following options are available:

- Trustworthy WRI >81 — These are well known sites with strong security practices and may not expose the user to security risks. There is a very low probability that the user will be exposed to malicious links or payloads.
- Low Risk WRI 61-80 — These are benign sites and may not expose the user to security risks. There is a low probability that the user will be exposed to malicious links or payloads.
- Moderate WRI 41-60 — These are generally benign sites, but may pose a security risk. There is some probability that the user will be exposed to malicious links or payloads.
- Suspicious WRI 21-40 — These are suspicious sites. There is a higher than average probability that the user will be exposed to malicious links or payloads.

- High Risk WRI<20 — These are high risk sites. There is a high probability that the user will be exposed to malicious links or payloads.

  c. Under **Action**, select **Allow** or **Deny** as required.

7. To set a bandwidth limit based on web category or web reputation score, select the **Application Throttling** check box and specify the downstream and upstream rates in Kbps. For example, you can set a higher bandwidth for trusted sites and a low bandwidth rate for high risk sites.

8. If required, select the following check boxes:

- **Log** — Select this check box if you want a log entry to be created when this rule is triggered. Central supports firewall based logging. Firewall logs on the IAPs are generated as security logs.
- **Blacklist** — Select this check box to blacklist the client when this rule is triggered. The blacklisting lasts for the duration specified as **Auth Failure Blacklist Time** on the **Blacklisting** pane of the **Security** window. For more information, see Blacklisting Clients on page 91.
- **Disable Scanning**—Select **Disable scanning** check box to disable ARM scanning when this rule is triggered. The selection of the **Disable scanning** applies only if ARM scanning is enabled, For more information, see Configuring Radio Parameters on page 69.
- **DSCP Tag**—Select this check box to add a Differentiated Services Code Point (DSCP) tag to the rule. DSCP is an L3 mechanism for classifying and managing network traffic and providing quality of service (QoS) on the network. To assign a higher priority, specify a higher value.
- **802.1 priority**—Select this check box to enable 802.1 priority. 802.1p is an L2 protocol for traffic prioritization to manage quality of service (QoS) on the network. There are eight levels of priority, 0-7. To assign a higher priority, specify a higher value.

9. Click **Save** to save the rules.

10. Click **Save Settings** in the **Roles** pane to save the changes to the role for which you defined ACL rules.

NOTE

In mixed versions of the groups, the application rule update is supported only at the VC level and not at the group level. If you have a group with multiple IAPs running 6.2.1.0-4.0 and if you upgrade one or more VC to 6.2.1.0-4.1, you can configure application rules at the VC level, but not at the group level. To use application rules at the group level, create a new group and move IAPs running 6.2.1.0-4.1 to the newly created group. If application rules are configured in this group, ensure that the IAPs with versions lower than 6.2.1.0-4.1 are not moved to that group.

Creating Custom Error Page for Web Access Blocked by AppRF Policies

You can create a list of URLs to redirect users to when they access blocked websites. You can define an access rule to use these redirect URLs and assign the rule to a user role in the WLAN network.

Creating a List of Error Page URLs

To create a list of error page URLs, complete the following steps:

1. Go to **Configuration** > **Access Points** > **Security** >**Custom Blocked Page URL**.
2. Click **+** and enter the URL to block.
3. Repeat the procedure to add more URLs. You can add up to 8 URLs to the list of blocked web pages.
4. Click **OK**.

Configuring ACL Rules to Redirect Users to a Specific URL

To configure ACL rules to redirect users to a specific URL:

1. Navigate to **Configuration** > **Access Points** > **Security** > **Roles**.

2. Select a role assigned to a network profile, and click **+** in the Access Rules section. The **New Rule window** is displayed.
3. Select the rule type as **Blocked Page URL**.
4. Select the URLs from the existing list of custom redirect URLs. To add a new URL, click **+**.
5. Click **OK**.
6. Click **OK** in the **Roles** tab to save the changes.

Chapter 9
Switch Configuration

This chapter provides the following information:

Aruba Switches

The Aruba Switches enable secure, role-based network access for wired users and devices, independent of their location or application.

The Switch operates as a wired access point when deployed with an Aruba Mobility Controller. As a wired access point, users and their devices are authenticated and assigned a unique role by the Mobility Controller. These roles are applied irrespective of whether the user is a Wi-Fi client, or is connected to a port on the Switch. The use of Switch allows an enterprise workforce to have consistent and secure access to network resources based on the type of users, client devices, and connection method used.

Central supports the following Aruba Switch platforms:

New Switch Platforms

- Aruba 2920 Switch Series
- Aruba 2930F Switch Series

Supported Firmware Versions

Central supports the following firmware versions on Aruba switches:

- Aruba 2920 Switch Series—WB.16.02.0010 or later
- Aruba 2930F Switch Series—WC.16.02.0010 or later

Legacy Aruba Switch Platforms

Central also supports the following legacy Switch models:

- S1500-12P
- S1200-24P
- S2500-24P
- S3500-24T

Supported Firmware Versions

The following ArubaOS software versions are supported on the legacy Switch platforms:

- 7.3.2.6
- 7.4.0.3
- 7.4.1.4

Configuring Switch Parameters

You can export configurations from an existing Switch to a new Switch within the same group. In this case, the new configuration of the Switch overwrites the existing configuration (including the device override).

You can configure parameters of a Switch through the UI. By default, these parameters have the values configured using the Switch.

If the switch inherits the group configuration, the configuration parameters are already defined. However, if required, you can edit these parameters.

To view the configuration parameters for the Switch, complete the following steps:

1. Click **Configuration**.

- To configure a legacy Aruba Switch, click **Switch-MAS**.
- To configure other Aruba Switches, click **Switch-Aruba**.

2. Click **Switches**. The Switches page displays information described in the following table.

Table 46: *Switches Pane*

Name	Description
MAC Address	MAC address of the Switch
Hostname	Name of the host.
IP Assignment	Method of IP assignment as Static or DHCP.
IP Address	IP address for static IP assignment.
Netmask	Netmask for static IP assignment.
Default Gateway	Default gateway for static IP assignment.

3. To view the details of the switch, click the MAC address of the switch.
4. To edit the switch configuration parameters, click the edit icon.

Viewing Port Details

To view the port details of a switch, complete the following steps:

1. Click **Configuration**.

- To configure a legacy Aruba switch , click **Switch-MAS**.
- To configure other Aruba switches, click **Switch-Aruba**.

2. Click **Ports**. The **Ports** page displays the list of ports configured on the switch.

For the legacy switches, the **Ports** page displays the following information:

Table 47: *Contents Of The Ports Page For Legacy Switches*

Name	Description
Port Number	Indicates the number assigned to the switch port.
Admin Status	Indicates the operational status of the port.
Port Mode	Indicates the mode of operation. The port can be configured to function in Trunk or Access mode.
VLAN	Shows the VLAN to which the port is assigned. Based on the port mode, you can assign different types of VLAN. ● For **Access** mode, an **Access VLAN** can be specified. ● For **Trunk** mode, the **Native VLAN** and **Allowed VLAN** can be configured.
PoE	Displays the enabled or disabled status of Power over Ethernet (PoE).
Auto Negotiation	Indicates the status of the Auto Negotiation. ● If auto negotiation is enabled, the Speed and Duplex fields are automatically set to **Auto**. ● If auto negotiation is disabled, the speed can be set to 10 Mbps, 100 Mbps, or 1 Gbps and the duplex mode can be set to half or full.
Speed/Duplex	Displays the speed and duplex configuration settings for the client traffic.
Trusted	Indicates if the port is trusted.

For the other Aruba switches, the **Ports** page displays the following information:

Table 48: *Contents Of The Ports Page For Other Aruba Switches*

Name	Description
Port Number	Indicates the number assigned to the switch port.
Admin Status	Indicates the operational status of the port.
PoE	Displays the enabled or disabled status of Power over Ethernet (PoE).

3. To edit port details, click **Edit** and configure the port parameters.
4. Click **Save**.

Configuring VLANs

The Aruba switches support the following types of VLANs:

- Port-based VLANs — In the case of trusted interfaces, all untagged traffic is assigned a VLAN based on the incoming port.
- Tag-based VLANs — In the case of trusted interfaces, all tagged traffic is assigned a VLAN based on the incoming tag.

The Aruba legacy switches such as the Mobility Access Switch also support the following types of VLANs.

- Voice VLANs — You can use voice VLANs to separate voice traffic from data traffic when the voice and data traffic are carried over the same Ethernet link.
- MAC-based VLANs — In the case of untrusted interfaces, you can associate a client to a VLAN based on the source MAC of the packet. Based on the MAC, you can assign a role to the user after authentication.

Viewing and Modifying VLAN Details

By default, all the ports in the Switches are assigned to VLAN 1. However, if the ports are assigned to different VLANs, the VLANs page displays these details.

To view the VLAN details, complete the following steps:

1. Click **Configuration**.
   - To configure a legacy Aruba switch , click **Switch-MAS**.
   - To configure other Aruba switches, click **Switch-Aruba**.
2. Click **VLANs**. The **VLANs** page is displayed.
3. To edit the VLAN details, click the edit icon and configure the following parameters:
   - **ID**—VLAN ID.
   - **Description**—A short description for VLAN.
   - **IP Address**—IP address of the VLAN interface.
   - **Netmask**—Netmask of the IP address of the VLAN interface.
   - **Tagged Ports**—Tagged ports if any. A tagged port will normally carry traffic for multiple VLANs from the switch to other network devices such as an upstream router or an edge switch.
   - **Untagged Ports**—Untagged ports if any. In case of untagged ports, the Ethernet frames are not VLAN tagged.
4. Click **Update**.
5. Click **Save Settings**.

Deleting VLAN Details

To delete the VLAN details, complete the following steps:

1. Ensure that the VLANs are not tagged to any ports.
2. Click the delete icon for the VLAN you want to delete.

NOTE

VLAN 1 is the primary VLAN and cannot be deleted.

Configuring DHCP Pools

To configure a new DHCP pool on the Mobility Access Switch, complete the following steps:

1. Click **Configuration**> **Switch-MAS** > **DHCP Pools**. The **DHCP Pools** page opens. If the DHCP pools are already configured, the **DHCP Pools** page displays the details such as the name of the pool, IP address of the network, netmask, and the IP address of the default router.
2. To activate the DHCP service, select the **Enable DHCP service** check box.

3. To edit the DHCP pool details, click the edit icon.

4. To delete a DHCP pool, click the delete icon. When the **Do you want to delete <DHCP Pool Name>?** pop-up window prompts you, click **Yes**.

Adding a New DHCP Pool

1. To add a new DHCP pool, click **New** and configure the following parameters:

- **Name**—Name of the pool.
- **Network**—IP address assigned to the DHCP pool
- **Netmask**—Netmask of the DHCP pool
- **Default Router**—IP address of the default router
- **DNS Server**—Address of the DNS server. To add multiple DNS servers, click +.
- **WINS Server**—Address of the WINS server. To add multiple WINS servers, click +.
- **Lease Time**—The lease time for the DHCP pool in days-hours-minutes format.
- **Exclude Address Range**—The IP address range to exclude. To add multiple excluded address range, click +.
- **Option**—The code and type of the DHCP option to configure.
- **Value**—The value to assign to the DHCP option. To add multiple values, click +.

2. Click **Add**.

Configuring System Parameters for a Switch

The **System** menu under **Switch-MAS** and **Switch-Aruba** allows you to configure administrator credentials and enable mode on a switch.

Configuring Administrator Credentials for Mobility Access Switch

To configure administrator credentials for a Mobility Access Switch, complete the following steps:

1. Click the **Configuration**> **Switch-MAS** > **System**. The **System** page opens.
2. Enter the password for admin in the **Admin Password** text box and confirm the administrator password.
3. Enter the password for enable mode in the **Enable Mode Password** text box and confirm the password.
4. Click **Save Settings**.

Configuring Administrator and Operator Credentials for Other Aruba Switches

To configure administrator credentials for other Aruba switches, complete the following steps:

1. Click the **Configuration** > **Switch-Aruba** > **System**. The **System** page opens.
2. Enter the username for the administrator user.
3. Enter the password for admin in the **Admin Password** text box and confirm the administrator password.
4. Enter the password for enable mode in the **Enable Mode Password** text box and confirm the password.
5. To configure the operator user credentials, complete the following steps:
6. Select the **Set Operator Username** check box.
7. Enter a username and password for the operator user.
8. Confirm the password.
9. Click **Save Settings**.

Configuring a Name Server

To set a static IP switches, you must configure a name server. To configure a name server, complete the following steps:

1. Click **Configuration**.

- To configure a legacy Aruba switch , click **Switch-MAS**.
- To configure other Aruba switches, click **Switch-Aruba**.

2. Enter the IP address of the name server obtained from the DNS server in the **Name Server** text box.
3. Click **Save Settings**.

Chapter 10
Managing Reports

The **Reports** pane displays the reports generated for network and the reports that configured to run a particular schedule.

This section includes the following topics:

- Generated Reports on page 140
- Contents of a Report on page 141
- Viewing a Generated Report on page 142
- Creating a Report on page 142

Generated Reports

On clicking the **Generated Reports**, a table listing the parameters used for generating a report is displayed.

Table 49: *Reports Pane*

Parameter	Description
Title	Displays the title name of the report generated.
Date Run	Displays the date on which report was generated.
Saved By	Indicates the user login name using which the report was generated.
Status	Displays the current status of the report generated.
Actions	Allows to either export the report locally or send to an email address.
Scheduled Type	Indicates when the report is triggered.

Contents of a Report

The following table displays the parameters for the reports generated for networks, security, and PCI compliance pages.

Table 50: *Report Parameters*

Report Type	Parameters Displayed
Network Summary Report	Displays the following parameters: ● Number of APs ● AP Model ● Top Ten Wireless Clients By Usage ● Top Ten APs By Usage ● Total Usage By SSID ● Device Types ● Wireless Clients ● Wireless Data Usage ● Wireless Data Peak Usage ● Top Ten Applications By Usage ● Top Ten Web Categories By Usage ● Switches ● Switch Model ● Top Ten Switches By Usage ● Top Ten Ports By Usage ● Wired Uplink Stats ● Wired Peak Uplink Stats
Security Report	Displays the following parameters: ● Rogue APs ● Total Rogue APs Detected ● Wireless Intrusions ● Total Wireless Intrusions
PCI Compliance	Displays the PCI Compliance result as **Fail** or **Pass**.
Client Inventory	Displays the client details summarized by all aggregation fields. The report includes the following details: ● Number of APs, APs and the AP model ● Number of Clients, Top 10 Clients by Usage, and the type of client device ● Top Ten APs by Usage ● Total Usage by SSID ● Wireless Clients

Report Type	Parameters Displayed
	- Wireless Data Usage graphs such as Top Ten APs by Usage, Total Usage by SSID, Wireless Clients, Wireless Data Usage, Wireless Data Peak Usage, Top 10 applications by usage, Top 10 web categories by usage - Switch information such as the Switches in the network, Switch model, Top 10 Switches by Usage, Top 10 Ports by Usage, wired uplink stats, and wired peak uplink stats graphs.
Infra Inventory	Displays device inventory and subscription information. The report includes the following details: - Number of APs - Number of Switches - IAP subscription information - Switches subscription information - Subscription utilization
Client Usage	Displays information about the client usage, client count, and client traffic to applications, application categories, web categories, and applications with web reputation score assigned.

Viewing a Generated Report

To view a generated report, complete the following steps:

1. Select **Reports > Generated Reports**.
2. Select the **Report Type**. The following types of reports are available:

- Network
- PCI Compliance
- Security
- Client Inventory
- Infra Inventory
- Client Usage

3. Select the desired report from the table.
4. Click the download icon to download the report.
5. Click the email icon to email the report to a specific email address.

Creating a Report

To create a report, complete the following steps:

1. Select **Reports > Configure Reports**. The **Create New Report** page is displayed.
2. Enter the name for the report in **Title**.
3. Select the type of the report to generate.
4. Select the period for which you want to view the report from **Time Span**.
5. Select **Now** from **Run Report** to generate report immediately. To run reports at a later time, select **Later** and specify the duration.

6. Select how often you want to generate the report by choosing **One Time**, **Daily Interval**, **Weekly Interval**, **Monthly Interval**, or **Yearly Interval** from **Repeat**.

7. To send the report through email, select **Email Report**, enter email address, and then click **Create**.

Chapter 11
Maintenance

The **Maintenance** tab displays the maintenance pane for the Central. The **Maintenance** pane consists of the following menu options:

- Firmware
- Subscription Keys
- Device Provisioning
- User Management
- Audit Trail
- Troubleshooting Devices
- API Gateway

Firmware

The **Firmware** tab provides an overview of the latest supported version of firmware for the device, details of the device, and the option to upgrade the device.

Table 51: *Firmware Maintenance*

Data Pane Item	Description
Latest Firmware Version	Displays the latest firmware version available on the public firmware server.
Virtual Controllers	Displays the following information: ● VC Name—Name of the VC ● APs—Number of APs associated to VC ● Location—Location of the IAP device ● Firmware Version—The firmware version on the IAP ● Status—The upgrade status of the IAP
Switch-MAS	Displays the following details about the legacy (Mobility Access Switch) and other Aruba switches managed through Central: ● Hostname—Host name of the switch ● MAC Address—MAC address of the switch ● Model—Model of the switch ● Firmware Version—The current firmware version running on the switch. ● Latest Available Version—The latest firmware version available for the switch platform ● Status—The upgrade status of the switch
Switch-Aruba	
Update Firmware	Allows you to upgrade the device firmware to the latest supported version. For more information, see Upgrading a Device on page 145.

Data Pane Item	Description
Update All	Allows you to simultaneously upgrade firmware for multiple devices.
Cancel Upgrade	Cancels a scheduled upgrade.
Cancel All	Cancels a scheduled upgrade for all devices.
Search Filter	Allows you to define a filter criterion for searching devices based on the host name, MAC address, location, firmware version, and the current upgrade status of the device.

Upgrading a Device

You can upgrade a device either manually or by using the automatic image check feature.

Automatically Upgrading Firmware on a Device

To check for a new version on the image server in the cloud, complete the following steps:

1. Go to **Maintenance > Firmware**. The **Firmware** window is displayed.
2. Select the devices to upgrade.
3. Click **Upgrade Firmware**, select **Automatic**.
4. Specify if the upgrade must be carried out immediately or at a later date and time.
5. Click **Upgrade**. The device downloads the image from the server, saves it to flash, and reboots. Depending on the progress and success of the upgrade, one of the following messages is displayed:

- Upgrading — While image upgrading is in progress.
- Upgrade failed — When the upgrade fails.

6. If the upgrade fails, retry upgrading your device.

Manually Upgrading Firmware on a Device

To manually upgrade to a new firmware image version, complete the following steps:

1. Select **Maintenance** > **Firmware**. The **Firmware** pane is displayed.
2. Click **Upgrade Firmware**.
3. Select the **Manual** option.
4. Select one of the following from the **Type** drop-down:

- General Availability Build
- Early Availability Build
- Custom Build

5. Select a firmware to upgrade from the **Select a firmware version** list. The list of available images for release firmware images are displayed. If you are upgrading to a custom build, enter a valid release version and then press Enter.

NOTE

To obtain custom build details, contact Aruba Support.

6. Specify the upgrade schedule. To upgrade now, click **Now**. To upgrade at a later date, click **Later Date** and specify the upgrade schedule.
7. Click **Upgrade**.

NOTE

After upgrading a switch, click **Reboot**.

Resetting an AP

You can reset the system configuration of an IAP by erasing the existing configuration on the IAP. To erase the existing configuration on an IAP, perform any of the following procedures:

Clearing IAP Configuration Using Groups

To reset an IAP using groups, complete the following steps:

1. Create a new group. Ensure that the group has no additional configuration.
2. Move the IAP that you want to reset, under the new group. After the IAP is moved to a new group, the configuration on the IAP is erased and the default group configuration is pushed to the IAP. However, in this procedure, only the system configuration is cleared and the **Per AP Settings** on the IAP are retained.

Resetting an AP through the Console

To reset an IAP from the IAP console, complete the following steps:

1. Log in to the IAP console. To access the IAP console, select **Monitoring > Access Points**. From the **Access Points** table in the **Access Points** pane, click the IAP to which you want to connect. The **Access Points> AP Details** page is displayed.
2. Click **Console Access**.
3. Execute the **write erase all** command at the command prompt.
4. Reboot the IAP. With this procedure, the complete configuration including the **Per AP Settings** on the IAP is reset.

   After the reboot, the IAP is moved to default group and will not be present in the group to which it was previously attached.

For information on resetting an IAP to factory default configuration by using the reset button on the device, see *Aruba Instant User Guide*.

Subscription Keys

The **Subscription Keys** tab provides details of the licenses assigned to a device.

Viewing Subscription Key Details

To view the subscription key details, click **Maintenance** > **Subscription Keys**.

Table 52: *Subscription Keys Pane*

Data Pane Item	Description
Virtual Controllers	Subscription details for the AP devices.
Switches	Subscription details for switches.
Total Licenses	The total number of licenses.
Used	The total number of licenses that are in use.

Data Pane Item	Description
Available	The total number of available licenses.
Expiring in 90 Days	The number of licenses about to expire in 90 days.
Name	Name of the license.
Start Date	Start date from which the license is valid.
Expires on	License expiration date.
Licenses	The number of licenses associated with the subscription.
Used	The number of licenses in use for the selected subscription.
Add Another Subscription Key	Allows you to add another subscription key.

On clicking a subscription key, the following details are displayed:

- **Serial Number**—Serial number of the device to which the subscription key is assigned.
- **MAC address**—MAC address of the device.
- **Model**—The hardware model of the device.
- **Status**—The status of the subscription key assignment.

Adding Another Subscription Key

When a subscription is extended or renewed, a new subscription key is assigned and is sent to the user. To activate the subscription key:

1. Click **Maintenance** > **Subscription Keys**. The **Subscription Keys** pane is displayed.
2. Click **Add Another Subscription Key** and enter the subscription ID.
3. Click **Activate**. The subscription key is added to the list.

Acknowledging License Expiry Notifications

The **Subscription Keys** page displays the licenses that are about to expire in 90 days. The users with evaluation subscription receive subscription expiry notifications on the 30th, 15th and 1 day before the subscription expiry and on day 1 after the subscription expires.

The users with paid subscriptions receive subscription expiry notifications on the 90th, 60th, 30th, 15th, and 1 day before expiry and two notifications per day on the day 1 and day 2 after the subscription expiry.

Acknowledging Notifications through Email

If the user has multiple subscriptions, a consolidated email with the expiry notifications for all subscriptions is sent to the user. The users can also acknowledge these notifications by clicking **Acknowledge** or **Acknowledge All** links in the email notification.

Acknowledging Notifications in the UI

If a license has already expired or is about to expire within 24 hours, a license expiry notification message is displayed in a pop-up window when the customer logs in to Central.

To prevent Central from generating expiry notifications, click **Acknowledge**. Central does not generate expiry notification messages either in the UI or through email for the acknowledged subscriptions.

Device Provisioning

This section describes the procedures for adding, viewing, and assigning devices to a group or license.

Adding Devices

Central allows you to import devices using your Aruba Activate user credentials, the MAC address and cloud activation key of a device, or the MAC address and Serial Number of a device. You can specify the method for retrieving device information when adding a device. For more information on manually adding devices, see Binding Devices to Your License.

Viewing Devices

To view the devices added to Central, click **Maintenance > Device Provisioning**. Table 53 shows the contents of the **Device Provisioning** page.

Table 53: *Device Provisioning Pane*

Parameter	Description
My Devices	Displays the devices connected to Central.
Manage Licenses	Allows you to assign or unassign licenses to one or several devices.
Pre-provision Groups	Allows you assign devices to a a group.
Device Type	Allows you to view details of the AP (Virtual Controllers) or Switch devices in the inventory.
Sync Now	Allows you to synchronize devices from the inventory.
Add Devices	Allows you to manually add devices to Central network. Typically, Central automatically retrieves the list of devices licensed to a customer account. If the automatic device addition fails, you can manually add the devices.
Serial Number	Displays Serial number of the device.
MAC Address	Displays the MAC address of the device.
Type	Indicates the model of the device.

Parameter	Description
Licensed?	Indicates if the device is assigned to a license.
Group	Displays the pre-assigned or pre-provisioned group to which the device is assigned. To assign a device to a group, see Assigning Devices to a Group. If the device is already provisioned in Central, the group assignment status is indicated in green.
Location	Displays the location of the device.

Assigning Licenses to Devices

The subscription keys associated with a customer account can have multiple licenses associated with it.

When a license assigned to a device expires, Central checks the inventory for the available subscriptions for the device and verifies if the subscription key has adequate license capacity. If a subscription key with adequate capacity is available, Central automatically assigns the longest available subscription to the device. If the subscription does not have adequate capacity, Central assigns as many devices as possible.

To assign license to a device, complete the following steps:

1. Click **Maintenance > Device Provisioning**. The **Device Provisioning** page opens.
2. Click **Manage Licenses**.
3. Select a device that is marked as unlicensed.
4. Click **Assign License(s)**.
5. To unassign licenses from a device, click **Unassign License**. The license is unassigned and available for assignment to other devices.

Assigning Devices to a Group

When the devices are added to Central, they are automatically provisioned. The devices connected to Central are indicated in green. The group assignment depends on the following conditions:

- If the device is connected to Central, irrespective of the operational status of the device, the **Assign Group** button is not displayed.
- If the device is not connected to Central, the **Assign Group** button is displayed.
- When a user selects devices that are not connected to Central along with another device that is connected to Central, although the **Assign Group** button is displayed, the group assignment operation is carried out only for the device that is not connected to Central.
- When the device is moved from one group to another, the group column in the **Device Management** page shows the new group name.

To assign devices to a group, complete the following steps:

1. Click **Maintenance > Device Provisioning**. The **Device Provisioning** page opens.
2. Click **Pre-provision Groups**.
3. Select the device which you want to assign to a group. To assign all unassigned devices at once, select the unassigned devices from a group.
4. Click **Assign Group**. The **Assign Group** pane is displayed.
5. Select the group to which you want to assign your device by using the scroll bar.
6. Click **Assign**.
7. To assign the device to a new group, complete the following steps:

a. Enter the name of the group in the text box and click **(+)**. The newly created group is displayed in the list of available groups.

b. Select the newly created group and click **Assign**.

User Management

The **User Management** pane provides details of the user such as username, user scope, access level, and allows you to add, edit or delete users.

NOTE

The **User Management** pane also includes the **Support Access** and **Two-factor Authentication (2FA)** options under **Actions**. For more information on two-factor authentication, see Two-Factor Authentication on page 150.

When **Support Access** is set to ON, Aruba support can access your Central account remotely.

Aruba Central User Roles

Central supports three types of users:

- **Administrator**—The Administrator users have full access to all the groups and have special rights to create or update user details, groups, and to provision devices.
- **Read/Write user**—These users have read/write access to the groups/devices assigned by the Administrator user. The Read/Write users can perform operations which can change the behavior of devices or groups such as modifying the configuration of a device, deleting a device and so on.
- **Read Only**—These users have only read access to the groups or devices assigned by the Admin user. The read only access is limited to view the statistics and other details for groups and devices.

NOTE

A user cannot have different access rights for different groups.

Adding a User

To add a new user account, complete the following steps:

1. Click **Maintenance** > **User Management**.
2. On the **User Management** page, click **+**. The **New User** window is displayed.
3. Enter the name of the user in the **Username** text box.
4. Select a group to which you want to assign the user, from the **User Scope** drop-down list.
5. Select a user role from the **Access Level** drop-down list.
6. Click **Save**. An email invite is sent to the user with a registration link. For more information on registering, see Adding User Accounts on page 18.
7. If the user has not received an email invite, click **Actions** > **Resend Invite Email** to resend the invitation.

Two-Factor Authentication

Central now supports two-factor authentication to offer a second layer of security to your login, in addition to password. When two-factor authentication is enabled on a user account, the users can sign in to their Central account either through the mobile app or the web application, only after providing their password and the six-digit verification code displayed on their trusted devices.

When two-factor authentication is enabled at the customer account level, all the users belonging to the customer account are required to complete the authentication procedure when logging in to Central. If a user account is associated with multiple customer accounts and if two-factor authentication is enabled on one of these accounts, the user must complete the two-factor authentication during the login procedure.

If two-factor authentication is enabled on your accounts, you must install the Google Authenticator app on your devices such as mobile phones to access the Central application. When the users attempt to log in to Central with their credentials, the Google Authenticator app provides a six-digit verification code to complete the login procedure.

Installing Google Authenticator App

For two-factor authentication, ensure that the Google Authenticator app is installed on your mobile device.

During the registration process, the Central application shares a secret key with the mobile device of the user over a secure channel when the user logs in to Central. The key is stored in the Google Authenticator app and used for future logins to the application. This prevents unauthorized access to a user account as this authentication procedure involves two-levels for secure transaction.

When you register your mobile device successfully, the Google Authenticator app generates a six-digit token for the second level authentication. The token is generated every thirty seconds.

Enabling Two-factor Authentication for User Accounts

To enable two-factor authentication, complete the following steps:

1. Click **Maintenance** > **User Management**. The **User Management** page opens.
2. From the **Actions** menu, set **Two-Factor Authentication (2FA)** to **ON**. The two-factor authentication is enabled for all the users associated with a customer account.

Two-factor Authentication for Central Web Application

When two-factor authentication is enabled for a customer account, the users associated with that customer account are prompted for two-factor authentication when they log in to Central.

To complete two-factor authentication, perform the following actions:

1. Access the Central website.
2. Log in with your credentials. If two-factor authentication is enforced on your account, the two-factor authentication page opens.
3. Install the Google Authenticator app on your mobile device if not already installed.
4. Click **Next**.
5. If this is your first login since two-factor authentication is enforced on your account, open Google Authenticator on your mobile device.
6. Scan the QR Code. If you are unable to scan the QR code, perform the following actions:
    a. Click the **Problem in Reading QR Code** link. The secret key is displayed.
    b. Enter this secret key in the Google Authenticator app.
    c. Ensure that the **Time-Based** parameter is set. Aruba Central is added to the list of supported clients and a six-digit token is generated.
7. Click **Next**.
8. Enter the six-digit token.
9. Select the **Remember 2FA for 30 Days** check box if you want the authentication to expire only after 30 days.
10. Click **Finish**.

Two-factor Authentication for the Central Mobile App

To log in to Central app on your mobile device, perform the following actions:

1. Open the Central app on your mobile device.

2. Enter your username and password and click **Log in**. If the registration process is pending, an error message is displayed.

NOTE

The registration process for two-factor authentication must be completed only through a web browser on your Desktop. Ensure that this procedure is completed before accessing the Central app on your mobile device if two-factor authentication is enabled on your account.

3. Enter the token.
4. Click **Authenticate**. On successful authentication, the Central app opens.

Registering a New Mobile Device

If you have changed your mobile device, you need to install Google Authenticator app on your new device and register again using a web browser on your Desktop for two-factor authentication.

To register your new mobile device, complete the following steps:

1. Log in to Central web application. The two-factor authentication page is displayed.
2. Click the **Changed Your Mobile Device?** link.
3. To register your new device and receive a reset email with instructions, click **Send 2FA Reset Email**. A reset email with instructions will be sent to your registered email address.
4. Follow the instructions in the email and complete the registration.

Audit Trail

The **Audit Trail** page shows the logs for all the events triggered in Central at the **All Groups** level. To view the details of a particular event, click the details icon under the **Details** column. Audit trail is supported for both IAP and Switches. In the current release, the Audit Trail logs are displayed for the following operations only:

- Device status and configuration
- Firmware upgrade

The **Audit Trail** page displays a table with the following details:

Table 54: *Audit Trail Pane*

Data Pane Content	Description
Time	Indicates the time at which the changes were made.
Username	Indicates the Central user who applied the changes.
IP Address	Indicates the IP address of the client device.
Classification	Indicates the type of modification and the affected module.
Target	Indicates if the changes were applied at the device or the group level.
Details	Provides a short description of the changes such as license assignment, firmware upgrade, and configuration changes.

API Gateway

Central supports an Application Programming Interface (APIs) to allow the administrator users to create and manage APIs. It supports the following types of APIs:

- A polling-based API—The Representational State Transfer (REST)-based APIs support HTTP GET operations by providing a specific URL for each query. The output for these operations are returned in the JSON format.
- Push or Event APIs—The Push API gives web applications the ability to receive messages pushed to them from a server.

The API Gateway feature in Central offers the following benefits:

- Provides an API management gateway to create, publish, mange the life cycle of APIs
- Provides a gateway that can run on public and private cloud as containers
- Displays the API usage pattern
- Provides a developer portal to develop applications using the APIs

The administrators of a web API gateway can create a API gateway cluster to route the API traffic to Aruba cloud services. Central offers the following consoles for API management:

- Administrator Console—The console for managing APIs and consumers.
- Publisher Console—The console for creating and publishing an API.

API Framework Plug-in

The Central API Framework plugin supports OAuth2 authentication and authorization, and provides all API services. To enable API services, you must configure the access token, refresh token, API logging level, and other security settings.

Using OAuth 2.0 to Access API

Central supports the OAuth 2 RFC 6749 specification for accessing a new set of modern APIs. All OAuth2 requests must use the SSL endpoint available at https://<host IP or FQDN>/api/oauth.

OAuth 2.0 is a simple and secure authorization framework. It allows applications to acquire an access token for Central through a variety of work flows supported within the OAuth2 specification. After an application is assigned an access token, it can access the various APIs serviced by Central.

Access and Refresh Tokens

The access token is a string that identifies a user, app, or web page and is used by the app to access an API. The access tokens provide a temporary and secure access to the APIs. The access tokens have a limited lifetime. If the application uses web server or user-agent OAuth authentication flows, a refresh token is provided during authorization that can be used to get a new access token.

Central supports the following methods of obtaining access token:

- Authorization code grant—The authorization code grant type enables the administrators to use third-party applications to access Central APIs without providing password on third-party applications. This method is optimized for confidential clients and is the preferred and the most secure option.
- REST API to download tokens—In this method, the administrator provides username and password to login to portal for initial bootstrapping. The access token can be downloaded after logging in.
- Offline Token Download—In this method, the administrator downloads access token flow from a device and uploads the file manually to client application.

Viewing APIs

To view the APIs managed by Central:

1. Click **Maintenance** > **API Gateway**. The **API Gateway** page shows the list of published APIs.
2. To view the details of an API, click **Details**.
3. To view the API documentation, click **Documentation**. The documentation is displayed in a new window.

Viewing Tokens

To view tokens, complete the following steps:

1. Click **Maintenance** > **API Gateway**. The **API Gateway** page is displayed.
2. Click **Authorized Apps & Tokens**.
3. To view tokens, click **View Tokens**. The Token List pop-up window opens.
4. To download tokens, click **Download Token**.
5. To revoke tokens, click **Revoke Token**.

Troubleshooting Devices

This section includes the following topics:

- Troubleshooting Overview
- Troubleshooting a Device
- Setting a Periodicity for Running Commands

Troubleshooting Overview

The **Troubleshooting** menu in the **Maintenance** tab in the Central UI allows the administrators and the users with read-write access to run the troubleshooting or diagnostics commands directly on the devices. When a troubleshooting session begins, Central establishes a session with the devices selected for the troubleshooting operation, retrieves the output of the selected diagnostics commands, and displays the output in the UI.

Central supports the troubleshooting operations at the device level, group level, and also at the **All Groups** level. If the user access is restricted to only certain groups within a network, Central allows the users to run the troubleshooting commands only on the devices in these groups. Similarly, the users with the administrator or read-write access to **All Groups** can execute the troubleshooting commands on the entire list of devices associated with a user account.

The users can run commands at a given time or set a periodic interval at which the selected commands can be run.

NOTE

You can execute the troubleshooting commands only on the IAPs running the 6.4.3.1-4.2.0.3 or later firmware versions.

Table 55 describes the contents of the **Troubleshooting** page:

Table 55: *Contents Of The Troubleshooting Page*

Data Pane Item	Description
AP Name	Allows you to select one or several devices for troubleshooting. You can also search for a specific device by typing the first few letters of the device name. Central allows you to select up to 10 devices for a troubleshooting operation.
Commands	Category—Allows you to select a category. The troubleshooting commands are segregated under the following categories: ● Wireless ● Security ● Network ● AirGroup ● System ● ARM ● Datapath ● Logs ● AirWave On selecting a category, the commands grouped under that category are displayed. You can select one or several commands to run on the devices.
Run	Executes the troubleshooting commands on the selected devices.
Auto Run	Sets a schedule for running the troubleshooting commands at specific user-defined intervals.
Filter	Sets a filter criteria for the command output. Enter a search text string to filter the command output. For example, if you enter DPI in the Filter text box, only the command output with the DPI text is displayed.
Clear All	Clears all the output.
Export All	Exports the output files generated for each device in a zip file.
Output pane	Shows the output for the commands that are run. The output contains commands with the UTC time stamp and is segregated per device. To view the command output for a specific device, select the IAP from the list of devices in the Output pane.

Troubleshooting a Device

To run troubleshooting commands on a device:

1. Click **Maintenance** > **Troubleshooting**. The **Troubleshooting** page opens.
2. Select a device from the **AP Name** drop-down. If the desired AP is not listed, type the first few letters or digits of the device name. The drop-down list displays a list of APs matching the text string you typed.
3. Select a category and the commands to run under that category. For example, select the **Security** category and then select the **AP Access Rule Table** command.

4. To run commands from a different category, select another category and the commands grouped under that category.

5. Click **Run**. The command output is displayed.

Setting a Periodicity for Running Commands

To set a frequency for automatically running the troubleshooting commands:

1. Select a device from the **AP Name** drop-down. If the desired AP is not listed, type the first few letters or digits of the device name. The drop-down list displays a list of APs matching the text string as you type.
2. Select a category and the commands to run under that category. To run commands from a different category, select another category and the commands grouped under that category.
3. Click **Auto Run**.
4. Specify the interval within a range of 30 seconds to 1 hour.
5. Select the duration for running the troubleshooting commands within a range of 1 minute to 1 hour.
6. Click **Start**.

Chapter 12
Presence Analytics

This section describes the Presence Analytics feature supported by Central.

Presence Analytics Overview

Central supports the **Presence Analytics** application to provide a solution for analyzing user traffic patters in public venues and enterprise environments. Using this feature, various businesses can analyze user traffic and a derive a usage pattern. Based on the analysis, businesses can develop or improve strategies for customer engagement, maximizing revenue opportunities, optimizing workspace, and increasing market presence.

Central provides an analytics dashboard view of the data aggregated from the IAPs. When the Presence Analytics service is enabled on the IAPs deployed in the network, Central receives RSSI feeds on the user traffic presence from the IAPs. The administrators can create labels for venues and assign these labels to the IAP s.

The traffic presence metrics are classified based on the following user traffic patterns:

- Passer By—An associated or unassociated client who is in vicinity of a store and has an RSSI value greater than or equal to -90 dBm.
- Visitor—A client who spends at least one minute in the store. The traffic presence for such a user must be equal to or more than the RSSI threshold value set in the **Presence Anayltics** > **Settings** page. By default, the RSSI threshold value is set to -65 dBm.
- Engaged—A visitor whose dwelling time is more than 5 minutes or the value configured for dwelling time in the **Presence Anayltics** > **Settings** page.

NOTE

If the user is idle for more than 30 minutes, Central removes the user traffic instance. When the user reappears, it creates a new instance for that user and applies the same user traffic classification criteria.

Configuring Stores

Stores refer to the locations or venues in which the user traffic presence is detected. For Presence Analytics, you can create labels for stores and assign these stores to the IAP s. For more information on creating labels, see Labels on page 173.

In the **Presence Analytics** application view, the stores configured in Central are listed under **All Stores**. The user traffic presence analysis applies only if the stores are distributed across different locations.

Configuring IAPs for Presence Analytics

Central supports the Presence Analytics feature for IAP deployments only. This feature is supported only on the IAPs running firmware versions 6.4.4.4-4.2.3.0 or later.

To allow Central to receive RSSI feeds from the IAPs, the RSSI feed parameter must be enabled on the IAP. To enable Presence Analytics on an IAP, complete the following steps:

1. Click **Configuration > Access Points** > **Services**. The **Services** pane is displayed.
2. Click **Presence Analytics**.
3. Select **Report RSSI**.
4. Select any of the following options for client type:

- **Unassociated Clients Only**—Reports RSSI feed from clients that are not associated.
- **Unassociated-and-Associated Clients**—Reports RSSI feed from both associated and unassociated clients

5. Specify an RSSI reporting interval within a range of 5–300 seconds. By default, the interval is set to 60 seconds.

6. Specify an RSSI threshold value. The IAP sends an RSSI feed when the clients exceed the RSSI threshold. Aruba recommends that you set the RSSI threshold value to 100 dBm.

7. Click **Save Settings**.

Using the Presence Analytics App in Central

The **Presence Analytics** app under **Aruba Central Apps** area in the left navigation pane of the Central UI allows you to analyze user traffic presence and configure parameters for user classification.

On clicking **Presence Analytics**, the following menu options are displayed.

- Monitoring—A dashboard that shows the user traffic details.
- Settings—The configuration page on which the RSSI threshold and dwelling time for the users can be set.

Analyzing User Traffic Presence

The Monitoring menu provides the following views:

- Presence
- Insights

Table 56: *Monitoring Dashboard For Presence Anaytics*

Dashboard View	Description
Presence	The **Presence** dashboard provides a view of the user traffic pattern detected for particular venue over the last 3 hours, 1 day, 1 week, or 1 month. By default the user traffic presence data is displayed for the last 3 hours. By default, the presence information is displayed for all venues. To view data for specific venue, select the required label from the **All Stores** setting icon on the header pane. **Time Range** You can view the traffic presence data for the following time ranges: ● 3 Hours—Data from the current time to last 3 hours. This is the default time range for which the data is presented. ● 1 day—Data from the current time to last 1 day. ● 1 week—Data from the 00:00 hour of the current week to 00:00 of last 1 week. ● 1 Month—Data from the 00:00 hour of the current week to 00:00 of last 1 month. **User Traffic Data** The administrator can select a time range and view the following information: ● User classification based on proximity and dwelling time inside a specific location. ● The count and percentage of clients classified as passer-by, visitor, or engaged user. ● The percentage of passer-by clients that are converted to visitors. ● The percentage of visitors that are converted to engaged users. ● Graphs for the passer-by, visitor, and engaged users showing the distance from the venue. ● User traffic and activity trends that display the following information: ● Passer By—The average number of Passer By clients at a given time interval. ● Visitor—The average number of visitors at a given time interval. ● Engaged—The average number of engaged clients at a given time interval. ● Dwell Time—The average time spent by the clients inside a store at a given point in time. The granularity of data point for activity trends is as follows: ● 5 min for a time range of 3 hours ● 1 hour for a time range of 1 day ● 1 day for a time range of 1 week and 1 month ● Passer By to visitor ratio, visitor to engaged ratio, rising and falling trends in these ratios as compared to the last time frame. For example, if the time range is set to 3 hours, the changes in the ratio between the current time and last 3 hours of data is displayed. Similarly, if the time range is set to 1 day or 1 week, the changes between the current day and last 1 day, or the current week and the last 1 week are displayed respectively. ● Graphs and statistics indicating the average of dwelling time spent by the visitor and engaged users inside a store.
Insights	The **Insights** dashboard displays the trends for top 5 and bottom 5 stores for the passer-by, visitor, and engaged users. The **Insights** page also displays a summary of user traffic patterns for all venues. **NOTE:** The **Insights** page displays the trends only if the stores are assigned to an IAP.

Setting RSSI Threshold and Dwelling Time

The RSSI and dwelling time configuration allows the administrators to classify the type of user, analyze traffic patterns, and determine if the usage has increased over a period of time.

By default, the RSSI threshold is set to -65 dBm. If the user traffic exceeds this RSSI threshold and the client spends more than one minute in the store, the client is considered a visitor. Typically, the dwelling time is set to 5 minutes by default. When a client spends more than 5 minutes in a store, the visitor user is classified as an engaged user.

To modify the default RSSI and dwelling time configuration, complete the following steps:

1. On the left navigation pane, click the **App Selector** icon.
2. Click **Presence Anaytics**. The top of the left navigation pane displays the **Presence Analytics** menu options.
3. Click **Settings** and modify the values for **RSSI threshold for passerby-to-visitor** and **Dwell Time for visitor-to-engaged**.
4. Click **Save Settings**.

This chapter describes the following topics:

- Guest Management on page 161
- Creating Apps for Social Login on page 161
- Configuring a Splash Page Profile on page 166
- Configuring Visitor Accounts on page 170

Guest Management

The guest management feature allows guest users to connect to the network and at the same time, allows the administrator to control guest user access to the network.

Central allows administrators to create a splash page profile for guest users. Guest users can access the Internet by providing either the credentials configured by the guest operators or their respective social networking login credentials. For example, you can create a splash page that displays a corporate logo, color scheme and the terms of service, and enable logging in from a social networking service such as Facebook, Google +, Twitter, and LinkedIn.

Businesses can also pair their network with the Facebook Wi-Fi service, so that the users logging into Wi-Fi hotspots are presented with a business page, before gaining access to the network.

To enable logging using Facebook, Google+, Twitter, and LinkedIn credentials, ensure that you create an application (app) on the social networking service provider site and enable authentication for that app. The social networking service provider will then issue a client ID and client secret key that are required for configuring guest profiles based on social logins.

Guest operators can also create guest user accounts. For example, a network administrator can create a guest operator account for a receptionist. The receptionist creates user accounts for guests who require temporary access to the wireless network. Guest operators can create and set an expiration time for user accounts. For example, the expiration time can be set to 1 day.

Creating Apps for Social Login

The following topics describe the procedures for creating applications to enable the social login feature:

- Creating a Facebook App on page 161
- Creating a Google App on page 162
- Creating a Twitter App on page 164
- Creating a LinkedIn App on page 165

Creating a Facebook App

Before creating a Facebook App, ensure that you have a valid Facebook account and you are registered as a Facebook developer with that account.

To create a Facebook app, complete the following steps:

1. Visit the Facebook app setup URL at https://developers.facebook.com/apps.
2. From **My Apps**, select **Add a New App**.

3. Select **Website** as the type of app. If you have already created any apps, the list of apps is displayed.

4. To create a new app, click **Skip and Create App ID**.

5. In the subsequent pane, enter a name for the application. For example, SampleNetworks.

6. Click **Create New Facebook App ID**.

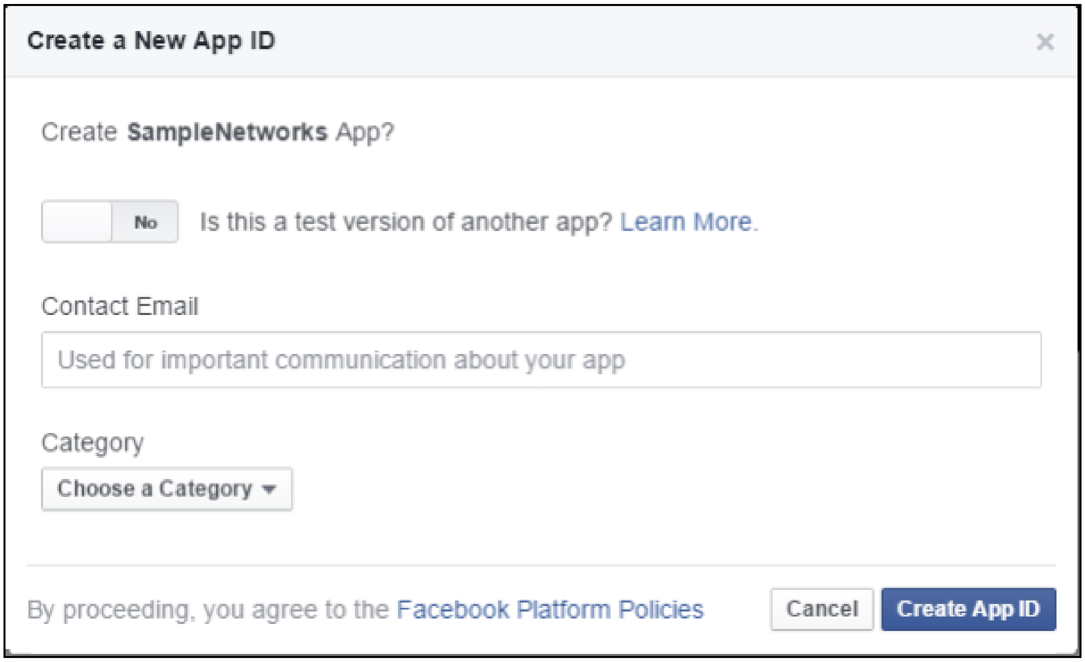
7. On the **Create a new App ID** pop-up pane:

   a. Select **No** for **Is this a test version of another app?**.

   b. Enter the contact email address.

   c. Select **Business** from the **Category** drop-down list.

Figure 13 *App ID Creation*



Create a New App ID

Create **SampleNetworks** App?

No | Is this a test version of another app? Learn More.

Contact Email

Used for important communication about your app

Category

Choose a Category

By proceeding, you agree to the Facebook Platform Policies

   d. Click **Create App ID**. The **Security Check** page is displayed.

8. Complete the security check and click **Submit**. The **Setup SDK** page is displayed.

9. Scroll down to the **Tell Us about Your Website** section and enter the URL of your main site as shown in the following figure. For example, www.arubanetworks.com.

10. Click **Next**.

11. In the subsequent screen, click **Skip to Developer Dashboard** under **Next Steps**. The **App Dashboard** is displayed.

12. Click **Add Product**, and then click **Facebook Login** > **Get Started**.

13. On the **Getting Started** page, enter a valid Oauth redirect URL and append /oauth/reply at the end of the URL and click **Save Changes**.

14. Click **app review** under Getting Started.

15. To make the app public, select **Yes** under **Make <app name> public**?

16. On the left pane, click the **Settings** icon. Note the app ID and app secret key. The app ID and secret key are required for configuring Facebook login in the Central UI.

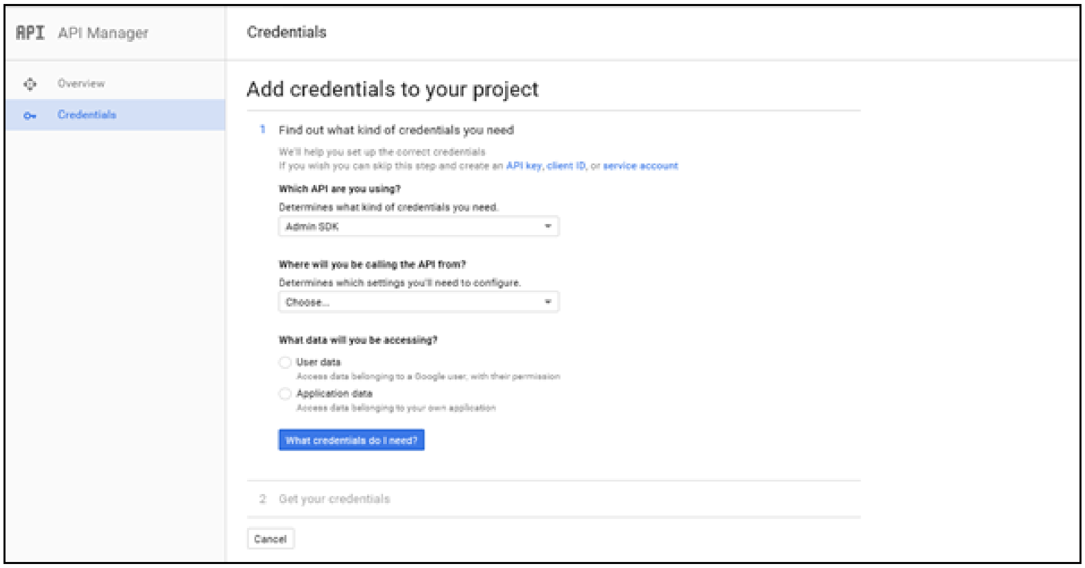
Creating a Google App

Before creating a Google app for Google+ based login, ensure that you have a valid Google+ account.

To create a Google+ app, complete the following steps:

1. Access the Google Developer site at https://code.google.com/apis/console.
2. Create a project if not already created.
3. Click the **Google API** settings icon > **API Manager**. The **Google API** window opens.
4. Under **Google Apps APIs**, click **Admin SDK**. The Admin SDK overview screen opens.
5. Click **Enable**.
6. Click **Go to Credentials**. The following page opens.

Figure 14 *Google+ Admin SDK Credentials*



Add credentials to your project

1 Find out what kind of credentials you need

We'll help you set up the correct credentials
If you wish you can skip this step and create an API key, client ID, or service account

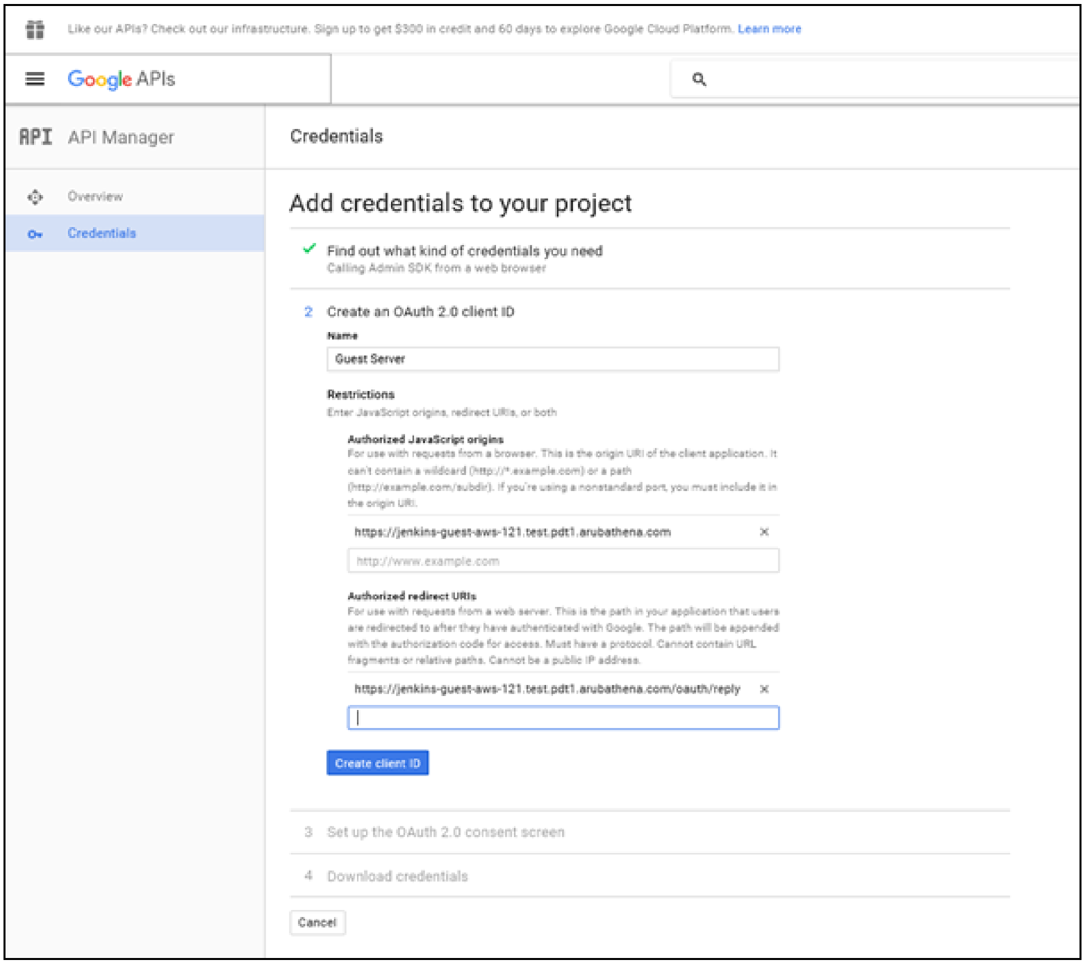
Which API are you using?
Determines what kind of credentials you need.
Admin SDK

Where will you be calling the API from?
Determines which settings you'll need to configure.
Choose...

What data will you be accessing?
○ User data
Access data belonging to a Google user, with their permission
○ Application data
Access data belonging to your own application

7. Under the **Where will you be calling the API from** section, select **Web Browser**.
8. Under the **What data you will be accessing** section, select **User Data**.
9. Click **What Credentials do I need**. The following page opens.

Figure 15 *OAuth URLs*



Like our APIs? Check out our infrastructure. Sign up to get $300 in credit and 60 days to explore Google Cloud Platform. Learn more

Google APIs

API Manager

Overview

Credentials

Credentials

Add credentials to your project

✓ Find out what kind of credentials you need
Calling Admin SDK from a web browser

2 Create an OAuth 2.0 client ID

Name: Guest Server

Restrictions
Enter JavaScript origins, redirect URIs, or both

Authorized JavaScript origins
For use with requests from a browser. This is the origin URI of the client application. It can't contain a wildcard (http://*.example.com) or a path (http://example.com/subdir). If you're using a nonstandard port, you must include it in the origin URI.

https://jenkins-guest-aws-121.test.pdt1.arubathena.com ×

http://www.example.com

Authorized redirect URIs
For use with requests from a web server. This is the path in your application that users are redirected to after they have authenticated with Google. The path will be appended with the authorization code for access. Must have a protocol. Cannot contain URL fragments or relative paths. Cannot be a public IP address.

https://jenkins-guest-aws-121.test.pdt1.arubathena.com/oauth/reply ×

Create client ID

3 Set up the OAuth 2.0 consent screen

4 Download credentials

Cancel

10. Enter the **OAuth 2.0 Client ID Name**.

11. Under **Authorized JavaScript Origins**, enter the base URL with FQDN of the cloud guest instance that will be hosting the captive portal. For example, https://%hostname%/.

12. Under **Authorized Redirect URIs**, enter the cloud server OAuth reply URL that includes the FQDN of the cloud server instance with /oauth/reply appended at the end of the URL.

NOTE

Ensure that the URL is an HTTPS URL with a domain name and not the IP address. For example, https://example1.cloudguest.examplenetworks.com/oauth/reply.

13. Click **Create Client ID**.

14. Under **Set up the OAuth 2.0 consent screen**, provide your **Email Address** and product name, and then click **Continue**. The client ID is displayed.

15. Click **Done**. A page showing the OAuth IDs opens.

16. Click the **Oauth ID** to view the client ID and client secret key. The client ID and client secret key are required for configuring Google+ login in the Central UI.

Creating a Twitter App

Before creating a Twitter app, ensure that you have a valid Twitter account.

To create a Twitter app, complete the following steps:

1. Visit the Twitter app setup URL at https://apps.twitter.com.

2. Click **Create New App**. The **Create an application** web page is displayed.

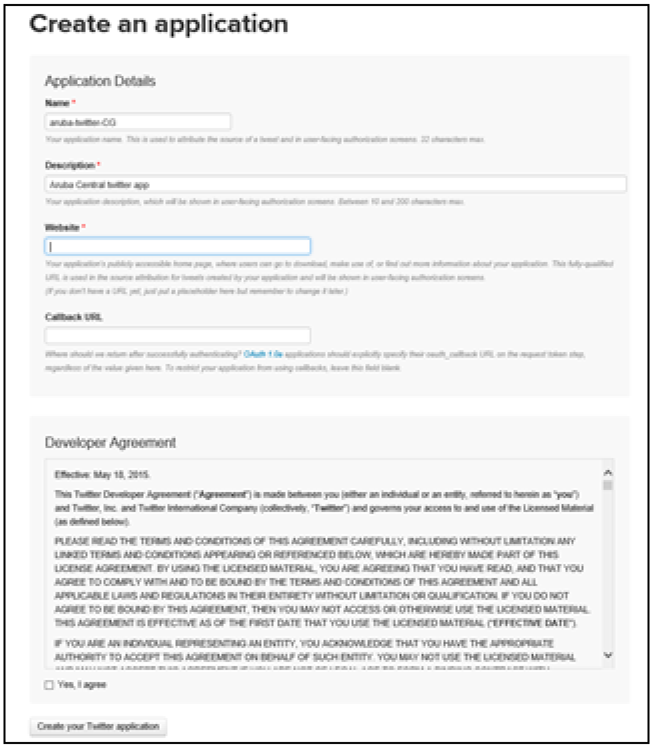
3. Enter the application name and description.

4. For OAuth 2.0 Redirect URLs, enter the HTTPS URL of the cloud guest server to which you want to connect this social authentication source, and append /oauth/reply at the end of the URL.

NOTE

Ensure that the URL is an HTTPS URL with a domain name and not the IP address. For example, https://exa.example.com/oauth/reply.

Figure 16 *Twitter App Creation*



Create an application

Application Details

Name *

aruba-twitter-CG

Your application name. This is used to attribute the source of a tweet and in user-facing authorization screens. 32 characters max.

Description *

Aruba Central twitter app

Your application description, which will be shown in user-facing authorization screens. Between 10 and 200 characters max.

Website *

Your application's publicly accessible home page, where users can go to download, make use of, or find out more information about your application. This fully-qualified URL is used in the source attribution for tweets created by your application and will be shown in user-facing authorization screens.
(If you don't have a URL yet, just put a placeholder here but remember to change it later.)

Callback URL

Where should we return after successfully authenticating? OAuth 1.0a applications should explicitly specify their oauth_callback URL on the request token step, regardless of the value given here. To restrict your application from using callbacks, leave this field blank.

Developer Agreement

Effective: May 18, 2015.

This Twitter Developer Agreement ("Agreement") is made between you (either an individual or an entity, referred to herein as "you") and Twitter, Inc. and Twitter International Company (collectively, "Twitter") and governs your access to and use of the Licensed Material (as defined below).

PLEASE READ THE TERMS AND CONDITIONS OF THIS AGREEMENT CAREFULLY, INCLUDING WITHOUT LIMITATION ANY LINKED TERMS AND CONDITIONS APPEARING OR REFERENCED BELOW, WHICH ARE HEREBY MADE PART OF THIS LICENSE AGREEMENT. BY USING THE LICENSED MATERIAL, YOU ARE AGREEING THAT YOU HAVE READ, AND THAT YOU AGREE TO COMPLY WITH AND TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT AND ALL APPLICABLE LAWS AND REGULATIONS IN THEIR ENTIRETY WITHOUT LIMITATION OR QUALIFICATION. IF YOU DO NOT AGREE TO BE BOUND BY THIS AGREEMENT, THEN YOU MAY NOT ACCESS OR OTHERWISE USE THE LICENSED MATERIAL. THIS AGREEMENT IS EFFECTIVE AS OF THE FIRST DATE THAT YOU USE THE LICENSED MATERIAL ("EFFECTIVE DATE").

IF YOU ARE AN INDIVIDUAL REPRESENTING AN ENTITY, YOU ACKNOWLEDGE THAT YOU HAVE THE APPROPRIATE AUTHORITY TO ACCEPT THIS AGREEMENT ON BEHALF OF SUCH ENTITY. YOU MAY NOT USE THE LICENSED MATERIAL

☐ Yes, I agree

5. Select **Yes, I agree** to accept the Developer Agreement terms.

6. Click **Create a Twitter application**.

7. Click **Manage Keys and Access Tokens**. The **Keys and Access Tokens** tab opens. The consumer key (API key) and consumer secret (API key) are displayed.

8. Note the ID and the secret key. The API key and API secret key are required for configuring Twitter login in Central UI.

Creating a LinkedIn App

Before creating a LinkedIn app, ensure that you have a valid LinkedIn account.

To create a LinkedIn app, complete the following steps:

1. Visit the LinkedIn app setup URL at https://developer.linkedin.com.

2. Click **My Apps**. You will be redirected to https://www.linkedin.com/secure/developer/apps.

3. Click **Create Application**. The **Create a New Application** web page is displayed.

4. Enter your company name, application name, description, website URL, application logo with the specification mentioned, application use, and contact information.

5. Click **Submit**. The **Authentication** page is displayed.

6. Note the client ID and client secret key displayed on the **Authentication** page.

7. For **OAuth 2.0 Redirect URLs**, enter the HTTPS URL of the cloud guest server to which you want to connect this social authentication source and append /oauth/reply at the end of the URL.
8. Click **Add** and then click **Update**. The API and secret keys are displayed.
9. Note the API and secret key details. The API ID and secret key are required for configuring LinkedIn login in the Central UI.

Configuring a Splash Page Profile

This topic describes the following procedures:

- Adding a Splash Page Profile on page 166
- Customizing a Splash Page Design on page 169
- Associating a Splash Page Profile to an SSID on page 170

Adding a Splash Page Profile

To create a splash page profile:

1. Click **Guest Access** on the bottom left pane. The guest access configuration and management menu options are displayed.
2. Click **Splash Page**. The **Splash Page** pane is displayed.
3. To create a new Splash page, Click the + icon. The **New Splash Page** pane is displayed.
4. On the **Configuration** tab, configure the parameters described in the following table:

Table 57: *Splash Page Configuration*

Data Pane Content	Description
Name	Enter a unique name to identify the splash profile.
Type	Configure any of the following authentication methods to provide a secure network access to the guest users and visitors. ● **Anonymous** ● **Authenticated** ● **Facebook Wi-Fi**
Anonymous	Configure the **Anonymous** login method if you want to allow guest users to log in to the Splash page without providing any credentials.
Authenticated	Configure authentication and authorization attributes, and login credentials that enable users to access the Internet as guests. You can configure an authentication method based on sponsored access and social networking login profiles. The authenticated options available for configuring the cloud guest splash page are described in the following rows.

Table 57: *Splash Page Configuration*

Data Pane Content	Description
Username/Password	The **Username/Password** based authentication method allows pre-configured visitors to obtain access to wireless connection and the Internet. The visitors or guest users can register themselves by using the splash page when trying to access the network. The password is delivered to the users through print, SMS or email depending on the options selected during registration. To allow the guest users to register by themselves: 1. Enable **Self-Registration**. 2. Set the **Verification Required** to **ON** if the guest user account must be verified. 3. Specify a verification criteria to allow the self-registered users to verify through email or phone. ● If email-based verification is enabled and the **Send Verification Link** is selected, a verification link is sent to the email address of the user. The guest users can click the link to obtain access to the Internet. ● If phone-based verification is enabled, the guest users will receive an SMS. The administrators can also customize the content of the SMS by clicking on **Customize SMS**. 4. Specify the duration within the range of 1-60 minutes, during which the users can access free Wi-Fi to verify the link. The users can log in to the network for the specified duration and click the verification link to obtain access to the Internet. By default, the expiration date for the accounts of self-registered guest users is set to infinite during registration. The administrator or the guest operator can set the expiration date after registration.
Social Login	**Social Login**—Enable this option to allow guest users to use their existing login credentials from social networking profiles such as Facebook, Twitter, Google+, or LinkedIn and sign into a third-party website. When a social login based profile is configured, a new login account to access the guest network or third-party websites is not required. ● **Facebook**— Allows guest users to use their Facebook credentials to log in to the splash page. To enable Facebook integration, you must create a Facebook app and obtain the app ID and secret key. For more information on app creation, see Creating a Facebook App. Enter the app ID and secret key for client ID and client Secret respectively to complete the integration. ● **Twitter**—Allows guest users to use their Twitter credentials to log in to the splash page. To enable Twitter integration, you must create a Twitter app and obtain the app ID and secret key. For more information, see Creating a Twitter App. Enter the app ID and secret key for client ID and client secret respectively to complete the integration. ● **Google+**—Allows guest users to use their Google+ credentials to log in to the splash page. To enable Google+ integration, you must create a Google app and obtain the app ID and secret key. For more information, see Creating a Google App on page 162. 1. Enter the app ID and secret key for client ID and client secret respectively. 2. To restrict authentication attempts to only the members of a Google hosted domain, enter the domain name in the **Gmail for Work Domain** text box. Ensure that you have a valid domain account licensed by Google Domains or Google Apps. For more information see: ● https://apps.google.com/intx/en_in/ ● https://domains.google.com/about/ 3. Specify a text for the Sign-In button.

Table 57: *Splash Page Configuration*

Data Pane Content	Description
	- **LinkedIn**—Allows guest user to use their LinkedIn credentials to log in to the splash page. To enable LinkedIn integration, you must create a LinkedIn app and obtain the app ID and secret key. For more information, see Creating a LinkedIn App. Enter the app ID and secret key for client ID and client secret respectively to complete the integration.
Facebook Wi-Fi	Select the **Facebook Wi-Fi** option if you want to enable network access through the free Wi-Fi service offered by Facebook. Click **Configure** to pair your network with a Facebook business page and allow guest users to log in from Wi-Fi hotspots using their Facebook credentials. Guest users can provide their location on Facebook to connect to free Wi-Fi, either by manually adding their location or by selecting a setting that automatically adds their location whenever they visit. When this option is enabled, the Wi-Fi users are presented with a specific Facebook page to access the Internet. For more information on Facebook Wi-Fi service, see **Setting up Facebook Wi-Fi for Your Business** at https://www.facebook.com/help/126760650808045.
Authentication Success Behavior	If **Anonymous** or **Authenticated** option is selected as the guest user authentication method, specify a method for redirecting the users after a successful authentication. Select one of the following options: - **Redirect to Original URL**— When selected, upon successful authentication, the user is redirected to the URL that was originally requested. - **Redirect URL**—Specify a redirect URL if you want to override the original request of users and redirect them to another URL.
Authentication Failure Message	If the **Authenticated** option is selected as the guest user authentication method, enter the authentication failure message text string returned by the server when the user authentication fails.
Session Timeout	Enter the maximum time in Day(s): Hour(s): Minute(s) format for which a client session remains active. The default value is 0:8:00. When the session expires, the users must re-authenticate. If MAC caching is enabled, the users are allowed or denied access based on the MAC address of the connective device.
Share This Profile	Select this check box if you want to allow the users to share the Splash Page profile. The Splash Page profiles under All Groups can be shared across all the groups.
Simultaneous Login Limit	To set limit for the simultaneous logins from the same user for authenticated Splash Page profiles, select a value from the **Simultaneous Login Limit** drop-down list.
Daily Usage Limit	To configure the connection time or data usage limit per day for the guest users, specify the following parameters: - By Time—Specify the number of hours, minutes and the timezone. - By Data—Specify the data usage limit.

4. Click **Next**. The **Customization** pane appears. Customizing a Splash Page Design on page 169.

NOTE

You can edit or delete a splash page profile by clicking the respective icons in the **Splash Page Profile** pane.

Customizing a Splash Page Design

To customize a splash page design, on the **Guest Access > Splash Page > New Splash Page > Customization** pane, configure the parameters described in the following table:

Table 58: *Splash Page Customization*

Data Pane Content	Description
Theme	Select a template from list. The theme template determines the look and feel of the splash page.
Background Color	To change the color of the splash page, select the required color from the **Background Color** palette.
Primary Color	Select the primary color of the splash page.
Font Color	Select the font color of the splash page.
Logo	To upload a logo, click **Browse**, and browse the image file.
Background Image	Click **Browse** to upload a background image.
Welcome Text	Enter the welcome text to be displayed on the splash page.
Terms & Conditions	Enter the terms and conditions to be displayed on the splash page. Specify an acceptance criteria for terms and condition by selecting any of the following options from the **Display "I Accept" Checkbox**: ● **No, Accept by default** ● **Yes, Display Checkbox** If the **I ACCEPT** check box must be displayed on the Splash page, select the display format for terms and conditions.

5. Click **Preview** to preview the customized splash page or click **Finish**.

Previewing and Modifying a Splash Page

To preview a splash page profile:

1. Select **Guest Access > Splash Page**. A list of Splash Page profiles is displayed.
2. Click the preview icon next to profile you want to preview. The Splash Page is displayed in a new window. To preview the Splash Page, ensure that the pop-up blocker is disabled.

To modify a splash page profile, click the edit icon next to the profile form list of profiles displayed in the Splash Page Profiles pane.

To delete a profile, select the profile and click the delete icon next to the profile.

Associating a Splash Page Profile to an SSID

To associate a splash page profile with an SSID:

1. Select **Configuration > Access Points > Networks** and then click **Create New**. The **Create a New Network** pane is displayed.
2. For **Type**, select **Wireless**.
3. Enter a name that is used to identify the network in the **Name(SSID)** box.
4. For **Primary Usage**, select **Guest** and click **Next**.
5. In the **VLANs** tab, if required, configure a VLAN assignment mode, and then click **Next**.
6. In the **Security** tab:
   1. Select **Cloud Guest** from the **Splash Page Type** list.
   2. Select the splash page profile name from the **Guest Captive Portal Profile** list and click **Next**.
   3. To enable encryption, set **Encryption** to **Enabled** and configure encryption parameters.
   4. To exclude uplink, select an uplink from **Disable If Uplink Type Is**.
   5. Click **Next**.
7. In the **Access** tab, if required, modify and create access rules set the configuration if required, and then click **Finish**.

Configuring Visitor Accounts

The **Visitors** pane displays information on the session and account details of the visitors who access the splash page.

Adding a visitor

To add a new visitor:

1. Select **Guest Access > Visitors** and then click **Add Visitor**. The **Add Visitor** pane is displayed.
2. Configure the parameters described in the following table:

Table 59: *Adding Visitors*

Data Pane Content	Description
Name	Enter a unique name to identify the visitor.
Company	Enter the company name of the visitor.
Email	Enter the email ID of the visitor.
Phone	Enter the phone number of the visitor.

Data Pane Content	Description
Password	Click **Generate**. The automatically generated password is displayed in the **PASSWORD** text box. Select **Send Access Code** to send the access code by email or SMS.
Valid Till	Specify the duration for the visitor account to expire in Day(S): Hour(s): Minute(s) format. To allow users to access the network for unlimited period of time, select **Unlimited**.
Enable	Select this checkbox to activate the user account.

3. Click **Save**.
4. Click **Save and Print** to print the details of the visitor.

NOTE

You can export the details of the visitor to an excel sheet by clicking **Export All**.

The following table displays the session details of the visitor:

Table 60: *Visitors Session Pane*

Parameter	Description
Visitors	Displays the name of the visitor.
Login Type	Displays the login type of the client (**Anonymous**, **Username/Password**, **Self-Registration**, **Facebook Wi-Fi**).
Browser	Displays the type of browser that the client is connected.
MAC Address	Displays the MAC address of the connected client device.
Device Type	Displays the type of the device.
OS Name	Displays the OS on the client device.
Login Time	Displays the login time of the client.
Session Time (Secs)	Displays the duration for which the client is connected.

The following table displays the account details of a visitor:

Table 61: *Visitor Accounts Pane*

Parameter	Description
Name	Displays the name of the visitor.
Email	Displays the email ID of the visitor.
Company	Displays the company name of the visitor.
Status	Indicates if the user account is in active or inactive state.
Created	Displays the date and time on which the visitor account is created.
Expired	Displays the date and time on which the visitor account expired.
Actions	Allows you to edit or a delete a specific visitor account.

Chapter 14
Labels

Labels are tags that can be used for filtering devices in the **Monitoring** dashboard. You can assign multiple labels to a device. For example, an AP can be labeled as Building 25 and Lobby. These labels can be used to tag the device to a location, or to specific owners or departments.

NOTE

The devices can also be classified using **Groups**. The group classification can be used for role-based access to a device, while labels can be used for tagging a device to a location or region. However, if a device is already assigned to a group and has a label associated with it, it is classified using both group and labels.

Label Classification

Labels are classified into the following categories:

- Default—A default label can be assigned to up to five devices.
- Stores—Each store can have multiple IAPs assigned to it. However, one IAP be assigned to only one store at any point in time. The **Store** label category is used only for the Presence Analytics application. For more information, see Presence Analytics on page 157.

Label Management

This section describes the following procedures:

- Creating a Label on page 173
- Editing or Deleting a Label on page 173
- Assigning a Device to a Label on page 174
- Detaching a Device from a Label on page 174

Creating a Label

To create a label, complete the following steps:

1. In the **Aruba Central Apps** selector area, click **General**. The **Label Management** page is displayed.
2. To add a new label, click the + icon. The **Create New Label** pop-up opens.
3. Select any of the following label categories:
   a. To create a default label, select **Default**.
   b. To create a store, select **Store**.
4. Enter a name for the label.
5. Click **Create**. The new label is added to the **All Labels** table.

Editing or Deleting a Label

To edit or delete a label, complete the following steps:

1. In the **Aruba Central Apps** selector area, click **General**. The **Label Management** page is displayed.
2. Select the label to edit or delete.
3. To edit the label, click the edit icon in the **Actions** column. Edit the label and click **Update**.
4. To delete the label, click the delete icon in the **Actions** column. To view the devices attached to the label before deleting, click **View Devices**. Click **Delete** to remove the label.

Assigning a Device to a Label

To assign a label to a device, complete the following steps:

1. In the **Aruba Central Apps** selector area, click **General**.
2. Click **Assignment**. The **Label Assignment** page is displayed.
3. To assign a label to an IAP, select the IAP and click **Edit**.
4. To assign a label to a switch:
   a. Click the **Switches** tab.
   b. Select a switch and click the edit icon.
5. On the **Label Assignment** pop-up window, select the label and click **Accept Changes**.

Detaching a Device from a Label

To remove a label assigned to a device, complete the following steps:

1. Click **Label Management** > **Assignment**. The **Label Assignment** page is displayed.
2. Select the device and click the edit icon.
3. In the **Label Assignment** pop-up window, delete the label under **Assigned Labels**.
4. Click **Accept Changes**.

Appendix A

Acronyms and Abbreviations

The following table lists the acronyms and abbreviations used in Aruba documents.

Table 62: *List Of Acronyms And Abbreviations*

Acronym or Abbreviation	Definition
3G	Third Generation of Wireless Mobile Telecommunications Technology
4G	Fourth Generation of Wireless Mobile Telecommunications Technology
AAA	Authentication, Authorization, Accounting
ABR	Area Border Router
AC	Access Category
ACC	Advanced Cellular Coexistence
ACE	Access Control Entry
ACI	Adjacent Channel interference
ACL	Access Control List
AD	Active Directory
ADO	Active X Data Objects
ADP	Aruba Discovery Protocol
AES	Advanced Encryption Standard
AIFSN	Arbitrary Inter-frame Space Number
ALE	Analytics and Location Engine
ALG	Application Level Gateway
AM	Air Monitor
AMON	Advanced Monitoring

Table 62: *List Of Acronyms And Abbreviations*

Acronym or Abbreviation	Definition
AMP	AirWave Management Platform
A-MPDU	Aggregate MAC Protocol Data Unit
A-MSDU	Aggregate MAC Service Data Unit
ANQP	Access Network Query Protocol
ANSI	American National Standards Institute
AP	Access Point
API	Application Programming Interface
ARM	Adaptive Radio Management
ARP	Address Resolution Protocol
AVF	AntiVirus Firewall
BCMC	Broadcast-Multicast
BGP	Border Gateway protocol
BLE	Bluetooth Low Energy
BMC	Beacon Management Console
BPDU	Bridge Protocol Data Unit
BRAS	Broadband Remote Access Server
BRE	Basic Regular Expression
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
BYOD	Bring Your Own Device
CA	Certification Authority
CAC	Call Admission Control

Table 62: *List Of Acronyms And Abbreviations*

Acronym or Abbreviation	Definition
CALEA	Communications Assistance for Law Enforcement Act
CAP	Campus AP
CCA	Clear Channel Assessment
CDP	Cisco Discovery Protocol
CDR	Call Detail Records
CEF	Common Event Format
CGI	Common Gateway Interface
CHAP	Challenge Handshake Authentication Protocol
CIDR	Classless Inter-Domain Routing
CLI	Command-Line Interface
CN	Common Name
CoA	Change of Authorization
CoS	Class of Service
CPE	Customer Premises Equipment
CPsec	Control Plane Security
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CRL	Certificate Revocation List
CSA	Channel Switch Announcement
CSMA/CA	Carrier Sense Multiple Access / Collision Avoidance
CSR	Certificate Signing Request
CSV	Comma Separated Values

Table 62: *List Of Acronyms And Abbreviations*

Acronym or Abbreviation	Definition
CTS	Clear to Send
CW	Contention Window
DAS	Distributed Antenna System
dB	Decibel
dBm	Decibel Milliwatt
DCB	Data Center Bridging
DCE	Data Communication Equipment
DCF	Distributed Coordination Function
DDMO	Distributed Dynamic Multicast Optimization
DES	Data Encryption Standard
DFS	Dynamic Frequency Selection
DFT	Discreet Fourier Transform
DHCP	Dynamic Host Configuration Protocol
DLNA	Digital Living Network Alliance
DMO	Dynamic Multicast optimization
DN	Distinguished Name
DNS	Domain Name System
DOCSIS	Data over Cable Service Interface Specification
DoS	Denial of Service
DPD	Dead Peer Detection
DPI	Deep Packet Inspection
DR	Designated Router

Table 62: *List Of Acronyms And Abbreviations*

Acronym or Abbreviation	Definition
DRT	Downloadable Regulatory Table
DS	Differentiated Services
DSCP	Differentiated Services Code Point
DSSS	Direct Sequence Spread Spectrum
DST	Daylight Saving Time
DTE	Data Terminal Equipment
DTIM	Delivery Traffic Indication Message
DTLS	Datagram Transport Layer Security
DU	Data Unit
EAP	Extensible Authentication Protocol
EAP-FAST	EAP-Flexible Authentication Secure Tunnel
EAP-GTC	EAP-Generic Token Card
EAP-MD5	EAP-Method Digest 5
EAP-MSCHAP EAP-MSCHAPv2	EAP-Microsoft Challenge Handshake Authentication Protocol
EAPoL	EAP over LAN
EAPoUDP	EAP over UDP
EAP-PEAP	EAP-Protected EAP
EAP-PWD	EAP-Password
EAP-TLS	EAP-Transport Layer Security
EAP-TTLS	EAP-Tunneled Transport Layer Security
ECC	Elliptical Curve Cryptography

Table 62: *List Of Acronyms And Abbreviations*

Acronym or Abbreviation	Definition
ECDSA	Elliptic Curve Digital Signature Algorithm
EIGRP	Enhanced Interior Gateway Routing Protocol
EIRP	Effective Isotropic Radiated Power
EMM	Enterprise Mobility Management
ESI	External Services Interface
ESS	Extended Service Set
ESSID	Extended Service Set Identifier
EULA	End User License Agreement
FCC	Federal Communications Commission
FFT	Fast Fourier Transform
FHSS	Frequency Hopping Spread Spectrum
FIB	Forwarding Information Base
FIPS	Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
FQLN	Fully Qualified Location Name
FRER	Frame Receive Error Rate
FRR	Frame Retry Rate
FSPL	Free Space Path Loss
FTP	File Transfer Protocol
GBps	Gigabytes per second
Gbps	Gigabits per second
GHz	Gigahertz

Table 62: *List Of Acronyms And Abbreviations*

Acronym or Abbreviation	Definition
GIS	Generic Interface Specification
GMT	Greenwich Mean Time
GPP	Guest Provisioning Page
GPS	Global Positioning System
GRE	Generic Routing Encapsulation
GUI	Graphical User Interface
GVRP	GARP or Generic VLAN Registration Protocol
H2QP	Hotspot 2.0 Query Protocol
HA	High Availability
HMD	High Mobility Device
HSPA	High-Speed Packet Access
HT	High Throughput
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAS	Internet Authentication Service
ICMP	Internet Control Message Protocol
IdP	Identity Provider
IDS	Intrusion Detection System
IE	Information Element
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol

Table 62: *List Of Acronyms And Abbreviations*

Acronym or Abbreviation	Definition
IGRP	Interior Gateway Routing Protocol
IKE PSK	Internet Key Exchange Pre-shared Key
IoT	Internet of Things
IP	Internet Protocol
IPM	Intelligent Power Monitoring
IPS	Intrusion Prevention System
IPsec	IP Security
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet Service Provider
JSON	JavaScript Object Notation
KBps	Kilobytes per second
Kbps	Kilobits per second
L2TP	Layer-2 Tunneling Protocol
LACP	Link Aggregation Control Protocol
LAG	Link Aggregation Group
LAN	Local Area Network
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LDPC	Low-Density Parity-Check
LEA	Law Enforcement Agency
LEAP	Lightweight Extensible Authentication Protocol
LED	Light Emitting Diode

Table 62: *List Of Acronyms And Abbreviations*

Acronym or Abbreviation	Definition
LEEF	Long Event Extended Format
LI	Lawful Interception
LLDP	Link Layer Discovery Protocol
LLDP-MED	LLDP–Media Endpoint Discovery
LMS	Local Management Switch
LNS	L2TP Network Server
LTE	Long Term Evolution
MAB	MAC Authentication Bypass
MAC	Media Access Control
MAM	Mobile Application Management
MBps	Megabytes per second
Mbps	Megabits per second
MCS	Modulation and Coding Scheme
MD5	Message Digest 5
MDM	Mobile Device Management
mDNS	Multicast Domain Name System
MFA	Multi-factor Authentication
MHz	Megahertz
MIB	Management Information Base
MIMO	Multiple-Input Multiple-Output
MLD	Multicast Listener Discovery
MPDU	MAC Protocol Data Unit

Table 62: *List Of Acronyms And Abbreviations*

Acronym or Abbreviation	Definition
MPLS	Multiprotocol Label Switching
MPPE	Microsoft Point-to-Point Encryption
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
MSS	Maximum Segment Size
MSSID	Mesh Service Set Identifier
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transmission Unit
MU-MIMO	Multi-User Multiple-Input Multiple-Output
MVRP	Multiple VLAN Registration Protocol
NAC	Network Access Control
NAD	Network Access Device
NAK	Negative Acknowledgment Code
NAP	Network Access Protection
NAS	Network Access Server Network-attached Storage
NAT	Network Address Translation
NetBIOS	Network Basic Input/Output System
NIC	Network Interface Card
Nmap	Network Mapper
NMI	Non-Maskable Interrupt
NMS	Network Management Server
NOE	New Office Environment

Table 62: *List Of Acronyms And Abbreviations*

Acronym or Abbreviation	Definition
NTP	Network Time Protocol
OAuth	Open Authentication
OCSP	Online Certificate Status Protocol
OFA	OpenFlow Agent
OFDM	Orthogonal Frequency Division Multiplexing
OID	Object Identifier
OKC	Opportunistic Key Caching
OS	Operating System
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
OVA	Open Virtual Appliance
OVF	Open Virtualization Format
PAC	Protected Access Credential
PAP	Password Authentication Protocol
PAPI	Proprietary Access Protocol Interface
PCI	Peripheral Component Interconnect
PDU	Power Distribution Unit
PEAP	Protected Extensible Authentication Protocol
PEAP-GTC	Protected Extensible Authentication Protocol-Generic Token Card
PEF	Policy Enforcement Firewall
PFS	Perfect Forward Secrecy
PHB	Per-hop behavior

Table 62: *List Of Acronyms And Abbreviations*

Acronym or Abbreviation	Definition
PIM	Protocol-Independent Multicast
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PMK	Pairwise Master Key
PoE	Power over Ethernet
POST	Power On Self Test
PPP	Point-to-Point Protocol
PPPoE	PPP over Ethernet
PPTP	PPP Tunneling Protocol
PRNG	Pseudo-Random Number Generator
PSK	Pre-Shared Key
PSU	Power Supply Unit
PVST	Per VLAN Spanning Tree
QoS	Quality of Service
RA	Router Advertisement
RADAR	Radio Detection and Ranging
RADIUS	Remote Authentication Dial-In User Service
RAM	Random Access Memory
RAP	Remote AP
RAPIDS	Rogue Access Point and Intrusuin Detection System

Table 62: *List Of Acronyms And Abbreviations*

Acronym or Abbreviation	Definition
RARP	Reverse ARP
REGEX	Regular Expression
REST	Representational State Transfer
RF	Radio Frequency
RFC	Request for Comments
RFID	Radio Frequency Identification
RIP	Routing Information Protocol
RRD	Round Robin Database
RSA	Rivest, Shamir, Adleman
RSSI	Received Signal Strength Indicator
RSTP	Rapid Spanning Tree Protocol
RTCP	RTP Control Protocol
RTLS	Real-Time Location Systems
RTP	Real-Time Transport Protocol
RTS	Request to Send
RTSP	Real Time Streaming Protocol
RVI	Routed VLAN Interface
RW RoW	Rest of World
SA	Security Association
SAML	Security Assertion Markup Language
SAN	Subject Alternative Name

Table 62: *List Of Acronyms And Abbreviations*

Acronym or Abbreviation	Definition
SCB	Station Control Block
SCEP	Simple Certificate Enrollment Protocol
SCP	Secure Copy Protocol
SCSI	Small Computer System Interface
SDN	Software Defined Networking
SDR	Software-Defined Radio
SDU	Service Data Unit
SD-WAN	Software-Defined Wide Area Network
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SIRT	Security Incident Response Team
SLAAC	Stateless Address Autoconfiguration
SMB	Small and Medium Business
SMB	Server Message Block
SMS	Short Message Service
SMTP	Simple Mail Transport Protocol
SNIR	Signal-to-Noise-Plus-Interference Ratio
SNMP	Simple Network Management Protocol
SNR	Signal-to-Noise Ratio
SNTP	Simple Network Time Protocol

Table 62: *List Of Acronyms And Abbreviations*

Acronym or Abbreviation	Definition
SOAP	Simple Object Access Protocol
SoC	System on a Chip
SoH	Statement of Health
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSO	Single Sign-On
STBC	Space-Time Block Coding
STM	Station Management
STP	Spanning Tree Protocol
STRAP	Secure Thin RAP
SU-MIMO	Single-User Multiple-Input Multiple-Output
SVP	SpectraLink Voice Priority
TAC	Technical Assistance Center
TACACS	Terminal Access Controller Access Control System
TCP/IP	Transmission Control Protocol/ Internet Protocol
TFTP	Trivial File Transfer Protocol
TIM	Traffic Indication Map
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TLV	Type-length-value
ToS	Type of Service

Table 62: *List Of Acronyms And Abbreviations*

Acronym or Abbreviation	Definition
TPC	Transmit Power Control
TPM	Trusted Platform Module
TSF	Timing Synchronization Function
TSPEC	Traffic Specification
TTL	Time to Live
TTLS	Tunneled Transport Layer Security
TXOP	Transmission Opportunity
U-APSD	Unscheduled Automatic Power Save Delivery
UCC	Unified Communications and Collaboration
UDID	Unique Device Identifier
UDP	User Datagram Protocol
UI	User Interface
UMTS	Universal Mobile Telecommunication System
UPnP	Universal Plug and Play
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTC	Coordinated Universal Time
VA	Virtual Appliance
VBN	Virtual Branch Networking
VBR	Virtual Beacon Report
VHT	Very High Throughput

Table 62: *List Of Acronyms And Abbreviations*

Acronym or Abbreviation	Definition
VIA	Virtual Intranet Access
VIP	Virtual IP Address
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice over IP
VoWLAN	Voice over Wireless Local Area Network
VPN	Virtual Private Network
VRD	Validated Reference Design
VRF	Visual RF
VRRP	Virtual Router Redundancy Protocol
VSA	Vendor-Specific Attributes
VTP	VLAN Trunking Protocol
WAN	Wide Area Network
WebUI	Web browser User Interface
WEP	Wired Equivalent Privacy
WFA	Wi-Fi Alliance
WIDS	Wireless Intrusion Detection System
WINS	Windows Internet Naming Service
WIPS	Wireless Intrusion Prevention System
WISPr	Wireless Internet Service Provider Roaming
WLAN	Wireless Local Area Network
WME	Wireless Multimedia Extensions

Table 62: *List Of Acronyms And Abbreviations*

Acronym or Abbreviation	Definition
WMI	Windows Management Instrumentation
WMM	Wi-Fi Multimedia
WMS	WLAN Management System
WPA	Wi-Fi Protected Access
WSDL	Web Service Description Language
WWW	World Wide Web
WZC	Wireless Zero Configuration
XAuth	Extended Authentication
XML	Extensible Markup Language
XML-RPC	XML Remote Procedure Call
ZTP	Zero Touch Provisioning

Glossary

The following table lists the terms and their definitions in this guide.

Table 63: *Terms And Definitions*

Term	Definition
802.11	An evolving family of specifications for wireless LANs developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE). 802.11 standards use the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance) for path sharing.
802.11a	Provides specifications for wireless systems. Networks using 802.11a operate at radio frequencies in the 5GHz band. The specification uses a modulation scheme known as orthogonal frequency-division multiplexing (OFDM) that is especially well suited to use in office settings. The maximum data transfer rate is 54 Mbps.
802.11b	WLAN standard often called Wi-Fi; backward compatible with 802.11. Instead of the phase-shift keying (PSK) modulation method historically used in 802.11 standards, 802.11b uses complementary code keying (CCK), which allows higher data speeds and is less susceptible to multipath-propagation interference. 802.11b operates in the 2.4 GHz band and the maximum data transfer rate is 11 Mbps.
802.11g	Offers transmission over relatively short distances at up to 54 Mbps, compared with the 11 Mbps theoretical maximum of 802.11b. 802.11g operates in the 2.4 GHz band and employs orthogonal frequency division multiplexing (OFDM), the modulation scheme used in 802.11a, to obtain higher data speed. Computers or terminals set up for 802.11g can fall back to speeds of 11 Mbps, so that 802.11b and 802.11g devices can be compatible within a single network.
802.11n	Wireless networking standard to improve network throughput over the two previous standards 802.11a and 802.11g with a significant increase in the maximum raw data rate from 54 Mbps to 600 Mbps with the use of four spatial streams at a channel width of 40 MHz. 802.11n operates in the 2.4 and 5.0 bands.
AP	An access point (AP) connects users to other users within the network and also can serve as the point of interconnection between the WLAN and a fixed wire network. The number of access points a WLAN needs is determined by the number of users and the size of the network.
access point mapping	The act of locating and possibly exploiting connections to WLANs while driving around a city or elsewhere. To do war driving, you need a vehicle, a computer (which can be a laptop), a wireless Ethernet card set to work in promiscuous mode, and some kind of an antenna which can be mounted on top of or positioned inside the car. Because a WLAN may have a range that extends beyond an office building, an outside user may be able to intrude into the network, obtain a free Internet connection, and possibly gain access to company records and other resources.

Table 63: *Terms And Definitions*

Term	Definition
ad-hoc network	A LAN or other small network, especially one with wireless or temporary plug-in connections, in which some of the network devices are part of the network only for the duration of a communications session or, in the case of mobile or portable devices, while in some close proximity to the rest of the network.
band	A specified range of frequencies of electromagnetic radiation.
DHCP	The Dynamic Host Configuration Protocol (DHCP) is an auto-configuration protocol used on IP networks. Computers or any network peripherals that are connected to IP networks must be configured, before they can communicate with other computers on the network. DHCP allows a computer to be configured automatically, eliminating the need for a network administrator. DHCP also provides a central database to keep track of computers connected to the network. This database helps in preventing any two computers from being configured with the same IP address.
DNS Server	A Domain Name System (DNS) server functions as a phonebook for the Internet and Internet users. It converts human readable computer hostnames into IP addresses and vice-versa. A DNS server stores several records for a domain name such as an address 'A' record, name server (NS), and mail exchanger (MX) records. The Address 'A' record is the most important record that is stored in a DNS server, because it provides the required IP address for a network peripheral or element.
DST	Daylight saving time (DST), also known as summer time, is the practice of advancing clocks, so that evenings have more daylight and mornings have less. Typically clocks are adjusted forward one hour near the start of spring and are adjusted backward in autumn.
EAP	Extensible authentication protocol (EAP) refers to the authentication protocol in wireless networks that expands on methods used by the point-to-point protocol (PPP), a protocol often used when connecting a computer to the Internet. EAP can support multiple authentication mechanisms, such as token cards, smart cards, certificates, one-time passwords, and public key encryption authentication.
fixed wireless	Wireless devices or systems in fixed locations such as homes and offices. Fixed wireless devices usually derive their electrical power from the utility mains, unlike mobile wireless or portable wireless which tend to be battery-powered. Although mobile and portable systems can be used in fixed locations, efficiency and bandwidth are compromised compared with fixed systems.
frequency allocation	Use of radio frequency spectrum regulated by governments.
frequency spectrum	Part of the electromagnetic spectrum.

Table 63: *Terms And Definitions*

Term	Definition
hotspot	A WLAN node that provides Internet connection and virtual private network (VPN) access from a given location. A business traveler, for example, with a laptop equipped for Wi-Fi can look up a local hot spot, contact it, and get connected through its network to reach the Internet and their own company remotely with a secure connection. Increasingly, public places, such as airports, hotels, and coffee shops are providing free wireless access for customers.
IEEE 802.11 standards	The IEEE 802.11 is a set of standards that are categorized based on the radio wave frequency and the data transfer rate.
POE	Power over Ethernet (PoE) is a method of delivering power on the same physical Ethernet wire used for data communication. Power for devices is provided in one of the following two ways: ● Endspan— The switch that an AP is connected for power supply. ● Midspan— A device can sit between the switch and APs The choice of endspan or midspan depends on the capabilities of the switch to which the IAP is connected. Typically if a switch is in place and does not support PoE, midspan power injectors are used.
PPPoE	Point-to-Point Protocol over Ethernet (PPPoE) is a method of connecting to the Internet typically used with DSL services where the client connects to the DSL modem.
QoS	Quality of Service (QoS) refers to the capability of a network to provide better service to a specific network traffic over various technologies.
RF	Radio Frequency (RF) refers to the portion of electromagnetic spectrum in which electromagnetic waves are generated by feeding alternating current to an antenna.
VPN	A Virtual Private Network (VPN) network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. A VPN ensures privacy through security procedures and tunneling protocols such as the Layer Two Tunneling Protocol (L2TP). Data is encrypted at the sending end and decrypted at the receiving end.
W-CDMA	Officially known as IMT-2000 direct spread; ITU standard derived from Code-Division Multiple Access (CDMA). Wideband code-division multiple access (W-CDMA) is a third-generation (3G) mobile wireless technology that promises much higher data speeds to mobile and portable wireless devices than commonly offered in today's market.
Wi-Fi	A term for certain types of WLANs. Wi-Fi can apply to products that use any 802.11 standard. Wi-Fi has gained acceptance in many businesses, agencies, schools, and homes as an alternative to a wired LAN. Many airports, hotels, and fast-food facilities offer public access to Wi-Fi networks.

Table 63: *Terms And Definitions*

Term	Definition
WEP	Wired equivalent privacy (WEP) is a security protocol specified in 802.11b, designed to provide a WLAN with a level of security and privacy comparable to what is usually expected of a wired LAN. Data encryption protects the vulnerable wireless link between clients and access points; once this measure has been taken, other typical LAN security mechanisms such as password protection, end-to-end encryption, virtual private networks (VPNs), and authentication can be put in place to ensure privacy.
wireless	Describes telecommunications in which electromagnetic waves (rather than some form of wire) carry the signal over part or all of the communication path.
wireless network	In a Wireless LAN (WLAN), laptops, desktops, PDAs, and other computer peripherals are connected to each other without any network cables. These network elements or clients use radio signals to communicate with each other. Wireless networks are set up based on the IEEE 802.11 standards.
WISP	Wireless ISP (WISP) refers to an Internet service provider (ISP) that allows subscribers to connect to a server at designated hot spots (access points) using a wireless connection such as Wi-Fi. This type of ISP offers broadband service and allows subscriber computers, called stations, to access the Internet and the Web from anywhere within the zone of coverage provided by the server antenna, usually a region with a radius of several kilometers.
wireless service provider	A company that offers transmission services to users of wireless devices through radio frequency (RF) signals rather than through end-to-end wire communication.
WLAN	Wireless local area network (WLAN) is a Local Area Network (LAN) that the users access through a wireless connection.