

Aruba Central



a Hewlett Packard
Enterprise company

User Guide

Copyright Information

© Copyright 2017 Hewlett Packard Enterprise Development LP.

Open Source Code

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

Hewlett Packard Enterprise Company
Attn: General Counsel
3000 Hanover Street
Palo Alto, CA 94304
USA

Contents	3
About this Guide	12
Intended Audience	12
Related Documents	12
Conventions	12
Contacting Support	13
About Aruba Central	14
Key Features	14
Operational Modes and Interfaces	14
Browser Compatibility Matrix	14
Supported Devices	15
Supported AP Platforms	15
Supported Switch Platforms	16
Subscriptions	17
Subscription Assignment	17
Automatic Subscription Assignment	17
Getting Started	18
Signing up for Aruba Central	18
Adding Devices to Central	19
Creating Customer and User Accounts	20
In the Managed Service Portal	21
In the Standard Interface View	21
Assigning Subscriptions	23
Assigning Devices to Groups	23
Central Interface	25

Header Pane	25
Aruba Central App Selection Pane	26
Network Management	27
Guest Access	28
Presence Analytics	28
Clarity	28
Global Settings	28
Data Pane	29
Other UI Elements and Functions	29
Labels	29
Variables	29
Groups	29
Overrides	30
Setting up Devices and Groups	31
Verifying and Configuring Ports	31
Provisioning Devices	31
Importing Configuration from a Device	31
Managing Groups	32
Provisioning Groups in the Managed Service Portal	32
Creating a Group	32
Editing a Group	33
Managing Configuration Overrides	33
Managing Overrides in the Standard Central Interface	33
Modifying AP Administrator Credentials	34
Monitoring Dashboard	35
Overview	35
Access Points	35
Access Points Page	36

AP Details Page	37
Clients	39
Clients Page	39
Client Details	40
AppRF	41
Switches	41
Switches Page	42
Switch Details Page	42
Wireless Security	44
Notifications	45
Setting Notification Alerts	46
Configuring APs	47
Configuring AP Settings	47
Configuring External Antenna	49
EIRP and Antenna Gain	49
Configuring Antenna Gain	49
Adding an AP	49
Removing an AP from the Network	49
Configuring System Parameters for AP Network	50
Configuring Networks	52
Configuring a WLAN SSID Profile	53
Configuring Captive Portal Profiles for Guest Network	59
Splash Page Profiles	60
Configuring Profiles for Wired Network	66
Editing a Network Profile	68
Deleting a Network Profile	68
Configuring Time Based Services	68
Configuring ARM and RF Parameters	70

ARM Overview	70
Configuring ARM Features	70
Configuring Radio Parameters	73
Configuring IDS Parameters	74
Rogue APs	74
Configuring Wireless Intrusion Detection and Protection Policies	74
Containment Methods	77
Configuring Authentication and Security Parameters	77
Supported Authentication Methods	78
Supported Authentication Servers	81
External RADIUS Server	81
RADIUS Server Authentication with VSA	82
Internal RADIUS Server	82
Authentication Termination on AP	82
Dynamic Load Balancing between Authentication Servers	83
Configuring External Servers for Authentication	83
Configuring Authentication Parameters for AP Management Users	85
Configuring AP Users	86
In the Central UI	86
Configuring Roles and Policies for User Access Control	87
ACL Rules	87
Configuring Network Address Translation Rules	88
Configuring Access Rules for Network Services	88
Configuring User Roles	90
Configuring Derivation Rules	90
Configuring Firewall Settings for Protection from ARP Attacks	92
Managing Inbound Traffic	92
Configuring ALG Protocols	93
Blacklisting Clients	93

Configuring VPN Networks	94
VPN Features	94
Supported VPN Protocols	95
Configuring VPN Tunnels	95
Configuring IPSec Tunnel	95
Enabling Automatic Configuration of GRE Tunnel	96
Configuring GRE Tunnel Manually	97
Configuring an L2TPv3 Tunnel	98
Configuring Routing Profiles	98
Configuring DHCP and Client IP Assignment Modes	99
Configuring DHCP Scopes	99
Configuring DHCP Server for Client IP Assignment	103
Configuring Services	104
Configuring AirGroup Services	104
Configuring an AP for RTLS Support	105
Configuring an AP for ALE Support	105
ALE with Central	106
Enabling ALE support on an AP	106
Configuring OpenDNS Credentials	106
Configuring CALEA Server for Lawful Intercept Compliance	106
Configuring CALEA Server Details on an AP	107
Integrating a Third-Party Network Firewall	107
Configuring an AP for Network Integration	107
Enabling AppRF™ Service	108
Configuring Uplinks	108
Uplink Interfaces	108
Uplink Preferences and Switching	114
Enforcing Uplinks	114
Setting an Uplink Priority	114

Enabling Uplink Pre-emption	114
Switching Uplinks based on the Internet Availability	115
Mobility and Client Management	115
Layer-3 Mobility for AP Clients	115
Home agent load balancing	115
Configuring L3 mobility domain	116
Configuring Enterprise Domains	116
Configuring SNMP Parameters	117
Configuring Community String for SNMP	117
Configuring SNMP Traps	118
Configuring Logs and TFTP Dump Servers	118
Configuring a Syslog Server	119
Configuring TFTP Dump Server	119
Resetting an AP	120
Uploading and Mapping AP Certificates	120
Uploading Certificate for an AP	120
Mapping AP Certificate	122
Analyzing Application Statistics	123
Application Visibility	123
AppRF Dashboard	123
Overview	124
Analyze	124
Configuring ACL Rules for Application Analytics	126
Configuring Web Policy Enforcement	127
Creating Custom URLs for Redirection	129
Creating a List of Error Page URLs	129
Configuring ACL Rules to Redirect Users to a Specific URL	129
Switch Configuration	130

Aruba Switches	130
New Switch Platforms	130
Legacy Aruba Switch Platforms	130
Configuring Switch Parameters	131
Configuring Ports	131
Configuring VLANs	133
Adding VLAN Details	133
Editing the VLAN Details	133
Deleting VLAN Details	134
Configuring DHCP Pools	134
Adding a New DHCP Pool	134
Configuring System Parameters for a Switch	135
Configuring Administrator Credentials for Mobility Access Switch	135
Configuring Administrator and Operator Credentials for Other Aruba Switches	135
Configuring a Name Server	135
Managing Reports	136
Generated Reports	136
Contents of a Report	137
Viewing a Generated Report	138
Creating a Report	139
Maintenance	140
Maintaining Firmware Versions	140
Viewing Firmware Details	140
Upgrading a Device	141
Managing User Accounts	142
Two-Factor Authentication	142
Viewing Audit Trails	144
API Gateway	145

API Framework Plug-in	145
Using OAuth 2.0 to Access API	145
Access and Refresh Tokens	145
Viewing APIs	146
Viewing Tokens	146
Adding a New Token	146
Troubleshooting Devices	146
Troubleshooting Overview	146
Troubleshooting a Device	147
Presence Analytics	149
Presence Analytics Overview	149
Configuring Sites	149
Configuring APs for Presence Analytics	150
Using the Presence Analytics App	150
Analyzing User Traffic Presence	150
Setting RSSI Threshold and Dwelling Time	151
Global Settings	152
Labels	153
Label Classification	153
Label Management	153
Managing Devices	154
Adding Devices	154
Viewing Devices	154
Assigning Subscriptions to Devices	156
Assigning Devices to a Group	156
Managing Subscriptions	157
Viewing Subscription Key Details	157
Adding Another Subscription Key	158

Acknowledging Subscription Expiry Notifications	158
Assigning Subscriptions to Devices	158
Guest Access	160
Guest Access Dashboard	160
Creating Apps for Social Login	161
Creating a Facebook App	161
Creating a Google App	162
Creating a Twitter App	164
Creating a LinkedIn App	165
Configuring a Cloud Guest Splash Page Profile	165
Adding a Cloud Guest Splash Page Profile	165
Customizing a Splash Page Design	168
Previewing and Modifying a Splash Page Profile	169
Associating a Splash Page Profile to an SSID	169
Configuring Visitor Accounts	170
Adding a visitor	170
Acronyms and Abbreviations	172
Glossary	187

This user guide describes the features supported by Aruba Central and provides detailed instructions to set up and configure devices such as APs 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
<i>Italics</i>	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:



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



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



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	hpe.com/networking/support
End-of-life Information	arubanetworks.com/support-services/end-of-life/
Security Incident Response Team	Site: arubanetworks.com/support-services/security-bulletins/ Email: sirt@arubanetworks.com

Aruba Central is a cloud-based platform that enables you to manage your Aruba Wi-Fi 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.

Key Features

Central offers the following key features:

- Streamlined management of devices
- Dashboard for network view and client monitoring
- Application Analytics
- Easy grouping of devices
- Centralized configuration of APs and Switches
- Easy management of user accounts
- Subscription based access to devices
- Guest Wi-Fi access configuration
- Report Generation
- Troubleshooting devices

Operational Modes and Interfaces

Aruba Central is now available in two operational modes:

- Standard Enterprise Mode—The standard enterprise mode provides a complete view of the devices that are monitored and managed by Central. It also allows end-end provisioning, management, monitoring, maintenance operations for the devices associated with the Central customer accounts.
- Managed Service Mode—The Managed Service Portal provides a consolidated view of the networks of customers. The service provider administrators can manage devices, and subscriptions associated with the customer accounts within their network.

Browser Compatibility Matrix



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

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

Supported Devices

Central supports the management of Aruba WLAN APs running Instant software and switches.

Supported AP Platforms

The current release of Central supports the following AP platforms:

- IAP-304/305
- IAP-207
- IAP-334/335
- IAP-314/315
- IAP-324/325
- IAP-277
- IAP-228
- IAP-205H
- IAP-103
- IAP-114/115
- IAP-204
- IAP-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-105
- IAP-92/93

Supported AP Firmware Versions

The current release of Central supports only the following AP 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
- 6.4.4.8-4.2.4.4
- 6.5.0.0-4.3.0.0
- 6.5.0.0-4.3.0.1
- 6.5.1.0-4.3.1.0

Supported Switch Platforms

Central supports the following Switch platforms:

New Switch Platforms

- Aruba 2920 Switch Series
- Aruba 2930F Switch Series
- Aruba 2540 Switch Series
- Aruba 3810 Switch Series

Central supports the following firmware versions on Aruba switches:

- Aruba 2920 Switch Series—WB.16.02.0012 or later
- Aruba 2930F Switch Series—WC.16.02.0012 or later
- Aruba 2540 Switch Series—YC.16.02.0012 or later
- Aruba 3810 Switch Series—WB 16.03.0003 or later

Legacy Aruba Switch Platforms

Central also supports the following legacy Switch models:

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

Central supports the following ArubaOS software versions on the legacy Switch platforms:

- 7.3.2.6
- 7.4.0.3
- 7.4.1.4

Subscriptions

Central offers a 90-day evaluation subscription for customers who want to try the Aruba cloud solution for managing their Wi-Fi networks. When you sign up for Central, an evaluation subscription is automatically assigned, unless you have bought a paid subscription. To obtain subscription and renew subscriptions, contact the Aruba Central support team.

Aruba Central now supports the following types of subscriptions:

- **Device management subscriptions**—Subscriptions for the devices. The device management subscription allows you to add and manage devices (APs and Switches), and avail basic services such as device configuration, monitoring dashboard, reports, and application analytics.
- **Cloud service subscriptions**—Subscriptions that enable an advanced cloud service on any capable device. For example, access to application services such as Presence Analytics is based on the cloud service subscription. As of today, the cloud services portfolio includes Presence Analytics, Guest Access, Clarity, and Unified Communication services.

Subscription Assignment

The Central subscriptions are assigned based tokens. Each subscription holds a specific number of subscriptions. The quantity of subscriptions available for a subscription is referred to as tokens. For example, when a subscription is assigned to a device, the device is bound with a token from the existing pool of subscriptions available for a subscription. To avail services, you may need to assign a set of tokens to the devices provisioned in Central.

Automatic Subscription Assignment

When a subscription assigned to a device expires or is canceled, Central checks the inventory for the available subscription tokens for the device and verifies if the subscription has adequate capacity. If the subscription has adequate capacity, Central automatically assigns the longest available subscription token to the device. If not, Central ensures that the subscriptions are utilized to the full capacity by assigning as many devices as possible.

To start using Aruba Central, complete the following steps:

- [Signing up for Aruba Central on page 18](#)
- [Adding Devices to Central on page 19](#)
- [Creating Customer and User Accounts](#)
- [Assigning Subscriptions](#)
- [Assigning Devices to Groups](#)

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.



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.

Adding Devices to Central

After you successfully log in to Central, a welcome message is displayed in the Central UI. To bind devices to your subscription, click **Manage Your Devices**. The **Device Provisioning** page is displayed. To view the subscription key details before binding devices, click **Subscription Keys** under **Global Settings > Devices & Subscriptions**.

Central supports zero touch provisioning of the devices. It automatically retrieves the devices associated with your subscription and Central subscription. To synchronize the devices from the inventory, click **Sync Now**. 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.

The evaluation subscription with device subscription tokens allows you to add up to 10 APs or 10 Switches, or a combination of 10 APs and Switches. With device subscription tokens, you can access basic network management services such as monitoring, configuration, and report generation.



The service evaluation subscription allows you to access application services, for example, Presence Analytics. With this subscription, you can add up to 20 APs.

For APs that dynamically form a cluster, the users must add the master AP from the **Device Provisioning** page whenever a slave AP joins the cluster, in order for the slave AP to inherit the configuration from the master AP.

To manually add a device, complete the following steps:

1. Click **Global Settings** on the left pane.
2. Click **Devices & Subscriptions**. The **Device Provisioning** page is displayed.
3. Click **Add Devices**. The **Manually Add Devices** window opens.
4. 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. If your account is already mapped to an Aruba Activate account, contact Aruba support team.
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 APs, execute the show about command at the AP CLI or click Maintenance > About in the AP 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.

The provisioning of the legacy ArubaSwitch 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 Aruba Switches 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.

If the switches ship with a version lower than the minimum supported firmware version, a factory reset may be required, so that the switch can initiate a connection to Central. For information, on the minimum firmware versions supported on the switches, see [Supported Switch Platforms on page 16](#).

Creating Customer and User Accounts

This section describes the procedures for configuring through the Managed Service Portal and Standard

Interface view.

In the Managed Service Portal

The customers who sign up for Central and obtain evaluation or paid subscription can log in and manage their devices through the Standard Enterprise interface. However, if these customers have multiple accounts associated with their service, they can use Managed Service portal to create and manage their respective customer accounts, and allocate devices to these accounts.

Adding Customer Accounts

To add customer accounts in the Managed Service Portal mode, complete the following steps:

1. Ensure that you have enabled the Managed Service Mode. To enable access to the Managed Service Portal mode, click the **Managed Service Mode** menu from the user settings menu on the header pane. The Managed Service Portal opens.
2. From the App selector, click **Network Management**, and then click **Customers**. The **Customers** page opens.
3. Click **+ Add Customer**. The **Customer > Create Customer** window opens.
4. Enter the name of the customer in the **Customer Name** text box.
5. Select a group to which you want to associate the customer account.
6. To add users to this account, enter the email address of the user. By default, the users are assigned the read-only privilege.
7. To add another user, click **+ Add User** and then enter the email address of the user.
8. Click **Save**. When the account is created successfully, an email invitation is sent to the user.

The customer accounts created and managed by the Managed Service Portal administrators have limited access to the Standard Enterprise interface.

Allocating Devices to Customer Accounts

Managed Service Portal users can allocate the devices in Central to specific customer accounts and assign subscription keys.

To assign a device to a customer account, complete the following steps:

1. Click **Global Settings > Devices & Subscriptions**. The **Device Provisioning** page opens.
2. Click **Manage Devices**.
3. To assign devices to a customer account, select the device, and click **Assign to Customer**.
4. Select the customer you want to assign to and then click **Assign**.

In the Standard Interface View

You can add users to an existing customer account in the Standard Enterprise view. If you have to devices from multiple locations with separate customer accounts, you can also create additional customer accounts.

Adding Users

To configure user accounts through the Standard Central Interface, 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.



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.



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.

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.

Assigning Subscriptions

You can assign any of the following types of subscriptions either through the Managed Service Portal or the Central Standard Interface.

- Device subscriptions—Subscriptions for the devices to avail basic services such as device configuration, monitoring, reporting, and analyzing application usage.
- Service subscriptions—Subscriptions based services for apps such as Presence Analytics, Guest Access, and so on.

To assign subscriptions to the devices, complete the following steps:

1. Click **Global Settings > Devices & Subscriptions > Subscription Assignment**.

The **Subscription Assignment** page allows you to assign subscriptions for the devices or services for which the users have subscribed.

2. To assign subscriptions to devices, complete the following steps:

- a. Move the slider to **Devices**.
- b. Select the device to which you want to assign a subscription.
- c. Click **Assign**.

3. To assign service subscriptions, complete the following steps:

- a. Move the slider to **Network Services**.
- b. Select the device to which you want to assign a service subscription token.
- c. Select the desired services.
- d. Click **Assign**.

Assigning Devices to Groups

When the devices are added to Central, they are automatically provisioned. The devices connected to Central are indicated in green in the Standard Enterprise view.

In the Standard Enterprise View

The group assignment in the Standard Enterprise view depends on the following conditions:

- If the device is not connected to Central, the **Assign Group** button is displayed.
- If the device is connected to Central, irrespective of the operational status of the device, the **Assign Group** button is not 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 **Global Settings > Devices & Subscriptions**. The **Device Provisioning** page opens.
2. Click **Pre-provision Groups**.
3. Select the devices.
4. Click **Assign Group**. The **Assign Group** pop-up window opens.
5. Select the group to which you want to assign the selected devices.
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**.

In the Managed Service Portal

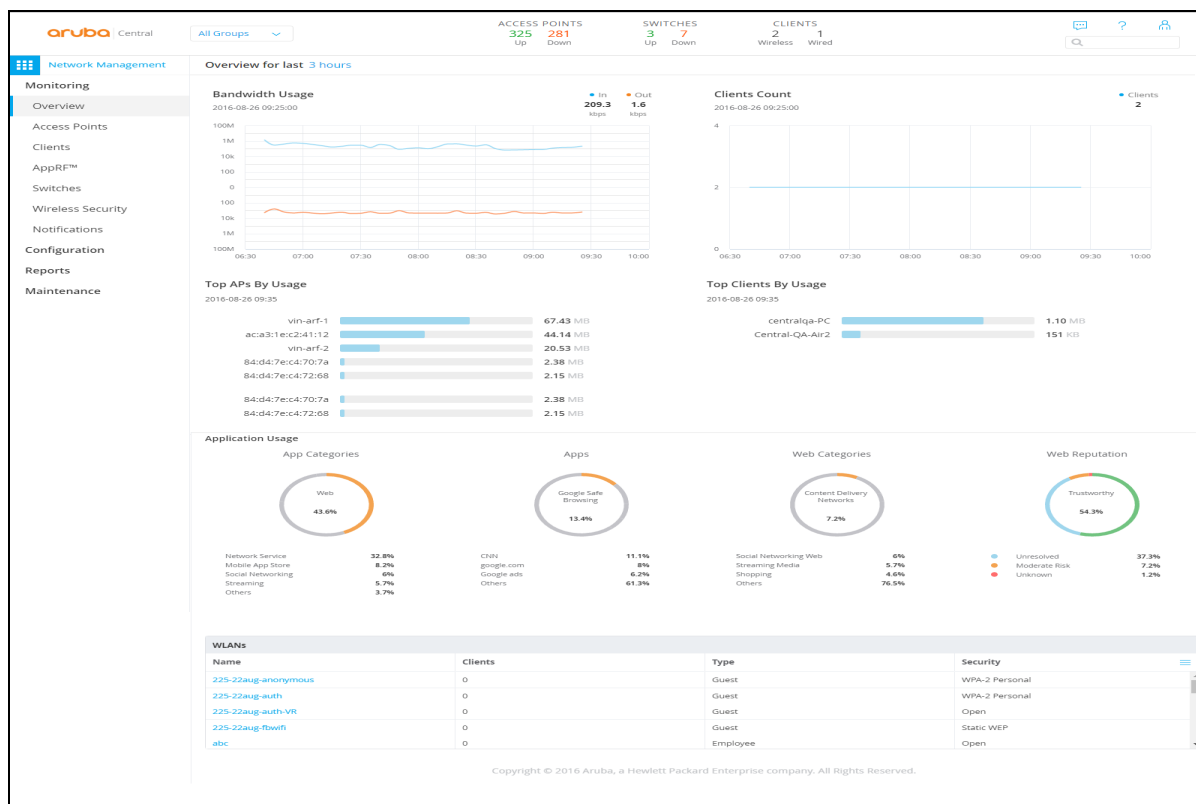
In the Managed Service Portal, the groups are assigned to a customer account. The provisioning status of the devices for each customer account is displayed in the **All Customers** table on the **Monitoring > All Customers** page. If a device is listed under the unprovisioned group for the customer account in the Standard Enterprise mode, the status of this device is displayed in the **All Customers**. To move the device from the unprovisioned group to the default group, the Managed Service Portal administrators must drill down to the customer account and move the device to default in the Standard Enterprise mode.

If a customer account is associated to a new group created in the Managed Service Portal, the configuration of the devices associated with this customer account is pushed to the **default** group in the Standard Enterprise view for that customer. However, the Managed Service Portal administrators can create more groups for a customer account by drilling down to the customer account in the Standard Enterprise view.

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

[Central Main Window](#) shows the Central main window.

Figure 1 *Central Main Window*



The main window consists of the following elements:

- [Header Pane](#)
- [Aruba Central App Selection 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 > Overview** page is displayed.
- **Group selector**—By default, the group selector view is set to **All Groups**. On clicking the group selector, the list of groups is displayed.
 - To search for groups, enter the name of the group in the search box.
 - To add a new group and add devices to the newly created group, click the + icon.
 - To manage groups, click the settings icon.

- If the group view is set to **All Groups**, you can search for a label.
- View the unprovisioned devices.

For more information on groups, see [Managing Groups on page 32](#).

- The number 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 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. If your account has the wired clients feature enabled and it does not have any WLAN SSIDs configured, the header displays only the wired client count.
- 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 bubble icon—Displays the following options:
 - **Documentation**—Opens the Central user documentation site.
 - **Support**—Directs you to the 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 22](#).
 - **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 the inactive user sessions. By default, the session timeout interval is set to 3000 minutes.



The Central UI is available in English, French, Spanish, Deutsche, and Chinese languages. 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 Portal mode and switches the interface to the Managed Service Portal.
- **Terms of Service**—Displays the terms and conditions for using Aruba Central services.
- **Logout**—Allows you to log out of your Aruba Central account.

Aruba Central App Selection Pane

The left navigation pane displays the **App Selector**  icon. On clicking the **App Selector** icon, the available apps are displayed. The contents on the top left navigation pane change dynamically based on the app you

select.

For example, clicking on **Guest Access** displays the function tabs and menu options for guest network configuration respectively. By default, the Network Management application view is selected.

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



The availability of apps such as Presence Analytics are based on service subscriptions. Contact your administrator and the Aruba Central Support team to obtain access to these application services.

Network Management

The following menu options are available in the **Network Management** application view:

- [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**—Displays details of the APs provisioned in the network.
- **Clients**—Displays details of the client devices associated with the AP.
- **AppRF™**—Provides a summary of client traffic to applications, application categories, websites category, and website reputation score.
- **Switches**—Displays details of the Switches provisioned in the network.
- **Wireless Security**—Displays information about the unauthorized presence of APs and clients in the network.
- **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, Client Usage, Capacity Planning, New Infra Inventory, and AppRF 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 perform the following actions:

- View the current firmware version of the devices and provides options to upgrade to the latest firmware version.
- 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 in the **Guest Access** application view:

- **Overview**—Displays a dashboard that shows the details of the cloud guest SSIDs, duration for which the guest users are connected, client count, and the type of client devices connected to the cloud guest SSIDs.
- **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 view provides a real-time and historical view of the user traffic patterns in public venues and enterprise environments.

The **Presence Analytics** application view 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.

Clarity

The Clarity application view provides an analytical dashboard for real-time monitoring of the client data flow, client association and authentication transactions, DHCP and DNS service request and responses.

The **Clarity** application view includes the following menu options:

- **Activities**—The **Activity** dashboard displays graphs for connectivity health, latency, performance of the network and the device, and the association and authentication transactions between the client device and the network.
- **Insights**—The **Insights** dashboard displays trends for the onboarding performance of the network for a time range of 1 day or 1 month.
- **Troubleshooting**—The **Troubleshooting** page allows you to view the onboarding details for a specific client device.

Global Settings

The **Global Settings** tab includes the following menu options:

- **Labels**—Create and manage labels for devices. The labels can use used to tag devices to a location, to specific owners, or departments.

- **Devices & Subscriptions**— This menu command allows you to perform the following actions:
 - View and manage devices.
 - View the details of subscription keys
 - Assign subscriptions to devices

Data Pane

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

Other UI Elements and Functions

Central UI also supports the following features and functions:

- [Labels](#)
- [Variables](#)
- [Groups](#)
- [Central Interface](#)

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 AP labeled as **Building 25** and **Lobby**. These tags identify the location of the AP within the enterprise campus and the building. The APs in other buildings can also be tagged as **Lobby** to enable all the APs in the lobbies of all these buildings in the campus. To filter and monitor APs in the lobbies of all the campus buildings, you can tag all the APs 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 153](#).

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 APs, you can configure the APs 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 APs using a group. The group configuration is shared across all devices. For more information on groups, see [Managing Groups on page 32](#).

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 Configuration Overrides on page 33](#).

This chapter describes the following topics:

- [Verifying and Configuring Ports on page 31](#)
- [Provisioning Devices on page 31](#)
- [Managing Groups on page 32](#)
- [Managing Configuration Overrides on page 33](#)
- [Modifying AP Administrator Credentials on page 34](#)

Verifying and Configuring Ports

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 AP comes up.
- TCP port 2083 for RADIUS authentication for guest management. If 2083 port is blocked, the HTTPS protocol is used.

Provisioning 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 **Global Settings > Device and Subscriptions > Pre-Provision Groups** 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 AP cluster joins Central:

- If the new AP 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 AP cluster was not associated with any existing cluster groups on Central, the device is moved to the unprovisioned group.

Importing 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.

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.

Provisioning Groups in the Managed Service Portal

Unlike the Standard Enterprise mode, the groups in the Managed Service Portal are associated with the customer accounts. The devices allocated to the customer account are associated to these groups.

Unlike in the Standard Enterprise mode, the monitoring dashboard or the network view is not determined by the selection of the groups. As devices are mapped to customer accounts, all information pertaining to customer accounts is displayed.

In the Managed Service Portal, the provisioning status of the devices for each customer account is displayed in the **All Customers** table. If a device is listed under the unprovisioned group for the customer account in the Standard Enterprise mode, the status of this device is displayed in the **All Customers**. To move the device from the unprovisioned group to the default group, the Managed Service Portal administrators must drill down to the customer account and move the device to default in the Standard Enterprise mode.

If a customer account is associated to a new group created in the Managed Service Portal, the configuration of the devices associated with this customer account is pushed to the **default** group in the Standard Enterprise view for that specific customer. However, the Managed Service Portal administrators can create more groups for a specific customer by drilling down to customer account in the Standard Enterprise view.

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. To use this group as a template group, select the **Set this group as a template group** check box and click **Save**.



If the group is set as a template group, the configuration is applied to all the devices in the group. For devices in such groups, the configuration wizards in the UI are disabled.

The current version of Central allows template group creation for AP devices only.

6. To create a non-template groups, click **Next** and complete the following steps:
 - a. Enter the default device password for the newly created group in the **Password** text box.
 - b. To reconfirm the password, re-enter the default device password in the **Retype Password** text box.
 - c. 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 the settings icon.
3. To create a clone of an existing group, complete the following steps:
 - a. Select the group and click the clone icon next to the group. The **Create New Group** pop-up window opens.
 - b. Enter a name for the group.
 - c. Click **Save**.



The cloning feature is supported only for the non-template groups. If a group is set as a template group, the cloning icon will not be displayed for that group.

4. To delete a group, select the group to delete and click the delete icon.
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 Configuration Overrides

This section describes how to resolve configuration overrides.

Managing Overrides in the Standard Central Interface

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**.

The **Monitoring** tab includes the following functional menu options for viewing the device and network details.

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 AP over a specific duration.
TOP APs By Bandwidth Usage	Displays the list of top APs that utilize the maximum bandwidth in the network.
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, and graphs showing bandwidth and application usage for the APs in provisioned in Central.

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

- **Usage**—Displays graphs for all APs in the group.

- **Top N**—Displays a list of APs sorted based on their usage.
- **List**—Displays a list of APs in the group. To view the details of an AP, click the AP entry in the **Access Points** table.

Access Points Page

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.
Bandwidth Usage per Network	Displays the aggregate incoming and outgoing traffic for all APs per SSID over a specific duration.
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.

Data Pane Content	Description
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—The AP radio mode such as access or monitor. ■ Type—Type of the 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 Page

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.
Status	Displays the current status of the AP.
SSID	Displays the SSIDs configured on the AP.
Uptime	Displays the time since which the AP is operational.
Alerts	Displays the alerts generated for the AP.
CPU	Displays the percentage of processing resources utilized on the AP.
Memory	Displays the percentage of memory utilized on the AP.

Parameter	Description
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. You can also click the Wired tab to view the wired client count for the selected AP. ○ 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. ■ Neighboring Clients—The number of clients in the AP neighborhood.
Interface	Displays the wired and wireless network interface details. ■ Wired Interface—Displays wired interface details such as Ethernet ports, MAC and IP addresses of the Ethernet interface link type, and duplex mode. ■ Wireless Interface—Displays wireless interface details such as the 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. ■ Interface Bandwidth Usage—Displays a graph that shows the bandwidth usage details for the selected wired interface. Click on the type of interface for which you want to view the graph for a given 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.
Clients	Displays the details of wired and wireless clients connected to the AP. If the wired clients feature is enabled for your account and there are no WLAN SSIDs configured in the provisioned network, only the wired clients are displayed. If the WLAN SSIDs are configured in the provisioned network, assign the wired network profiles to the Ethernet ports of an AP to view the wired clients information. For more information on wired network profiles, see Configuring Profiles for Wired Network on page 66.
Alerts and Event Log	Displays the alerts generated for the AP and the list of events associated with the AP.
VPN	Displays the following information: ■ The Bandwidth Usage per VPN graph—This graph shows the bandwidth usage by VPN. It displays the inbound and outbound traffic for both primary and backup VPNs for the last 3 hours (default). ■ The VPN table—It provides details about the Primary and Backup VPNs, their corresponding peer names, and indicates which VPN is active at any point of time.
Uplink History	Displays uplink connection history for 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.

Parameter	Description
	■ Mode—The radio mode in which the AP operates. ■ Mesh Role—Role of the mesh AP. ■ Country Code—Country code in which the AP operates. ■ VC Name—Name of the VC to which the AP is connected. ■ VC MAC—The MAC address of the VC. ■ AP Model Type—The AP hardware model. ■ Firmware Version—The firmware version running on the AP. ■ Modem status—Status of the cellular modems connected to the AP. ■ Current Uplink—Current uplink connection on the AP. ■ Group Name—The group to which the AP belongs. ■ Location—Location of the AP.
Map	Displays the geographical location of the AP.
Actions drop-down	Displays the following menu options: ■ 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 146. ■ Tech. Support—Allows administrators to generate a tech support dump required for troubleshooting the device.

Clients

The **Clients** menu displays the details of the clients connected to the devices in Central.

Clients Page

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

Data Pane Content	Description
	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.
Distribution	Displays the type of client device connected to the wireless network.
Top N	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	If the wired clients feature is enabled for your account and there are no WLAN SSIDs configured in the provisioned network, the wired clients are displayed. If the wired clients are enabled in the provisioned network that has WLAN SSIDs configured, assign wired network profiles to the Ethernet ports of an AP to view the wired clients. The following details are displayed for the clients. ■ MAC Address—The MAC address of the client. ■ IP Address—The IP address of the client. ■ User name—The user name of the client. ■ Hostname—The host name of the client. ■ Device type—The type of the client device. ■ SSID—The SSID to which the clients are connected. ■ Labels—Labels associated with the clients. To expand or collapse the column view, click the column settings icon next to the last column of the table.



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.

Data Pane Content	Description
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 AP and client association.
Alert and Event Log	Displays the alerts and events generated for the client.
Info	Displays the following details about the client device: ■ Connection rate—Data rate for client connection. ■ Username—Username for the client device. ■ Manufacturer—Client device manufacturer details.

AppRF

The AppRF pane displays the traffic summary for APs 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 AP.

For more information, see [Application Visibility on page 123](#).

Switches

The **Switches** menu displays the details of the Switches provisioned in Central.

Switches Page

The **Switches** page displays the status and usage of all switches provisioned in Central:

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 sorted based on maximum usage. It also shows the data traffic transmitted (Tx) and received (Rx) from clients.
List view—Switches table	Displays a list of Switches 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. ■ 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 Page

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.
Ports	Displays the following details of the Switch ports:

Data Pane Content	Description
	Graphs ■ Throughput—Indicates the aggregate client data traffic detected on the Switches. ■ Connected Clients—Indicates the number of clients connected to the Switch. ■ 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).
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 Switch platforms, 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. ■ Troubleshoot—Opens the Troubleshooting Devices page for running troubleshooting commands on the device. ■ Tech. Support—Allows the administrators to generate a tech support dump for troubleshooting the device. 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.



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 APs, interfering APs, 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.

Data Pane Content	Description
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 table displays information for the following types of WIDS events: ■ Rogues ■ Interferences ■ Infrastructure Attacks ■ Client Attacks The Rogues table displays information for the following types of WIDS events: ■ Rogues—The Rogues widget displays the following information: ○ Last Seen—The time stamp at which the rogue device was last detected in the network. ○ Reason for Classification—Reasons for classifying the device as a rogue device. ○ ESSID—The ESSIDs broadcast by the rogue device. ○ Channel—Radio channels detected on the rogue device. ○ SSID—SSIDs broadcast by the rogue device. ○ Manufacturer—Manufacturer details of the rogue device. ○ Containment Status—Details of the containment status. The Interferences, Infrastructure Attacks, and Client Attacks widgets display the following information: ■ Type—The type of the interference or attack detected. ■ Level—The level of the interference or attack detected. ■ Date/Time—Date and time of the interference or attack. ■ Description—Description of the attack ■ Detecting AP—The MAC address of the AP that detected the interference or attack. ■ Virtual Controller—The VC name of the IAP cluster in which the interference or attack was detected. ■ Station MAC—MAC address of the station ■ Radio—Radio band on which the interference was detected.

Notifications

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



The UI also shows the alerts and pending actions such as importing a device, setting country code of APs 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**.

This chapter describes how to configure APs provisioned in Central. For detailed instructions on AP configuration, see the following topics:

- [Configuring AP Settings on page 47](#)
- [Configuring Networks on page 52](#)
- [Configuring Time Based Services on page 68](#)
- [Configuring ARM and RF Parameters on page 70](#)
- [Configuring IDS Parameters on page 74](#)
- [Configuring Authentication and Security Parameters on page 77](#)
- [Configuring VPN Networks on page 94](#)
- [Configuring DHCP and Client IP Assignment Modes on page 99](#)
- [Configuring Services on page 104](#)
- [Configuring Uplinks on page 108](#)
- [Mobility and Client Management on page 115](#)
- [Configuring Enterprise Domains on page 116](#)
- [Configuring Logs and TFTP Dump Servers on page 118](#)
- [Resetting an AP on page 120](#)
- [Uploading and Mapping AP Certificates on page 120](#)

Configuring AP Settings

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

To customize AP parameters, complete the following steps:

1. Click **Configuration** > **Wireless**.
2. Select a group and then click **Access Points**. The **Access Points** page is displayed.
3. Click the AP that you want to customize.
4. Click **Edit**. The **Edit** pane for modifying the AP details is displayed.
5. Configure the parameters described in [Table 14](#) as required and then click **Save Settings**.

Table 14: Access Points Configuration

UI	Parameters	Description
Basic Info	Name	Configures a name for the AP. You can specify a character string of up to 32 ASCII characters.
	AP Zone	Configures the AP zone. When a zone is configured for an AP and if the same zone details are configured on an SSID, the SSID can be broadcast only by the APs in that specific zone. Only one zone can be configured on an SSID. An AP can belong to only one zone at any point in time.
	Preferred Master	Provisions the AP as a master AP.
	IP Address for Access Point	Allows IP to get an IP address from the DHCP server. By default, the APs obtain IP address from a DHCP server. The users can also assign a static IP address to the AP. To specify a static IP address for the AP, complete the following steps: 1. Enter the new IP address for the AP 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 AP serves clients, while also monitoring for rogue APs in the background. ■ Monitor—In the Monitor mode, the AP acts as a dedicated monitor, scanning all channels for rogue APs and clients. ■ Spectrum Monitor—In the Spectrum Monitor mode, the AP functions as a dedicated full-spectrum RF monitor, scanning all channels to detect interference, whether from the neighboring APs or from non-Wi-Fi devices such as microwaves and cordless phones. NOTE: In the Monitor and Spectrum Monitor modes, the APs do not provide access services to clients.
		You can configure a radio profile on an AP 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 APs.
Uplink	Uplink Management VLAN	The uplink traffic on AP is carried out through a management VLAN. However, you can configure a non-native VLAN as an uplink management VLAN. After an AP is provisioned with the uplink management VLAN, all management traffic sent from the AP 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.
	USB Port	Enable the USB port if you do not want to use the cellular uplink or 3G/4G modem in your current network setup.

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

Configuring External Antenna

If your AP 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 AP is deployed. You can also measure or calculate additional attenuation between the device and antenna before configuring the antenna gain. To know if your AP device supports external antenna connectors, see the *Installation Guide* that is shipped along with the AP 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):

$$\text{EIRP} = \text{Tx RF Power (dBm)} + \text{GA (dB)} - \text{FL (dB)}$$

The following table describes this formula:

Table 15: *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 APs 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 AP

To add an AP to Central, assign an IP address and a subscription.

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

Removing an AP from the Network

To remove an AP from the network:

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

Configuring System Parameters for AP 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 16: *System parameters*

Data Pane Item	Description
Virtual Controller	■ Name—Name of the VC ■ IP address—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 AP 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, click edit icon and update the name and IP address.
Timezone	To configure a timezone, select a timezone from the Timezone drop-down list. 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 AP 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 AP clock to set the correct time. If NTP server is not configured in the AP network, an AP reboot may lead to variation in time data. By default, the AP 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.

Table 16: *System parameters*

Data Pane Item	Description
Virtual Controller Netmask Virtual Controller Gateway Virtual Controller VLAN	NOTE: The IP configured for the VC can be in the same subnet as AP 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 AP.
Dynamic CPU Utilization	APs 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 APs 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. ■ 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 enabled, APs 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 APs to the network. If this feature is disabled, the inactive APs are displayed in red.
Terminal Access	When enabled, the users can access the AP CLI through SSH.
Telnet Server	When enabled, the users can start a Telnet session with the AP CLI.
LED Display	Enables or disables the LED display for all APs in a cluster. NOTE: The LED display is always enabled during the AP reboot.
Extended SSID	Extended SSID is enabled by default in the factory default settings of APs. This disables mesh in the factory default settings.

Table 16: *System parameters*

Data Pane Item	Description
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, move the slider to the right.
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 AP 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, move the slider to the right.
Dynamic RADIUS Proxy	When enabled, 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.
Cluster Security	Enables or disables the cluster security feature. When enabled, the the control plane communication between the AP cluster nodes is secured. For secure communication between the cluster nodes, the Internet connection must be available, or at least a local NTP server must be configured. NOTE: After enabling or disabling cluster security, ensure that the configuration is synchronized across all devices in the cluster, and then reboot the cluster.
Mobility Access Switch Integration	To enable LLDP protocol for Switch integration. With this protocol, APs 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 APs are connected.

Configuring Networks

This section describes the following procedures:

- [Configuring a WLAN SSID Profile on page 53](#)
- [Configuring Captive Portal Profiles for Guest Network on page 59](#)
- [Configuring Profiles for Wired Network on page 66](#)
- [Editing a Network Profile on page 68](#)
- [Deleting a Network Profile on page 68](#)

Configuring a WLAN SSID Profile



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

Configuring WLAN Settings

To configure WLAN settings, complete the following steps:

1. Click **Configuration > Wireless**.
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.



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 AP drops all broadcast and multicast frames except DHCP and ARP, IGMP group queries, and IPv6 neighbor discovery protocols. ■ ARP—The AP 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 AP 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 AP at every beacon. You can also configure a higher DTIM value for power saving.
Multicast Transmission Optimization	Select Enabled if you want the AP 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 AP 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 non-video 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 AP 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 AP sends multicast traffic over the wireless link.
Transmit Rates	Specify the following parameters: ■ 2.4 GHz—If the 2.4 GHz band is configured on the AP, specify the minimum and 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 AP, 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 AP, the SSID is broadcast by that IAP. ■ If an SSID belongs to a zone, all APs in this zone can broadcast this SSID. ■ If no AP belongs to the zone configured on the SSID, the SSID is not broadcast.

Parameter	Description
	■ If an SSID does not belong to any zone, all APs can broadcast this SSID.
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.
WiFi Multimedia	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 Filtering	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.
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.

Parameter	Description
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.
SSID Encoding	To encode the SSID, select UTF-8.
ESSID	Enter the Extended Service Set Identifier (ESSID). If the value defined for ESSID value is not the same as the profile name, the SSIDs can be searched based on the ESSID value and not by its profile name.
Deny Inter User Bridging	Disables bridging traffic between two clients connected to the same SSID on the same VLAN. When this option is enabled, 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.
Time Range Profiles	Click Edit . Select a time range profile from the list and a status to apply and then click Save .

6. Click **VLAN** 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—When selected, the client obtains the IP address from the VC.

Network Assigned—When selected, the client obtains the IP address from the network.

2. Based on the type of client IP assignment mode selected, you can configure the VLAN assignment for clients as described in the following table:

Table 18: VLAN Assignment

Parameter	Description
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 AP 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 99 .
Network Assigned	If this option is selected, , specify any of the following options: ■ Default—Assigns IP address to the client in the same subnet as the APs. By default, the client VLAN is assigned to the native VLAN on the wired network. ■ Static—Allows you 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—Assigns the VLANs dynamically from a DHCP server. You can also create a new VLAN assignment rules.

3. Click **Security** 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 19: WLAN security settings

Data pane item	Description
Encryption > 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.
Authentication	Configure the following parameters: ■ MAC Authentication—To enable MAC address based authentication for Personal and Open security levels, set MAC Authentication to Enabled. ■ Termination—Terminates the EAP portion of 802.1X authentication on the AP instead of the RADIUS Server. When enabled, the AP acts as an authentication server and terminates the outer layers of the EAP and relays only the innermost layer to the external RADIUS Server. If you are using LDAP for authentication, ensure that AP termination is configured to support EAP. ■ Primary Server—Sets a primary authentication server. ○ 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.

Data pane item	Description
	- To add a new server, click +. For information on configuring external servers, see Configuring External Servers for Authentication on page 83. ■ Secondary Server—To add another server for authentication, configure another authentication server. ■ Authentication Survivability—If an external server is configured for authentication, you can enable authentication survivability. 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. By default, authentication survivability is disabled. ■ 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 83.
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 APs and clients to dynamically measure the available radio resources. When 802.11k is enabled, APs and clients send neighbor reports, beacon reports, and link 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.
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.
Advanced > MAC Authentication for Enterprise Networks	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. If MAC authentication is enabled, configure the following parameters: ■ Delimiter Character—Specify a character (for example, colon or dash) as a delimiter for the MAC address string. When configured, the AP 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 AP to use uppercase letters in MAC address string for MAC authentication. This option is available only if MAC authentication is enabled.
Advanced > Reauth Interval	Specify a value for Reauth Interval. When set to a value greater than zero, APs periodically re-authenticate 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.

Data pane item	Description
	■ 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.
Advanced > 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.
Advanced > Enforce DHCP	Enforces WLAN SSID on AP clients. When DHCP is enforced: ■ A layer-2 user entry is created when a client associates with an AP. ■ The client DHCP state and IP address are tracked. ■ When the client obtains an IP address from DHCP, the DHCP state changes to complete. ■ If the DHCP state is complete, a layer-3 user entry is created. ■ When a client roams between the APs, the DHCP state and the client IP address will be synchronized with the new AP.

3. Click **Access** 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:
 - a. Click (+) icon.
 - b. Select appropriate options in the **New Rule** pane.
 - c. 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 Profiles for Guest Network on page 59](#).
 - Create a role assignment rule.
2. Click **Save Settings**.

Configuring Captive Portal Profiles for Guest Network

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 AP.

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.

For information on how to creating splash page profile, see the following sections:

- [Configuring Captive Portal Profiles for Guest Network on page 59](#)
- [Configuring Internal Captive Portal Splash Page Profile on page 61](#)
- [Configuring External Captive Portal Splash Page Profile on page 63](#)
- [Associating a Cloud Guest Splash Page Profile to a Guest SSID on page 65](#)
- [Disabling Captive Portal Authentication on page 66](#)

Configuring a WLAN SSID for Guest Access

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

1. Click **Configuration > Wireless > Networks**. The **Networks** page is displayed.
2. To create a new SSID profile, click the + icon. The **Create a New Network** pane is displayed.
3. 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**.
4. If configuring a wireless guest profile, set the required WLAN configuration parameters described in [Table 17](#).
5. Click **VLAN** to configure VLAN settings. The VLAN details are displayed.
6. Select any of the following options for **Client IP Assignment**:

- **Virtual Controller Assigned**—Allows the VC to assign IP address to the clients. The VC creates a private subnet and VLAN on the AP 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 99](#).
- **Network Assigned**—If the **Network Assigned** is selected, specify any of the following options:
 - **Default**— On selecting this option, the client obtains the IP address in the same subnet as the APs. 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. You can also set a VLAN assignment rule by clicking **New**.

7. Click **Save Settings**.

Configuring Internal Captive Portal Splash Page Profile

To configure internal captive portal profile, complete the following steps:

1. Open the guest SSID to edit and configure the following parameters in the **Networks > Security** page.

Table 20: 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.
Splash Page Properties	Under Splash Page Properties, 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. ■ Top Banner Title—Enter a title for the banner. To preview the page with the new banner title, click Preview Splash Page. ■ Header fill color—Specify a background color for the header. ■ Welcome Text—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. ■ Policy Text—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. ■ Page Fill Color—To change the color of the splash page, click the Splash page rectangle and select the required color from the color palette. ■ Redirect URL—To redirect users to another URL, specify a URL in Redirect URL. ■ Logo Image—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 delete an image, click Delete. ■ To preview the captive portal page, click Preview splash page. ■ Captive-portal proxy server IP and Port—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.
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.
Authentication	Configure the following parameters: ■ MAC Authentication—To enable MAC address based authentication for Personal and Open security levels, set MAC Authentication to Enabled. ■ Primary Server—Sets a primary authentication server. ○ 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. ○ To add a new server, click +. For information on configuring external servers, see Configuring External Servers for Authentication on page 83. ■ Secondary Server—To add another server for authentication, 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 83.
Reauth Interval	Specify a value for Reauth Interval. When set to a value greater than zero, APs periodically re-authenticate all associated and authenticated clients.

Table 20: Internal Captive Portal Configuration Parameters

Parameter	Description
Accounting	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.
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.
Disable If Uplink Type Is	To exclude uplink, select an uplink type.

2. Click **Save Settings**.

Configuring External Captive Portal Splash Page Profile

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. Open the guest SSID to edit and configure the following parameters in the **Networks > Security** page.
2. Select the Splash Page type as **External**.
3. 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.
4. Select a captive portal profile. To add a new profile, click + and configure the following parameters:

Table 21: 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.

Data Pane Item	Description
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.
Server Offload	Select the checkbox to enable the server offload feature. The server offload feature ensures that the non-browser client applications are not unnecessarily redirected to the external captive portal server, thereby reducing the load on the external captive portal server.
Prevent Frame Overlay	Select this checkbox to prevent the overlay of frames. When enabled, the frames display only those pages that are in the same domain as the main page.
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.

5. Click **Save**.

6. On the external captive portal splash page configuration page, specify encryption settings if required.

7. Specify the following authentication parameters:

- **MAC Authentication**—To enable MAC address based authentication for **Personal** and **Open** security levels, set **MAC Authentication** to **Enabled**.
- **Primary Server**—Sets a primary authentication server.
 - 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.
 - To add a new server, click +. For information on configuring external servers, see [Configuring External Servers for Authentication on page 83](#).
- **Secondary Server**—To add another server for authentication, 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.

8. If required, under **Walled Garden**, create a list of domains that are blacklisted and also a white list of websites that the users connected to this splash page profile can access.

9. To exclude uplink, select an uplink type.

10. If MAC authentication is enabled, you can configure the following parameters:

- **Delimiter Character**—Specify a character (for example, colon or dash) as a delimiter for the MAC address string. When configured, the AP 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 AP to use uppercase letters in MAC address string for MAC authentication. This option is available only if MAC authentication is enabled.
11. Configure the **Reauth Interval**. Specify a value for **Reauth Interval**. When set to a value greater than zero, APs periodically re-authenticate all associated and authenticated clients.
 12. If required, enable blacklisting. Set a threshold for blacklisting clients based on the number of failed authentication attempts.
 13. Click **Save Settings**.

Associating a Cloud Guest Splash Page Profile to a Guest SSID

To use the Cloud Guest Splash page profile for the guest SSID, ensure that the Cloud Guest Splash Page profile is configured through the **Guest Management** app.

To associate a Cloud Guest splash page profile to a guest SSID, complete the following steps:

1. Open the guest SSID to edit and click the **Security** tab:
 - a. Select **Cloud Guest** from the **Splash Page Type** list.
 - b. Select the splash page profile name from the **Guest Captive Portal Profile** list and click **Next**.
 - c. To enable encryption, set **Encryption** to **Enabled** and configure the encryption parameters.
 - d. To exclude uplink, select an uplink from **Disable If Uplink Type Is**.
 - e. Click **Next**.
2. Click **Save Settings**.

Configuring Access Rules for Guest Users

To configure access rules for a guest network, complete the following steps:

1. Go to **Configuration > Wireless > Networks** and open the guest SSID to edit.
2. 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:
 - a. Click **(+)** icon and select appropriate options for **Rule Type**, **Service**, **Action**, **Destination**, and **Options** fields.
 - b. 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**.
3. Click **Save Settings**.

Disabling Captive Portal Authentication

To disable captive portal authentication, perform the following steps:

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

Configuring Profiles for Wired Network

If the WLAN SSIDs are configured on the devices and wired clients must be supported on the APs must, configure the wired network profiles and assign these profiles to the Ethernet ports of an AP.

The Ethernet ports of an AP 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 > Wireless**.
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 APs 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 83](#).
 - **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 83](#).

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**.



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 AP 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 > Wireless**.
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 > Wireless**.
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 > Wireless**.
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 > Wireless > 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 70](#)
- [Configuring ARM Features on page 70](#)
- [Configuring Radio Parameters on page 73](#)

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 AP 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 AP 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 AP RF environment. Each AP gathers other metrics on its ARM-assigned channel to provide a snapshot of the current RF health state.

APs support the following ARM features:

- Channel or Power Assignment—Assigns channel and power settings for all the APs in the network according to changes in the RF environment.
- Voice Aware Scanning—Improves voice quality by preventing an AP from scanning for other channels in the RF spectrum during a voice call and by allowing an AP 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 APs 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 AP reassignment for roaming mobile clients.



When Client Match is enabled on 802.11n capable APs, 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 APs do not support the legacy band steering, station hand off or load balancing settings, so these APs 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 > Wireless > 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 AP 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 APs.
Balance Bands	Allows the AP 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 2.4GHz 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 APs with active clients. When the Client Match mode is set to Disabled , an AP may change to a more optimal channel, which disrupts current client traffic. The Client Aware option is Enabled by default.

Data pane item	Description
Scanning	Allows the AP 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 AP, 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 AP 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 AP 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 AP spends on PHY processing.

Data pane item	Description
	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.
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 AP, it is automatically enabled for all SSIDs configured on an AP. By default, VHT is enabled on all SSIDs. NOTE: If you want the 802.11ac APs to function as 802.11n APs, 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 APs and clients. It also logs information about the unauthorized APs 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, APs 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.



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 Central section describes the authentication and security parameters to configure on an AP provisioned in :

- [Supported Authentication Methods on page 78](#)
- [Supported Authentication Servers on page 81](#)
- [Configuring External Servers for Authentication on page 83](#)
- [Configuring Authentication Parameters for AP Management Users on page 85](#)
- [Configuring AP Users on page 86](#)
- [Configuring Roles and Policies for User Access Control on page 87](#)
- [Configuring ALG Protocols on page 93](#)
- [Blacklisting Clients on page 93](#)

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 APs 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 AP. The wireless client can pass data traffic only after successful 802.1X authentication.



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 > Wireless > 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 AP 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 AP 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 > Wireless > 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 > Wireless > Networks**, 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 59](#).

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 Profiles for Guest Network 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 AP assigns the default WISPr user role to the client when your ISP sends an authentication message to the AP.

APs 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 AP.

Configuring WISPr Authentication

To configure WISPr authentication, complete the following steps:

1. Click **Configuration > Wireless > 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 AP, 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>).



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 > Wireless > 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, AP 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 AP 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 AP 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 AP 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 AP has an instance of free RADIUS server operating locally. When you enable the internal RADIUS server option for the network, the client on the AP 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 AP. 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.



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

Authentication Termination on AP

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 AP 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 APs to perform load balancing of authentication requests destined to authentication servers such as RADIUS or LDAP.

The load balancing in AP 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 > Wireless > 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:

Table 32: Authentication Server Configuration

Type of Server	Parameters
RADIUS	Configure the following parameters: ■ Name—Name of the external RADIUS server. ■ IP Address—IP address or the FQDN 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 AP 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 AP. 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 AP 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. ■ 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

Type of Server	Parameters
	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. ■ Dead Time (in mins)—Specify a dead time for authentication server in minutes. When two or more authentication servers are configured on the AP 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.
Change of Authorization Only	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.



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 AP Management Users

You can configure RADIUS or TACACS authentication servers to authenticate and authorize the management users of an AP. 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 APs 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 > Wireless > System > Administrator** and configure the following parameters:

Table 33: Configuration Parameters for the AP 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

Type of the User	Authentication Options	Steps to Follow
		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 83.
	TACACS accounting	If a TACACS server is selected, enable TACACS accounting to report management commands if required.
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 AP Users

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.

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



The local user database of APs can support up to 512 user entries except IAP-92/93. IAP-92/93 supports only 256 user entries. If there are already 512 users, IAP-92/93 will not be able to join the cluster.

In the Central UI

To configure users:

1. Click the **Configuration > Wireless > Security**.

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 user names that you want to delete
 - b. Click **Delete All**.
 - c. Click **OK**.



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

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 APs 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 AP. 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 AP 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.



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.

For more information on roles and policies, see the following topics:

- [Configuring Access Rules for Network Services on page 88](#)
- [Configuring User Roles on page 90](#)
- [Configuring Derivation Rules on page 90](#)
- [Managing Inbound Traffic on page 92](#)

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 Analytics on page 126](#).
- Configuring access rules based on web categories and web reputation, see [Configuring Web Policy Enforcement on page 127](#).

To configure access rules, complete the following steps:

1. Select **Configuration > Wireless > 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 > Wireless > Networks > Create a New Network > Access** page.
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 34: 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 APs 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 93 .
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: ■ 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 73 .
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 AP involves the following procedures:

- [Creating a User Role on page 90](#)
- [Assigning Bandwidth Contracts to User Roles on page 90](#)

Creating a User Role

To create a user role, complete the following steps:

1. Select **Configuration** > **Wireless** > **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**.



You can also create a user role when configuring wireless profile. For more information, see [Configuring Access Rules on page 59](#).

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 AP) or downstream (AP 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** > **Wireless** > **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 Rules 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.



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 > Wireless > 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 82](#).
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 > Wireless > 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 Firewall Settings for Protection from ARP Attacks

To configure firewall settings, complete the following steps:

1. Select **Configuration > Wireless > 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 AP 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 > Wireless > 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 AP, including clients connected to a slave AP.

To configure restricted corporate access, complete the following steps:

1. Select **Configuration > Wireless > 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 > Wireless > 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**.



When the protocols for the ALG are **Disabled** the changes do not take effect until the existing user sessions have expired. Reboot the AP 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 AP 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 > Wireless > Security > Blacklisting**.
2. Click + 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 AP.

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 > Wireless > 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 Blacklisted Time**, enter the duration after which the clients can be blacklisted due to an ACL rule trigger.



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 57](#).

Configuring VPN Networks

This section describes the following VPN configuration procedures:

- [VPN Features on page 94](#)
- [Configuring VPN Tunnels on page 95](#)
- [Configuring Routing Profiles on page 98](#)

VPN Features

As APs use a Virtual Controller architecture, the AP 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 AP networks at branch locations or data centers, where the Aruba controller acts as a VPN concentrator.

When the VPN is configured, the AP 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 AP 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

APs support the following VPN protocols for remote access:

Table 35: *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 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 AP MAC addresses to the whitelist database stored on the controller or an external server. IPsec supports Local, L2, and L3 modes of IAP-VPN operations. NOTE: The APs 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. APs support the configuration of L2 GRE (Ethernet over GRE) tunnel with an ArubaController to encapsulate the packets sent and received by the AP. You can use the GRE configuration for L2 deployments when there is no encryption requirement between the AP and controller for client traffic. APs 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 AP, 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 AP 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: APs support manual and Aruba GRE configuration only for L2 mode of operations. Aruba GRE configuration is supported only with Aruba Controllers.
L2TP	The Layer 2 Tunneling Protocol version 3 (L2TPv3) feature allows AP 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 AP 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

AP 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 AP to enable communication with a controller in a remote location:

- [Configuring IPsec Tunnel on page 95](#)
- [Enabling Automatic Configuration of GRE Tunnel on page 96](#)
- [Configuring GRE Tunnel Manually on page 97](#)
- [Configuring an L2TPv3 Tunnel on page 98](#)

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 > Wireless > 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 AP 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 AP 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 AP can verify if an active VPN connection is available. The default value is 5 seconds, which means that the AP 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 AP 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 AP are encrypted.

Enabling Automatic Configuration of GRE Tunnel

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

1. Click the **Configuration > Wireless > 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 AP 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 AP 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 AP can verify if an active VPN connection is available. The default value is 5 seconds, which means that the AP 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 AP 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 AP to the VPN/GRE Endpoint rather than the tunnels created just from the master AP. When enabled, the traffic to the corporate network is sent through a Layer-2 GRE tunnel from the AP itself and need not be forwarded through the master AP.

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 AP 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 AP IP to create the GRE tunnel at the controller side depending upon the following AP 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 AP IP is used to create the GRE tunnel.

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

1. Click the **Configuration > Wireless > 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 AP to the VPN/GRE Endpoint rather than the tunnels created just from the master AP. When enabled, the traffic to the corporate network is sent through a Layer-2 GRE tunnel from the AP itself and need not be forwarded through the master AP.



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

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

Configuring an L2TPv3 Tunnel

The Layer 2 Tunneling Protocol version 3 (L2TPv3) feature allows AP 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 AP 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 > Wireless > 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 > Wireless > 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 99](#)
- [Configuring DHCP Server for Client IP Assignment on page 103](#)

Configuring DHCP Scopes

The VC supports the following types different modes of DHCP address assignment:

- [Configuring Distributed DHCP Scopes on page 99](#)
- [Configuring a Centralized DHCP Scope on page 100](#)
- [Configuring Local DHCP Scopes on page 102](#)

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 36: *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 discontinuous 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 AP 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 AP 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 > Wireless > 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 37: 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 APs to intercept the broadcast packets and relay DHCP requests.
Helper Address	Enter the IP address of the DHCP server.
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**.



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 AP.

Table 38: *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 DHCP Scopes

You can configure the following types of local DHCP scopes on an AP:

- **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 AP 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 AP.
- **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 AP routes the packets sent by clients on its uplink. This DHCP assignment mode is used with the L3 forwarding mode.

To configure a new local DHCP scope, complete the following steps:

1. Select **Configuration > Wireless > 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 39: *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 AP. 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.

Table 39: Local DHCP configuration parameters

Data pane item	Description
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 , 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 Name	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.

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 AP automatically determines a suitable DHCP pool for **Virtual Controller Assigned** networks. The AP typically selects the 172.31.98.0/23 subnet. If the IP address of the AP is within the 172.31.98.0/23 subnet, the AP 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 > Wireless > 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.



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.

Configuring Services

This section describes how to configure AirGroup, location services, Lawful Intercept, OpenDNS, and Firewall services.

- [Configuring AirGroup Services on page 104](#)
- [Configuring an AP for RTLS Support on page 105](#)
- [Configuring an AP for ALE Support on page 105](#)
- [Managing BLE Beacons](#)
- [Configuring OpenDNS Credentials on page 106](#)
- [Configuring CALEA Server for Lawful Intercept Compliance on page 106](#)
- [Integrating a Third-Party Network Firewall on page 107](#)
- [Enabling AppRF™ Service on page 108](#)

Configuring AirGroup Services

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 AirGroup solution 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 Virtual Controller.

AirGroup Features

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.

For more information on AirGroup solution, see *Aruba Instant User Guide*.

AirGroup Services

Bonjour supports zero-configuration services. The services are pre-configured 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 AP clients:

- AirPlay — Apple AirPlay allows wireless streaming of music, video, and slide shows 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 > Wireless > Services > AirGroup**.
2. Select the **AirGroup** check box. The **AirGroup** configuration parameters are displayed.
3. To allow the users to use AirGroup services enabled in a guest VLAN, select the **Guest Bonjour 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.
4. Select **AirGroup Across Mobility Domains** to enable Inter cluster mobility.
5. Select required services. To allow all services, select **Allow All**.
6. 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 AP. 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 AP 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 AP cluster.
7. To enable DLNA support, select the **DLNA** check box and select the DLNA services such as AmazonTV, Google Cast, DLNA print or media. DLNA is a network standard derived from UPnP, which enables devices to discover the services available in a network. DLNA also provides the ability to share data between the Windows or Android-based multimedia devices.
8. Click **Save Settings**.

Configuring an AP for RTLS Support

Central supports the real time tracking of devices. With the help of the RTLS, the devices can be monitored in real time or through history.

To configure RTLS, complete the following steps:

1. Select **Configuration > Wireless > Services > Real Time Locating System**.
2. Select **Aruba RTLS** to send the RFID tag information to the Aruba RTLS server.
3. Click **3rd Party** and select **Aeroscout** to send reports on the stations to a third-party server.
4. Specify the IP address and port number of the RTLS server, to which location reports must be sent.
5. If **Aruba RTLS** is selected, enter the passphrase required for connecting to the RTLS server.
6. Select **Include Unassociated Stations** to send reports on the stations that are not associated to any AP.
7. Click **Save Settings**.

Configuring an AP for ALE 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 AP sends client information and all status information to the ALE server.

To integrate AP with ALE, the ALE server address must be configured on an AP. 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 AP

To configure an AP for ALE support:

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

Configuring CALEA Server for 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, Service Providers are required to ensure LI compliance based on Communications Assistance for Law Enforcement Act (CALEA) specifications.

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



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

For more information on the communication and traffic flow from an AP to CALEA server, see *Aruba Instant User Guide*.

Configuring CALEA Server Details on an AP

To enable an AP to communicate with the CALEA server, complete the following steps:

- [Creating a CALEA Profile](#)
- [Creating an Access Rule for CALEA](#)

Creating a CALEA Profile

You can create a CALEA profile by using Central.

1. Click **Configuration** > **Wireless** > **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, open an SSID.
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**.

Integrating a Third-Party Network Firewall

APs maintains the network (such as mapping IP address) and user information for its clients in the network. To integrate the AP network with a third-party network, you can enable an AP to provide this information to the third-party servers.

To integrate an AP with a third-party network, you must add a global profile. This profile can be configured on an AP with information such as IP address, port, user name, password, firewall enabled or disabled status.

Configuring an AP for Network Integration

To configure an AP for network integration:

1. Select **Configuration** > **Wireless** > **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 application details for the clients associated with an AP, you must enable the AppRF service.

To enable AppRF, complete the following steps:

1. Navigate to **Configuration > Wireless>Services**.
2. Click **AppRF™** and then select the **Deep Packet Inspection** check box.

For more information on AppRF, see [Application Visibility on page 123](#).

Configuring Uplinks

This section provides the following information:

- [Uplink Interfaces on page 108](#)
- [Uplink Preferences and Switching on page 114](#)

Uplink Interfaces

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

[Figure 2](#) illustrates a scenario in which the APs join the Virtual Controller as slave APs through a wired or mesh Wi-Fi uplink:

Figure 2 *Uplink Types*



The following types of uplinks are supported on Central:

- [3G/4G Uplink](#)
- [Ethernet Uplink on page 112](#)
- [Wi-Fi Uplink on page 113](#)

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 40: *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)
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))

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

Table 40: *List of Supported 3G Modems*

Modem Type	Supported 3G Modems
	■ 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)) ■ 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 41: *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 **Configuration > Wireless > System**.
2. 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.

3. 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.

4. Click **OK**.

5. Reboot the AP for changes to affect.

Ethernet Uplink

The Ethernet 0 port on an AP is enabled as an uplink port by default. The 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 AP 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 AP for the configuration to take effect. The PPPoE connection is dialed after the AP comes up. The PPPoE configuration is checked during AP 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 > Wireless > 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 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 AP.

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

Wi-Fi Uplink

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

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



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 AP.
- If Wi-Fi uplink is used on the 5 GHz band, mesh is disabled. The two links are mutually exclusive.

To provision an AP with Wi-Fi Uplink, complete the following steps:

1. If you are configuring a Wi-Fi uplink after restoring factory settings on an AP, connect the AP to an Ethernet cable to allow the AP to get the IP address. Otherwise, go to step 2.
2. Select **Configuration > Wireless > 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



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**.

Uplink Preferences and Switching

This topic describes the following procedures:

- [Enforcing Uplinks on page 114](#)
- [Setting an Uplink Priority on page 114](#)
- [Enabling Uplink Pre-emption on page 114](#)

Enforcing Uplinks

The following configuration conditions apply to the uplink enforcement:

- When an uplink is enforced, the AP 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 AP 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 AP 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 AP tries to find an available uplink based on the priority configured. If current uplink is active, the AP 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 AP, complete the following steps:

1. Select **Configuration > Wireless > 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 AP.

Setting an Uplink Priority

To set an uplink priority:

1. Select **Configuration > Wireless > 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 AP 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 AP 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 > Wireless > >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 AP 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 AP switches to a different connection.

To configure uplink switching, complete the following steps:

1. Select **Configuration > Wireless > 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**.



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

Mobility and Client Management

This section provides the following information on layer-3 mobility for AP clients:

- [Layer-3 Mobility for AP Clients on page 115](#)
- [Configuring L3 mobility domain on page 116](#)

Layer-3 Mobility for AP Clients

APs 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 APs in a given Central network can roam to APs 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.

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 AP cluster.

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.

Aruba recommends 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.

To configure L3 mobility domain, complete the following steps:

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**.

Configuring 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.

To configure an enterprise domain, complete the following steps:

1. Select **Configuration > Wireless > 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.

Configuring SNMP Parameters

This section provides the following information:

- [SNMP Configuration Parameters on page 117](#)
- [Configuring Community String for SNMP on page 117](#)
- [Configuring SNMP Traps on page 118](#)

SNMP Configuration Parameters

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

You can configure the following parameters for an AP:

Table 42: *SNMP parameters*

Data Pane Item	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 AP, 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 **Configuration > Wireless > System > SNMP**.
2. Click +.
3. Enter the string in the **New Community String** text box.

4. Click **OK**.
5. 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 **Configuration > Wireless > System > SNMP**.
2. Click + in the **Users for SNMPV3** box. A window for specifying SNMPv3 user information is displayed.
3. Enter the name of the user in the **Name** text box.
4. Select the type of authentication protocol from the **Auth protocol** drop-down list.
5. Enter the authentication password in the **Password** text box and retype the password in the **Retype** text box.
6. Select the type of privacy protocol from the **Privacy protocol** drop-down list.
7. Enter the privacy protocol password in the **Password** text box and retype the password in the **Retype** text box.
8. Click **OK**.
9. To edit the details for a particular user, select the user and click **Edit**.
10. To delete a particular user, select the user and click **Delete**.

Configuring SNMP Traps

Central supports the configuration of external trap receivers. Only the AP 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 + 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 Logs and TFTP Dump Servers

This section provides the following information:

- [Configuring a Syslog Server on page 119](#)
- [Configuring TFTP Dump Server on page 119](#)

Configuring a Syslog Server

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

1. Select **Configuration > Wireless > System > Logging**.
2. In the **Syslog Server** box, enter the IP address of the server to which you want to send system logs.
3. 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 AP 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 43: *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.

4. Click **Save Settings**.

Configuring TFTP Dump Server

To configure a TFTP server for storing core dump files, complete the following steps:

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

Resetting an AP

You can reset the system configuration of an AP by erasing the existing configuration on the AP. To erase the existing configuration on an AP, perform any of the following procedures:

Clearing AP 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 AP that you want to reset, under the new group. After the AP is moved to a new group, the configuration on the AP is erased and the default group configuration is pushed to the AP. However, in this procedure, only the system configuration is cleared and the **Per AP Settings** on the AP are retained.

Resetting an AP through the Console

To reset an AP from the IAP console, complete the following steps:

1. Log in to the AP console. To access the AP console, select **Monitoring > Access Points** and click the AP to reset.
2. Click **Console Access**.
3. Execute the **write erase all** command at the command prompt.
4. Reboot the AP. With this procedure, the complete configuration including the **Per AP Settings** on the AP is reset.

After the reboot, the AP is moved to default group and will not be present in the group to which it was previously attached.

For information on resetting an AP to factory default configuration by using the reset button on the device, see *Aruba Instant User Guide*.

Uploading and Mapping AP Certificates

When an AP joins a group that does not have a certificate, the AP's existing certificate is retained. When an AP joins a group that already has a certificate, the AP's certificate is overwritten by the group's certificate.

This section provides the following information:

[Uploading Certificate for an AP on page 120](#)

[Mapping AP Certificate on page 122](#)

Uploading Certificate for an AP

You can upload a CA certificate or a Server certificate for an AP from the Central UI. When a certificate is uploaded at group level, the same certificate can be used for different groups, devices, or templates.

To upload a certificate for an AP, perform any of the following procedures:

Uploading a CA Certificate

To upload a CA certificate for an AP, complete the following steps:

1. Select a group from the Group selector at the header pane in the main window.
2. Select **Configuration > Security**.
3. Click **Certificate**. The Certificate Store pane with a list available certificates is displayed.
4. Click **Add** available under the Certificate Store pane. The Add Certificate dialog box is displayed.
5. Enter the certificate name in the **Name** text box. The certificate name can be up to 64 characters.

6. Select the certificate format from the **Format** drop-down list. For CA certificate, PEM or DER format is applicable.
7. Select **CA Certificate** from the **Type** drop-down list.
8. Click **Choose File** to browse to the location and select the certificate.
9. Click **Save**.

Uploading a Server Certificate

To upload a Server certificate for an AP, complete the following steps:

1. Select a group from the Group selector in the header pane of the main window.
2. Select **Configuration > Security**.
3. Click **Certificate**. The Certificate Store pane with a list available certificates is displayed.
4. Click **Add** available under the Certificate Store pane. The Add Certificate dialog box is displayed.
5. Enter the certificate name in the **Name** text box.
6. Select the certificate format from the **Format** drop-down list. For Server certificate, PEM or PKCS12format is applicable.
7. Select **Server Certificate** from the **Type** drop-down list.
8. Type a passphrase in the **Passphrase** text box. Confirm this passphrase in the **Retype Passphrase** text box.
9. Click **Choose File** to browse to the location and select the certificate.
10. Click **Save**

Uploading a Custom Certificate for Cloud Guest Services

To upload a custom certificate in Central for Cloud Guest Services, perform the steps listed in Phase 1 and Phase 2.

Phase 1

To upload a custom certificate for Cloud Guest Services, complete the following steps:

1. Select a group from the Group selector in the header pane of the main window.
2. Select **Configuration > Security**.
3. Click **Certificate**. The Certificate Store pane with a list available certificates is displayed.
4. Click **Add** available under the Certificate Store pane. The Add Certificate dialog box is displayed.
5. Enter the certificate name in the **Name** text box.
6. Select the certificate format from the **Format** drop-down list.
7. Select **Cloud-Guest-portal** from the **Type** drop-down list.
8. Click **Choose File** to browse to the location and select the certificate.
9. Click **Save**.
10. In the **Certificate Usage** section, select the certificate in the **Captive Portal** category.

After uploading and mapping the custom certificate, Central will push the certificate to all APs in that group.

Phase 2



This phase is only required for the current release until the customers are allowed to configure CName as part of the configuration.

1. To activate new certificate for Cloud Guest Service, customer must open a TAC ticket.

2. The TAC team must open a Redmine ticket for the customer ID to activate the new uploaded certificate for Cloud Guest Service. The steps are mentioned in Redmine ticket number 44112, which is available in the path <https://redmine1.lab1.arubathena.com/issues/44112>.
3. The customer must email the TAC ticket number to hpe-aruba-cloud-devops@hpe.com.

Mapping AP Certificate

You can view the mapping of an AP certificate to the certificate type from the Central UI.

If a certificate is mapped to a device, the certificate cannot be deleted.

Viewing AP Certificate Mapping

To view the mapping of an AP certificate to a specific certificate type or category, perform the following steps:

1. Select a group from the Group selector in the header pane of the main window.
2. Select **Configuration > Security**.
3. Click **Certificate**. The Certificate Store pane with a list of available certificates is displayed.
4. Select a certificate name from the list.
5. The selected certificate name is displayed in one of the drop-down lists under **Certificate Usage**. The drop-down lists that are available are CA, Auth Server, Captive Portal, Radsec, and Radsec CA.

Mapping AP Certificate

To map an AP certificate name to a specific certificate type or category, complete the following steps:

1. Select a group from the Group selector in the header pane of the main window.
2. Select **Configuration > Security**.
3. Click **Certificate**. The Certificate Store pane with a list of available certificates is displayed.
4. Select a certificate name from the list.
5. The selected certificate name is displayed in one of the drop-down lists under **Certificate Usage**. The drop-down lists that are available are CA, Auth Server, Captive Portal, Radsec, and Radsec CA .
6. If you want to change the certificate for specific certificate type, select the required certificate from the corresponding drop-down list.

AppRF is a custom built Layer 7 firewall capability supported for APs 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.

APs 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.



The Deep Packet Inspection feature is supported on AP 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.

For more information on DPI and application analytics, see the following topics:

- [Application Visibility on page 123](#)
- [Configuring ACL Rules for Application Analytics on page 126](#)
- [Configuring Web Policy Enforcement on page 127](#)
- [Creating Custom URLs for Redirection on page 129](#)

Application Visibility

The **AppRF** option under the **Monitoring** tab provides a detailed information on application usage. 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](#).

Application Visibility is supported for APs 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-224/225, IAP-274/275, IAP-228, IAP-277, IAP-205, IAP-214, and IAP-324/325 devices. The AP-104/105, AP-134/135, RAP3WNP, and AP-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 Analytics](#) 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.

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.

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.

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.

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.

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.

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.



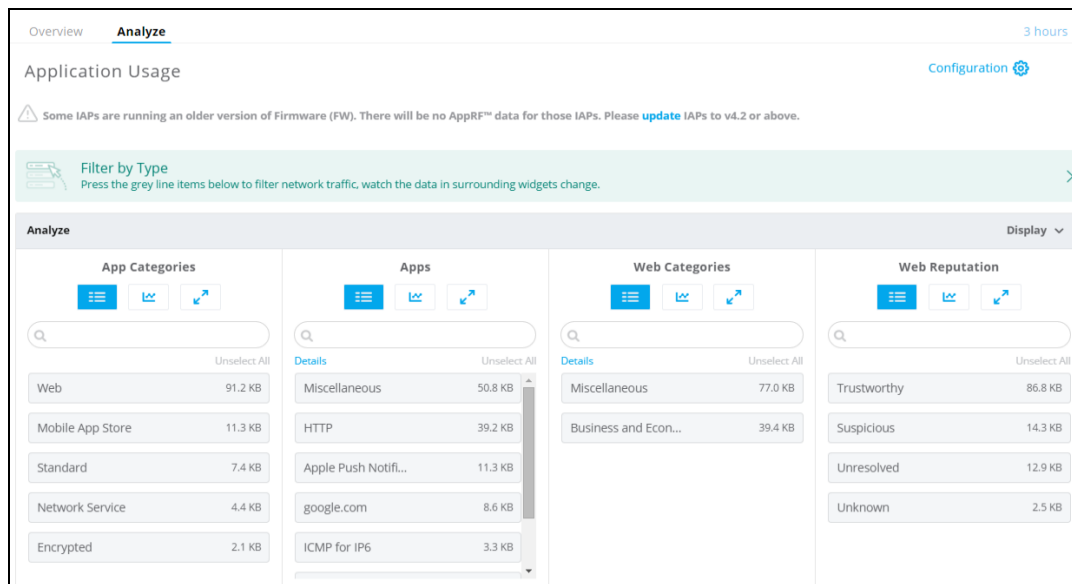
The **SSID, Device Type, and User Role** widgets are not displayed by default. These can be displayed by selecting them from the **Display** drop-down list.

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 3 *Analyze Tab Dashboard*

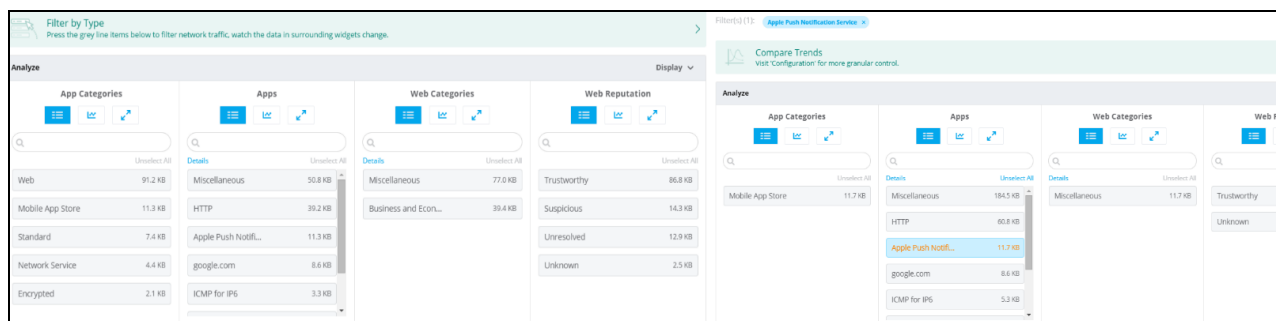


Filter

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 4](#) shows the data without filters and data with filters on:

Figure 4 *Data Without Filter And With Filter*



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 44: *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 45: *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 Analytics

This section describes the procedure for configuring access rules for application analytics. For information on configuring access rules based on web categories and web reputation, see [Configuring Web Policy Enforcement on page 127](#).

To configure ACL rules for a user role, complete the following steps:

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 46: 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 APs 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 93 .
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 ARRM scanning is enabled, For more information, see Configuring Radio Parameters on page 73 .
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 802.1p 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 APs 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 93](#).
 - **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 73](#).
 - **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.
 - **802.1p priority**—Select this check box to enable 802.1p 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.



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 APs 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 APs running 6.2.1.0-4.1 to the newly created group. If application rules are configured in this group, ensure that the APs with versions lower than 6.2.1.0-4.1 are not moved to that group.

Creating Custom URLs for Redirection

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 > Wireless > 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 > Wireless > 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.

This chapter describes the procedure for configuring Switches. For more information on Switch configuration, see the following topics:

- [Aruba Switches on page 130](#)
- [Configuring Switch Parameters on page 131](#)
- [Configuring Ports on page 131](#)
- [Configuring Access Policies](#)
- [Configuring VLANs on page 133](#)
- [Configuring DHCP Pools on page 134](#)
- [Adding CLI Snippets](#)
- [Configuring System Parameters for a Switch on page 135](#)

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
- Aruba 2540 Switch Series
- Aruba 3810 Switch Series

Supported Firmware Versions

Central supports the following firmware versions on Aruba switches:

- Aruba 2920 Switch Series—WB.16.02.0012 or later
- Aruba 2930F Switch Series—WC.16.02.0012 or later
- Aruba 2540 Switch Series—YC.16.02.0012 or later
- Aruba 3810 Switch Series—WB 16.03.0003 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 47: *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.

Configuring Ports

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 48: *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.
Power over Ethernet	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 49: *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.
Power over Ethernet	Displays the enabled or disabled status of Power over Ethernet (PoE).
Access Policy (In)	Allows you to apply an existing access policy for the inbound traffic on the port.
Access Policy (Out)	Allows you to apply an existing access policy for the outbound traffic on the port.

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.

Adding 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 add a VLAN, 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. Click + add a VLAN and configure the following parameters:
 - **ID**—The 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.
 - **DHCP**—Slider for enabling DHCP pool associated with the VLAN.
 - **Access Policy (In)**—Access policy assignment to VLAN for the inbound traffic (vlan-in). The VLAN-IN rule is applied for the bridged and routed inbound packets on a VLAN.
 - **VLAN Port Mode**—Port mode to apply on the VLAN. To apply a port, complete the following steps:
 - a. Select the port number.
 - b. Select any of the following port modes:
 - **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.
 - c. Click **Apply**.
4. Click **OK**.

Editing the VLAN Details

To edit the VLAN details, select the VLAN row and click the edit icon.

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.



VLAN 1 is the primary VLAN and cannot be deleted.

Configuring DHCP Pools

To configure a new DHCP pool on a switch, complete the following steps:

1. To configure a DHCP pool on a Mobility Access Switch, click **Configuration > Switch-MAS > DHCP Pools**.

To configure a DHCP pool on other Aruba switches, click **Configuration > Switch-Aruba > DHCP Pools**.

DHCP is supported only on Aruba Switches running the following versions:

- Aruba 2920 Switch Series—WB.16.02.0012 or later
- Aruba 2930F Switch Series—WC.16.02.0012 or later
- Aruba 2540 Switch Series—YC.16.02.0012 or later

If any of the devices is running a lower version, a warning message is displayed, and the DHCP configuration changes are pushed only to the devices that support the DHCP. If the devices are upgraded to a supported version or moved out of the group, the warning message will not be displayed.

2. To activate the DHCP service, select the **Enable DHCP service** check box. The DHCP service can be enabled only if there is a valid DHCP pool.
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**—A valid network IP address to assigned to the DHCP pool.
- **Netmask**—Netmask of the DHCP pool.
- **Lease Time**—The lease time for the DHCP pool in days-hours-minutes format. You can set a maximum value of 365 days 23 hours and 59 minutes in the DD-HH-MM format.
- **Default Router**—IP address of the default router in the subnet. You can add up to 8 IP addresses.
- **DNS Server**—Address of the DNS server. To add multiple DNS servers, click +. You can add up to 8 DNS servers.
- **WINS Server**—Address of the WINS server. The WINS server address is required for legacy Aruba switches only. To add multiple WINS servers, click +.
- **Netbios server**—Address of the Netbios server. The Netbios server address configuration is not required for legacy Aruba switches. To add multiple WINS servers, click +. You can add up to 8 Netbios servers.
- **IP address Range**—IP address range within the network and network mask combination.
- **Exclude Address Range**—IP address range to exclude. This field is available for legacy Aruba Switches such as Mobility Access Switches. To add multiple excluded address range, click +.

- **Option**—The code and type of the DHCP option to configure. A value within the range of 2-254 with type as hexadecimal and ASCII is valid.
 - **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**.

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 136](#)
- [Managing Reports on page 136](#)
- [Viewing a Generated Report on page 138](#)
- [Creating a Report on page 139](#)

Generated Reports

On clicking the **Generated Reports**, a table listing the parameters used for generating a report is displayed.

Table 50: *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 51: Report Parameters

Report Type	Parameters Displayed
All	Displays all scheduled and generated reports.
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 (Tx/Rx) ■ Top Ten Ports By Usage (Tx/Rx) ■ 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 ■ 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 the inventory and subscription information for the devices that are online during a specific duration. The report includes the following details: ■ Number of APs ■ Number of Switches ■ AP interfaces summary ■ Model and Firmware version for APs

Report Type	Parameters Displayed
	■ Model and Firmware version for Switches ■ AP and Switches subscription information ■ Subscription utilization graph
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.
New Infra Inventory	Displays the inventory and subscription information to the devices that are newly added in Central.
Capacity Planning	Displays the throughput and client density information for devices provisioned in Central. The report includes the following details: ■ Top 25 APs by throughput ■ Top-25 APs by peak client density ■ Top-25 APs by average client density ■ Top-25 Switches by throughput ■ Subscription usage
AppRF	Displays application usage report for a specific device group. The report displays the following widgets: ■ Top 10 applications accessed by the clients ■ Top 10 web categories accessed by the clients ■ Top 10 applications accessed by each type of the client device. ■ Top 10 applications for the user roles assigned to the client devices. ■ Top 10 applications for the SSIDs on which the client devices are connected.
Client Session	Displays the details of client sessions for the SSIDs provisioned on APs. The report also displays the client count, the number of sessions, cumulative duration, and the usage based on the following parameters : ■ Client Device OS ■ Connection mode ■ SSIDs ■ User roles ■ MAC address vendors of the device
RF Health	Displays the following RF usage statistics for the AP radios. ■ Channel changes ■ Transmission power changes ■ Average Noise (in dBm) ■ Average channel utilization (%) ■ Total error (%) ■ Interfering devices ■ Clients ■ Usage

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
- New Infra Inventory
- Capacity Planning
- Client Session
- RF Health

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. If you are creating a PCI Compliance report, specify the Cardholder Data Environment (CDE) subnets or CDE SSIDs for which you want to generate the report. You can also run report on all SSIDs.
8. Select a group from **Device Groups**. If no group is selected, the report is generated for all groups.
9. To send the report through email, select **Email Report**, enter email address, and then click **Create**.

The **Maintenance** tab displays the maintenance pane for the Central. The **Maintenance** pane consists of the following menu options:

- [Maintaining Firmware Versions](#)
- [Managing User Accounts](#)
- [Viewing Audit Trails](#)
- [Troubleshooting Devices](#)
- [API Gateway](#)

Maintaining Firmware Versions

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.

Viewing Firmware Details

To view the firmware details for devices provisioned in Central, go to **Maintenance > Firmware**. The **Firmware** window opens and displays the following information:

Table 52: *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 AP device ■ Firmware Version—The firmware version on the AP ■ Status—The upgrade status of the AP
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	
Filter by Upgrade Status	Filters the device list based on firmware upgrade status.
Update Firmware	Allows you to upgrade the device firmware to the latest supported version. For more information, see Automatically Upgrading Firmware on a Device on page 141 .

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.



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**.



After upgrading a switch, click **Reboot**.

Managing User Accounts

The **User Management** pane in the Central UI provides details of the user such as username, user scope, access level, and allows you to add, edit or delete users.



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 142](#).

When **Support Access** is set to on, the Aruba support team 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.



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 Devices to Central on page 19](#).
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.



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.

Viewing Audit Trails

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 AP and Switches. In the current release, the Audit Trail logs are displayed for the following operations only:

- Device status and configuration
- Firmware upgrade
- Device assignment to subscriptions and groups
- Label assignment to devices
- User addition and deletion

The **Audit Trail** page displays a table with the following details:

Table 53: *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 subscription 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, manage 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**.

Adding a New Token

To add a new token, complete the following steps:

1. Click **Maintenance > API Gateway**. The **API Gateway** page is displayed.
2. Click **Authorized Apps & Tokens**.
3. Click + to add a new token.
4. Enter the application name and then click **Generate**.

Troubleshooting Devices

This section includes the following topics:

- [Troubleshooting Overview](#)
- [Troubleshooting a Device](#)

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.



If you want to run the troubleshooting commands on an AP, ensure that the AP is upgraded to 6.4.3.1-4.2.0.3 or later firmware versions.

Troubleshooting a Device

To run troubleshooting commands on a device, complete the following steps

1. Click **Maintenance > Troubleshooting**. The **Troubleshooting** page opens.
2. Select the device category. [Table 54](#) describes the contents of the **Troubleshooting** page:

Table 54: *Contents of the Troubleshooting Page*

Data Pane Item	Description
Switches	Allows you to run the troubleshooting commands on a Switch.
Access Points	Allows you to run the troubleshooting commands on an AP.
AP Name	Allows you to select the 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.
Switch Name	Allows you to specify the devices for troubleshooting.
Tools	Allows you to run commands such as Ping and Traceroute from the UI. To execute a command, complete the following steps: 1. Select the type of the command to run from the Tools drop-down. 2. Specify the host name or the IP address of the device on which you want to run the command. 3. Click the command name.
Commands	Category—Allows you to select a category. The troubleshooting commands are segregated under the following categories: Access Points ■ Wireless ■ Security ■ Network ■ AirGroup ■ System ■ ARM ■ Datapath ■ Logs ■ AirWave Switches ■ Physical Connection ■ PoE and Media Access ■ L2 loop prevention ■ Link aggregation ■ Loop detection ■ Routing ■ Management ■ Security and traffic ■ Show tech 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.

Table 54: *Contents of the Troubleshooting Page*

Data Pane Item	Description
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 AP from the list of devices in the Output pane.

4. To troubleshoot an AP, click the **Access Points** tab, specify the AP name. 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.
5. To troubleshoot a Switch, click the **Switches** tab and specify the name of the Switch.
6. Select a category and the commands to run under that category.
7. To run commands from a different category, select another category and the commands grouped under that category.
8. Click **Run**. The command output is displayed.
9. To set a frequency for automatically running the troubleshooting commands, perform the following actions:
 - a. Click **Auto Run**.
 - b. Specify the interval within a range of 30 seconds to 1 hour.
 - c. Select the duration for running the troubleshooting commands within a range of 1 minute to 1 hour.
 - d. Click **Start**.

This section describes the Presence Analytics application:

- [Presence Analytics Overview on page 149](#)
- [Configuring Sites on page 149](#)
- [Configuring APs for Presence Analytics on page 150](#)
- [Using the Presence Analytics App on page 150](#)
- [Analyzing User Traffic Presence on page 150](#)
- [Setting RSSI Threshold and Dwelling Time on page 151](#)

Presence Analytics Overview

Central supports the Presence Analytics application to provide a solution for analyzing user traffic patterns in public venues and enterprise environments. Using this feature, various businesses can analyze user traffic and 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.

The Presence Analytics application is available only if the Presence Analytics service subscription is enabled on any one AP. If the Presence Analytics subscription is enabled on an AP, the configuration changes are applied. If the subscription is disabled, the Presence Analytics application is disabled on the AP. To start using the Presence Analytics application service, contact your administrator or the Aruba Central Support team and obtain a subscription.

Central provides an analytics dashboard view of the data aggregated from the APs. When the Presence Analytics service is enabled on the APs deployed in the network, Central receives the RSSI feeds on the user traffic presence from the APs. The administrators can create labels for venues and assign these labels to the APs.

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 specific site and has an RSSI value greater than or equal to configured value for the RSSI threshold.
- **Visitor**—A client who spends at least 2 minutes at the site. The traffic presence for such a user must be equal to or more than the RSSI threshold value set in the **Presence Analytics > 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 Analytics > Settings** page.



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 Sites

Sites refer to the locations or venues in which the user traffic presence is detected. For Presence Analytics, you can create labels for sites and assign these sites to the APs. For more information on creating labels, see [Labels on page 153](#).

In the **Presence Analytics** application view, the sites configured in Central are listed under **All Sites**. The user traffic presence analysis applies only if the sites are distributed across different locations.

Configuring APs for Presence Analytics

Central supports the Presence Analytics feature for AP deployments only. This feature is supported only on the APs running firmware versions 6.4.4.4-4.2.3.0 or later.

To allow Central to receive RSSI feeds from the APs, the RSSI feed parameter must be enabled on the AP. To enable RSSI feeds, complete the following steps:

1. Click **Configuration > Access Points > Services**. The **Services** pane is displayed.
2. Expand **Presence Analytics**.
3. For **RSSI Report Interval**, specify an RSSI reporting interval within a range of 5–300 seconds. By default, the interval is set to 60 seconds.
4. For **Report RSSI Threshold**, specify a value for the RSSI threshold. The AP sends an RSSI feed when the clients exceed the configured RSSI threshold value. By default, the RSSI threshold value is set to 0 dBm.
 - For APs running 6.5.1.0-4.3.1.0, you can set a value within the range of 0–100 dBm. When set to 0 dBm, the AP reports the RSSI data of all clients to Central. When set to 20 dBm, the AP sends a report for all clients whose RSSI value is in the range of 20–100 dBm.
 - For APs running 6.5.0.0-4.3.0.x or a lower firmware version, Aruba recommends that you set a value of 100 dBm.



Ensure that the RSSI threshold value is not set to 0 dBm for APs running 6.5.0.0-4.3.0.x or a lower firmware version.

5. Click **Save Settings**.

Using the Presence Analytics App

The **Presence Analytics** app under **Aruba Central Apps** area in the left navigation pane of the 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 55: Monitoring Dashboard for Presence Analytics

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 Sites 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 engaged clients in a site 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 at a site.
Insights	The Insights dashboard displays the trends for top 5 and bottom 5 sites 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 sites are assigned to an AP.

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 two minutes at the site, 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 at a specific site, 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 Analytics**. 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**.

Global Settings

The **Global Settings** link allows you to perform the following actions:

- [View and Assign Labels](#)
- [Manage Devices](#)
- [Manage Subscriptions](#)

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.



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 based on both groups and labels.

Label Classification

Labels are classified into the following categories:

- **Default**—A default label can be assigned to up to five devices.
- **Sites**—Each site can have multiple APs assigned to it. However, one AP can be assigned to only one site at any point in time. The **Site** label category is used only for the Presence Analytics application. For more information, see [Presence Analytics on page 149](#).

Label Management

This section describes the following procedures:

- [Creating a Label on page 153](#)
- [Editing or Deleting a Label on page 153](#)
- [Assigning a Device to a Label on page 154](#)
- [Detaching a Device from a Label on page 154](#)

Creating a Label

To create a label, complete the following steps:

1. On the Aruba Central App selector area, click **Global Settings**. 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 site, select **Site**.
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 App selector area, click **Global Settings**. 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 App selector area, click **Global Settings**.
2. Under Labels, click **Assignment**. The **Label Assignment** page is displayed.
3. To assign a label to an AP, select the AP 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 **Labels > 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**.

Managing Devices

This section describes the procedures for adding, viewing, and assigning devices to a group or subscription.

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 [Adding Devices to Central on page 19](#).

Viewing Devices

To view the devices added to Central, click **Global Settings > Devices & Subscriptions**. [Table 56](#) shows the contents of the **Device Provisioning** page.

Table 56: *Device Management Page in the Standard Interface View*

Parameter	Description
My Devices	Devices connected to Central. The My Devices tab view allows you to perform the following actions: ■ Sync Now—Synchronizes devices from the inventory. ■ Add Devices—Adds devices to Central network. Typically, the devices assigned to a customer account are automatically retrieved. If the automatic device addition fails, you can manually add the devices.
Pre-provision Groups	Devices assigned to a group.
Access Points	List of AP devices connected to Central.
Switches	List of Switches connected to Central.
Filter by Subscription Status	Devices sorted based on their subscription assignment status.
Serial Number	Serial number of the device.
MAC Address	MAC address of the device.
Model	Hardware model of the device.
Subscription Status	Status of the subscription assignment.
Group	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	Physical location of the device.

Table 57: *Device Management Pane in Managed Service Portal*

Parameter	Description
My Devices	Devices that are allocated to a customer account. The My Devices tab view allows you to perform the following actions: ■ Sync Now—Synchronizes devices from the inventory. ■ Add Devices—Adds devices to Central network. Typically, the devices assigned to a customer account are automatically retrieved. If the automatic device addition fails, you can manually add the devices.
Manage Devices	Devices available in the inventory. You can also allocate devices to customer accounts.
Access Points	List of AP devices connected to Central.
Switches	List of Switches connected to Central.

Parameter	Description
Filter by subscription status	Filter for viewing devices based on their subscription status.
Allocated Devices	Devices allocated or assigned to customer accounts.
Available Devices	Devices available in the inventory for assignment.
Total Devices	The total number of devices in Central.
Serial Number	Serial number of the device.
MAC Address	MAC address of the device.
Model	Hardware model of the device.
Subscription Status	Subscription assignment status of the device.
Customer	The customer account to which the device is associated.
Location	Physical location of the device.

Assigning Subscriptions to Devices

For information on assigning subscriptions, see [Managing Subscriptions on page 157](#).

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.

Mapping devices Groups in the Managed Service Portal

The Managed Service Portal maintains the list of devices owned by the Managed Service Portal customer account in the device table. The Managed Service Portal periodically synchronized with Aruba Activate to keep the device table up-to-date. It also maintains the customer and device association map. After this registration, the Managed Service Portal administrators can log in into Central and add devices in the Standard Enterprise mode. The devices can be assigned to customers and subscriptions in the Managed Service Portal mode.

In the Managed Service Portal, the groups are assigned to a customer account. The provisioning status of the devices for each customer account is displayed in the **All Customers** table on the **Monitoring > All Customers** page. If a device is listed under the unprovisioned group for the customer account in the Standard Enterprise mode, the status of this device is displayed in the **All Customers**. To move the device from the unprovisioned group to the default group, the Managed Service Portal administrators must drill down to the customer account and move the device to default in the Standard Enterprise mode.

Group Assignment in the Standard Interface View

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 **Global Settings > Devices & Subscriptions**. The **Device Provisioning** page opens.
2. Click **Pre-provision Groups**.
3. Select the devices.
4. Click **Assign Group**. The **Assign Group** pop-up window opens.
5. Select the group to which you want to assign the selected devices.
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**.

For more information on configuring and managing devices, see the following topics:

- [Verifying and Configuring Ports](#)
- [Provisioning Devices](#)
- [Managing Configuration Overrides](#)
- [Troubleshooting Devices](#)

Managing Subscriptions

The **Subscription Keys** and the **Subscription Assignment** menu options allow you to view and assign subscriptions to devices respectively.

Viewing Subscription Key Details

To view the subscription key details, click **Global Settings > Devices & Subscriptions > Subscription Keys**.

Table 58: *Subscription Keys Pane*

Data Pane Item	Description
Devices	Device management subscriptions.
Network Services	Subscriptions for cloud services. The network services subscriptions allow you to avail services such as Presence Analytics, Guest Access, and so on.
Total subscriptions	The total number of subscriptions.
Used	The total number of subscriptions that are in use.
Available	The total number of available subscriptions.

Data Pane Item	Description
Expiring in 90 Days	The number of subscriptions about to expire in 90 days.
Add Another Subscription Key	Allows you to add another subscription key.
Name	Name of the subscription.
Start Date	Start date from which the subscription is valid.
Expires on	subscription expiration date.
Subscriptions	The number of subscriptions associated with the subscription.

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 **Global Settings > Devices & Subscriptions > Subscription Keys**. The **Subscription Keys** page opens.
2. Click **Add Another Subscription Key** and enter the subscription key.
3. Click **Activate**. The subscription key is added to the list.

Acknowledging Subscription Expiry Notifications

The **Subscription Keys** page displays the subscriptions 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 subscription has already expired or is about to expire within 24 hours, a subscription 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.

Assigning Subscriptions to Devices

The subscription keys associated with a customer account can have multiple subscriptions associated with it.

When a subscription assigned to a device expires, Central checks the inventory for the available subscriptions for the device and verifies if the subscription key has adequate 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 subscription to a device, complete the following steps:

1. Click **Global Settings > Devices & Subscriptions > Subscription Assignment**. The **Subscription Assignment** page allows you to assign subscriptions for the devices or services for which the users have subscribed.
2. To assign subscriptions to devices, move the slider to **Devices** and select a device. For service subscriptions, move the slider to **Network Services** and then select the devices and services.
3. Click **Assign**.
4. To unassign subscription from a device, click **Unassign**. The subscription is unassigned and available for assignment to other devices.

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.

For more information, see the following topics:

- [Guest Access Dashboard on page 160](#)
- [Creating Apps for Social Login on page 161](#)
- [Configuring a Cloud Guest Splash Page Profile on page 165](#)
- [Configuring Visitor Accounts on page 170](#)

Guest Access Dashboard

The **Overview** page in the **Guest Access** app provides a dashboard displaying the number of guests, guest SSID, client count, type of clients, application usage, and guest connection for the selected group.

[Table 59](#) describes the contents of the **Guest Access Overview** page:

Table 59: *Guest Access Overview Pane*

Data Pane Item	Description
Time Range	Time range for the graphs and charts displayed on the Overview pane. You can choose to view graphs for a time period of 1 day, 1 week, and 1 month.
Guests	Number of guests connected to the SSIDs with Cloud Guest splash page profiles.
Guest SSID	Number of guest SSIDs that are configured to use the Cloud Guest splash page profiles.
Avg. Duration	The average duration of client connection on the SSIDs with Cloud Guest splash page profiles.

Data Pane Item	Description
MAX Concurrent Guests	Maximum number of client devices connected concurrently on the guest SSIDs.
Guest Connection Graph	Time stamp for the client connections on the cloud guest for the selected time range.
Client Count by Guest Authentication	Number of client devices based on the authentication type configured on the cloud guest SSIDs.
Guest count by SSID	Number of guest connections per SSID.
Client Type	Type of the client devices connected on the guest SSIDs.
Application Usage	The application usage by the guest clients connected to the APs on which the Deep Packet Inspection feature is enabled.

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. Specify a display name.
 - b. Select **No** for **Is this a test version of another app?**
 - c. Enter the contact email address.
 - d. Select **Business** from the **Category** drop-down list.

Figure 5 App ID Creation

The screenshot shows the 'Create a New App ID' form. At the top, it says 'Create a New App ID' and 'Get started integrating Facebook into your app or website'. Below this is a 'Display Name' field with a placeholder 'The name of your app or website'. There is a checkbox labeled 'No' and the text 'Is this a test version of another app? Learn More.' Below that is a 'Contact Email' field with a placeholder 'Used for important communication about your app'. Then there is a 'Category' dropdown menu with 'Choose a Category' selected. At the bottom, there is a line of text 'By proceeding, you agree to the Facebook Platform Policies' and two buttons: 'Cancel' and 'Create App ID'.

- e. 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. Under Getting Started, click **app review**.
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 6 Google+ Admin SDK Credentials

API Manager

Overview
Credentials

Add credentials to your project

- 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

[What credentials do I need?](#)

- Get your credentials

Cancel

- Under the **Where will you be calling the API from** section, select **Web Browser**.
- Under the **What data you will be accessing** section, select **User Data**.
- Click **What Credentials do I need**. The following page opens.

Figure 7 OAuth URLs

Google APIs

API Manager

Overview
Credentials

Add credentials to your project

✓ Find out what kind of credentials you need
Calling Admin SDK from a web browser

- 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 X

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 X

[Create client ID](#)

- Set up the OAuth 2.0 consent screen
- Download credentials

Cancel

- 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.



Ensure that the URL is an HTTPS URL with a domain name and not the IP address. For example, `https://example1.cloudguest.exampnenetworks.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.



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 8 *Twitter App Creation*

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 Cloud Guest Splash Page Profile

This topic describes the following procedures:

- [Adding a Cloud Guest Splash Page Profile on page 165](#)
- [Configuring a Cloud Guest Splash Page Profile on page 165](#)
- [Associating a Splash Page Profile to an SSID on page 169](#)

Adding a Cloud Guest 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 60: *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.
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.

Table 60: *Splash Page Configuration*

Data Pane Content	Description
	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. ■ 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	If you want to enable network access through the free Wi-Fi service offered by Facebook. Select the Facebook Wi-Fi option. The Facebook Wi-Fi feature allows you to pair your network with a Facebook business page, thereby allowing the guest users to log in from Wi-Fi hotspots using their Facebook credentials. After selecting the Facebook Wi-Fi option, complete the following steps to continue with the Facebook Wi-Fi configuration. 1. Click the Configure Now link. 2. Sign in to your Facebook account. 3. If you do not have a business page, click Create Page. For more information on setting Facebook Wi-Fi service, see Setting up Facebook Wi-Fi for Your Business at https://www.facebook.com/help/126760650808045. If the Facebook Wi-Fi business page is set up, when the users try to access the Internet, the browser redirects the user to the Facebook page. The user can log in with their Facebook account credentials and can either check in to access free Internet or skip checking in and then continue. NOTE: AP devices support Facebook Wi-Fi services on their own, without Central. However, for enabling social login based authentication, the guest splash pages must be configured in Central. For more information on Facebook Wi-Fi configuration on an AP, see the <i>Aruba Instant User Guide</i>.
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.

Table 60: *Splash Page Configuration*

Data Pane Content	Description
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.
Whitelist URL	To allow a URL, click + and add the URL to the whitelist. For example, if the terms and conditions configured for the guest portal include URLs, you can add these URLs to the whitelist, so that the users can access the required web pages.

4. Click **Next**. The **Customization** pane appears. [Configuring a Cloud Guest Splash Page Profile on page 165.](#)



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 61: *Splash page customization*

Data Pane Content	Description
Background Color	To change the color of the splash page, select a color from the Background Color palette.
Button Title	Specify a title for the sign in button.
Button Color	To change the color of the sign in button, select a color from the Button Color palette.
Page Font Color	To change the font color of the text on the splash page, select a color from the Page Font Color .
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.
Page Title	Add a suitable title for the splash page.

Data Pane Content	Description
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. The text box also allows you to use HTML tags for formatting text. For example, to highlight text with italics, you can wrap the text with the <code><i> </i></code> HTML tag. 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.
Ad Settings	If you want to display advertisements on the splash page, enter the URL of the advertisement and upload the image for the advertisement.

5. Click **Preview** to preview the customized splash page or click **Finish**.

Previewing and Modifying a Splash Page Profile

To preview a splash page profile, complete the following steps:

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, complete the following steps:

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:
 - a. Select **Cloud Guest** from the **Splash Page Type** list.
 - b. Select the splash page profile name from the **Guest Captive Portal Profile** list and click **Next**.
 - c. To enable encryption, set **Encryption** to **Enabled** and configure encryption parameters.
 - d. To exclude uplink, select an uplink from **Disable If Uplink Type Is**.
 - e. 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 62: *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.
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.



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 63: *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.

Parameter	Description
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 64: *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 delete a specific visitor account.

The following table lists the acronyms and abbreviations used in Aruba documents.

Table 65: *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, and 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 Layer Gateway
AM	Air Monitor
AMON	Advanced Monitoring
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

Table 65: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
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
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

Table 65: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
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
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	Discrete Fourier Transform
DHCP	Dynamic Host Configuration Protocol
DLNA	Digital Living Network Alliance
DMO	Dynamic Multicast optimization

Table 65: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
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
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

Table 65: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
ECC	Elliptical Curve Cryptography
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
GIS	Generic Interface Specification
GMT	Greenwich Mean Time
GPP	Guest Provisioning Page
GPS	Global Positioning System

Table 65: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
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
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

Table 65: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
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
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

Table 65: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
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
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

Table 65: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
NMS	Network Management Server
NOE	New Office Environment
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
PIM	Protocol-Independent Multicast
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard

Table 65: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
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 Intrusion Detection System
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

Table 65: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
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
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

Table 65: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
SKU	Stock Keeping Unit
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
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

Table 65: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
TIM	Traffic Indication Map
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TLV	Type-length-value
ToS	Type of Service
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
VCN	Virtual Branch Networking
VBR	Virtual Beacon Report
VHT	Very High Throughput

Table 65: *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
WMI	Windows Management Instrumentation
WMM	Wi-Fi Multimedia
WMS	WLAN Management System
WPA	Wi-Fi Protected Access
WSDL	Web Service Description Language

Table 65: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
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

The following table lists the terms and their definitions in this guide.

Table 66: *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 66: *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 66: *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 AP 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 66: *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.