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

- Contacting Support ............................................................................... 7

### Configuring APs .................................................................................. 8
  - Configuring AP Settings .................................................................... 8
  - Configuring External Antenna ........................................................ 10
    - EIRP and Antenna Gain .............................................................. 10
    - Configuring Antenna Gain ........................................................ 10
    - Adding an AP .............................................................................. 10
    - Removing an AP from the Network .............................................. 10
  - Configuring System Parameters for AP Network ................................ 11

### Configuring Networks ......................................................................... 13
  - Configuring a WLAN SSID Profile ................................................ 14
  - Configuring Captive Portal Profiles for Guest Network .................. 20
    - Splash Page Profiles ................................................................ 21
  - Configuring Profiles for Wired Network ........................................ 27
  - Editing a Network Profile ................................................................ 29
  - Deleting a Network Profile .......................................................... 29

### Configuring Time Based Services ....................................................... 29

### Configuring ARM and RF Parameters ............................................... 31
  - ARM Overview ............................................................................. 31
  - Configuring ARM Features .......................................................... 31
  - Configuring Radio Parameters ....................................................... 34

### Configuring IDS Parameters .............................................................. 35
  - Rogue APs .................................................................................... 35
  - Configuring Wireless Intrusion Detection and Protection Policies .... 35
Contents

Aruba Central | User Guide
Getting Started

Containment Methods ................................................................. 38
Configuring Authentication and Security Parameters ......................... 38
Supported Authentication Methods .................................................... 39
Supported Authentication Servers ..................................................... 42
  External RADIUS Server ............................................................. 42
  RADIUS Server Authentication with VSA ........................................ 43
  Internal RADIUS Server ............................................................. 43
  Authentication Termination on AP ............................................... 43
  Dynamic Load Balancing between Authentication Servers ............... 44
Configuring External Servers for Authentication ..................................... 44
Configuring Authentication Parameters for AP Management Users .......... 46
Configuring AP Users ................................................................... 47
  In the Central UI ......................................................................... 47
Configuring Roles and Policies for User Access Control ......................... 48
  ACL Rules ................................................................................. 48
  Configuring Network Address Translation Rules .............................. 49
  Configuring Access Rules for Network Services .............................. 49
  Configuring User Roles ................................................................ 51
Configuring Derivation Rules .......................................................... 51
Configuring Firewall Settings for Protection from ARP Attacks ............. 53
Managing Inbound Traffic .............................................................. 53
Configuring ALG Protocols ............................................................ 54
Blacklisting Clients ...................................................................... 54
Configuring VPN Networks ............................................................ 55
  VPN Features ............................................................................. 55
    Supported VPN Protocols .......................................................... 56
Configuring VPN Tunnels ............................................................... 56
    Configuring IPSec Tunnel .......................................................... 56
    Enabling Automatic Configuration of GRE Tunnel .......................... 57
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring GRE Tunnel Manually</td>
<td>58</td>
</tr>
<tr>
<td>Configuring an L2TPv3 Tunnel</td>
<td>59</td>
</tr>
<tr>
<td>Configuring Routing Profiles</td>
<td>59</td>
</tr>
<tr>
<td>Configuring DHCP and Client IP Assignment Modes</td>
<td>60</td>
</tr>
<tr>
<td>Configuring DHCP Scopes</td>
<td>60</td>
</tr>
<tr>
<td>Configuring DHCP Server for Client IP Assignment</td>
<td>64</td>
</tr>
<tr>
<td>Configuring Services</td>
<td>65</td>
</tr>
<tr>
<td>Configuring AirGroup Services</td>
<td>65</td>
</tr>
<tr>
<td>Configuring an AP for RTLS Support</td>
<td>66</td>
</tr>
<tr>
<td>Configuring an AP for ALE Support</td>
<td>66</td>
</tr>
<tr>
<td>ALE with Central</td>
<td>67</td>
</tr>
<tr>
<td>Enabling ALE support on an AP</td>
<td>67</td>
</tr>
<tr>
<td>Managing BLE Beacons</td>
<td>67</td>
</tr>
<tr>
<td>Configuring OpenDNS Credentials</td>
<td>68</td>
</tr>
<tr>
<td>Configuring CALEA Server for Lawful Intercept Compliance</td>
<td>68</td>
</tr>
<tr>
<td>Configuring CALEA Server Details on an AP</td>
<td>68</td>
</tr>
<tr>
<td>Integrating a Third-Party Network Firewall</td>
<td>69</td>
</tr>
<tr>
<td>Configuring an AP for Network Integration</td>
<td>69</td>
</tr>
<tr>
<td>Enabling AppRF™ Service</td>
<td>69</td>
</tr>
<tr>
<td>Configuring Uplinks</td>
<td>70</td>
</tr>
<tr>
<td>Uplink Interfaces</td>
<td>70</td>
</tr>
<tr>
<td>Uplink Preferences and Switching</td>
<td>75</td>
</tr>
<tr>
<td>Enforcing Uplinks</td>
<td>75</td>
</tr>
<tr>
<td>Setting an Uplink Priority</td>
<td>75</td>
</tr>
<tr>
<td>Enabling Uplink Pre-emption</td>
<td>75</td>
</tr>
<tr>
<td>Switching Uplinks based on the Internet Availability</td>
<td>76</td>
</tr>
<tr>
<td>Mobility and Client Management</td>
<td>76</td>
</tr>
<tr>
<td>Layer-3 Mobility for AP Clients</td>
<td>76</td>
</tr>
<tr>
<td>Home agent load balancing</td>
<td>76</td>
</tr>
</tbody>
</table>
Configuring L3 mobility domain ................................................................. 77
Configuring Enterprise Domains ............................................................... 77
Configuring SNMP Parameters ................................................................. 78
Configuring Community String for SNMP .................................................. 78
Configuring SNMP Traps .......................................................................... 79
Configuring Logs and TFTP Dump Servers .................................................. 79
Configuring a Syslog Server ...................................................................... 80
Configuring TFTP Dump Server .................................................................. 80
Resetting an AP ......................................................................................... 81
Uploading and Mapping AP Certificates ....................................................... 81
Uploading Certificate for an AP ................................................................. 81
Mapping AP Certificate .............................................................................. 83

**Analyzing Application Statistics** ......................................................... 84
Application Visibility ................................................................................. 84
AppRF Dashboard ...................................................................................... 84
Overview .................................................................................................... 85
Analyze ....................................................................................................... 85
Configuring ACL Rules for Application Analytics ...................................... 87
Configuring Web Policy Enforcement ......................................................... 88
Creating Custom URLs for Redirection ....................................................... 90
Creating a List of Error Page URLs ............................................................ 90
Configuring ACL Rules to Redirect Users to a Specific URL ...................... 90
## Contacting Support

**Table 1: Contact Information**

<table>
<thead>
<tr>
<th>Service</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main Site</td>
<td><a href="http://arubanetworks.com">arubanetworks.com</a></td>
</tr>
<tr>
<td>Support Site</td>
<td><a href="http://support.arubanetworks.com">support.arubanetworks.com</a></td>
</tr>
<tr>
<td>Airheads Social Forums and Knowledge Base</td>
<td><a href="http://community.arubanetworks.com">community.arubanetworks.com</a></td>
</tr>
<tr>
<td>North American Telephone</td>
<td>1-800-943-4526 (Toll Free) 1-408-754-1200</td>
</tr>
<tr>
<td>International Telephone</td>
<td><a href="http://arubanetworks.com/support-services/contact-support/">arubanetworks.com/support-services/contact-support/</a></td>
</tr>
<tr>
<td>Software Licensing Site</td>
<td><a href="http://hpe.com/networking/support">hpe.com/networking/support</a></td>
</tr>
<tr>
<td>Security Incident Response Team</td>
<td>Site: <a href="http://arubanetworks.com/support-services/security-bulletins/">arubanetworks.com/support-services/security-bulletins/</a> Email: <a href="mailto:sirt@arubanetworks.com">sirt@arubanetworks.com</a></td>
</tr>
</tbody>
</table>
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 8
- Configuring Networks on page 13
- Configuring Time Based Services on page 29
- Configuring ARM and RF Parameters on page 31
- Configuring IDS Parameters on page 35
- Configuring Authentication and Security Parameters on page 38
- Configuring VPN Networks on page 55
- Configuring DHCP and Client IP Assignment Modes on page 60
- Configuring Services on page 65
- Configuring Uplinks on page 70
- Mobility and Client Management on page 76
- Configuring Enterprise Domains on page 77
- Configuring Logs and TFTP Dump Servers on page 79
- Resetting an AP on page 81
- Uploading and Mapping AP Certificates on page 81

**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 2** as required and then click **Save Settings**.
Table 2: Access Points Configuration

<table>
<thead>
<tr>
<th>UI</th>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Info</td>
<td>Name</td>
<td>Configures a name for the AP. You can specify a character string of up to 32 ASCII characters.</td>
</tr>
<tr>
<td>AP Zone</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Preferred Master</td>
<td></td>
<td>Provisions the AP as a master AP.</td>
</tr>
<tr>
<td>IP Address for</td>
<td></td>
<td>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:</td>
</tr>
<tr>
<td>Access Point</td>
<td></td>
<td>1. Enter the new IP address for the AP in the IP Address text box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Enter the subnet mask of the network in the Netmask text box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Enter the IP address of the default gateway in the Default Gateway text box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Enter the IP address of the Domain Name System (DNS) server in the DNS Server text box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Enter the domain name in the Domain Name text box.</td>
</tr>
<tr>
<td>RADIO</td>
<td>Mode</td>
<td>Select any of the following options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Access—in the Access mode, the AP serves clients, while also monitoring for rogue APs in the background.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Monitor—in the Monitor mode, the AP acts as a dedicated monitor, scanning all channels for rogue APs and clients.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> In the Monitor and Spectrum Monitor modes, the APs do not provide access services to clients.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Uplink</td>
<td>Uplink Management VLAN</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To configure a non-native uplink VLAN, click Uplink and specify the VLAN in Uplink Management VLAN.</td>
</tr>
<tr>
<td></td>
<td>Eth0 Bridging</td>
<td>Select <strong>Enable</strong> from Eth0 Bridging if you want to convert the Eth0 uplink port to a downlink port.</td>
</tr>
<tr>
<td></td>
<td>USB Port</td>
<td>Enable the USB port if you do not want to use the cellular uplink or 3G/4G modem in your current network setup.</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Formula Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EIRP</td>
<td>Limit specific for each country of deployment</td>
</tr>
<tr>
<td>Tx RF Power</td>
<td>RF power measured at RF connector of the unit</td>
</tr>
<tr>
<td>GA</td>
<td>Antenna gain</td>
</tr>
<tr>
<td>FL</td>
<td>Feeder loss</td>
</tr>
</tbody>
</table>

Table 3: Formula Variable Definitions

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>
<thead>
<tr>
<th>Data Pane Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 4: System parameters

<table>
<thead>
<tr>
<th>Data Pane Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Controller Netmask</td>
<td><strong>NOTE:</strong> 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. <strong>NOTE:</strong> Ensure that VC VLAN is not the same as native VLAN of the AP.</td>
</tr>
<tr>
<td>Virtual Controller Gateway</td>
<td></td>
</tr>
<tr>
<td>Virtual Controller VLAN</td>
<td></td>
</tr>
</tbody>
</table>
| 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 4: System parameters

<table>
<thead>
<tr>
<th>Data Pane Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deny Inter-user Bridging</td>
<td>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.</td>
</tr>
<tr>
<td>Deny Local Routing</td>
<td>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.</td>
</tr>
<tr>
<td>Dynamic RADIUS Proxy</td>
<td>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.</td>
</tr>
<tr>
<td>Cluster Security</td>
<td>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. <strong>NOTE:</strong> After enabling or disabling cluster security, ensure that the configuration is synchronized across all devices in the cluster, and then reboot the cluster.</td>
</tr>
<tr>
<td>Mobility Access Switch</td>
<td>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.</td>
</tr>
</tbody>
</table>

## Configuring Networks

This section describes the following procedures:

- [Configuring a WLAN SSID Profile on page 14](#)
- [Configuring Captive Portal Profiles for Guest Network on page 20](#)
- [Configuring Profiles for Wired Network on page 27](#)
- [Editing a Network Profile on page 29](#)
- [Deleting a Network Profile on page 29](#)
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>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>If an SSID does not belong to any zone, all APs can broadcast this SSID.</td>
</tr>
</tbody>
</table>
| 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. |
<p>| Content Filtering      | Select <strong>Enabled</strong> 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 <strong>2.4 GHz, 5 GHz, or All</strong>. The <strong>All</strong> 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.                                            |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Probe Request Threshold</td>
<td>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.</td>
</tr>
<tr>
<td>SSID Encoding</td>
<td>To encode the SSID, select UTF-8.</td>
</tr>
<tr>
<td>ESSID</td>
<td>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.</td>
</tr>
<tr>
<td>Deny Inter User Bridging</td>
<td>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.</td>
</tr>
<tr>
<td>Time Range Profiles</td>
<td>Click Edit. Select a time range profile from the list and a status to apply and then click Save.</td>
</tr>
</tbody>
</table>

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 6: VLAN Assignment**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Virtual Controller Assigned</strong></td>
<td>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 60.</td>
</tr>
</tbody>
</table>
| **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 7: WLAN security settings**

<table>
<thead>
<tr>
<th>Data pane item</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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.
<p>|                                 | ◦ To use an internal server, select <strong>Internal server</strong> and add the clients that are required to authenticate with the internal RADIUS Server. Click <strong>Users</strong> to add the users. |</p>
<table>
<thead>
<tr>
<th>Data pane item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>○ To add a new server, click +. For information on configuring external servers, see Configuring External Servers for Authentication on page 44.</td>
<td></td>
</tr>
<tr>
<td>■ Secondary Server—To add another server for authentication, configure another authentication server.</td>
<td></td>
</tr>
<tr>
<td>■ 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.</td>
<td></td>
</tr>
<tr>
<td>■ 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 44.</td>
<td></td>
</tr>
<tr>
<td>Fast Roaming</td>
<td>Enable the following fast roaming features as per your requirement:</td>
</tr>
<tr>
<td>■ 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.</td>
<td></td>
</tr>
<tr>
<td>■ 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.</td>
<td></td>
</tr>
<tr>
<td>■ 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.</td>
<td></td>
</tr>
<tr>
<td>Accounting</td>
<td>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.</td>
</tr>
<tr>
<td>Advanced &gt; MAC Authentication for Enterprise Networks</td>
<td>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:</td>
</tr>
<tr>
<td>■ Perform MAC Authentication Before 802.1X — Select this to use 802.1X authentication only when the MAC authentication is successful.</td>
<td></td>
</tr>
<tr>
<td>■ MAC Authentication Fail-Thru — On selecting this, the 802.1X authentication is attempted when the MAC authentication fails.</td>
<td></td>
</tr>
<tr>
<td>If MAC authentication is enabled, configure the following parameters:</td>
<td></td>
</tr>
<tr>
<td>■ 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 xxxxxx:xxxx format is used. This option is available only when MAC authentication is enabled.</td>
<td></td>
</tr>
<tr>
<td>■ 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.</td>
<td></td>
</tr>
<tr>
<td>Advanced &gt; Reauth Interval</td>
<td>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:</td>
</tr>
<tr>
<td>■ 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.</td>
<td></td>
</tr>
<tr>
<td>Data pane item</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
|                | - 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:
     o Create a user role if required.
     o 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 20**.
     o 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 20
- Configuring Internal Captive Portal Splash Page Profile on page 22
- Configuring External Captive Portal Splash Page Profile on page 24
- Associating a Cloud Guest Splash Page Profile to a Guest SSID on page 26
- Disabling Captive Portal Authentication on page 27

**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 5.
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 60.

■ **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 8: Internal Captive Portal Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Splash Page Type</td>
<td>Select any of the following:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Internal - Authenticated</strong>—When <strong>Internal Authenticated</strong> 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.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Internal - Acknowledged</strong>— When <strong>Internal Acknowledged</strong> is enabled, the guest users are required to accept the terms and conditions to access the Internet.</td>
</tr>
<tr>
<td>Splash Page Properties</td>
<td>Under <strong>Splash Page Properties</strong>, 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.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Top Banner Title</strong>—Enter a title for the banner. To preview the page with the new banner title, click <strong>Preview Splash Page</strong>.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Header fill color</strong>—Specify a background color for the header.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Welcome Text</strong>—To change the welcome text, click the first square box in the splash page, enter the required text in the <strong>Welcome Text</strong> box, and click <strong>OK</strong>. Ensure that the welcome text does not exceed 127 characters.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Policy Text</strong>—To change the policy text, click the second square in the splash page, enter the required text in the <strong>Policy Text</strong> box, and click <strong>OK</strong>. Ensure that the policy text does not exceed 255 characters.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Page Fill Color</strong>—To change the color of the splash page, click the Splash page rectangle and select the required color from the color palette.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Redirect URL</strong>—To redirect users to another URL, specify a URL in <strong>Redirect URL</strong>.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Logo Image</strong>—To upload a custom logo, click <strong>Upload</strong>, browse the image file, and click <strong>upload image</strong>. Ensure that the image file size does not exceed 16 KB. To delete an image, click <strong>Delete</strong>.</td>
</tr>
<tr>
<td></td>
<td>- To preview the captive portal page, click <strong>Preview</strong> splash page.</td>
</tr>
<tr>
<td></td>
<td>- 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 <strong>Captive-portal proxy server IP</strong> and <strong>Captive Portal Proxy Server Port</strong> fields.</td>
</tr>
<tr>
<td>Encryption</td>
<td>Select <strong>Enabled</strong> and configure the following encryption parameters:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Key Management</strong>—Specify an encryption and authentication key</td>
</tr>
<tr>
<td></td>
<td>- <strong>Passphrase format</strong>—Specify a passphrase format.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Passphrase</strong>—Enter a passphrase and retype to confirm.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Configure the following parameters:</td>
</tr>
<tr>
<td></td>
<td>- <strong>MAC Authentication</strong>—To enable MAC address based authentication for <strong>Personal</strong> and <strong>Open</strong> security levels, set <strong>MAC Authentication</strong> to <strong>Enabled</strong>.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Primary Server</strong>—Sets a primary authentication server.</td>
</tr>
<tr>
<td></td>
<td>- To use an internal server, select <strong>Internal server</strong> and add the clients that are required to authenticate with the internal RADIUS Server. Click <strong>Users</strong> to add the users.</td>
</tr>
<tr>
<td></td>
<td>- To add a new server, click <strong>.</strong> For information on configuring external servers, see <strong>Configuring External Servers for Authentication on page 44</strong>.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Secondary Server</strong>—To add another server for authentication, configure another authentication server.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Load Balancing</strong>—Set this to <strong>Enabled</strong> 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 <strong>Dynamic Load Balancing between Authentication Servers on page 44</strong>.</td>
</tr>
<tr>
<td>Reauth Interval</td>
<td>Specify a value for <strong>Reauth Interval</strong>. When set to a value greater than zero, APs periodically re-authenticate all associated and authenticated clients.</td>
</tr>
</tbody>
</table>
Table 8: *Internal Captive Portal Configuration Parameters*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting</td>
<td>Select an accounting mode for posting accounting information at the specified <em>Accounting interval</em>. When the accounting mode is set to <em>Authentication</em>, 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 <em>Association</em>, the accounting starts when the client associates to the network successfully and stops when the client disconnects. This is applicable for WLAN SSIDs only.</td>
</tr>
<tr>
<td>Blacklisting</td>
<td>If you are configuring a wireless network profile, select <em>Enabled</em> to enable blacklisting of the clients with a specific number of authentication failures. This is applicable for WLAN SSIDs only.</td>
</tr>
<tr>
<td>Disable If Uplink Type Is</td>
<td>To exclude uplink, select an uplink type.</td>
</tr>
</tbody>
</table>

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 9: *External Captive Portal Profile Configuration Parameters*

<table>
<thead>
<tr>
<th>Data Pane Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the profile.</td>
</tr>
</tbody>
</table>
| 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 44](#).
   - **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 xxxxxxxxxxxxxx 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:
      i. **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 44.

- **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 44.

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 10: Time Range Profile Configuration Parameters**

<table>
<thead>
<tr>
<th><strong>Parameter</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify a name for the time range profile.</td>
</tr>
<tr>
<td>Type</td>
<td>Select the type of time range profile.</td>
</tr>
<tr>
<td>Periodic</td>
<td><strong>Periodic</strong>—When configured, the state of the SSID changes based on the time range configured in the profile.</td>
</tr>
<tr>
<td>Absolute</td>
<td><strong>Absolute</strong>—When configured, the state of the SSID changes during a specific date / day and time.</td>
</tr>
<tr>
<td>Period Type</td>
<td>For periodic time range profiles, specify a periodic interval (day / weekday / weekend / daily) at which the time range profile must be applied.</td>
</tr>
<tr>
<td>Start Day and End Day</td>
<td>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.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Select the start time for the time range profile in the hh:mm format.</td>
</tr>
<tr>
<td>End Time</td>
<td>Choose the end time for the time range profile in hh:mm format.</td>
</tr>
</tbody>
</table>

**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 31
- Configuring ARM Features on page 31
- Configuring Radio Parameters on page 34

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>
<thead>
<tr>
<th>Data pane item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefer 5 GHz</td>
<td>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.</td>
</tr>
<tr>
<td>Force 5 GHz</td>
<td>Enforces 5 GHz band steering mode on the APs.</td>
</tr>
<tr>
<td>Balance Bands</td>
<td>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.</td>
</tr>
<tr>
<td>Disable</td>
<td>Allows the clients to select the band to use.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Data Pane Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Access</td>
<td>Allows access based on client requests. When <strong>Air Time Fairness</strong> is set to default access, per user, and per SSID bandwidth limits are not enforced.</td>
</tr>
<tr>
<td>Fair Access</td>
<td>Allocates air time evenly across all the clients.</td>
</tr>
<tr>
<td>Preferred Access</td>
<td>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.</td>
</tr>
</tbody>
</table>

5. For **Client Match**, configure the following parameters:
Table 13: Additional ARM Configuration Parameters

<table>
<thead>
<tr>
<th>Data Pane Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Match</td>
<td>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. <strong>NOTE:</strong> When the Client Match is disabled, channels can be changed even when the clients are active on a BSSID.</td>
</tr>
<tr>
<td>CM Calculating Interval</td>
<td>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.</td>
</tr>
<tr>
<td>CM Neighbor Matching%</td>
<td>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%.</td>
</tr>
<tr>
<td>CM Threshold</td>
<td>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.</td>
</tr>
</tbody>
</table>
| 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 14: AP Control Configuration Parameters

<table>
<thead>
<tr>
<th>Data pane item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customize Valid Channels</td>
<td>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 <strong>Customize Valid Channels</strong>, a list of valid channels for both 2.4 GHz and 5 GHz are displayed. The valid channel customization feature is disabled by default. The valid channels automatically show in the <strong>static channel assignment</strong> data pane.</td>
</tr>
<tr>
<td>Minimum Transmit Power</td>
<td>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.</td>
</tr>
<tr>
<td>Maximum Transmit Power</td>
<td>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.</td>
</tr>
<tr>
<td>Client Aware</td>
<td>Allows ARM to control channel assignments for the APs with active clients. When the Client Match mode is set to <strong>Disabled</strong>, an AP may change to a more optimal channel, which disrupts current client traffic. The <strong>Client Aware</strong> option is <strong>Enabled</strong> by default.</td>
</tr>
</tbody>
</table>
**Table 15: Radio Configuration Parameters**

<table>
<thead>
<tr>
<th>Data pane item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scanning</td>
<td>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. <strong>NOTE:</strong> For Client Match configuration, ensure that scanning is enabled.</td>
</tr>
<tr>
<td>Wide Channel Bands</td>
<td>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.</td>
</tr>
<tr>
<td>80 MHz Support</td>
<td>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. <strong>NOTE:</strong> Only the APs that support 802.11ac can be configured with 80 MHz channels.</td>
</tr>
</tbody>
</table>

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.

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>
<thead>
<tr>
<th>Data pane item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Channel Switch Announcement Count</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Background Spectrum Monitoring</strong></td>
<td>When set to <strong>ON</strong>, 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.</td>
</tr>
<tr>
<td><strong>Customize ARM Power Range</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Very high throughput</strong></td>
<td>When set to <strong>ON</strong>, 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. <strong>NOTE:</strong> If you want the 802.11ac APs to function as 802.11n APs, clear this check box to disable VHT on these devices.</td>
</tr>
</tbody>
</table>

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 16: Infrastructure Detection Policies**

<table>
<thead>
<tr>
<th>Detection level</th>
<th>Detection policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td>Rogue Classification</td>
</tr>
<tr>
<td>Low</td>
<td>Detect AP Spoofing, Detect Windows Bridge, IDS Signature — Deauthentication Broadcast, IDS Signature — Deassociation Broadcast</td>
</tr>
<tr>
<td>Medium</td>
<td>Detect Adhoc networks using VALID SSID — Valid SSID list is auto-configured based on AP configuration, Detect Malformed Frame — Large Duration</td>
</tr>
<tr>
<td>High</td>
<td>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</td>
</tr>
</tbody>
</table>
The following table describes the detection policies enabled in the Client Detection Custom settings field.

**Table 17: Client Detection Policies**

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

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 18: Infrastructure Protection Policies**

<table>
<thead>
<tr>
<th>Protection level</th>
<th>Protection policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td>All protection policies are disabled</td>
</tr>
<tr>
<td>Low</td>
<td>- Protect SSID — Valid SSID list is auto derived from AP configuration</td>
</tr>
<tr>
<td></td>
<td>- Rogue Containment</td>
</tr>
<tr>
<td>High</td>
<td>- Protect from Adhoc Networks</td>
</tr>
<tr>
<td></td>
<td>- Protect AP Impersonation</td>
</tr>
</tbody>
</table>
The following table describes the detection policies that are enabled in the Client Protection Custom settings field.

**Table 19: Client Protection Policies**

<table>
<thead>
<tr>
<th>Protection level</th>
<th>Protection policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td>All protection policies are disabled</td>
</tr>
<tr>
<td>Low</td>
<td>Protect Valid Station</td>
</tr>
<tr>
<td>High</td>
<td>Protect Windows Bridge</td>
</tr>
</tbody>
</table>

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

- Supported Authentication Methods on page 39
- Supported Authentication Servers on page 42
- Configuring External Servers for Authentication on page 44
- Configuring Authentication Parameters for AP Management Users on page 46
- Configuring AP Users on page 47
- Configuring Roles and Policies for User Access Control on page 48
- Configuring ALG Protocols on page 54
- Blacklisting Clients on page 54
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-fallback 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-fallback 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 20.

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 20](#).

### 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](http://www.iso.org) and [http://www.itu.int](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.

---

**NOTE**

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 20: Authentication Server Configuration

<table>
<thead>
<tr>
<th>Type of Server</th>
<th>Parameters</th>
</tr>
</thead>
</table>
| 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
<table>
<thead>
<tr>
<th>Type of Server</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>TACACS client and server.</td>
</tr>
<tr>
<td></td>
<td>• Auth Port—The TCP IP port used by the server. The default port number is 49.</td>
</tr>
<tr>
<td></td>
<td>• Timeout—A number between 1 and 30 seconds to indicate the timeout period for TACACS+ requests. The default value is 20 seconds.</td>
</tr>
<tr>
<td></td>
<td>• IP Address—IP address of the server.</td>
</tr>
<tr>
<td></td>
<td>• Retry Count—The maximum number of authentication attempts to be allowed. The default value is 3.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td>Change of Authorization Only</td>
<td>Configure the following parameters:</td>
</tr>
<tr>
<td></td>
<td>• Name—Name of the server.</td>
</tr>
<tr>
<td></td>
<td>• IP Address—IP address of the server.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• Shared Key and Retype Key—A shared key for communicating with the external RADIUS server.</td>
</tr>
</tbody>
</table>

4. Click **Save Server**.

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

---

**NOTE**

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

### Configuring Authentication Parameters for 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 21: Configuration Parameters for the AP Users

<table>
<thead>
<tr>
<th>Type of the User</th>
<th>Authentication Options</th>
<th>Steps to Follow</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Control</td>
<td>Internal</td>
<td>Select <strong>Internal</strong> if you want to specify a single set of user credentials. If using an internal authentication server: 1. Enter a <strong>Username</strong> and <strong>Password</strong>. 2. Retype the password to confirm.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Authentication server w/ fallback to internal option if you want to use both internal and external</td>
</tr>
</tbody>
</table>
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 49
- Configuring User Roles on page 51
- Configuring Derivation Rules on page 51
- Managing Inbound Traffic on page 53

**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 87.
- Configuring access rules based on web categories and web reputation, see Configuring Web Policy Enforcement on page 88.

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 22: Access rule configuration parameters

<table>
<thead>
<tr>
<th>Data Pane Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Type</td>
<td>Select a rule type from the list, for example Access Control.</td>
</tr>
<tr>
<td>Service</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>- any—Access is allowed or denied to all services.</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> If TCP and UDP uses the same port, ensure that you configure separate access rules to permit or deny access.</td>
</tr>
<tr>
<td>Action</td>
<td>Select any of the following attributes:</td>
</tr>
<tr>
<td></td>
<td>- Select Allow to allow access users based on the access rule.</td>
</tr>
<tr>
<td></td>
<td>- Select Deny to deny access to users based on the access rule.</td>
</tr>
<tr>
<td></td>
<td>- Select Destination-NAT to allow changes to destination IP address.</td>
</tr>
<tr>
<td></td>
<td>- Select Source-NAT to allow changes to the source IP address.</td>
</tr>
<tr>
<td>Destination</td>
<td>Select a destination option. You can allow or deny access to any of the following destinations based on your requirements:</td>
</tr>
<tr>
<td></td>
<td>- To all destinations — Access is allowed or denied to all destinations.</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td>Log</td>
<td>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.</td>
</tr>
<tr>
<td>Blacklist</td>
<td>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 54.</td>
</tr>
<tr>
<td>Classify Media</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>- Video: Priority 5 (Critical)</td>
</tr>
<tr>
<td></td>
<td>- Voice: Priority 6 (Internetwork Control)</td>
</tr>
<tr>
<td>Disable Scanning</td>
<td>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 34.</td>
</tr>
<tr>
<td>DSCP Tag</td>
<td>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.</td>
</tr>
<tr>
<td>802.1 priority</td>
<td>Select 802.1 priority to specify an 802.1 priority. Specify a value between 0 and 7.</td>
</tr>
</tbody>
</table>

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 51
- Assigning Bandwidth Contracts to User Roles on page 51

Creating a User Role

To create a user role, complete the following steps:

2. Click Roles. The Roles pane contents are displayed.
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 20.

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,

2. Click Roles. The Roles pane contents are displayed.
3. Create a new role or select an existing role.
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 43.
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 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 18**.

---

**Configuring VPN Networks**

This section describes the following VPN configuration procedures:

- [VPN Features on page 55](#)
- [Configuring VPN Tunnels on page 56](#)
- [Configuring Routing Profiles on page 59](#)

**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>
<thead>
<tr>
<th><strong>Table 23: VPN Protocols</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VPN Protocol</strong></td>
</tr>
<tr>
<td>Aruba IPsec</td>
</tr>
</tbody>
</table>
| 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 56
- **Enabling Automatic Configuration of GRE Tunnel** on page 57
- **Configuring GRE Tunnel Manually** on page 58
- **Configuring an L2TPv3 Tunnel** on page 59

**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.

   **NOTE**

   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.
2. Click Routing.
3. Click New. The route parameters to configure are displayed.
4. 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 60](#)
- [Configuring DHCP Server for Client IP Assignment on page 64](#)

### Configuring DHCP Scopes

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

- [Configuring Distributed DHCP Scopes on page 60](#)
- [Configuring a Centralized DHCP Scope on page 61](#)
- [Configuring Local DHCP Scopes on page 63](#)

### 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 24: Distributed DHCP scope configuration parameters

<table>
<thead>
<tr>
<th>Data pane item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the DHCP scope.</td>
</tr>
<tr>
<td>Type</td>
<td>Select any of the following options:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Distributed, L2</strong> — On selecting <strong>Distributed, L2</strong>, the VC acts as the DHCP Server but the default gateway is in the data center. Traffic is bridged into VPN tunnel.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Distributed, L3</strong> — On selecting <strong>Distributed, L3</strong>, the VC acts as both DHCP Server and default gateway. Traffic is routed into the VPN tunnel.</td>
</tr>
<tr>
<td>VLAN</td>
<td>Specify a VLAN ID. To use this subnet, ensure that the VLAN ID specified here is assigned to an SSID profile.</td>
</tr>
<tr>
<td>Netmask</td>
<td>If <strong>Distributed, L2</strong> is selected for type of DHCP scope, specify the subnet mask. The subnet mask and the network determine the size of subnet.</td>
</tr>
<tr>
<td>Default Router</td>
<td>If <strong>Distributed, L2</strong> is selected for type of DHCP scope, specify the IP address of the default router.</td>
</tr>
<tr>
<td>DNS Server</td>
<td>If required, specify the IP address of a DNS server.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>If required, specify the domain name.</td>
</tr>
<tr>
<td>Lease Time</td>
<td>Specify a lease time for the client in minutes.</td>
</tr>
<tr>
<td>IP Address Range</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td></td>
<td>- For Distributed, L3 mode, you can configure any contiguous IP ranges. The configured IP range is divided into multiple IP subnets that are sufficient to accommodate the configured client count.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: 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.</td>
</tr>
<tr>
<td>Option</td>
<td>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.</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Data pane item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the DHCP scope.</td>
</tr>
<tr>
<td>VLAN</td>
<td>Specify a VLAN ID. To use this subnet, ensure that the VLAN ID specified here is assigned to an SSID profile.</td>
</tr>
<tr>
<td>DHCP Relay</td>
<td>Select <strong>Enabled</strong> to allow the APs to intercept the broadcast packets and relay DHCP requests.</td>
</tr>
<tr>
<td>Helper Address</td>
<td>Enter the IP address of the DHCP server.</td>
</tr>
<tr>
<td>VLAN IP</td>
<td>Specify the VLAN IP address of the DHCP relay server.</td>
</tr>
<tr>
<td>VLAN Mask</td>
<td>Specify the VLAN subnet mask of the DHCP relay server.</td>
</tr>
<tr>
<td>Option 82</td>
<td>This option is available only if Centralized is selected. Select <strong>Alcatel</strong> 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</td>
</tr>
</tbody>
</table>

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 25: DHCP mode configuration parameters**

---

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

---

The following table describes the behavior of the DHCP Relay Agent and Option 82 in the AP.
Table 26: DHCP relay and option 82

<table>
<thead>
<tr>
<th>DHCP relay</th>
<th>Option 82</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Enabled</td>
<td>DHCP packet relayed with the ALU-specific Option 82 string</td>
</tr>
<tr>
<td>Enabled</td>
<td>Disabled</td>
<td>DHCP packet relayed without the ALU-specific Option 82 string</td>
</tr>
<tr>
<td>Disabled</td>
<td>Enabled</td>
<td>DHCP packet not relayed, but broadcast with the ALU-specific Option 82 string</td>
</tr>
<tr>
<td>Disabled</td>
<td>Disabled</td>
<td>DHCP packet not relayed, but broadcast without the ALU-specific Option 82 string</td>
</tr>
</tbody>
</table>

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 27: Local DHCP configuration parameters

<table>
<thead>
<tr>
<th>Data pane item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the DHCP scope.</td>
</tr>
</tbody>
</table>
| 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 27: *Local DHCP configuration parameters*

<table>
<thead>
<tr>
<th>Data pane item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Excluded Address</td>
<td>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 <strong>Excluded address</strong>, the IP addresses either before or after the defined range are excluded.</td>
</tr>
<tr>
<td>Default Router</td>
<td>Enter the IP address of the default router.</td>
</tr>
<tr>
<td>DNS Server</td>
<td>Enter the IP address of a DNS server.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Enter the domain name.</td>
</tr>
<tr>
<td>Lease Time</td>
<td>Enter a lease time for the client in minutes.</td>
</tr>
<tr>
<td>Option</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 65
- Configuring an AP for RTLS Support on page 66
- Configuring an AP for ALE Support on page 66
- Managing BLE Beacons on page 67
- Configuring OpenDNS Credentials on page 68
- Configuring CALEA Server for Lawful Intercept Compliance on page 68
- Integrating a Third-Party Network Firewall on page 69
- Enabling AppRF™ Service on page 69

**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 server 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**.

**Managing BLE Beacons**

APs running the 6.4.3.4-4.2.1.0 firmware version support support Aruba Bluetooth Low Energy (BLE) devices, such as BT-100 and BT-105, which are used for location tracking and proximity detection. The BLE devices can be connected to an AP and are managed by a cloud-based Beacon Management Console. The BLE Beacon Management feature allows you to configure parameters for managing the BLE beacons and establishing secure communication with the Beacon Management Console.

To manage beacons and configure BLE operation mode, complete the following steps:

1. Select **Configuration > Wireless > Services > Real Time Locating System**.
2. To manage the BLE devices using BMC, select the **Manage BLE Beacons** checkbox.
3. Enter the authorization token. The authorization token is a text string of 1–255 characters used by the BLE devices in the HTTPS header when communicating with the BMC. This token is unique for each deployment.
4. In **Endpoint URL**, enter the URL of the server to which the BLE sends the monitoring data.
5. Select any of the following options from **BLE Operation Mode** drop-down list:
Table 28: BLE Operation Modes

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Beaconing</td>
<td>The built-in BLE chip in the AP functions as an iBeacon combined with the beacon management functionality.</td>
</tr>
<tr>
<td>Disabled</td>
<td>The built-in BLE chip of the AP is turned off. The BLE operation mode is set to Disabled by default.</td>
</tr>
<tr>
<td>DynamicConsole</td>
<td>The built-in BLE chip of the AP functions in the beaconing mode and dynamically enables access to AP console over BLE when the link to the LMS is lost.</td>
</tr>
<tr>
<td>PersistentConsole</td>
<td>The built-in BLE chip of the AP provides access to the AP console over BLE and also operates in the Beaconing mode.</td>
</tr>
</tbody>
</table>

6. Click **Save Settings**.

**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.

---

**NOTE**

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.
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 84](#).
Configuring Uplinks
This section provides the following information:

- Uplink Interfaces on page 70
- Uplink Preferences and Switching on page 75

Uplink Interfaces
Central supports 3G and 4G USB modems, and the Wi-Fi uplink to provide access to the corporate network. Figure 1 illustrates a scenario in which the APs join the Virtual Controller as slave APs through a wired or mesh Wi-Fi uplink:

Figure 1  Uplink Types

The following types of uplinks are supported on Central:

- 3G/4G Uplink
- Ethernet Uplink on page 73
- Wi-Fi Uplink on page 74

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 29: List of Supported 3G Modems**

<table>
<thead>
<tr>
<th>Modem Type</th>
<th>Supported 3G Modems</th>
</tr>
</thead>
<tbody>
<tr>
<td>True Auto Detect</td>
<td>USBConnect 881 (Sierra 881U)</td>
</tr>
<tr>
<td></td>
<td>Quicksilver (Globetrotter ICON 322)</td>
</tr>
<tr>
<td></td>
<td>UM100C (UTstarcom)</td>
</tr>
<tr>
<td></td>
<td>Icon 452</td>
</tr>
<tr>
<td></td>
<td>Aircard 250U (Sierra)</td>
</tr>
<tr>
<td></td>
<td>USB 598 (Sierra)</td>
</tr>
<tr>
<td></td>
<td>U300 (Franklin wireless)</td>
</tr>
<tr>
<td></td>
<td>U301 (Franklin wireless)</td>
</tr>
<tr>
<td></td>
<td>USB U760 for Virgin (Novatel)</td>
</tr>
<tr>
<td></td>
<td>USB U720 (Novatel/Qualcomm)</td>
</tr>
<tr>
<td></td>
<td>UM175 (Pantech)</td>
</tr>
<tr>
<td></td>
<td>UM150 (Pantech)</td>
</tr>
<tr>
<td></td>
<td>UMW190 (Pantech)</td>
</tr>
<tr>
<td></td>
<td>SXC-1080 (Qualcomm)</td>
</tr>
<tr>
<td></td>
<td>Globetrotter ICON 225</td>
</tr>
<tr>
<td></td>
<td>UMG181</td>
</tr>
<tr>
<td></td>
<td>NTT DoCoMo L-05A (LG FOMA L05A)</td>
</tr>
<tr>
<td></td>
<td>NTT DoCoMo L-02A</td>
</tr>
<tr>
<td></td>
<td>ZTE WCDMA Technologies MSM (MF668?)</td>
</tr>
<tr>
<td></td>
<td>Fivespot (ZTE)</td>
</tr>
<tr>
<td></td>
<td>c-motech CNU-600</td>
</tr>
<tr>
<td></td>
<td>ZTE AC2736</td>
</tr>
<tr>
<td></td>
<td>SEC-8089 (EpiValley)</td>
</tr>
<tr>
<td></td>
<td>Nokia CS-10</td>
</tr>
<tr>
<td></td>
<td>NTT DoCoMo L-08C (LG)</td>
</tr>
<tr>
<td></td>
<td>NTT DoCoMo L-02C (LG)</td>
</tr>
<tr>
<td></td>
<td>Novatel MC545</td>
</tr>
<tr>
<td></td>
<td>Huawei E220 for Movistar in Spain</td>
</tr>
<tr>
<td></td>
<td>Huawei E180 for Movistar in Spain</td>
</tr>
<tr>
<td></td>
<td>ZTE-MF820</td>
</tr>
<tr>
<td></td>
<td>Huawei E173s-1</td>
</tr>
<tr>
<td></td>
<td>Sierra 320</td>
</tr>
<tr>
<td></td>
<td>Longcheer WM72</td>
</tr>
<tr>
<td></td>
<td>U600 (3G mode)</td>
</tr>
<tr>
<td>Auto-detect + ISP/country</td>
<td>Sierra USB-306 (HK CLS/1010 (HK))</td>
</tr>
<tr>
<td></td>
<td>Sierra 306/308 (Telstra (Aus))</td>
</tr>
<tr>
<td></td>
<td>Sierra 503 PCIe (Telstra (Aus))</td>
</tr>
<tr>
<td></td>
<td>Sierra 312 (Telstra (Aus))</td>
</tr>
<tr>
<td></td>
<td>Aircard USB 308 (AT&amp;T’s Shockwave)</td>
</tr>
<tr>
<td></td>
<td>Compass 597(Sierra) (Sprint)</td>
</tr>
<tr>
<td></td>
<td>U597 (Sierra) (Verizon)</td>
</tr>
<tr>
<td></td>
<td>Tstick C597(Sierra) (Telecom(NZ))</td>
</tr>
<tr>
<td></td>
<td>Ovation U727 (Novatel) (Sprint)</td>
</tr>
<tr>
<td></td>
<td>USB U727 (Novatel) (Verizon)</td>
</tr>
<tr>
<td></td>
<td>USB U760 (Novatel) (Sprint)</td>
</tr>
<tr>
<td></td>
<td>USB U760 (Novatel) (Verizon)</td>
</tr>
<tr>
<td></td>
<td>Novatel MiFi 2200 (Verizon Mifi 2200)</td>
</tr>
<tr>
<td></td>
<td>Huawei E272, E170, E220 (ATT)</td>
</tr>
<tr>
<td></td>
<td>Huawei E169, E180,E220,E272 (Vodafone/SmarTone (HK))</td>
</tr>
<tr>
<td></td>
<td>Huawei E160 (O2(UK))</td>
</tr>
<tr>
<td></td>
<td>Huawei E160 (SFR (France))</td>
</tr>
<tr>
<td></td>
<td>Huawei E220 (NZ and JP)</td>
</tr>
<tr>
<td></td>
<td>Huawei E176G (Telstra (Aus))</td>
</tr>
</tbody>
</table>
The following table lists the types of supported 3G modems:

**Table 29: List of Supported 3G Modems**

<table>
<thead>
<tr>
<th>Modem Type</th>
<th>Supported 3G Modems</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Huawei E1553, E176 (3/HUTCH (Aus))</td>
</tr>
<tr>
<td></td>
<td>Huawei K4505 (Vodafone/SmarTone (HK))</td>
</tr>
<tr>
<td></td>
<td>Huawei K4505 (Vodafone (UK))</td>
</tr>
<tr>
<td></td>
<td>ZTE MF656 (Netcom (norway))</td>
</tr>
<tr>
<td></td>
<td>ZTE MF636 (HK CSL/1010)</td>
</tr>
<tr>
<td></td>
<td>ZTE MF633/MF636 (Telstra (Aus))</td>
</tr>
<tr>
<td></td>
<td>ZTE MF637 (Orange in Israel)</td>
</tr>
<tr>
<td></td>
<td>Huawei E180, E1692,E1762 (Optus (Aus))</td>
</tr>
<tr>
<td></td>
<td>Huawei E1731 (Airtel-3G (India))</td>
</tr>
<tr>
<td></td>
<td>Huawei E3765 (Vodafone (Aus))</td>
</tr>
<tr>
<td></td>
<td>Huawei E3765 (T-Mobile (Germany))</td>
</tr>
<tr>
<td></td>
<td>Huawei E1552 (SingTel)</td>
</tr>
<tr>
<td></td>
<td>Huawei E1750 (T-Mobile (Germany))</td>
</tr>
<tr>
<td></td>
<td>UGM 1831 (TMobile)</td>
</tr>
<tr>
<td></td>
<td>Huawei D33HW (EMOBILE(Japan))</td>
</tr>
<tr>
<td></td>
<td>Huawei GD01 (EMOBILE(Japan))</td>
</tr>
<tr>
<td></td>
<td>Huawei EC150 (Reliance NetConnect+ (India))</td>
</tr>
<tr>
<td></td>
<td>KDDI DATA07(Huawei) (KDDI (Japan))</td>
</tr>
<tr>
<td></td>
<td>Huawei E353 (China Unicom)</td>
</tr>
<tr>
<td></td>
<td>Huawei EC167 (China Telecom)</td>
</tr>
<tr>
<td></td>
<td>Huawei E367 (Vodafone (UK))</td>
</tr>
<tr>
<td></td>
<td>Huawei E352s-5 (T-Mobile (Germany))</td>
</tr>
<tr>
<td>No auto-detect</td>
<td>Huawei D41HW</td>
</tr>
<tr>
<td></td>
<td>ZTE AC2726</td>
</tr>
</tbody>
</table>

**Table 30: 4G supported modem**

<table>
<thead>
<tr>
<th>Modem Type</th>
<th>Supported 4G Modem</th>
</tr>
</thead>
<tbody>
<tr>
<td>True Auto Detect</td>
<td>Pantech UML290</td>
</tr>
<tr>
<td></td>
<td>Ether-ite</td>
</tr>
</tbody>
</table>

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.

---

**NOTE**

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.

**NOTE**

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 75
- Setting an Uplink Priority on page 75
- Enabling Uplink Pre-emption on page 75

**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**.

---

**NOTE**

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 76](#)
- [Configuring L3 Mobility domain on page 77](#)

### 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 78
- Configuring Community String for SNMP on page 78
- Configuring SNMP Traps on page 79

**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 31: SNMP parameters**

<table>
<thead>
<tr>
<th>Data Pane Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community Strings for SNMPv1 and SNMPv2</td>
<td>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.</td>
</tr>
<tr>
<td>If you are using SNMPv3 to obtain values from the AP, you can configure the following parameters:</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>A string representing the name of the user.</td>
</tr>
<tr>
<td>Authentication Protocol</td>
<td>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:</td>
</tr>
<tr>
<td>Authentication protocol password</td>
<td>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.</td>
</tr>
<tr>
<td>Privacy protocol</td>
<td>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).</td>
</tr>
<tr>
<td>Privacy protocol password</td>
<td>If messages sent on behalf of this user can be encrypted/decrypted with DES, the (private) privacy key for use with the privacy protocol.</td>
</tr>
</tbody>
</table>

**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 80](#)
- [Configuring TFTP Dump Server on page 80](#)
Configuring a Syslog Server

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

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 32: Logging levels**

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

4. Click **Save Settings**.

**Configuring TFTP Dump Server**

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

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 81](#)
- [Mapping AP Certificate on page 83](#)

**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 PKCS12 format 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](https://redmine1.lab1.arubathena.com/issues/44112).

3. The customer must email the TAC ticket number to [hpe-aruba-cloud-devops@hpe.com](mailto: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 84
- Configuring ACL Rules for Application Analytics on page 87
- Configuring Web Policy Enforcement on page 88
- Creating Custom URLs for Redirection on page 90

### 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.


### 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 2  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 3** shows the data without filters and data with filters on:

**Figure 3  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 33: Details—Apps**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Name of the application.</td>
</tr>
<tr>
<td>Total Usage</td>
<td>The total usage of the application bandwidth.</td>
</tr>
<tr>
<td>Usage(%)</td>
<td>Percentage of client traffic to an application.</td>
</tr>
<tr>
<td>#SSID</td>
<td>Number of SSIDs through which the clients access an application.</td>
</tr>
</tbody>
</table>

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 34: Details—Web Categories**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Name of the web category.</td>
</tr>
<tr>
<td>Total Usage</td>
<td>The total bandwidth used by clients accessing the web category.</td>
</tr>
<tr>
<td>Usage(%)</td>
<td>Percentage of clients traffic to the web category.</td>
</tr>
<tr>
<td>#SSID</td>
<td>Number of SSIDs used for accessing the web category.</td>
</tr>
</tbody>
</table>

**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 88](#).

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 35: Access Rule Configuration Parameters

<table>
<thead>
<tr>
<th>Service category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Category</td>
<td>Select the application categories to which you want to allow or deny access.</td>
</tr>
<tr>
<td>Application</td>
<td>Select the applications to which you want to allow or deny access.</td>
</tr>
<tr>
<td>Application Throttling</td>
<td>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.</td>
</tr>
<tr>
<td>Action</td>
<td>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.</td>
</tr>
<tr>
<td>Log</td>
<td>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.</td>
</tr>
<tr>
<td>Blacklist</td>
<td>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 54.</td>
</tr>
<tr>
<td>Disable Scanning</td>
<td>Select Disable scanning check box to disable ARM scanning when this rule is triggered. The selection of the Disable scanning applies only if AARM scanning is enabled. For more information, see Configuring Radio Parameters on page 34.</td>
</tr>
<tr>
<td>DSCP Tag</td>
<td>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.</td>
</tr>
<tr>
<td>802.1 priority</td>
<td>Select this check box to enable 802.1 priority. 802.1p is an L2 protocol for traffic prioritization to manage quality of service (QoS) on the network. There are eight levels of priority, 0-7. To assign a higher priority, specify a higher value.</td>
</tr>
</tbody>
</table>

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:

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:
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 54.
- 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 34.
- DSCP Tag — Select this check box to add a Differentiated Services Code Point (DSCP) tag to the rule. DSCP is an L3 mechanism for classifying and managing network traffic and providing quality of service (QoS) on the network. To assign a higher priority, specify a higher value.
- 802.1 priority — Select this check box to enable 802.1 priority. 802.1p is an L2 protocol for traffic prioritization to manage quality of service (QoS) on the network. There are eight levels of priority, 0-7. To assign a higher priority, specify a higher value.

9. Click Save to save the rules.

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

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:
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.