<table>
<thead>
<tr>
<th>Headquarters</th>
<th>Support</th>
<th>Sales</th>
</tr>
</thead>
<tbody>
<tr>
<td>5453 Great America Parkway</td>
<td>408547-5502</td>
<td>408 547-5501</td>
</tr>
<tr>
<td>Santa Clara, CA 95054</td>
<td>866 476-0000</td>
<td>866 497-0000</td>
</tr>
<tr>
<td>USA</td>
<td><a href="mailto:support-wifi@arista.com">support-wifi@arista.com</a></td>
<td><a href="mailto:sales@arista.com">sales@arista.com</a></td>
</tr>
<tr>
<td>408 547-5500</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="http://www.arista.com">www.arista.com</a></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© Copyright 2021 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista Networks and the Arista logo are trademarks of Arista Networks, Inc in the United States and other countries. Other product or service names may be trademarks or service marks of others.
# Contents

Chapter 1: What's New in CloudVision WiFi 11.0.1............................. 1

Chapter 2: Access CloudVision WiFi.................................................... 3
  2.1 Get Details of CloudVision WiFi Version, Build and License Agreement.................. 3
  2.2 Get Details of Logged In User.............................................................................. 3
  2.3 Sign Out of CloudVision WiFi.............................................................................. 4
  2.4 View Open Source Software Licenses................................................................... 4

Chapter 3: Common Operations............................................................ 5
  3.1 WiFi Network Counters....................................................................................... 5
  3.2 Search.................................................................................................................. 7
  3.3 Table level Operations.......................................................................................... 8
    3.3.1 Freeze Columns............................................................................................. 8
    3.3.2 Add/Remove Columns.................................................................................. 8
  3.4 Filters on Widgets.............................................................................................. 9
  3.5 IPv6 Support in UI Fields................................................................................ 12

Chapter 4: Arista Navigator................................................................. 15
  4.1 Managing Navigator............................................................................................ 15
    4.1.1 Add a Folder or Floor................................................................................... 16
    4.1.2 Add Multiple Folders or Floors.................................................................... 16
    4.1.3 Delete Folders and Floors............................................................................ 17
    4.1.4 Rename Folder or Floor................................................................................ 17
    4.1.5 Search Folder or Floor.................................................................................. 17
    4.1.6 Set Timezone for Folders............................................................................ 18
    4.1.7 Set Location Tag.......................................................................................... 18
  4.2 Introduction to Groups....................................................................................... 18
    4.2.1 Add a Group.................................................................................................. 19
    4.2.2 Delete a Group.............................................................................................. 19

Chapter 5: Baselines............................................................................. 21
  5.1 Baselines versus Thresholds.............................................................................. 21
  5.2 How to Read a Baseline Graph?........................................................................ 21
  5.3 CloudVision WiFi Baselines.............................................................................. 22
  5.4 Data Reporting and Retention........................................................................... 24
  5.5 Data Point Drill Down....................................................................................... 25

Chapter 6: Dashboards......................................................................... 27
  6.1 Connectivity Dashboard.................................................................................... 27
    6.1.1 Client Journey.............................................................................................. 27
    6.1.2 Top Locations Affected by Failures.............................................................. 30
    6.1.3 Clients by Most Failed Connections............................................................ 30
  6.2 Performance Dashboard.................................................................................... 31
    6.2.1 Client Health............................................................................................... 31
Chapter 7: Monitoring WiFi

7.1 Clients

7.1.1 Client Connection Logs

7.1.2 Client Events Logs

7.1.3 Top Applications by Traffic in Client Tab

7.1.4 Client Traffic Volume

7.1.5 Application Session Logs

7.1.6 Devices Seeing This Client

7.1.7 Rename a Client

7.2 Access Points

7.2.1 Clients by Avg. Data Rate for an AP

7.2.2 Currently Associated Clients for an AP

7.2.3 Top Applications by Traffic for an AP

7.2.4 Network Usage

7.2.5 Network Usage - Poor Application Experience

7.2.6 Spectrum Occupancy

7.2.7 RF Explorer

7.2.8 Channel Utilization

7.2.9 AP Health

7.2.10 Visible Access Points

7.2.11 Radios Seeing this AP(Access Point)

7.2.12 Visible VLANs

7.2.13 Visible Clients

7.2.14 View Access Point Event Logs

7.2.15 View on Floor Map

7.2.16 Customize Transmit Power or Channel

7.2.17 Customize VLANs to Monitor per AP

7.2.18 Move an AP

7.2.19 Reboot Access Points

7.2.20 Rename Access Points

7.2.21 Delete Access Points

7.2.22 View Ongoing Activities on AP

7.2.23 Assign a Device to a Group from Access Points tab

7.2.24 Re-assign a Device to Another Group

7.2.25 About Device Firmware Update in CloudVision WiFi

7.2.26 Access Point Web Shell

7.3 Radios

7.3.1 Turn Radio On or Off

7.4 Active SSIDs
### Chapter 8: Configure WiFi

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.5 Application Visibility</td>
<td>85</td>
</tr>
<tr>
<td>7.5.1 Application Traffic</td>
<td>86</td>
</tr>
<tr>
<td>7.5.2 Monitoring an Application</td>
<td>86</td>
</tr>
<tr>
<td>7.6 Application Traffic</td>
<td>87</td>
</tr>
<tr>
<td>7.6.1 Clients with Most Application Traffic</td>
<td>87</td>
</tr>
<tr>
<td>7.7 Root Cause Analysis Using the Inference Engine</td>
<td>88</td>
</tr>
<tr>
<td>7.7.1 Root Cause Analysis for a Single Client Vs Total Clients</td>
<td>88</td>
</tr>
<tr>
<td>7.7.2 Looking for Root Causes</td>
<td>89</td>
</tr>
<tr>
<td>7.7.3 Perform Root Cause Analysis for a Single Client</td>
<td>91</td>
</tr>
</tbody>
</table>

### Chapter 9: SSID Settings

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1 SSID Basic Settings</td>
<td>97</td>
</tr>
<tr>
<td>9.1.1 Configure SSID Basic Settings</td>
<td>98</td>
</tr>
<tr>
<td>9.2 SSID Security Settings</td>
<td>98</td>
</tr>
<tr>
<td>9.2.1 Configure SSID Security Settings</td>
<td>100</td>
</tr>
<tr>
<td>9.2.2 Group PSKs</td>
<td>101</td>
</tr>
<tr>
<td>9.3 SSID Network Settings</td>
<td>102</td>
</tr>
<tr>
<td>9.3.1 Example Use Case</td>
<td>105</td>
</tr>
<tr>
<td>9.3.2 Configure SSID Network Settings</td>
<td>106</td>
</tr>
<tr>
<td>9.3.3 SSID VLAN Mapping</td>
<td>107</td>
</tr>
<tr>
<td>9.4 SSID Access Control</td>
<td>107</td>
</tr>
<tr>
<td>9.4.1 Configure SSID Access Control</td>
<td>110</td>
</tr>
<tr>
<td>9.4.2 L3-4 Firewall</td>
<td>110</td>
</tr>
<tr>
<td>9.4.3 Application Firewall</td>
<td>112</td>
</tr>
<tr>
<td>9.4.4 L3-4 versus Application Firewall Decision Table</td>
<td>113</td>
</tr>
<tr>
<td>9.4.5 Configure Firewall in SSID</td>
<td>113</td>
</tr>
<tr>
<td>9.4.6 What is Bonjour Gateway?</td>
<td>114</td>
</tr>
<tr>
<td>9.4.7 How Arista Supports Bonjour Gateway</td>
<td>114</td>
</tr>
<tr>
<td>9.4.8 Configure Bonjour Gateway</td>
<td>115</td>
</tr>
<tr>
<td>9.4.9 Configure Redirection in SSID Access Control</td>
<td>115</td>
</tr>
<tr>
<td>9.4.10 What is a Walled Garden?</td>
<td>116</td>
</tr>
<tr>
<td>9.4.11 How the Client MAC Allow and Deny Lists Work</td>
<td>117</td>
</tr>
<tr>
<td>9.4.12 Requirements for Allow Deny Lists of Client MAC Addresses</td>
<td>117</td>
</tr>
<tr>
<td>9.4.13 Google Integration for Client Device Authorization</td>
<td>117</td>
</tr>
<tr>
<td>9.4.14 Configure Client Authentication</td>
<td>118</td>
</tr>
<tr>
<td>9.4.15 Configure Role Based Control</td>
<td>118</td>
</tr>
<tr>
<td>9.4.16 Typical RADIUS MAC Authentication Flow</td>
<td>119</td>
</tr>
<tr>
<td>9.4.17 Implementation Using Role Profiles</td>
<td>120</td>
</tr>
<tr>
<td>9.5 SSID Analytics</td>
<td>124</td>
</tr>
<tr>
<td>9.5.1 HTTP POST Format</td>
<td>125</td>
</tr>
<tr>
<td>9.5.2 Configure Analytics in SSID Settings</td>
<td>125</td>
</tr>
<tr>
<td>9.5.3 Analytics Parameter</td>
<td>126</td>
</tr>
<tr>
<td>9.6 SSID Captive Portal</td>
<td>128</td>
</tr>
<tr>
<td>9.6.1 Walled Garden Sites for Captive Portal</td>
<td>130</td>
</tr>
<tr>
<td>9.6.2 Configure AP Hosted Captive Portal</td>
<td>131</td>
</tr>
<tr>
<td>9.6.3 Configure Cloud Hosted Captive Portal</td>
<td>132</td>
</tr>
<tr>
<td>9.6.4 Guest Wi-Fi User Authentication with Host Approval</td>
<td>133</td>
</tr>
<tr>
<td>9.6.5 Design a Splash Page</td>
<td>135</td>
</tr>
<tr>
<td>9.6.6 Configure Common Settings for Plugins</td>
<td>136</td>
</tr>
<tr>
<td>9.6.7 Configure Email Account Settings</td>
<td>136</td>
</tr>
<tr>
<td>9.6.8 Configure SMS / MMS Account Settings</td>
<td>137</td>
</tr>
<tr>
<td>9.6.9 Configure Payment Gateway Settings</td>
<td>138</td>
</tr>
</tbody>
</table>
# Chapter 13: Remote Access Point

- 13.1 Configure a Remote Access Point ......................................................... 189
- 13.2 Configure IPSec Credentials for Each Remote AP .............................. 190

# Chapter 14: Radio Settings

- 14.1 How Unified Client Steering Works ......................................................... 204
  - 14.1.1 General Considerations ................................................................. 195
  - 14.1.2 Inter AP Sync .............................................................................. 195
  - 14.1.3 Frequency of Client Steering ......................................................... 196
- 14.2 Configure Client Steering Common Parameters in Radio Settings ........ 197
  - 14.2.1 What is Unified Client Steering ...................................................... 197
  - 14.2.2 Client Steering Parameters ........................................................... 197
- 14.3 Configure Basic Radio Settings ............................................................ 198
  - 14.3.1 Basic Radio Settings Parameters .................................................. 198
- 14.4 Configure 802.11ax Settings ................................................................. 200
  - 14.4.1 MU-MIMO .................................................................................... 200
  - 14.4.2 OFDMA ....................................................................................... 201
- 14.5 Configure Transmit Power Selection in Radio Settings ....................... 202
  - 14.5.1 Transmit Power Selection Parameters .......................................... 203
- 14.6 Configure Smart Steering in Radio Settings ........................................... 203
- 14.7 Configure Smart Client Load Balancing in Radio Settings .................... 204
- 14.8 Configure Band Steering in Radio Settings ........................................... 204
- 14.9 Configure WMM Admission Control Policy in Radio Settings ............... 205

# Chapter 15: Device Settings

- 15.1 Device Tab ............................................................................................ 207
- 15.2 Turn Access Point into a WIPS Sensor .................................................. 209
- 15.3 Configure Scanning ............................................................................. 209
  - 15.3.1 Background Scanning Parameters ................................................. 210
- 15.4 Configure Inter Access Point Sync for Client Steering in Device Settings .. 210
- 15.5 Configure Client RSSI Update Interval in Device Settings ................... 211
- 15.6 Configure VLAN Extension in Device Settings .................................... 211
- 15.7 Configure Link Aggregation in Device Settings .................................... 211
- 15.8 Configure AeroScout Integration ......................................................... 212
- 15.9 Configure Antenna Settings in Device Settings ..................................... 212
- 15.10 Configure Device Password in Device Settings ................................... 212
- 15.11 Configure Device Access Logs in Device Settings ............................... 213
- 15.12 Configure IPv4/IPv6 Dual Stack in Device Settings ............................ 213
- 15.13 Enable SSH IP Allow List .................................................................... 213
  - 15.13.1 SSH IP Allow List Parameters .................................................... 214
- 15.14 Configure NTP in Device Setting ....................................................... 214
- 15.15 Configure Access Radio Exceptions in Device Settings ...................... 215
Chapter 21: Floor Plans ................................................................. 265
  21.1 Add A Floor Plan............................................................... 265
  21.2 Perform Operations on an AP from Floor Plan............... 266

Chapter 22: Heat Maps ................................................................. 267
  22.1 Default View................................................................. 267
  22.2 AP Coverage View......................................................... 268
  22.3 AP Link Speed View....................................................... 268
  22.4 AP Channel Coverage View............................................ 269
  22.5 Resolution and Frequency Filters................................. 270

Chapter 23: Locate Access Points and Clients............................. 271
  23.1 Locationing Criteria....................................................... 271
  23.2 Locate an AP or a Client in a Floor Plan......................... 272
  23.3 Drill Down from a Device.............................................. 273
    23.3.1 Locate a Specific Device........................................ 274
    23.3.2 What You Can See on the Floor Plan...................... 274

Chapter 24: Reports in CloudVision WiFi................................. 277
  24.1 Scheduling Reports....................................................... 277
  24.2 On-Demand Generation of Reports................................. 279
  24.3 Archive a Report......................................................... 281

Chapter 25: Third-Party Servers................................................ 283
  25.1 Google Integration......................................................... 283
  25.2 ArcSight Integration....................................................... 283
  25.3 SMTP........................................................................... 284
  25.4 SNMP........................................................................ 285
    25.4.1 SNMP - Alerts...................................................... 285
    25.4.2 SNMP - Server Health......................................... 287
  25.5 Syslog....................................................................... 289

Chapter 26: Advanced System Settings....................................... 291
  26.1 License Settings for On-Premises Users......................... 291
  26.2 Language Settings....................................................... 291
  26.3 High Availability Status............................................... 291
  26.4 System Status............................................................ 292
  26.5 NTP Configuration....................................................... 292
# What's New in CloudVision WiFi 11.0.1

CloudVision WiFi (CVW) 11.0.1 introduces the following features and functionalities. This release is available on request only.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Settings in the Configure menu</td>
<td>The Device Settings option is available in the Configure menu. You can configure device settings for WIPS-only licences as well.</td>
</tr>
<tr>
<td>Graph View for Client Event Logs</td>
<td>The client event logs are available as a chart instead of the timeline. Each event in the graph represents an activity for the connected client. You can switch between the Graph view and the existing Grid view.</td>
</tr>
<tr>
<td>Group PSK</td>
<td>Network administrators often want to use the same SSID for different client device categories (e.g., printers and video cameras), but assign different VLANs or access lists to them. With Group PSKs, you can configure the same SSID with up to 32 different PSKs, each for a group of WiFi clients.</td>
</tr>
<tr>
<td>Enhancements to ACS DCS</td>
<td>The Auto Channel Selection (ACS) and Dynamic Channel Selection (DCS) algorithms have been enhanced for optimal channel selection. ACS uses unoccupied DFS channels better and DCS responds faster to interference events.</td>
</tr>
</tbody>
</table>
Access CloudVision WiFi

CloudVision WiFi is a part of the Arista Cloud services. To access CloudVision WiFi, you must log in to Launchpad.

You get the same user privileges in CloudVision WiFi that were assigned to you for Wireless Manager. For example, if you have the Superuser role in Wireless Manager, you will be able to operate and access CloudVision WiFi as a Superuser.

Perform the following, to access CloudVision WiFi:

1. Log in to Launchpad.
   Refer the Launchpad User Guide for more information.
   The services that you have been provided access to are seen as tiles, under Services on the dashboard. Similarly, the applications provided in the cloud are also seen as tiles under Apps on the Dashboard.
2. Click the CloudVision WiFi tile under Apps to access CloudVision WiFi.
   CloudVision WiFi is opened on a new browser tab.

2.1 Get Details of CloudVision WiFi Version, Build and License Agreement

The page displays the version number, build number, and the terms and conditions and the license agreement for CloudVision WiFi.

To view the CloudVision WiFi version number, build number and license agreement:

1. On the top-left corner of the screen, click the Arista icon.
   The following information is displayed on the CloudVision WiFi page:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Version number of CloudVision WiFi</td>
</tr>
<tr>
<td>Build</td>
<td>Build number of CloudVision WiFi</td>
</tr>
<tr>
<td>Service Build</td>
<td>Build number of Wireless Manager</td>
</tr>
</tbody>
</table>

2.2 Get Details of Logged In User

You can view the basic information of the user who is logged in to CloudVision WiFi.

To view the details of the logged in user, click on the initials of the user on the bottom-left corner of the Service menu. The following information is displayed:

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login ID</td>
<td>The username of the user that has logged in.</td>
</tr>
<tr>
<td>Options</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>User Role</td>
<td>The role of the user. For example, Super User, Admin, and so on. These roles are configured in Wireless Manager.</td>
</tr>
<tr>
<td>Email</td>
<td>The Email address of the user. Note: The Login Id and the Email address of the user can be the same.</td>
</tr>
<tr>
<td>Current Time</td>
<td>The current time and date on the system.</td>
</tr>
<tr>
<td>Timezone</td>
<td>The time zone as selected by the user.</td>
</tr>
</tbody>
</table>

### 2.3 Sign Out of CloudVision WiFi

You can sign out of CloudVision WiFi and its services.

To sign out of CloudVision WiFi, perform the following steps:

1. On the bottom-left corner of the screen, click the icon that has your login name initials below Services.
2. Click Sign Out.
   
   You will be signed out and redirected to the Launchpad Sign In page.

### 2.4 View Open Source Software Licenses

You can view the open source software (OSS) licenses from the UI. The licenses are downloaded to your local drive.

1. Log in to CVW and click Arista.
2. Under OSS Licenses, click the link for each component. The license is downloaded to your local drive.
Chapter 3

Common Operations

3.1 WiFi Network Counters

WiFi network counters provide network administrators with a quick summary of their WiFi network infrastructure for the selected location. The counters are accessible in the top-right corner on the CloudVision WiFi UI and also serve as a shortcut to quickly drill down to more details. The counters provide the following information.

**Managed WiFi Devices**

Active and inactive status of managed WiFi devices including access points (APs), sensors and network detectors, and if any of the devices are running an outdated firmware version or configuration.

![Table of Managed WiFi Devices]

**WiFi Clients**

Types of clients that are currently connected to the managed WiFi network.
Threat-Posing Devices

Presence of threat-posing devices, e.g., rogue, misconfigured APs, rogue clients, misbehaving authorized clients.
Common Operations

Alerts

Raised alerts related to WiFi performance and security, and system health.

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2246</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Wi-Fi</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>WIPS</td>
<td>1703</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>System</td>
<td>543</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Tunnels

Up/down status of tunnels, e.g., EoGRE, VxLAN, configured on the WiFi APs.

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Active</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Inactive</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

3.2 Search

Global search helps to find a client or AP, by typing the MAC or IP address, user name, or the device name.

Global search is placed next to Global counters, at the top-right corner of the page, across the Dashboard and Access pages.

Only those clients/devices that are available on a selected folder or floor can be searched. Therefore, if a client, say LAP-ATN-424, is not connected to an SSID on the selected folder or floor, then the search will not show any results.

When you type the (full or partial) MAC or IP address, User Name, or the device name in the Global Search box, a detailed information of the device is displayed. Refer to Clients and Access Points section that provide more information on clients and APs.

You must make a note of the following points when using Global Search:

- Global Search is not case-sensitive.
- The search results are segregated for clients and access points. The search result shows the device/client name, irrespective of the search criteria used.
• It lists out the devices/clients as you type the string or substring. For example, if you type lap, the search lists only the first 10 instances that have lap as part of their name or username along with a See More link. On clicking See More, you are redirected to the page with the complete search results.
• The search results are segregated for clients and access points.
• The search result shows the device/client name, irrespective of the search criteria used.
• You can search for clients in all categories:
  • Clients currently associated to an Arista AP
  • Clients associated to an Arista AP in the past
  • Clients that are trying to or have tried to connect (but failed) to an Arista AP
• It does not support pattern-based search with the use of special characters such as * or ?. For example, the Global Search will not list any results if you type la*.

3.3 Table level Operations
CloudVision WiFi provides a set of table level operations for the monitoring tables. These operations are available for the monitoring tables available on the MONITOR tab. Some or all the operations are applicable for the tables. These set of operations help users to filter the data or change the view of the table according to their convenience.

All the operations are available on the right top corner of the table.

Table level operations are:
• **Freeze Columns**: Freeze Columns operation allows user to freeze or unfreeze the columns on the table. To know more about this operation refer Freeze Columns.
• **Add/Remove Columns**: Add/Remove Columns operation is used to add or remove multiple columns. To know more about this operation refer Add/Remove Columns.
• **Filter**: Filter operation helps user to filter the data. This filtering of data helps user to either sort the data based on certain criteria or search any specific data. Depending on the column on which filter is to be applied, the filtering criteria may vary. You can filter the data by providing the range of values, or can always select the appropriate value from the provided options and many more.
• **Full Screen**: Selecting the Full Screen operation allows user to view the table in full screen mode. The same operation helps user to exit from full screen mode.

3.3.1 Freeze Columns
A vertical line on the monitoring table divides the table in two. The left section contains freeze columns. These columns are locked, making them always visible when scrolling vertically or horizontally in an open document. The right section contains unfreeze columns. These columns are unlocked.

Freeze Columns operation allows user to freeze or unfreeze these columns. Not more than five columns can be freeze. For every table there are at least two bi-default columns that are always freeze and can never be unfreeze.

To Freeze or unfreeze columns:
1. Click the Freeze Columns icon on the top right corner of the table.
2. List of all the columns with checkbox adjacent to their names appear.
3. Select or unselect the column you prefer to freeze or unfreeze.

3.3.2 Add/Remove Columns
Add/Remove Columns operation adds or removes the columns from the table. Bi-default all the columns are added in the table.

To add or remove the column:
1. Click the **Add/Remove Columns** icon on the top right corner of the table.
   List of all the columns with checkbox adjacent to their names appear.

2. Select or unselect the column you prefer to add or remove.

### 3.4 Filters on Widgets

Widgets in CloudVision WiFi allow you to view or retrieve the data using the filters. They are available to the right top corner of the widget.

The available filters are:

- SSID Filter
- Frequency Band Filter
- Duration Filter
- Mode of communication
- Conferencing Apps Filter
- Any Failure
- Any Issue

**Note:** All the filters may not be available for all the widgets. Their availability may vary for every widget.

#### SSID Filter

The information for charts or widgets can also be viewed for specific SSID. Selecting a specific SSID from the drop-down provides relevant data for the selected SSID. Selecting All SSIDs option provides aggregated data on a graph for all the SSIDs. The default value is **All SSIDs**.

![SSID Filter Example](image)

#### Frequency Band Filter

The data can be filtered based on frequencies. The data for applications working on the selected frequency is provided. The possible values for the frequency band filter are:

- 2.4 GHz
- 5 GHz
- 2.4 and 5 GHz

The default value is **2.4 and 5 GHz**.
Duration Filter

You can view or fetch the information for the following time intervals:

- 2 hours
- 4 hours
- 8 hours
- 12 hours
- 1 day
- 1 week
- 1 month

Selecting the specific time slot will provide data accordingly. For example, selecting 2 hours will provide statistical data for last 2 hours.

Note: All the provided time intervals may not be available for every widget.

Mode of communication

This option is only specific for the Application Latency's baseline graph. Select the mode of communication from the following options:

- Wired/Wireless
- Wired
- Wireless
The default value is **Wired/Wireless**.

**Conferencing Applications Filter**

Conferencing Applications Filter allows viewing the statistical data for a specific conferencing app. The available applications for which the data can be viewed are:

- WebEx
- Skype
- GoToMeeting
- Hangouts
- Slack
- Microsoft Teams
- Zoom

Selecting **All Conferencing Applications** option provides details for all the above-listed applications at once.

**Any Failure**

The Failure filter allows to view or retrieve data based on the available failure type. The applicable values are:

- Any failure
- Association
- Authentication
- Network
Selecting **Any Failure** option provides details for all the above-listed failures at once. The default value is **Any Failure**.

![Any Failure Options]

**Any Issue**

The Issue filter provides the output based on the selected issue. The applicable values are:

- Any issue
- Low RSSI
- Low Data Rate
- High Retry %
- Sticky Clients

Selecting **Any Issue** option provides details for all the above listed issues at once. The default value is **Any Issue**.

![Any Issue Options]

### 3.5 IPv6 Support in UI Fields

The following table lists UI fields that use IP addresses and whether they support only IPv4, or both IPv4 and IPv6.

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Supports IPv4</th>
<th>Supports IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configure Tab</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tunnel Interface</td>
<td>Primary / Secondary endpoint</td>
<td>Y</td>
</tr>
<tr>
<td>RADIUS Profile</td>
<td>RADIUS server IP Address</td>
<td>Y</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------------------</td>
<td>----</td>
</tr>
<tr>
<td>Role Profile</td>
<td>Redirect URL (when Redirection is enabled)</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>IP/ Hostname under Firewall Rules</td>
<td>Y</td>
</tr>
<tr>
<td>Device Settings</td>
<td>NTP Server IP/Hostname</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>Syslog server IP/Hostname under Device Access Logs</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>IP Addresses under Enable SSH IP Allow List</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>Server URL under Analytics Integration with Third-Party Server</td>
<td>Y</td>
</tr>
<tr>
<td>SSID</td>
<td>Network tab: IP addresses under NAT Configuration</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>Access Control tab: IP/Hostname under Firewall rules</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>Access Control tab: Redirect URL when Redirection is enabled</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>Analytics tab: Server URL when Push Analytics to Third-Party Server is enabled</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>Captive Portal tab: Websites that users can access before login</td>
<td>Y</td>
</tr>
</tbody>
</table>

**Troubleshoot Tab**

<table>
<thead>
<tr>
<th>Client Connectivity Test</th>
<th>URL to test internet access under Portal Authentication Test</th>
<th>Y</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IP Address/Hostname under Custom Application Test</td>
<td>Y</td>
<td>N</td>
</tr>
</tbody>
</table>

**System Tab**

<table>
<thead>
<tr>
<th>SMTP</th>
<th>SMTP Server IP</th>
<th>Y</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP-Alerts</td>
<td>SNMP Trap Destination Server IP/Hostname</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Syslog</td>
<td>Syslog Server IP/Hostname</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------------</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>WLAN Integration</td>
<td>Aruba Controller IP/Hostname</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td>Cisco Controller IP/Hostname</td>
<td>Y</td>
<td>N</td>
</tr>
</tbody>
</table>
Arista Navigator

4.1 Managing Navigator

Arista Navigator enables you to define a hierarchical structure to organize how your WLAN network is deployed. This hierarchical structure can be based on any criteria, such as the location where the APs are deployed, the organizational departments using a set of APs, Test vs Production network, and so on.

Arista Navigator comprises of folders and floors. Folders can represent any logical grouping such as departments of an organization, business units, physical locations such as country, city, and building, and so on. Floors can represent a more granular level of deployment such as a group using a common set of access points, or a physical location such as a floor in a building where the access points are deployed. For example, Hawaii Conference Room, Bldg 15-Cubicle G2, or Executive Area.

Click **System** to view, edit and manage the hierarchy of folders and floors. Only a Superuser, Administrator, and Operator user can edit Arista Navigator. Users with the Viewer role can only view the Arista Navigator.

The following figure shows Arista Navigator. Right-click on a folder or a floor to perform various tasks and edit Arista Navigator.
4.1.1 Add a Folder or Floor
You can add one or more folders under the root folder or under other folders. You cannot add a folder or a floor to the Unknown folder. Only Superuser, Administrator, and Operator can add a folder or a floor. A Viewer can only view the Arista Navigator.

To add a folder or floor, perform the following steps:

1. Click System.
   A hierarchy of folders and floors is displayed.
2. Select a folder under which you want to add a new folder or floor. Right-click and select Add a Folder/Floor.
   New Folder/Floor dialog box is displayed.
3. Select Folder to add a folder or select Floor to add a floor.
4. Type the name of the folder or floor and click Add.
   A new folder or floor is added under the selected folder.

   **Important:** You cannot add a folder or floor under a floor.

4.1.2 Add Multiple Folders or Floors
You can add multiple folders and floors at the same time. You can add multiple folders under the root folder or other folders. You can add multiple floors under a folder. You cannot add folders or floors under the Unknown folder.

To add multiple folders or floors, perform the following tasks:

1. Click System.
   A hierarchy of folders and floors is displayed.
2. Right-click a folder under which you want to add multiple folders and floors and select Add Multiple Folders/Floors.
   New Folders/Floors dialog box is displayed.
3. Type the folder and floor names in the given text area that you want to add.
   You can have only one name per line.
4. To create a hierarchy of folders and floors, use the Tab key.
   A sample hierarchy of folders and floors would look like this:
Important: Prefix * to make a floor. You cannot add a folder or floor under a floor.

5. Click Add.
Multiple folders and floors are added under the selected folder.

4.1.3 Delete Folders and Floors
Use this feature to get rid of unwanted and redundant folders and floors that are not applicable.
To delete the folders or floors, perform the following tasks:

1. Click System.
   A hierarchy of folders and floors is displayed.
2. Select the folders and floors that you want to delete.
3. Right-click any of the selected folder or floor and select Delete.
   A dialog box for Delete is displayed.
4. Click Delete to confirm the deletion.

A message is displayed that confirms the successful deletion of single or multiple folders or floors.

Important: Alternatively, you can also delete the folders and floors in a similar manner using the delete icon located above the hierarchy of folders and floors.

4.1.4 Rename Folder or Floor
Use this feature to change the name of a single or multiple folders or floors.
To rename a file, perform the following tasks:

1. Click System.
   A hierarchy of folders and floors is displayed.
2. Select the folders and floors that you want to rename.
3. Right-click any of the selected folder or floor and select Rename.
   The Rename dialog box is displayed.
4. Do the required changes and click Rename to save the changes.

A message is displayed that confirms the successful renaming of the selected folders or floors.

Important: You can also rename the folders and floors in a similar manner using the rename icon located above the hierarchy of folders and floors.

4.1.5 Search Folder or Floor
You can type a string of letters or the name of a folder or floor to locate it on the Navigator.
To search a folder, perform the following tasks:

1. Click System.
   A hierarchy of folders and floors is displayed.
2. Enter the text substring matching the name of the folder or floor in Search Folders/Floors text box.
   The folders or floors matching the pattern of the text string or substring is displayed along with the parent folder.

Note: Pattern-based search with the use of special characters, such as * and ? is not supported.
4.1.6 Set Timezone for Folders

Set the appropriate time zone for the selected folder using the System > Navigator page. Only a Superuser, Administrator, and Operator user can configure the location time zone for a location.

The time zone settings help in accurate analytics. Ensure that you select the correct time zone for the selected folder.

⚠️ Important: You cannot set a time zone for a floor. The time zone set for the immediate parent folder of a floor applies to the floor.

To set the timezone for a folder, perform the following tasks:

1. Go to System > Navigator.
2. On the Navigator page, right-click the folder name and select Set Timezone.
   The Set Timezone dialog box is displayed.
3. Select the appropriate timezone from the drop-down list and click Set.
   A message is displayed that confirms that the timezone was set successfully.

⚠️ Important: You can also set the timezone in a similar manner using the Set timezone icon.

4.1.7 Set Location Tag

To assign a location tag to a folder or floor, perform the following steps:

1. Go to System > Navigator > Folders/Floors.
2. Right-click the folder or floor to which you want to assign the tag.
3. On the right-click menu, select Location Properties > Location Tag.
4. In the Location Tag window, enter the location tag and click Set.
5. Select Apply recursively to subfolders if you want the same location tag to be used by child locations. When selecting this option, keep in mind that mDNS gateways return devices based on the location tag.

✨ Note: mDNS Packet Tagging uses the location tag to help WiFi clients locate network services such as printers. When assigning the location tag, note the following:

- Arista mDNS gateways truncate the location tag to the first 128 characters.
- We recommend that you use only numbers, letters, and hyphens in the location tag because Arista switches do not support special characters in mDNS tags.

4.2 Introduction to Groups

Until now CloudVision WiFi allowed users to configure only the WiFi configuration for a selected location. You couldn't do custom configuration on a device or a set of devices. To overcome this restriction, Groups have been introduced in CloudVision WiFi.

Groups will facilitate faster customization of Arista APs by allowing you to apply custom configuration (e.g., SSIDs, Radio Settings, and Device Settings) to APs located across different branches of a hierarchical location tree. A group will always have a unique name. You can access a group only if you can access the folder where the group was created. A user who does not have access to a group can view devices in that group, but cannot perform actions such as rename or delete.

After the group is created, you can configure it. You can configure a group either by turning an SSID ON at the folder where the group was created, or by modifying the Device Settings or Radio Settings.

APs in a configured group use the same configuration as the group. Moreover, each group has a single WiFi configuration. APs which are not part of any group will continue to use the WiFi
configuration of the location on which they are created. When you delete a location, groups at the deleted location are deleted and devices assigned to the group will be moved to their parent location.

Note: An Arista device can be part of one and only one group at a time.

4.2.1 Add a Group

To add a group, perform the following steps:

1. Go to System > Navigator > Groups .
2. Click the Plus Icon to add a group.

An Add Group dialog box opens, exposing the location name where the group is created.

3. Type a unique name for the group and click Add.

The group name should be unique across all the available groups and folders.

CloudVision WiFi searches for a common root folder (Root) for all the locations that a user can access and accordingly creates a group at that folder. If a user does not have permissions on the root folder, then the group will be created at the next topmost folder to which a user has access.

4.2.2 Delete a Group

Deleting a group would impact few of the functionalities:

• If a group is deleted, devices assigned to that group will start using the default WiFi configuration of their respective folders.
• Similarly, if you delete a folder, then the groups created under it will also get deleted. And the devices will start using the default WiFi configuration of their respective folders.

To delete a group, perform the following steps:

1. Go to System > Navigator > Groups.

A list of groups is displayed.

2. Right-click on the name of the group you want to delete or click on the menu icon (three vertical dots) and click Delete.

3. Click Yes.

A message is displayed that confirms the deletion of the Group.
4.2.2.1  **Show Assigned Devices**

This action results in showing the list of APs assigned to the particular group. Access Point listing would show columns: Name, MAC Address, Model, Group, and Location with the applicable filters. To know more in detail about the specified columns and applicable filters refer the topic Access Points.

![Note: This action is not allowed for multiple groups.]

To perform this action follow the below steps:

1. Go to **System ->Navigator ->Groups**.
2. Click on the three vertical dots next to the group for whom you choose to see the device list.
3. Select **Show Assigned Devices** option.

Access Point listing grid would be shown for the selected group with the group name.

4.2.2.2  **Rename a Group**

You can change the name of a group, if required.

To rename a group, perform the following steps:

1. Go to **System > Navigator > Groups**.
2. Right-click on the name of the group you want to rename or click on the menu icon (three vertical dots) and click **Rename**.
3. Change the name of the group and click **Rename** to save the changes.

A message is displayed that confirms the change in the name of the group.

4.2.2.3  **Delete a Group**

Deleting a group would impact few of the functionalities:

- If a group is deleted, devices assigned to that group will start using the default WiFi configuration of their respective folders.
- Similarly, if you delete a folder, then the groups created under it will also get deleted. And the devices will start using the default WiFi configuration of their respective folders.

To delete a group, perform the following steps:

1. Go to **System > Navigator > Groups**.
   A list of groups is displayed.
2. Right-click on the name of the group you want to delete or click on the menu icon (three vertical dots) and click **Delete**.
3. Click **Yes**.
   A message is displayed that confirms the deletion of the Group.
Baselines

CloudVision WiFi dynamically computes and updates a baseline for normal performance and connectivity of the network. The baseline adjusts as the network behavior changes, eliminating the false positive and false negative alerts associated with thresholds.

5.1 Baselines versus Thresholds

A baseline is used as a basis against which things are measured. Baselines have been traditionally used when you want to determine the effect of a change. For example, if you want to optimize your wireless network, you need to take a baseline of metrics such as retry rates or average data rates so that you can measure if the changes had a positive or negative impact.

A threshold is a level that must be exceeded to trigger an action. Thresholds are commonly used in network monitoring systems for alerts. For example, if a retry rate threshold were set at 50%, the system would trigger a warning when the retry rate exceeded 50%.

CloudVision WiFi studies the behavior from the historical data of clients, APs and applications, automatically calculates a baseline. The baseline is calculated at an interval of 15 minutes. Any behaviour that deviates significantly from the baseline is considered to be an anomaly and highlighted in the graph. In controller based network monitoring systems, thresholds are static and the same value gets applied globally. This creates problems for network admins because wireless network characteristics can be different in different environments.

Thresholds are good for monitoring information where there is a clear, non-arbitrary delineation between acceptable and not acceptable. Thresholds are static. They do not adjust to changing conditions. Wireless networks are dynamic and change over time. The normal level of retry rates may be very different today and a month from now. Clients change, environments change, applications change, and usage changes rapidly. A static threshold is a challenge because it doesn't adapt to what is normal for the network. Then, if some metric regularly crosses its static threshold, the network admin is bombarded with irrelevant warnings. The network admin must then go in and reset the threshold. The problem lies in determining what the correct threshold is. If the threshold is set low, there will be too many alarms as to cause alarm fatigue. This is dangerous because valid alarms are lost in the sea of unimportant, false positive alarms. To counter alarm fatigue, many network admins set the threshold too high. This is dangerous because valid problems (false negatives) do not trigger action.

5.2 How to Read a Baseline Graph?

CloudVision WiFi takes the idea of the baseline and makes it dynamic. Dynamic baselines determine what is normal for a network and adjust as network conditions change. For example, retry rates may be low when the WiFi is first set up with only a few clients. Later, when many more clients are added to the WiFi network, the retry rate may be very different. Dynamic baselines adjust as networks change. This avoids the problem of thresholds while allowing comparisons to the baseline to identify real problems.

Each baseline graph is made up of these four elements:

- Baseline - Blue line
- Deviation Range - the light blue shaded area around the baseline
- Observation points - Purple dots are an average of the data at 15 minute intervals
- Anomalies - Red dots are observation points that are well outside the norm

The Baseline Graph has a provision to filter data. You can zoom in and zoom out the graph to view the granularity in detail. The zoom feature is at the bottom of the graph.

5.3 CloudVision WiFi Baselines

CloudVision WiFi includes baselines for both connectivity and performance events. The table below lists the available baselines and where they can be found on the CloudVision WiFi interface.

Note: Wherever applicable, CloudVision WiFi shows separate baselines for IPv4 and IPv6.

<table>
<thead>
<tr>
<th>Type</th>
<th>Baseline Chart</th>
<th>Per</th>
<th>Location on CloudVision WiFi UI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connectivity</td>
<td>Clients Affected by Failures</td>
<td>Location</td>
<td>DASHBOARD / Connectivity</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AP</td>
<td>MONITOR / Access Points / AP Drill Down</td>
</tr>
<tr>
<td></td>
<td>Baseline - AAA Latency</td>
<td>Location</td>
<td>Dashboard / Performance / Avg. Latencies Chart / AAA Drill Down</td>
</tr>
<tr>
<td></td>
<td>Baseline - DHCP Latency</td>
<td>Location</td>
<td>Dashboard / Performance / Avg. Latencies Chart / DHCP Drill Down</td>
</tr>
<tr>
<td></td>
<td>Baseline - DNS Latency</td>
<td>Location</td>
<td>Dashboard / Performance / Avg. Latencies Chart / DNS Drill Down</td>
</tr>
<tr>
<td>Performance</td>
<td>Data Rate</td>
<td>Client</td>
<td>MONITOR / Clients / Clients Drill Down</td>
</tr>
<tr>
<td></td>
<td>Retry Rate %</td>
<td>AP</td>
<td>MONITOR / Access Points / AP Drill Down</td>
</tr>
<tr>
<td></td>
<td>Client Affected by Poor Performance</td>
<td>Location</td>
<td>Dashboard / Performance</td>
</tr>
</tbody>
</table>

### Baselines

<table>
<thead>
<tr>
<th>Type</th>
<th>Baseline Chart</th>
<th>Per</th>
<th>Location on CloudVision WiFi UI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clients Affected</td>
<td>AP Located in location</td>
<td>Location</td>
<td>MONITOR / Access Points / AP Drill Down</td>
</tr>
<tr>
<td>% Poor Application Experience</td>
<td>Located in location</td>
<td>Location</td>
<td>Dashboard / Applications</td>
</tr>
<tr>
<td>Baseline - Application Latency</td>
<td>Located in location</td>
<td>Location</td>
<td>Dashboard / Performance / Avg. Latencies Chart / Application Drill Down</td>
</tr>
</tbody>
</table>

**Note:** You can filter the data on each of these widgets. To know more about filters refer Filters on Widgets.

**Example 1: Baseline - Clients Affected by Failures (AP Based)**

The chart provides a baseline for the clients affected by connection failures for the selected AP.

The data points are determined by the total number of connected clients and the last connectivity state of clients in a 15-minute interval. When you hover on the data point it provides a tooltip. The tooltip contains the consolidated information in the percentage that indicates the good and bad experience of the clients along with the calculated baseline for the given point of time. Click the data point on the graph to retrieve the detailed information.

**Example 2: Baseline - Data Rate**

The following image displays the baseline graph for Data Rate:
The graph displays the calculated baseline of the average data rate consumed by an individual client. The anomalies are calculated by comparing the data rate against the globally configurable threshold. Data Rate is a metric where what is acceptable is not unique per network or environment so the use of a threshold to detect anomalies is appropriate. The baseline and deviation band are still calculated, but anomalies are determined by the data rate threshold.

5.4 Data Reporting and Retention

Client connection success and failure with root cause analysis are reported by the AP to Arista Cloud almost immediately after it occurs. Performance and other data are aggregated and reported every 15 minutes.

Except for Client Application Data, the last week’s worth of information is retained in the cloud and available in CloudVision WiFi.

<table>
<thead>
<tr>
<th>Data Type</th>
<th>AP Reporting Interval</th>
<th>Cloud Storage Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Connection Attempts</td>
<td>Immediately</td>
<td>1 week</td>
</tr>
<tr>
<td>AAA, DHCP, DNS, &amp; TCP Latencies</td>
<td>Soon after detection</td>
<td>1 week</td>
</tr>
<tr>
<td>Client Application Data</td>
<td>15 minutes</td>
<td>12 hours</td>
</tr>
<tr>
<td>Client Performance Metrics</td>
<td>15 minutes</td>
<td>1 week</td>
</tr>
<tr>
<td>BSSID Performance Metrics</td>
<td>15 minutes</td>
<td>1 week</td>
</tr>
<tr>
<td>SSID Application Data</td>
<td>15 minutes</td>
<td>1 week</td>
</tr>
<tr>
<td>Baseline Data</td>
<td>15 minutes</td>
<td>1 week</td>
</tr>
</tbody>
</table>
## 5.5 Data Point Drill Down

The below table contains the attributes specifying the detailed info about the connected clients. The info is available in the tabular format on data point drill down from any baseline chart. The attributes with no specific name of a baseline chart are common for all the charts.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the client.</td>
</tr>
<tr>
<td>User Name</td>
<td>User name of the client.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>A unique 48-bit IEEE format address of the client assigned to the network adapter by the manufacturer.</td>
</tr>
<tr>
<td>Last Failure Time <em>(Available for Baseline - Clients affected by failure)</em></td>
<td>The latest date and time when the client failed to connect to the network.</td>
</tr>
<tr>
<td>Associated SSID</td>
<td>SSID of the WLAN to which the client is connected.</td>
</tr>
<tr>
<td>Associated Access Point</td>
<td>The AP with which a client is associated. This is the AP through which the client communicates with other clients and devices on the network.</td>
</tr>
<tr>
<td>Location</td>
<td>Location of the client.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the client.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Indicates the 802.11 protocol used.</td>
</tr>
<tr>
<td>Channel</td>
<td>Operating channel of the AP to which the client attempted to connect.</td>
</tr>
<tr>
<td>OS</td>
<td>Name of operating system running on the client.</td>
</tr>
<tr>
<td>Average RSSI(dBm)</td>
<td>The observed RSSI (Received Signal Strength Indicator) value for the client.</td>
</tr>
<tr>
<td>Up/Down Since</td>
<td>The latest date and time since when the client is up or down.</td>
</tr>
<tr>
<td>Connected/Disconnected Since <em>(Available for Baseline - Clients Affected by Poor Performance graphs)</em></td>
<td></td>
</tr>
<tr>
<td>First Detected At</td>
<td>The date and time when the client was first detected.</td>
</tr>
<tr>
<td>Role</td>
<td>The role assigned to the client on associating with an SSID.</td>
</tr>
<tr>
<td>Google Authorized</td>
<td>A boolean value indicating whether the client is in the authorized list of clients imported through Google Integration.</td>
</tr>
<tr>
<td>Vendor Name</td>
<td>Indicates the vendor name.</td>
</tr>
<tr>
<td>Uplink Data <em>(Available for Baseline - ClientsAffected by Poor Performance graphs)</em></td>
<td>The amount of data transferred by the client.</td>
</tr>
<tr>
<td>Downlink Data <em>(Available for Baseline - ClientsAffected by Poor Performance graphs)</em></td>
<td>The amount of data received by the client.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Retry Rate (Not available for Baseline - Clients affected by failure)</td>
<td>The retry rate in percentage.</td>
</tr>
<tr>
<td>Sticky (Not available for Baseline - Clients affected by failure)</td>
<td>A boolean value indicating if the client is a &quot;sticky client&quot;, i.e., if it is connected to an AP even though it sees better signal strength from a neighboring AP.</td>
</tr>
<tr>
<td>Application Name (Available for Baseline - Poor Application Experience)</td>
<td>Name of an application.</td>
</tr>
<tr>
<td>Application Usage Time (Available for Baseline - Poor Application Experience)</td>
<td>The time duration for which a client has accessed an application.</td>
</tr>
<tr>
<td>Poor Application Experience (Available for Baseline - Poor Application Experience)</td>
<td>The poor application usage experience for a client connection.</td>
</tr>
<tr>
<td>Uplink Bitrate (Available for Baseline - Poor Application Experience)</td>
<td>The rate at which the client transmits data (in bits).</td>
</tr>
<tr>
<td>Downlink Bitrate (Available for Baseline - Poor Application Experience)</td>
<td>The rate at which the client receives data (in bits).</td>
</tr>
<tr>
<td>Downlink Jitter (Available for Baseline - Poor Application Experience)</td>
<td>Variation in the delay of packets received by a client. It is used to measure the quality of VoIP applications.</td>
</tr>
<tr>
<td>Uplink Jitter (Available for Baseline - Poor Application Experience)</td>
<td>Variation in the delay of packets transferred by a client. It is used to measure the quality of VoIP applications.</td>
</tr>
</tbody>
</table>
Dashboards

CloudVision WiFi provides varied widgets on its Connectivity and Performance dashboards that promote actual cause of issue, not just related client statistics, to drive faster troubleshooting efforts. With Dashboards, you receive immediate feedback when performing remediation thus democratizing Wi-Fi troubleshooting for level one and junior support staff.

Where applicable, dashboard widgets show values for both IPv4 and IPv6. This gives a more granular view of the network. For example, the Average Latencies widget on the Performance Dashboard shows the latency values for both v4 and v6 paths, helping you identify if the issue lies with only one of the IP addresses.

6.1 Connectivity Dashboard

The Connectivity Dashboard provides the health of all the clients and devices that are present in a WLAN network, on the selected folder or floor. It comprises of a number of widgets which provide information of the connectivity strength in a single glance.

Navigate to Dashboard > Connectivity to view the Connectivity Dashboard.

The Connectivity Dashboard contains the following widgets:

**Client Journey**
It provides an overview of various aspects of the client such as number of active clients, associations to the Wi-Fi, successfully authenticated clients, total number of clients connected to the network, and number of online clients.

**Clients by Most Failed Connections**
Lists the number of times a client failed to connect. The clients are listed in decreasing order of failed attempts and then alphabetically.

**Top Locations Affected by Failures**
Displays the top five locations which are affected by association, authentication or network failure. The locations are listed in decreasing order based on the percentage of connection failures.

**Baseline - Clients Affected by Failures**
CloudVision WiFi calculates a baseline for the percentage of clients that failed due to connectivity issues. The connectivity issues taken into consideration are: Authentication failure, Association failure, and Network failure.

6.1.1 Client Journey

Client Journey depicts the current state of the network for the selected folder or floor. It provides an overview of various aspects of the client such as number of active clients, associations to the Wi-Fi,
successfully authenticated clients, total number of clients connected to the network, and number of online clients.

You can hover the mouse over the different phases of the client journey to get additional information. For example, if you hover the mouse over the Authentication phase, a tool tip displays information such as percentage of authenticated clients, number of clients who failed to authenticate, type of authentication failure with the number of clients that failed to authenticate for a type of authentication.

You can click on the different phases to view detailed information of each phase. For example, if you click Association, you will be redirected to a page that provides detailed information of the client health displaying a list of clients that failed to associate.

The client journey is presented on the Connectivity Dashboard as follows:

**Total Clients**

The Total Clients section displays the number of clients that connected or tried to connect to the network. It includes the total number of clients that associated with an SSID on the network and the total number of clients that failed to associate. Click Total Clients to view a list of clients with their detailed information.

**Association**

The Association section displays the total number of clients that are successfully associated to a Wi-Fi network and the total number of clients that failed to associate to the Wi-Fi network. Click Associations to view a list of clients with failed associations.

**Authentication**

The Authentication section displays the total number successfully authenticated clients and the clients that failed to authenticate through the Wi-Fi network.

**Network**

The Network section displays the total number of clients that could successfully access the network services like DHCP, DNS and also those that failed to access these services.

**Online**

The Online section displays the total number of online clients that successfully connected to the Wi-Fi network. It also displays the total number of clients that failed to authenticate, associate or access the network.

You can search a client by providing MAC address, IP address, user name or device name. You get the status of the various phases of that client, with the time stamp.
Dashboards

Search Icon on Client Journey

You can search an active client by providing MAC address, IP address, user name or device name. You get the status of the last attempted connection, in the various phases of the active client, with a time stamp.

Only those active clients that are available on a selected folder or floor can be searched. Therefore, if a client with device name, say LAP-ATN-424, is not connected to an SSID of the selected folder or floor, then the search for such a client will show the following:

- **No connection records found in currently active clients**: No results are displayed because the searched active client is not available on the selected folder or floor.
- **Search historical client records?**: A link that suggests to look for the searched client in the historical records. This option is displayed when the searched client was active in the past and unavailable at the moment. After clicking on the link, you are redirected to the list of clients and you can click on the name of the client for a detailed information. Refer Client Connection Logs for more information about the logs. The historical data for the last seven days is available in the logs.

If the searched client is active and connected to an SSID of the selected folder or floor, you can view the status of the last attempted connection, in the various phases of the client connection with a timestamp. The following figure shows the various phases of the client connection:

When an active client is searched, the widget displays the following information for the various phases:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tried to connect</td>
<td>Name of the client and a link that redirects you to the Connection log for the searched active client.</td>
</tr>
</tbody>
</table>
| Association  | • Status (Successful or Failed)  
• The timestamp when the association was successful  
• The name of the AP the client is connected to  
• The name of the SSID |
| Authentication | • Status (Successful or Failed)  
• The timestamp when the authentication was successful  
• The name of the authentication server and the average latency time |
| Network      | • Status (Successful or Failed)  
• The timestamp of last successful connection  
• The name of the authentication server and the average latency time |
| Online       | • Status (Successful or Failed)  
• The timestamp of last successful connection |
The data on the widget can be filtered using the available filters on the top right corner of the widget. To know more about the filters refer Filters on Widgets.

6.1.2 Top Locations Affected by Failures

The widget displays a horizontal bar graph depicting the top five locations that are affected by association, authentication, or network connection failure. The graph contains the data for the selected parent and its immediate child folders.

The graph shows the top five locations with highest connection failure percentage in decreasing order. If you hover the mouse over a bar in the graph, the tool-tip displays the number of clients that are affected due to the connectivity failure with respect to the total number of clients associated to an AP at that location. When you click a bar, on that location, you are redirected to a page that has detailed information of the clients affected by the connection failure at that location.

You can select the failure type from the drop-down list given on the top-right corner of the widget. To know more about the Any failure filter refer Filters on Widgets.

![Top Locations Affected by Failures]

6.1.3 Clients by Most Failed Connections

Clients by Most Failed Connections lists the number of times a client failed to connect. The clients are listed in a decreasing order of failed attempts and then alphabetically.

The data is represented in tabular format displaying the name of the client that failed to connect and the total number of times the client failed to connect. Refer to the following widget for a sample listing.

![Clients by Most Failed Connections]

When you click on the client name, you are directed to the Client connections log widget, where you get the detailed information of the failures. The maximum duration supported by the graph is 1 week.
and the minimum duration is 2 hours. You can select the duration from the drop-down list which is located at the top-right corner of the widget.

6.2 Performance Dashboard

The Performance Dashboard provides detailed information about the performance of the Wi-Fi network with the help of a number of graphs and widgets.

Navigate to Dashboard > Performance to view the Performance page. The page contains the following graphs and widgets:

<table>
<thead>
<tr>
<th>Graph/Widget</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Health</td>
<td>Displays the total number of clients for the selected folder or floor, with Low RSSI, Low Data Rate, High Retry %, and Sticky Clients.</td>
</tr>
<tr>
<td>Avg Latencies</td>
<td>Displays the average latency time (response time) taken by the servers like DHCP, DNS, and AAA servers with respect to the clients on a selected folder or floor.</td>
</tr>
<tr>
<td>Baseline - Clients Affected by Poor Performance</td>
<td>Displays the baseline for the percentage of clients affected by poor performance for all the clients over a period of time.</td>
</tr>
<tr>
<td>Clients by Avg. Data Rate</td>
<td>Displays a bar graph that shows the average data rate of the clients on a selected folder or floor.</td>
</tr>
<tr>
<td>Clients by RSSI</td>
<td>Displays a bar graph showing the total number of clients and the RSSI values.</td>
</tr>
<tr>
<td>Clients With Most Traffic</td>
<td>Displays a horizontal bar graph of clients with highest data usage.</td>
</tr>
<tr>
<td>Top Locations Affected by Poor Performance</td>
<td>Displays a horizontal bar graph of locations with highest performance issues, in a decreasing order.</td>
</tr>
<tr>
<td>Network Usage</td>
<td>Displays a line graph showing the number of client association and a bar graph that shows the traffic volume.</td>
</tr>
</tbody>
</table>

6.2.1 Client Health

Client Health displays, for the selected folder or floor, clients that have Low RSSI, Low Data Rate, High Retry %, and those that are Sticky Clients. The Total Affected field shows the total number of clients on this folder or floor affected by these issues. Go to Dashboard > Performance to view the Client Health widget.

The values in the Client Health widget are clickable. For example, if you click the Low RSSI value, you will be redirected to a page that lists all the clients with low RSSI values and their relevant details. With reference to the image below, if the widget shows four clients with a low RSSI value, then on clicking the Low RSSI value, you will be redirected to a page that has detailed information of the four clients. The clients could be active or inactive. The information is updated every 2 minutes.
The Client Health widget lists the following:

**Total Affected**

Some clients could have more than one issue — for example, both Low RSSI and Low Data Rate. Such clients would then appear in both categories. CloudVision WiFi ensures that such clients aren’t counted twice and shows the total number of distinct clients affected by the issues listed below in the Total Affected field.

**Low RSSI**

The number of clients that are below the set RSSI threshold value.

**Low Data Rate**

The number of clients that are below the set data rate value.

**High Retry %**

The number of clients that have the retry rate % more than 20%. Retry rate % is the number of retry packets divided by the total number of data packets of a client.

**Sticky Clients**

The number of sticky clients present on the selected folder or floor.

A Sticky Client is a device that tends to stay associated with an access point, even when the signal strength is poor, rather than roaming to another Access point in the vicinity that might offer better signal strength.

---

**Note:** For more information on setting threshold values, refer to Set Threshold for a Folder or Floor.

**6.2.2 Average Latencies**

Average latencies shows the average latency time (response time) taken by servers like DHCP, DNS, AAA and Network servers with respect to the clients that are present on a selected folder or floor.

The average latency is calculated for the following services:

- DHCP
- DNS
- AAA
- Application
6.2.3 Clients by Average Data Rate

Clients by Average Data Rate is a widget that displays the average data rate consumed by the clients on the selected folder or floor.

Navigate to Dashboard > Performance to view the Clients by Average Data Rate widget. There are a number of clients accessing data through the Wi-Fi network. This widget calculates and displays a graph of the average data rate used by the total number of clients. You can set the threshold for the data rate.

In the image, you can see a bar graph in three colors; red, green and yellow. The classification is as follows:

- The clients with data rate, below the set threshold value are in red.
- The clients with data rate above the set threshold value are in green.
- The clients that are in the bucket where the threshold value falls, are in yellow. For example, in the above image, a threshold value that is set as 75 Mbps, falls in the bucket of 50 MBps to 100 Mbps. The clients that have threshold values between 50 Mbps and 100 Mbps are marked in yellow.

Refer Set Threshold for a Folder or Floor for more information on how to set a threshold value.

The data on the widget can be filtered using the available filters on the top right corner of the widget. To know more about the filters refer Filters on Widgets.

6.2.4 Clients by RSSI

Clients by RSSI is a widget that displays the average RSSI (dBm) of the clients on the selected folder or floor.

Navigate to Dashboard > Performance to view the Clients by RSSI widget. Clients accessing the network can have varied RSSI levels. This widget calculates and displays the average RSSI used by the total number of clients. You can set the threshold for RSSI.
In the image, you can see a bar graph in three colors; red, green and yellow. The classification is as follows:

- The clients with RSSI, below the set threshold value are in red.
- The clients with RSSI above the set threshold value are in green.
- The clients that are in the bucket where the threshold value falls, are in yellow. For example, in the above image, a threshold value that is set as -60 dBm, falls in the bucket of -65 dBm to -55 dBm. The clients that have threshold values between -65 dBm and -55 dBm are marked in yellow.

Refer Set Threshold for a Folder or Floor for more information on how to set a threshold value.

6.2.5 Clients with Most Traffic

Clients with Most Traffic widget displays a bar chart showing clients with highest data usage. The data shown is for clients on the selected folder or floor.

Top 5 clients names with highest data usage in a network are listed in decreasing order. When you click on the name of the client you are redirected to the Client details page where detailed information of the client activities is presented. If you hover the mouse over the list, you can view the total amount of data used by a client. You can select the duration from the drop-down list that is located on the top-right corner of the widget.

The data on the widget can be filtered using the available filters on the top right corner of the widget. To know more about the filters refer Filters on Widgets.

6.2.6 Top Locations Affected by Poor Performance

The widget displays a horizontal bar graph depicting the top five locations and their clients, that are affected by poor performance of Wi-Fi network. The graph contains the data for the selected parent and its immediate child folders.

The poor performance is calculated based on the following factors:

- Low RSSI
- Low Data Rate
- High Retry %
- Stickey Clients
Top 5 locations with poor performance issues, on the selected folder or floor is listed in a decreasing order.

If you hover the mouse over the bar in the chart, the tool-tip displays the number of clients affected by poor performance with respect to the total number of clients on that location. When you click on a bar you are redirected to a page that lists all the clients that are affected by poor performance. For example, if you click the Low RSSI value, you will be redirected to a page that lists all the clients with low RSSI values and their relevant details at that location.

You can select the type of factor from the drop-down list given on the top-right corner of the widget.

The data on the widget can be filtered using the available filters on the top right corner of the widget. To know more about the filters refer Filters on Widgets.

6.2.7 Network Usage

You can access the Network Usage chart in two different ways from CloudVision WiFi UI. If you access the chart from the performance dashboard, it displays a line graph showing the number of clients associated with the SSID and its traffic volume, for all the clients on the selected folder or floor. Whereas when you access the chart through AP drill down, it displays similar data, but this time for the selected AP.

If you hover over the graph, a tooltip providing quick information like timestamp, the number of clients associated and the used traffic volume appears.

You can view or retrieve data using the filters. To know more about these filters refer Filters on Widgets.

The data of the network usage chart can be filtered based on two parameters; a client's data and the amount of data used by an application.
Drill down on the **data point** on the graph, redirects you to the page containing client connections table. This table contains the list of all the client connections along with their detailed information for the selected timestamp. For client details refer, Filtered Network Usage Chart

Drill down on the **bar**, redirects you to another page that contains:

- **Client Connections table** - contains the list of all the client connections along with their detailed information for the selected timestamp.
- **Top Applications** - that shows top ten applications with highest data usage. You can select an app from the drop-down list given on the top left corner of the table. Along with the selected application name it displays application specific data consumption.
- **All Application traffic** - it displays the total amount of data used by the applications for a selected Access Point or a location. This information is shown at the top-right corner of the table.
- **Client Connections** - selecting client connection displays the list of all the clients using the application selected from the top applications list.
- **Access Points Distribution** - selecting access points distribution displays the list of all the associated APs.

### 6.2.8 Set Data Rate and RSSI Threshold for Folder or Floor

Thresholds are global settings and can be configured only on the root folder. You must be a Superuser, Administrator, or Operator to set the thresholds. If you have the Viewer privileges, you can only view the thresholds. The same threshold values are applicable on all the folders and floors in the Navigator.

You can set the threshold values for RSSI and data rate. The range for these are as follows:

<table>
<thead>
<tr>
<th>Threshold Name</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Rate</td>
<td>20 Mbps to 100 Mbps</td>
</tr>
<tr>
<td></td>
<td>For example, if the threshold value is 80, clients below the set Data Rate threshold will be classified as Low Data Rate clients.</td>
</tr>
<tr>
<td>RSSI</td>
<td>-45 dBm to -75 dBm</td>
</tr>
<tr>
<td></td>
<td>For example, if the threshold value is -60, the clients below the set RSSI threshold will be classified as Low RSSI clients.</td>
</tr>
</tbody>
</table>

To set the threshold values, perform the following tasks:

1. Go to DASHBOARD > Performance.
2. Ensure that you are in the correct folder or floor in the Location tree.
3. Click Set Thresholds.
4. On the Set Thresholds page, type the values for Low RSSI and Low Data Rate, within the allowed range.
5. Save the settings.

CVW uses the threshold values to render various charts, such as Client Health, Clients by Average Data Rate, and so on.
6.3 Applications Dashboard

The applications dashboard gives you the quality of experience of each monitored application. You get an overall view of top ten applications that have maximum traffic in your network. The baseline gives you an insight into the percentage of poor application experience over a period of time.

6.3.1 Application Experience

Navigate to Dashboard > Applications to view the Application Experience chart. You can monitor the performance of web-based enterprise applications (such as Email applications, HR and Project Management applications, Intranet, Online Drive, and others) along with VOIP-based applications such as Zoom, Hangouts, and others. Arista APs capture essential details of the TCP flows of a web application and send it to the server to determine the health of the application. If the overall health is calculated as poor, CVW displays the percentage of application experience for the duration. A lower percentage indicates a poor application experience whereas a higher percentage indicates a good application experience.

The Clients by Application Experience widget provides a client distribution for aggregated application experience or experience for each application.

Note:

- Web applications running on UDP are not supported for Web Quality of Experience (QoE).
- The algorithm only inspects information carried in the IP and TCP headers for each TCP stream that are related to the monitored applications. It doesn’t inspect the user's data in the process.
- Only the 802.11 ac Wave 2 and WiFi 6 APs support QoE monitoring of web-based applications.

By default, the most affected or most used applications are shown in a card view in the Dashboard > Applications tab. If you have a preference for specific applications, you can also pin them to the Application Experience widget.

In each card, the red bar indicates the percentage of poor application experience, whereas the green bar indicates the percentage of good application experience. If we take the case of Google APIs and Youtube in the above image, the Google API users faced poor application experience 56% of the time, whereas the YouTube users faced poor application experience 30% of the time.
You can also view the application health for a specific SSID using the SSID filter (it’s set to “All SSIDs” by default). Select All SSIDs to see a graph of the aggregated data for all SSIDs and all applications.

The data can also be filtered based on frequencies. Selecting a band shows you the data for all applications running on the band. The possible values for frequency filter are:

- 2.4 GHz
- 5 GHz
- 2.4 and 5 GHz

When you click any application card, you drill down to application details. The application details are provided using the following widgets:

- Baseline - %Poor App Experience
- Application Traffic
- Application Traffic - Clients
- Application Traffic - Sessions
- Application Traffic - Quality of Experience
- Clients using this Application
- Clients with Most Application Traffic

6.3.2 Monitor Selected Applications

You can monitor a maximum of 25 applications for application experience, including TCP and VOIP-based applications.

Web QoE is a global setting and you must configure the applications to monitor at the root folder. You can’t have a different Web QoE setting for each folder in the Navigation tree.

1. Go to DASHBOARD > Applications tab. Ensure that you are at the root folder.
2. On the Application Experience widget, click the Monitor Application Experience icon.
3. On the Monitor Application Experience right panel, click Add to monitor the applications. You can add up to 25 applications for monitoring.
4. Save the list of selected applications.

The selected applications are added to the Application Experience widget.

6.3.3 Monitor Custom Applications

Your organization may use applications that are not predefined in CVW. You may want to monitor such applications for QoE. Add such applications as custom applications and monitor them from Dashboard.

Follow these steps to add and monitor custom applications:

1. Go to DASHBOARD > Applications tab. Ensure that you are at the root folder.
2. On the Application Experience widget, click the Monitor Application Experience icon.
3. On the Monitor Application Experience right panel, click Custom Applications.
4. Provide the Application Name, IP address and port number used by the application. The application is added to the Monitor Application Experience right panel. Use the Plus icon to add multiple applications.
5. Save the applications.
6. On the Monitor Application Experience right panel, search the custom application and click **Add**.

### 6.3.4 View and Pin Applications on the Dashboard

On the landing page of Applications Dashboard, the Application Experience widget displays only 5 applications out of 25 in a card view. To see the card view of all 25 applications, click **Show All**.

You can choose which applications you want to view on the landing page by pinning your desired applications. To pin the applications on the Dashboard landing page for default view, click **Show All** in the Application Experience widget. Pin the application using the Pin button.
If you don’t pin any applications, then CVW displays the applications based on its usage or application experience. Use the Most Affected or Most Used filter to view the applications without pinning them.

### 6.3.5  Clients by Application Experience Widget

The widget shows the application QoE by client count for each application in the last 2 hours. There is also an aggregated view which shows how many clients had poor experience across all selected applications in the last 2 hours. To display the application experience graph for a single application, click **All Selected Applications** and then select the application from the list.

The application QoE is available for the last two hours. For example, in the following image, you can view the application experience for the Google Hangouts application in the last 2 hours. So, from the image you can infer that in the past 2 hours, around 10 clients faced poor application experience.
between 90 to 100 percent of the time, which indicates a bad user experience. Similarly, around 12 clients faced poor application experience between 0 to 10 percent of the time, which indicates a good user experience.

### 6.4 Logical Categorization of Clients and Failures

CloudVision WiFi creates logical categories of clients, grouping them based on properties such as their band of operation (2.4GHz or 5GHz), OS type, etc. You can then drill-down from Client Journey and troubleshoot issues based on these client properties - for example, you can check if Association failures occurred for clients on a particular band. The grouping of clients into meaningful logical categories speeds up Root Cause Analysis (RCA) of client connectivity issues. You no longer need to spend time trying to extract patterns from a row-column grid of data.

CloudVision WiFi logically groups clients into categories based on the following properties:

- **OS Type** - The client operating system type, e.g. Android, iOS.
- **Protocol / Band** - The 802.11 protocols or bands the client is operating on, e.g. b/g, ac.
- **Manufacturer** - The client manufacturer, e.g. Apple, Samsung.
- **Sticky Status** - Indicates if it is a "sticky client", i.e., if it is connected to an AP even though it sees better signal strength from a neighboring AP.

The Dashboard > Connectivity and Performance views show clients grouped by categories.

### 6.4.1 Drill-Down by Logical Client Category

You can drill-down and analyse client Connectivity and Performance issues by filtering on logical client categories - for example, you can view all Authentication failures for Windows 10 clients.

To analyse connectivity issues by logical client categories:

1. Go to DASHBOARD > Connectivity > Client Journey.
2. Select the stage in the client journey that you want to analyse.
   - For example, to analyse Authentication failures, select Authentication.
You will see the list of clients that failed authentication, with filter tabs for the most prominent characteristics, i.e., logical groupings. For example, the following figure shows tabs for client Protocol, Operating System, Vendor, and Associated Access Point.

3. Select the characteristic (i.e. logical category) by which you want to filter the list of clients.
   For example, to see the list of Windows 10 clients that failed authentication, select the **Microsoft Windows10** filter tab.
   The following figure shows a filtered list of Windows10 clients that failed authentication.

4. You can see the distribution of clients across logical categories by selecting the pie chart to the right of the filter tabs.
   A Distribution window pane opens up, containing client details grouped by logical categories such as Manufacturer, OS Type, etc. as shown below. You can then select a category from this window to filter the list of clients by that category.
Chapter 7

Monitoring WiFi

The Monitoring tab in CloudVision WiFi is primarily used for monitoring the Clients, APs, Radios, WLANs, and Applications in the network. You can perform troubleshooting operations based on the information collected for each of the components that the Monitoring tab monitors.

Select **MONITOR** tab from the left panel to get an overall view of your network that is categorized into the following tabs:

**Clients**
- Presents a list of clients connected to and clients that failed to connect to Arista devices.

**Access Points**
- Lists the Arista devices that are operating in AP or in AP/Sensor mode.

**Radios**
- Lists the radios operating on 2.4GHz and 5 GHz frequencies.

**WLANs**
- Lists the SSID profiles

**Application Visibility**
- Lists the applications with details about their data usage for a specific SSID.

The **global counters** at the top-right corner provide you the summary of Clients and Access Points.

You can use global counters to get the count of:

- Total Access Points
- Total Active Access Points
- Total Inactive Access Points
- Total Currently Online Clients

### 7.1 Clients

The Clients tab displays the clients that are connected to Arista devices. The type of Clients differ depending on their association with Arista AP.

The Client grid has drop-down list at the top-right corner, with options **Live** and **All**. The clients are listed on the following criteria:

If you select Live: A list of clients with the following status are displayed:

- Clients that are successfully connected to Arista APs.
- Clients that failed to connect.

If you select All: A list of clients with the following status (including Live clients) are displayed:

- Clients that are successfully connected to Arista APs.
- Clients that failed to connect.
- Clients that are currently visible but not connected to an Arista AP.
- Clients that are currently not visible, but connected earlier to an Arista AP.
- Clients that are currently not visible and failed to connect in their last attempt.

To know the status, hover the mouse over the Status icon.

When you click the name of a client, you are redirected to the Client Connection Logs widget.
The following properties of clients are displayed in a tabular format:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Indicates if the client is successfully associated or failed to connect.</td>
</tr>
<tr>
<td>Name</td>
<td>Specifies the user-defined name of the client.</td>
</tr>
<tr>
<td>User Name</td>
<td>Provides Username of the client.</td>
</tr>
<tr>
<td>Role</td>
<td>After client is connected via any SSID, it is assigned with Role configured in SSID profile.</td>
</tr>
<tr>
<td>Google Authorized</td>
<td>It is boolean value to represent whether client is authorized using google integration.</td>
</tr>
<tr>
<td>Location</td>
<td>Location of the client.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Specifies the unique 48-bit IEEE format address of the client assigned to the network adapter by the manufacturer.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the client.</td>
</tr>
<tr>
<td>OS</td>
<td>Name of Operating System running on the client.</td>
</tr>
<tr>
<td>Associated AP</td>
<td>Specifies the AP with which a client is associated. This is the AP through which the client communicates with other clients and devices on the network.</td>
</tr>
<tr>
<td>Associated SSID</td>
<td>Specifies the operating SSID of the AP with which the client is associated.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------------------------------------------------------</td>
</tr>
<tr>
<td>Avg. data rate</td>
<td>Refers to the average amount of data transferred per unit of time</td>
</tr>
<tr>
<td>RSSI(dbm)</td>
<td>Displays the observed RSSI (Received Signal Strength Indicator) value for the client.</td>
</tr>
<tr>
<td>Uplink Data</td>
<td>Indicates the amount of data transferred by the client.</td>
</tr>
<tr>
<td>Downlink Data</td>
<td>Indicates the amount of data received by the client.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Indicates the 802.11 protocol (with or without 802.11n or 802.11ac capability) used.</td>
</tr>
<tr>
<td>Up/Down Since</td>
<td>Date and time since the client is up or down.</td>
</tr>
<tr>
<td>First Detected At</td>
<td>Indicates the time and day when the client was first detected.</td>
</tr>
<tr>
<td>Retry Rate (%)</td>
<td>Indicates the retry rate in percentage</td>
</tr>
<tr>
<td>Sticky</td>
<td>Denotes whether client is sticky or not. Sticky client means if client is connected to AP and while roaming it found better AP with more better signal strength, still it decides to stay connected with older AP.</td>
</tr>
</tbody>
</table>

You can view ongoing activities of a Client using View Ongoing Activities option available to the right top corner on the Client table. The available activities are:

- Live Client Debugging: The Live Client Debugging feature enables you to troubleshoot client activities. Selecting this feature displays the list of the clients, for those any live activities are in progress.
- Packet Trace: Capture Packet Trace action on a client to intercept a data packet that is crossing or moving over a specific network. Selecting this activity displays the list of those clients for which packet trace is in session.
- Prevention: Prevention activity displays the list of all quarantined clients.
- None: Selecting **None** provided the list of all the clients without any filters.

You can perform the following actions on every client, these actions are available on a right click on any client:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rename Client</td>
<td>To change the name of a client.</td>
</tr>
<tr>
<td>Capture Packet Trace</td>
<td>Responsible for intercepting a data packet that is crossing or moving over a specific computer network</td>
</tr>
<tr>
<td>Packet Trace History</td>
<td>Displays packet traces captured in the last 30 minutes</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>Start Live Client Debugging</td>
<td>Displays live client logs of a client.</td>
</tr>
<tr>
<td>Disconnect</td>
<td>Disconnects the client.</td>
</tr>
</tbody>
</table>

Click on a client in the Clients list to view the following:

- Client Connection Logs
- Client Events Logs
- Baseline - Data Rate
- Top Applications by Traffic
- Client Traffic Volume
- Application Session Logs
- APs Seeing a Client

### 7.1.1 Client Connection Logs

Selecting a client in the Clients list displays the connection logs.

Client Connection Logs shows the list of successful or failed connection attempts made by client. The list provides information about every attempt of connection made by a client. Green color represents successful connection. Red color represents failed connections. Client connection logs can be retrieved only for 802.11ac or higher APs.

You can view or fetch the connection logs for the following time intervals:

- 2 hours
- 4 hours
- 8 hours
- 12 hours
- 1 day
- 1 week

You can view the Client Connection Logs in one of the following views:

- Timeline View
- Grid View

The Timeline View appears as follows:

![Client Connection Logs Timeline View](image)

The Timeline View displays the list of connections logs with additional information as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timestamp</td>
<td>Indicates the date and time when the client connected to an AP.</td>
</tr>
<tr>
<td>Average Latencies</td>
<td>Average latencies of various stages and their sub-stages in the WiFi connection for the client.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSSID</td>
<td>BSSID is the MAC address of the AP to which the client attempted to connect.</td>
</tr>
<tr>
<td>AP Name</td>
<td>Name of the AP to which the client attempted to connect.</td>
</tr>
<tr>
<td>SSID</td>
<td>SSID of the WLAN to which the client is connected.</td>
</tr>
<tr>
<td>Channel</td>
<td>Operating channel of the AP to which the client attempted to connect.</td>
</tr>
<tr>
<td>Disconnect</td>
<td>Disconnects client from AP.</td>
</tr>
</tbody>
</table>

The Grid View appears as follows:

![The Grid View](image)

The Grid View contains detailed information in a tabular format:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSSID</td>
<td>BSSID is the MAC address of the AP to which the client attempted to connect.</td>
</tr>
<tr>
<td>AP Name</td>
<td>Name of the AP to which the client attempted to connect.</td>
</tr>
<tr>
<td>SSID</td>
<td>SSID of the WLAN to which the client is connected.</td>
</tr>
<tr>
<td>Channel</td>
<td>Operating channel of the AP to which the client attempted to connect.</td>
</tr>
<tr>
<td>Timestamp</td>
<td>Indicates the date and time when the client connected to an AP.</td>
</tr>
<tr>
<td>Event</td>
<td>Indicates if the client successfully connected.</td>
</tr>
</tbody>
</table>

A red symbol in the Event column of the connection logs denotes client connection failure. Hover on the red text to know about the failure type. The types of failures are:

<table>
<thead>
<tr>
<th>Failure Categories</th>
<th>Main Failure Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Association Failure</td>
<td>AP association limit exceeded</td>
</tr>
<tr>
<td></td>
<td>Capability mismatch</td>
</tr>
<tr>
<td></td>
<td>Association failure</td>
</tr>
<tr>
<td>Authentication Failures</td>
<td>Eapol 4-way handshake failed</td>
</tr>
<tr>
<td></td>
<td>RADIUS authentication failure</td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>Failure Categories</th>
<th>Main Failure Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Radius server not responding</td>
</tr>
<tr>
<td></td>
<td>Incorrect Pre-Shared Key</td>
</tr>
<tr>
<td></td>
<td>Fast roaming failed</td>
</tr>
<tr>
<td>Network Failures</td>
<td>Captive portal - shared secret mismatch</td>
</tr>
<tr>
<td></td>
<td>Captive Portal authentication failed</td>
</tr>
<tr>
<td></td>
<td>Captive portal - client in blackout period</td>
</tr>
<tr>
<td></td>
<td>DHCP failed</td>
</tr>
<tr>
<td></td>
<td>DNS failure</td>
</tr>
</tbody>
</table>

You can filter connection logs data in Grid View using the Filter icon on the top right corner. Filter is applied on the following column:

<table>
<thead>
<tr>
<th>Column</th>
<th>Filtering Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event</td>
<td>All</td>
<td>Retrieves all the event logs.</td>
</tr>
<tr>
<td></td>
<td>Successful</td>
<td>Retrieves only successful event logs.</td>
</tr>
<tr>
<td></td>
<td>Failed</td>
<td>Retrieves only unsuccessful event logs.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Filtering Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the From and To dates.</td>
<td>Retrieves client connection logs between the From and To dates.</td>
</tr>
<tr>
<td>Check the Long Time Ago check box and enter the To date.</td>
<td>Retrieves all client connection logs till the To date.</td>
</tr>
<tr>
<td>Enter the From date and check the Now check box.</td>
<td>Retrieves client connection logs between the From date and the current date.</td>
</tr>
<tr>
<td>Check the Long Time Ago and Now check boxes.</td>
<td>Retrieves all the available client connection logs.</td>
</tr>
</tbody>
</table>

### 7.1.2 Client Events Logs

You can view Client Events Logs by navigating to Clients -> Client Connection Logs drop-down menu -> Client Events Logs.

Client Event Logs by default opens in a full screen mode. It lists majority of client events including connection attempts. The list provides information about client connectivity events. Green color represents successful connection events. Grey color represents intermediate events. Red color represents failed connection events.

You can view or fetch the connection logs for the following time intervals:

- 2 hours
- 4 hours
- 8 hours
- 12 hours
- 1 day
- 1 week
You can view the Client Connection Logs in one of the following views:

- Graph View
- Grid View

**Graph View**

The Graph view displays the connection events of the client at a specific time. When you hover over each event, some of the information you see in the tooltip is:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timestamp</td>
<td>Indicates the date and time when the client connected to an AP.</td>
</tr>
<tr>
<td>Average Latencies</td>
<td>Average latencies of various stages and their sub-stages in the WiFi connection for the client. This is seen in case of a successful connection event.</td>
</tr>
<tr>
<td>BSSID</td>
<td>BSSID is the MAC address of the AP radio for that SSID.</td>
</tr>
<tr>
<td>AP Name</td>
<td>Name of the AP to which the client attempted to connect.</td>
</tr>
<tr>
<td>SSID</td>
<td>SSID of the WLAN to which the client is connected.</td>
</tr>
<tr>
<td>Channel</td>
<td>Operating channel of the AP to which the client attempted to connect.</td>
</tr>
<tr>
<td>Location</td>
<td>Location of the AP to which the client is connected.</td>
</tr>
<tr>
<td>Frequency Band</td>
<td>Frequency band of the client connected to the AP.</td>
</tr>
</tbody>
</table>

The Graph view appears as follows:
If you are interested in a specific event, you can apply filters based on various criteria to view the specific event. The filter is applied on the Grid view but the filter criteria are reflected in the Graph view as well. You can remove the filter from the Grid view.

Use the range scroll to limit the time period of the graph. If you don’t want to use the scroll, you can also select the desired area in the graph using a mouse pointer. To go back to the original full range time period, click *Reset Zoom*.

The Graph view is effective in full screen mode. Click the Full Screen icon (expand icon) to enter the full screen mode.

The Full Screen appears as follows:
You can click a specific event in the graph and the corresponding event detail is highlighted in the table.

**Grid View**

The Grid View appears as follows. The red, green and grey colored symbols in event column of the client event logs denotes unsuccessful, successful and intermediate events respectively. Hover on each text to know about type of event occurred.

Client Events are categorized into 5 major categories and further divided into various intermediate events.

The Grid View contains detailed information in a tabular format:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSSID</td>
<td>BSSID is the MAC address of the AP to which the client attempted to connect.</td>
</tr>
<tr>
<td>AP Name</td>
<td>Name of the AP to which the client attempted to connect.</td>
</tr>
<tr>
<td>SSID</td>
<td>SSID of the WLAN to which the client is connected.</td>
</tr>
<tr>
<td>Channel</td>
<td>Operating channel of the AP to which the client attempted to connect.</td>
</tr>
<tr>
<td></td>
<td>The channel is shown as Dual for sensor that operates on both 802.11a and</td>
</tr>
<tr>
<td></td>
<td>802.11b/g simultaneously.</td>
</tr>
<tr>
<td>Timestamp</td>
<td>Indicates the date and time when the client connected to an AP.</td>
</tr>
<tr>
<td>Event</td>
<td>Indicates if the client successfully connected.</td>
</tr>
<tr>
<td>Packet Capture</td>
<td>It provides the link of the wireshark file, that contains a packet capture</td>
</tr>
<tr>
<td></td>
<td>for all failure events. User can open the file in Arista packets or</td>
</tr>
<tr>
<td></td>
<td>download the file.</td>
</tr>
</tbody>
</table>

7.1.3 **Top Applications by Traffic in Client Tab**

Top Applications by Traffic chart graphically represents data usage for applications. It always represents data for top five applications, with highest traffic. To view exact data usage, hover on the specific bar in the graph.
The data on the widget can be filtered using the available filters on the top right corner of the widget. To know more about the filters refer Filters on Widgets.

7.1.4 Client Traffic Volume

The Client Traffic Volume graph represents the data traffic sent and received by the client every 15 minutes. X-axis in the graph denotes the time period for which the Data Usage is plotted and Y-axis denotes the Traffic Volume.

This data usage includes Uplink Data as well as Downlink Data for all applications. User can choose to view the Client Traffic for:

- 2 hours
- 4 hours
- 8 hours
- 12 hours
- 1 day
- 1 week

Hovering the mouse on data point provides detail information about data usage.
The graph contains the following details about the data:

- Time stamp: It includes day, date, month, year, and time of data usage.
- Uplink Data: It states Uplink Data usage.
- Downlink Data: It states Downlink Data usage.
- Data Usage: It states Data Usage for all applications.

### 7.1.5 Application Session Logs

Application Session Logs provides details of the applications used by the client. Select a client from MONITOR > Clients to view Application Session Logs.

The top left corner denotes the total number of application session logs.

Hover on the pie chart icon to view overall aggregated data. The data provides information about Total Sessions, percentage count of Affected Sessions, Total Experience Time and percentage count for Poor App Experience.

The logs on the widget can be filtered using the available filters on the top right corner of the widget. To know more about the filters refer Filters on Widgets.

Detailed information about session logs is displayed in tabular format:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>App Name</td>
<td>Name of the application.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Session start time.</td>
</tr>
<tr>
<td>End Time</td>
<td>Session end time.</td>
</tr>
<tr>
<td>Duration(min)x</td>
<td>Session duration in minutes.</td>
</tr>
<tr>
<td>% of Bad Time</td>
<td>Percentage of time for which app experience was bad for the specified clients</td>
</tr>
<tr>
<td>Location</td>
<td>Location at which the client connected.</td>
</tr>
<tr>
<td>Potential Cause</td>
<td>Potential root cause for application performance to be poor.</td>
</tr>
<tr>
<td>Average Bitrate Uplink</td>
<td>Indicates average of the number of bits sent per second by the client in that session.</td>
</tr>
<tr>
<td>Average Bitrate Downlink</td>
<td>Indicates average of the number of bits received per second by the client in that session.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Average Bitrate Jitter Uplink</td>
<td>Average standard deviation in uplink bitrate.</td>
</tr>
<tr>
<td>Average Bitrate Jitter Downlink</td>
<td>Average standard deviation in downlink bitrate.</td>
</tr>
<tr>
<td>Average RSSI (dbm)</td>
<td>Average Received Signal Strength Indicator.</td>
</tr>
<tr>
<td>Average Retry Rate</td>
<td>Average percentage of retry packets out of the total packets sent or received by the client.</td>
</tr>
<tr>
<td>Average Data Rate Upstream</td>
<td>Average upstream data rate.</td>
</tr>
<tr>
<td>Average Data Rate Downstream</td>
<td>Average downstream data rate.</td>
</tr>
<tr>
<td>Roaming Count</td>
<td>Number of APs involved during the session.</td>
</tr>
<tr>
<td>Associated AP(s)</td>
<td>List of APs involved in the client session.</td>
</tr>
</tbody>
</table>

### 7.1.6 Devices Seeing This Client

Devices Seeing This Client represents list of APs currently watching the client. The top-left corner denotes the total number of APs seeing the client and the name of the AP associated with the client.

![Devices Seeing This Client](image)

The detailed information is as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of APs seeing the client.</td>
</tr>
<tr>
<td>RSSI (dbm)</td>
<td>RSSI states signal strength of an AP as seen by the client.</td>
</tr>
<tr>
<td>2.4 GHz Operating Channel</td>
<td>Channel Operating on 2.4GHz</td>
</tr>
<tr>
<td>5 GHz Operating Channel</td>
<td>Channel Operating on 5GHz</td>
</tr>
<tr>
<td>2.4 GHz Association</td>
<td>It states number of clients associated with 2.4GHz radio.</td>
</tr>
<tr>
<td>5GHz Association</td>
<td>It states number of clients associated with 5GHz radio.</td>
</tr>
</tbody>
</table>

Clicking on the name of AP takes you to the Access Points Information page.

### 7.1.7 Rename a Client

You can change the name of a client.

Perform the following tasks to rename a client:
1. Go to **MONITOR > Clients**.
   A list of clients that are being monitored is displayed.

2. Right-click on the name of the client you want to rename or click on the menu icon (three vertical dots) and select **Rename Client**.
   Rename Client page is displayed.

3. Change the name of the client and click **Done** to save the changes.
   A message is displayed that confirms the change in the name of the client.

### 7.2 Access Points

Access Point tab provides detailed information of an AP such as its name, IP Address, status, and the switch it is connected to.

You can view ongoing activities on an AP using View Ongoing Activities option available to the right top corner on the AP table. The list of live activities that can be viewed for AP are:

- **Packet Trace**
  Capture Packet Trace action on an AP captures the packet and inspects it to help diagnose and solve network problems. Selecting this activity displays the list of those devices for which packet trace is in session.

- **Prevention**
  Prevention activity displays the list of all quarantine devices.

- **Client Connectivity Test**
  Client Connectivity Test is performed to troubleshoot an AP that has client connectivity issues. Client Connectivity Test action displays the list of such devices, for those the troubleshooting is in progress.

- **None**
  Selecting **None** provided the list of all the APs without any filters.

You can perform the following actions on every AP, these actions are available on a right click on any AP:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update Firmware</td>
<td>Using this option you can update the firmware on the AP to the latest or any previously released version.</td>
</tr>
<tr>
<td>Access Point Event Logs</td>
<td>A log table that maintains event logs of APs.</td>
</tr>
<tr>
<td>Run Client Connectivity Test</td>
<td>Runs the Client Connectivity Test.</td>
</tr>
<tr>
<td>View RF Explorer</td>
<td>The RF Explorer shows you information such as the channels occupied by other APs in the vicinity of the AP and the RSSI values for each of the neighboring APs as seen by the AP.</td>
</tr>
<tr>
<td>Capture Packet Trace</td>
<td>This option helps troubleshoot Arista devices operating in AP or AP/Sensor mode.</td>
</tr>
<tr>
<td>Packet Trace History</td>
<td>You can view the Packet Trace History for a selected AP.</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>View on Floor Map</td>
<td>This option redirects you to the location on the floor map where the AP is placed.</td>
</tr>
<tr>
<td>Customize Transmit Power or Channel</td>
<td>Transmit Power Selection enables you to control the transmission power of the AP.</td>
</tr>
<tr>
<td>Move</td>
<td>Using Move operation you can change location of an AP.</td>
</tr>
<tr>
<td>Reboot</td>
<td>This operation Reboot's the AP.</td>
</tr>
<tr>
<td>Rename</td>
<td>Renames the AP.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the APs from the list of available APs.</td>
</tr>
</tbody>
</table>

Click on an AP in the list on the **Monitor > Access Points** page to go to the AP details page. The AP details page shows the event logs of the AP, a list of clients associated with the AP and their details, a graph showing clients by average data rate, top applications by traffic, and network usage. The selected AP's name is displayed on the top-right of the page. You can select another AP from the drop-down list.

The AP details page provides the following information:

**Network Usage - Traffic**

The chart displays a line graph showing the number of client association and its traffic volume, for all the clients on the selected folder or floor.

**Network Usage - Poor Application Experience**

This chart provides overall application usage analysis.

**Baseline - Clients Affected By Poor Experience**

The Baseline - Clients Affected By Poor Performance graph calculates the baseline for the percentage of clients affected by poor performance, for the selected AP, over a period of time.

**Baseline - Retry Rate%**

The graph calculates baseline for the Retry Rate % of the clients connected to the selected AP.

**Baseline - Average Data Rate**

The graph calculates the data rates for 2.4GHz or 5GHz for the selected SSID(s) and duration.

**Baseline - Clients Affected by Failure**

Baseline - Clients Affected by Failure chart provides calculated baseline for the percentage of clients that failed due to connectivity issues.
Baseline - Clients Affected by Poor App Experience

Baseline - Clients Affected chart provides the calculated baseline for the percentage of clients affected by poor app experience. This data is provided for the selected AP.

Clients by Average Data Rate

Displays a bar graph of the clients and their data usage, for the selected AP.

Top Applications by Traffic

Displays a bar graph of the top 5 applications that have highest data usage, for the selected AP.

Spectrum Occupancy

Shows the number of active radios and clients across the Rf spectrum.

Channel Utilization

Shows the AP channel utilization.

Currently Associated Clients

Currently Associated Clients widget provides the list of clients that are currently associated with the AP.

Ap Health

Shows the CPU and memory utilization of an AP.

Devices Seeing this AP

The widget displays the list of managed devices observing the selected device.

Visible VLANs

The widget displays details of the VLANs visible to the managed device.

Visible Access Points

Provides the list of the APs visible to the selected AP.

Visible Clients

Provides the list of clients visible to the selected AP.

Note: Views and charts that show information about channels other than the operating channels of the AP work best when the AP has a dedicated scanning radio. APs that do not have a dedicated scanning radio use background scanning, where typically an AP goes off-channel once every 60 seconds to scan one channel for 100 ms. Because background scanning takes a long time to scan all channels in the band, an AP in background scanning mode has a snapshot of the network that is anywhere between five minutes to an hour old. During this time, the radio environment could have changed significantly.

In the AP details view, you can click on the AP name under the AP icon (when you hover, you see the View Properties tool tip) to open the AP properties right panel. The panel shows you the wired side properties and health stats for the AP.

Note: The wired properties of only the primary interface (eth0) of the AP are shown, and LLDP must be enabled on the switch for current switch properties to be shown.

The following table shows whether, depending on the state of the AP, the wired properties are current or they reflect the last known values. For example, for active APs, the wired properties shown are the current ones but for inactive APs they’re the last known values. The values are not displayed for APs 802.11ac Wave-1 or lower and for APs with firmware older than version 8.9. Some properties (e.g., Health Stats) are updated at periodic intervals; others (e.g. Switch Name) are updated if and when needed.

<table>
<thead>
<tr>
<th>AP State</th>
<th>Switch Properties</th>
<th>VLANs Detected</th>
<th>IPv4 or IPv6 Properties</th>
<th>Link Speed</th>
<th>Health Stats</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Switch Name</td>
<td>Switch Vendor</td>
<td>Switch Port</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active</td>
<td>Current</td>
<td>Current</td>
<td>Current</td>
<td>Current</td>
<td>Current</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inactive or Offline</td>
<td>Last Known</td>
<td>Last Known</td>
<td>Last Known</td>
<td>Last Known</td>
<td>Last Known</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------</td>
<td>------------</td>
<td>------------</td>
<td>------------</td>
<td>------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Last Known with a note in the right panel: "Values when AP was last active" (shown "--" in the Managed Devices and AP listing)

<table>
<thead>
<tr>
<th>Mesh Root</th>
<th>Current</th>
<th>Current</th>
<th>Current</th>
<th>Current</th>
<th>Current</th>
<th>Current</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mesh Non-Root (Powered by DC or PoE brick)</td>
<td>Not Displayed (&quot;--&quot;)</td>
<td>Not Displayed (&quot;--&quot;)</td>
<td>Not Displayed (&quot;--&quot;)</td>
<td>Current</td>
<td>Current</td>
<td>Not Displayed (&quot;--&quot;)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mesh Non-Root (Used for network extension and connected to a switch)</th>
<th>Current</th>
<th>Current</th>
<th>Current</th>
<th>Current</th>
<th>Current</th>
<th>Current</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Link Aggregation: eth0 Up (regardless of whether eth1 is Up or Down)</th>
<th>Current</th>
<th>Current</th>
<th>Current</th>
<th>Current</th>
<th>Current</th>
<th>Current</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Link Aggregation: eth0 Down and eth1 is Up</th>
<th>Last known</th>
<th>Last known</th>
<th>Last known</th>
<th>Last known</th>
<th>Current</th>
<th>Last known</th>
</tr>
</thead>
</table>

Link Aggregation: eth0 Down and eth1 is Up

Link Aggregation: eth0 Up (regardless of whether eth1 is Up or Down)

Mesh Non-Root (Powered by DC or PoE brick)
The wired properties of only the primary interface (eth0) of the AP are shown. Thus, when using link aggregation, the switch and VLAN wired properties reflect the information available on the primary interface only; their values do not depend on the state of the secondary interface (eth1). The IP and health stats, however, do not depend on a particular interface; their values are current as long as at least one of the two interfaces is up.

### 7.2.1 Clients by Avg. Data Rate for an AP

The Clients by Avg. Data Rate graph displays clients classified based on data rate. CloudVision WiFi has pre-defined, fixed thresholds for Average Data Rate. Since thresholds are configurable, user may select a value that falls in between a bucket on the X-axis. For instance, if a user sets the data rate threshold to 75 Mbps and RSSI threshold to -68 dBm, then these values fall in the "50 to 100 Mbps" data rate bucket and "-65 to -75 dBm" RSSI bucket, respectively.

The following logic is used to determine the color of the bar that falls in such a bucket:

- If all values in the "50 to 100 Mbps" bucket are below 75 Mbps, then the bar in the "50 to 100 Mbps" bucket is red.
- If all values in the "50 to 100 Mbps" bucket are above 75 Mbps, then the bar in the "50 to 100 Mbps" bucket is green.
- If some values in the "50 to 100 Mbps" bucket are above and below 75 Mbps, then the bar in the "50 to 100 Mbps" bucket is yellow.

The chart can be observed for:

- 2.4GHz
- 5GHz
- 2.4GHz and 5GHz both.
7.2.2 Currently Associated Clients for an AP

Currently Associated Clients widget provides the list of clients that are currently associated to the AP.

The graph displays the following information:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of a device to which AP is connected.</td>
</tr>
<tr>
<td>User Name</td>
<td>Name of a user.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Unique 48-bit address of the AP/ 802.11 PHY modes used by the AP.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the AP</td>
</tr>
<tr>
<td>Associated SSID</td>
<td>Name of a SSID to which client is connected.</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System running on the client.</td>
</tr>
<tr>
<td>UP/Down Since</td>
<td>Up since time or Down since time</td>
</tr>
<tr>
<td>RSSI (dBm)</td>
<td>Received Signal Strength Indicator.</td>
</tr>
<tr>
<td>Sticky</td>
<td>Denotes whether client is sticky or not. Sticky client means if client is connected to AP and while roaming it found better AP with more better signal strength, still it decides to stay connected with older client.</td>
</tr>
<tr>
<td>Tx Data Rate</td>
<td>Tx Data Rate is Transmission Data Rate of a client.</td>
</tr>
<tr>
<td>Rx Data Rate</td>
<td>Rx Data Rate is Received Data Rate of a client.</td>
</tr>
<tr>
<td>Avg Data Rate</td>
<td>Avg Data Rate is Average Data Rate of a client</td>
</tr>
<tr>
<td>Retry Rate (%)</td>
<td>Retry Rate (%) is Retransmission rate of a client.</td>
</tr>
</tbody>
</table>
7.2.3 Top Applications by Traffic for an AP

Top Applications by Traffic chart graphically represents data usage for applications. It always represents data for top five applications that have highest data usage (transmit and receive). To view exact data usage, hover on the specific bar in the graph.

You can choose to view the top applications by traffic for the following time intervals:

- 2 hours
- 4 hours
- 8 hours
- 12 hours
- 1 day
- 1 week

7.2.4 Network Usage

You can access the Network Usage chart in two different ways from CloudVision WiFi UI. If you access the chart from the performance dashboard, it displays a line graph showing the number of clients associated with the SSID and its traffic volume, for all the clients on the selected folder or floor. Whereas when you access the chart through AP drill down, it displays similar data, but this time for the selected AP.

If you hover over the graph, a tooltip providing quick information like timestamp, the number of clients associated and the used traffic volume appears.

You can view or retrieve data using the filters. To know more about these filters refer Filters on Widgets.

The data of the network usage chart can be filtered based on two parameters; a client's data and the amount of data used by an application.
Drill down on the **data point** on the graph, redirects you to the page containing client connections table. This table contains the list of all the client connections along with their detailed information for the selected timestamp. For client details refer, **Filtered Network Usage Chart**

Drill down on the **bar**, redirects you to another page that contains:

- **Client Connections table** - contains the list of all the client connections along with their detailed information for the selected timestamp.
- **Top Applications** - that shows top ten applications with highest data usage. You can select an app from the drop-down list given on the top left corner of the table. Along with the selected application name it displays application specific data consumption.
- **All Application traffic** - it displays the total amount of data used by the applications for a selected Access Point or a location. This information is shown at the top-right corner of the table.
- **Client Connections** - selecting client connection displays the list of all the clients using the application selected from the top applications list.
- **Access Points Distribution** - selecting access points distribution displays the list of all the associated APs.

### 7.2.5 Network Usage - Poor Application Experience

This chart provides overall application usage analysis. It states the time for which application quality was good and the time for which it was bad.

The graph displays poor app experience in red colour and good app experience in green colour. X-axis displays time slots and Y-axis displays amount of time app quality was good or bad.

Hover on the graph provides a tool tip with the following information:

- **Timestamp**
- **No of associations**
- **Aggregated value for poor app experience in percentage.**

![Network Usage Chart](image)

Click the data point or bar graph in the chart to view more details.

There are four filters provided on the right corner of the chart to filter the data:

**Conferencing Apps Filter**

The graph can be viewed for specific conferencing app using **All Conferencing Apps** filter. Filter can be applied on the following apps:

- **WebEx**
- **Skype**
- **GoToMeeting**
- **Hangouts**
- **Slack**
- **Microsoft Teams**
- **Zoom**
Selecting **All Conferencing Apps** option provides details for all the above listed apps at once.

**SSID Filter**

The application quality can also be viewed for specific SSID, using **All SSIDs** filter. Selecting a specific SSID provides a application quality graph for the specified SSID. Selecting All SSIDs provides an aggregated data on a graph for all the SSIDs.

**Frequency Filter**

The data can be filtered based on frequencies. The data for applications working on the selected frequency is represented graphically. The possible values for frequency filter are:

- 2.4 GHz
- 5 GHz
- 2.4 and 5 GHz

**Time Filter**

You can view or fetch the Application Session Logs for the following time intervals:

- 2 hours
- 4 hours
- 8 hours
- 12 hours
- 1 day
- 1 week

### 7.2.6 Spectrum Occupancy

As shown in the following figure, you can filter on a band and duration to see the number of radios and clients that were active in that band in that duration. This can help you identify congested or under-utilized bands.

![Spectrum Occupancy](image)

### 7.2.7 RF Explorer

You can launch the **RF Explorer** from the Spectrum Occupancy chart or from the AP listing under **Monitor > WiFi > Access Points** by right-clicking on an AP and selecting **Troubleshoot > View RF Explorer**.
As seen in the previous figure, the RF Explorer shows you what an AP sees in its RF neighborhood. For example, it shows you the channels occupied by other APs in the vicinity of the AP and the RSSI values for each of the neighboring APs as seen by the AP.

You can use the RF Explorer to identify issues such as co-channel and adjacent channel interference, and DFS channels occupied by APs. The grey rectangle stretching across the RSSI axis represents the operating channel of the AP itself; the heights of the other channel trapezoids indicate the RSSI values of those channels as seen by the AP. You can click on an AP from the list of APs to see its channel details on the chart (as seen in the callout in the previous figure).

### 7.2.8 Channel Utilization

As shown in the following figure, the channel utilization chart shows the AP channel utilization (as a percentage value) averaged over 15-minute intervals for both the 2.4GHz and 5GHz bands, for the selected duration.

### 7.2.9 AP Health

As shown in the following figure, the chart shows the average CPU and memory utilization of an AP for the selected duration.
Visible Access Points

The Visible Access Points widget provides the list of the APs visible to the selected AP. The widget provides two different views: one for Managed APs and the other for Unmanaged APs.

Visible Access Points - Managed

Selecting Managed from the drop-down list displays APs that belong to your network and are in the vicinity of the selected AP.

<table>
<thead>
<tr>
<th>Name</th>
<th>Associated SSID</th>
<th>RSSI (dBm)</th>
<th>Channel</th>
<th>Clients</th>
</tr>
</thead>
<tbody>
<tr>
<td>CT10_Philadelphia</td>
<td>Spectrum</td>
<td>-87</td>
<td>11</td>
<td>15</td>
</tr>
<tr>
<td>CT10_Philadelphia</td>
<td>Spectrum</td>
<td>-86</td>
<td>11</td>
<td>6</td>
</tr>
<tr>
<td>CGSO_Omaha</td>
<td>Spectrum</td>
<td>-79</td>
<td>44</td>
<td>22</td>
</tr>
<tr>
<td>CGO_GroundFloor</td>
<td>Spectrum</td>
<td>-84</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>CGO_Gamma_D07</td>
<td>morguest</td>
<td>-91</td>
<td>159</td>
<td>12</td>
</tr>
</tbody>
</table>

Visible Access Points - Un-managed

Selecting un-managed from the drop-down list displays the Access Points that do not belong to your network but are in the vicinity of the selected AP.
7.2.11  Radios Seeing this AP (Access Point)

This widget is available on drilling down from any WiFi device. The widget displays the list of managed WiFi device radios observing the selected device with the best RSSI.

<table>
<thead>
<tr>
<th>BSSID</th>
<th>Associated SSID</th>
<th>RSSI (dBm)</th>
<th>Channel</th>
<th>Clients</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:5C:6F:02:01:04:04</td>
<td>TP-LINK_B01CF</td>
<td>-88</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>08:5C:6F:02:01:04:04</td>
<td>close</td>
<td>-88</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>08:5C:6F:02:01:04:04</td>
<td>HP_Slave_2814</td>
<td>-87</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>08:5C:6F:02:01:04:04</td>
<td>ST1103</td>
<td>-93</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>08:5C:6F:02:01:04:04</td>
<td>AOChromebook</td>
<td>-71</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>08:5C:6F:02:01:04:04</td>
<td>Airtel_S01S</td>
<td>-90</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>08:5C:6F:02:01:04:04</td>
<td>ZT5Ya2V01W4tGc0V2</td>
<td>-83</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>08:5C:6F:02:01:04:04</td>
<td>ZT5Ya2V01W4tGc0V2</td>
<td>-83</td>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>

7.2.12  Visible VLANs

The visible VLANs widget is available on drilling down from any managed WiFi device. The widget displays details of the VLANs visible to the managed device. "Monitored" in the Status column
indicates that the VLAN is being monitored by that managed device. "Not monitored" indicates that it is being monitored by another managed device.

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>IP Address</th>
<th>Net Mask</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>9011</td>
<td>10.88.57/10</td>
<td>255.255.248.0</td>
<td>Monitored</td>
</tr>
<tr>
<td>Untagged</td>
<td>10.88.114/10</td>
<td>255.255.255.0</td>
<td>Not Monitored</td>
</tr>
</tbody>
</table>

The VLANs that can be seen by the selected device are populated depending on the following:

1. If the VLAN is used by the device to communicate with the Wireless Manager (aka communication VLAN); shown marked with an asterisk.
2. If the ID of the VLAN is added while configuring the SSID.
3. If you enable Auto VLAN monitoring from CloudVision WiFi > Device Settings > VLAN Monitoring, the active VLAN is monitored by the device with the highest MAC address.

Thus the monitored VLAN's ID is added to the monitoring device's list and the VLAN's status is set to Monitored.
4. If you choose to enable **Monitor Additional VLANs**, one needs to specify a comma-separated list of VLANs to be monitored. In this situation, any active VLAN from the specified list is monitored. The device with the highest MAC address monitors the VLAN. The monitored VLAN's ID is added to the monitoring device's list and VLAN's status is set to **Monitored**.
7.2.13 Visible Clients

The Visible Client widget provides the list of clients visible to the selected AP. It also provides the total number of visible clients on the top left corner of the widget.

<table>
<thead>
<tr>
<th>Name</th>
<th>MAC Address</th>
<th>RSSI (dBm)</th>
</tr>
</thead>
<tbody>
<tr>
<td>LWP-558</td>
<td>80:50:71:01:FF:BD</td>
<td>-83</td>
</tr>
<tr>
<td>IAP-556</td>
<td>80:59:71:01:FE:E6</td>
<td>-88</td>
</tr>
<tr>
<td>Motorola-Mobility_29.BBDF</td>
<td>F0:07:AA:29:BBDF</td>
<td>-69</td>
</tr>
<tr>
<td>Guangdong Oppo Mobile_4E:8D:63</td>
<td>EC:01:8C:4E:8D:63</td>
<td>-91</td>
</tr>
</tbody>
</table>

7.2.14 View Access Point Event Logs

AP event logs table maintain event logs of AP. The captured events are from an AP perspective and do not include data related to clients and their connectivity information. These events are sent by the AP to Wireless Manager in real time and logged at Wireless Manager.

You can view AP Event Logs, by selecting the option View Event logs with a right-click on any AP from MONITOR > Access Points > Troubleshoot.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>It is a category of event.</td>
</tr>
<tr>
<td>Type</td>
<td>It is a type of event.</td>
</tr>
<tr>
<td>Description</td>
<td>It is description of event.</td>
</tr>
<tr>
<td>Date</td>
<td>Timestamp at which event occurred.</td>
</tr>
</tbody>
</table>

The detailed information about the event logs is as follows:

The AP Event Logs details can also be fetched for specified durations using Duration Filter. To know more about the duration filter refer Filters on Widgets.
The various types of events that are logged for an AP are:

- AP Memory Status
- AP Reboot
- AP IP Conflict
- AP System Service Crash
- AP Ethernet Port Status
- AP Upgrade Failure
- AP Upgraded
- AP CLI config change
- AP DHCP lease status, etc.

7.2.15  View on Floor Map

View on Floor Map option redirects you to the location on the floor map where the AP is placed.

To view the AP on the Floor Map:

1. Navigate to MONITOR > Access Points.
2. Right click on the AP, you wish to locate on the Floor Map.
3. Select View on Floor Map.
   These option is enabled only if the selected AP is placed on any of the floor maps. Else it is disabled.

It redirects you to the Floor Map where the selected AP is placed.

7.2.16  Customize Transmit Power or Channel

Transmit Power Control enables you to control the transmission power of the AP. Transmit Control Settings are configured from Radio Settings. These settings are the generic settings for all the APs.

CloudVision WiFi facilitates AP specific Transmit Control Settings.

To know more about Transmit Power Selection refer Configure Transmit Power Selection in Radio Settings and for Channel settings refer Configure Basic Radio Settings

For AP specific customization:

1. Navigate to MONITOR > Access Points.
2. Right click on the AP, for which you wish to customize the settings.
3. Select Customize Transmit Power or Channel.
   A Customize Transmit Power or Channel window appears to the right of the screen.
4. Select appropriate frequency for which you wish to customize the settings.
   Possible frequencies are 2.4 GHz and 5GHz.
5. Select Customize Transmit Power for transmit power settings.
   a. Select Auto or Manual option.
   Selection of Manual option enables the Transmit Power text box to provide transmission power of the AP in dBm.
6. Select Customize Channel Settings for channel settings.
   a. Select Operating Channel as either Auto or Manual.
   Selection of Manual option enables the Channel Number text box to provide a channel number.
7. Click Save.

The customization settings are saved.
7.2.17 Customize VLANs to Monitor per AP

You can configure custom VLANs for individual APs to monitor. The steps to do so are as follows:

1. Go to MONITOR > WIPS > Managed WiFi Devices or MONITOR > WiFi > Access Points, or go to a floor plan and select an AP on the floor plan.
2. Right click on the AP and click Customize > VLANs. The Customize Access Point VLANs right panel appears.
3. Add the VLANs you want the AP to monitor.
   Detected VLANs are VLANs that the AP has detected on the network. They might help you select VLANs to monitor.
4. Select whether you want the VLAN to use a Static IP or DHCP. For the Static IP case, enter the IP network configuration.
5. Select a Communication VLAN from among the monitored VLANs.
   The AP communicates with the WiFi server over the Communication VLAN. So the Communication VLAN must be one of the VLANs that the AP monitors.
6. Save the configuration.

7.2.18 Move an AP

CloudVision WiFi provides the facility to change the location of an AP using the Move option.

To move an AP:

1. Go to MONITOR > Access Points.
   A list of APs that are being monitored is displayed.
2. Right-click on the name of the AP that you want to move and select Move.
   Location Navigator is displayed.
3. Select the new location, where you wish to move the AP.
4. Click Move.
   A confirmation window is displayed.
5. Select appropriate option to confirm.
   If you select Yes the selected access points will adopt the configuration applied at the destination folder. Also if the AP is currently placed on any of the floor map, then the AP will be removed from that map.

An appropriate message is displayed that confirms the change in location.

7.2.18.1 Behavior - Move Devices

When you move devices across locations, the behavior of the devices may change depending on multiple factors.

The factors to be considered are captured below.

Suppose that you select a mix of devices to move, i.e., some are part of a group and others are not.

- For devices that are not part of any group, the behavior is exactly as expected - when moved from one folder to another, these devices start using the default configuration of the destination folder.
- If the destination folder has no groups, devices from the source groups will be removed from their respective groups and all devices will start using the default configuration of the destination folder.
- For devices that were part of some group in the source folder, see the table below.

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is the device in a group?</td>
<td>Does the group have a config?</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Source</td>
<td>Destination</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### 7.2.19 Reboot Access Points

You can reboot an AP, with the help of CloudVision WiFi.

Perform the following tasks to reboot an AP:

1. Go to **MONITOR > Access Points**.
   
   A list of APs that are being monitored is displayed.
2. Right-click on the name of the AP that you want to reboot and select **Reboot**.
   
   Reboot dialog box is displayed.
3. Click **Yes** to reboot the AP.

   A message is displayed that confirms the reboot. You can check the status after some time.

### 7.2.20 Rename Access Points

You can change the name of the AP.

Perform the following tasks to rename an AP:

1. Go to **MONITOR > Access Points**.
   
   A list of APs that are being monitored is displayed.
2. Right-click on the name of the AP that you want to rename and select **Rename**.
   
   Rename AP page is displayed.
3. Change the name of the AP and click **Done** to save the changes.

   A message is displayed that confirms the change in the name of the AP.

### 7.2.21 Delete Access Points

You can delete the APs from the list of APs available on Access Points tab.

Perform the following tasks to delete an AP:
1. Go to **MONITOR > Access Points**.
   A list of APs that are being monitored is displayed.

2. Right-click on the name of the AP that you want to delete and select **Delete**.
   A Delete dialog box is displayed.

3. Click **Yes** to confirm the deletion.
   A message is displayed that confirms the deletion of the AP.

   **Important:** If the AP is physically active on the network after deletion, then:
   - CloudVision WiFi marks the AP to Unknown location.
   - The default device template of the Unknown location is applied.
   - The default SSIDs are pushed on the active AP, if the AP is configured in the Device Template.
   - No SSIDs are applied, if the AP is not configured.

7.2.22  **View Ongoing Activities on AP**

View Ongoing Activities is an action available on Access Points screen.

To view the ongoing activities on an AP, perform the following steps:

1. In CloudVision WiFi navigate to Access > Access Points
2. Click on View Ongoing Activities action present on the top right hand corner of the screen.
3. From the drop-down menu, select one of the following:
   - Packet Trace
     It displays the list of APs with their information on which the Packet Trace Activity is in progress.
   - Prevention
     It displays the list of APs in quarantined status.
   - None
     It displays the list of APs on which no activity is going on.

7.2.23  **Assign a Device to a Group from Access Points tab**

One of the ways to assign access points to a group is from the access point list available on the access point page.

To assign a device to an existing group, perform the following steps:

1. Go to **Monitor > Access Points**
2. Right-click on the name of a single AP, that you want to assign to a group or click on the menu icon (three vertical dots) and select **Assign/Reassign to a Group**.
   A **Select a Group** window appears on the right panel.
3. Select the group to which you want to assign the selected AP.

In case the group is not available in the list, you can add a new group from this panel. The newly added group will always be created at the top-most allowed folder of the selected locations. Adding a group option is disabled, if the user does not have access to the folder.

**Note:** When assigning multiple APs, only those groups which are available to the selected access points’ folders will be listed under the **Select a Group** panel.

4. Click **Assign**.

### 7.2.23.1 Assign a Device to a Group

You can assign one or more access points from a location subtree to a group. It is a method used to apply a single WiFi configuration to multiple devices across different locations. If a group has no configuration, then the assigned devices will use the default WiFi configuration of their respective
Monitoring WiFi

locations. On the other hand, suppose an AP already has custom WiFi configuration applied to it. Then if you assign such an AP to a group it will start using the WiFi configuration of the group.

Assigning a device to a group can be performed from two different tabs:

- Access Points
- Folders/Floors Page

7.2.23.2 Assign a Device to a Group from the Folders/Floors Page

In addition to assigning a device to a group from access point's page, you can also do this from the folder/floor page.

To assign a device to an existing group, perform the following steps:

1. Go to SYSTEM > Navigator -> Folders/Floors.
2. Right-click on the name of a single AP that you want to assign to a group or click on the menu icon (three vertical dots) and select Show Available Devices option from the list.
   
   A list of available access points available at the selected folder appears on the right panel.
3. Right-click on the name of a single AP that you want to assign to a group or click on the menu icon (three vertical dots) and select Assign/Reassign to a Group.

   A Select a Group window appears on the right panel.
4. Select the group to which you want to assign to the selected AP.

   In case, the group is not available in the list, you can add a new group from this panel. You cannot add a group if you do not have access to the top-most allowed parent folder. The newly added group will always be created at the top-most allowed parent folder of the selected locations.
5. Click Assign.

7.2.24 Re-assign a Device to Another Group

This operation allows you to move the access points from one group to another. Once reassigned, selected access points will start using target group's WiFi configuration. If the target group doesn't have WiFi configuration applied to it, access points will use their location's default WiFi configuration. Even if the selected access points were not assigned to any group, reassigning will assign them to the target group.

Note: If the device is re-assigned to a group that doesn't have any configuration, then such devices will use the default WiFi configuration of the respective folder.

Re-assigning a device to a group can be done from three different tabs:

- Access Points
- Folders/Floors
- Groups

The first two methods are the same as for assigning a device to a group. The third one is applicable only to re-assigning devices.

To re-assign a device to another group from one group's page, perform the following steps:

1. Go to System > Groups.
2. Right-click on a selected group and select Show Assigned Devices.

   A list of Access Points available at the selected location will display on the right panel.
3. Right-click on the name of the AP you want to reassign and click **Assign/Reassign to a Group**. A **Select a Group** window appears at the right side of the screen.

4. Select a group from the list to re-assign that device to the selected group.
5. Click Assign.

7.2.25 About Device Firmware Update in CloudVision WiFi

You can configure an automatic update that includes upgrade or downgrade of Arista devices deployed at your enterprise premises. The device update can be configured or scheduled for devices that connect to the server for the first time as well as for existing devices that are already placed at various locations.

A device firmware update configuration is specific to a location and applies to all Arista devices placed at the location. An individual Arista device cannot have an independent device firmware update configuration.

A device firmware update configuration can be created for location folders only. A location floor cannot have its own device firmware update configuration; it inherits the device firmware update configuration from the parent location folder. When you do not recursively apply a device firmware update configuration to the child location folders, the configuration is applied only to the selected location folder and the location floors directly under the selected location folder.

You can choose to apply a device firmware update configuration recursively to the child location folders, when you are creating or editing the device firmware update configuration. However, a child location folder can have its own device firmware update configuration. If you define the firmware update configuration specific to the child location folder when a schedule for its parent location folder is already defined, the schedule configured to the child location applies to the child location folder.

When an active schedule is deleted or modified for a location, the sensors of that location on which the update process is already started or the update command is scheduled would still be upgraded.

The device firmware update setting for a location applies to all active devices deployed at the location. The update can be applied to both existing Arista devices and new devices connecting to the Arista Server for the first time. A schedule can be configured for existing Arista devices at a location. The device firmware update configuration is not tied to release numbers. If a server is updated multiple times between the creation of the update configuration and scheduled time of device update, the devices are updated to the latest firmware release.
7.2.25.1 Update AP Firmware
You can update the firmware on the AP to the latest or any previously released version. The AP automatically reboots after the firmware update is complete.

Perform the following tasks to update the firmware of an AP:

1. Go to MONITOR > Access Points.
   A list of APs that are being monitored is displayed.
2. Click the Options icon (three vertical dots) or right-click on the name of the AP and select Update Firmware.
3. Select the required firmware version from the Version drop-down list.
   You can update the AP firmware to any version.
4. Click Update.
   A message is displayed that confirms that the firmware update is initiated. You can check the firmware update status after some time.

7.2.25.2 Update Firmware for Multiple APs
You can update the firmware for multiple APs at the same time.

To update the firmware for multiple APs, perform the following steps:

1. Go to MONITOR > Access Points.
   A list of APs that are being monitored is displayed.
2. Select the required APs, click the Options icon (three vertical dots) and click Update Firmware.
   Update Firmware page is displayed as follows:
   • The model names of the selected APs.
   • Number of access points selected for each device model.
   • Version, drop-down list that contains the available firmware versions for each device model.
3. Select the required version number per AP model, from the Version drop-down list.
4. Click Update to update the firmware.
   A message is displayed that confirms that the firmware update is initiated. You can check the firmware update status after some time.

7.2.25.3 Schedule Firmware Update of a Single AP
Follow these steps to create a recurring or one-time schedule to update the AP firmware:

1. Go to MONITOR > WiFi > Access Points.
2. Right click the AP and select Update Firmware.
3. Select the version from the right panel.

7.2.25.4 Schedule Firmware Update of Multiple APs
Follow these steps to create a recurring or one-time schedule to update the AP firmware:

1. Go to MONITOR > WiFi > Access Points.
2. Click the Firmware Update Settings icon.
3. Provide the schedule for update in the Firmware Update Settings right panel.
The following table provides additional information for some of the options the Firmware Update Settings panel:

<table>
<thead>
<tr>
<th>UI Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply Update Settings Recursively to Subfolders</td>
<td>Applies the update settings to the selected folder location and also to all its subfolders, if any.</td>
</tr>
<tr>
<td>Hitless Update</td>
<td>Updates access points with minimum impact to WiFi clients. In certain situations, when the selected AP is the only AP on the floor and there are no APs around for clients to connect, then the WiFi will be impacted.</td>
</tr>
<tr>
<td>Update Window</td>
<td>Defines the duration for the firmware update. For example, if the Start Time is 1 hour 15 minutes and the Update Window is 20 hours 30 minutes, then the update will begin at 1:15 AM and end at 9:45 PM. Firmware updates are not initiated after the expiry of the Update Window. However, ongoing updates during the Update Window can continue even after the Update Window expires.</td>
</tr>
</tbody>
</table>

The Scheduled state is indicated by an orange calendar icon in the Update column under Monitor > WiFi > Access Points. You can also see which APs are scheduled for a firmware update by clicking on the AP icon of the WiFi Network Counters as shown in the following figure.

7.2.25.5 Cancel Firmware Update

You can cancel the firmware update for an AP. When an update is initiated for an Arista AP, the AP is initially in Active state and changes to Inactive state after a while. You can cancel the update only until the Arista AP is in Active state. Once the device is in Inactive state, you cannot cancel the firmware update.

Perform the following tasks to cancel firmware update.

1. Go to Monitor > Access Points. A list of APs that are being monitored is displayed.
2. Right-click the AP for which you want to cancel the firmware update and select Cancel Update. A message is displayed that confirms the cancellation of the firmware update.
3. Click Yes to cancel the update.
7.2.26  Access Point Web Shell

Web Shell is an online interface to remotely log into an AP via SSH. An administrator or a superuser can open Web Shell for a specific access point (AP) from CloudVision WiFi (CVW). Web Shell is helpful to troubleshoot AP issues, especially if an AP is behind a NAT. The URL for the Web Shell is specific to an AP. You can bookmark the URL to open a shell session to the AP directly instead of opening the shell session from CVW.

Depending on the limit defined in the config parameter, you can open concurrent Web Shell sessions to an AP. Web Shell is unavailable for inactive APs.

Note:

If the AP is overburdened with data-heavy operations, then there could be a delay with an ongoing Web Shell session or a new Web Shell may not open. For example, if you are already performing a task in the Web Shell, and then you start some data-heavy operations such as packet capture, generate debug logs, or live client troubleshooting, you would see a latency in the Web Shell. If you are performing live client debugging (or similar other data-heavy operations), and then you try to open the Web Shell, you may receive an error and the Web Shell may not open.

For the list of APs supporting Web Shell, see the Access Point Feature Matrix article.

You can open an AP web shell from:

- MONITOR > WiFi > Access Points
- MONITOR > WIPS > Managed WiFi Devices
- Floor Plan

7.2.26.1  Open Access Point Web Shell

You can open the access point (AP) web shell from CVW for an individual AP and perform basic operations using CLI commands.

To open the AP Web Shell:

1. Go to MONITOR > WiFi > Access Points.
2. Right click the AP and go to Troubleshoot > Open Web Shell.
   Web Shell opens in a new tab.
3. Enter the root credentials and log in to the web shell.
   You can now type your AP-CLI commands.

To terminate the session, close the browser.

7.3  Radios

The Radios tab under MONITOR tab displays a list of all the radios operating on 2.4GHz and 5GHz bands. It displays a list of clients that are recently associated to the selected Radio. The recent associations are either those that happened in the last 4 hours or the latest 100 clients. This is the total number of associations in the system and not per device.
The Radios tab displays the following information about radios:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Indicates whether the radio is on or off.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the AP.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Unique 48-bit address of the AP.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Displays the IP address.</td>
</tr>
<tr>
<td>Device Template</td>
<td>Indicates the device template applied to the device.</td>
</tr>
<tr>
<td>Channel</td>
<td>Displays the Channel number on which the AP radio operates.</td>
</tr>
<tr>
<td>Clients</td>
<td>Displays the number of clients connected to the radio.</td>
</tr>
<tr>
<td>Tx. Power(dbm)</td>
<td>Indicates the transmission power.</td>
</tr>
<tr>
<td>Frequency</td>
<td>Indicates the frequency on which radio is operating.</td>
</tr>
<tr>
<td>RF Utilization</td>
<td>Indicates the frequency utilization in percentage.</td>
</tr>
<tr>
<td>Upstream Usage</td>
<td>Indicates upstream data usage.</td>
</tr>
<tr>
<td>Downstream Usage</td>
<td>Indicates downstream data usage.</td>
</tr>
<tr>
<td>Worst Client RSSI (dbm)</td>
<td>Displays the worst client signal strength.</td>
</tr>
<tr>
<td>Retry Rate (%)</td>
<td>Indicates the re-transmission rate in percentage.</td>
</tr>
<tr>
<td>Location</td>
<td>Displays the radio location.</td>
</tr>
<tr>
<td>Model</td>
<td>Displays the name of the device model.</td>
</tr>
</tbody>
</table>
### 7.3.1 Turn Radio On or Off

You can turn individual access point (AP) radios on or off. To understand the motivation for this, consider a floor where WiFi access points (APs) with both 2.4GHz and 5GHz radios are deployed. Since the 2.4GHz signal propagates better than 5GHz and APs are often deployed to provide high 5GHz RSSI all over the floor, some areas on the floor end up having an “excess” of 2.4GHz signal, i.e., these areas get high RSSI signal from multiple 2.4GHz AP radios. This could cause interference in those areas because the 2.4GHz band has only three non-overlapping channels. You can then simply turn off the 2.4GHz radio for APs near these high 2.4GHz interference spots on the floor.

You can turn an AP radio on or off only if:

- The AP is active and
- The radio is not part of a mesh network.

The steps to turn a radio on or off are as follows:

1. Select the location of the AP whose radio you want to turn on or off.
2. Go to Monitor > WiFi > Radios.
3. Right-click on the radio and select Turn Radio Off or Turn Radio On.

**Note:**

- When you turn a radio off, all SSIDs on that radio are turned off. For uninterrupted WiFi in the coverage area of an AP, make sure that at least one AP radio is on.
- Turning a radio on or off can take a few minutes; the radio appears in italics until its status has changed, after which the UI shows the updated status—on or off, as the case may be.
- A radio that has been turned off manually is not turned on automatically when its AP reboots or when an SSID of that AP is scheduled to be on.

### 7.4 Active SSIDs

The Active SSIDs page displays a list of active SSID Profiles.

Go to MONITOR > Active SSIDs to view the Active SSIDs page.
Monitoring WiFi

The Active SSIDs page displays the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID Profile</td>
<td>Name of the profile.</td>
</tr>
<tr>
<td>Security</td>
<td>The mode of security used.</td>
</tr>
<tr>
<td>Authentication</td>
<td>The authentication method used.</td>
</tr>
<tr>
<td>2.4Ghz Clients</td>
<td>The number of clients connected on the 2.4 GHz frequency.</td>
</tr>
<tr>
<td>5 GHz Clients</td>
<td>The number of clients connected on the 5 GHz frequency.</td>
</tr>
<tr>
<td>2.4Ghz Radios</td>
<td>The number of 2.4 GHz radios on which an SSID is being broadcasted.</td>
</tr>
<tr>
<td>5 GHz Radios</td>
<td>The number of 5 GHz radios on which an SSID is being broadcasted.</td>
</tr>
<tr>
<td>Uplink Data</td>
<td>The uplink data usage.</td>
</tr>
<tr>
<td>Downlink Data</td>
<td>The downlink data usage.</td>
</tr>
</tbody>
</table>

7.5 Application Visibility

Application information page provides detailed monitoring information for an application selected from the Application Visibility tab. It displays a list of top 10 clients using the selected application and a line graph plotting the usage of the selected application over a period of time.

The name of the selected application is displayed on the top-left of the page. You can select another application from the drop-down list.
The application information page displays the following information:

**Baseline - Clients Affected**

**Baseline - % Poor Application Experience**

**Application Traffic**

It displays the usage of data of the selected application, over a period of time. Refer **Application Traffic** section for more information.

**Application Traffic - Clients**

**Application Traffic - Sessions**

**Application Traffic - Quality of Experience**

**Clients Using This Application**

It displays a list of the top 10 clients with highest data usage for the selected application along with the detailed information of the client like Username, MAC address, IP address, Recently Associated SSID and so on. Refer **Clients Using This Application** section for more details.

### 7.5.1 Application Traffic

### 7.5.2 Monitoring an Application

You can monitor an application, from the list of applications that are displayed in the Application Visibility tab.

To Monitor an application, perform the following tasks:

1. Go to **MONITOR > Application Visibility**.

   A list of applications that are being monitored is displayed.
2. Click on the name of the application that you want to monitor. A page providing detailed application information is displayed as follows:

- Top 10 clients using the selected application. Refer **Clients with Most Application Traffic** section for more details.
- Application Data Usage Over Time. Refer **Application Traffic** section for more information.

### 7.6 Application Traffic

Application Data Usage Over Time widget displays the usage of data of the selected application, over a period of time. The data is displayed for clients using the selected application, on the selected folder or floor.

You can view or retrieve data using the three filters SSID, Frequency Filter and Time Filter. To know more about these filters refer **Filters on Widgets**. Use **Start Live** button for live data.

The graph is plotted at a time interval of 15 minutes. If its live data it is plotted every 3 seconds. If you hover the mouse over the graph, you can get a quick view of the timestamp and the data consumption by the selected application, at the given time.

#### 7.6.1 Clients with Most Application Traffic

The **Clients with Most Application Traffic** widget displays a list of the clients with highest usage of the selected application along with the detailed information of the client. The number on the top left corner indicates the total number of clients with the most traffic.

The widget has a provision to view or retrieve data using the filters. To know more about these filters refer **Filters on Widgets**.

You can modify the view of the table by using the set of tools provided in the top-right corner of the widget. You can sort the data in an ascending or descending order by clicking on the **Name** column.
7.7 Root Cause Analysis Using the Inference Engine

Arista CloudVision WiFi (CVW) eliminates the need to manually troubleshoot some commonly occurring network issues. CVW has a powerful, intelligent engine called Inference Engine that identifies the root causes of network issues for a single client or total clients, and recommends solutions to those problems.

The Inference Engine can diagnose and recommend solutions for the following symptoms:

- Low RSSI
- Low data rate
- High retry

Note that root cause analysis is not supported for sticky clients.

Inference Engine analyzes the following causes to display the matching symptoms:

- Poor Coverage
- Low RSSI
- Low SNR
- High Interference
- Low Data Rate
- High Retry Rate
- High Contention (BSSID/Clients)
- Sticky Clients
- Client doesn’t support the latest 2.4 GHz or 5 GHz protocol
- Band Issues such as Client doesn’t support the 5 GHz band, 5 GHz capable client is operating in 2.4 GHz band, No 5 GHz SSID for 5 GHz capable client

The Inference Engine finds the root cause of a failure based on the following parameters:

- Symptoms and the number of clients that are showing the symptoms at a location.
- The domain knowledge determines the reason because of which an issue has occurred. For example, frequency band issues, too many clients with high uplink traffic, poor coverage, etc. are potential reasons for an issue.
- The system knowledge informs you about the WiFi configuration settings that might have caused the issue. For example: is transmit power set to “Auto”? is Dynamic Channel Selection enabled?

Note: The Inference Engine provides recommendations for some specific root cause types only. There is no recommendation available if the root cause is based on location, SSID, vendor name, OS, or AP.

7.7.1 Root Cause Analysis for a Single Client Vs Total Clients

CVW performs root cause analysis on single clients as well as on the total number of clients facing problems.
For single clients, you don’t have to run the Inference Engine. You can view the recommendations from **Monitor > Clients**.

For total clients, you have to run the Inference Engine in the Client Health widget and the root cause analysis runs based on the locations. You run it from **Dashboard > Performance > Client Health > Total Affected**.

### 7.7.2 Looking for Root Causes

The intelligent view is available for performance issues specific to Client Health widget. The generated view expires after an interval of 60 minutes.

Follow the steps below to generate the intelligent view:

1. Go to Dashboard > Performance > Client Health.
2. Select a parameter (Low RSSI, Low Data Rate, High Retry) that you want to analyze. For example, let's consider "Low Data Rate".
3. Click on the value showing the total number of clients facing low data rate.
4. Click *Should I look for root causes?* This will start the root cause analysis in the background. You can continue navigating to other parts of CloudVision WiFi while it is generating the intelligent view.

After the background process is completed, a message containing the number of clients for whom the root cause analysis is done appears next to the robot icon. Also, an "Ongoing activity" message box linking to the result of the root cause analysis appears in the lower-right corner of the screen. The link contains the number of clients for which the root cause was found. For example, "Found root causes for 10 out of 20 clients."

5. Click *Should I look for root causes?* Or click on the link in the **Outgoing Activity** message box to view the result of the root cause analysis.
You are redirected to the Intelligent View page that provides the detailed information about the top affected locations due to the root cause and the top root causes like poor coverage, high contention, or any more such issues. In the above example, the engine has found that 5 clients were affected at /Pune/Beta region and 5 clients were affected at /Pune/Gamma region.

6. Click See All Root Causes to view all the results of the analysis at one glance.

The See All Root Causes panel appears on the top right-side of the page.

7. To view recommendations, click the bulb icon next to the root cause.
8. To go back to the normal view, first close the recommendation panel.

Note:
If you do not close the existing ongoing activity message and attempt to look for another set of root causes, then the following message appears.

7.7.3 Perform Root Cause Analysis for a Single Client

When you open the details of a single client, you see the symptoms faced by the client and reason for the issue. Inference Engine automatically does all the calculations in the background and displays the symptoms as well as the probable solution. If there are no issues with the client, then you see a confirmation message.
1. Click MONITOR > WiFi > Clients.
2. Click the client name from the list.
   
   If the client is facing any issue, you will see the symptom and the reason below the client details.

3. To view recommendations for the symptom, click the How do I fix this icon (bulb icon) next to the root cause.
Configure WiFi

CloudVision WiFi provides a convenient way to configure your WiFi network via the Configuration tab. All configuration in CloudVision WiFi is done at the location level. So when you create an SSID or enable Smart Steering, you do this for a location. This is because most configuration parameters are relevant to a location rather than a particular device. For example, all devices in an office are likely to broadcast the same SSID’s.

**Note:** By default, configurations at a location are automatically inherited by its child locations. For example, suppose there is an HQ location with two child locations: Branch 1 and Branch 2. Then a configuration applied to HQ automatically applies to Branch 1 and Branch 2. You can, however, customize the configuration of a child location so that it is different from that of its parent.

The Configuration tab allows you to configure the following:

- SSID
- RADIUS
- Tunnel Interface
- Role Profile
- Radio Settings
- Device Settings
- Configure a Group

**Service Impact of Configuration Changes**

CloudVision WiFi (CVW) warns a user of any service impact caused by settings changed on the UI. In general, the configuration changes affect the WiFi service as follows:

- Changes to SSID settings cause the SSID to restart.
- Changes to RADIUS profiles, Role Profiles, and Tunnel Interfaces cause SSIDs using these profiles to restart.
- Changes to Device and Radio Settings can cause either SSIDs using these settings to restart or access points (APs) using these settings to reboot.

Exceptions to the general rule exist—settings that do not cause any service interruptions.

The table below is a tab-wise list of the impact that each setting change has on the WiFi service.

<table>
<thead>
<tr>
<th>Tab and Action</th>
<th>Settings</th>
<th>Impact of Setting Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID</td>
<td>Client Isolation</td>
<td>No impact.</td>
</tr>
<tr>
<td></td>
<td>Hide SSID</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SSID Profile Name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Any other setting</td>
<td>SSID restarts.</td>
</tr>
<tr>
<td>Role Profile</td>
<td>Profile Name</td>
<td>No impact.</td>
</tr>
<tr>
<td></td>
<td>Any other setting</td>
<td>SSIDs using these settings restart.</td>
</tr>
<tr>
<td>Tunnel Interface</td>
<td>Profile Name</td>
<td>No impact.</td>
</tr>
<tr>
<td>Feature</td>
<td>Setting Description</td>
<td>Impact</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>--------------------------------------------------------------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td><strong>RADIUS Profile</strong></td>
<td>Any other setting</td>
<td>SSIDs using these settings restart.</td>
</tr>
<tr>
<td><strong>Profile Name</strong></td>
<td>No impact</td>
<td></td>
</tr>
<tr>
<td><strong>Any other setting</strong></td>
<td>SSIDs using these settings restart.</td>
<td></td>
</tr>
<tr>
<td><strong>Radio Settings</strong></td>
<td>Any other setting</td>
<td></td>
</tr>
<tr>
<td><strong>WiFi Regulatory Domain</strong></td>
<td>APs using these settings reboot</td>
<td></td>
</tr>
<tr>
<td><strong>Any other setting</strong></td>
<td>SSIDs using these settings restart.</td>
<td></td>
</tr>
<tr>
<td><strong>Device Settings</strong></td>
<td>- Access Radio Exceptions</td>
<td>SSIDs using these settings restart.</td>
</tr>
<tr>
<td></td>
<td>- Scanning</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- WiFi Scan Duration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- WiFi Access Duration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Inter-Access Point Sync for Client Steering</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Inter AP Sync Period</td>
<td></td>
</tr>
<tr>
<td><strong>Mesh Profile</strong></td>
<td>- SSID VLAN Monitoring</td>
<td>APs using these settings reboot</td>
</tr>
<tr>
<td></td>
<td>- IPv4/IPv6 Dual Stack</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Turn Access Points into Dedicated WIPS Sensors</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Link Aggregation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Transmit Hash Policy</td>
<td></td>
</tr>
<tr>
<td><strong>Mesh Profile Enabled</strong></td>
<td>Mesh APs reboot</td>
<td></td>
</tr>
<tr>
<td><strong>Mesh Profile Disabled</strong></td>
<td><strong>Note</strong>: When you edit an “enabled” mesh profile, mesh links are re-established, which may disrupt WiFi service to clients.</td>
<td></td>
</tr>
<tr>
<td><strong>Monitor &gt; WiFi &gt; Access Points &gt; Customize VLANs</strong></td>
<td>Any setting</td>
<td>AP reboots.</td>
</tr>
<tr>
<td><strong>Monitor &gt; WiFi &gt; Access Points &gt; Customize Transmit Power or Channel</strong></td>
<td>Any setting</td>
<td>SSIDs on the AP restart.</td>
</tr>
<tr>
<td><strong>Monitor &gt; WiFi &gt; Access Points &gt; Assign/Reassign to Group OR Remove Access Points from Group</strong></td>
<td>The service impact depends on which settings at the current location change because of the operation.</td>
<td>APs or the SSIDs on these APs may restart.</td>
</tr>
<tr>
<td><strong>Other screens from which you can change AP-group assignment:</strong></td>
<td>- System &gt; Navigator&gt; Show Available Devices</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Floor Plan</td>
<td></td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
<td>Implications</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Get Configuration from another folder/group.</td>
<td>The service impact depends on which settings at the current location change because of the operation.</td>
<td>APs or the SSIDs on these APs may restart.</td>
</tr>
<tr>
<td>Monitor &gt; WiFi &gt; Radios &gt; Turn Off Radio</td>
<td>-</td>
<td>All SSIDs on the radio are turned off.</td>
</tr>
<tr>
<td>Customize or Inherit Configuration at a Location</td>
<td>The service impact depends on which settings at the current location change because of the operation.</td>
<td>APs or the SSIDs on these APs may restart.</td>
</tr>
<tr>
<td>Move AP to another location</td>
<td>The service impact depends on which settings at the current location change because of the operation.</td>
<td>APs or the SSIDs on these APs may restart.</td>
</tr>
<tr>
<td>Troubleshoot &gt; Auto Packet Trace</td>
<td>Enable or disable auto packet trace on an SSID</td>
<td>SSIDs for which auto packet trace is enabled or disabled will restart.</td>
</tr>
</tbody>
</table>
SSID Settings

You can configure SSID settings on the Configure > WiFi > SSID tab.

The SSID tab shows all the SSIDs configured on your WiFi network along with their key features. You can switch between a Card View, where the SSIDs and their key configurations are shown as cards, and a Table View that lists these items in a table. You can add and edit an SSID. You can also turn an SSID on or off. You can click on an SSID to configure it.

Note: By default, the configuration of a folder is automatically inherited by its child folders. For example, suppose there is an HQ folder with two child folders: Branch 1 and Branch 2. Then a configuration applied to HQ automatically applies to Branch 1 and Branch 2. You can, however, customize the configuration of a child folder so that it is different from that of its parent.

SSID Configuration Tabs

For each SSID, there are nine functional settings: Basic, Security, Network, Access Control, Analytics, Captive Portal, RF Optimization, SSID Scheduling, and Traffic Shaping and QoS.

Of these, the first three — Basic, Security, and Network — are essential to an SSID, i.e., you must configure these settings before you can save an SSID and turn it on. You can configure the remaining tabs if you need to, otherwise they assume default values.

You can add up to 8 SSIDs on the 2.4GHz band and up to 8 SSIDs on the 5GHz band in each folder.

Add New SSID

To add an SSID, go to Configure > WiFi > SSID, and click Add SSID. Enter the details in each tab sequentially. You must configure at least the Basic, Security, and Network tabs before you can save the SSID. To configure any of the other SSID tabs, click the three-dot menu next, which is typically next to the Network tab, and select the tab you want to configure.

9.1 SSID Basic Settings

The Basic tab is the first of the three SSID tabs (Basic, Security and Network) that you must configure before you can save an SSID and turn it on.

Some of the fields in the Basic tab are self explanatory; the remaining fields are described in the following table:

<table>
<thead>
<tr>
<th>SSID Profile Name</th>
<th>Typically, this is the same as the SSID Name. It is primarily meant to distinguish between duplicate SSIDs. So, duplicate SSIDs at the same location have different profile names. For example, if you duplicate &quot;ABC Corp&quot; at the same location, then the new SSID name will be &quot;ABC Corp&quot; but its profile name will be &quot;Copy of ABC Corp(1)&quot;. You can modify the profile name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID Type</td>
<td>This could be a Public or a Guest SSID. If you select Guest, the UI you can see the Captive Portal tab next to the Network tab, since Guest SSIDs typically use captive portal logins.</td>
</tr>
</tbody>
</table>
If you select this, the SSID will be hidden, i.e., it will not be broadcast on the wireless link.

### 9.1.1 Configure SSID Basic Settings

The Basic tab is the first of the three SSID tabs (Basic, Security and Network) that you must configure before you can save an SSID and turn it ON.

Enter information on the following fields:

1. Enter the name you want to assign the SSID in **Enter SSID Name**. The **Enter Profile Name** field gets populated automatically with the SSID name, except if this is a duplicate SSID at the same location as the original.

2. Select if you want this to be a **Private** SSID or a **Guest** SSID.

3. Select **Hide SSID** if you do not want this SSID to be broadcast.

4. The next step depends on whether you are adding a new SSID or updating an existing one:
   - If you are adding a new SSID, click **Next** to move to the **Security** tab.
   - If you are updating an existing SSID, click **Save** or **Save & Turn SSID On**. In this case, an "SSID updated successfully" message appears.

### 9.2 SSID Security Settings

The Security tab is the second of the three SSID tabs (Basic, Security and Network) that you must configure before you can save an SSID and turn it on.

#### Select Security Level for Associations

The Security Level defines the authentication mechanisms for users of this SSID. The options are:

**Open**
Open means no security settings are to be applied. This is the default security setting.

**OWE (Enhanced Open)**
OWE (Enhanced Open), as the name suggests, is an enhancement to open networks. It provides data security for open networks. Open SSID networks are widely used in coffee shops, shopping malls, airport lounges, and enterprise guest networks, and OWE offers data security to your clients with encrypted sessions.

**WPA2**
The WPA2 security protocol was created to fix the vulnerabilities of WPA and therefore it is more robust than WPA. It fully implements the IEEE 802.11i standard. You can use WPA2 with **PSK** (Pre-Shared Key), **Group PSKs**, or **802.1x**, i.e., RADIUS-based authentication.

**WPA / WPA2 Mixed Mode**
This stands for a mix of the WPA and WPA2 protocols. You can use WPA with **PSK** (Pre-Shared Key), **Group PSKs** or **802.1x**, i.e., RADIUS-based authentication.

**WPA3**
The WPA3 security protocol mitigates the vulnerabilities of WPA2. You can use WPA3 Personal or WPA3 Enterprise.
SSID Settings

WPA3 Personal is typically meant for home users. Its robust password-based authentication and 128-bit data AES encryption provides stronger security and protection than WPA2. WPA3 Personal provides protection against attacks such as offline dictionary attacks that attempt to guess passwords. WPA3 Enterprise has an option to use 192-bit encryption and it is meant for enterprises and office networks where the need for data security and protection is higher.

Management Frame Protection is mandatory for both WPA3 Enterprise and WPA3 Personal.

WPA2/WPA3 Mixed Mode

This stands for a mix of WPA2 and WPA3 protocols. If your SSID operates in WPA2/WPA3 Mixed Mode, then WPA2-only clients can also connect with the same SSID along with WPA3-supported clients. In this mode, WPA3 clients use WPA3 Personal.

Note: 802.11w and 802.11r are supported in WPA2, WPA3, and WPA2/WPA3 Mixed Mode. WPA/WPA2 Mixed Mode doesn't support 802.11w and 802.11r.

RADIUS Settings

See 802.1X or RADIUS Settings for details.

802.11w

802.11w offers Management Frame Protection (MFP). MFP is an additional security mechanism that protects the De-authentication, Disassociation and Robust Action management frames and prevents some spoofing attacks. The Integrity Group Temporal Key (IGTK) is used to provide integrity check for multicast management action frames, while the Pairwise Transient Key (PTK) is used to encrypt and protect unicast management action frames. The Group Management Cipher Suite is the combination of security and encryption algorithms used to protect management frames. Arista uses the AES-128-CMAC algorithm, so that's what is selected by default.

Association frames are not protected as they need to be open for a client to establish an association with an AP. To make sure that a client Association Request isn't spoofed, the AP sends a Security Association (SA) query to a client requesting association. A genuine client responds to the protected frames. The SA Query Max Timeout is the time, in seconds, for which the AP waits for a client to respond to an SA query. If the AP receives no response within this period, it ignores the client. Since clients that spoof Association Requests don't respond, the AP rejects them. The SA Query Retry Timeout is the time, in milliseconds, for which a client can request to associate with the AP after the SA Query max timeout.

802.11r

With WPA2, you can also enable 802.11r. 802.11r or Fast Transition (FT) allows clients to re-establish security and QoS parameters before associating with a new AP, significantly reducing the interruption that the client experiences during the transition.

Select Over the DS if you want to set a preference for clients to roam by using the Over the Distribution System (DS) mode of roaming. Client devices govern the mode of roaming from one AP to another. When you don't select Over the DS, clients roam over the air. Note that this is just a preference. A client can roam over the air irrespective of the preference. Select Mixed Mode to allow both 802.11r compatible and 802.11r non-compatible clients to connect to the SSID.
9.2.1 Configure SSID Security Settings

The Security tab is the second of the three SSID tabs (Basic, Security and Network) that you must configure before you can save an SSID and turn it ON.

Steps to configure the SSID security settings are:

1. Go to the Security tab under CONFIGURE > SSID.
2. Select Security Level for Associations for this SSID
   - If you select Open, there is nothing more you need to do for security. Click Next to move to the Network tab if you are adding a new SSID, or click Save or Save and Turn SSID On if you are updating an existing SSID.
   - If you select OWE (Enhanced Open), there is nothing more you need to do for security. Click Next to move to the Network tab if you are adding a new SSID, or click Save or Save and Turn SSID On if you are updating an existing SSID.
   - If you select WPA2, you need to select either PSK or 802.1x.
   - If you selected WPA2 and PSK, Enter a Passphrase. You can also enable Group PSK. For information on Group PSKs, refer to Group PSKs.
   - If you select WPA2 and 802.1x, you need to enter the RADIUS Settings. RADIUS settings include:
     - The RADIUS servers you want to use as Authentication Server and Accounting Server.
       You can add up to four RADIUS servers. One is the primary server and the other three are fallback or additional servers. If the Primary server is not reachable, the AP tries to reach the second server defined on the UI. If the second RADIUS server is not reachable, then the AP tries to reach the third server and so on. The AP follows the same order of hierarchy for the additional RADIUS servers that you define on the UI.

       **Note:** If you have not yet defined a RADIUS profile to choose as your Authentication or Accounting server, you can do so by clicking Add / Edit. This opens a RADIUS Profile window on the right pane. You can create the RADIUS profile and return to security settings. See Configure RADIUS Profile for details.

     - The Called Station / NAS ID, IDs that the AP or a Network Access Server (NAS) send the RADIUS server.

       **Note:** No two SSIDs on the same AP should use the same NAS ID.

     - The Retry Parameters that control how often the AP attempts to authenticate with RADIUS.
     - Fast Handoff Support which saves clients some authentication time when the roam from one AP to another.
     - Dynamic VLANs to enable RADIUS-based assignment of VLANs.
     - Change of Authorization (CoA) to change a client's authorization. For example, you can use CoA to assign VLANs to a user or to assign roles to a user when implementing Role-Based Access Control.

       **Note:** For CoA, open Port 3799 on your firewall from the RADIUS server to the AP.

     - Enable Prefer Primary RADIUS Server if you want the authentication to fall back to the primary RADIUS server once it comes back up after a failover. This helps if, for example, your secondary RADIUS servers have lower capacity than the primary servers. Another example where this helps is when enterprises use two data centers, each one configured as the “secondary” of the other. You would then want the authentication to fall back to the primary or “home” data center RADIUS server once it comes back up.

       Once an AP detects a failover to the secondary RADIUS server, it waits for the Dead Time interval before falling back to the primary. This ensures that fallback doesn’t happen too soon, allowing time for the primary server to stabilize if it had been flapping.

     - Select the type of Framed IPv6 Address that you want the RADIUS Accounting message to report to an authenticated WiFi client. The choice depends on whether your network
SSID Settings

uses solicited IPv6 addresses or unsolicited ones obtained via SLAAC (Stateless Address Autoconfiguration). For solicited IPv6 addresses, select **Report Full IPv6 Address**; for the unsolicited case, select **Report Only IPv6 Prefix**.

- If you select **WPA2**, you can configure **802.11w** for Management Frame Protection (MFP), and **802.11r** for Fast Transition (FT). If you select **PSK**, you can enable Group PSK. To enable Group PSK, select **Group PSK** and enter the passphrase.

  **Note:** 802.11w and 802.11r are supported only in the WPA2 mode, not in the Open or WPA/WPA2 Mixed Mode.

- If you select **WPA/WPA2 Mixed Mode**, you need to select either **PSK** or **802.1x**. If you select **PSK**, you can enable Group PSK. To enable Group PSK, select **Group PSK** and enter the passphrase. You can then proceed in exactly the same manner as when you select **WPA2**, except that 802.11w and 802.11r are not supported in WPA/WPA2 Mixed Mode.

- If you select **WPA3**, you need to select either **WPA3 Personal** or **WPA3 Enterprise**. WPA3 Personal uses Simultaneous Authentication of Equals (SAE) to secure data and it is meant for home users. WPA3 Enterprise is meant for organizations as it includes an option to add 192-bit security for data security.

3. The next step depends on whether you are adding a new SSID or updating an existing one:

- If you are adding a new SSID, click **Next** to move to the **Network** tab.
- If you are updating an existing SSID, click **Save** or **Save & Turn SSID On**. In this case, an "SSID updated successfully" message appears.

### 9.2.2 Group PSKs

A single SSID can support up to 32 Group PSKs, each for a group of WiFi clients. To appreciate Group PSKs, consider the following use cases:

- An enterprise might require IoT devices to connect to the WiFi network. Network administrators often want to use the same SSID for different client device categories, but assign different VLANs or access lists to them—for example, they might want to map printers and video cameras to separate VLANs. IoT devices typically do not support 802.1X-based authentication methods that enterprises use to segment clients into separate VLANs. With Group PSKs, you can configure the same SSID with different PSKs: one PSK for printers, another one for video cameras, and so on. You can also assign roles to each Group PSK.

- A small branch office or a retail establishment might want to segment users on the same SSID by department (HR, finance, legal, etc.). Such establishments typically do not have 802.1X infrastructure; they can use Group PSKs to segment users.

#### Limitations

Group PSKs have the following limitations:

- Group PSKs are supported for only the following security methods:
  - WPA2 with PSK and
  - WPA/WPA2 Mixed Mode with PSK.
- Secondary Authentication (e.g., RADIUS MAC Authentication or Google Authentication) is not supported for Group PSKs.
- Captive Portal is not supported with Group PSKs.
- Group PSKs are not supported for SSIDs using VPN (L3 tunnel) or NAT.
9.3 SSID Network Settings

The Network tab is the third of the three SSID tabs (Basic, Security and Network) that you must configure before you can save an SSID and turn it ON.

You must enter the default VLAN ID for this SSID.

You can have access points on this SSID operate in bridged, NAT or Tunneled modes.

**Bridged**

Use a bridged network when you want an AP and clients associated with the AP to be on the same subnet.

**NAT**

When you want an AP and its clients on separate subnets, use Network Address Translation (NAT). With NAT, clients have a private IP address pool and it is easier to add more clients to the network as they do not require a public IP address. NAT translates local IP addresses to global ones (and vice versa).

**Note:** NAT cannot be selected if under SSID Security Settings, you have enabled Dynamic VLANs with 802.1X authentication.

To configure NAT, you need to enter the **Start IP Address**, the **End IP Address**, and the **Subnet Mask**. Together, these define the IP pool from which the AP will assign IP addresses to clients. The **Local IP Address** is the IP address of the AP on the wireless side, i.e., the client-facing IP address. It serves as the gateway for associated clients. Upon successful association, wireless clients get their DNS information from the list of IP addresses you have entered in the **DNS Servers** field. You must enter at least one DNS server IP address. You can enter up to six DNS server IP addresses. The **Lease Time** is the DHCP lease time in minutes, after which the IP allocated to the client expires.

With **Wired Extension**, you can extend a NAT-enabled wireless LAN to the wired side using the second Ethernet port on the AP. You can do so by creating an isolated wired LAN with one or more wired devices connected through layer-2 switches, and connecting the second Ethernet port of the AP to this wired subnet. The wired LAN then becomes an extension of the wireless LAN with this SSID profile. All network settings configured on this SSID profile then apply to the wired devices as well.

**Note:** The second Ethernet port is available only on some Arista AP models.

**Tunneled**

A Tunnel Interface is useful when you want to route network traffic on the SSID to and from a single end point, and apply policies at this end point. In the tunneled mode, APs on the SSID route all traffic via the tunnel to a remote endpoint configured on the **Tunnel Interface** that you select. See **Tunnel Interface** for details. If you haven't yet defined a Tunnel Interface, you can do it from within the Network tab using the **Add / Edit** link.

In tunneled networks, the RADIUS server could be located in the private corporate network behind the remote endpoint. When you enable **Use Tunnel for RADIUS Messages**, CloudVision WiFi tunnels RADIUS messages between the AP and the RADIUS server. Key characteristics are:

- All types of tunnel interfaces support tunneling of RADIUS messages between APs and a RADIUS server located behind the tunnel endpoint.
- For tunnel types other than the RAP VPN tunnel, an AP obtains its IP address from the DHCP server in the remote network on the SSID VLAN. A RAP running an SSID with a VPN tunnel obtains its VPN IP address from the remote VPN endpoint, e.g., a firewall appliance.
- The RAP VPN tunnel does not support IPv6. So for a RAP to communicate with a RADIUS server, the RADIUS server must have an IPv4 address.

The following RADIUS message types are supported for communication via tunnel:
SSID Settings

- Authentication (802.1X or RADIUS MAC Authentication)
- Accounting
- CoA (Change of Authorization)

With **Layer 2 Traffic Inspection and Filtering** (L2TIF) enabled on an SSID, Arista APs running the SSID send all packets to a wired endpoint, i.e., a tunnel endpoint or a switch. You can then configure the wired endpoint to inspect and filter traffic. An effect of enabling L2TIF on an SSID is that two clients associated with the SSID cannot communicate directly with each other on the wireless link; their packets are sent to the wired endpoint. What happens to these packets depends on the policies configured at the endpoint.

Consider two WiFi clients, Client 1 and Client 2, associated with the same AP and the same SSID. As shown in the figure below, with L2TIF enabled, packets originating from Client 1 and destined for Client 2 are sent to the switch.

Switches typically discard packets whose source and destination are on the same port. If you wish to allow some types of direct Layer 2 communication on your network (for example, peer-to-peer file-sharing applications or access to printers) while still sending all packets to the wired endpoint for inspection, you can do so by configuring appropriate policies at the endpoint.

**Note:** L2TIF is applicable only to SSIDs in the bridged mode; in the tunneled mode, SSID traffic is anyway tunneled to an endpoint. Also, L2TIF is not supported for SSIDs that have NAT enabled. This is because an AP running a NAT-ed SSID becomes the gateway node of its own private subnet; its clients are not visible to the wired endpoint.

**Inter AP Coordination** is the mechanism where Arista APs exchange information with each other. You can select how APs exchange this information by choosing one of the three options:

**L2 Broadcast**
APs broadcast their information over the wired network. L2 broadcast works on the SSID VLAN and, if Layer 2 GRE is enabled, it works on the communication VLAN. You can **Use Tunneling for Inter AP Coordination** so that information related to inter-AP coordination flows through the tunnel, i.e., from one AP to the tunnel endpoint to another AP.

**RF Neighbors**
APs exchange information only with their RF neighbors. Dual-radio APs use Background Scanning to find their RF neighbors, tri-radio...
APs use their third radio. If you have not enabled **Background Scanning** under **Device Settings**, CloudVision WiFi prompts you to do so when you turn the SSID ON. You can use **Tunneling for Inter AP Coordination** so that information related to inter-AP coordination flows through the tunnel, i.e., from one AP to the tunnel endpoint to another AP.

**Note:** RF Neighbor can be used only with 802.11ac or higher Arista APs.

### This Server

APs exchange information via the Wireless Manager server. The information is shared from a parent location to its child locations.

**Note:** Since the Arista server is involved, you cannot use the tunneling mode for inter-AP information.

If you select **Advertise Client Associations on SSID VLAN**, APs on this SSID broadcast their client associations to other APs on the same SSID VLAN. This helps clients in fast roaming.

**DHCP Option 82** (DHCP Agent Information Option) is generally used in a distributed DHCP server environment to assign IP addresses to clients based on their location. The AP inserts DHCP Option 82 in all DHCP packets, such as DHCP Discover and DHCP Request, thereby providing additional information to identify the client’s point of attachment. DHCP Option 82 contains a **Circuit ID** that you can configure at this location and on the DHCP server as well. The DHCP server then selects an appropriate IP pool for the Circuit ID it receives, and assigns an IP address to the client from this pool. For an example, see **Example Use Case for DHCP Option 82**.

**Multicast DNS (mDNS) Packet Tagging** helps WiFi clients discover network services such as printers or conference room displays. A WiFi client sends an mDNS packet querying for services on the network—for example, printers. An Arista AP can tag client mDNS query packets with a location name. The AP adds its location, i.e. the name of the folder in the location tree, as a tag to the mDNS query. mDNS gateways running on Arista aggregation switches use the location tag to filter services that they return in response to the mDNS query. This filtering is based on rules configured in the mDNS gateway—for example, the mDNS gateway in the following figure can be configured so that when it receives a query tagged with “Floor 1” as the location, it returns only “Printer 1”, the printer located on floor 1.
SSID Settings

Note:

- mDNS tagging is not supported in NAT or VPN Tunnel modes.
- For mDNS tagging to work, make sure your aggregation switch supports mDNS gateways. See the Supported Features page on the Arista website to check if a particular switch model supports an mDNS gateway.
- Make sure you have assigned the correct location tag to each location because mDNS gateways return devices based on location tags. See Set Location Tag for steps on how to assign location tags.

9.3.1 Example Use Case

Let’s consider an enterprise deployment with two branch offices and a single DHCP server hosted in the data center at the HQ. Only one SSID is configured and the same configuration is assigned to all the branch office locations. The same VLAN ID is configured but different subnets are assigned to the branch office locations.

In this case, we create three SSID profiles:

- HQ
- Branch1
- Branch2

We also configure the appropriate location tags for each location (HQ and branch offices) in the location tree.
DHCP Option 82 is enabled and the Circuit ID is set to “%l” which sends the location tag to the DHCP server.

On the DHCP server, we configure policies based on the information received from the DHCP Option 82:

- If Circuit ID = HQ then assign IP from 172.16.0.0/16 – 172.16.8.255/16 subnet
- If Circuit ID = Branch1 then assign IP from 172.16.9.0/16 – 172.16.12.255/16 subnet
- If Circuit ID = Branch2 then assign IP from 172.16.13.0/16 – 172.16.15.255/16 subnet

9.3.2 Configure SSID Network Settings

The Network tab is the third of the three SSID tabs (Basic, Security and Network) that you must configure before you can save an SSID and turn it ON.

Steps to configure the SSID network settings are:

1. Go to CONFIGURE > SSID > Network.
2. Enter the default VLAN ID for the SSID.
3. Select the AP mode of operation for the SSID.
   - If you select Bridged mode, you do not need to configure anything more and you can proceed to the next step.
   - If you select NAT, you need to configure the following NAT-related parameters:
     - **Start IP Address** defines the starting IP address of the IP pool from which the AP assigns IP addresses to clients.
     - **End IP Address** defines the end IP address of the IP pool from which the AP assigns IP addresses to clients.
     - **Local IP Address** is the local IP address of the APs on the wireless side.
     - **Subnet Mask** is the subnet mask for the IP pool.
     - **DNS Servers** are the DNS servers that clients will use to get DNS information. You must enter at least one DNS server IP address. You can enter up to three such DNS server IP addresses.
     - **Lease Time** is the DHCP lease time in minutes, after which the IP allocated to the client expires.
     - Select **Wired Extension** to extend a NAT-enabled wireless LAN to the wired side using the second Ethernet port on the AP.
   - If you select L2 Tunnel or VPN Tunnel, you need to select the **Tunnel Interface** which contains the endpoint to which the AP will tunnel all traffic. If you have not yet defined a tunnel interface, you can do so by clicking Add / Edit. This opens a Tunnel Interface window on the right-pane. You can create the interface and return to network settings.
     - Enable **Use Tunnel for RADIUS Messages** if the enterprise RADIUS server is behind the tunnel endpoint and you wish to tunnel RADIUS messages to the endpoint.
       - **Note:** Either 802.1X or RADIUS MAC Authentication must be enabled for communication with a remote RADIUS server.
     - For EoGRE tunnels, you can **Synchronize Failover and Fallback of RADIUS Server with EoGRE Interface.** This is helpful if the primary and secondary RADIUS servers are bound to the respective EoGRE interfaces but they do not mutually sync client authentication states. In such cases, selecting this prevents a “split-brain” situation, where the client data flows via the secondary EoGRE tunnel while RADIUS messages are exchanged with the primary RADIUS.
4. Select the **Inter AP Coordination** mechanism
   - If you select L2 Broadcast, APs broadcast their information over the wired network. Select **Use Tunneling for Inter AP Coordination** if you want the inter-AP coordination related information to flow through the tunnel.
SSID Settings

- If you select RF Neighbors, APs exchange information only with their RF neighbors. Select Use Tunneling for Inter AP Coordination if you want the inter-AP coordination related information to flow through the tunnel.
- If you select This Server, APs exchange information via the Wireless Manager server.

**Note:** Since the Arista server is involved, you cannot use the tunneling mode for inter-AP information.

5. Select Advertise Client Associations on SSID VLAN if you want APs on the SSID to broadcast their client associations to other APs on the same SSID VLAN.

6. Select DHCP Option 82 to assign clients IP addresses based on their location in a distributed DHCP server environment.

7. Select Multicast DNS (mDNS) Packet Tagging if you want APs to tag client mDNS query packets with the location name. mDNS gateways running on the switch return appropriate network services (printers) based on the location tag.

8. Click Save or Save & Turn SSID On.
   - If you select Save & Turn SSID On, see Turn an SSID On for details.

If you are adding a new SSID, an "SSID created successfully" message appears. If you are updating an SSID, an "SSID updated successfully" message appears.

**9.3.3 SSID VLAN Mapping**

To enable SSID VLAN mapping:

1. Go to Configure > WiFi > SSID > Add SSID.
2. Click the Network tab.
3. In VLAN, select the VLAN Name radio button and provide your VLAN name.
4. Provide a fallback VLAN ID.
5. Click SSID VLAN Mapping.
   - A right panel opens where you can map the name to a VLAN ID. You can also see the location where this mapping is used.
6. Add the VLAN name and ID and save the settings.
7. Save and turn on the SSID.

**9.4 SSID Access Control**

The SSID Access Control tab contains settings that control access to the SSID, for example, Firewall and Client Authentication settings.

You can configure the following firewalls on the Access Control tab:

- L3-4 Firewall
- Application Firewall

**Note:** You can not enable firewall settings if Dynamic VLANs is enabled under CONFIGURE > SSID >Security > 802.1X

To configure the firewall settings, see Configure Firewall Settings.

You can enable Apple’s Bonjour Gateway feature that allows access to Apple devices on the network.

**Note:** Bonjour Gateway does not work when the Network is set to NAT mode. If you have set the Network to NAT mode, CloudVision WiFi grays out Bonjour Gateway and prompts you to change the Network setting from within the Access Control tab.

For details, see How Arista Supports Bonjour Gateway. To configure Bonjour Gateway, see Configure Bonjour Gateway.
You can enable **Redirection** to redirect either Smartphones & Tablets or all clients of the SSID to the **Redirect URL** that you specify. This could be useful, for example, in an enterprise network where you might want smartphones and tablets to be redirected when accessing the SSID, but allow laptops and desktops to directly start using WiFi. You can also have a **Walled Garden** of sites that the user can access before login.

**Note:** You must enter at least the Redirect URL in the **Walled Garden** field, since the user must be able to access that URL before login.

To configure Redirection, see **Configure Redirection in SSID Access Control**.

Organizations such as enterprises and educational institutions (K-12 and higher education) often implement a centralized AAA (Authentication, Authorization and Accounting) management to enforce **Role Based Control**, also called Role Based Access Control (RBAC). RBAC enables network administrators to restrict system access to authorized users. Users are granted controlled access to network resources based on the roles assigned to them or the groups to which they belong. Typically, organizations implement this kind of controlled access by using RADIUS. When users connect to the network, they are first authenticated and then authorized to access appropriate resources on the network.

In the case of a WLAN network, user access restrictions could mean that only specific VLANs or a fixed bandwidth is provided to users based on the user roles defined in the RADIUS server. You can also enforce which applications a user can access over the WLAN network based on the user role.

Arista uses Role Profiles to define various WLAN access roles, and to create RADIUS Vendor Specific Attribute (VSA) based rules and Google Organizational Unit (OU) rules to authorize Wi-Fi users. A network administrator can define various role profiles that specify the restrictions to be placed on the Wi-Fi user to whom the profile is assigned. The administrator can then define multiple VSA rules (for RADIUS) or Google OU rules (for Google Integration) here in SSID Access Control, and assign role profiles through these rules to the Wi-Fi users that connect to the SSID.

Let's consider an example. When you define a **Rule Type** for RBAC, then the OU returned from Google or the role obtained from the RADIUS VSA must contain the string entered in the **Enter Value** field. For example, if the string in the **Enter Value** field is ‘/*/Elementary School/*/Student’, then this will match with ‘/SJUSD/Elementary School/Almaden Elementary/Student’ in Google/VSA.

It could happen that you have different settings in the SSID tabs and different ones in the Role Profiles tab. What happens then? For the answer, see **Role Profile**.

To configure Role Based Control, see **Configure Role Based Control**.

To control clients that can access this SSID, you can create Allow and Deny lists of client MAC addresses. See **How the Client MAC Allow and Deny Lists Work** and **Requirements** for details on the feature.

With **Client Isolation** enabled on an SSID, WiFi clients associated with the SSID are allowed to communicate only with their gateway; they cannot communicate directly with any other hosts on the same subnet—including other clients on the same SSID, clients associated with other SSIDs on the same subnet, and hosts connected to the wired network on the same subnet. An AP running an SSID with Client Isolation discards all packets from a client if the destination IP address is on the same network as the client, except for packets destined to the gateway.

Consider two WiFi clients, Client 1 and Client 2, associated with different APs on the same SSID, SSID 1. As shown in the figure below, with Client Isolation enabled, AP1 discards packets originating from Client 1 and destined to Client 2.
SSID Settings

If NAT is enabled on an SSID, an AP running the SSID becomes the gateway node of its own private subnet. Consider Client 1 and Client 2 in the figure above. If these clients are associated with a NAT-ed SSID, they cannot see each other’s IP address. Thus, it is NAT rather than Client Isolation that prevents direct connections between these clients; Client Isolation prevents direct connections only between clients of the same AP.

Note that even with a NAT-ed SSID, the net effect of enabling Client Isolation is the same as in the case of a bridged or tunneled SSID: clients on the same SSID cannot communicate directly with each other. But the mechanisms that prevent such communication are different: NAT prevents direct communication between clients on different APs and Client Isolation prevents direct communication between clients of the same AP.

Client Authentication adds another layer of security to your network. It authenticates clients, i.e. user devices, in addition to mechanisms configured in the SSID Security tab that authenticate users (e.g. WPA2-PSK). Client Authentication uses either Google Integration or RADIUS MAC Authentication. See Google Integration for more information.

Note: If you have configured 802.1X authentication in the SSID Security tab, then CloudVision WiFi grays out the RADIUS MAC Authentication option, since 802.1X already is a RADIUS-based mechanism.

Some WiFi clients send Diassociation messages whenever they enter a "sleep" mode. If the AP immediately sends an Accounting Stop request to the RADIUS server, the RADIUS server clears the client info and the client has to reauthenticate when it wakes up. This could cause frequent and unnecessary reauthentication. The Accounting Stop Delay is the number of minutes that the AP waits between the time it receives the Disassociation and the time it sends the Accounting Stop message to the RADIUS server. If the client wakes up in the interim and communicates with the AP, the Accounting Stop message is not sent and the client does not need to reauthenticate.

For the other RADIUS settings, see Configure SSID Security Settings.

You can choose to either Disconnect or Stay Connected and Assign Role to the user. To assign a role, you need to select one from those defined on the Role Profile tab. You might configure Client Authentication before you have created any Role Profile. When you click Add / Edit under Select Role, a window appears in the right pane, allowing you to define a Role Profile without having to leave Client Authentication.
To configure Client Authentication, see Configure Client Authentication.

9.4.1 Configure SSID Access Control
You can configure settings that control access to the SSID, for example, Firewall and Client Authentication settings.

SSID Access Control consists of the following settings:

1. Configure the **Firewall** settings.
   See Configure Firewall Settings for details.

2. Configure **Bonjour Gateway** settings
   See Configure Bonjour Gateway for details.

3. Configure **Redirection** settings.
   See Configure Redirection Settings for details.

4. Configure **Role Based Control** settings.
   See Configure Role Based Control for details.

5. Configure **WiFi Clients in Allow List and Deny List** settings.
   See Configure Allow and Deny Lists of WiFi Clients for details.

6. Enable **Client Isolation** to prevent clients of the same AP from being able to access each other's data.

7. Configure **Client Authentication** settings.
   See Configure Client Authentication for details.

8. Click **Save** or **Save & Turn SSID On**.
   If you select **Save & Turn SSID On**, see Turn an SSID On for details.

If you are adding a new SSID, an "SSID created successfully" message appears. If you are updating an SSID, an "SSID updated successfully" message appears.

9.4.2 L3-4 Firewall
Arista Access Points (APs) have firewall capabilities. The AP firewall monitors the traffic passing through the AP and takes actions based on user-defined rules.

The firewall is stateful, that is to say, it keeps track of whether the connection has been opened in the outgoing direction (wireless to wired-side) or in the incoming direction (wired-side to wireless), and takes appropriate actions on the packets based on the direction in which the connection was opened. The following image illustrates the conventions used for directions.

Note that this is not the Internet facing firewall. Its main purpose is to facilitate traffic controls, such as allowing/disallowing access to certain assets and/or applications for wireless users. The firewall rules are defined and enforced on a per SSID basis. Arista APs support multiple SSID profiles, thereby enabling multiple firewall configurations to co-exist.

The following use cases illustrate typical applications for the Arista AP firewall functionality:

- Block guest Wi-Fi users from accessing the private/corporate subnet. This serves as an additional security control to ensure that guest Wi-Fi users can access only public Internet and nothing in the private address space.
- Block or allow access to specific domain names.
- Allow guest Wi-Fi users to access only HTTP and HTTPS content in the Internet. This is typically done to control the type of traffic guest users can generate.
- Implement DNS-based content filtering to prevent access to non-family-friendly web sites, security threats, and peer-to-peer file sharing. The firewall can be used to ensure that Wi-Fi clients necessarily use the specified content filtering DNS server, such as Norton ConnectSafe, and cannot bypass it.
- Enforce use of IPsec VPN for wireless clients.
Note:

• When you enable L3-4 Firewall Rules, you can see the default rule Action: Block on the UI. If you enable L3-4 Firewall Rules and do not define any rules at all, the default rule applies, i.e., all traffic is blocked.
• The AP compares traffic with rules from top to bottom until it finds the first match. Once it finds the first match, the AP does not compare the rest of the rules. If it finds no match with any of the defined rules, the AP uses the default rule at the end. You can re-order the rules using the drag-and-drop feature to reposition them at the desired level.

In case of a conflict between rules on the L3-4 Firewall and those on the Application Firewall, the AP decides using this Decision Table.

Example Use Case of L3-4 Firewall

Let's look at a rule set that might be found on a Guest SSID in a retail store deployment.

Goal for Retail Store: Allow only HTTP/HTTPS Internet access, with content filtering and no access to private subnets.

Table 1: Example Rules Table for Retail Store

<table>
<thead>
<tr>
<th>Rule Number</th>
<th>Rule Name</th>
<th>IP / Hostname</th>
<th>Port</th>
<th>Action</th>
<th>Protocol</th>
<th>Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Content Filtering DNS1</td>
<td>199.85.126.30</td>
<td>53</td>
<td>Allow</td>
<td>UDP</td>
<td>Outgoing</td>
</tr>
<tr>
<td>2</td>
<td>Content Filtering DNS2</td>
<td>199.85.127.30</td>
<td>53</td>
<td>Allow</td>
<td>UDP</td>
<td>Outgoing</td>
</tr>
<tr>
<td>3</td>
<td>Block All Other DNS</td>
<td>*</td>
<td>53</td>
<td>Block</td>
<td>UDP</td>
<td>Outgoing</td>
</tr>
<tr>
<td>4</td>
<td>No Local Access</td>
<td>192.168.0.0/16, 172.17.0.0/21, 10.0.0.0/8</td>
<td>Block</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
</tr>
<tr>
<td>5</td>
<td>Allow HTTP / HTTPS</td>
<td>*</td>
<td>80, 443</td>
<td>Allow</td>
<td>TCP</td>
<td>Outgoing</td>
</tr>
<tr>
<td>6</td>
<td>Default</td>
<td></td>
<td></td>
<td>Block</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Rule 1 - Allow outbound UDP port 53 to Content Filtering (Norton) DNS1/199.85.126.30. This rule implements DNS-based content filtering to block access to web sites that contain non-family-friendly content, pose security risks, and promote file sharing applications. DNS uses UDP port 53. So this rule allows outgoing UDP connections destined to port 53 on a content filtering DNS server with the 199.85.126.30 host IP address.

Because the firewall is stateful, the return path is automatically allowed and you don't need a separate rule for the return path. This is true for the other rules as well.

Rule 2 - Allow outbound UDP port 53 to Content Filtering (Norton) DNS2/199.85.127.30. Like Rule 1, this rule also implements DNS-based content filtering. This rule provides DNS server redundancy.

Rule 3 - Block all outbound UDP 53. This rule blocks all DNS traffic excluding that which is allowed by Rules 1 and 2. This rule prevents users from statically configuring DNS server addresses on their clients to circumvent content filtering.

Rule 4 - Block traffic to destination 192.168.0.0/16, 172.17.0.0/21 and 10.0.0.0/8. Blocks access to private/corporate subnets. This rule blocks any wireless traffic addressed to any host in the 192.168.0.0/16, 172.17.0.0/21 and 10.0.0.0/8 subnets. The Protocol specified for this rule is Any, which covers any protocol carried over IP. Because there are protocols that do not implement the port concept (e.g. ICMP), the port number gets grayed out when Any is selected as protocol. This rule is ideal for restricting users on the Guest Wi-Fi from accessing private subnets.
Rule 5 - Allow any traffic outbound to TCP port 80, 443. Allow clients to open outgoing TCP connections to port 80 (allows outgoing HTTP connections) and allow clients to open outgoing TCP connections to port 443 (allows outgoing HTTPS connections). The wildcard character (*) represents “any” hosts.

Rule 6 - Default rule is set to Block, which means that all other kinds of communication, except the ones enabled by the rules 1-5, are disallowed.

9.4.3 Application Firewall

You can define firewall rules at the application level.

Note:

- To enable Application Firewall Rules, you must enable Application Visibility under the SSID Analytics tab. CloudVision WiFi prompts you to enable Application Visibility from within the Application Firewall Settings, so you don’t need to navigate to the Analytics tab.
- When you enable Application Firewall Rules, you can see the default rule Action : Block on the UI. If you enable Application Firewall Rules and do not define any rules at all, the default rule applies, i.e., all traffic is blocked.
- The AP tests packets with rules from top to bottom until it finds the first match. Once it finds the first match, the AP does not compare the rest of the rules. If it finds no match with any of the defined rules, the AP uses the default rule at the end. You can re-order the rules using the drag-and-drop feature to reposition them at the desired level.

In case of a conflict between rules on the L3-4 Firewall and those on the Application Firewall, the AP decides using this Decision Table.

Example Use Case of Application Firewall

Shown below is a rule for an enterprise that wants to block Facebook and Twitter on their corporate SSID.

Table 2: Example Rule for Enterprise Corporate SSID

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Category</th>
<th>Application Name</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block Facebook and Twitter</td>
<td>Social Networking</td>
<td>Facebook, Facebook Apps, Facebook Event, Facebook Messages, Facebook Post, Facebook Search, Facebook Video, Facebook Video Chat, Twitter</td>
<td>Block</td>
</tr>
<tr>
<td>Default</td>
<td></td>
<td></td>
<td>Block</td>
</tr>
</tbody>
</table>
9.4.4 L3-4 versus Application Firewall Decision Table

Table 3: Decision Table for L3-4 Firewall versus Application Firewall

<table>
<thead>
<tr>
<th>L3 Firewall Action</th>
<th>Application Firewall Action</th>
<th>Final Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deny</td>
<td>Any</td>
<td>Deny</td>
</tr>
<tr>
<td>Allow</td>
<td>Deny</td>
<td>Deny</td>
</tr>
<tr>
<td>Allow</td>
<td>No Match</td>
<td>Allow</td>
</tr>
<tr>
<td>No Match</td>
<td>Deny</td>
<td>Deny</td>
</tr>
<tr>
<td>No Match</td>
<td>Allow</td>
<td>Allow</td>
</tr>
<tr>
<td>No Match</td>
<td>No Match</td>
<td>Default</td>
</tr>
<tr>
<td>Allow and Mark</td>
<td>Allow and Mark</td>
<td>Allow with App Mark</td>
</tr>
<tr>
<td>Allow and Mark</td>
<td>Allow</td>
<td>Allow with L3 Mark</td>
</tr>
<tr>
<td>Allow and Mark</td>
<td>No Match</td>
<td>Allow with L3 Mark</td>
</tr>
<tr>
<td>No Match</td>
<td>Allow and Mark</td>
<td>Allow with App Mark</td>
</tr>
<tr>
<td>No Match</td>
<td>No Match</td>
<td>Default Mark</td>
</tr>
</tbody>
</table>

9.4.5 Configure Firewall in SSID

You can configure both L3-4 and Application firewalls.

To configure firewalls:

1. Go to Configure > SSID > Access Control.
2. Click Firewall
   The Layer 3-4 Firewall Rules and Application Firewall Rules options appear.
3. Select Layer 3-4 Firewall Rules to set up a L3-4 firewall.
   a. Click the "+" sign to add a new rule to the firewall.
   b. Configure the following details of the firewall rule:
      • Enter the Rule Name, what you want to call the rule.
      • Enter IP / Hostname to which you want to apply the rule.
      • Enter the Port number to which you want to apply the rule.
      • Select the Action, whether you want to Allow, Block, or Allow and Mark the packets under this rule.
      • Select the Protocol to which you want to apply the rule.
      • Select the Direction, whether you want the rule to apply to Any direction, to Incoming packets or to Outgoing packets.
4. Select Application Firewall Rules to set up an application firewall.
   a. Click the "+" sign to add a new rule to the firewall.
   b. Configure the following details of the firewall rule:
      • Enter the Rule Name, what you want to call the rule.
      • Select the application Category to which you want to apply the rule.
      • Select the Application Name to which you want to apply the rule.
      • Select the Action, whether you want to Allow, Block, or Allow and Mark the packets under this rule.

To see what takes precedence between L3-4 and Application Firewall rules, see L3-4 versus Application Firewall Decision Table.
5. Click **Save** or **Save & Turn SSID On**.
   If you select **Save & Turn SSID On**, see Turn an SSID On for details.

If you are adding a new SSID, an “SSID created successfully” message appears. If you are updating an SSID, an “SSID updated successfully” message appears.

### 9.4.6 What is Bonjour Gateway?

Bonjour is Apple’s implementation of zero-configuration networking (Zeroconf). It is used to discover devices and services advertised by Bonjour capable devices on a local network using multicast Domain Name System (mDNS).

Generally, Bonjour devices run on local networks and the Bonjour service advertisements do not cross network boundaries. They are restricted to the broadcast domain of a single VLAN / Subnet. Clients that are connected on a different VLAN than the one on which the Bonjour devices are connected, cannot discover these services.

![Figure 1: Bonjour Devices Running on Local Networks](image)

### 9.4.7 How Arista Supports Bonjour Gateway

Arista APs provide support for clients to automatically detect and connect to Bonjour capable devices and the services running on such devices. For the sake of understanding how the clients can connect to Bonjour capable devices over an Arista WLAN, let’s consider just two VLANs as follows:

- A service VLAN on which the Bonjour capable devices are deployed
- A client VLAN on which the clients are deployed
As shown in the figure **Bonjour Gateway Enabled on an SSID**, after a client connects to an SSID that has Bonjour Gateway enabled and the service VLAN configured, the AP forwards the mDNS packets from the service VLAN to the client VLAN (i.e. the VLAN ID configured in the SSID) and vice versa. The client now knows about the Bonjour services available on the WLAN and can connect to such services.

**Note:** Bonjour Gateway can be configured only if the Network type on the SSID is set to Bridged. This feature is not available for a NAT type network.

### 9.4.8 Configure Bonjour Gateway

You can configure Apple's Bonjour Gateway feature that allows access to Apple devices on the network.

To configure Bonjour Gateway:

1. Go to **Configure > SSID > Access Control**.
2. Select **Bonjour Gateway**.

   ![Diagram of Bonjour Gateway](image)

   **Figure 2: Bonjour Gateway Enabled on an SSID**

   As shown in the figure **Bonjour Gateway Enabled on an SSID**, after a client connects to an SSID that has Bonjour Gateway enabled and the service VLAN configured, the AP forwards the mDNS packets from the service VLAN to the client VLAN (i.e. the VLAN ID configured in the SSID) and vice versa. The client now knows about the Bonjour services available on the WLAN and can connect to such services.

   **Note:** Bonjour Gateway does not work when the Network is set to **NAT** mode. If you have set the Network to NAT mode, CloudVision WiFi grays out Bonjour Gateway and prompts you to change the Network setting from within the Access Control tab.

3. Enter the **Service VLANs**.
   
   These are the VLANs with the Bonjour devices. The AP forwards packets from the service VLAN to the client VLAN (i.e. the VLAN ID configured in the SSID) and vice versa.
4. Click **Save** or **Save & Turn SSID On**.

   If you select **Save & Turn SSID On**, see **Turn an SSID On** for details.

   If you are adding a new SSID, an "SSID created successfully" message appears. If you are updating an SSID, an "SSID updated successfully" message appears.

### 9.4.9 Configure Redirection in SSID Access Control

You can redirect clients of the SSID to a URL of your choice.

To configure Redirection:
1. Go to Configure > SSID > Access Control.
2. Select Redirection
   Options for the redirection mechanism appear.
3. Select whether you want to redirect Smartphones / Tablets only or All Clients.
4. Enter the Redirect URL.
5. Select HTTPS Redirection if you wish to move to secure version of HTTP.
   Enabling HTTPS Redirection enables three fields, these three fields provide the information of the customer using the certificate.
   • Common Name: Identifies the host name associated with the certificate.
   • Organization: Name of an organization.
   • Organization Unit: Name of an organizational unit.
6. Enter the list of Walled Garden sites.
   The user can access these sites before login.
   
   Note: You must enter at least the Redirect URL in the Walled Garden field, since the user must be able to access that URL before login.
7. Click Save or Save & Turn SSID On.
   If you select Save & Turn SSID On, see Turn an SSID On for details.

If you are adding a new SSID, an “SSID created successfully” message appears. If you are updating an SSID, an “SSID updated successfully” message appears.

9.4.10  What is a Walled Garden?

Let's understand the concept of a “walled garden” and its typical applications within Arista WiFi. A walled garden allows WiFi providers to control which destinations users can or cannot access on a wireless network.

Walled garden functionality is used in conjunction with Arista’s captive portal. The captive portal function serves as a vehicle to interact with users when they log into WiFi network.

When a captive portal is enabled on an SSID, a splash page is presented to the users before allowing them WiFi access. The splash page serves as a gatekeeper for allowing WiFi access and facilitates user interactions such as:

• Asking the user to accept terms and conditions
• Facilitating user authentication using a web-based login and password screen
• Facilitating logins using social WiFi credentials

Sometimes it is necessary to bypass the gatekeeping function of the splash page and this bypass function is facilitated by the walled garden. By defining specific destinations inside the walled garden, it is possible to bypass the splash page allowing a user to access those specified destinations directly. See Figure Splash Page and Walled Garden.
9.4.11 How the Client MAC Allow and Deny Lists Work

You can define either an Allow list or a Deny list of client MAC addresses on a per SSID basis. It's basically an Access Control List for an SSID – you get to decide which devices can or cannot connect to an SSID. For example, you might want to allow only employees on the Corporate SSID. You could then create an Allow list of MAC addresses that can connect to the Corporate SSID. Conversely, you might want to restrict some clients from connecting to an SSID. You could then create a Deny list of client MAC addresses for that SSID to prevent those clients from connecting to the SSID. Below are the definitions of Allow and Deny lists.

Allow list: Only clients in the Allow list can connect to the SSID. No other clients are allowed.

Deny list: Clients in the Deny list cannot connect to the SSID. All other clients are allowed.

9.4.12 Requirements for Allow Deny Lists of Client MAC Addresses

Allow and Deny lists need to meet the following requirements:

- For a given SSID, you can create either an Allow list or a Deny list, but not both
- Per SSID Allow list or a Deny list works only for 802.11ac and higher Arista devices
- For each SSID, you can add a maximum of 1024 clients to its Allow list or Deny list

9.4.13 Google Integration for Client Device Authorization

Google provides App sets for enterprises (Google for Work) and educational institutions (Google for Education). These enable users to communicate and collaborate from a single platform. From network administrators’ perspective, key functions provided by Google are User and Device Management, and Organizational Units. Network administrators can create an organizational structure and control which settings and policies must be applied to users and devices. User directory offers SSO for all Google applications, while device management enables administrators to authorize devices that can access the network and restrict access based on the user role. Once a user logs in with his official Google credentials, the device MAC is listed on the Google Device Management page. The administrator can then authorize or reject the device when it attempts to connect to the network.
9.4.14 Configure Client Authentication

You can configure client authentication using either Google Integration or RADIUS MAC Authentication.

To configure client authentication:

1. Go to Configure > SSID > Access Control.
2. Select Client Authentication
   - Options for Google Integration or RADIUS MAC Authentication appear.
3. Select either Google Integration or RADIUS MAC Authentication
   - If you select Google Integration, then select what happens If Client Authentication Fails:
     - Select Disconnect to disconnect the client if authentication fails.
     - Select Stay Connected and Apply Role and select the role you want to assign to the client if authentication fails. If you want to define a role, click Add / Edit. A right-panel window appears where you can configure the Role Profile and continue with Client Authentication. See Configure a Role Profile.
   - If you select RADIUS MAC Authentication, RADIUS Settings appear.
   - Note: RADIUS MAC Authentication is not available if you have configured 802.1X authentication in the SSID Security tab, since 802.1X already is a RADIUS-based mechanism.

The RADIUS Settings for Client Authentication are:
   - The Primary and Secondary RADIUS servers you want to use as Authentication Server and Accounting Server.
   - The Retry Parameters that control how often the AP attempts to authenticate with RADIUS.
   - The Username and the Password. For each of these fields, you can select from among the MAC address formats in the list.
   - The Called Station / NAS ID, IDs that the AP or a Network Access Server (NAS) send the RADIUS server.
   - Note: No two SSIDs on the same AP should use the same NAS ID.

Select what happens If Client Authentication Fails:
   - Select Disconnect to disconnect the client if authentication fails.
   - Select Stay Connected and Apply Role and select the role you want to assign to the client if authentication fails. If you want to define a role, click Add / Edit. A right-pane window appears where you can configure the Role Profile and continue with Client Authentication.
4. Click Save or Save & Turn SSID On.
   - If you select Save & Turn SSID On, see Turn an SSID On for details.

If you are adding a new SSID, an “SSID created successfully” message appears. If you are updating an SSID, an “SSID updated successfully” message appears.

9.4.15 Configure Role Based Control

You can assign role profiles to users connecting to the SSID based on the Google Integration or RADIUS rules you define here in Role Based Control.

- To implement Role Based Control using Google, you must enable Google Integration.
- To implement Role Based Control using RADIUS, you must enable 802.1x.

You don’t have to leave the SSID Access Control tab to configure Google or RADIUS. Just click Change Settings? under Role Based Control. CloudVision WiFi opens a right-pane window, allowing you to configure and save the relevant settings and continue with Role Based Control.

To configure Role Based Control:
1. Select **Role Based Control**.
   - Select **RADIUS VSA** to assign roles based on rules for the RADIUS server.
     - Select the **Rule Type**. This could be either **Arista-Role RADIUS VSA** or **Custom RADIUS attributes VSA**.
     - Enter the **Vendor ID** and **Attribute ID** if you selected **Custom RADIUS attributes VSA**. For the **Arista-Role RADIUS VSA** case, the vendor is Arista and the Vendor ID and Attribute ID are pre-defined in the RADIUS server, so you don't have to enter those values here.
     - Select the **Operand** for the string pattern that you want to use for the rule.
     - Enter the string pattern in the **Enter Value** field.
     - Select the role you want to assign for this rule in **Assign Role**. If you have not yet defined the role you want to assign, click **Add / Edit**. A right-pane window appears allowing you to define a role and continue with Role Based Control. See **Configure a Role Profile** for details.
   - Select **Google OU** to assign roles based on rules for Google OU.
     - The **Rule Type** is preset to Google OU.
     - Select the **Operand** for the string pattern that you want to use for the rule.
     - Enter the string pattern in the **Enter Value** field.
     - Select the role you want to assign for this rule in **Assign Role**. If you have not yet defined the role you want to assign, click **Add / Edit**. A right-pane window appears allowing you to define a role and continue with Role Based Control. See **Configure a Role Profile** for details.

2. Click **Save** or **Save & Turn SSID On**.
   - If you select **Save & Turn SSID On**, see **Turn an SSID On** for details.

   If you are adding a new SSID, an “SSID created successfully” message appears. If you are updating an SSID, an “SSID updated successfully” message appears.

### 9.4.16 Typical RADIUS MAC Authentication Flow

With the 8.8.1 release, you can configure RADIUS MAC Authentication in CloudVision WiFi to assign roles to clients both before and after authentication. Let’s look at a typical use case to understand how this works. Consider an SSID that uses RADIUS MAC Authentication to authenticate clients associating with it. A typical RADIUS MAC authentication workflow is shown in the figure below.

1. When the client first connects to the SSID, the WiFi access point (AP) sends an Authentication Request containing the client’s MAC address to the RADIUS server.
2. The RADIUS server notifies the AP that the client MAC is unknown. The AP then redirects the client to a login portal.
3. The user enters a username and password into the portal. The RADIUS server authenticates these credentials and registers the client MAC address against this user.
4. The RADIUS server notifies the AP of the successful authentication. The user is now connected to the network.
Typically, in such cases, subsequent attempts by this client to connect to the SSID are seamless, i.e., the RADIUS server knows its MAC address and the client is not redirected to the login portal.

Role-based control with RADIUS MAC authentication can be implemented in CloudVision WiFi using any of the following:

- Role Profiles
- Captive Portal hosted on the Arista Cloud
- Captive Portal hosted on a Third Party server

CloudVision WiFi supports integration with Forescout, ISE and ClearPass.

9.4.17 Implementation Using Role Profiles

To implement Role-based control with RADIUS MAC authentication using Role Profiles, you need to define two roles in CloudVision WiFi: a Pre-Authentication role and a Post-Authentication role. The workflow using roles is as shown in the figure below.

1. When the client first connects to the SSID, the WiFi access point (AP) sends an Authentication Request containing the client’s MAC address to the RADIUS server.
2. The RADIUS server responds with an Access-Accept message containing the Pre-Authentication role. The Pre-Authentication role redirects the client to a web authentication portal hosted on the RADIUS server.
3. The user enters a username and password into the portal. The RADIUS server authenticates these credentials and registers the client MAC address against this user.
4. The RADIUS server sends a Change of Authorization (CoA) message containing the Post-Authentication role to the AP. The AP connects the client to the network.
9.4.17.1 Configure Roles with RADIUS MAC Authentication

Let’s look at how to define the two roles in CloudVisionWiFi to implement the role-based MAC authentication workflow.

RADIUS Profile

Under Configure > WiFi > RADIUS profile, select “Add RADIUS Server” and enter the RADIUS server details as shown below.

![RADIUS Profile Configuration](image)

Pre-Authentication Role

The Pre-Authentication role profile enables redirection to the URL of the web authentication portal, as shown below.

Note: You must add the web authentication portal URL and ports 80 and 443 to the “Websites That Can Be Accessed Before Authorization” list.
This implements Step 2) from the workflow above, redirecting the client to the RADIUS server authentication portal. You need to configure the RADIUS server to return this role in the Access-Accept message it sends to the AP.
Post-Authentication Role

The Post-Authentication role profile defines the connection settings (e.g., VLAN, Firewall rules) for successfully authenticated clients as shown below.

RADIUS MAC Authentication and Role-Based Control

Note: RADIUS MAC Authentication is available only if the Security Mode is set to Open, WPA2, or Mixed mode. For WPA2 and Mixed mode, PSK must be selected. This option is not available with 802.1x.

The steps to configure RADIUS MAC Authentication and Role-Based Control are:

1. Under SSID > Access Control, enable Client Authentication > RADIUS MAC Authentication and select “Disconnect” if authentication fails. This causes the client to disconnect if authentication fails. If authentication succeeds, roles defined in the SSID are applied.
2. Next, under RADIUS Settings, select the RADIUS server you want to use.

Note: Set the Calling Station ID to %m-%s (MAC Address and SSID), and the NAS ID to “%s” (only the SSID).
3. Finally, enable Role-Based Control on the SSID and assign the two roles via the RADIUS VSA, as shown below.

Note: The VSA and its value may vary depending on the RADIUS server used.

9.5 SSID Analytics

The SSID Analytics tab contains settings to control what analytics information is stored and where. Arista APs collect, process and present useful and easy-to-understand Analytics information. You can choose to store this information on the Arista server and/or on a third-party server of your choice. Analytics information is broadly classified into Association and Application Visibility analytics.

Association

Association analytics includes information on clients that associate with the SSID. An Arista AP collects the following data:

- Client MAC address
- Protocol
- SSID of the network to which the client connects
- Location of the client in the Arista Location Hierarchy
- Start time of client association with the AP (GMT)
- End time of client association with the AP (GMT)
SSID Settings

• Start time of client association with the AP according to local time of the user
• End time of client association with the AP according to local time at the user
• Session duration
• Data transfer from client device in bytes
• Data transfer to client device in bytes
• Data rate in Kbps
• Smart device type
• Local Time Zone

If you select Association, you can also select HTTP Content analytics. Content analytics include:

• Domain name accessed by the clients
• Data transferred to the domain (in bytes)
• Data received from the domain (in bytes)

The Arista server stores the data in CSV format so you can download it as reports.

Application Visibility

Application Visibility is where the AP monitors all applications above Layer 2 for this SSID. It tells you what applications are most popular on your network. It can also help you identify unwanted or harmful applications. You can view these Applications on the Monitor tab in CloudVision WiFi either on a per-Client basis or on a per-Application basis.

Note: Application Visibility is not supported on 802.11n devices. Additionally, we recommend that you do not enable Application Visibility for C-65, C-75, W-68 and O-90 as it might adversely affect performance.

You can choose to send the analytics to a third-party server. In this case, when you select HTTP Content, you need to enter the Username and Password for the server. The Send Interval determines how often the data are sent to the server.

You can select which HTTP fields you want to send as part of the analytics. Arista APs send client MAC and RSSI data as part of the HTTP Post message. For details, see HTTP Post Format.

9.5.1 HTTP POST Format

The curl program is used to post the RSSI values to the server. The command format used is as follows:

curl <upload_URL>?sensor_mac=<sensor's MAC address>&timestamp=<time in seconds> -F data="<file_on_airtight_device>"

The post command contains two arguments:

• sensor_mac: The MAC address of the Arista device. Example 00:11:74:90:00:1F
• timestamp: The time in number of seconds from boot of the Arista device.

The contents of this post command is the upload file, which contains RSSI data of clients. The file name is rssi_data.

Each line in the file is of the following format:

<client_mac>, <RSSI in dBm>, <time in seconds at which RSSI reading was taken>

9.5.2 Configure Analytics in SSID Settings

To configure Analytics in SSID, includes two steps, one is to store analytics information on the server, and to push analytics information to third-part server.

To know more about parameters required in configuring Analytics in SSID Settings refer Analytics Parameter.
To configure Analytics in SSID Settings:

1. Navigate to **Configure > SSID**.
2. Configure settings within the **Store Analytics on This Server** tab to store analytics information on the server.
   a. Select **Association** for information about the clients that connect to or associate with the Arista APs.
      Selecting this enables **HTTP Content** field.
   b. Select **HTTP Content** to capture information about the internet domains accessed by the clients associated with the Arista APs.
   c. Select **Application Visibility** to turn ON the application visibility feature.
3. Scroll down to **Push Analytics to Third-Party Server** tab and configure the below settings to push analytics data to third-party server.
   a. Enter **Server URL** of the external server.
   b. Enter **Username** to log in to external server.
   c. Enter **Password** for the user to log in to external server.
   d. Enter **Send Interval** in minutes.
4. Select **HTTP Content** information like **Post Request Body**, **User Agent**, **Referer** that you would like to share with the third party server.
5. Click **Save**.

If the configuration is correct and saved successfully, CloudVision WiFi displays a success message.

### 9.5.3 Analytics Parameter

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Store Analytics on This Server</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Application Visibility</strong></td>
<td>This check box turns ON the application visibility feature. If you enable Application Visibility for a selected SSID, then a list of all applications above layer 2 for the selected SSID will be displayed in the Monitoring &gt; Applications tile. Note: We recommend not to enable Application Visibility feature for C-65, C-75, W68, and O-90. If you enable Application Visibility for these models, then it may impact the AP performance. Application Visibility feature is not supported on 802.11n and older devices.</td>
</tr>
<tr>
<td>Fields</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Association     | This check box, if enabled presents information about the clients that connect to or associate with the Arista APs. You can choose to collect analytics data for reporting purpose about the client-AP association. Association analytics and content analytics can be collected if you enable the collection of these analytics in the Wi-Fi profile. Association Analytics comprises the data related to the client - AP communication. The following data is collected as association analytics:  
  • Client MAC address  
  • Protocol  
  • SSID of the network to which the client connects  
  • Location of the client  
  • Start time of client association with the AP (GMT)  
  • End time of client association with the AP (GMT)  
  • Start time of client association with the AP according to local time of the user  
  • End time of client association with the AP according to local time at the user  
  • Session duration  
  • Data transfer from client device in bytes  
  • Data transfer to client device in bytes  
  • Data rate in Kbps  
  • Smart device type  
  • Local Time Zone  
| HTTP Content    | This check box captures information about the internet domains accessed by the clients associated with the Arista APs. This information is present in the association analytics file. The following information is present for each internet domain as content analytics information:  
  • Domain name  
  • Data transferred to the domain (in bytes)  
  • Data received from the domain (in bytes)  
| Push Analytics to Third-Party Server | URL of the external server where the information is to be stored.  
Username                      | Username to log in to external server.  
Password | Password for the user to log in to external server.
### Fields

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send Interval</td>
<td>Recurrent time interval, in minutes, after which the HTTP content analytics JSON file must be sent to the external server. Value can vary from [1 - 60] mins, default value is 10 mins.</td>
</tr>
</tbody>
</table>

**HTTP Fields**

<table>
<thead>
<tr>
<th>HTTP Content</th>
<th>Arista AP supports the transfer of client HTTP content analytics or browsing data from clients over HTTP or HTTPS to an external server where this information can be stored. If this feature is enabled then user has to configure below options.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Post Request Body</td>
<td>If checked then include the POST method request body in the JSON file.</td>
</tr>
<tr>
<td>User Agent</td>
<td>If checked then include the user agent (browser) in the JSON file.</td>
</tr>
<tr>
<td>Referer</td>
<td>If checked then include the HTTP referrer in the JSON file.</td>
</tr>
</tbody>
</table>

### 9.6 SSID Captive Portal

A Captive Portal is a page that appears when a user attempts to access the SSID. This could be a Facebook login enabled page for a public WiFi network, a simple Terms-of-Use page for a Guest SSID on a corporate network, or a custom-branded page for a coffee shop chain. The Captive Portal tab in CloudVision WiFi is designed so that you can configure all portal related settings for your SSID (social media plugins, splash page, etc.) from this tab.

The captive portal can reside on the Arista AP, on Arista Cloud or on a third-party server. The **AP Hosted** portal is the simplest case. It is simply a clickthrough splash page, typically asking a user to accept some terms of use. You can upload a splash page bundle, which is a " .zip" file containing components of the splash page. A Download Sample can help you with creating your own bundle.

A **Cloud Hosted** captive portal is one that resides on Arista Cloud. You can do a lot with this option, authenticating users via a wide variety of methods — called plugins — and defining Quality of Service (QoS) settings for each authentication method. When you click **Select login method for guest Wi-Fi users**, a right-panel window opens up allowing you to choose plugins and define the QoS settings for each of them. QoS Settings include login and blackout timeouts, and download and upload bandwidth limits. Below are the plugins through which users can access Arista Cloud hosted captive portal:

- **Click-Through**: This is basically no authentication, only a Welcome or Terms-of-Use type page on which the user can click and access WiFi.
- **Social Media Plug-Ins**: Users authenticate using their social media login credentials to access the WiFi. For details, see Access WiFi Using Social Media Plug-ins. Arista supports the following social media plugins: Facebook, Twitter, LinkedIn, Foursquare, Instagram, and Google+.
- **Username and Password**: There are two options within this method:
  - You can **Allow Guest Users to Self-Register**. Self-Registration can be for Free WiFi, Paid WiFi, a combination of the two, or with Host Approval. For the **Free** case, there are options to allow guest users to set their own passwords or to auto-login, to enable "Forgot Password" links, and to activate expired accounts. For the **Paid** case, Arista uses the Stripe Payment Gateway. You can define tiers of payment. So, you can charge different amounts for different session durations — say, $1 for an hour and $3 for 2 hours. The access time must be consumed as soon as it is purchased. So, if a guest user purchases 1 hour of access for $1, the session will expire after exactly 1 hour of purchase, irrespective of how much session time the guest actually
consumes. Even if the user explicitly logs off, the session continues to be billed. The Free + Paid case is a mixed mode - in addition to combining options from both cases, it allows you to keep the WiFi free for some time and then start charging. For example, many airports offer free WiFi for the first half an hour and charge users after that. Host Approval is for enterprise setups, where you want to authorize the guest WiFi access. The host, whom the guest has come to visit in the enterprise, can be the authorizer. Host-approved WiFi access ensures that only authorized users can access the WLAN network. To understand how host-approved guest access works, see Guest WiFi Authentication with Host Approval.

- **Admin Generated Credentials** uses the Guestbook method. This is where you maintain a private guestbook and allow guest users to log in and access WiFi with guest user account credentials that you have defined. The guestbook can include other user-specific information. When you enable this in CloudVision WiFi, it opens up in a new tab once you save the SSID.

- **Passcode through SMS**: Users provide their mobile number to receive an authentication code via SMS. They use this code to authenticate and access the WiFi. You can define settings related to the passcode (such as maximum length) and to the SMS (such as maximum number of times the SMS is resent).

- **Web Form**: This is an enhanced form of clickthrough. There is no authentication. To access WiFi, users fill out specific information such as their name, e-mail address, and contact number.

- **External RADIUS**: Authentication happens via an external RADIUS server. You can select a RADIUS server from the ones you have added, or add a new one using the Add / Edit option. CloudVision WiFi allows you to add and save the new RADIUS server and return to the portal settings.

**Note:** You cannot use the RADIUS plugin with any other plugins. If you select External RADIUS, CloudVision WiFi automatically disables the other plugins.

### Important Notes on Payment Gateway

If you use the Paid or the Free + Paid option, you're using a payment gateway. There are a few important things to keep in mind when using a payment gateway:

- Some scripts from the payment gateway do not load in Android native web view (i.e. the native browser that Android uses). To avoid this, you must add ssl.gstatic.com to the Walled Garden list of the captive portal. If you don't add this entry to the Walled Garden, the user sees an error message saying that the page could not be loaded and asking them to use a different browser.

- For best WiFi user experience, we recommend that you add the general sites mentioned in Walled Garden Sites for Captive Portal to the Walled Garden list of the captive portal. The reason for this is that when a user attempts to access a WiFi connection, some operating systems (e.g. iOS) try to reach some sites — let's call them "test sites" — to detect if the user is behind a captive portal. If they're unable to reach the "test sites", these operating systems conclude that the user is behind a captive portal and open the splash page using an "in-app" browser. This could cause problems because, in conventional browsers, the page containing the usage time and the logout option opens in a separate tab from the splash page. Thus, with an "in-app" browser, users could end up not being able to see the usage and logout page at all. While users are sent reminders to logout once they close their sessions, they could miss these messages or attend to them after a while. This means that users could get billed for time they haven't spent using the WiFi. To avoid such problems, it's best to add those "test sites" to your Walled Garden so that users can access the time and logout tab as well.

- Currently, you can define only time limits on the payment gateway. You cannot define bandwidth or data limits; usage evaluation based on either bandwidth or data volume is not supported.

- You can define amounts with up to 2 decimal points (e.g. $1.35).

**Note:** The QoS settings you configure for the plugins override those in the SSID > Access Control tab.

Apart from the plugins, you can configure Common Settings such as e-mail, SMS and payment gateway accounts used to communicate with your WiFi users. Common settings are applicable not only across plugins within an SSID captive portal, but also across SSIDs and across locations. So if
you define a new location and an SSID at that location, the common settings apply there as well. This means that WiFi users of an organization see the same e-mail and use the same SMS account, no matter what location they're at.

You can use a combination of plug-ins on your captive portal. For example, you can use all the social media plugins to provide guests with the option of using any social media account of their choice to authenticate and access the WiFi. Or, if you are organizing an event and want to provide WiFi access to guests, you can create a batch of guest user accounts in Guest Manager and provide the account details to the guests to access the WiFi by using these account credentials.

Another use case is to give users the option to access WiFi without any authentication. Say, you have configured the social media plug-ins on your portal. But you also want to provide WiFi access to guests who do not have a social media account or do not wish to use their social media account credentials. In this case, you can provide a link on the portal page that allows users to access the WiFi by just accepting certain Terms and Conditions. This can be done using the Clickthrough plugin.

Note: The Terms and Conditions are user-defined and not Arista specific. You can choose not to provide any Terms and Conditions.

A Third-Party Hosted captive portal resides on an external server. As such, you must enter the Splash Page URL and the Shared Secret of the server that hosts the portal. You can enable RADIUS Authentication and enter the 802.1X Settings. See 802.1X RADIUS Settings for details. With third-party hosted portal, you need to configure Advanced Portal Parameters, namely the Request and Response Attributes that the portal uses for its challenge-response based user authentication.

There are some general fields that apply to AP-hosted, Cloud Hosted and Third-Party hosted portals. For example, you can define Websites that users can access before login and some Post Login fields such as a URL the user is redirected to after login (for instance, a coupon for the 100th customer), and login and blackout times. For a third-party hosted portal, you can define a post-login Service Identifier for the user.

9.6.1 Walled Garden Sites for Captive Portal

For best results with splash pages, there are some sites you need to add to the Walled Garden list of the captive portal. Some of these sites are general, for all splash page based captive portals, while others are for specific plugins or content type.

General Sites

Add the following sites to the Walled Garden list for your captive portal:

- Host name of the Guest Manager; for example, gms.cloudwifi.com.
- akamaihd.net
- googleapis.com
- gstatic.com
- Country specific Google domain where the access point using the SSID profile is deployed. For example, if an AP deployed in France is using the SSID profile, then you must add google.co.fr to the walled garden. If the SSID profile is used by access points deployed in different geographies, then the corresponding geography-specific Google domain must be included in the walled garden.

Due to some third-party application issues, some of the plug-ins do not respond properly on Apple iOS clients. To work-around these issues, you must add the following entries in the walled garden for enabling the captive portals to function properly on Apple iOS clients:

- appleiphonecell.com
- captive.apple.com
- itools.info
- ibook.info
- airport.us
- thinkdifferent.us
Note: For an Apple iOS client, if you have a video in the splash page then add the walled garden entries. However, if there is no video in the splash page and you need Automatic Internet Detection then do not add the walled garden entries.

Site for Payment Gateway

If you use the Paid or the Free + Paid option, you’re using a payment gateway. Some scripts from the payment gateway do not load in Android native web view (i.e. the native browser that Android uses). To avoid this, you must add ssl.gstatic.com to the Walled Garden list of the captive portal. If you don’t add this entry to the Walled Garden, users see an error message saying that the page could not be loaded and asking them to use a different browser.

Sites based on Content

Based on the content type used in the splash page, add the following domains to the walled garden.

<table>
<thead>
<tr>
<th>Content Type</th>
<th>Walled Garden Entries</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vimeo</td>
<td>vimeo.com</td>
</tr>
<tr>
<td></td>
<td>vimeocdn.com</td>
</tr>
<tr>
<td></td>
<td>google-analytics.com</td>
</tr>
<tr>
<td>PollDaddy</td>
<td>polldaddy.com</td>
</tr>
<tr>
<td>YouTube</td>
<td>youtube.com</td>
</tr>
<tr>
<td></td>
<td>googlevideo.com</td>
</tr>
<tr>
<td></td>
<td>ytimg.com</td>
</tr>
<tr>
<td></td>
<td>google.com</td>
</tr>
<tr>
<td></td>
<td>googleusercontent.com (for thumbnail images)</td>
</tr>
<tr>
<td></td>
<td>lh5.googleusercontent.com (for thumbnail images)</td>
</tr>
</tbody>
</table>

9.6.2 Configure AP Hosted Captive Portal

To configure AP Hosted Captive Portal settings:

1. Navigate to CONFIGURE > SSID > Captive Portal.
2. Select the Captive Portal check box to display a portal page to be shown to the client on using the guest network.
3. Select the mode of access as AP Hosted to the internet through the captive portal.
4. Click Download Sample to download the factory default portal bundle file.
   You can download the factory default portal bundle file and use it as a template to create a custom portal bundle.
5. Click Upload Custom Splash Page Bundle to upload the bundle.

   The bundle must be a .zip file of the portal page along with any other files like images, style sheets and upload this file. The zip file must satisfy the following requirements for the portal to work correctly:

   a. The zip file should have a file with the name "index.html" at the root level (i.e., outside of any other folder). This is the main portal page. It can have other files and folders, (and folder within folders) at the root level that are referenced by the index.html file.

   b. The total unzipped size of the files in the bundle should be less than 100 KB. In case, large images or other content is to be displayed on the page, this content can be placed on an
external web server with references from the index.html file. In this case, the IP address of the external web server must be included in the list of exempt hosts (see below).

c. The index.html file must contain the following HTML tags for the portal to work correctly:
   • A form element with the exact starting tag: `<form method="POST" action="$action">
   • A submit button inside the above form element with the name "mode_login". For example: `<input type="image" name="mode_login" src="images/login.gif">`. The exact tag: `<input type="hidden" name="redirect" value="$redirect">` inside the above form element.

6. Select HTTPS Redirection if you wish to move to secure version of HTTP.

   Enabling HTTPS Redirection enables three fields, these three fields provide the information of the customer using the certificate.
   • Common Name: Identifies the host name associated with the certificate.
   • Organization: Name of an organization.
   • Organization Unit: Name of an organizational unit.

7. Enter the list of Websites that users can access before login.

8. For Post Login configuration enter details for the below fields:
   a. Specify the Redirect URL.
      The browser is redirected to this URL after the user clicks the submit button on the portal page. If left empty, the browser is redirected to the original URL accessed from the browser for which the portal page was displayed.
   b. Specify Login Timeout, in minutes, for which a wireless user can access the guest network after submitting the portal page.
      After the timeout, access to guest network is stopped and the portal page is displayed again. The user has to submit the portal page to regain access to the guest network. If the user disconnects and reconnects to the guest network before his session times out, he does not have to enter his credentials on the splash page.
   c. Specify Blackout Time, in minutes.
      This is the time for which a user is not allowed to login after his previous successful session was timed out. For example, if the session time-out is 1 hour and the blackout time is 30 minutes, a user will be timed out one hour after a successful login. Now after this point, the user will not be able to login again for 30 minutes. At the end of 30 minutes, the user can login again.
   d. Select Detect when Internet connection is down and inform guest users, if you want to check the internet connectivity and inform guest users in case of loss of Internet connectivity.

9. Click Save.

9.6.3 Configure Cloud Hosted Captive Portal

   This is the default option when you first access the SSID > Captive Portal tab. With this option, the captive portal is hosted on Arista Cloud.

   To configure Cloud Hosted captive portal:

1. Go to SSID > Captive Portal.
2. Select Captive Portal.
   The Cloud Hosted option appears by default.
3. Design the splash page.
   See Design a Splash Page for details.
4. Configure the plugins you want to use.
   The default plugin is Clickthrough. The settings are different for different plugins. For information on these settings, see:
   • Configure Clickthrough Plugin
   • Configure Social Media Plugins
   • Configure Username Password Plugin
SSID Settings

- Configure Passcode Through SMS Plugin
- Configure Webform Plugin
- Configure External RADIUS Plugin

5. Select Skip Splash Page and the Duration in days, if you want to skip presenting the splash page to the user for that duration.

6. Select HTTPS Redirection if you wish to move to secure version of HTTP.
   
   Enabling HTTPS Redirection enables Certificate Information section. This section provides the information of the customer using the certificate.

7. Enter the valid information for the below fields from Certificate Information section.
   
   - Common Name: Identifies the host name associated with the certificate.
   - Organization: Name of an organization.
   - Organization Unit: Name of an organizational unit.

8. Enter the Websites that users can access before login.
   
   This is the Walled Garden of sites that you're allowing the user to access before login. For best results with captive portal, we recommend that you add some sites to the walled garden. See Walled Garden Sites for Captive Portal.

9. Configure the Post Login parameters.
   
   These include:
   
   - Redirect URL to which you want to redirect the user.
   - Login Timeout after which the user's login expires.
   - Blackout Time which is the time period for which a user cannot log in to the portal after the last successful login has timed out.

10. Select if you want the AP to detect when the internet is down and inform users.

11. Click Save to save the SSID or Save & Turn SSID On to save and turn it on.

9.6.4 Guest Wi-Fi User Authentication with Host Approval

An overview of how the user will gain access to Wi-Fi using the guestbook plugin with host approval is described as follows:

1. The guest user connects to the SSID and is redirected to a splash page. The guest user registers on the splash page by providing his contact information and the email address of the host. The guest user account information is stored in the guestbook of the portal.
2. The user is shown a message that the request has been sent for approval.

3. The host receives an email for the registration performed by the guest user.

A sample email is displayed as follows:
4. Once the host clicks Approve in the email, the guest user will receive an approval message. If the approval is granted within 5 minutes from the time of request, the guest user can access Wi-Fi without logging in again. The login page is displayed as follows:

The guest user is automatically logged in after clicking **Continue**.

5. If the request approval is granted after 5 minutes, the guest user must explicitly log in using the provided username and password. The guest user must click **Click Here to Login** to authenticate and access Wi-Fi.

### 9.6.5 Design a Splash Page

The Cloud Hosted captive portal comes with a default splash page. You can edit this splash page. You must select **Cloud Hosted** captive portal under **SSID > Captive Portal** to edit the splash page.

To edit the splash page:

1. Click the "pen" (edit) icon on the Splash Page section.
   
   A right panel Splash Page window opens up, where you can edit the elements of your splash page.

2. Expand the **Logo** option to add your logo to the splash page.
a. Click **Upload Logo Image** and select the logo image you want to upload.
b. You can use the slider below the image to adjust the size of the logo.

3. Expand the **Background Image** option to add your background image to the splash page.
   a. Click **Upload Image** and select the background image you want to upload.

4. Expand the **Background Color** option
   a. Select the background color from the color bar on the right.
      The rectangle on the left shows shades of the color you selected.
   b. Select the exact shade of the color by clicking at a particular location on the rectangle.
   c. Set the level of **Transparency** using the slider below the color pane.
      The **rgba** values below the slider correspond to the color, shade and the transparency level you select. **RGBA** stands for Red, Green, Blue and Alpha, where Alpha is the transparency parameter (0 - fully transparent, 1 - fully opaque).

5. Expand the **Terms of Use** option to define the terms of use.
   a. Enter the **Title** for the terms of use.
   b. Enter the **Body** of text for the terms of use.

6. Expand the **Privacy Policy** option.
   a. Enter the **Title** of the privacy policy.
   b. Enter the **Body** of the privacy policy.

7. Expand the **Text** option.
   You can use this to enter your caption or welcome message (e.g. “Enjoy Free WiFi”) and your copyright info.
   a. Enter the **Plugin Title**.
      This is your caption or welcome message.
   b. Enter the **Copyright** text.

8. Click **Save**.
   You can see a preview of the splash page.

The splash page you have designed appears on the **SSID > Captive Portal** tab.

### 9.6.6 Configure Common Settings for Plugins

Common settings are system wide — they’re applicable not only across plugins within an SSID captive portal, but also across SSIDs and across locations. Common settings include settings for email, SMS and payment gateway accounts used to communicate with your WiFi users.

You must select **Cloud Hosted** captive portal under **SSID > Captive Portal** to configure common settings.

Common settings consist of the following tasks:

- Configure Email Account Settings
- Configure SMS / MMS Account Settings
- Configure Payment Gateway Settings

### 9.6.7 Configure Email Account Settings

This is the email account used to communicate with your WiFi users.

You must select **Cloud Hosted** captive portal under **SSID > Captive Portal** to configure common settings.

To configure e-mail account settings:

1. On the **SSID > Captive Portal** tab, click Select login method for guest WiFi users.
SSID Settings

The Plugins & QoS window appears on the right panel.

2. Click the "gear" icon for Common Settings
   Icons for email, SMS / MMS, payment gateway and country code appear.

3. Click the "envelope" icon for Email Account.
   The Email Account Settings appear.

4. Select the Email Service Type.
   - If you select System Email:
     - Enter the From Email ID and the From Name. These will appear in the "From" field of the email the user gets.
     - Enter the Return Email ID. This is the email ID to which the user can send a response. You can test by clicking Verify to receive a test message on the return ID.
   - If you select SMTP Configuration:
     - Enter the From Email ID and the From Name. These will appear in the "From" field of the email the user gets.
     - Enter the Return Email ID. This is the email ID to which the user can send a response.
     - Enter the SMTP Server Host name or IP address.
     - Enter the Server Port number of the SMTP server.
     - Select the Login Method for the SMTP server.
     - Enter the Login Username and the Login Password for the SMTP server.
     - Select the Connection Security type for the connection to the SMTP server.

5. You can enter a Test Account and click Send Test Email to verify that the configuration works.
   If you have configured everything right, this will send a test email with the correct parameters to the account you entered.

6. Click Save to save the configuration.

9.6.8 Configure SMS / MMS Account Settings

This is the SMS / MMS account used to communicate with your WiFi users.

You must select Cloud Hosted captive portal under SSID > Captive Portal to configure common settings.

To configure SMS / MMS account settings:

1. On the SSID > Captive Portal tab, click Select login method for guest WiFi users.
   The Plugins & QoS window appears on the right panel.

2. Click the "gear" icon for Common Settings
   Icons for email, SMS / MMS, payment gateway and country code appear.

3. Click the "message" icon for SMS / MMS Account.
   The SMS / MMS Account Settings appear.

4. Under the Account option, select an existing account or select Add New to add a new account.

5. Enter a Name for the account.

6. Select a Service Provider.
   You can select Twilio, Msg91 or a custom service provider. The configuration varies depending on your choice.
   - If you select Twilio, enter the Account SID, the Auth Token and the Twilio Number.
   - If you select Msg91, enter the Username, Password, and Sender ID, and select the SMS Route.
   - If you select Custom, enter the Service URL.

7. You can enter a Test Account number and Test SMS Settings to verify that the configuration works.
If you have configured everything right, this will send a test SMS to the number you entered.

8. Click **Save** to save the configuration.

### 9.6.9 Configure Payment Gateway Settings

This is the payment gateway used to bill users when you select Paid or Free + Paid WiFi.

You must select **Cloud Hosted** captive portal under **SSID > Captive Portal** to configure common settings.

**Note:** When using Paid or Free + Paid WiFi, we recommend that you add the general sites mentioned in **Walled Garden Sites for Captive Portal** to the Walled Garden list in the captive portal settings. This will ensure that the captive portal isn't suppressed and users are not forced into an "in-app" browser.

Arista currently supports only the Stripe payment gateway. To configure payment gateway account settings:

1. On the **SSID > Captive Portal** tab, click **Select login method for guest WiFi users**.
   
   The **Plugins & QoS** window appears on the right panel.
2. Click the "gear" icon for **Common Settings**
   
   Icons for email, SMS / MMS, payment gateway and country code appear.
3. Click the "two coins" icon for **Payment Gateway**.
   
   The **Payment Gateway Settings** appear.
4. Under the **Stripe Account** option, select an existing account or select **Add New** to add a new account.
5. **Enter a Name** for the account.
6. Open the Stripe website in a new tab and login to your Stripe account.
7. On the Stripe home page, click **API** on the left navigation menu.
   
   **Note:** If you were already logged in to Stripe, you need to logout and log back in to be able to access the API menu.
8. Copy the **Live Publishable Key** and the **Live Secret Key** from the Stripe API menu, and paste them in the respective fields in the payment gateway settings in CloudVision WiFi.
   
   See **Configure Paid WiFi Authentication in CloudVision WiFi**.
9. Click **Save** to save the configuration.
9.6.10  Configure Clickthrough Plugin
The Clickthrough plugin has no authentication, only a Welcome or Terms-of-Use type page on which the user can click and access WiFi.

You must select Cloud Hosted captive portal under SSID > Captive Portal to configure plugins.

To configure Clickthrough plugin:

1. On the SSID > Captive Portal tab, click Select login method for guest WiFi users.
   The Plugins & QoS window appears on the right panel.
2. Select Clickthrough and click the edit icon (pencil) to edit settings.
   The Clickthrough Settings appear.
3. Configure the Common Plugin Settings.
4. Click Save.
   This takes you back to the Plugin & QoS page.
5. Click Save on the Plugin & QoS page to save the clickthrough settings.
6. Save the SSID.

9.6.11  Access Wi-Fi Using Social Media Plug-Ins
The figure below explains how Arista authenticates the guests using social media plug-ins.

![Figure 4: Arista Social Media Login Workflow](image)

Figure 4: Arista Social Media Login Workflow
When guests try to access the Wi-Fi through an access point (AP), the captive portal page is displayed. The portal provides options for authenticating with social media accounts. When a guest chooses a social media to authenticate, the portal redirects the user to the social media login page for his social media account credentials. The social media validates the user account credentials. If successful, the portal and the social media exchange certain information and perform a handshake. The user is requested for permission to share some of the information in his social media account with the social media App. The social media checks whether the user Likes or Follows your page on the social media and, if not, requests the user to Like or Follow your page. The AP then opens the gate for the users to access the Internet.
9.6.12 Configure Social Media Plugins

You can configure social media plug-ins on your captive portal. You must configure only the plug-ins that you have selected for your portal. Following are the social media plugins that can be configured from captive portal:

- Facebook
- Foursquare
- Google+
- Instagram
- Linkedin
- Twitter

9.6.13 Configure Facebook Plug-In

To configure the Facebook plug-in on your captive portal, you need to know App ID and App Secret of your Facebook App.

To configure the Facebook plug-in:

1. Navigate to **CONFIGURE > SSID > Captive Portal > Authentication Plugins & Quality of Service > Social**.
2. Select **Facebook**.
3. Enter **App ID** provided by Facebook to communicate with the Facebook API.
4. Enter **App Secret**. App Secret that Guest Manager uses to connect to Facebook App.
5. Select **Display Like Page** if you wish the guests must Like your Facebook page when they authenticate using their Facebook account credentials.
   If selected, a text box requesting the user to Follow the facebook page is displayed.
6. Enter **Like Page URL** of the the Facebook page that guests see and can 'Like'.
7. Select **Extended Profile Permissions** if you want to ask the guest user for permission to access additional information such as email address, birthday, likes and location.
   If selected, the user is asked for permissions to access above-mentioned information from the user profile. Select the check boxes for the information fields (**Email address**, **Birthday**, **Likes**, **Location**) that you want to request access for from the guest user.
8. Refer **Configure Common Social Media Plugin Settings** for **Quality of Service** and **Redirect URL** configuration.
9. Click **Save**.

9.6.14 Configure Twitter Plug-In

You can configure Twitter plug-ins on your captive portal. You must have the Administrator role to configure the Twitter plug-ins. Before you configure the Twitter plug-in you must ensure that you have created your application/ project in the social media.

To configure the Twitter plug-in:

1. Navigate to **CONFIGURE > SSID > Captive Portal > Authentication Plugins & Quality of Service > Social**.
2. Select **Twitter**.
3. Enter **Customer Key** provided by Twitter to communicate with the Twitter API.
4. Enter **Customer Secret**.
   Secret that Guest Manager uses to connect to Twitter.
5. Select **Display Follow Page** if you wish the guests must Follow you on Twitter when they authenticate using their Twitter account credentials.
If selected, a text box to provide Follow Page URL is enabled.

6. Enter the **Follow Page URL** for the Twitter page that the guests can see and ‘Follow’.

7. Refer **Configure Common Social Media Plugin Settings** for **Quality of Service** and **Redirect URL** configuration.

8. Click **Save**.

### 9.6.15 Configure LinkedIn Plug-In

You can configure LinkedIn plug-ins on your captive portal. You must have the Administrator role to configure the LinkedIn plug-ins. Before you configure the LinkedIn plug-in you must ensure that you have created your application/project in the social media.

To configure the LinkedIn plug-in:

1. Navigate to **CONFIGURE > SSID > Captive Portal > Authentication Plugins & Quality of Service > Social**.
2. Select **LinkedIn**.
3. Enter **App ID** provided by LinkedIn to communicate with the LinkedIn API.
4. Enter **Secret Key**.

   Secret that Guest Manager uses to connect to LinkedIn.

5. Select **Display Follow Page** if you wish the guests must Follow you on LinkedIn when they authenticate using their LinkedIn account credentials.

   If selected, a text box requesting the user to Follow the LinkedIn page is displayed.

6. Enter the **Follow Page URL** to be displayed to the guest.

7. Select **Extended Profile Permissions** if you want to ask the guest user for permission to access additional information such as Email Address.

   If selected, the user is asked for permissions to access above-mentioned information from the user profile. Select the check boxes for the information fields (**Email address**) that you want to request access for from the guest user.

8. Refer **Configure Common Social Media Plugin Settings** for **Quality of Service** and **Redirect URL** configuration.

9. Click **Save**.

### 9.6.16 Configure Foursquare Plug-In

To configure the Foursquare plug-in:

1. Navigate to **CONFIGURE > SSID > Captive Portal > Authentication Plugins & Quality of Service > Social**.
2. Select **Foursquare**.
3. Enter **Client ID** provided by Foursquare to communicate with the Foursquare application that uses OAuth 2.0 protocol to call Foursquare APIs.
4. Enter **Client Secret**.

   Secret that Guest Manager uses to connect to LinkedIn. Secret or passphrase that the portal uses to connect to and communicate securely with Foursquare.

5. Refer **Configure Common Social Media Plugin Settings** for **Quality of Service** and **Redirect URL** configuration.

6. Click **Save**.

### 9.6.17 Configure Google+ Plug-In

To configure the Google+ plug-in:
1. Navigate to **CONFIGURE > SSID > Captive Portal > Authentication Plugins & Quality of Service > Social**.
2. Select **Google+**.
3. Enter the **Client ID** provided by Google+ to communicate with the Google+ application that uses OAuth 2.0 protocol to call Google APIs.
4. Enter the **Client Secret**.
   
   Secret or passphrase that the portal uses to connect to and communicate securely with Google+.
5. Enter an **API Key** generated by Google+ for each project and is used to communicate with other APIs enabled in the project.
6. Select **Extended Profile Permissions** if you want to ask the guest user for permission to access additional information such as email address, and advanced profiles.
   
   If selected, the user is asked for permissions to access above-mentioned information from the user profile. Select the check boxes for the information fields (Email address, and Advanced Profiles) that you want to request access for from the guest user.
7. Refer [Configure Common Social Media Plugin Settings](#) for **Quality of Service** and **Redirect URL** configuration.
8. Click **Save**.

### 9.6.18 Configure Instagram Plug-In

To configure the Instagram plug-in:

1. Navigate to **CONFIGURE > SSID > Captive Portal > Authentication Plugins & Quality of Service > Social**.
2. Select **Instagram**.
3. Enter the **Client ID** provided by Instagram to communicate with the Instagram application that uses OAuth 2.0 protocol to call Instagram APIs.
4. Enter the **Client Secret**.
   
   Secret or passphrase that the portal uses to connect to and communicate securely with Instagram.
5. Refer [Configure Common Social Media Plugin Settings](#) for **Quality of Service** and **Redirect URL** configuration.
6. Click **Save**.

### 9.6.19 Configure Okta Plug-In

You must be an Administrator to configure the Okta plug-in on your captive portal. Before you configure the plug-in, ensure that you have created your application/project in the social media.

To configure the Okta plug-in:

1. Log in to CVW, and go to **CONFIGURE > WiFi > SSID**.
2. Create a new SSID or edit an existing SSID. Click the **Captive Portal** tab.
3. Click the **Captive Portal** check box and then ensure that **Cloud Hosted** is selected from the dropdown list.
4. Click **Social** in the Authentication Plugins and Quality of Service tile.
5. Select the **Okta** check box under the **Social** check box.
6. Configure the Client ID, Client Secret and Organization Domain. Use the values that you have previously noted during Okta Configuration.
7. Refer [Configure Common Social Media Plugin Settings](#) for **Quality of Service** and **Redirect URL** configuration.
8. Save the Okta configuration and then save the SSID configuration.
9.6.20 Configure QOS and Redirect Settings

Quality of Service and Redirect URL are the two common settings to be configured for every plugin.

To know more about the below configuring parameters refer QoS Settings for Plugins.

To configure Quality of Service and Redirect URL:

1. Scroll down to Quality of Service on Social Media Plugin Settings page.
2. Enter the Login Timeout.
3. Enter the Blackout Time.
4. Enter **Limit the maximum download bandwidth to**.
   - The maximum download bandwidth, in Kbps or Mbps for the guest user.
5. Enter **Limit the maximum upload bandwidth to**.
   - The maximum upload bandwidth, in Kbps or Mbps for the guest user.
6. Enter Custom URL in Redirect URL section.
   - The URL of the page to which a guest must be redirected to on successful authentication.

9.6.21 Configure Username Password Plugin

With the Username / Password plugin, you can allow users to self-register or have them use Guestbook, i.e., admin generated credentials.

You must select Cloud Hosted captive portal under SSID > Captive Portal to configure plugins.

To configure Username / Password plugin:

1. On the SSID > Captive Portal tab, click Select login method for guest WiFi users.
   - The Plugins & QoS window appears on the right panel.
2. To let users self-register, select Allow Guest Users to Self-Register.
   - The options for self-registering appear.
3. Select the option you want to use for self-registration.
   - Select **Free Wi-Fi** to allow free WiFi access to users. Click on the "gift" icon to configure the free WiFi. With free WiFi you can:
     - Allow self-registered users to set password
     - Enable Forgot Password Link
     - Allow guest users to activate expired account
     - Allow self-registered guest users to auto login
     - Show credentials to a self-registered guest user on a webpage
   - Select **Paid Wi-Fi** to have users pay for WiFi access. Click on the "$" icon to configure paid WiFi. With paid WiFi, you can do all of the things listed in free WiFi above, such as allow self-registered users to set password, enable forgot password link, etc. Additionally, you can define Payment Tiers for a payment gateway to bill users. The steps are:
     - If you have not yet configured a payment gateway, you must do so before you can proceed any further. Click Configure to set up a payment gateway. See Configure Payment Gateway Settings for details.
     - Select Currency for payment
     - Click the "+" icon to Add Tier.
     - Configure the Amount, and the access Duration for this amount.
     - Enter the Email Content you want to include as part of the paid WiFi welcome message.
     - Enter the SMS Content you want to include as part of the paid WiFi welcome message.
   - Select **Free & Paid Wi-Fi** to offer users free access for some time and then charge them. The configuration is essentially a combination of the items in the free WiFi and the paid WiFi cases.
The only additional task is that you need to define the initial period for which the WiFi is free and how often you want to renew this free period. The steps for this task are:

- Expand the Free for first option.
- Enter the Free WiFi Duration.
- Select Renew Every and enter the period after which you want to renew the free access.

Note: Some scripts from the payment gateway do not load in Android native web view (i.e. the native browser that Android uses). To avoid this, you must add ssl.gstatic.com to the Walled Garden list of the captive portal. If you don’t add this entry to the Walled Garden, the user sees an error message saying that the page could not be loaded and asking them to use a different browser.

- Select Host Approval for users to request host approval via email. To understand how this works, see Guest WiFi Authentication with Host Approval. Click on the host approval icon (person with tick mark) to configure the Host Approval Settings. For host approval settings:
  - Enter the Email domains to receive approval requests for guest access. With this you can ensure that requests are only sent to authorized domains.
  - You can define approvers by entering Approver Email Addresses.

Additionally, you can:

- Allow guest users to skip host's email on splash page
- Allow self-registered guest users to auto login
- Show credentials to a self-registered guest user on a webpage

4. To use a Guestbook to authorize logins, select Admin Generated Credentials.

Note: You can use the Guestbook icon only after you have saved the SSID.

a. Click on the Guestbook icon.

This opens a new Guest Manager tab in your browser, where you can define new guest WiFi accounts. For details on how to configure Guestbook, see the Guest Manager User Guide.

5. Click Save.

This takes you back to the Plugin & QoS page.

6. Click Save on the Plugin & QoS page to save the plugin settings.

7. Save the SSID.

9.6.22 Configure Passcode Through SMS Plugin

In this method, users provide their mobile numbers and receive a passcode for WiFi access via SMS. You must select Cloud Hosted captive portal under SSID > Captive Portal to configure plugins.

To configure Passcode through SMS plugin:

1. On the SSID > Captive Portal tab, click Select login method for guest WiFi users.

   The Plugins & QoS window appears on the right panel.

2. Select Passcode through SMS and click the edit icon (pencil) to edit settings.

   The Passcode through SMS Settings appear.

3. Select the limit for the maximum number of devices per user.

   This is the maximum number of devices that can use the same passcode to access WiFi.

4. Select the Passcode Length and the Passcode Validity.

   The passcode will expire after the validity time interval elapses.

5. Select the parameters for re-sending the SMS: the limit for the maximum number of times you want the SMS to be re-sent, and the minimum time interval that must elapse before an SMS is re-sent.

6. Enter the text to be sent to guest users in the SMS.

7. Configure the Quality of Service settings and the Redirect URL. See Common Plugin Settings.
8. Click Save. This takes you back to the Plugin & QoS page.
9. Click Save on the Plugin & QoS page to save the clickthrough settings, and then save the SSID.

9.6.23 Configure Webform Plugin
This is an enhanced form of clickthrough. There is no authentication but users fill out their details such as name, email, and contact number.

You must select Cloud Hosted captive portal under SSID > Captive Portal to configure plugins.

To configure Webform plugin:
1. On the SSID > Captive Portal tab, click Select login method for guest WiFi users.
The Plugins & QoS window appears on the right panel.
2. Select Webform and click the edit icon (pencil) to edit settings.
The Webform Settings appear.
3. For each Field (e.g. First Name), select whether you want to Display the field on the webform and whether you want the field to be Mandatory.
4. Configure the Common Plugin Settings.
5. Click Save.
This takes you back to the Plugin & QoS page.
6. Click Save on the Plugin & QoS page to save the clickthrough settings.
7. Save the SSID.

9.6.24 Configure External RADIUS Plugin
In this method, authentication happens via an external RADIUS server.

You must select Cloud Hosted captive portal under SSID > Captive Portal to configure plugins.

Note: You cannot use the RADIUS plugin with any other plugins. If you select External RADIUS, CloudVision WiFi automatically disables the other plugins.

To configure external RADIUS plugin:
1. On the SSID > Captive Portal tab, click Select login method for guest WiFi users.
The Plugins & QoS window appears on the right panel.
2. Select External RADIUS
The 802.1X Settings appear. For an explanation of these settings, see 802.1X or RADIUS Settings.
3. For common plugin settings, click the edit icon (pencil).
The External RADIUS Settings window appears. For details on these settings, see Common Plugin Settings.
4. Select the Authentication Server.
If you have not yet added any RADIUS servers, you can do so by clicking Add / Edit. The RADIUS Server Settings window appears. For details on how to add a RADIUS server, see Configure RADIUS Profile.

Note: You must select at least one Primary Authentication server. Optionally, you can select a Primary Accounting server and Secondary Authentication and Accounting servers as well.
5. Select the Accounting Server.
If you have not yet added any RADIUS servers, you can do so by clicking Add / Edit. The RADIUS Server Settings window appears. For details on how to add a RADIUS server, see Configure RADIUS Profile.
6. Select the Accounting Interval.
7. Enter the Called Station and NAS ID values.
   
   Note: No two SSIDs on the same AP should use the same NAS ID.

8. Click Save.
   This takes you back to the Plugin & QoS page.

9. Click Save on the Plugin & QoS page to save the plugin settings, and then save the SSID.

### 9.6.25 QoS Settings for Plugins

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login Timeout</td>
<td>The time period after which the guest user session for the portal expires. The user must re-authenticate with his login credentials if he wants to continue using the WiFi service. &quot;0&quot; indicates that the user session does not timeout and the user must explicitly log out from the portal. A non-zero timeout configured on the plug-in takes precedence over the timeout configured on the SSID profile. The time period, can be specified in Hours, Minutes, Days, Weeks or Months.</td>
</tr>
<tr>
<td>Blackout Time</td>
<td>The time period for which a user cannot log in to the portal after the last successful login has timed out. &quot;0&quot; indicates no blackout time. The blackout time configured on the plug-in takes precedence over the blackout time configured on the SSID profile. The time period, can be specified in Hours, Minutes, Days, Weeks or Months.</td>
</tr>
<tr>
<td>Redirect URL</td>
<td>The URL of the page to which the guest user must be redirected to on successful login from the portal using the plug-in.</td>
</tr>
<tr>
<td>Max Download Bandwidth</td>
<td>Maximum download bandwidth, in Kbps or Mbps, for this plug-in on the portal.</td>
</tr>
<tr>
<td>Max Upload Bandwidth</td>
<td>Maximum upload bandwidth, in Kbps or Mbps, for this plug-in on the portal.</td>
</tr>
</tbody>
</table>

### 9.6.26 Configure Third-Party Hosted Captive Portal

To configure Third-Party Hosted Captive Portal settings:

1. Navigate to **CONFIGURE > SSID > Captive Portal**.
2. Select **Captive Portal** to display a portal page to be shown to the client on using the guest network.
3. Select the mode of access as **Third-Party Hosted**.
   
   The guest user is redirected to a portal hosted on an external server.

4. To configure basic settings within Third-Party Hosted do the following

   a. Select **With RADIUS Authentication**.
      
      The guest user is authenticated by a RADIUS server, when he logs in to the external portal.
      
      Once you select **With RADIUS Authentication** a link to configure **802.1X Settings**.

   b. To configure **802.1X Settings**, see **Configure External RADIUS Plugin**.

   c. Enter **Splash Page URL**.
      
      Using this URL wireless user will be redirected to external portal.

   d. Enter a **Shared Secret** for SSID-external portal communication.
e. Select HTTPS Redirection if you wish to move to secure version of HTTP.

Enabling HTTPS Redirection enables three fields, these three fields provide the information of
the customer using the certificate.

- Common Name: Identifies the host name associated with the certificate.
- Organization: Name of an organization.
- Organization Unit: Name of an organizational unit.

f. Enter Websites that users can access before login.

5. For Post Login configuration enter details for the below fields:

   a. Specify the Redirect URL.

      The browser is redirected to this URL after the user clicks the submit button on the portal page.
      If left empty, the browser is redirected to the original URL accessed from the browser for which
      the portal page was displayed.

   b. Specify the value of the Service Identifier.

      This is a free form parameter that can be passed to the external portal.

   c. Specify Login Timeout, in minutes, for which a wireless user can access the guest network
      after submitting the portal page.

      After the timeout, access to guest network is stopped and the portal page is displayed again.
      The user has to submit the portal page to regain access to the guest network. If the user
      disconnects and reconnects to the guest network before his session times out, he does not have
      to enter his credentials on the splash page.

   d. Specify Blackout Time, in minutes.

      This is the time for which a user is not allowed to login after his previous successful session was
      timed out. For example, if the session time-out is 1 hour and the blackout time is 30 minutes, a
      user will be timed out one hour after a successful login. Now after this point, the user will not be
      able to login again for 30 minutes. At the end of 30 minutes, the user can login again.

   e. Select the Detect when Internet connection is down and inform guest users, if you want to
      check the internet connectivity and inform guest users in case of loss of Internet connectivity.

6. To configure Advanced Portal Parameters refer Request and Response Parameters.

7. Click Save.

### 9.6.27 Request and Response Parameters

<table>
<thead>
<tr>
<th>Request Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request Type</td>
<td>Field name for request type field.</td>
</tr>
<tr>
<td>Challenge</td>
<td>Field name for random text used for authentication.</td>
</tr>
<tr>
<td>Client MAC Address</td>
<td>Field name for the MAC address of the client.</td>
</tr>
<tr>
<td>Access Point MAC Address</td>
<td>Field name for MAC address of the access point that is communicating with the external portal.</td>
</tr>
<tr>
<td>Access Point IP Address</td>
<td>Field name for the IP address of the access point that is communicating with the external portal. This should match the field name used by the external portal.</td>
</tr>
<tr>
<td>Access Point Port Number</td>
<td>Field name for the AP port number on which the AP and external server communicate.</td>
</tr>
<tr>
<td>Failure Count</td>
<td>Field name for the count of the number of failed login attempts.</td>
</tr>
<tr>
<td>Request Attributes</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Requested URL</td>
<td>Field name for the requested URL that is the URL requested by the client through the AP, to the external server.</td>
</tr>
<tr>
<td>Login URL</td>
<td>Field name for the login URL.</td>
</tr>
<tr>
<td>Logoff URL</td>
<td>Field name for the logoff URL.</td>
</tr>
<tr>
<td>Remaining Blackout Time</td>
<td>Field name for the remaining blackout time.</td>
</tr>
<tr>
<td>Service Identifier</td>
<td>Name of the portal parameter that is used to pass the service identifier value to the external portal. The service identifier value is specified in the Captive Portal section of the SSID Profile. This parameter can be used by the external portal to implement SSID profile specific functionality like different portals for different SSIDs etc.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Response Attributes</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Challenge</td>
<td>Field name for the challenge</td>
</tr>
<tr>
<td>Response Type</td>
<td>Field name for the response type.</td>
</tr>
<tr>
<td>Challenge Response</td>
<td>Field name for the challenge response.</td>
</tr>
<tr>
<td>Redirect URL</td>
<td>Field name for the redirect URL</td>
</tr>
<tr>
<td>Login Timeout</td>
<td>Field name for login timeout.</td>
</tr>
<tr>
<td>User name</td>
<td>Field name for user name.</td>
</tr>
<tr>
<td>Password</td>
<td>Field name for password.</td>
</tr>
</tbody>
</table>

### 9.7 SSID RF Optimization

The RF (Radio Frequency) Optimization tab is where you can enable RF related optimizations on the SSID.

Arista uses a Unified Client Steering approach. That is, the various client steering mechanisms work together to improve the client Quality of Experience (QoE). On the SSID RF Optimization tab, you simply enable different types of steering for this SSID. To configure the parameters related to client steering you need to go to the Radio Settings tab. The **Minimum Association RSSI** is the minimum RSSI at which a client is allowed to associate with an AP on this SSID. The value comes from the **Steering RSSI Threshold** in the common steering parameters. See Configure Common Steering Parameters.

**Enforce Steering** is enabled by default. Some clients directly send Association Request packets by listening to beacons. Enforce Steering causes an AP to reject such requests on 2.4GHz, thereby force- steering clients to 5GHz.

You can enable **802.11k Neighbor List**. This allows clients to request neighbor lists from APs, which speeds up roaming. See **802.11k Use Case** for details. When you enable 802.11k, you can select **Neighbor List Dual Band** if you want the AP to send the client neighbor information on both bands. While 802.11k defines methods that help *individual* clients understand their radio environment, 802.11v defines services that help improve overall *network* performance. See **802.11v Use Case** for details.

You can enable or disable 802.11k Neighbour List and 802.11v BSS Transition by navigating to:
Address Resolution Protocol (ARP) is an IPv4 protocol used to resolve a device’s IP address to its physical MAC address so communication can occur on the Layer 2 segment. A device sends an ARP broadcast packet containing an IP address, in effect asking who on the Layer 2 segment knows which MAC address is associated with that IP address. A client may also send an ARP broadcast that contains its own IP and MAC address to update Layer 2 device ARP tables. IPv6 doesn’t use broadcast packets, it uses a Neighbor Discovery Protocol (NDP). NDP uses multicast to resolve addresses and to find other network resources.

An AP can act as a proxy for the wireless clients associated to it. When you enable Proxy ARP and NDP, the AP itself responds to the ARP and NDP requests instead of forwarding them and transmitting them at a low, basic data rate. Downstream Group-Addressed Forwarding (DGAF) blocks all broadcast/multicast traffic from the wired to the wireless side. It is used only with Hotspot 2.0. You can disable it by selecting Disable DGAF.

When you enable Broadcast / Multicast Control, the AP blocks broadcast/multicast packets from Ethernet to wireless. This cleans up the RF airspace is by blocking unnecessary traffic. You can also block broadcast/multicast packets from wireless to Ethernet by selecting Block Wireless to Wired. Broadcast / Multicast Control should be used carefully as many network functions use broadcast packets for basic operations.

For applications that must be allowed to use broadcast / multicast packets, you can create an exemption by adding the protocol information to the Exemption List.

Bonjour is an Apple protocol designed to make Bonjour-enabled devices and services easy to use and configure over the network. Bonjour makes heavy use of broadcast and is essential for Apple products. You can select Allow Bonjour to automatically apply an exemption.

IGMP Snooping is a mechanism to prune multicast packets so that they are forwarded only to ports on which clients have subscribed. This saves bandwidth by avoiding unnecessary packet flows. For details, see IGMP Snooping.

9.7.1 802.11k - Use Case

Consider a client moving from one AP (AP1 in the figure Moving Client Scenario) towards another AP (AP2 in the figure below). The strength of the signal received from AP1 gets weaker as the client moves away from it. Without 802.11k, a client needs to scan several channels before it can determine which AP has the best signal. Clients typically scan channels at 100ms intervals looking for beacons. Assuming there are 21 channels available in the 5GHz band (with DFS), a complete scan of all available channels could take as long as 2.1 seconds. Real-time applications have strict timing requirements (one-way delay must be < 50ms for Voice over Wi-Fi (VoFi)). A complete scan could thus result in poor user experience. 802.11k provides a better alternative.
The IEEE 802.11k amendment, also called Radio Resource Measurement (RRM), defines methods allowing stations to inform each other about their respective radio frequency (RF) environments. That way, they can make faster and better informed decisions on roaming. With 802.11k, a client can request an Arista AP to send a Neighbor Report. In case of the client in the above figure, it requests a Neighbor Report from AP1. It's basically asking AP1, “Which APs are advertising my current SSID? What channels are these APs operating on? What are their signal strengths as you see them?” AP1 reports on all the APs it can sense that are advertising this SSID. Suppose there are 4 such neighbors in the 5GHz band (AP2 through AP5 in the Moving Client Scenario figure). The client then receives a Neighbor Report containing 4 candidate channels to scan. At 100ms a channel, the client can decide in under half a second which AP to move to. It no longer needs to spend 2.1 seconds scanning all available channels for target APs.

Table 4: Scan Times with and without 802.11k

<table>
<thead>
<tr>
<th>5GHz (w DFS)</th>
<th>All Channels</th>
<th>11k Neighbors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channels to scan</td>
<td>21</td>
<td>4</td>
</tr>
<tr>
<td>Scan Time</td>
<td>2.1s</td>
<td>400ms</td>
</tr>
</tbody>
</table>

The Neighbor Report from an Arista AP to a Client figure shows an example of the Neighbor Report message that an Arista AP sends its client. The report informs the client that channels 157 and 11 are available on neighboring APs. The client now needs to scan only these channels and pick the AP with the best signal as its target. This saves time and improves user experience.
9.7.2 802.11v - Use Case

Consider a client connected to an AP. The signal strength from the client could drop below a configured threshold, or the network's load balancing algorithm might decide that a different AP can serve the client better. In such situations, an AP might disassociate with the client. This can be an unexpected shock to a client, causing it to go through a complete scan before selecting an AP to associate with. This could cause poor user experience, especially for real-time applications.

The IEEE 802.11v amendment is also called Wireless Network Management (WNM). As the name suggests, 802.11v has a broader scope than 802.11k. While 802.11k defines methods that help individual clients understand their radio environment, 802.11v defines services that help improve overall network performance.

An important service is BSS Transition Management (BSTM). When an Arista AP decides to disassociate with a client, it sends an 802.11v frame called a BSTM Request. It's basically the AP warning the client, “Beware. I am going to disassociate in 60 seconds.” (The actual time interval is configurable.) This is called an Unsolicited Request. It allows a client some time to find and associate with another AP. The message includes a list of neighboring APs on the same ESS that the client can associate with. In an 802.11v message called the BSTM Response, the client can accept or reject the AP's request. It can also ask the AP for more time – the BSTM Response message includes a BSS Termination Delay field. Essentially, it’s the client saying, "60 seconds is too short. Let’s disassociate after 3 minutes". The AP honors this request.

Note that with 802.11k, only a client can request a Neighbor List. With 802.11v, however, either the client or the AP can initiate a conversation about transitioning. So, a client can send a BSTM Query asking an Arista AP, “Should I associate with a different AP? If yes, which one?” Depending on its implementation, the client may send this query periodically or based on triggers such as low signal strength. The AP responds with a BSTM Request - called a Solicited Request - containing the list of recommended APs the client can associate with.
Every time an Arista AP sends an 802.11v frame, it does not necessarily want to disassociate. It might simply want to nudge the client into looking for another AP by sending a BSTM Request with the list of neighbors but without a disassociation warning. This could happen, for instance, if a neighbor AP is less loaded and close enough. Since 802.11v has a network-wide view of things, it might recommend (but not force) the client to move to the less loaded AP. To allow this, 802.11v provides a Disassociation Imminent flag bit, which indicates whether the AP intends to disassociate with the client.

9.7.3 Configure RF Optimization in SSID Profile

To enable RF related optimizations navigate to CONFIGURE > SSID > RF Optimization.

1. Select types of steering you want to enable.
   Types of steering are:
   • Smart Client Load Balancing
   • Smart Steering
   • Min Association RSSI
   • Band Steering
     • Enforce Steering

2. You can enable 802.11k Neighbour List and 802.11v BSS Transition. By default these two standards are disabled. Enabling these standards enables few new sub fields.
   • If you enable 802.11k Neighbour List:
     • You can also optionally enable Neighbor List for Both 2.4 GHz and 5 GHz Bands.
   • If you enable 802.11v BSS Transition:
     • You must enable the Disassociation Imminent and configure it in the Disassociation Timer field. This is the time after which the client will be disconnected from the AP. The Disassociation Timer is expressed in number of beacon intervals. The range of the Disassociation Timer should be between 10 to 3000 TBTT (Target Beacon Transmission Time). Once the Disassociation Timer reaches zero, then the client can be disassociated based on the Force Disconnection setting.
     • You can select Force Disconnection to forcefully disconnect the client after the disassociation timer expires. The client will be disconnected even if it responds with a negative BSS transition response. When Force Disconnection is not selected, the AP doesn't disconnect the client (but waits for the client to disconnect on its own).

3. Select Proxy ARP and NDP.
   When you enable Proxy ARP and NDP, then the AP filters downstream ARP (IPv4) and NDP (IPv6) packets and also responds as appropriate on behalf of wireless clients to conserve wireless bandwidth. Enabling Proxy ARP and NDP enables a field that allows you to Disable DGAF.

4. Select Disable DGAF.
   If this option is enabled then AP starts proxy ARP for IPv4 and proxy NDP for IPv6. It also drops all Multicast and Broadcast packets in the transmit path. Selecting this option disables Broadcast/Multicast control and IGMP Snooping.

5. Click Save.

9.7.4 IGMP Snooping

Multicast is often used to stream video. Multicast packets need to flood the network to reach their recipients. Multicast packets are forwarded to many network segments. Video streaming packets, for example, could end up being sent to segments with no video streaming clients. These packets waste network bandwidth. The Internet Group Membership Protocol (IGMP) protocol was developed to cull such wasteful data. IGMP provides a way for a client to inform the Layer 2 device it is connected to that it wants to receive a multicast stream. A client does this by sending an IGMP Report with the
multicast address of the multicast session it wants to join. Layer 2 devices use **IGMP Snooping** to look at multicast packets and match them to a list of multicast addresses that clients have joined. IGMP and IGMP snooping are effective ways to prune multicast packets so that they are forwarded only to ports on which clients have subscribed. When you enable IGMP Snooping, the AP blocks multicast traffic from Ethernet to wireless. To receive multicast packets, a client must send an IGMP Report with the address of the multicast group it wants to join (IGMP Report - Join).

The client application is responsible for sending the IGMP Report. If the client application does not support IGMP (e.g. legacy applications), you can still enable IGMP snooping. But you need to add the multicast address that the application uses to the **IGMP Snooping Exception List**. This will allow multicast traffic for that application to flow. When you add an address to the exception list, all APs using the SSID forward all multicast packets with that address, regardless of whether a client sent an IGMP Report to join. You can add a maximum of 30 multicast addresses to the exception list.

When a client receiving multicast packets roams to another AP, the snoop table is forwarded. The client does not need to send a new IGMP Report to join. **Convert Multicast to Unicast** converts multicast packets to unicast, except for the addresses in the exception list.

**Table 2 – IGMP Snoop Table**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Default</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP Snooping</td>
<td>Enables IGMP Snooping</td>
<td>Enabled</td>
<td>-</td>
</tr>
<tr>
<td>IGMP Snooping Exception List</td>
<td>Allow multicast to be delivered without client sending an IGMP Report (Join)</td>
<td></td>
<td>30 Max</td>
</tr>
</tbody>
</table>

**Table 3 – IGMP Snooping Restrictions**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP Snooping</td>
<td>Enabled by default</td>
</tr>
<tr>
<td></td>
<td>Based on client IGMP Report (Join)</td>
</tr>
<tr>
<td></td>
<td>Enable – blocks multicast, Disable – forwards all multicast</td>
</tr>
<tr>
<td></td>
<td>Applies to multicast going from Ethernet to wireless</td>
</tr>
<tr>
<td></td>
<td>Independent of multicast/unicast conversion</td>
</tr>
<tr>
<td></td>
<td>Snoop table forwarded when client roams</td>
</tr>
<tr>
<td></td>
<td>AP does not send IGMP Query</td>
</tr>
<tr>
<td>IGMP Snoop Protected Address</td>
<td>Max 30 multicast addresses</td>
</tr>
<tr>
<td></td>
<td>Internal protected addresses</td>
</tr>
<tr>
<td></td>
<td>224.0.0.1/24 – query for all systems</td>
</tr>
<tr>
<td></td>
<td>224.0.0.22/24 – IGMP v3 addresses</td>
</tr>
<tr>
<td></td>
<td>Not converted to unicast even if <strong>Convert Multicast to Unicast</strong> is enabled.</td>
</tr>
<tr>
<td></td>
<td>All packets forwarded on match even if no client sends an IGMP Report to join</td>
</tr>
</tbody>
</table>
9.7.5 Configure IGMP Snooping in SSID Profile

IGMP is Internet Group Management Protocol (IGMP). IGMP snooping is the process of listening to IGMP network traffic. Enabling IGMP Snooping for a selected SSID blocks the multicast packets if no client joins the multicast group. Enabling the IGMP snooping does not convert the packets from multicast to unicast until you specifically enable Multicast to Unicast.

To know more about parameters required in configuring IGMP Snooping refer IGMP Snooping Parameters.

To configure IGMP Snooping:
1. Navigate to Configure > SSID.
2. Scroll down and select IGMP Snooping.
3. Enter IP address in IGMP Snooping Exception List.
4. Enter Snoop Timeout in minutes.
5. Select Convert Multicast to Unicast
   The Convert Multicast to Unicast is disabled by default. You can enable it only if IGMP Snooping is enabled. If you enable Convert Multicast to Unicast, then all the multicast packets are converted to MAC layer unicast packets after passing the snoop check.
6. Select the appropriate value for Tag Packets with Selected Priority.
7. Click Save.

9.8 SSID Traffic Shaping and QoS

You can optimize bandwidth utilization and Quality of Service (QoS) settings for this SSID on the Traffic Shaping & QoS tab.

Traffic Shaping

You can restrict the upload and download bandwidths on the SSID. Such restrictions could be really useful for Guest or student SSIDs, for example. You can also limit the number of simultaneous associations that the SSID allows.

Depending on how you've set up the SSID, the bandwidth limits could come from a source other than the Traffic Shaping parameters defined here. For example, enterprise networks often use RADIUS servers to propagate network policies across APs. Users are divided into groups and policies are applied to each group. So the Sales group might have different bandwidth limits than those of the HR group. In such cases, the bandwidth limits could come from the RADIUS server. If an AP doesn't get values from the RADIUS server, it uses values defined on the Traffic Shaping & QoS tab.

Below are the possible sources from where an SSID might get its bandwidth control values:

- From a RADIUS server being used for authentication by an external Captive Portal. This is if you have configured an external Captive Portal on this SSID and that portal uses a RADIUS server to propagate policies.
- From a Captive Portal on Arista Cloud. This is if you have configured the SSID to use a Captive Portal on Arista Cloud.
- From a RADIUS server when you have configured the SSID to use 802.1X security.
- From the values defined here, in the Traffic Shaping & QoS tab on the Arista server.

Typically, only one of the above sources will apply. For example, if you have defined an external Captive Portal on this SSID, then obviously there is no portal on the Arista Cloud for this SSID. The only possibility is that a RADIUS server or a Captive Portal does not pass bandwidth control values on to an Arista AP, in which case the values defined in Traffic Shaping & QoS apply.

You can limit the data rate for Unicast traffic between a minimum and maximum value. The Set the data rate for multicast, broadcast and management traffic to parameter sets the Basic or...
Mandatory rate of the AP. This not only controls the data rate at which broadcast / multicast packets are sent but also sets the data rate at which Beacons are sent. You must set this rate carefully. Increasing the basic rate of the AP does reduce the transmission airtime, but it also reduces the effective coverage area. This could cause problems for the client if the AP’s coverage at the client is not enough for that data rate. For example, real-time streaming of audio and video are applications that commonly use multicast packets for delivery. If clients have problems receiving multicast packets because the AP coverage is not good enough to support higher data rates, they will experience choppy audio or pixilation and screen freezing.

Select **Per User Bandwidth Control** to restrict bandwidth on a per-user basis (the bandwidth controls discussed earlier were for a per-SSID basis). The RADIUS attributes used to set per-user bandwidth control fall under vendor-specific attributes, IETF ID:26. The table below shows the mapping of Arista attributes to RADIUS attributes. The vendor ID for Arista is 16901.

**Table 5: Arista to RADIUS - Mapping of Bandwidth Control Attributes**

<table>
<thead>
<tr>
<th>Arista Attribute</th>
<th>RADIUS Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Per-user download limit</td>
<td>5</td>
</tr>
<tr>
<td>Per-user upload limit</td>
<td>6</td>
</tr>
</tbody>
</table>

**QoS**

Quality of Service determines the priorities assigned to various types of traffic. Applications such as voice over IP, video, and online games need a service guarantee. When network bandwidth is shared, defining priorities becomes a must for such applications. You must define the QoS parameters if you are using the SSID for such applications. QoS ensures that applications that need higher priority get it. The service guarantee for such applications is met by allocating adequate bandwidth based on the QoS priority.

QoS is essentially about differentiating between services. So, a QoS mechanism might classify traffic as Background, Best Effort, Video and Voice, in increasing order of priority, i.e., Background traffic has the lowest priority while Voice calls have the highest. The main QoS standards in use are:

- Type of Service (TOS) - a field in older versions of IPV4 header.
- Differentiated Services Code Point (DSCP) - the TOS field redefined for better QoS differentiation. DSCP is also specified in the IP header.
- 802.1p Class of Service - a field in the Ethernet frame
- 802.11e WiFi Multi-Media (WMM) - an 802.11 enhancement that alters MAC-layer behavior based on the traffic type

These standards differ from each other in how they classify traffic.

Select **Enforce WMM Admission Control** if you want to enforce the admission control parameters configured under **SSID Radio Settings > Advanced Radio Settings**.

**Note:** The WMM Admission Control settings configured under Radio Settings override the QoS Settings configured in the Traffic Shaping & QoS tab.

For an 802.11n AP, WMM (Wi-Fi multimedia) is mandatory. For 802.11n APs, if you don’t enable QoS, the system uses the default QoS parameters.

The default QoS settings are:

- SSID Priority is Voice.
- Priority Type is Ceiling.
- Downstream Mapping is DSCP.
- Upstream Marking is enabled and the value is 802.1p Marking.

The system applies user-configured QoS settings if you enable QoS.
With **SSID Priority**, you can select which type of traffic — Background, Best Effort, Video or Voice — you want to prioritize. There are two types of priority:

**Fixed**
Select this if you want all traffic transmitted on this SSID to have the selected priority, irrespective of the priority indicated in the 802.1p or IP header. For example, you could set all traffic to Background, in which case the SSID treats even voice and video packets as Background traffic.

**Ceiling**
Select this if you want traffic on this SSID to have priorities equal to or lower than the selected priority. For example, if you set SSID Priority to Video and **Type** to Ceiling, the SSID differentiates Background, Best Effort, and Video traffic but not Voice, since that is higher than Video. In effect, it treats Voice and Video equally.

If you select **Fixed**, CloudVision WiFi grays out the Downstream Mapping, since all traffic is marked with the selected priority and there is no downstream mapping to be done. If you select **Ceiling**, however, you can choose from among DSCP, 802.1p or TOS to map downstream traffic.

An Arista AP translates the traffic class mark from a standard (say, DSCP) to a service guarantee by mapping the downstream traffic to a WMM Access Category, since 802.11e WMM is what induces MAC-layer behavior to allocate appropriate WiFi bandwidth. So an AP extracts the priority from the selected standard (802.1p, DSCP or TOS) and maps it to the WMM Access Category, subject to a maximum of the selected SSID Priority (i.e. the Ceiling). For downstream traffic, the mapping depends on the first 3 bits (Class selector) of the DSCP value, TOS value, or 802.1p access category. The only exception is DSCP value 46 which is mapped to WMM access category 'Voice'. The table below shows downstream traffic mapping.

<table>
<thead>
<tr>
<th>DSCP / TOS / 802.1p Class of Service</th>
<th>802.11e/WMM access category</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 (Background)</td>
<td>1 (Background)</td>
</tr>
<tr>
<td>1 (Best Effort)</td>
<td>0 (Best Effort)</td>
</tr>
<tr>
<td>2 (Excellent Effort)</td>
<td>3 (Best Effort)</td>
</tr>
<tr>
<td>3 (Critical Apps)</td>
<td>4 (Video)</td>
</tr>
<tr>
<td>4 (Video)</td>
<td>5 (Video)</td>
</tr>
<tr>
<td>5 (Voice)</td>
<td>6 (Voice)</td>
</tr>
<tr>
<td>6 (Internetwork Ctrl)</td>
<td>7 (Voice)</td>
</tr>
<tr>
<td>7 (Network Ctrl)</td>
<td>7 (Voice)</td>
</tr>
</tbody>
</table>

For **Upstream Mapping**, you can enable both 802.1p and DSCP / TOS Marking, since 802.1p is an Ethernet frame field and DSCP / TOS is in the IP header. The table below shows the mapping used for upstream traffic.

<table>
<thead>
<tr>
<th>802.1p Class of Service</th>
<th>DSCP</th>
<th>802.11e/WMM Access Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>18</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>26</td>
<td>4</td>
</tr>
</tbody>
</table>
### Configure Traffic Shaping

Traffic Shaping helps in effective utilization of network bandwidth by setting an upload and download limit for the network, restricting the number of client association, band steering etc. You can opt for one or more of these ways depending on the network traffic, the applications used on the SSID, and the Arista device model in use.

To configure Traffic Shaping and QoS:

1. Navigate to Configure > SSID > Traffic Shaping and QOS.
2. You can limit the upload and/or download bandwidth on an SSID in SSID Bandwidth Control. To restrict the upload bandwidth on the SSID:
   a. Select Limit the maximum upload bandwidth on the SSID to and enter a data rate, from 0 through 1024 Kbps, to restrict the upload bandwidth for the SSID to the value specified here.
   b. Select Limit the maximum download bandwidth on the SSID to and enter a data rate, from 0 through 1024 Kbps, to restrict the download bandwidth for the SSID to the value specified here.
3. You can limit the number of clients associating with an SSID per radio. To limit the number of clients association:
   a. Select the Limit maximum number of simultaneous associations to, if you want to specify the maximum number of clients that can associate with an SSID per radio.
   b. Specify the maximum number of clients in the field below to the Limit maximum number of simultaneous associations to field.
4. You can specify the minimum and maximum data rate for the AP-client communication in Unicast Rate Control. To specify a minimum and maximum data rate:
   a. Select Limit the maximum unicast traffic data rate to and Specify the minimum data rate for communication in the field below the Limit the minimum unicast traffic data rate to field.
   b. Select Limit the maximum data rate for unicast traffic to and Specify the maximum data rate for communication in the field below the Limit the minimum unicast traffic data rate to field.
   c. Select Apply to all clients, including 802.11n and higher if you wish to apply the specified maximum data rate for unicast traffic to all clients, including those that support higher data rate 802.11 protocols.

5. Click Save.

### Configure Quality of Service (QoS)

Quality of Service determines the priorities assigned to various types of traffic. The service guarantee is imperative in case of streaming multimedia applications, for example, voice over IP, video, online games etc.

Before you configure Quality of Service settings for the SSID, refer SSID Traffic Shaping and QoS to understand the Quality of Service concept.

To configure Quality of Service (QoS):

1. Navigate to Configure > SSID > Traffic Shaping and QOS.
2. Scroll down and Select QoS to define your own QoS settings for Wi-Fi multimedia on the SSID profile.
   Selecting QoS enables parameters required for QoS settings.
3. Select **Enforce WMM Admission Control**.
   This field helps you specify whether the admission control parameters configured in the device template applied to the Arista device must be enforced for the network. The admission control parameters are configured under Radio Advanced Settings for Arista devices functioning as access points.

   **Note:** The WMM Admission Control settings configured for the radio on which the Wi-Fi profile is applied, override the QoS Settings configured in the Wi-Fi profile.

4. Select voice, video, best effort or background as the **SSID Priority** depending on your requirement.

5. Select **Priority Type** as **Fixed** or **Ceiling**.
   Priority Type is selected as **Fixed** if all traffic of this SSID has to be transmitted at the selected priority irrespective of the priority indicated in the 802.1p or IP header. Priority Type is selected as **Ceiling** if traffic of this SSID can be transmitted at priorities equal to or lower than the selected priority.

6. **Downstream mapping** option is enabled if **Priority Type** is selected as **Ceiling**. Select the appropriate Mapping Type.
   The priority is extracted from the selected field (802.1p, DSCP or TOS) and mapped to the wireless access category for the downstream traffic subject to a maximum of the selected SSID Priority. For the downstream mappings, the mapping depends on the first 3 bits (Class selector) of the DSCP value, TOS value or 802.1p access category. The only exception will be DSCP value 46 which will be mapped to WMM access category 'Voice'.

7. Select the **Upstream marking** option as per the requirement.
   The incoming wireless access category is mapped to a priority subject to a maximum of the selected SSID priority and set in the 802.1p header and the IP header as selected.

8. Click **Save**.

**9.9 SSID Scheduling**

If you want to limit the duration for which the SSID is active, you can define a schedule for the SSID.

You can also specify if an SSID is to be permanently active or valid for only a limited time duration. This could be useful if, for example, you have an event coming up for which you want to use a special Guest SSID with a different splash page. Another use case might be to restrict employee SSID use to office hours. When you enable **Select Timeslot**, CloudVision WiFi shows a calendar view of the week split into days (rows) and hours (columns). You can then go ahead and select the timeslots when you want the **SSID Turned On**.

**9.9.1 Configure SSID Scheduling**

After you create a SSID profile, by default, the profile remains active throughout until you delete it. However, you can make a SSID available or active only for a limited time period, or only for a limited number of hours during the day, by using the SSID scheduling feature.

To configure SSID Scheduling:

1. Navigate to **Configure > SSID**.
2. Click **Add New SSID**.
3. Click menu icon (three vertical dots) next to **Network** tab.
4. Select **SSID Scheduling**.

5. Select **Validity Type** as **Now to Forever** or **Custom** depending on you want to keep a SSID active throughout or for specific hours.
   - **Now to Forever** indicates that the SSID is deployed permanently. Selecting **Custom** enables From and To fields.

6. If you select **Custom** as validity type then specify start and end date in **From** and **To** fields.
   - This will deploy SSID for a limited time duration.

7. Select **Select Timeslot**.

8. Select the active timeslots for the SSID.
   - Active timeslots is the time during which the SSID is active. The minimum active time duration that you can select is 30 minutes. Click between the squares representing the time of the day (12 a.m. - 11 p.m.) to select the desired active intervals. The blue color indicates active duration and the white color indicates inactive duration.

9. Click **Save**.

### 9.10 Turn an SSID On

You need to turn an SSID on before it becomes available for access to users.

1. You can turn on a new SSID once you're done configuring it, or you can turn an existing SSID on.
   - If you are adding a new SSID, you can click **Save & Turn SSID On** after you are done configuring at least the three mandatory SSID tabs (Basic, Security and Network).
   - If you are turning an existing SSID on, just go to **Configure** and click the **OFF / ON** switch on the SSID you want to turn on.

   A **Turn SSID On** dialog window opens up.

2. Select whether you want the SSID on the 2.4GHz band, the 5GHz band or **Both** bands. and click **Turn SSID On**.
   - Some features in an SSID depend on **Background Scanning** under **CONFIGURE > Device** settings. If you have enabled any such features on the SSID, but you have not enabled background scanning, then the dialog window prompts you to do so. Click **Continue** on the
dialog window. This takes you to stage 2, where CloudVision WiFi recommends that you turn background scanning on. You can still turn the SSID on without enabling background scanning, but features in the SSID that depend on background scanning might not work properly.

The following message appears: "SSID turned on successfully. It may take some time for these changes to take effect on the access point(s)".

9.11 **Edit an SSID**

You can modify an existing SSID.

To edit an existing SSID at a location:

1. Go to **Configure**.
   This takes you to the **SSID** tab by default.

2. On the SSID you want to edit, click **Edit** (the pencil icon).
   The Basic tab opens up.

3. To modify the settings on any of the SSID tabs, simply click the tab you want to edit.
   If the tab you want to edit is not visible, click the Menu icon (three vertical dots) next to the **Network** tab to see all the SSID tabs.

4. Click **Save** to save the SSID or click **Save & Turn SSID On** to save and turn it on.
   An "SSID updated successfully" message appears.

9.12 **Delete an SSID**

You can delete an SSID from a location.

To delete an SSID at a location:

1. Go to **Configure**.
   This takes you to the **SSID** tab by default.
2. On the SSID you want to delete, click the Menu icon (three vertical dots) and select **Delete**.
   A dialog appears confirming that you want to delete the SSID.
3. Click **Delete**.
   An "SSID deleted successfully" message appears.

### 9.13 Create a Copy of an SSID

You can create a copy of an SSID at the same location or at a different one.

To create a copy of an SSID:

1. Go to **Configure**.
   This takes you to the **SSID** tab by default.
2. On the SSID you want to duplicate, click the Menu icon (three vertical dots) and select **Create a Copy**.
   A popup dialog appears, asking you if you want to create a copy the SSID in the current folder or a different one.
3. Select **Currently Selected Folder** to create a copy of the SSID in the current folder or **At a Different Folder** to create a copy of it at a different location, and click **Continue**.
   - If you chose **Currently Selected Folder**, an appropriate message appears and you can see a copied SSID in the current location.
   - **Note:** If you copy the SSID at the current location, the SSID Profile Name is different for the copied copy. For example, if you copy "ABC Corp" at the same location, then the new SSID name will be "ABC Corp" but its profile name will be "Copy of ABC Corp(1)".
   - If you chose **At a Different Folder**, the location hierarchy appears on the right pane window. Select the location where you want the SSID copied and click **Create a Copy**. An appropriate message appears.

### 9.14 Location Based VLAN Mapping

Location-based VLAN mapping takes precedence over SSID VLAN mapping. To enable location-based VLAN mapping:

1. Go to **Configure > WiFi**.
2. Click the three-dot menu and click **Location Based VLAN Mapping**.
3. Add the VLAN name, ID, and provide the location for the mapping.
4. Save the settings.
RADIUS

You can create, edit and delete RADIUS servers on the RADIUS tab.

Enterprise networks often use RADIUS (Remote Authentication Dial-In User Service) servers for Authentication, Authorization and Accounting (AAA) in the network. You can define the IP Address of the RADIUS server, the port numbers for Authentication and Accounting, and the Shared Secret between the APs at this location and the RADIUS server.

You can define multiple RADIUS profiles at a location. You can then directly invoke these RADIUS profiles in different SSID contexts by just selecting one of them. For example, if you use 802.1X Authentication in the SSID Security settings or in the SSID Captive Portal settings, you can select from among the RADIUS profiles defined here on the RADIUS tab. To take some use cases, an “Employee” SSID and a “Guest” SSID could both use the same RADIUS profile but in different contexts — employees might use WPA2-PSK with 802.1X, while guests might use a captive portal. Or, SSIDs at child “Branch” locations of an enterprise, for example, could all use the same “HQ RADIUS” profile defined at the parent HQ location.

10.1 Configure RADIUS Profile

RADIUS server configuration is location hierarchy specific. RADIUS server configuration defined at a specific location is visible at all its child locations. Whereas, vice versa is not true. RADIUS server listing is available in the card view layout. You can edit, copy and delete an existing RADIUS server from the card view layout.

To configure a RADIUS Server, follow these steps:

1. Navigate to CONFIGURE -> WIFI CONFIGURE.
2. Click the Add RADIUS Server button.
3. Specify a name for the new RADIUS server in RADIUS Server Name field.
4. Specify the server IP or hostname in IP Address/Hostname field. The maximum limit for the hostname is 200 characters.
   Note: RADIUS server configured with hostname cannot be used with captive portal.
5. Specify the port number of authenticating RADIUS server in Authentication Port field. The RADIUS server listens for authentication requests at this port number. The value can be between 1 to 65535. The default value is 1812.
6. Specify the port number of accounting RADIUS server in Accounting Port field. The value can be between 1 to 65535. The default value is 1813.
7. Specify a Shared Secret key. The primary RADIUS server and the AP identify themselves using the shared secret key.
8. Save the settings.

10.2 Edit a RADIUS Profile

Any existing RADIUS profile can be edited at the location it was created. Changes made in profile created on the parent location reflect in the inherited profile on the child location.

To know more about parameters required in editing RADIUS Settings refer RADIUS Settings Parameters.
To edit the RADIUS profile:

1. Click on the options tab (three vertical dots), of the RADIUS profile that is to be edited.
2. Select Edit.
   - If you are on the location where profile was created, then directly go to step 3.
   - If you are on the child location and the profile is a inherited profile, then choose the appropriate option.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you select GO to Parent Folder and Edit.</td>
<td>Then perform the Step 2 again and then perform step 3.</td>
</tr>
<tr>
<td>If you select Duplicate &amp; Continue.</td>
<td>Then a ready to edit duplicate profile gets created on the child location.</td>
</tr>
</tbody>
</table>

3. Make the necessary changes and click on Save.

Once the Profile is edited successfully, CloudVision WiFi displays a success message.

10.3 Create a Copy of RADIUS Server

Any existing RADIUS server can be copied to same or different locations. The process, creates an exact copy. The copied profile contains name and configured properties as that of the original profile. The copy of a server created on parent location exists on child location as well. Where as vise versa is not true.

To make a copy of the existing RADIUS server:

1. Click on the options tab (three vertical dots), of the RADIUS server that is to be duplicated.
2. Select Create a Copy.
3. Select option dependent on location where you would like to copy the RADIUS Server.

   - If you select Currently Selected Folder in the above step, then the RADIUS server gets copied in the current location.
   - If you select At a Different Folder in the above step, then select the new location from the Create a Copy window, at which the RADIUS server is to be copied.

4. Click on Copy.

Once the Profile is copied successfully, CloudVision WiFi displays a success message.

10.4 Delete a RADIUS Profile

An existing RADIUS profile and a duplicate RADIUS profile can be deleted using the delete option. The profile once deleted is removed permanently from its specific location and its child location as
well. Inherited profiles can not be deleted from the child location. Profiles can be deleted only on the location, where they were created.

Note: You cannot delete a RADIUS profile that is currently in use on an SSID. You need to disable / remove the RADIUS profile from the SSID configuration before you delete it.

To delete the RADIUS profile:

1. Click on the options tab (three vertical dots), of the RADIUS profile that is to be deleted.
2. Select Delete.
3. Perform the below location dependent actions:
   • If you are on the location where you had created the RADIUS profile, then select Delete.

   ![Delete RADIUS Profile](image)

   This action will divert you to its parent location, with an appropriate message. Once you are diverted to the parent location, perform all the above steps again.

Once the Profile is deleted successfully, CloudVision WiFi displays a success message.
Role Profile

A Role Profile defines restrictions such as VLAN, Firewalls and Bandwidth control for users to whom the role is assigned.

Role Profiles are an Arista way to implement Role Based Access Control (RBAC). RBAC enables network administrators to restrict system access to authorized users. Users are granted controlled access to network resources based on the roles assigned to them or the groups to which they belong. RBAC often involves a RADIUS server that propagates policies to the network.

You can configure these aspects - VLAN, firewall rules and bandwidth controls - in different places. For example, you can set the VLAN ID for an SSID in the SSID > Network tab, the firewall rules in the SSID > Access Control tab, and the bandwidth control values in the SSID > Traffic Shaping & QoS tab. (For information on firewall rules, see L3-4 Firewall and Application Firewall). So, what happens if you have different settings in one or more of the SSID tabs and different ones here in the Role Profile tab? The answer is that there is a well-defined precedence in which roles are assigned to users. The figure below shows this precedence.

The precedence can be summarized as:

1. RADIUS settings, if configured, always trump both Role Profile settings and SSID settings
2. Role Profile settings trump SSID settings unless you select Inherit from SSID.

One way to understand this precedence is to look at the scope of the three contenders: the RADIUS server and the Role Profile are defined at the level of a location, which could cover multiple SSIDs, while the SSID settings obviously apply only to a single SSID.

Some important things to keep in mind when configuring the Role Profile:

1. Inherit from SSID: If you select this option, you can give the SSID settings preference over the Role Profile. But remember: if these settings are defined in the RADIUS server, then those always
trump any other settings. By default, it’s always RADIUS, Role Profile, and SSID Settings in
decreasing order of precedence — this option is the only way you can modify the default behavior
by having the Role Profile inherit its settings from the SSID. You would choose to inherit the SSID
settings if you do not want to enforce an alternate setting. For example, if you have set the firewall
rules in the SSID > Access Control tab, and want the same rules to be applied to all users, then
you can select this option in the role profile and you need not configure the firewall rules in the role
profile.

**Note:** Not selecting the Inherit from SSID option has some consequences that you should
keep in mind. Suppose you don’t select the Inherit from SSID option and you don’t specify
any firewall rules. Then, because Role Profile settings trump SSID settings, no firewall rules
are applied to the user at all, even if you have defined rules in the SSID settings.

- **VLAN:** If you do not configure this setting in the Role Profile, then you must select the Inherit from SSID option, since the role must have at least one VLAN assigned. Conversely, if you do not select the Inherit from SSID, then you must select VLAN.

- **Bandwidth Control:** If you configure Bandwidth Control in the role profile, then you must select Enable per user bandwidth control in the SSID > Traffic Shaping & QoS tab.

The following table lists the precedence for each setting if a role profile is applied to a user. The
footnotes below explain what settings apply to the user’s session.

<table>
<thead>
<tr>
<th>Setting</th>
<th>SSID Profile</th>
<th>Role Profile</th>
<th>Inherit from SSID</th>
<th>Precedence</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>Yes/No 1</td>
<td>Yes</td>
<td>Yes/No</td>
<td>Role Profile</td>
</tr>
<tr>
<td>VLAN</td>
<td>Yes</td>
<td>No</td>
<td>Yes 2</td>
<td>SSID Profile</td>
</tr>
<tr>
<td>Bandwidth Control</td>
<td>Yes/No</td>
<td>Yes</td>
<td>Yes/No</td>
<td>Role Profile</td>
</tr>
<tr>
<td>Bandwidth Control</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>SSID Profile</td>
</tr>
<tr>
<td>Bandwidth Control</td>
<td>Yes</td>
<td>Yes 3</td>
<td>Yes</td>
<td>Role Profile/ SSID Profile 3</td>
</tr>
<tr>
<td>Bandwidth Control</td>
<td>Yes</td>
<td>Yes/No 4</td>
<td>No</td>
<td>Role Profile</td>
</tr>
<tr>
<td>Firewall Rules</td>
<td>Yes/No</td>
<td>Yes</td>
<td>Yes/No</td>
<td>Role Profile</td>
</tr>
<tr>
<td>Firewall Rules</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>SSID Profile</td>
</tr>
<tr>
<td>Firewall Rules</td>
<td>Yes</td>
<td>Yes 5</td>
<td>Yes</td>
<td>Role Profile/ SSID Profile 5</td>
</tr>
<tr>
<td>Firewall Rules</td>
<td>Yes</td>
<td>Yes/No 6</td>
<td>No</td>
<td>Role Profile</td>
</tr>
<tr>
<td>Redirection</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes/No</td>
<td>SSID Profile</td>
</tr>
<tr>
<td>Redirection</td>
<td>Yes 7</td>
<td>No</td>
<td>Yes</td>
<td>Role Profile</td>
</tr>
<tr>
<td>Redirection</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Role Profile</td>
</tr>
</tbody>
</table>

1. If no VLANs are configured in the SSID, the default value of 0 indicating untagged VLAN is set.
2. If you have not enabled Inherit from SSID, then you must define VLAN settings in the role profile.
3. In Bandwidth Control, you can set the upload and download bandwidth limits. If you don’t set any
   of these values in the Role Profile, then, because Inherit from SSID is “Yes”, the corresponding
   value in the SSID > Traffic Shaping & QoS settings is applied to a user’s session.
4. In Bandwidth Control, you can set the upload and download bandwidth limits. If any of these
   values are not set in the Role Profile, then, because Inherit from SSID is “No”, only values defined
   in the Role Profile are applied to the user’s session. Any corresponding values defined in the SSID
   settings are ignored.
5. In **Firewall**, you can enable and configure L3-4 and application firewall rules. If you have not configured either of the firewalls in the Role Profile tab, then, because **Inherit from SSID** is "Yes", the corresponding configuration in the SSID settings is applied to the user's session.

6. In **Firewall**, you can enable and configure L3-4 and application firewall rules. If you have not configured either of the firewalls in the Role Profile tab, then, because **Inherit from SSID** is "No", only the firewall rules defined in the Role Profile are applied to the user's session. Any firewall rule defined in the SSID settings is ignored.

7. **Redirection** in Role Profile maps to Access Control or Captive Portal configuration on the SSID. You can configure either Redirection in Access Control, or Captive Portal settings in an SSID, but not both. If you do not select **Redirection** on the Role Profile tab, then, because **Inherit from SSID** is "Yes", any Redirection or Captive Portal configuration defined in the SSID settings is applied to the user's session.

### 11.1 Configure a Role Profile

A Role Profile is created to enforce Role Based Access Control on Wi-Fi users. Role Profiles defined at a specific location is visible at all its child locations. Whereas vice versa is not true. Role Profile listing is available in Card Grid View layout.

To create a Role Profile:

1. Navigate to **CONFIGURE -> Role Profile**
2. Click **Add New Role Profile**.
3. Enter the role name in **Enter Role Name** field. You can use the same role name that you have defined in your RADIUS server for ease of mapping.
4. Enter a profile name in **Enter Profile Name** field.
5. Click **Save**.

Once the Profile is configured successfully, CloudVision WiFi displays a success message.

### 11.2 Configure Inherit from SSID in Role Profile

All of the above listed configurations are also available in the SSID profile and apply to user that connect to the SSID profile. You can choose to inherit the configurations from the SSID profile for one or more of the above listed settings, if you do not want to enforce an alternate setting. For example, if you have set the firewall rules in the SSID profile and want the same to be applied to all users, then you can select this option in the role profile and need not configure the firewall rules in the role profile.

To configure Inherit from SSID:

1. Navigate to **CONFIGURE -> Role Profile**
2. Select **Inherit from SSID** to inherit the role attributes from the SSID profile.
   
   You can optionally choose to inherit the role profile settings from the SSID profile in which the role profile is added to a role based control rule.
3. Click **Save**.

If the configuration is correct and saved successfully, CloudVision WiFi displays a success message.
11.3 Configure VLAN in Role Profile

You can specify one or more VLANs that the user to whom the profile is assigned can access over the WLAN network. Any VLAN setting configured in the role profile will override the corresponding setting in the SSID profile, when the role is assigned to a Wi-Fi user.

**Important:** If you do not configure this setting in the Role Profile, then you must select the Inherit from SSID option.

<table>
<thead>
<tr>
<th>SSID Profile</th>
<th>Role Profile</th>
<th>Inherit from SSID</th>
<th>Precedence</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes / No</td>
<td>Yes</td>
<td>Yes / No</td>
<td>Role Profile</td>
<td>If no VLANs are configured in the SSID, the default value of 0 indicating untagged VLAN is set.</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>SSID Profile</td>
<td>If Inherit from SSID is not enabled in the role profile, then VLAN settings must be configured in the role profile.</td>
</tr>
</tbody>
</table>

To configure VLAN:

1. Navigate to **CONFIGURE -> Role Profile**
2. In the VLAN section, enable **VLAN**.
3. Specify a **VLAN ID** that the user can access if the role profiles is assigned to the user.
   - The VLAN ID range is between 0 to 4094. To map to untagged VLAN in switch port, enter VLAN ID = 0, irrespective of what VLAN ID is assigned to untagged VLAN in switch.
4. Click **Save**.

If the configuration is correct and saved successfully, CloudVision WiFi displays a success message.

11.4 Configure Firewall Rules in Role Profile

You can define two sets of firewall rules. The L3 firewall rules that define whether communication to a host/IP:port is allowed or disallowed using a particular protocol. The communication can be blocked/allowed to or from the client device or in both directions. The second set of firewall rules define which applications in each system-defined application category that the client device can access. The rule can be defined for allowing and disallowing such access. Additionally, you can define the default rule that must be applied on the client device if none of the defined rules are applicable. The default rule is common for L3 and application firewall.

Based on the SSID Profile and Role Profile configurations, the following table lists the precedence for Firewall Rules configuration if a role profile is applied on the user.

<table>
<thead>
<tr>
<th>SSID Profile</th>
<th>Role Profile</th>
<th>Inherit from SSID</th>
<th>Precedence</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes / No</td>
<td>Yes</td>
<td>Yes / No</td>
<td>Role Profile</td>
<td>-</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>SSID Profile</td>
<td>-</td>
</tr>
<tr>
<td>SSID Profile</td>
<td>Role Profile</td>
<td>Inherit from SSID</td>
<td>Precedence</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------</td>
<td>------------------</td>
<td>------------</td>
<td>-------</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Role Profile / SSID Profile</td>
<td>In Firewall Rule, you can enable and configure L3 and application firewall rules. If either of the firewall is not configured in the Role Profile, then the corresponding configuration in the SSID Profile is applied to the user session.</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes / No</td>
<td>No</td>
<td>Role Profile</td>
<td>In Firewall Rule, you can enable and configure L3 and application firewall rules. If either of the firewall is not configured in the Role Profile, then only the firewall rules defined in the Role Profile are applied to the user session. Any firewall rule defined in the SSID Profile is not applied to the user session.</td>
</tr>
</tbody>
</table>

To configure Firewall Rules:

1. Navigate to **CONFIGURE -> Role Profile**
2. Click **Firewall**.
   
   Enable Firewall and define the L3 firewall rules. For specifying application firewall rules, enable Application Firewall. If you enable Application Firewall, you must select Application Visibility in the SSID profile
3. Enable and define **L3 Firewall Rules**.
4. Enable and define **Application Firewall** rules.
   
   If you enable Application Firewall, you must select Application Visibility in the SSID profile.
5. In **Default Rule** section provide an **Action**.
   
   Action can be one of the following, **Allow**, **Block** and **Allow and Mark**.
6. Click **Save**.

If the configuration is correct and saved successfully, CloudVision WiFi displays a success message.
11.5 Configure User Bandwidth Control in Role Profile

Bandwidth control lets you define the limits to be applied on the upload and download bandwidth available to a user. This can range from 0 Kbps through to 1024 Mbps.

⚠️ **Important:** If you configure Bandwidth Control in the role profile then Enable per user bandwidth control must be selected in the Traffic Shaping & QoS section of the SSID Profile.

Based on the SSID Profile and Role Profile configurations, the following table lists the precedence for Bandwidth Control configuration if a role profile is applied on the user.

<table>
<thead>
<tr>
<th>SSID Profile</th>
<th>Role Profile</th>
<th>Inherit from SSID</th>
<th>Precedence</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes / No</td>
<td>Yes</td>
<td>Yes / No</td>
<td>Role Profile</td>
<td>-</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>SSID Profile</td>
<td>-</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes / No</td>
<td>No</td>
<td>Role Profile</td>
<td>In Bandwidth Control, you can set the upload and download bandwidth. If any of these values are not set it the Role Profile, then only values defined in the Role Profile are applied to the user session. Any corresponding values defined in the SSID Profile are ignored.</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Role Profile / SSID Profile</td>
<td>In Bandwidth Control, you can set the upload and download bandwidth. If any of these values are not set it the Role Profile, then the corresponding value configured in the SSID Profile is applied to the user session.</td>
</tr>
</tbody>
</table>

To configure User Bandwidth Control:

1. Navigate to **CONFIGURE -> Role Profile**
2. Scroll down to **User Bandwidth Control** tab.
3. Select **Limit the maximum upload bandwidth per user to** to set the upload limit.
4. Enter upload limit value in Kbps.
   - A value between 0 -1024 should be entered over here.
5. Select **Limit the maximum download bandwidth per user to** to set the download limit.
6. Enter download limit value in Kbps.  
   A value between 0 - 1024 should be entered over here.
7. Click Save.
   If the configuration is correct and saved successfully, CloudVision WiFi displays a success message.

11.6 Configure Redirection in Role Profile

You can specify whether a user to whom the profile is assigned must be redirected to a URL whenever the user accesses the SSID. This URL can host an informative page stating what the access the user has or does not have on the WLAN network. Additionally, you can specify sites in the Walled Garden that such a user can access. Any site that is not in the Walled Garden list will not be accessible to the user.

Based on the SSID Profile and Role Profile configurations, the following table lists the precedence for Bandwidth Control configuration if a role profile is applied on the user.

<table>
<thead>
<tr>
<th>SSID Profile</th>
<th>Role Profile</th>
<th>Inherit from SSID</th>
<th>Precedence</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes / No</td>
<td>Yes</td>
<td>Yes / No</td>
<td>Role Profile</td>
<td>-</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>SSID Profile</td>
<td>Redirection in Role Profile maps to BYOD or Captive Portal configuration on the SSID Profile. You can configure either BYOD or Captive Portal settings in an SSID Profile, not both. If Redirection is not configured and Inherit from SSID is selected in the Role Profile, then any BYOD or Captive Portal configuration defined in the SSID Profile is applied to the user session.</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Role Profile</td>
<td>-</td>
</tr>
</tbody>
</table>

To configure Redirection:

1. Navigate to CONFIGURE -> Role Profile
2. Select Redirection.
3. Enter Redirect URL.
4. Select HTTPS Redirection if you wish to move to secure version of HTTP.
   Enabling HTTPS Redirection enables three fields, these three fields provide the information of the customer using the certificate.

   • Common Name: Identifies the host name associated with the certificate.
Enter the name of website that will be accessible before login in field Websites That Can Be Accessed Before Login.

6. Click Save.

If the configuration is correct and saved successfully, CloudVision WiFi displays a success message.

11.7 Edit a Role Profile

An existing Role profile can be edited at the location it was created. Changes made in profile created on parent location reflect in the inherited profile on child location.

To edit the Role Profile:

1. Click on the options tab (three vertical dots), of the Role Profile that is to be edited.
2. Select Edit.
   - If you are at a specific location where profile was created, then directly go to step 3.
   - If you are on the child location and the profile is an inherited profile, then choose the appropriate option.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you select GO to Parent Folder and Edit.</td>
<td>Then perform the Step 2 again and then perform step 3.</td>
</tr>
<tr>
<td>If you select Duplicate &amp; Continue.</td>
<td>Then a duplicate profile gets created and then you can edit the profile on the child location by performing step 2 and then step 3 on the duplicate profile.</td>
</tr>
</tbody>
</table>

3. Make the necessary changes.
4. Click Save.

Once the Profile is edited successfully, CloudVision WiFi displays a success message.

11.8 Create a Copy of Role Profile

Any existing Role profile and an inherited profile both can be copied to same or different locations. The process, creates an exact copy of an existing Role Profile. The copy of a profile contains name and configured properties as that of the original profile. The copy of a profile created on parent location exists on child location as well. Where as vise versa is not true.

To make a copy of the existing Role profile:

1. Click on the options tab (three vertical dots), of the Role profile that is to be duplicated.
2. Select **Create a Copy**.
3. Select the option dependent on location where you would like to copy the Role Profile.

![Duplicate Role Profile](image)

- If you select **Currently Selected Folder** in the above step, then the Role profile gets copied to the current location.
- If you select **At a Different Folder** in the above step, then select the new location from the **Create a Copy** window, at which the Role profile is to be copied.

4. Click on **Copy**.

Once the Profile is copied successfully, CloudVision WiFi displays a success message.

## 11.9 Delete a Role Profile

An existing Role profile and a duplicate Role profile both can be deleted using the delete option. The profile once deleted is removed permanently from its specific location and its child location as well. Inherited profiles can not be deleted from the child location. Profiles can be deleted only on the location, where they were created.

**Note:** You cannot delete a Role Profile that is currently in use on an SSID. You need to disable / remove the Role Profile from the SSID configuration before you delete it.

To delete the Role profile:

1. Click on the options tab (three vertical dots), of the Role profile that is to be deleted.
2. Select **Delete**.
3. Perform the below location dependent actions:
   - If you are on the specific location where you had created the Role profile, then select **Delete**.

![Delete](image)
• If you are on the child location and profile to be deleted is an inherited profile then click on **Go to Parent Folder & Delete**.

This action will divert you to its parent location, with an appropriate message. Once you are diverted to the parent location, perform the step 3 again.

Once the Profile is deleted successfully, CloudVision WiFi displays a success message.
Tunnel Interface

A Tunnel Interface is used to route network traffic on an SSID to and from a single aggregation point or endpoint. For instance, a distributed enterprise can channel WiFi traffic from remote locations to the enterprise HQ for inspection, applying policies, and regulatory compliance.

CloudVision WiFi supports the following types of tunneling protocols:

- **EoGRE**: Ethernet over GRE. See EoGRE for details.
- **EoGRE over IPsec**: Ethernet over GRE over IPsec where Ethernet frames are encapsulated using GRE and then encrypted using IPsec. See EoGRE over IPsec for details.
- **VXLAN (Virtual Extensible LAN)**: Virtual Extensible LAN (VXLAN) was originally developed to overcome the limited scalability of VLANs in large network deployments such as datacenters. See VXLAN for details.

### 12.1 What is EoGRE?

The Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a variety of network layer protocols inside virtual point-to-point links over an IP internetwork. Ethernet over GRE (EoGRE) encapsulates Ethernet frames and provides the ability to set up one or more EoGRE tunnels from an access point to an aggregation device such as a router.

The packet sent by the client contains the following:

- **Inner Eth** – source: client MAC / destination: gateway MAC address.
- **Inner IP** – source: client IP / destination: IP of the destination the client is trying to reach Data.

The AP appends this packet with the following:

- **SSID VLAN (optional)** – If a VLAN ID is configured in the SSID, then it is appended to the packet.
- **GRE** – All flags set to 0; Ether-Type set to 0x6558 for native Ethernet
- **Outer IP source** – IP of the AP / IP of the tunnel end-point
- **N/W VLAN (optional)** – If a VLAN is configured for the tunnel, then it is appended to the packet.
- **Outer Eth source** – AP MAC / destination: MAC of the next hop.
12.2 What is EoGRE over IPsec?

EoGRE over IPsec is a method of providing security to the Ethernet packets traversing a GRE tunnel. GRE encapsulates the data packets, while IPsec ensures the security of such encapsulated data packets by using different encryption methods. Using IPsec, an extra layer of security is added to the GRE packets in order to protect client’s sensitive information against eavesdropping or any modification. GRE packets are secured in two phases:

Using IPsec, an extra layer of security is added to the GRE packets in order to protect client’s sensitive information against eavesdropping or any modification.

GRE packets are secured in two phases:

- **Phase I**: This phase describes different security mechanisms used to authenticate and validate the keys that are shared between the endpoints.

- **Phase II**: This phase describes different methods to encrypt the payload of the packet, to provide a high level of privacy, confidentiality, and security from spoofing or any possible threat of tampering.

**Default Cipher Combination for a Better Throughput**

Some cipher combinations consume more computing resources for data encryption. Hence, they reduce the throughput. Use the following cipher combinations in Phase 1 and Phase 2 for a better throughput:

- Aes-128-sha1-modp1024
- Aes-128-sha2_256-modp1024
- Aes-256-sha1-modp1024
- Aes-256-sha2_256-modp1024

These cipher combinations are default options on the CVW UI when you set up an IPsec tunnel.

12.3 What is VXLAN?

VXLAN was developed to overcome the limited scalability of VLANs in large network deployments, e.g., datacenter networks. VXLAN creates a virtual network on top of a physical network. The virtual network is called an “overlay” while the physical network infrastructure it runs on is called an “underlay.” Switches and routers that participate in VXLAN have a special interface called a VTEP. The VTEP provides the connection between the underlay and the overlay. The ethernet frames traveling over the VXLAN tunnel are encapsulated in IP and UDP headers at the source host and decapsulated at the destination client.

Arista switches support VXLAN to enable scalable virtualized datacenter networking. In addition, Arista WiFi access points (APs) also support VXLAN to allow tunneling of data from WiFi APs to a central aggregation point, e.g., an Arista switch. This allows enterprises to migrate their existing controller-based WiFi networks to Arista’s controller-less cloud architecture without having to change the design of their underlying campus network.
12.4 MSS Clamping

Path maximum transmission unit (MTU) is the lowest of the switch and router MTU values along a network path; it basically determines the maximum allowable size of a packet traveling along the path. Enterprise networks often tunnel WiFi traffic to a wired endpoint. When TCP sessions are tunneled, the frame size of each packet increases by 50 to 200 bytes because of headers added at each protocol layer. Because the new frame size could be larger than the tunnel MTU, packets must now either be fragmented or combined into jumbo frames. Both approaches, however, could pose problems for tunneled networks. Tunnel endpoints might not support fragmentation and reassembly—for instance, in the case of VXLAN tunnels, Arista switches do not support fragmentation and reassembly—and the underlay network might not support jumbo frames.

With the 8.8.2 release, Arista access points (APs) support maximum segment size (MSS) clamping for tunneled networks. APs clamp the MSS to a value lower than the tunnel maximum transmission unit (MTU) value, thereby ensuring that no packet flowing through the tunnel exceeds the tunnel MTU in size. When a WiFi client attempts to set up a TCP connection with an MSS larger than the tunnel MTU, the AP modifies the MSS value in the TCP Syn and Syn-Ack messages so that the packet size does not exceed the tunnel MTU. (See How an AP Calculates the MSS based on the tunnel MTU.)

12.5 Configure Tunnel Interface

A Tunnel Interface represents the tunnel through which network traffic from the configured SSIDs can be routed to a remote endpoint. Using this feature you can configure EoGRE (Ethernet over Generic Routing Encapsulation), EoGRE over IPsec (Internet Protocol security), or VXLAN (Virtual Extensible Local Area Network) tunnel.

Multiple such tunnels can be configured. The tunnel Interface configuration is location hierarchy specific. Tunnel Interface Profile defined at a specific location is visible at all its child locations.

Let's configure a VXLAN tunnel, to understand the process of creating a tunnel interface profile through CloudVision WiFi.

1. To create a network interface profile navigate to CloudVision WiFi > CONFIGURE > Tunnel Interface.
2. Configure primary endpoint as shown below:
3. You can optionally configure a secondary endpoint as shown below:
Create an SSID Profile with a valid VLAN ID (e.g. 10 as discussed above) and add the recently created Remote-vxlan-bridging network profile to it.
On successful creation of a tunnel, the Up/Down status of a tunnel can be seen on the WiFi Network Counters.
12.5.1 Configure MSS Clamping

Arista APs support both automatic and manual tunnel MTU discovery. For reasons described in the following sub-section, manual tunnel MTU discovery is the better of the two options. The steps to configure MSS Clamping in CloudVision WiFi are:

1. Go to Configure > WiFi > Tunnel Interface.
2. Select the Tunnel Type.
3. Enable MSS Clamping.
4. Select Auto or Manual under Tunnel MTU Discovery.
   For the Manual case, set the appropriate tunnel MTU value.
5. Add this tunnel interface to the SSID by selecting Tunneled under the SSID > Network tab.
12.5.2 How an AP Calculates the MSS

Suppose that the tunnel MTU (TMTU) = 1550 bytes. Depending on whether the tunnel MTU discovery was set to Auto or Manual, this is the value that the AP discovers (Auto) or the value configured on the UI (Manual).

Then, the MSS = TMTU - (TUNNEL_HDR + (IPHDR + TCPHDR))

If both the overlay and underlay traffic is IPv4,
TUNNEL_HDR = eth + ipv4 + udp + vxlan = 50 bytes
TCP + IPv4 header = (20 + 20) = 40 bytes

The new MSS value, therefore, is 1550 - (50) - (20 + 20) = 1460.
This is the value to which the AP clamps client connections.

12.6 Tunnel Interface Parameters

The table below provides information required to configure a Tunnel Interface Profile.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel Interface Name</td>
<td>Name of the tunnel interface profile.</td>
</tr>
<tr>
<td>Tunnel Type</td>
<td>Select appropriate network tunnel type: EoGRE, EoGRE over IPSec, or VXLAN.</td>
</tr>
<tr>
<td>Primary Endpoint Parameters</td>
<td></td>
</tr>
<tr>
<td>Remote Endpoint (IP/Hostname)</td>
<td>The IP address or hostname of the primary remote server or endpoint.</td>
</tr>
<tr>
<td>Local Endpoint VLAN</td>
<td>This is the VLAN ID with which the tunneled traffic is tagged. A value between 0 and 4094 should be entered here.</td>
</tr>
<tr>
<td>Secondary Endpoint Parameters</td>
<td></td>
</tr>
<tr>
<td>Enable Secondary Endpoint</td>
<td>The secondary endpoint is a remote endpoint to which the wireless traffic is diverted if the primary endpoint goes down. Select this checkbox if you want to enable a secondary endpoint.</td>
</tr>
<tr>
<td>Remote Endpoint(IP/Hostname)</td>
<td>The IP address or hostname of the secondary remote server or endpoint.</td>
</tr>
<tr>
<td>Local Endpoint VLAN</td>
<td>This is the secondary VLAN ID that the tunneled traffic is tagged with. A value between 0 and 4094 should be entered here.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Prefer Primary Endpoint</td>
<td>Select the checkbox if you want the AP to check for the availability of the primary tunnel. The traffic is bridged to the secondary endpoint if the primary endpoint fails. If this option is checked, the secondary endpoint checks for the availability of the primary endpoint and transfers control back to the primary endpoint once it is up and running.</td>
</tr>
</tbody>
</table>

**Retry Parameters** (They govern how the AP pings the remote endpoint to check for connectivity)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Probe Interval</td>
<td>The interval, in seconds, after which the AP checks connectivity with remote endpoint by sending a ping request packet. This can have a value between 10 and 3600. The interval must be a multiple of 10. It should be greater than Network Ping Timeout.</td>
</tr>
<tr>
<td>Network Ping Retry Count</td>
<td>Count of ping request packets that the AP sends to the remote endpoint. The default value is 2.</td>
</tr>
<tr>
<td>Network Ping Timeout</td>
<td>Time, in seconds, till which the AP waits for a ping reply. The default value is 10 seconds.</td>
</tr>
</tbody>
</table>

**Ethernet over GRE Parameters**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRE Primary Key</td>
<td>This is an optional setting. If configured, the same key should be used at both ends of the tunnel.</td>
</tr>
<tr>
<td>GRE Secondary Key</td>
<td>This is an optional setting. If configured, the same key should be used at both ends of the tunnel.</td>
</tr>
</tbody>
</table>

### 12.7 Configure an IPSec Tunnel

The configuration considers the Tunnel Mode with IKE Version 2 security association (SA) protocol and ESP IPSec protocol. Refer to IPSec Parameters to know more about the IPSec configuration parameters.

**Note:** If you are configuring an IPSec tunnel for the first time, then we advise you to enable the help before you start the configuration; the tooltips and context-based help will help you in the configuration.

(If you are configuring an IPSec tunnel for the first time, then we advise you to enable the help before you start the configuration; the tooltips and context-based help will help you in the configuration.)

1. Navigate to **CONFIGURE > WiFi > Tunnel Interface**.
2. Select the **Tunnel Type** as **EoGRE over IPSec**.
3. Specify the primary endpoint details such as the remote endpoint, GRE primary key, and VLAN ID.
4. Specify the secondary endpoint details so that APs can communicate with it when the primary endpoint becomes unreachable. Refer to **How the Failover Works in an IPSec Tunnel** to understand how the tunnel switches between primary and secondary. The following fields are specific to the secondary endpoint configuration:
• **Network Probe Interval**: The interval, in seconds, after which the AP checks connectivity with the remote endpoint by sending a ping request packet. You can define a value between 10 and 3600. The interval must be in multiple of 10. Also, the value must be greater than the Network Ping Timeout value.

• **Network Ping Retry Count**: Count of ping requests that the AP sends to the remote endpoint. The default value is 2.

• **Network Ping Timeout**: Time, in seconds, until which the AP waits for a ping reply. The default value is 10 seconds.

5. Click **Configure IPSec**.

6. Select the mode as **Tunnel**.

7. Enter the IP address or the hostname of the remote endpoint of the GRE tunnel.

8. Select the Virtual IP address support checkbox. On selecting this field, the remote endpoint assigns a virtual IP address for incoming packets.

9. Click **Phase 1 Parameter**. Phase I Parameter consists of IKE Settings and cipher configuration.

10. Specify the **Lifetime/IKE keepalive** value.

   • Internet Key Exchange (IKE) keepalive is the duration (in hours) for which the generated keys are active.

   • After the specified time, new keys are generated and get shared between the endpoints.

11. Select the authentication method and authentication parameters for **Local (Left)** and **Remote (Right)**. The available authentication methods are: PSK and EAP. The authentication parameters vary between PSK and EAP.

12. Select the cipher, hash algorithm, and DH group values.

   **Note**: Use one of the following combination of ciphers for the maximum throughput. If you use any other cipher combination, your throughput may decrease.

   - Aes-128-sha1-modp1024
   - Aes-128-sha2_256-modp1024
   - Aes-256-sha1-modp1024
   - Aes-256-sha2_256-modp1024

13. Click **Phase 2 Parameter**. Phase 2 Parameter has cipher configurations.

14. Specify the **Lifetime/Phase 2 keepalive** value.

15. Select **ESP** (Encapsulating Security Payloads) or **AH** (Authentication Header) protocol, and then select cipher, hash algorithm, and DH group values.

16. Specify the values for **MSS Clamping**.

17. Save the configuration.
12.8 How Failover Works in a Tunneled Network

In a global organization, most of the communication happens over a tunneled network. To maintain high availability and to report the tunnel health to Access Points (APs), you configure primary and secondary endpoints in a tunnel. AP uses the tunnel health to detect whether the tunnel is down. If the AP can’t reach the primary endpoint, it connects with the secondary endpoint and, thus, eliminates the network downtime.

APs use ICMP requests and responses to determine whether the endpoint is reachable or not. An AP that has active clients can suppress ICMP requests, if it receives encapsulated packets from the remote endpoint. If the AP doesn’t have active clients, it may not suppress ICMP requests.

When you configure the secondary endpoint in a tunnel, you can configure the following parameters:

- **Network Probe Interval** is the time duration between the ping requests. The default value is 10. So, the AP sends the ping 10 seconds apart.

- **Network Retry Count** is the number of times the AP sends the ping request if it doesn't receive the response. By default, the AP sends 2 ping requests in total. After each ping is sent, the AP waits for 10 seconds (Network Probe Interval time) and if no response is received, the AP sends the next ping.

- **Network Timeout** is the time the AP waits to switch the tunnel.

An AP uses these parameters to detect whether the remote endpoint is reachable or not. The AP sends an ICMP request at each network probe interval and waits for the ICMP response from the remote endpoint. If there is no ICMP response, the AP retries and sends another ICMP request based on the **Network Ping Retry Count** value.

If you have enabled the **Prefer Primary Endpoint** parameter during the configuration, then every time the primary endpoint is active, the AP will switch to the primary endpoint. For example, suppose that the AP could not establish a connection with the primary endpoint and, hence, it switched over to the secondary endpoint. At any point, if the primary endpoint starts functioning again and the AP can establish a connection with it, then the AP will disconnect from the secondary endpoint and switch over to the primary endpoint. Also, every time the AP restarts, it tries to establish a connection with the primary endpoint first. If the AP can’t establish the connection with the primary endpoint, it switches over to the secondary endpoint.

For example, using default values, the failover time is calculated as follows:

Consider the time as T. At time = T0, the AP sends an ICMP echo request and waits for 10 seconds. The default Network Probe Interval is 10 seconds.

At T1 = T0+10, if no response is received, the AP sends another ping. The default Network Ping count is 2. So, the AP sends two pings after T0.

At T2 = T1+10, the AP sends the second ping. If no response is received, the AP starts the Network Timeout counter.

At T3 = T2+10 (because the default Network Timeout value is 10 seconds), the AP switches the tunnel.

Note that the above calculation is applicable only after the receiver increment counter stops. So, with the default values, it takes around 35 seconds for the tunnel to failover from one endpoint to the other.
Chapter 13

Remote Access Point

The Remote Access Point (RAP) solution enables organizations to extend their Enterprise SSIDs to an Arista AP installed at a remote worker’s home office or a small branch office. The RAP solution uses industry-standard protocols to securely connect the remote AP deployed at a workplace with the enterprise data center over the public Internet.

The Network Administrators configure the APs with appropriate security and settings, and handover the APs to remote employees. Remote employees simply have to install the AP at their location and get connected to the broadcasted Enterprise SSID. All communication between the AP and the remote endpoint happens over a secure IPSec VPN tunnel. Network administrators can also delete the VPN tunnel for each remote AP when needed. For example, if a remote employee quits the organization, then network administrators can terminate the VPN tunnel for the specific remote AP so that the remote employee can no longer connect to the enterprise network.

13.1 Configure a Remote Access Point

You can configure all Wave 2 and WiFi 6 Arista access points, except C-100 and C-110, to function as a remote AP using CloudVision WiFi. First you create an IPSec VPN tunnel profile, then you add the IPSec VPN tunnel profile to an SSID, and finally deploy the SSID to the remote AP.

1. In CVW, navigate to the Configure > WiFi > Tunnel Interface and click Add Tunnel Interface Profile.
2. From the Tunnel Type dropdown list, select VPN with IPSec.
3. Provide the endpoint details for Primary and Secondary servers.
4. Click the **Use Standard Port** checkbox to use the following IKE ports for UDP:
   - Port 500, if no NAT detected
   - Port 4500, if NAT is detected between two endpoints

   If you have configured a custom port for IKE connections and want to use it, then clear the **Use Standard Port** checkbox, and specify the custom port number in the **Port** field.

5. Provide the details for IPSec Phase 1 and Phase 2 parameters.

   **Note:** For PANOS, when you configure the IKE Version 1 parameters for XAUTH authentication, you must provide only hexadecimal (hex) strings in Local (Left) Identifier. The Convert to Hex button appears when you enter any ASCII strings in the Identifier field. Click Convert to Hex to convert and add the hex strings to the Identifier field. Also, the hex string must always begin with @#. The Convert to Hex button automatically prepends the string with @#. If you use any other ASCII to Hex convertor, then ensure to prepend the hex string with @# before you add the string to the Identifier field.

   For more information on other IPSec parameters, see Configure an IPSec Tunnel and Tunnel Interface Parameters topics in the CVW User Guide.

### 13.2 Configure IPSec Credentials for Each Remote AP

**Note:** When you configure the IPSec credentials for each AP, this setting takes precedence over the IPSec credentials defined in the Tunnel profile.

The custom IPSec credential per AP provides network administrators the option to disable or break any tunnel between a remote AP and the enterprise data center. For example, when a remote employee quits an organization, network administrators can block the remote AP by changing the credentials so that the AP can no longer form the tunnel to the enterprise data center.

To configure the IPSec credentials for each AP:

1. In CVW, navigate to the **Monitor WiFi Access Points**.
2. Right-click the AP and select **Customize IPSec Credentials**.
3. Click **Customize**, and provide either PSK or XAUTH/EAP credentials.

Similarly, you can also use the following navigation to access the Customize IPSec Credentials page for each AP:

- Monitor > WIPS > Managed WiFi Devices
- Floor Plans
Chapter 14

Radio Settings

The Radio Settings tab allows you to configure settings related to the WiFi access point radios at a location.

**Note:** By default, Radio Settings applied to a location are automatically inherited by its child locations. For example, suppose there is an HQ location with two child locations: Branch 1 and Branch 2. Then a radio setting applied to HQ automatically applies to Branch 1 and Branch 2. You can, however, customize the radio settings of a child location so that they are different from those of its parent.

An Arista AP has two radios (except for tri-radio models such as the C-110 and C-130, where a third radio acts as a sensor). One of the two radios operates in the 2.4GHz band and the other one in the 5GHz band. You can configure radio settings for each of these bands using the 2.4GHz and the 5GHz tabs.

By default, an Arista AP selects its operating channel automatically when in AP mode. It picks a channel with minimum Wi-Fi interference. The AP first selects a channel when it boots. Then, it periodically looks for a better channel and changes its operating channel if necessary; you can specify this period in the Selection Interval field. So, once every Selection Interval, the AP checks if the Wi-Fi interference on the current channel has increased. If the interference has increased, then the AP looks for a channel with minimum Wi-Fi interference and starts operating on that channel.

In case of the 2.4GHz (i.e. 802.11 b/g/n) radio, you can select some or all of the available candidate channels. Similarly, for the 5GHz (i.e. 802.11 a/n/ac) radio, you can select some or all of the available DFS channels and/or non-DFS channels as candidate channels. DFS stands for dynamic frequency selection. It is a mechanism using which interference by RADAR signals in 5GHz is prevented. The available candidate channels depend on the country selected.

**Note:** If channel 14 is available as a candidate channel, and it is the only channel selected, we recommended you use the manual option and then select this channel. Channel 14 does not work with auto mode when it is the only candidate channel selected.

An Arista AP can steer a client to a different band or to another Arista AP. The **Client Steering Common Parameters** link at the bottom of the screen allows you to configure parameters common to both radios and to the different types of client steering. With these common settings, the different types of client steering work together towards the common goal of improving client Quality of Experience (QoE). For example, Smart Steering and Band Steering use the Common RSSI threshold as their reference. See **What is Unified Client Steering** for details.

**Advanced Radio Settings**

Under Advanced Radio Settings, you can configure transmit power, client steering and load balancing parameters, and admission control policies.

**Transmit Power Selection**

The Transmit Power value corresponds to the EIRP (Effective Isotropic Radiated Power). This is the value radiated by the antenna, i.e., the actual power transmitted "over-the-air". In case of external antennas, the transmit power at the AP port is adjusted according to the antenna gain to ensure that the power radiated over-the-air does not exceed regulatory restrictions.

You can set the Transmit Power Selection to Manual or Auto. In the Auto mode, an Arista AP automatically adjusts its transmit power to minimize interference with neighboring Arista APs.
Note: In addition to the minimum and maximum values specified on the UI, the actual transmit power used is constrained by the following factors:

- The maximum value allowed in the regulatory domain,
- The maximum power supported by the radio, and
- The antenna gain.

Smart Steering

Smart Steering solves the "sticky client" problem. A sticky client is one that stays connected to an AP with poor signal strength, even when there is another AP that can offer better signal strength. In such situations, an Arista AP smartly steers a client to the better AP. Smart Steering thresholds ensure that an Arista AP doesn't steer clients too frequently, since that can worsen QoE.

Smart Client Load Balancing

In high-density user environments (Auditoriums, Lecture Halls, Conference Centers, Company meetings etc.) where APs are densely deployed to provide bandwidth to all clients, a client sees multiple APs with very good signal strength. Most clients will connect to the AP/band with the best signal strength resulting in a few heavily loaded APs. This could result in poor performance. Smart Client Load Balancing corrects this situation by steering clients to less loaded APs with good signal strength.

Band Steering

Band Steering is when an Arista AP steers a client from the 2.4GHz radio to the 5GHz radio because the 5GHz band has more non-overlapping channels and offers better speeds.

Note: Band steering is unidirectional, i.e., clients are always steered from 2.4GHz to 5GHz. As a result, you can configure Band Steering parameters only on the 2.4GHz tab, and not on the 5GHz tab.

WMM Admission Control Policy

Wi-Fi Multi Media (WMM) prioritizes the network traffic based on four access categories - voice, video, best effort and background. You can make Admission Control mandatory. If you do so, you must configure the admission control parameters for voice and video calls — the Maximum Allowed Calls count and the Maximum Share of Medium Time. You also need to set aside a fraction of these resources for roaming clients, under Roaming Reservation. This ensures that clients that roam on this SSID are guaranteed some resources when they're on a voice or a video call.

### 14.1 How Unified Client Steering Works

Table Types of Client Steering shows the different types of client steering. They are classified based on when the client is steered (pre-association or post-association) and the criteria used to steer the client (received signal strength (RSSI), load or band).

<table>
<thead>
<tr>
<th>Stage</th>
<th>Method</th>
<th>Short Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-Association</td>
<td>Min Association RSSI</td>
<td>Rejects association request if client’s RSSI is less than the configured threshold</td>
</tr>
</tbody>
</table>
## Radio Settings

<table>
<thead>
<tr>
<th>Stage</th>
<th>Method</th>
<th>Short Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Band Steering</td>
<td>Rejects association requests on 2.4 GHz for dual band clients. Band steering is unidirectional. The AP always steers a client from 2.4GHz to 5GHz because the 5GHz band has more non-overlapping channels and offers higher speeds.</td>
</tr>
<tr>
<td></td>
<td>Smart Client Load Balancing</td>
<td>Rejects association request if the client load on an AP is high and less loaded neighbor APs are available</td>
</tr>
<tr>
<td>Post-Association</td>
<td>Smart Steering</td>
<td>Disconnects client if RSSI drops below a certain threshold</td>
</tr>
<tr>
<td></td>
<td>Band Steering</td>
<td>When a 5GHz AP radio comes up after being down for a while (for example, due to Radar detection, auto channel selection epoch, or channel change due to high RF interference detection), AP steers dual band clients that were connected to 2.4 GHz when 5 GHz was down</td>
</tr>
</tbody>
</table>

**Note:** Unified Client Steering works only on 11ac Arista devices. It is not supported for 11n Arista devices.

### 14.1.1 General Considerations

Unified Client Steering binds different types of steering together in a well-defined, coherent framework. Two general considerations motivate Unified Client Steering:

- APs must have a unified view of the network
- Clients should not be steered too frequently

### 14.1.2 Inter AP Sync

An AP must have a unified, client-aware view of the network. That is, it must know how the network looks to its neighboring APs and to clients – both its own clients and those of the neighbors. The AP can then make informed steering decisions to ensure optimum client QoE.

To facilitate this, Arista APs periodically exchange information about their respective clients with each other. An Arista AP sends client RSSI value updates to its RF neighbors on the wired network. Only its RF neighbors update the client RSSI values. So, each Arista AP maintains a database of the RSSI values of its clients and of the clients connected to its neighboring Arista APs. The AP incorporates this information into its steering algorithms. It steers a client only if the client’s RSSI is above the minimum threshold for at least one RF neighbor, i.e., only if the client has at least one other AP that it can successfully connect to.

**Note:** Sharing of client RSSI values among APs works only for tri-radio platforms such as C-130. All other features described in the document work for both dual-radio and tri-radio APs.
Example: Minimum Association RSSI

To appreciate the value of a unified view of the network, consider the client in figure Minimum Association RSSI Example. It is located between two APs, AP1 and AP2. Suppose the client’s RSSI values, as seen by both APs, are lower than the minimum needed to associate with them. Then, without Unified Client Steering, the client cannot connect because neither AP1 nor AP2 accepts the client’s association request. With Unified Client Steering, however, AP1 is CloudVision WiFi of the client’s RSSI as seen by AP2 and vice versa. Because AP1 knows that there is no neighboring AP that can see the client with an RSSI greater than the minimum association threshold, it does not reject the client’s association request. This allows the client to connect, improving user experience.

Figure 7: Minimum Association RSSI Example

14.1.3 Frequency of Client Steering

APs must not steer clients too frequently. Clients that are moving or happen to be in the coverage overlap region of two APs could “ping-pong” between the two APs because of constant back and forth steering. This is wasteful signaling and could cause poor user experience.

To avoid this, Arista APs should not attempt to steer a client too often. You can configure a Steering Attempts Threshold parameter that determines the maximum number of attempts to steer a client allowed in a 10-minute window (see Configuration section for details). The default value is 2. So, if an Arista AP has attempted to steer a client twice in 10 minutes, the client enters a configurable Blackout Interval (default 15 minutes). The AP does not attempt to steer such a client until the Blackout Interval has elapsed. An Arista AP shares the steering attempt epochs of its clients with its RF neighbors in its periodic wired-side broadcasts.

Example: Smart Steering

Figure Smart Steering Example shows a client located in the coverage overlap region between two APs, AP1 and AP2. The client’s RSSI could change quite frequently because of channel fading or because it might be moving. Without Unified Client Steering, when the client’s RSSI at AP1 drops below the configured threshold, AP1 steers it to AP2; when the RSSI at AP2 drops, the client is steered in the opposite direction. The client could thus constantly “ping-pong” between two APs. With Unified Client Steering, after being steered at most twice in 10 minutes, the client enters a 15-minute Blackout Interval (assuming all default values). This solves the client’s frequent “ping-pong” problem.
14.2 Configure Client Steering Common Parameters in Radio Settings

In Client Steering Common Parameters, the different types of client steering work together towards the common goal of improving client Quality of Experience (QoE).

To know more about parameters required in configuring Client Steering Common Parameters refer Client Steering Parameters.

To configure the Client Steering Common Parameters:
1. Navigate to CONFIGURE > WiFi > Radio Settings.
2. Click the Client Steering Common Parameters link at the bottom of the screen.
3. Enter value for Steering RSSI Threshold.
4. Set max number of steering attempts for a client in Steering Attempts Threshold field.
5. Set steering suspension period for a client in Steering Blackout Period field.
6. Click Save.

14.2.1 What is Unified Client Steering

An Arista AP can steer a client to a different band or to another Arista AP. Clients can be steered before or after association. The decision to steer a client is based on considerations such as signal strength, load (i.e. number of clients connected to the radio) and the preferred band of operation. While client steering is important for best user Quality of Experience (QoE), frequent and ad-hoc steering of the client can in fact worsen the QoE. Arista APs use an approach called Unified Client Steering. In this approach, APs exchange information with each other, resulting in a “big picture” view of the client experience. Different types of client steering then work together towards the common goal of improving client QoE. For example, Smart Steering and Band Steering use the Common RSSI threshold as their reference.

14.2.2 Client Steering Parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Steering Common Parameters</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Client Steering Common Parameters</td>
<td>Client Steering Common Parameters can be configured only on 11ac devices.</td>
</tr>
<tr>
<td>Steering RSSI Threshold</td>
<td>The steering RSSI threshold can be between -60 to -85 dBm. Default value is -70 dBm.</td>
</tr>
<tr>
<td>Steering Attempts Threshold</td>
<td>This is the max number of steering attempts for a client within a 10 minutes window after which the client's steering is suspended for a period specified by Steering Blackout Period. The default value for steering attempts is 2. The minimum value is 1 and maximum value is 5.</td>
</tr>
<tr>
<td>Steering Blackout Period</td>
<td>This is the steering suspension period for a client. No steering methods would be employed for a client if it sojourns within this time period. The default value for steering blackout period is 15 minutes. The minimum value is 10 minutes and maximum is 60 minutes.</td>
</tr>
</tbody>
</table>

14.3 Configure Basic Radio Settings

You can configure Radio Settings for both 2.4GHz and 5GHz. The configuration is location specific.

To know more about the Radio Settings parameters refer Basic Radio Settings Parameters.

To configure basic radio settings:

1. Navigate to CONFIGURE -> Radio Settings.
2. Select the Wi-Fi Regulatory Domain.
   - Selecting the Wi-Fi Regulatory Domain displays the set of channels available in the 2.4GHz and 5GHz bands.
3. Select the frequency band.
4. Configure the Operating Channel section.
5. Choose Auto or Manual Channel Selection.
   - If Channel Selection is Auto, then provide appropriate values for the fields below.
     - Channel Width.
     - Selection Interval in hours.
     - Dynamic Channel Selection to enable automatic switching of the current channel to an available channel with lower interference.
     - Select Candidate Channels depending on the chosen Wi-Fi Regulatory Domain.
   - If Channel Selection is Manual then provide the appropriate Channel Number.
6. Click Save.

14.3.1 Basic Radio Settings Parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating Region</td>
<td>contains list of region or country, default it United States. User is allowed to change it if he has an entitlement or license.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Frequency Band</td>
<td>The radio frequency band. The possible values are 2.4 GHz and 5 GHz. Default value is 2.4 GHz.</td>
</tr>
<tr>
<td>Channel</td>
<td></td>
</tr>
<tr>
<td>Operating Channel</td>
<td>The operating channel for the radio. By default, the AP automatically selects the operating channel as automatically (Auto). User can manually set the channel if desired. Select Manual, to set the operating channel. Based on the location selected, a list of channel numbers are presented for manual channel selection. If the manually selected channel is not present in the country of operation selected for the device in the applied AP template, the AP automatically reverts to Auto mode and selects a channel.</td>
</tr>
<tr>
<td>Channel Width</td>
<td>The channel width for the radio. Possible values are 20 MHz or 20 MHz /40 MHz. In case of a/n/ac devices, the 20/40/80 MHz option is available. The options are enabled for 2.4 GHz and 5 GHz modes.</td>
</tr>
<tr>
<td>Selection Interval</td>
<td>This field is visible only when the Operating Channel is set to <strong>Auto</strong>. This field specifies the time interval, in hours, at which the channel selection happens. You can enter any value from 1 to 48. The channel may change automatically after this time interval if some other channel is found to have lower interference than the current channel.</td>
</tr>
<tr>
<td>Dynamic Channel Selection</td>
<td>This field is visible only when the Operating Channel is set to <strong>Auto</strong>. Select the Dynamic Channel Selection check box to enable automatic switching of the current channel to an available channel with lower interference, when the interference on the current channel increases. The mechanism is independent of the Selection Interval, and channel is changed only when the interference on current channel is very high.</td>
</tr>
<tr>
<td>Candidate Channels</td>
<td>This field is relevant in case of auto-channel selection. It enhances the behavior of auto-channel selection. The AP dynamically checks if the current channel interference has increased and selects a channel with lower interference and diverts the traffic to this channel. For countries where channel 13 or above are permitted on the b/g band, only the channels 1,5,9,13 are selected, by default. You can modify the candidate channel list.</td>
</tr>
</tbody>
</table>
14.4 Configure 802.11ax Settings

Until 802.11ac, WiFi standards focused on increasing peak data rates. With 802.11ax, although the data rates increase, the focus is on improving WiFi capacity—a must for high-density environments. Given the large number and variety of WiFi devices in dense environments, capacity is no longer just about the number of simultaneous users supported; it is about optimally allocating resources to meet the Quality of Service (QoS) requirements for the largest number of users. 802.11ax features such as OFDMA and MU-MIMO are best understood in this light.

Note: All Arista 802.11ax APs do not support all the enhancements. For details on which AP supports which 802.11ax features, please check the AP datasheet on the https://www.arista.com/en/products/cognitive-wifi page or the AP Feature Matrix on the WiFi Help Portal.

14.4.1 MU-MIMO

Multiple Input Multiple Output (MIMO) refers to the use of multiple antennas on WiFi APs and clients to increase data rates (via spatial multiplexing) and reduce interference (via spatial diversity). Multiple antennas result in multiple, simultaneous “streams” of data between an AP and a client on the same channel. Multi-user MIMO (MU-MIMO) uses the multiple-antenna streams not to improve the transmission to a single user but to simultaneously serve multiple users, i.e., to improve capacity rather than user data rates. The figure below shows an example of MU-MIMO where four streams on the AP can simultaneously serve two clients, each with support for two streams.

Downlink MU-MIMO

Depending on the channel conditions of a client, an AP can use Single User MIMO (SU-MIMO) to improve the client’s data rates or reduce its error rates. Both, however, are per-link improvements. Since dense environments are about capacity and not just individual user data rates, downlink MU-
MIMO can help in dense environments by allocating resources (i.e. streams) more efficiently among a large number of users. 802.11ax supports 8x8 MIMO on the downlink, i.e., an AP can simultaneously send data to eight users.

Uplink MU-MIMO

Uplink MU-MIMO is especially useful for uplink-heavy applications such as social media, content sharing, and video calls. As with the downlink, uplink MU-MIMO increases capacity compared to the SU-MIMO case. This results in a better user experience when uploading content. 802.11ax supports 8x8 MIMO on the uplink, i.e., eight users can simultaneously send their data to an AP. Early 802.11ax WiFi clients might not support uplink MU-MIMO and for the ones that do, the implementation is not yet mature across client manufacturers. If your 802.11ax network has throughput problems, you might want to disable uplink MU-MIMO.

14.4.2 OFDMA

Orthogonal Frequency Division Multiple Access (OFDMA) divides the WiFi channel into subcarriers, also called “tones”, each 78.125 KHz wide. Tones are combined to form resource units (RUs) of different widths. As shown in the representation below, an RU can consist of 26, 52, 106, or 242 tones—corresponding to channel widths of approximately 2 MHz, 4 MHz, 8 MHz, and 20 MHz. In each scheduling interval, OFDMA allocates one or more RUs of different widths to multiple users, resulting in an efficient and flexible use of the channel.

802.11ax uses OFDMA to support multiple users simultaneously, but the underlying multiple access mechanism continues to be CSMA-CA with backoff. Users are scheduled simultaneously, but only when CSMA-CA determines that the medium is available for transmission.

Downlink OFDMA

On the downlink, an 802.11ax Arista AP intelligently schedules clients and allocates resources. Until 802.11ac, an entire 20/40/80 MHz channel would be allocated to a single user during one time slot. This is not optimal because the client application may use only a fraction of the channel. Downlink OFDMA uses the channel much more efficiently by distributing it among clients, allocating only as much of the channel to each client as needed and changing the allocation when needed. The resource allocation and scheduling are based on factors such as the application QoS required and the channel conditions. An 802.11ax AP has the flexibility to allocate any combination of...
RUs. The figure below shows an example of an AP allocating RUs in three scheduling intervals.

In the first scheduling interval, the AP allocates two 52-tone RUs to Client 1 and Client 2, and one 26-tone RU to Client 3. In the second interval, it allocates the whole 20 MHz channel—a single, 242-tone RU—to Client 1. And in the third interval, it allocates two 106-tone RUs to Client 2 and Client 3.

**Uplink OFDMA**

The WiFi uplink is a distributed form of communication because the transmitters (i.e., clients) cannot coordinate their schedules (unlike the downlink, where the AP is both the transmitter and the scheduler). Until 802.11ac, WiFi uplink was uncoordinated: clients contended for the medium and, based on randomly distributed timing, sent packets to the AP. This works reasonably well for single or sparse AP deployments, but for dense deployments, this can cause high uplink contention in presence of a large number of clients. With 802.11ax, the WiFi uplink is coordinated. The AP manages the uplink resource allocation via mechanisms that essentially coordinate the transmission schedule among clients while using CSMA-CA to ensure that the medium is available for transmission. This leads to reduced uplink contention, thereby improving capacity and user experience. Early 802.11ax WiFi clients might not support uplink OFDMA and for the ones that do, the implementation is not yet mature across client manufacturers. This may adversely affect the 802.11ax AP throughput. If your 802.11ax network has throughput problems, you might want to disable uplink OFDMA.

### 14.5 Configure Transmit Power Selection in Radio Settings

You can fix the transmit power of an AP manually or you can configure an AP to automatically adjust its own transmit power.

To know more in detail about the configuring parameters refer Transmit Power Selection Parameters.

To configure Transmit Power Control in radio settings:

1. Navigate to **CONFIGURE > Radio Settings**.
2. Click **Advance Radio Settings**.
3. Move to **Transmit Power Selection Settings**.
   
   Transmission power settings can be configured auto as well as manually.
4. Select **Auto** option.
   
   Selection of **Auto** option enables the threshold fields.
5. Enter the appropriate values for the following fields:
   
   - **Loudness RSSI**
   - **Neighbor Count**
   - **Minimum Transmit Power**
   - **Maximum Transmit Power**
Radio Settings

Selecting Manual optional enables a text box to enter the transmission control power in dbm.

7. For access points that use an external antenna, select Use External Antennas and enter the External Antenna Gain in dB.

8. Click Save.

If the configuration is correct and saved successfully, CloudVision WiFi displays a success message.

### 14.5.1 Transmit Power Selection Parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Radio Settings</td>
<td></td>
</tr>
<tr>
<td>Transmit Power Selection (Auto and Manual radio buttons)</td>
<td>This field enables you to control the transmission power of the AP. It is a mandatory field.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Manual</td>
<td>Manual - Select the Manual option to manually specify the transmission power of the AP in dbm.</td>
</tr>
<tr>
<td>Automatic</td>
<td>Automatic - Select the Automatic option to have the AP automatically adjust its transmit power so as to minimize interference with neighboring Arista APs. The neighbor APs must be connected to the same Wireless Manager instance ID (should have same CUSTOMER ID) and must have at least one profile ID.</td>
</tr>
<tr>
<td>Loudness RSSI</td>
<td>An AP is considered loud if it can be heard by a neighbor AP with an RSSI greater than this value. Allowed range is -95 dBm to 0 dBm. The default is -75 dBm.</td>
</tr>
<tr>
<td>Neighbor Count</td>
<td>Maximum number of allowed loud neighbor APs. Allowed range is 1 - 10. The Default value is default 3.</td>
</tr>
<tr>
<td>Minimum Transmit Power</td>
<td>Minimum transmission power. Allowed range is 4 - 30 dBm. The Default value is 4 dBm.</td>
</tr>
<tr>
<td>Maximum Transmit Power</td>
<td>Maximum transmission power. Allowable range is 4 - 30 dBm. The Default value is 30 dBm.</td>
</tr>
</tbody>
</table>

### 14.6 Configure Smart Steering in Radio Settings

Smart Steering feature helps you to resolve the issue of sticky client.

To configure Smart Steering in Radio Settings:

1. Navigate to CONFIGURE > Radio Settings.
2. Click Advance Radio Settings.
3. In the Smart Steering section enter the time interval, in seconds for Roam Initiation Interval. Roam Initiation Interval is the time interval, for which the client's signal strength should be lower than the Roam Initiation RSSI Threshold for the AP to initiate the roam. The time can range from 5 to 900. Default value is 10.
4. Enter the RSSI threshold to disconnect a client in Roam Initiation Packet Threshold field.
When the signal strength of the client is less than this threshold, the AP disconnects the client and initiates a roam. The packet threshold can be between 5 to 500. Default value is 5.

5. Click Save.

If the configuration is correct and saved successfully, CloudVision WiFi displays a success message.

14.7 Configure Smart Client Load Balancing in Radio Settings

Smart Client Load Balancing is configured per SSID but it acts per radio. The radio is shared by all SSIDs associated with the band (2.4 or 5GHz). Balancing clients across APs provides each client a larger slice of radio time. The balancing mechanism may deny immediate access to the AP when a client roams. Clients that use real-time applications such as video and voice may be impacted. It is not recommended that Smart Client Load Balancing be enable on SSIDs that support real-time applications.

To configure Smart Client Load Balancing in radio settings:

1. Navigate to CONFIGURE > Radio Settings.
2. Click Advance Radio Settings.
3. In the Smart Client Load Balancing section enter the minimum number of clients that can connect to an AP in Minimum Client Load field.
   This field lets you specify the minimum number of clients that can connect to an AP before client load balancing is triggered. The default value for this field is 30 and the threshold is 45. The minimum client load on each radio is taken into consideration while the load on a single AP is checked.
4. Enter the minimum difference between the number of clients connected on neighboring APs in Minimum Client Load Difference field.
   This minimum difference is considered to balance client load. Default value is 5 and range varies from 2 to 10.
5. Click Save.

If the configuration is correct and saved successfully, CloudVision WiFi displays a success message.

14.8 Configure Band Steering in Radio Settings

Band steering is a load balancing feature that lets the Wi-Fi client switch to the other available band to balance the load of the Arista access point in case more clients are operating on a single band.

To configure Band Steering in Radio Settings:

1. Navigate to CONFIGURE > Radio Settings.
2. Click Advance Radio Settings.
3. Scroll down to Band Steering section.
4. Enter the value for Band Steering Client Load Difference.
   It is the load balancing parameter that is useful for tuning the load distribution between 2.4 GHz and 5 GHz bands. If the difference between the number of clients associated in 5 GHz and 2.4 GHz exceeds the threshold, band steering to 5 GHz is not performed until the difference comes below the threshold. Default value for this field is 25 and the threshold is 50.
5. Click Save.

If the configuration is correct and saved successfully, CloudVision WiFi displays a success message.
14.9 Configure WMM Admission Control Policy in Radio Settings

Wi-Fi Multi Media (WMM) prioritizes the network traffic. Configuration is done for the admission control parameters for voice and video calls. All the fields involved in configuration will be configured depending upon the choice made between video or voice calls.

To configure WMM admission control policy in radio settings:

1. Navigate to CONFIGURE -> Radio Settings -> Advanced Radio Settings.
2. Scroll Down to WMM Admission Control Policy.
3. Select Admission control policy as Voice Calls or Video Calls.
4. Select Admission Control Mandatory to make admission control mandatory.
5. Select No Ack Policy to enable no acknowledgement policy.
   When you enable no acknowledgement policy, the acknowledgement for the unicast QoS data packets is not required from the receiver. No retransmission take place for the QoS data packets when the no ack policy is enabled.
6. Provide the maximum number of allowed voice or video calls depending upon choice in Maximum Allowed Calls field.
   Limit for number of voice calls is 127.
7. Enter the maximum percentage share of the medium time for voice calls in Maximum Share Of Medium Time field.
   The value for maximum percentage share ranges from 0 to 100. Default value is 0.
8. Enter the number of voice calls reserved for roaming clients in Call Reserved field.
   The range for this field is from 0 to the number of maximum allowed calls specified in Maximum Allowed Calls field.
9. Enter the percentage share of the medium time reserved for roaming clients in Share Of Medium Time Reserved field.
   The range for percentage share is from 0 to the percentage share specified in Maximum Share Of Medium Time field.
10. Click Save.

If the configuration is correct and saved successfully, CloudVision WiFi displays a success message.
Device Settings

Under Device Settings, you can configure Device related settings such as Background Scanning and Security related settings such as WIPS. Device Settings is available as a submenu in CONFIGURE.

Note: By default, Device Settings applied to a location are automatically inherited by its child locations. For example, suppose there is an HQ location with two child locations: Branch 1 and Branch 2. Then a device setting applied to HQ automatically applies to Branch 1 and Branch 2. You can, however, customize the device settings of a child location so that they are different from those of its parent.

Configurations in Device Settings typically apply to a device, i.e., to all the radios of the device. Since an Arista AP can operate as an access point and/or as a WIPS sensor, Device Settings in CloudVision WiFi is further divided into two tabs: Device tab and Security tab.

You can make changes to Device Settings even when the AP is offline, i.e., not connected to the Wireless Manager (WM). WM pushes the changes onto the AP when the AP reconnects with WM.

15.1 Device Tab

You can configure device related settings such as Background Scanning on the Device Tab.

You can turn the access point into a WIPS sensor on the Device tab. When you do so, CloudVision WiFi permanently erases WiFi access related settings (Background Scanning, for example) in that folder.
You can enable Background Scanning on the Device tab. When you enable Background Scanning, an access point radio periodically scans channels in its band (2.4GHz or 5GHz). You can configure for how long the AP scans channels (say, for 100ms) and how often it does so (say, every 10 seconds). An Arista AP uses information obtained during a background scan mainly for two purposes: performance optimization (e.g. Dynamic Channel Selection, Client Steering) and security (e.g. WIPS rogue AP detection). As a result, many of the RF Optimization features require Background Scanning to be enabled.

With Inter-Access Point Sync for Client Steering, APs exchange client information with each other. This helps steer clients between APs.

Bluetooth Low Energy (BLE) is used for proximity based services on mobile devices via an application ecosystem. Arista APs now support the iBeacon BLE standard. You can set the BLE iBeacon parameters in Device Settings.

VLAN Extension applies only to the W-68 model and only when it's in AP mode (i.e. not configured as a sensor). VLAN Extension allows you to map a W-68 LAN port to a VLAN ID. It's essentially a way to extend your wired network - a typical use case could be plugging a laptop in to one of these ports to connect directly to the wired network.

**Note:** You can map multiple LAN ports to the same VLAN ID but one LAN port can have only one VLAN ID.

Link Aggregation applies only to the Arista C-120 and C-130 models. When you enable Link Aggregation, multiple ports merge into a single logical link. This results in higher aggregate bandwidth on servers with heavy traffic. It also utilizes the bandwidth more efficiently since the logical overheads are shared between two physical links.

**Note:** If you enable Link Aggregation, you must use a switch capable of link aggregation.

AeroScout Tags are small, battery-powered devices mounted on equipment or carried by personnel. The AeroScout Engine Server (AES) determines the location of these tags based on the signal strength information that it receives from Arista WiFi access points (APs).

Antenna Settings allow you to choose whether APs at the location use internal or external antennas.

Device Password allows you to set the username and password for devices at the location.

You can enable Device Access Log and specify the hostname or IP address of a Syslog server to which you want devices to send their access logs.

IPv4/IPv6 Dual Stack enables both stacks in the devices.

Enable SSH IP Allow List allows you to restrict the IP addresses that are allowed to SSH to Arista APs.

Selecting Disable LEDs will turn off all the LEDs on APs to which you apply this device settings. The LEDs are turned off once the AP boot-time setup is complete. This is useful in environments where you do not want the LEDs to be visible - for example, hospitals, classrooms etc.

**Note:** Only the following platforms support disabling of LEDs: C-100, C-110, C-120 and C-130.

NTP Configuration defines the primary and secondary servers that an Arista device uses to get its clock reference.

When you enable Analytics Integration with Third Party Server, an Arista device sends analytics information to an external server. You can specify the format in which the analytics information is sent, the server URL, and the interval for sending the analytics.

Access Radio Exceptions apply to Single Radio devices or to dual-radio devices that can operate in a "combo" mode with one radio in access mode and the other one in WIPS mode. For Single Radio devices, you can select the band you want the device to operate on. For Dual Radio AP-Sensor Combo devices, you can select the band of operation of the access radio.
15.2 **Turn Access Point into a WIPS Sensor**

Turning access points into a WIPS sensors permanently erases Wi-Fi access related settings at the selected folder.

To turn access point into a WIPS sensor:

1. Navigate to **CONFIGURE > Device Settings > Device**.
2. Select **Turn Access Point into a WIPS Sensor**.

It asks for confirmation.

3. Click **Continue** to turn APs into WIPS sensor.
4. Click **Save**.

If the configuration is correct and saved successfully, CloudVision WiFi displays a success message. Turning Access Point into a WIPS Sensor skips the configuration for **Background Scanning** and **Client RSSI Update Interval** settings.

15.3 **Configure Scanning**

Arista APs have the capability to scan the radio channels at a periodic interval. The scan duration and the interval at which the scans must run can be configured.

The available scanning options are:

- Background Scanning
- VoIP Scanning
- No Scanning

---

**Important:** Do not enable background scanning if the radio is being used for Voice over IP (VoIP).

**Important:** If **No scanning** is selected, then features such as "Smart Client Load Balancing", "RF Neighbors", "Smart Steering, and "Minimum RSSI Based Association" configured in the SSID profile will be rendered non-functional.

**Background Scanning**

A method where a radio providing WiFi access service scans off-service channels intermittently. The scan timings are variable and can be configured by the user. By default, the scan duration and access duration is 100ms and 10ms respectively.

For tri-radio devices, background scanning is disabled by default as the one of the radios is always in WIPS mode. To know more about parameters required in configuring Background Scanning refer Background Scanning Parameters.

**VoIP Scanning**
Background scanning can disrupt high-bandwidth applications like voice and video. To avoid this disruptive behavior, use VoIP Scanning on radios containing SSIDs that are used for high bandwidth applications.

If VoIP Scanning is enabled, the AP performs a quick scan of channels for a duration of 30 ms instead of a full scan.

If a voice or video application is in progress, an access radio, after every 10 sec spent on the service channel to serve WiFi clients will make a visit to a single off-service channel for 30 ms.

To configure Scanning:
1. Navigate to CONFIGURE > Device Settings > Device.
2. Under Scanning, select any of the available options.
3. If you select Background Scanning, you can configure the Wi-Fi Scan Duration and Wi-Fi Access Duration. Refer Background Scanning Parameters.
4. Click Save.

If the configuration is correct and saved successfully, CloudVision WiFi displays a success message. Enabling Background Scanning enables Wi-Fi Security Features and Inter AP Sync for Client Steering settings.

### 15.3.1 Background Scanning Parameters

The below table provides information about parameters of Background Scanning. It includes possible values, behavior, and all the related information about the parameters.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wi-Fi Scan Duration</td>
<td>Time duration, in milliseconds, for which the AP scans a background channel when background scanning is turned on. Scan duration alternates with the AP interval. Connected clients remain connected to the AP for the scan duration. You can specify a value between 50 and 150 milliseconds. The default value is 100 milliseconds.</td>
</tr>
<tr>
<td>Wi-Fi Access Duration</td>
<td>Time duration, in seconds, after which the AP scans a background channel when background scanning is turned on. Background scanning does not happen during this duration. AP interval alternates with the scan duration. You can specify a value between 5 and 3600 seconds. The default value is 10 seconds.</td>
</tr>
</tbody>
</table>

### 15.4 Configure Inter Access Point Sync for Client Steering in Device Settings

Inter Access Point Sync if enabled syncs with neighboring APs to share client visibility information for an improved steering experience.

You should enable inter Access Point sync for multiple AP deployments only.

Background scanning must be turned on all AP radios except for the devices with 3rd scanning radio.
To configure Inter Access Point Sync for Client Steering:
1. Navigate to CONFIGURE > Device Settings > Device.
2. Select Inter Access Point Sync for Client Steering.
3. Enter Sync Period in seconds.
   Sync Period is the time interval specified to broadcast periodic Sync messages. The time interval can be minimum 10 seconds and maximum 60 seconds.
4. Click Save.
   If the configuration is correct and saved successfully, CloudVision WiFi displays a success message.

15.5 Configure Client RSSI Update Interval in Device Settings

This feature provides Client RSSI Update after every specific interval.

To configure Client RSSI Update Interval:
1. Navigate to CONFIGURE > Device Settings > Device.
2. Scroll down to Client RSSI Update Interval tab.
3. Enter Interval in seconds.
   Device updates the RSSI of visible WiFi clients with this periodicity.
4. Click Save.
   If the configuration is correct and saved successfully, CloudVision WiFi displays a success message.

15.6 Configure VLAN Extension in Device Settings

Enabling VLAN Extension, takes precedence over the Wired Extension configured in the Wi-Fi Profile.

To configure VLAN Extension:
1. Navigate to CONFIGURE > Device Settings > Device.
2. Select VLAN Extension.
3. Select the LAN port and specify the VLAN ID.
   The applicable values are 0 through 4094, where 0 indicates an untagged VLAN. A LAN port can be mapped to only one VLAN ID. But, the same VLAN ID can be mapped with more than one LAN port.
4. Click Save.
   If the configuration is correct and saved successfully, CloudVision WiFi displays a success message.

15.7 Configure Link Aggregation in Device Settings

Enabling Link Aggregation allows multiple ports to merge logically in a single link. This leads to minimizing the wastage of bandwidth as the full bandwidth of each physical link is available. Link aggregation offers higher aggregate bandwidth on servers having heavy traffic.

If you enable Link Aggregation for the device, the Enable Wired Extension option in the SSID profile, if set, will be ignored and not take effect. This option is applicable only for C-120 and C-130 devices.

To configure Link Aggregation:
1. Navigate to CONFIGURE > Device Settings > Device.
2. Select Link Aggregation.
3. Select the Transmit Hash Policy.
   You can choose from one of the following options to define the transmit hash policy:
• Layer 2 (MAC)
• Layer 3+4 (IP+Port)
• Layer 2+3 (MAC+IP)

Note: If you enable link aggregation, then you must use a switch that is capable of link aggregation.

4. Click Save.

If the configuration is correct and saved successfully, CloudVision WiFi displays a success message.

15.8 Configure AeroScout Integration

Configuring CloudVision WiFi for integration with AeroScout comprises the following steps:

1. Make sure the APs at the locations where you want Aeroscout to work are broadcasting at least one SSID on the 2.4 GHz band. AeroScout tags use this band to communicate with WiFi APs. You can set up SSIDs under Configure > WiFi.
2. To enable integration with AeroScout, go to Configure > Device Settings. Enable the AeroScout checkbox and set the port number (1144) to be used for the AP-AeroScout communication.

Note: Make sure that the port (1144) is open for bidirectional UDP communication between the AES and the APs.
3. Make sure that APs at this location use only channels 1, 6, and 11 on the 2.4 GHz band. AeroScout tags typically use these channels to communicate with WiFi APs. You can configure Channel Settings under Configure > WiFi > Radio Settings.

15.9 Configure Antenna Settings in Device Settings

This configuration is applicable for C-50, C-60, C-10, SS-200-AT-01. User can select internal or external antenna depending on preferences.

To configure Antenna Settings:

1. Navigate to CONFIGURE > Device Settings > Device.
2. Scroll down to Antenna Settings.
3. Select the Antenna Type.
   This field has 2 values-internal and external. If you want to work with internal antennas, select Internal. If you want to work with external antennas, select External.
4. Click Save.

If the configuration is correct and saved successfully, CloudVision WiFi displays a success message.

15.10 Configure Device Password in Device Settings

Device Password configuration helps you manage the password for the Arista device. By defining a password in this setting, you can manage the password for a group of devices without having to change it on each device separately.

To configure Device Password:

1. Navigate to CONFIGURE > Device Settings > Device.
2. Scroll down to Device Password tab.
3. Enter username.
   Default user name is config.
4. Enter Password.
The password should be at least 6 characters long and it cannot contain spaces or your login ID.
5. Confirm the new password by entering again the same password in **Confirm Password** field.
6. Click **Save**.

If the configuration is correct and saved successfully, CloudVision WiFi displays a success message. The new password is applied on all the associated devices.

### 15.11 Configure Device Access Logs in Device Settings

Wireless Manager provides you with a functionality to send the sensor access logs to the Syslog server. This functionality is useful for audit purposes and can be enabled or disabled.

To configure Device Access Logs:
1. Navigate to **CONFIGURE > Device Settings > Device**.
2. Select **Device Access Logs**.
3. Enter **Syslog Server IP/Hostname**.
   - Syslog server IP/Hostname to which the access logs are to be sent.
4. Click **Save**.

If the configuration is correct and saved successfully, CloudVision WiFi displays a success message.

### 15.12 Configure IPv4/IPv6 Dual Stack in Device Settings

You can enable or disable the support for IPv4/IPv6 dual stack network. When you enable support for IPv4/IPv6 dual stack network, the AP, to which the device settings are applied, is able to operate on both IPv4 and IPv6 addresses simultaneously. When you disable support for IPv4/IPv6 dual stack network, the AP, to which the device template is applied, can operate on IPv4 networks only.

To configure IPv4/IPv6 Dual Stack:
1. Navigate to **CONFIGURE > Device Settings > Device**.
2. Select **IPv4/IPv6 Dual Stack**.
3. Click **Save**.

If the configuration is correct and saved successfully, CloudVision WiFi displays a success message.

### 15.13 Enable SSH IP Allow List

The **Enable SSH IP Allow List** option under the Device Settings tab is unchecked by default. You can enforce SSH access from specific IP addresses by checking this option. If this option is enabled, only IP addresses that match the specified criteria can SSH to the AP.

For more details on SSH IP Allow List parameters refer *SSH IP Allow List Parameters*.

To enable SSH IP Allow List:
1. Navigate to **CONFIGURE > Device Settings > Device**.
2. Select **Enable SSH IP Allow List**.
3. Enter an IPv4 IP address in the **IP Address** field.
4. Enter a Wildcard Mask in the **Wildcard Mask** field.
5. Click **Add**.

You must provide at least one IP address and wildcard mask. You can provide a maximum of 20 such entries. SSH access to the communication IP of the access point is enabled only from the IP addresses that match the IP address and wildcard mask criteria.
15.13.1 SSH IP Allow List Parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>A valid IP address.</td>
</tr>
<tr>
<td>Wildcard Mask</td>
<td>The wildcard mask is a mask of bits that helps identify the parts of the IP address that must match and the parts that can be ignored. The binary equivalent of the IP address and wildcard mask is used for examining the bits that must match. Wildcard mask acts as an inverted subnet masks, i.e., the zero bits in the mask indicate that the corresponding bit position in the IP addresses must match. The one bits indicate that the corresponding bit position doesn't have to match. For example: if the IP address is 10.10.0.0 and the mask is 0.0.0.255 then the IP addresses 10.10.0.0 through 10.10.0.255 will match. However, if the mask is 0.0.1.255 then the IP address 10.10.0.0 through 10.10.0.255 and 10.10.1.0 through 10.10.1.255 will match.</td>
</tr>
</tbody>
</table>

15.14 Configure NTP in Device Setting

The Arista device system clock resets itself to Epoch time (that is, January 1 1970) after every reboot as it does not have an internal battery to maintain time across reboots. The system clock is used to timestamp the logs. You can ensure that the timestamp on the logs reflect the correct date and time by synchronizing the Arista device system clock with an NTP server. This can be done by specifying the details of the NTP server for Arista device time synchronization under device settings.

**Important:** NTP synchronization happens over the communication VLAN of the Arista device. Ensure that the incoming UDP port 123 is open on the firewall for the communication VLAN.

To Configure NTP:

1. Navigate to **CONFIGURE > Device Settings > Device.**
2. Scroll down to **NTP Configuration** tab.
3. Enter **Primary NTP Server IP/Hostname.**
   The default primary NTP server is the NIST (National Institute of Standards and Technology) NTP server, *time.nist.gov*. The NIST NTP server is a server cluster maintained by the US federal government and is connected to high precision atomic clocks. The NIST NTP server is accessible from almost every corner of the globe.
4. Enter **Secondary NTP Server IP/Hostname.**
   The Arista device synchronizes time with the secondary NTP server, if specified, when the primary NTP server is unavailable or inaccessible. It is not mandatory to specify the secondary NTP server.
5. Click **Save.**

If the configuration is correct and saved successfully, CloudVision WiFi displays a success message.
15.15  Configure Access Radio Exceptions in Device Settings

Access Radio Exception is configured for Single Radio or Dual Radio devices. This configuration helps devices to choose the frequency band in case of model agnostic configuration.

To configure Access Radio Exceptions:

1. Navigate to CONFIGURE > Device Settings > Device.
2. Scroll down to Access Radio Exceptions.
3. Select the type of AP between Single Radio AP and Dual Radio AP-Sensor Combo for which configuration is to be done.
   - If you have a single radio AP, then select the frequency band on which your AP should operate below Single Radio AP tab.
   - If you have a dual-radio AP that can operate as an AP and Sensor, then select the frequency band for an AP to operate.
4. Click Save.

If the configuration is correct and saved successfully, CloudVision WiFi displays a success message.

15.16  Device Security Settings

On the Security tab under Device Settings, you can configure VLAN Monitoring and WIPS.

CloudVision WiFi can monitor devices on a VLAN and clients associated with these devices. For details on Auto VLAN Monitoring, see How Auto VLAN Monitoring Works. You can specify any additional VLANs you want monitored.

Note: There are limitations on how many VLANs an Arista AP can monitor. See Number of VLANs Monitored.

It's really easy to set up an unauthorized WiFi network. Small plug-and-play devices can act as access points. Smart phones and tablets can act as WiFi hotspots. Clients can connect to any such access point or hotspot and easily access a network that is not adequately protected against wireless threats. In this way, a network could easily become vulnerable to wireless attacks. It is therefore important to understand and control authorized and unauthorized access to WiFi networks. A good Wireless Intrusion Prevention System (WIPS) is a must to prevent unauthorized access to a network.

Arista AirTight, Arista’s industry-best WIPS solution, can automatically classify devices to detect rogues, and prevent rogue devices from accessing your WiFi network.

Under WIPS Settings, you can enable Offline Mode and select the channels to monitor and defend. The Offline Mode feature provides some security coverage even when there is no connectivity between an Arista sensor and the server. Offline Mode applies only to an Arista device functioning as a sensor. In the Offline Mode, the sensor continues some device classification and prevention, even when it is disconnected from the server. The sensor also raises events, stores them, and pushes them back to the server on re-connection.

You can select the channels to monitor for WIPS detection and the channels to defend for WIPS prevention.

15.16.1  How Auto VLAN Monitoring Works

Virtual Local Area Network (VLAN) Monitoring allows you to monitor devices on a VLAN and clients associated with these devices. Arista AirTight, Arista’s patented Wireless Intrusion Prevention System (WIPS) solution, automatically classifies devices on the monitored VLAN as Authorized, Rogue or External.
Under **Device Settings > Security > VLAN Monitoring**, you can enable the following types of VLAN Monitoring:

- **SSID VLAN Monitoring**: APs monitor their SSID VLANs.
- **Auto VLAN Monitoring**: APs automatically monitor any VLAN on which they detect activity.
- **Additional VLANs**: Additional VLANs to be monitored by APs in that folder or group.

These settings apply to the folder (location) or group. In enterprise WiFi deployments, each AP can often see a different set of VLANs. In such cases, you can define custom VLANs to be monitored on a per-AP basis (under **MONITOR > WiFi > Access Points**, as described in the Monitoring WiFi > Access Points section.

**SSID VLAN Monitoring** is enabled by default. You can disable it if you do not want the AP to monitor VLANs corresponding to the SSIDs configured on the AP.

### 15.16.2 Number of VLANs Monitored

An Arista device can operate in Access Point (AP), Sensor or Network Detector (ND) mode. The table below shows the maximum number of VLANs an Arista device can monitor in each of these modes.

**Table 7: Maximum number of VLANs monitored**

<table>
<thead>
<tr>
<th>Model</th>
<th>AP Mode</th>
<th>Sensor Mode</th>
<th>ND Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>C-50</td>
<td>12</td>
<td>16</td>
<td>50</td>
</tr>
<tr>
<td>Other Arista devices</td>
<td>20</td>
<td>20</td>
<td>100</td>
</tr>
</tbody>
</table>

The order in which an AP monitors VLANs is as follows:

1. **Communication VLAN**: By default, an AP monitors the VLAN it uses to communicate with the Wireless Manager (WM) server.
2. **SSID VLANs**: If SSID VLAN Monitoring is enabled, an AP monitors its SSID VLANs.
3. **Per-AP VLANs**: If customized VLANs are configured for monitoring on a particular AP, then the AP monitors these custom VLANs.
4. **Additional VLANs**: VLANs configured for monitoring (under **Device Settings**) for the folder (location) or group.
5. **Auto VLAN Monitoring**: If Auto VLAN Monitoring is enabled, an AP monitors any VLANs (other than the ones already being monitored) on which it detects activity.

If an AP reaches the maximum number of VLANs it can monitor, then the order listed above determines which VLANs the AP monitors and which ones it does not.

Let’s consider two cases: when SSID VLAN Monitoring is enabled, and when it is not.

- When SSID VLAN Monitoring is enabled, the number of VLANs that an AP automatically monitors is equal to the maximum number it can monitor minus the sum of the number of SSID VLANs and user-defined VLANs. (User-defined VLANs include per-AP VLANs and additional VLANs for the folder or group.)

  \[
  Number\ of\ automatically\ monitored\ VLANs = Max - (SSID\ VLANs + User-Defined\ VLANs)
  \]

  For example, a C-120 in AP mode can monitor a maximum of 20 VLANs. If there are 4 SSID VLANs and 2 user-defined VLANs, the number of automatically monitored VLANs is:

  \[
  20 - (4+2) = 14.
  \]

  Apart from its SSID and user-defined VLANs, the C-120 AP then monitors the first 14 VLANs that it detects as being active.

- When SSID VLAN Monitoring is disabled, the number of VLANs that an AP automatically monitors is equal to the maximum number it can monitor minus the number of user-defined VLANs.
15.17 Configure BLE Settings

Bluetooth Low Energy (BLE) is used for proximity based services on mobile devices via an application ecosystem. Arista APs support the iBeacon BLE standard.

You can set the following BLE iBeacon parameters in CloudVision WiFi:

- **UUID** - This identifies the beacon. It is defined for a Location in the Arista Location Hierarchy. The default value of the UUID is a pre-defined random string at the Root location. You can keep this value or generate a new one.
- **Major** - This is a number that identifies a subset of beacons within a large group. It is defined for a Location in the Arista Location Hierarchy. Its range is from 0 - 65535. The default value is 0.
- **Minor** - This is a number that identifies a specific beacon. It is defined at a device level. Its range is from 0 - 65535. The default value is 0.
- **Advertising Interval** - This is the periodic interval at which beacons are transmitted.

The UUID and Major values are defined at a location in the Arista location hierarchy. For child locations, you can copy the values of these parameters from the parent locations. The Minor and Advertising Interval values are configured in the device settings for an AP.

For details on which APs support BLE, see the BLE Support article on the WiFi Help portal.

15.17.1 Example Use Case for BLE

Let's consider a retail store chain with outlets at two locations - Westside and Eastside. You can then generate different UUID's for iBeacons in each location, i.e., one for Westside and one for Eastside. Within each location, you can further define different Minor values for APs based on the department / aisle within the store - for example, you can have different Minor values for APs in the food and clothing sections. The application ecosystem that you use to provide proximity based services can then use these values to offer location-appropriate options to customers in the store.

15.17.2 Configure BLE from Device Settings

Configure BLE involves configuring UUID, Major, Advertising Interval and Minor. The BLE UUID and Major are defined at a location level. Advertising and Minor are defined at device level.

To configure BLE parameters:

1. Go to **CONFIGURE > Device Settings**.
2. To configure BLE UUID and Major, click the **Set UUID and Major** link.
   a. Select the location where you want to set the BLE parameters and click **Next**.
   b. Enter the **UUID** or click **Generate UUID** to generate one.
   c. Enter a value for the **Major** number.
   d. Click **Save**.
3. To configure Advertising Interval and Minor, select **Bluetooth Low Energy (BLE)** to enable BLE.
   a. Enter the **Advertising Interval**.
   b. Enter a value for the **Minor** number.
   c. Save the Device Settings.

15.17.3 Customize the BLE Minor of an AP

The steps to customize the BLE Minor value of an AP are as follows:

1. Go to **Monitor > WiFi > Access Points**.
2. Right-click the AP for which you want to configure the BLE Minor and select **Customize BLE**.
3. Select **Bluetooth Low Energy (BLE)** to enable BLE on this AP.
4. Enter a value for the **Minor** number.
5. Save the settings.

### 15.18 Configure VLAN Monitoring in Device Settings

VLAN monitoring is essential for the wired-side connection status detection, host name detection, smart device detection, rogue AP detection, and so on.

VLAN Monitoring can be configured and will take effect only if the devices are:

- Configured as WIPS sensors, or
- Configured in the AP mode and have Background Scanning enabled and Wireless Security Features enabled, or
- Tri-radio devices.

While configuring VLAN Monitoring, two tasks can be performed i.e Auto VLAN Monitoring and Monitoring Additional VLANs. To know more about parameters required in configuring VLANs refer to **VLAN Monitoring Parameters**

To configure VLAN Monitoring:

2. In the VLAN Monitoring tab, select **Auto VLAN Monitoring** to automatically monitor the VLANs.
3. Select **Monitor Additional VLANs** to enable the device to monitor additional VLANs.
   A text box to add VLAN IDs is enabled.
4. Enter the additional VLANs to be monitored as a comma-separated list.
5. Click **Save**.

If the configuration is correct and saved successfully, CloudVision WiFi displays a success message.

### 15.18.1 VLAN Monitoring Parameters

The below table gives you a brief overview of the parameters related to **VLAN Monitoring**. It includes possible values, behavior, and all the related information about the parameters.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Auto VLAN Monitoring       | Parameter to automatically monitor the VLANs that are added by the SSID, configured through additional VLANs or through CLI. The behavior of the automatically monitored VLANs is as follows:  
  - Priority is always given to the user configured VLANs. In addition, to the SSID VLANs, 4 additional VLANs can be monitored.  
  - In sensor mode, upto 16 VLANs can be monitored.  
  - In ND mode, 50 VLANs for C50 and 100 VLANs for other platforms can be monitored. |
| Monitor Additional VLANs   | Parameter to enable the device to monitor additional VLANs.                                                                                                                                               |
### Device Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comma separated list of VLAN IDs</td>
<td>The VLAN used by the device to communicate with the server is always monitored and need not be specified here. VLAN IDs can be between 0 to 4094. The additional VLANs to be monitored must be configured on the switch port where the device is connected and must be DHCP enabled. A VLAN ID '0' indicates untagged VLAN on the switch port where the device is connected, irrespective of the actual VLAN number on the switch.</td>
</tr>
<tr>
<td></td>
<td>⚠️ <strong>Important:</strong> If a VLAN is configured with a static IP address, then configure the VLAN from the CLI.</td>
</tr>
</tbody>
</table>

#### 15.19 Configure WIPS Settings in Device Settings

In Device Settings while configuring WIPS Settings, you can enable **Offline Mode features** as well as you can set channels to monitor and defend intrusion under **Channel Settings**.

To know in detail about parameters required while configuring WIPS Settings refer **WIPS Settings Parameters**.

**Prerequisites**

To configure WIPS Settings:

2. Scroll down for the WIPS Settings.
3. Select **Offline Mode**.
   
   A text box to enter time to switch to offline mode is enabled.
4. Enter time in minutes to state the time constraint after which device should switch to offline mode after it detects loss of connectivity.
5. Select **Channels To Monitor** from **Channel Settings** to select the list of channels for monitoring intrusion.

   You can optionally select Select All Standard Channels, Select all Allowed Channels and Additionally, select intermediate channels.

6. Select **Channels to Defend** from **Channel Settings** to select the list of channels for defending intrusion.

   You can optionally select Select All Standard Channels and Select all Allowed Channels
7. Click **Save**.

   If the configuration is correct and saved successfully CloudVision WiFi displays a success message.
15.19.1 WIPS Settings Parameters

The below table contains detail information about the parameters included in **WIPS Settings**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offline Mode</td>
<td>This feature provides some security coverage even when there is no connectivity between an Arista device and the server. The feature is relevant to an Arista device functioning as a sensor. The sensor provides some device classification and prevention capabilities when it is disconnected from the server. The sensor also raises events, stores them, and pushes them back to the server on reconnecting. You can specify the time, in minutes, for the device to switch to offline mode after the device detects loss of connectivity from the server. (Minimum: 1 minute; Maximum: 60 minutes; Default: 15 minutes).</td>
</tr>
</tbody>
</table>

**Channel Settings**

- List of channels for the sensor to monitor and defend intrusion. These channels will differ according to your country of operation. Refer the table for the channel number, its protocol and respective frequency.

**Channels To Monitor**

- List of channels to be selected to monitor intrusion.

**Channels to Defend**

- List of channels to be selected to defend intrusion.

**Select All Standard Channels**

- It auto selects all the standard channels.

**Select all allowed channels**

- It auto selects all the

**Additionally, select intermediate channels**

<table>
<thead>
<tr>
<th>Channel</th>
<th>Protocol</th>
<th>Frequency (GHz)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>b/g/n</td>
<td>2.412</td>
</tr>
<tr>
<td>2</td>
<td>b/g/n</td>
<td>2.417</td>
</tr>
<tr>
<td>3</td>
<td>b/g/n</td>
<td>2.422</td>
</tr>
<tr>
<td>4</td>
<td>b/g/n</td>
<td>2.427</td>
</tr>
<tr>
<td>5</td>
<td>b/g/n</td>
<td>2.432</td>
</tr>
<tr>
<td>6</td>
<td>b/g/n</td>
<td>2.437</td>
</tr>
<tr>
<td>7</td>
<td>b/g/n</td>
<td>2.442</td>
</tr>
<tr>
<td>8</td>
<td>b/g/n</td>
<td>2.447</td>
</tr>
<tr>
<td>9</td>
<td>b/g/n</td>
<td>2.452</td>
</tr>
<tr>
<td>10</td>
<td>b/g/n</td>
<td>2.457</td>
</tr>
<tr>
<td>11</td>
<td>b/g/n</td>
<td>2.462</td>
</tr>
<tr>
<td>Channel</td>
<td>Protocol</td>
<td>Frequency (GHz)</td>
</tr>
<tr>
<td>---------</td>
<td>----------</td>
<td>----------------</td>
</tr>
<tr>
<td>12</td>
<td>b/g/n</td>
<td>2.467</td>
</tr>
<tr>
<td>13</td>
<td>b/g/n</td>
<td>2.472</td>
</tr>
<tr>
<td>14</td>
<td>b/g/n</td>
<td>2.487</td>
</tr>
<tr>
<td>184</td>
<td>a/n/ac</td>
<td>4.92</td>
</tr>
<tr>
<td>188</td>
<td>a/n/ac</td>
<td>4.94</td>
</tr>
<tr>
<td>192</td>
<td>a/n/ac</td>
<td>4.96</td>
</tr>
<tr>
<td>196</td>
<td>a/n/ac</td>
<td>4.98</td>
</tr>
<tr>
<td>208</td>
<td>a/n/ac</td>
<td>5.04</td>
</tr>
<tr>
<td>212</td>
<td>a/n/ac</td>
<td>5.06</td>
</tr>
<tr>
<td>216</td>
<td>a/n/ac</td>
<td>5.08</td>
</tr>
<tr>
<td>34</td>
<td>a/n/ac</td>
<td>5.17</td>
</tr>
<tr>
<td>36</td>
<td>a/n/ac</td>
<td>5.18</td>
</tr>
<tr>
<td>38</td>
<td>a/n/ac</td>
<td>5.19</td>
</tr>
<tr>
<td>40</td>
<td>a/n/ac</td>
<td>5.2</td>
</tr>
<tr>
<td>42</td>
<td>a/n/ac</td>
<td>5.21</td>
</tr>
<tr>
<td>44</td>
<td>a/n/ac</td>
<td>5.22</td>
</tr>
<tr>
<td>46</td>
<td>a/n/ac</td>
<td>5.23</td>
</tr>
<tr>
<td>48</td>
<td>a/n/ac</td>
<td>5.24</td>
</tr>
<tr>
<td>50</td>
<td>a/n/ac</td>
<td>5.25</td>
</tr>
<tr>
<td>52</td>
<td>a/n/ac</td>
<td>5.26</td>
</tr>
<tr>
<td>56</td>
<td>a/n/ac</td>
<td>5.28</td>
</tr>
<tr>
<td>58</td>
<td>a/n/ac</td>
<td>5.28</td>
</tr>
<tr>
<td>60</td>
<td>a/n/ac</td>
<td>5.29</td>
</tr>
<tr>
<td>64</td>
<td>a/n/ac</td>
<td>5.3</td>
</tr>
<tr>
<td>100</td>
<td>a/n/ac</td>
<td>5.5</td>
</tr>
<tr>
<td>104</td>
<td>a/n/ac</td>
<td>5.52</td>
</tr>
<tr>
<td>108</td>
<td>a/n/ac</td>
<td>5.54</td>
</tr>
<tr>
<td>112</td>
<td>a/n/ac</td>
<td>5.56</td>
</tr>
<tr>
<td>116</td>
<td>a/n/ac</td>
<td>5.58</td>
</tr>
<tr>
<td>120</td>
<td>a/n/ac</td>
<td>5.5</td>
</tr>
<tr>
<td>124</td>
<td>a/n/ac</td>
<td>5.62</td>
</tr>
<tr>
<td>128</td>
<td>a/n/ac</td>
<td>5.64</td>
</tr>
<tr>
<td>132</td>
<td>a/n/ac</td>
<td>5.66</td>
</tr>
<tr>
<td>Channel</td>
<td>Protocol</td>
<td>Frequency (GHz)</td>
</tr>
<tr>
<td>---------</td>
<td>----------</td>
<td>----------------</td>
</tr>
<tr>
<td>136</td>
<td>a/n/ac</td>
<td>5.68</td>
</tr>
<tr>
<td>140</td>
<td>a/n/ac</td>
<td>5.7</td>
</tr>
<tr>
<td>149</td>
<td>a/n/ac</td>
<td>5.745</td>
</tr>
<tr>
<td>152</td>
<td>a/n/ac</td>
<td>5.76</td>
</tr>
<tr>
<td>153</td>
<td>a/n/ac</td>
<td>5.765</td>
</tr>
<tr>
<td>153</td>
<td>a/n/ac</td>
<td>5.765</td>
</tr>
<tr>
<td>157</td>
<td>a/n/ac</td>
<td>5.785</td>
</tr>
<tr>
<td>160</td>
<td>a/n/ac</td>
<td>5.8</td>
</tr>
<tr>
<td>161</td>
<td>a/n/ac</td>
<td>5.805</td>
</tr>
<tr>
<td>161</td>
<td>a/n/ac</td>
<td>5.805</td>
</tr>
<tr>
<td>165</td>
<td>a/n/ac</td>
<td>5.825</td>
</tr>
</tbody>
</table>

### 15.20 Send Device Analytics to a Third-Party Server

An Arista access point (AP) can send Received Signal Strength Indicator (RSSI) values of associated and unassociated visible WiFi clients, and neighboring Arista APs to an external third-party server. The data shared with a third-party server include:

- LAN MAC of the neighboring Arista AP or client
- RSSI value
- Band: 2.4 GHz or 5 GHz
- Time stamp
- Type: client or AP
- Transmit channel

The AP sends this data as a JSON or CSV file at a recurring interval that you can configure.

Perform the following steps in CloudVision WiFi to send the RSSI data to a third-party server:

1. Select the location at which you want APs to send analytics information to third-party servers.
2. Go to **CONFIGURE > Device Settings > Device**.
3. Scroll down and select the **Push Visibility Analytics to Third-Party Server** check box.
4. Configure the fields shown in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visibility Analytics Format</td>
<td>You can view the analytics data in CSV or JSON format.</td>
</tr>
<tr>
<td>Server URL</td>
<td>The URL of the third-party server.</td>
</tr>
<tr>
<td>Authorization</td>
<td>You can choose the authorization mechanism used by the AP to communicate with the third-party server. Provide either an authorization key, or a username and password.</td>
</tr>
<tr>
<td>Send Interval</td>
<td>The interval in seconds at which the AP sends RSSI values to the server.</td>
</tr>
</tbody>
</table>

5. Save the settings.
Configure a Group

Once the group is created successfully, you can configure it. You can configure a group in two ways. Firstly, you can switch on an available SSID for the group. This will apply the configuration of the SSID to the group. Or, if you do not wish to switch on the SSID, then you can simply configure and save the Device and Radio Settings to apply these settings to the group. For a detailed, stepwise procedure to apply configuration to groups refer Apply configuration on a group by switching on the SSID.

16.1 Apply configuration to a group by switching on the SSID.

To configure a group by switching on the SSID:

1. Navigate to CONFIGURE -> Wi-Fi -> SSID.
2. Click on the hamburger icon (three horizontal lines) on the top left corner of the page.
3. Expand the list of groups, available at the bottom of the location pane.
4. Select the group to which you would like to apply the configuration.
   On selecting the group the list of SSIDs on the right hand side panel is refreshed.
5. Turn ON the desired SSID from the list of SSIDs.

On successful execution of the above steps the configuration of the SSID will be applied to the selected Group.

16.2 Copy Configuration from a Folder/Group

This option allows you to copy WiFi configuration settings from a folder/group to an another folder/group.

To copy the settings to a different location or group, perform the following steps:

1. Go to Configure > WiFi.
   This takes you to the SSID tab by default.
2. Select the location where you want to copy the WiFi settings and click Copy Configuration from a Folder/Group.
   This opens a Select Folder or Group window on the right pane.
3. **Under the Select Folder tab, select the location whose settings you want to copy.**

4. **Click Copy Configuration.**
   A pop-dialog appears asking you whether to replace the existing settings with the selected folder.

5. **Click Continue in the pop-up dialog to copy the Wi-Fi configuration to the selected location.**
   Similarly, you can copy the settings of a group at a location to another group at a different location using Groups Navigator.
Chapter 17

Configure Alerts

CloudVision WiFi allows you to configure the behavior of each alert under **Configure > Alerts**. You can define the severity level of an alert, select what means are used to notify administrators of an alert, and—in the case of System and WIPS alerts—decide whether or not an alert affects the security status of your network.

Like many other policies, the configuration of alerts is a location-based policy, i.e., an alert defined at a location is inherited by its child locations. You can customize the alert configuration at a child location to break the inheritance from the parent location. An alert is raised at the location of the device that triggers the alert. You can also **Download Alerts** as a "tsv" file.

The following sections discuss the configuration of WiFi, WIPS, and System alerts in detail.

17.1  **Configure WiFi Alerts**

You can define when WiFi alerts occur and how a network administrator is notified. Certain alerts can only be enabled or disabled, e.g., an alert for a client connectivity test failure, while others additionally have configurable thresholds. By defining thresholds, an administrator can configure alerts for events that cross these thresholds and need attention. An alert is raised when the actual value exceeds the configured threshold, e.g., an alert based on the number of clients associated with an access point exceeding the configured threshold. You can also configure how alerts should be communicated: on the UI or sent via email, Syslog messages, or SNMP traps.

Let's discuss two examples of how WiFi alerts can be configured.
Example 1: Poor Client Performance Alert

Suppose that you want CloudVision WiFi to raise an alert whenever the number of clients affected by poor performance on the 5 GHz band across all your SSIDs exceeds a threshold. As shown in the figure above, you can configure such an alert as follows:

- Select Baseline alerts under WiFi.
- Select "Clients Affected by Poor Performance" as the metric.
- Select "Any" SSID and the "5 GHz" band.
- Define the threshold in terms of the percentage value above which you want an alert to be raised.
- Select "Email" and "Display" to send an email to the administrator and show the alert on the UI.
Example 2: DHCP Latency Alert

Suppose that you want CloudVision WiFi to raise an alert if the DHCP latency for a particular SSID exceeds a threshold, and you want to notify a Syslog/SNMP server of this alert. As shown in the figure above, you can configure such an alert as follows:

- Select Performance alerts under WiFi.
- Select “DHCP” as the component for which latency triggers the alert.
- Select the SSID and “Any” band.
- Define the latency threshold above which you want an alert to be raised.
- Select all the notification types for the alert.

17.2 Configure WIPS Alerts

Let us look at an example WIPS alert configuration.
Example: Banned AP Active

If a banned AP becomes active, it could pose a serious threat to your network. As shown in the figure above, you can configure the "Banned AP active" alert as follows:

- Set the Severity of the alert to "High".
- Have this alert displayed on the UI under Monitor > Alerts > WIPS.
- Send an email to an administrator and notify an external entity such as a Syslog server about this alert.
- Have the alert affect the security status of your network.

WIPS Alert Types

The table below lists the WIPS alert types with descriptions and examples.

<table>
<thead>
<tr>
<th>WIPS Alert Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rogue AP</td>
<td>Alerts for any potentially rogue APs. Examples: Unauthorized AP connected to the enterprise wired network, Banned AP, Unauthorized AP on non-allowed channels.</td>
</tr>
<tr>
<td>WIPS Alert Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Misconfigured APs</td>
<td>Alerts for any AP behavior that deviates from the authorized WiFi policy.</td>
</tr>
<tr>
<td></td>
<td>Examples: Change in an authorized AP's SSID, No encryption on an authorized AP.</td>
</tr>
<tr>
<td>Misbehaving Clients</td>
<td>Alerts for any client behavior that could compromise network security.</td>
</tr>
<tr>
<td></td>
<td>Examples: Authorized client association with an external AP, Unauthorized client association with an authorized AP.</td>
</tr>
<tr>
<td>Man-in-the-middle</td>
<td>Alerts for potential man-in-the-middle type attacks.</td>
</tr>
<tr>
<td></td>
<td>Examples: Honeypot/evil twin active, PS-poll attack.</td>
</tr>
<tr>
<td>MAC Spoofing</td>
<td>Alerts for AP and client MAC spoofing.</td>
</tr>
<tr>
<td>Ad-hoc Network</td>
<td>Alerts for an authorized client participating in an ad-hoc network.</td>
</tr>
<tr>
<td>Prevention</td>
<td>Intrusion prevention related alerts.</td>
</tr>
<tr>
<td></td>
<td>Examples: Device reached maximum prevention capacity, AP/client needs to be prevented.</td>
</tr>
<tr>
<td>DoS</td>
<td>Alerts for potential DoS type attacks.</td>
</tr>
<tr>
<td></td>
<td>Examples: Disassociation flood attacks, Deauthentication flood attacks.</td>
</tr>
</tbody>
</table>

### 17.3 Configure System Alerts

System alerts are triggered by events related to the WiFi server (e.g., the active server switches to the standby server) or the AP/Sensor (e.g., a new network is detected). You can define the severity of a system alert and choose how to notify a user. You can also select if the alert affects the security status of your network; for example, when a server stops, some WIPS functionality is lost, which could make your network vulnerable.
Example: New network detected

When a new network is detected, CloudVision WiFi generates an alert as shown in the figure above. You can configure this alert as follows:

- Set the Severity of the alert to "Low".
- Display this alert on the UI.
- Do not send an email to an administrator.
- Notify an external entity such as a Syslog server about this alert.
- Do not have the alert affect the security status of your network.

17.4 Alerts Auto-Deletion

You can specify the duration to retain alerts on the server. After the specified duration, the alerts are automatically deleted.

Follow these steps to auto-delete alerts:

1. Go to CONFIGURE > Alerts.
2. In the Configure Alerts tab, click Auto Deletion.
3. From the Auto Deletion right panel, specify the number of security and system alerts that you want to retain.
4. Specify the duration to retain alerts.
5. Save the settings.
Alerts are categorized into three types: WiFi, System, and WIPS (see the sections below for details) and are further classified as follows, based on the nature of events that trigger the alerts.

- **Instantaneous** - Alerts generated for events that are instantaneous, i.e., one-off events that do not persist over time. For example, the failure of a scheduled client connectivity test is an instantaneous WiFi alert. Similarly, an authorized client probing for a vulnerable SSID is an instantaneous WIPS alert.

- **Live** - Alerts generated for events that persist over time. These alerts are triggered by some condition and persist until the condition holds true. For example, the number of clients experiencing authentication failure exceeding a threshold is a WiFi alert that persists over time. Similarly, a rogue AP becoming active is a WIPS alert that persists over time.

- **Expired** - A live alert expires when the condition that triggered the alert no longer holds true.

### 18.1 Monitor WiFi Alerts

Under **Monitor > Alerts > WiFi**, you can review WiFi alerts that have been configured to be displayed on the UI.

![Alerts screenshot](image)

WiFi alerts capture network connectivity and performance events such as client authentication failures and high latencies. As shown in the figure above, alerts are categorized by the aspect of the WiFi network that they pertain to—for example, client connectivity test or connection failure. You can mark a WiFi alert as "Read" or "Unread" and you can delete it.
18.2 Monitor WIPS Alerts

Under Monitor > Alerts > WIPS, you can review WIPS alerts that have been configured to be displayed on the UI.

WIPS alerts are related to WiFi vulnerabilities and attacks that may pose a security threat to your network. You can turn on or off the security status of a WIPS alert, i.e., decide whether an alert affects the security status of your network. A network administrator can acknowledge an alert. This then shows up in the acknowledgment trail that other administrators can check to know which user has acknowledged an alert. Wherever needed, WIPS alerts have recommended actions that you can undertake to secure your network.

18.3 Monitor System Alerts

Under Monitor > Alerts > System, you can review System alerts that have been configured to be displayed on the UI.
Monitor Alerts

System alerts are for events related to the overall health of the WiFi server and infrastructure, e.g., when a WiFi server switches from active to standby or an AP gets disconnected from the network. As shown in the figure above, they are categorized into Server or AP/Sensor alerts. You can change whether an alert affects the security status of your network. For example, when a server stops, some WIPS functionality is lost, which could make your network vulnerable. Like WIPS alerts, a network administrator can acknowledge and check acknowledgment trails for a system alert. Wherever needed, system alerts have recommended actions that you can undertake to address the issue.

18.4 Security Status

An alert is raised at the location of the device that triggers the alert. Security status shows you which locations in your network are vulnerable, i.e., which locations have live security alerts. As shown below, from the menu icon (three vertical dots) on a location, you can select Show Status > Security Status to see a color-coded view of network vulnerability: red for locations that are vulnerable and green for locations that aren't. Whether or not a WIPS or System alert contributes to the security status can be set while configuring those alerts.
<table>
<thead>
<tr>
<th>Access Point Classification</th>
<th>Authorized</th>
<th>Rogue</th>
<th>External</th>
<th>Uncategorized</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Status</td>
<td>Vulnerable</td>
<td>42</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Intrusion Prevention Status</th>
<th>Access Points</th>
<th>Clients</th>
</tr>
</thead>
</table>
Wireless Intrusion Prevention Techniques

A large number of WiFi devices-access points (APs) and clients-are commonly present in the vicinity of an enterprise. While most are legitimate devices, belonging either to the enterprise or businesses around it, manually tracking the presence of any threat-posing devices among them or WiFi connections violating the enterprise security policy is impractical.

Arista wireless intrusion prevention system (WIPS) can automate that process and protect enterprise networks from WiFi-based vulnerabilities and attacks. It can also track the physical location of WiFi devices on enterprise premises.

Arista WIPS uses a variety of patented techniques to classify WiFi devices automatically and accurately as follows.

- Authorized: Owned and officially deployed by the enterprise,
- External: Legitimate WiFi devices in the enterprise vicinity, and
- Rogue: Unauthorized WiFi devices on the enterprise network.

This serves as the foundation for enforcing WiFi security policies. Based on the accurate device classification, Arista WIPS can automatically block threat-posing WiFi devices and connections (shown in red in the figure below).

You can enable automatic intrusion prevention using Arista CloudVision WiFi, by navigating to Configure--> WIPS--> Automatic Intrusion Prevention or from Dashboard--> WIPS

Depending on the type of threat, intrusion prevention can be defined in the following ways.

**Access Point Prevention**

To automatically block all connections to threat-posing APs such as rogue APs, banned APs, and misconfigured APs.

**Client Prevention**

To automatically prevent client connections based on the type of client involved, e.g., authorized, guest, rogue, external, banned, and the type of AP (or client) to which it tries to connect. Thus, **Client**
Prevention can block various types of threat-posing WiFi connections, e.g., an authorized client could be blocked from connecting to an external AP that is a WiFi hotspot while allowing other external clients to connect to that AP; an unauthorized client could be blocked from connecting to an authorized AP while allowing authorized clients to connect to that AP.

Threat Prevention

Arista WIPS can also be configured to automatically protect enterprises from malicious WiFi-based attacks such as:

1. **ARP spoofing/MAC spoofing**: In ARP spoofing, an attacker sends a spoofed ARP reply, on behalf of an authorized AP, for a legitimate connection request by a WiFi client. The reply contains the spoofed MAC address of the legitimate AP and links with the legitimate IP address, thus establishing the connection between them. The attacker can potentially receive all the data intended for the legitimate user.

2. **Honeypot**: In a honeypot or man-in-the-middle attack, an unauthorized AP, in the vicinity of an enterprise, tries to lure authorized enterprise clients to connect to it by broadcasting the same SSID as an authorized one, but at a higher RSSI. An attacker could also launch multiple honeypots (aka multipots) simultaneously to evade security.

3. **DoS Attack**: By using a variety of techniques, an attacker can flood an enterprise network with a number of junk WiFi frames or frames that consume a significant amount of airtime, starving legitimate APs and clients from transmitting, thus, disrupting the WiFi service of the legitimate users.

Such severe attacks/threats can make the user information vulnerable. Arista WIPS automatically classifies the APs in the vicinity as authorized, rogue, or external in compliance with the AP auto-classification policy. Classification helps to alert the system of any vicious activity by an AP other than the authorized ones by defining Intrusion Prevention Levels. To safeguard, WIPS has some Intrusion Prevention Methods:

1. **Inline**: It is the background scanning done by the third radio of an AP. An inline technique is majorly acquired in the absence of WIPS or when automatic intrusion prevention is turned off. When a client sends a request for connection, the AP detects the client as rogue or authorized as per the client auto-classification policy already defined. If it is rogue, the AP keeps on discarding the request packets on the driver level itself but if it is an authorized client the AP itself authenticates it. This happens for both open and encrypted APs.

2. **De-Auth**: This technique is useful to prevent the authorized connection by sending the de-auth packets in compliance with the 802.11 messaging format for disconnecting the unauthorized ones. When a misbehaving client connects to a rogue AP and tries to access the network, the authorized AP senses the unauthorized connection and unicasts a de-auth packet to the client. By sending de-auth packets, the connection is disrupted with the rogue AP. For encrypted Adhoc client prevention, where prevention beacons are sent can also be prevented using the same technique. This can also happen in offline mode. Offline Mode- When an AP is in online mode, it keeps on receiving and storing the data of all the rogue or misconfigured connections in a list as defined by AP auto-classification. So, even when the AP goes into offline mode, this list helps to detect the rogue APs and automatically prevent any activity from them.

3. **Wireless ARP Prevention**: ARP poisoned packets are sent over a network when the multipot attack happens where the transit between multiple APs is so fast that the de-authentication technique is not effective. So, the WIPS sensor sends a spoofed de-authentication packet with a spoofed MAC address over the wireless medium, thus, preventing any authorized clients to connect to a rogue AP.

4. **Wired ARP**: Any activity from a rogue AP should be detected and disabled. When any unauthorized activity is detected, poisoned ARP packets are sent on open Adhoc or wired connections as well. Wired ARP technique also takes place when the defined intrusion prevention level capacity becomes full. For example, if we had selected "Block" level which prevents one channel per radio and a threat posing device is detected then we switch to wired ARP. With this technique, ARP poisoning packets are sent from the wired interface to prevent any wireless clients to connect to
the secured wired network through a rogue AP. The packets are unicast to the authorized client, thus, not affecting the other connections.

5. Selective NAV: The prevention technique is used for Dos attacks. DoS attacks can prove harmful as they disrupt the legitimate receiver from any services. To mitigate this attack, WIPS allows the APs to allow a definite time slot for the clients. In this way, the rogue AP trying to flood the network with useless packets never gets a chance to connect.

6. Cell Splitting: Cell splitting is used to prevent encrypted ad hoc wifi mode where fake beacons are sent with random cell id so that the clients in ad hoc mode think that the preventing device is the ad hoc owner while the id keeps on changing randomly where the owner actually never settles on a particular cell id.

19.1 Intrusion Prevention Level

Arista WIPS offers four levels of automatic intrusion prevention, listed below.

<table>
<thead>
<tr>
<th>Level</th>
<th>Number of channels-per-radio prevented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block</td>
<td>1</td>
</tr>
<tr>
<td>Disrupt</td>
<td>2</td>
</tr>
<tr>
<td>Interrupt</td>
<td>3</td>
</tr>
<tr>
<td>Degrade</td>
<td>4</td>
</tr>
</tbody>
</table>

Each automatic intrusion prevention level defines the number of channels-per-radio that an AP can prevent. To detect an intrusion, an AP radio scans all the channels in its frequency band of operation, spending 120 ms on each channel. One scan cycle is the time it takes an AP radio to complete scanning all the channels once. At each level, Arista WIPS can prevent up to 10 intruding devices.

Consider an AP whose intrusion prevention level is set to “Block”. Suppose this AP detects an intrusion on channel 36. Since the level is set to “Block”, the AP can prevent one channel per band—in this case, channel 36. Then, during its scan cycle, the AP “visits” channel 36 more frequently, sending deauthentication packets to block the unwanted communication on channel 36. (Intrusions subsequently detected on other channels are put in a “Pending” list.) If the intrusion prevention level is set to “Disrupt” and the AP detects intrusions on two channels, then it divides the time it spends sending deauthentication packets between the two channels. This disrupts the unwanted communication on each of the two channels but doesn’t block it completely. “Disrupt” is, therefore, a weaker form of prevention than “Block”; some packets belonging to the intruding device may get through. This logic extends to “Interrupt” and “Degrade” as well—these levels respectively interrupt and degrade the unwanted communication; they do not disrupt or block it.

So the trade-off is between the effectiveness of intrusion prevention and its coverage—in terms of the number of channels across which threats can be prevented. Larger the number of channels-per-radio prevented, the weaker the prevention since the AP has to divide the time it spends sending deauthentication packets among a larger number of channels. Choose the intrusion prevention level based on the needs of your WiFi environment. By default, the intrusion prevention level is set to “Disrupt”.

19.2 Authorized WiFi Policy

Arista wireless intrusion prevention system (WIPS) uses a variety of patented techniques to automatically and accurately classify WiFi access points (APs) and clients as follows.

- Authorized: Owned and officially deployed by the enterprise,
• External: Legitimate WiFi devices in the enterprise vicinity, and
• Rogue: Unauthorized WiFi devices on the enterprise network.

An Authorized WiFi Policy forms the basis of this automatic device classification; it can be defined in terms of:

1. The characteristics of the official enterprise WiFi network, e.g., SSID name, whether or not the SSID is a guest SSID, the type of authentication and encryption used, a mapping of SSIDs to specific enterprise subnetworks they are allowed to run on, allowed vendors, etc.

2. A pre-classification of WiFi APs as potentially authorized or rogue based on whether or not they are connected to one of the monitored enterprise subnetworks (enabled by default), or based on the signal strength (RSSI) with which those APs are visible to Arista WIPS.

You can implement an authorized WiFi policy in two ways: either using the SSID Profile settings to validate the configuration running on your Arista WiFi APs or by creating an Authorized WiFi Profile for each SSID. Each method is described below.

Using SSID Profile Settings

You may choose to simply leverage the settings of the SSID Profiles in use to validate the configuration running on the enterprise WiFi APs: this can be done by enabling the Use SSID Profiles to verify managed access point configuration option as shown below.

Note: This option is enabled by default. You will have to disable it if you choose to define your enterprise authorized WiFi policy in terms of Authorized WiFi Profiles.

Authorized WiFi Profile per SSID

The figure below shows an Authorized WiFi Profile for a corporate SSID. The SSID must conform to the restrictions set by the profile. For example, the SSID must run on an Arista AP because that's the only allowed AP vendor; similarly, it must use PSK authentication.
When an SSID configuration does not match the authorized WiFi policy, the SSID is marked as a Misconfigured SSID. As shown in the figure below, you can filter on the **Classification** column under **Monitor > WIPS > Access Points** to find APs running misconfigured SSIDs.
You can select an AP to see the SSIDs that are misconfigured and to view the reasons for the configuration mismatch. Active APs running misconfigured SSIDs are marked orange on the Monitor > WIPS and the Monitor > WiFi tabs.

19.3 Access Point Auto Classification

Arista wireless intrusion prevention system (WIPS) continuously scans the WiFi frequency spectrum to detect other WiFi devices present in the vicinity.

Whenever a new WiFi AP is detected, it is initially considered to be uncategorized. Arista's unique <Marker Packets> technology helps determine whether or not the detected AP is connected to the enterprise wired network. If an AP is on the enterprise wired network, it is pre-classified as Potentially Authorized or Potentially Rogue, depending on whether or not the AP complies with the Authorized WiFi Policy. If the AP is not on the enterprise wired network, it is pre-classified as Potentially External. The pre-classification is an advanced setting under Authorized WiFi Policy.
Arista managed APs that are on the wired network and comply with the <Authorized WiFi Policy> are automatically classified as Authorized. The AP Auto-Classification Policy allows you to let the Arista WIPS automatically classify potentially rogue APs as rogue APs and potentially external APs as external APs. By default, the AP auto-classification is enabled. You can edit the policy under Configure--> WIPS--> Access Point Auto-Classification.

You can also freeze the list of your authorized APs by using the <Authorized AP List Locking> feature so that no more APs get automatically classified as authorized.

19.4 Client Prevention

Client prevention allows you to choose the types of WiFi client communication you want to prevent.

The types of client communication are based on two factors:

- The type of the client (Rogue, Authorized, External, or Guest) as determined by Client auto-classification.
- The device that the client attempts to connect to—Authorized access point (AP), other clients, etc.

The examples below show how specific client types and connection attempts can be prevented depending on the use case.

**Authorized Client Misassociation**

An authorized enterprise WiFi client could attempt to associate with access points in the vicinity of your enterprise. To protect authorized clients on an enterprise WiFi network, you might want to prevent them from associating with any non-authorized APs as shown below.
Client Bridging/ICS

Client bridging is when a laptop connected to the wired network acts as an access point, thereby allowing unauthorized clients access to an enterprise network. Internet Connection Sharing (ICS) is a service that turns a computer into a router to which other clients can connect directly. Both methods compromise the security of an enterprise Wi-Fi network by exposing it to unauthorized access. To prevent client bridging or ICS, you can enable the relevant prevention as shown below.

Unauthorized Associations To Authorized Access Points

For guest WiFi access, suppose that your Client Auto-Classification is configured to re-classify all External and Uncategorized clients connecting to a Guest SSID as "Guest". In that case, you do not want to prevent unauthorized clients from accessing an authorized AP running the Guest SSID because an unauthorized client needs to associate with an authorized AP before it can be marked as a "Guest" client. You can allow such associations by not enabling prevention as shown below.

19.5 Client Auto-Classification

Classifying WiFi clients can help you automatically enforce your WiFi security policies.

Usually, clients are classified as:

- **Authorized**: These are enterprise-owned, managed clients that are expected to comply with the enterprise security policies, e.g., they are allowed to connect to the enterprise-managed WiFi access points (APs) but not to other APs.
- **Guest**: These are clients that are brought along by visitors in your organization. Guest clients are normally allowed to connect to the guest WiFi network for Internet access and have limited or no access to the internal network.
Wireless Intrusion Prevention Techniques

- **External**: These are unmanaged clients detected in the vicinity of your enterprise. They are normally blocked from connecting to your managed APs but could connect to other APs. Such clients could be typically ignored unless their behavior poses a threat to your enterprise security.

- **Rogue**: These are typically unauthorized clients that try to intrude into your enterprise network, for instance, by connecting to a rogue AP. The activity of such clients should be monitored and their unauthorized access should be blocked.

Manually keeping track of the list of clients that are authorized to access your enterprise WiFi network is not scalable and is prone to errors, especially in large organizations. Arista CloudVision WiFi provides a simpler way to automatically classify clients. The client auto-classification policy settings are available under **CONFIGURE > WIPS > Client Auto-Classification**.

By default, clients are left uncategorized initially and classified based on the type of AP or WiFi network they connect. You can optionally choose to classify any newly discovered client as either External, Authorized, or Guest, and let them be reclassified based on association. Association-based classification can be based on the type of AP that the client connects to. For example, an uncategorized client attempting to connect to any external AP is classified as external.

The examples below show how clients can be auto-classified depending on their association.

### Clients Connecting to Authorized Access Points

Depending on the initial classification, the clients connecting to your authorized access points can be reclassified based on their association. A sample screenshot showing the default values is shown below. You can change the settings based on your security policy.

![Clients Connecting to Authorized Access Points](image)

### Clients Connecting to Rogue Access Points

A client may attempt to associate with a rogue AP. In such a case, reclassification is based on the initial classification of the client and on the classification of an AP. In this scenario, AP could be rogue or potentially rogue.
Note: Once the client is manually classified as Rogue or Authorized, it is not reclassified automatically unless it is deleted and discovered again.

19.6 Banned Device List

You can ban certain WiFi devices from accessing the enterprise network when needed. For instance, if an enterprise laptop gets stolen, its unauthorized access to the enterprise network needs to be restricted.

To prevent such access, you can add those WiFi access points or clients to the Banned Access Points and Banned Clients, respectively. This can be done either by entering the MAC addresses of the individual access points or clients or by uploading a .csv file with the list of comma-separated MAC addresses. The banned devices can be defined only at the topmost or root folder of the location tree.

In addition, you can configure an alert that will warn you if a banned access point or client from the list is detected in the vicinity. WiFi connectivity with a banned access point or client can also be prevented automatically by configuring the relevant intrusion prevention policy.

19.7 WLAN Integration

Whether you are using Arista WIPS or transitioning to cloud-based WiFi, integrating the Arista Cloud WiFi server with your on-premises WLAN controller allows you to leverage key advantages of the cloud server while continuing to use your controller-based WLAN.

The Arista cloud-based WiFi server fetches information about access points, clients, and signal strengths from WLAN controllers using Simple Network Management Protocol (SNMP). Arista WIPS can then use this information to automatically classify authorized devices managed by the controller and track WiFi client locations.

Arista supports integration with Aruba Mobility Controllers and Cisco WLC.

19.7.1 Configure WLAN Integration

To add WLAN controllers, go to System > WIPS > WLAN Integration in CloudVision WiFi. Select whether you want to add an Aruba or a Cisco controller, and click Add on the Wireless LAN Controllers grid. The Add Controller panel shown in the figure below opens up. Enter the settings (described in the table below) and click Done. Note that, as shown in the figure below, if your controller uses a private IP address, then you will need a Cloud Integration Point to integrate the controller with the Arista Cloud.
On the main WLAN Integration tab, set the Automatic Synchronization Interval; this is the interval that defines how frequently the Arista Cloud fetches information from the controller. Save the settings to complete adding the controller.
### 19.7.2 Controller Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller (IP Address/Hostname)</td>
<td>Enter the IP address or hostname of the controller.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If the controller uses a private IP address, you need to select a Cloud Integration Point.</td>
</tr>
<tr>
<td>Port Number</td>
<td>The controller port number from which data is imported.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Primary Cloud Integration Point (CIP)</td>
<td>From the drop-down list, select an Arista device that you want to use as the primary Cloud Integration Point (CIP) for this controller.</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong> You must open port number 3852 in your network from the CIP to Arista cloud.</td>
</tr>
<tr>
<td>Secondary Cloud Integration Point (CIP)</td>
<td>From the drop-down list, select an Arista device that you want to use as the secondary Cloud Integration Point (CIP) for this controller.</td>
</tr>
<tr>
<td></td>
<td>If the primary CIP goes down, the secondary one ensures connectivity of your service to the cloud.</td>
</tr>
<tr>
<td>SNMP Version</td>
<td>Select SNMP V2 or V3 for the Arista cloud communication with the controller.</td>
</tr>
<tr>
<td>Community String</td>
<td>User-defined community string using which Arista cloud communicates with the controller. The default value is ‘public’.</td>
</tr>
<tr>
<td>Import</td>
<td>Select to enable the import of data from the controller.</td>
</tr>
<tr>
<td>Managed Access Points</td>
<td>Select to import managed access point information from the controller.</td>
</tr>
<tr>
<td>Managed Clients</td>
<td>Select to import information about clients associated with access points managed by the controller.</td>
</tr>
<tr>
<td>Unmanaged Access Points</td>
<td>Select to import information about access points not managed by the controller.</td>
</tr>
<tr>
<td>Unmanaged Clients</td>
<td>Select to import information about clients associated with access points not managed by the controller.</td>
</tr>
<tr>
<td>Signal Strength</td>
<td>Select to import signal strength information from the controller.</td>
</tr>
</tbody>
</table>

19.8 **Monitor Networks**

Under **Monitor > WIPS > Networks**, you can see the networks being monitored by WIPS. As shown below, networks that are not being monitored (because they are unreachable) are shown in red.
Card Dataholder Environment (CDE) networks are networks that store, process, or transmit payment card transactions and sensitive cardholder data. CDE networks are in the scope of PCI DSS compliance. You can right-click on a network and change its type from CDE to Non-CDE or vice versa.

19.9 Auto-Deletion Settings

Using auto-deletion settings, you can specify parameters to automatically rogues access points (APs) and clients.

You can automatically delete the following items:

- APs
- Clients
- Network
- Alerts
- Inactive Authorized APs

You must have superuser, administrator, or operator privileges to use auto-deletion settings.

19.9.1 Auto-Delete Access Points, Clients, and Network

You can specify the duration of inactivity after which rogue access points (APs) or clients are automatically deleted. For networks, you can define the duration for which the networks are retained on the server. After the specified retention duration, the networks are automatically deleted from the server. If you want to retain manually classified APs or clients, you can specify that in the auto-deletion parameters.

You can also delete authorized but inactive APs from the current location. Click Delete Inactive Authorized Access Points at the bottom of the Access Points tab.

Follow these steps to auto-delete APs, clients, and network:

1. Go to MONITOR > WIPS > Access Points.
2. Click Auto Deletion.
3. From the right pane, define the parameters to delete access points, clients, and network.
4. Save the settings.

19.10 WIPS Advanced Settings

Under Configure > WIPS > Authorized WiFi Policy, you can define Advanced Settings that allow you to pre-classify access points (APs) and define No-WiFi networks.

Access Point Pre-Classification

Pre-classification of access points helps WIPS identify potential authorized and rogue APs. As shown in the figure below, by default, access points connected to a monitored subnet are pre-classified as potentially authorized or rogue. These APs then show up with the appropriate classification on the Monitor > WIPS tab. This helps if, for instance, an unclassified AP is connected to the network. The AP appears on the Monitor > WIPS tab. You can then re-classify it appropriately as either rogue or authorized and—for rogue APs—take appropriate action.
You can also have WIPS pre-classify APs based on the signal strength with which they are visible. As shown in the figure below, if you enable signal strength based pre-classification, CloudVision WiFi allows you to define a signal strength threshold. APs with signal strength greater than the threshold are automatically classified as potentially authorized or rogue.

Relying on signal strength based classification alone, however, is not advisable, especially if you plan to enable automatic intrusion prevention. First, if a legitimate AP from a neighboring facility is visible with a signal strength higher than the threshold, then classifying it as rogue could disrupt legitimate WiFi connections to the AP. Therefore, use this classification only if you are sure that no unauthorized WiFi operates in the vicinity of your location. Second, signal strength based classification will not detect rogue APs that operate with a signal strength weaker than the threshold (smartphones running WiFi hotspots, for example).

**Define No-WiFi Networks**

Security-sensitive environments might need to ensure that no WiFi network operates at certain locations. As shown in the figure below, you can define "No-WiFi" networks for a location, i.e., specify subnets where no WiFi is allowed. If you define such networks, an AP detected on the network at that location is automatically classified as a rogue AP, even if it conforms to the authorized policy.
Wireless Intrusion Prevention Techniques

Advanced Settings

Define No WiFi Networks

Enter the networks that are not allowed to have any WiFi APs connected to them. If an AP at this location is connected to a "No WiFi" network, it will be treated as a Rogue AP even if it matches an Authorized SSID policy applied at this location. The "No WiFi" network selection takes precedence over any Authorized SSID policy templates applied at that location.

System Detected Networks

- 10.86.56.0/21
- 10.86.114.0/24
- 172.16.0.0/24

Drag into below input area.

Add Networks

- 10.86.114.0/24

Enter
Troubleshooting WiFi

The TROUBLESHOOT view in CloudVision WiFi provides tools that help the network administrators troubleshoot issues in the Wi-Fi network.

The troubleshooting tools provided by CloudVision WiFi include:

- Packet Trace
- Client Connectivity Test

20.1 Capture Packet Trace for a Client

You can perform the Capture Packet Trace action on a client to intercept a data packet that is crossing or moving over a specific network. The captured packet is stored temporarily for analysis. The packet is inspected to help diagnose and solve network problems.

To capture a packet in CloudVision WiFi:

1. Go to MONITOR > Clients.
   A list of APs seeing the client is displayed.
2. Right-click on the name of the AP or select the menu icon (three vertical dots) to view the available actions and select Capture Packet Trace.
   The Capture Packet Trace dialog box opens.
3. On the Capture tab, enter the following details and click Start Packet Capture.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeout</td>
<td>It is the time in minutes that specify the time interval for the packet trace capture. The range is from 1 min to 720 min.</td>
</tr>
<tr>
<td>Streaming Option</td>
<td>It specifies the type of packet capture to be used:</td>
</tr>
<tr>
<td></td>
<td>• Upload to server: It creates a file to capture the packet trace which can be viewed only after the entire packet capture process is complete.</td>
</tr>
<tr>
<td></td>
<td>• Wireshark on local machine: The packet trace can be opened during an ongoing capturing process.</td>
</tr>
<tr>
<td>Filename Prefix</td>
<td>It is mandatory field to specify the prefix for a filename. For example, Packet_wireless_143438.pcap, where:</td>
</tr>
<tr>
<td></td>
<td>• Packet: is the prefix of the file name.</td>
</tr>
<tr>
<td></td>
<td>• _wireless_143438: is the name of the file.</td>
</tr>
<tr>
<td></td>
<td>• .pcap: is the file extension which is compatible with Wireshark.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Wireless Settings</td>
<td>Select this option to edit advanced wireless settings.</td>
</tr>
<tr>
<td>Traffic Selection</td>
<td>It is the type of traffic that you prefer while troubleshooting.</td>
</tr>
<tr>
<td>• All packets on the channel</td>
<td>To capture all packets from all clients visible to the troubleshooting AP sensor.</td>
</tr>
<tr>
<td>• Only packets for the selected Client &lt;MAC address&gt;</td>
<td>To view only packets from the selected AP.</td>
</tr>
<tr>
<td>Packet Types</td>
<td>select the type of packets that you want to capture.</td>
</tr>
<tr>
<td>Protocol and Channel Selection</td>
<td>Select the protocols and channel for which you want to troubleshoot. If you want to select a single channel, select the Select Channel option and specify the channel number and Width (channel offset). By default, the protocol and channels are displayed based on the device template applied to the troubleshooting sensor. You can select a different protocol and/or channel, if required. Alternatively, you can select the Rotate on all Channels option, to troubleshoot on all available channels.</td>
</tr>
</tbody>
</table>

A dialog displaying the ongoing progress for the capture packet trace is displayed. Click Stop to forcibly stop the packet capture.

4. After the successful completion of the packet trace, click Download to view the file in Wireshark.

### 20.2 View Packet Trace History for a Client

You can view the Packet Trace History for a selected client. The packet traces captured only during the last 30 minutes are displayed in the history.

To view the packet trace history, perform the following steps:

The Packet Trace History displays packet traces captured in the last 30 minutes.

1. Right-click the client or select the menu icon (three vertical dots) to view the available actions.
2. Select Packet Trace History.
3. Select the History tab in the Capture Packet Trace window to view the packet capture history.
4. Select any Packet Trace to view the following detailed information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filename</td>
<td>Filename specifies the name of the captured packet trace.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>MAC Address of the device for which packet trace is captured.</td>
</tr>
<tr>
<td>Capturing Device MAC Address</td>
<td>MAC Address of the device that has captured the packet trace.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start</td>
<td>Start time of packet capture.</td>
</tr>
<tr>
<td>End</td>
<td>End time of packet capture.</td>
</tr>
<tr>
<td>Troubleshooting Mode</td>
<td>Mode of troubleshooting.</td>
</tr>
<tr>
<td>Status</td>
<td>Status specifies if the trace is completed or in progress.</td>
</tr>
</tbody>
</table>

5. Click on the three vertical dots for a packet capture file to view the available actions:

6. Choose one of the following actions:
   - Download - to download the trace file
   - Delete - to delete the trace file
   - Open - to open the trace file. You need to access Arista Packets in order to open the trace file. If Arista Packets is not accessible, the Open option is disabled.

### 20.3 Capture Packet Trace for an AP

You can troubleshoot Arista devices operating in AP or AP/Sensor mode. The packet is captured and inspected to help diagnose and solve network problems.

1. Go to **MONITOR > Access Points**.
   A list of APs that are being monitored is displayed.
2. Right-click on the name of the AP for which you want to capture the packet trace and select **Capture Packet Trace**.
   The Capture Packet Trace dialog box opens.
3. On the Capture tab, enter the following details and click **Start Packet Capture**.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeout</td>
<td>It is the time in minutes that specify the time interval for the packet trace capture. The range is from 1 min to 720 min.</td>
</tr>
<tr>
<td>Streaming Option</td>
<td>It specifies the type of packet capture to be used:</td>
</tr>
<tr>
<td></td>
<td>• Upload to server: It creates a file to capture the packet trace which can be viewed only after the entire packet capture process is complete.</td>
</tr>
<tr>
<td></td>
<td>• Wireshark on local machine: The packet trace can be opened during an ongoing capturing process.</td>
</tr>
<tr>
<td>Filename Prefix</td>
<td>It is mandatory field to specify the prefix for a filename. For example, Packet_wireless_143438.pcap, where:</td>
</tr>
<tr>
<td></td>
<td>• Packet: is the prefix of the file name.</td>
</tr>
<tr>
<td></td>
<td>• _wireless_143438: is the name of the file.</td>
</tr>
<tr>
<td></td>
<td>• .pcap: is the file extension which is compatible with Wireshark.</td>
</tr>
<tr>
<td>Wireless Settings</td>
<td>Select this option to edit advanced wireless settings.</td>
</tr>
<tr>
<td>Traffic Selection</td>
<td>It is the type of traffic that you prefer while troubleshooting.</td>
</tr>
<tr>
<td></td>
<td>• All packets on the channel: To capture all packets from all clients visible to the troubleshooting AP sensor.</td>
</tr>
<tr>
<td></td>
<td>• Only packets for the selected Client &lt;MAC address&gt;: To view only packets from the selected AP.</td>
</tr>
<tr>
<td>Protocol and Channel Selection</td>
<td>Select the protocols and channel for which you want to troubleshoot. If you want to select a single channel, select the Select Channel option and specify the channel number and Width (channel offset). By default, the protocol and channels are displayed based on the device template applied to the troubleshooting sensor. You can select a different protocol and/or channel, if required. Alternatively, you can select the Rotate on all Channels option, to troubleshoot on all available channels.</td>
</tr>
<tr>
<td>Wired Settings</td>
<td>Select this option to capture packets from wired devices.</td>
</tr>
<tr>
<td>Interface</td>
<td>Select from the available ethernet ports from the list. The default value is eth0.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>Enter the VLAN Id.</td>
</tr>
</tbody>
</table>
### 20.4 View Packet Trace History for an AP

You can view the **Packet Trace History** for a selected AP. The packet traces captured only during the last 30 minutes are displayed in the history.

To view the packet trace history, perform the following steps:

1. Right-click the AP or select the menu icon (three vertical dots) to view the available actions.
2. Select **Troubleshoot > Packet Trace History**.
3. Select the **History** tab in the **Capture Packet Trace** window to view the packet capture history.
4. Select any Packet Trace to view the following detailed information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filename</td>
<td>Filename specifies the name of the captured packet trace.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>MAC Address of the device for which packet trace is captured.</td>
</tr>
<tr>
<td>Capturing Device MAC Address</td>
<td>MAC Address of the device that has captured the packet trace.</td>
</tr>
<tr>
<td>Start</td>
<td>Start time of packet capture.</td>
</tr>
<tr>
<td>End</td>
<td>End time of packet capture.</td>
</tr>
<tr>
<td>Troubleshooting Mode</td>
<td>Mode of troubleshooting.</td>
</tr>
<tr>
<td>Status</td>
<td>Status specifies if the trace is completed or in progress.</td>
</tr>
</tbody>
</table>

5. Click on the three vertical dots for a packet capture file to view the available actions:
6. Choose one of the following actions:
   • Download - to download the trace file.
   • Delete - to delete the trace file.
   • Open - to open the trace file. You need to access Arista Packets in order to open the trace file. If Arista Packets is not accessible, the Open option is disabled.

20.5 Live Client Debugging

The Live Client Debugging feature enables you to troubleshoot client activities. You can view live the logs of a client connection.

The Live Client Debugging can be used by an user with Operator role and above. A Viewer role cannot perform the live client debugging nor access the logs.

You can perform the following tasks with the Live Client Debugging feature:

• Start Live Debugging
• Stop Live Debugging
• Archive the Debugging Log
• Download the Debugging Log
• Delete the Debugging Log
• View Live Client Debugging

20.5.1 Start Live Debugging

You can start the live debugging for one client at a time. However, you can parallelly debug maximum 10 clients on CloudVision WiFi.

To start live client debugging, perform the following tasks:

1. Navigate to MONITOR > Clients.
The page displays the list of clients on the selected folder in the Navigator that are monitored by CloudVision WiFi.

2. Right-click on the client that you want to debug and select **Start Client Live Debugging**. The Live Client Debugging page is displayed.

3. On the Live Client Debugging page, from the **Select Time Duration** drop-down list select the time duration for which the client debugging must be performed.

4. (Optional) Select **Change Location**. Use this option only when you want to track the logs of a client, for a location other than its default location. This is useful when the client is roaming across locations.

5. Select **Archive Logs** or **Discard Logs** to save or discard the client logs.

   If you select Archive, the logs are saved on the server after the time-out duration or if you stop the Live Client Debugging session. If you select Discard, the log is discarded, 30 minutes after the live debugging is stopped.

6. Click **Start** to start the live client debugging.

   You are redirected to the Live Client Debugging page, where the client logs are displayed live.

   **Note:** On the Clients page, the name of the client in bold and italics indicates that the Live Client Debugging is in progress.

The logs can be accessed as a text file. The logs contain the following information:

- Client MAC address
- SSID
- BSSID
- Name of the AP
- Channel
- Timestamp of when the log started
- Time diff in milliseconds between 2 consecutive events
- Event

A sample of the log files is as follows:

```
Client MAC: 5C:51:88:31:05:67
SSID: WebAppsDevC090
BSSID: 00:11:74:F2:17:80
AP NAME: MDJOF2:17:BF
Chan: 11
Time: 2017.04.03 11:00:21 (Aclia/Kolkata)
Tdiff (sec)  Event  Timestamp
0 2017.04.03 11:00:21  Deauthentication received from client because sending STA is leaving Node LeftSSID: WebAppsDevC090 BSSID: 00:11:74:F2:17:BF AP NAME: MDJOF2:17:BF
2 2017.04.03 11:00:21  Client successfully (re)associated
12 2017.04.03 11:00:23  First phase of WPA2-AES Handshake Completed
19 2017.04.03 11:00:23  Second phase of WPA2-AES Handshake Completed
68 2017.04.03 11:00:23  Third phase of WPA2-AES Handshake Completed
67 2017.04.03 11:00:23  Node Authorized
95 2017.04.03 11:00:23  Fourth phase of WPA2-AES Handshake Completed
95 2017.04.03 11:00:23  Client sent DHCP DISCOVER
203 2017.04.03 11:00:23  DHCP OFFER sent to Client from [172.16.100.254]
271 2017.04.03 11:00:23  Client has received IP [172.16.100.1]
272 2017.04.03 11:00:23  Client sent DHCP REQUEST
295 2017.04.03 11:00:23  DHCP ACK sent to Client from [172.16.100.254]
```

**Note:**
- You can also start Live Client Debugging from the **TROUBLESHOOT > Live Client Debugging**. Search the required client and click **Start Live Client Debugging** hyperlink located at the top-right corner of the page.
• To access the archived client logs, navigate to TROUBLESHOOT > Live Client Debugging. The name of the log in highlighted in bold italics indicates that the debugging is in progress.

20.5.2 Stop Live Debugging
You can stop a Live Client Debugging, while the debugging is in progress.

To stop the debugging session, perform the following tasks:
1. Navigate to the TROUBLESHOOT > Live Client Debugging.
   The logs that are in progress are highlighted in bold italics.
2. Right-click on any such log, and select Stop Live Debugging.
   Note: Alternatively, you can stop the debugging, by navigating to MONITOR > Clients. On the Clients page, the clients with live debugging are indicated in bold italics. Right-click the required client (in bold italics) and select Stop Client Debugging. A message is displayed that confirms that the debugging has stopped.

20.5.3 View Live Client Debugging
You can view the logs live on the Live Client Debugging page. You can view the live debugging only for those events of the client that are in progress and have not ended.

To view the live client debugging, perform the following tasks:
1. Navigate to the TROUBLESHOOT > Live Client Debugging.
   A list of logs is displayed. The logs that are still in progress are in bold and italics.
2. Right-click any such .log file and select View Client Debugging. You will be redirected to the Live Client Debugging page.
   Note: To view the Live Client Debugging, you can also navigate to MONITOR > Clients. The clients in bold and italics are the clients where live client debugging is in progress. Right-click any such client for which you want to view the live debugging logs and select Live Client Debugging. The events after opening the .log file are seen in the live debugging session. The events that occur while the Live Client Debugging is running in the background are recorded and can be downloaded. To know more about downloading a log file, refer Download Live Client Debugging Logs.

20.5.4 Delete Live Client Debugging Logs
You can delete the Live Client Debugging log files for completed sessions. You cannot delete a log file that is still in progress.

To delete the logs, perform the following tasks:
1. Navigate to the TROUBLESHOOT > Live Client Debugging.
   A list of logs is displayed.
2. Right-click on the log that you want to delete and select Delete Live Client Debugging.
3. If you want to delete multiple logs, select the logs, right-click and select Delete Live Client Debugging. A message is displayed that confirms that the logs are deleted.

20.5.5 Download Live Client Debugging Logs
You can download the logs of a Live Client Debugging session.

To download the logs, perform the following tasks:
1. Navigate to the TROUBLESHOOT > Live Client Debugging.
A list of logs is displayed.

2. Click the log name to download the file in ZIP format. Alternately, right-click the log that you want to download and select Download Live Client Debugging.

If you want to download multiple logs, select the logs, right click and select Download Live Client Debugging.

The log is downloaded as a .zip file. A customer can archive maximum 500 log files on the server. If the size of the log file reaches 2MB, the live debugging will stop after 1 minute.

20.5.6 Blinking LEDs

Suppose that for troubleshooting purposes you want to physically access an AP that is deployed on a large floor with many APs. To locate this AP, you can use the UI to make the AP LEDs blink.

To make AP LEDs blink, perform the following steps:

1. Go to Monitor > WiFi > Access Points (or Monitor > WIPS > Access Points)
2. Select the AP you want to locate.
3. Click the three-dot menu.
4. Select Troubleshooting > Start LED Blinking and the time interval for which you want the AP LEDs to continue blinking (while you physically locate it). When you click Start LED Blinking, the power, radio, and LAN LEDs of the AP blink one after another (like a moving spot of light on the AP), allowing you to easily locate the AP on the floor.

You can also follow the steps above to stop LED blinking on an AP for which you started LED blinking by selecting Troubleshooting > Stop LED Blinking in step 4 above.

You can also start (or stop) LED blinking from a floor plan. To make AP LEDs blink from a floor plan, perform the following steps:

1. Go to the Locations tab and navigate to the floor plan where the AP is placed.
2. Select the AP you want to locate.
3. Select Troubleshooting > Start LED Blinking and the time interval for which you want the AP LEDs to continue blinking.

20.6 Audit Logs

Audit logs are logs of various user actions such as logging into CVW or logging out of CVW, changes in location hierarchy, etc. Logs help in tracking user actions, which can be used for user accountability.

Only a Superuser can download audit logs or configure the audit logs retention settings.

20.6.1 Audit Log Types

<table>
<thead>
<tr>
<th>Log Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>Includes all log types</td>
</tr>
<tr>
<td>User Access</td>
<td>Logs user action related to user access such as password changes, RADIUS authentication changes, and others</td>
</tr>
<tr>
<td>Devices</td>
<td>Logs user action related to the AP such as AP name changes, AP reboot, AP firmware upgrade, and others</td>
</tr>
<tr>
<td>Alerts</td>
<td>Logs user action related to alerts such as deleting an alert</td>
</tr>
<tr>
<td>Global Settings</td>
<td>Logs user action related to global settings such as changes to Google integration, Syslog server, and SNMP settings, and so on</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Location Based Settings</td>
<td>Logs user action related to location based settings such as SSID settings, which includes firewall, role-based access control, network, and others</td>
</tr>
<tr>
<td>Location Hierarchy</td>
<td>Logs user action related to the location hierarchy such as adding or deleting a folder or group, floor map related changes, and others</td>
</tr>
<tr>
<td>Reports</td>
<td>Logs user action related to the location hierarchy such as adding or deleting a folder or group, floor map related changes, and others</td>
</tr>
<tr>
<td>Start/Stop Functions</td>
<td>Logs user action related to system services such as database, web server, and so on</td>
</tr>
<tr>
<td>System</td>
<td>Logs user action related to system related operations such as adding or deleting a network, changes in the service module, time zone related changes, and so on</td>
</tr>
<tr>
<td>Third Party and Others</td>
<td>Includes changes related to third party servers and custom files</td>
</tr>
</tbody>
</table>

### 20.6.2 Download Audit Logs

1. Click **System > Logs** to open the Audit Logs page.
2. Select the log type and specify the duration for which you want to download the logs.
3. Specify the Sort By value to sort your downloaded logs.
4. Click **Download** to download the logs in the tsv format.

### 20.6.3 Configure Audit Logs Retention Settings

You can define a custom retention period from 7 days to 365 days (both inclusive) for audit logs. You can also restore the previously set duration and reset to the system default log retention period as well. The default retention period is 10 days.

To configure the audit logs retention policy:

1. Click **System > Logs** to open the **Audit Logs** page.
2. Click **Audit Logs Retention Policy**.
3. In the right panel, specify the number of days in the **Maintain User Action Logs for last** field.
4. Save your settings.
You can add floor plans to a location in CloudVision WiFi.
You can then drag and drop APs onto the floor plan, and perform some operations on the AP from the floor plan. This helps when you want to perform some operations on an AP somewhere on the floor — for example, you might want to view the packet trace history of an AP near a user who has problems connecting to the network. You can then right-click the AP on the floor plan to view its packet trace history.

**Note:** At any location in CloudVision WiFi, you can see a card view of only the floor plans of that location and those of its immediate child locations. You will not see floor plans of locations that are further down in the location hierarchy. For example, suppose that “Town” is a child location of “West Region”, which is in turn a child location of “HQ”. Then, when you go to Floor Plans on HQ, you will see a card view of only the HQ and West Region floor plans, and not those of Town.

You can import an image or a ".spm” file as a floor plan. A ".spm” file is an Arista Planner file. Arista Planner is a tool that allows you to model obstacles and generate heat maps for coverage, link speed, etc. The ".spm” file contains a model of the obstacles on the floor — for example walls, glass partitions, and doors. This gives you a better picture of the floor. Future releases of CloudVision WiFi will allow you to view heat maps as well.

### 21.1 Add A Floor Plan

You can add floor plans to a location in CloudVision WiFi.

To add a floor plan to a location:

1. In the CloudVision WiFi location hierarchy, go to the location where you want to add the floor plan.
2. Go to Floor Plans and click Add New Floor Plan.
   An Add New Floor Plan dialog appears.
3. Enter the name you want to give to the floor plan.
4. Click Upload Image or Upload SPM.
The file selection window appears. Select the file you want to upload and click Open.
5. Set the dimensions of the floor plan.
6. Click Save to save the floor plan.

21.2 Perform Operations on an AP from Floor Plan

You can perform various operations on an AP from a floor plan.

To perform operations on the AP from a floor plan:

1. In the CloudVision WiFi location hierarchy, go to the location of the floor plan.
2. Click and open the floor plan.
3. Drag and drop APs from the right panel to wherever you want to place them on the floor plan.
4. Right-click the AP you want to perform the operations for and select the operation you want to perform.
Heat Maps

Heat Maps are used to help the user to visualize the coverage, link speed and channels of placed devices on the floor plan.

User can select different view for the floor plan to visualize the device placements, AP Coverage, AP Link Speed and AP Channel Coverage of the floor plan.

Different views for the floor plans are:

- Default View
- AP Coverage View
- AP Link Speed View
- AP Channel Coverage View

22.1 Default View

Default View shows the floor plan and placed devices on the floor.

1. Select FLOOR PLANS tab from the left panel.
2. Select the existing floor plan for which you wish to see the Default View.
3. Choose RF Heatmaps option from the right hand side panel.
4. Select Default View.

It shows Default View of the floor plan.
22.2 AP Coverage View

AP Coverage View allows user to view AP coverage for the selected floor plan. AP coverage view has floating windows that allow user to select resolution, frequency band, RSSI threshold configuration and color palette corresponding to different RSSI value range.

There are two types of filters available, Resolution and frequency. On basis of these filters the AP Coverage view can be modified. To know more about these filters refer Resolution and Frequency Filters topic.

RSSI Threshold check box if checked, allows user to view the RSSI threshold coverage as per the currently configured value for RSSI threshold. Otherwise coverage view will be shown as per the default RSSI configuration from RSSI color palette. User can change the RSSI threshold value by adjusting the scale.

To open AP Coverage View

1. Select FLOOR PLANS tab from the left panel.
2. Select the existing floor plan for which you wish to see the AP Coverage.
3. Choose RF Heatmaps option from the right hand side panel.
4. Select AP Coverage.

It shows the AP coverage on the floor plan.

22.3 AP Link Speed View

AP Link Speed view allows user to view the AP link speed for the selected floor plan. AP link speed view has floating windows that allow user to select resolution, frequency band and a color palette corresponding to different link speed value range.

There are two types of filters available, Resolution and frequency. On basis of these filters the AP Coverage view can be modified. To know more about these filters refer Resolution and Frequency Filters topic.

1. Select FLOOR PLANS tab from the left panel.
2. Select the existing floor plan for which you wish to see the AP Link Speed.
3. Choose RF Heatmaps option from the right hand side panel.
4. Select **AP Link Speed**.

It shows AP link speed for the floor plan.

---

**22.4 AP Channel Coverage View**

AP Channel Coverage View allows user to view the AP channel coverage for the selected floor plan. AP channel coverage has floating windows that allow user to select resolution, frequency band and a color palette corresponding to different channels.

There are two types of filters available, Resolution and frequency. On basis of these filters the Channel Coverage View can be modified. To know more about these filters refer Resolution and Frequency Filters topic.

1. Select **FLOOR PLANS** tab from the left panel.
2. Select the existing floor plan for which you wish to see the AP Channel Coverage.
3. Choose **RF Heatmaps** option from the right hand side panel.
4. Select **AP Channel Coverage**.

It shows AP channel coverage for the floor plan.
22.5 Resolution and Frequency Filters

Resolution and Frequency are the two filters available for heat maps. These filters are available for all the views except Default View.

Resolution Filter

Resolution filter is used to set the resolution settings for the floor plan. There are three types of resolution settings:

- **Low**: Accuracy of calculation and visualization will be low but it will take less time to show the result.
- **Medium**: Accuracy of calculation and visualization will be moderate and will take moderate time to show the result.
- **High**: Accuracy of calculation and visualization will be highest but it will take maximum time to show the output.

Frequency Filter

Frequency Filter is used to filter data based on the frequency on which AP is working. The data is filtered based on three types of criteria:

- **2.4 GHz**: Data for only 2.4 GHz AP radios will be shown.
- **5 GHz**: Data for only 5 GHz AP radios will be shown.
- **2.4 & 5 GHz**: Data for 2.4 and 5 GHz AP radios will be shown.
You can locate a specific access point (AP) or client that is added to a floor plan from the UI. You can use this feature to locate a rogue AP or client in your floor plan. However, you can’t locate multiple devices or clients. APs or clients are located based on the triangulation method.

You can locate a device from the following places in CVW:

- FLOOR PLANS
- MONITOR > WiFi > Clients
- MONITOR > WiFi > Access Points
- MONITOR > WIPS > Managed WiFi Devices
- MONITOR > WIPS > Access Points
- MONITOR > WIPS > Clients
- Alert Drilldown

### 23.1 Locationing Criteria

The server runs the locationing algorithm and, based on it, APs report another AP or client’s RSSI. Whether APs can detect another AP or client depends on three criteria:

- The AP or client must be active.
  - Clients must actively transmit data packets for locationing to work.
  - Unplaced, managed devices that operate in WIPS-only mode can’t be located.
- The device must be visible to at least three APs. At least three APs must report the device and the APs must be placed on the floor. For example, if there are only two APs on a floor, then you can’t locate the device on the floor plan. Instead, you see a Proximity view.
- The three placed APs must operate in the same frequency band. For example, if there are three APs on a floor, where two APs are operating on 2.4 GHz and one AP is operating on 5 GHz, then you can’t use locationing to track an AP or client. All three APs must operate in the same frequency band.

You must understand the difference between managed and unmanaged devices to understand locationing. The following points briefly describe what each of these terms mean:

- Managed devices are Arista APs that are configured either in AP mode or in WIPS mode. You can place Managed devices on the floor plan.
- Unmanaged devices are WiFi devices such as mobile phones, APs that are in the vicinity and visible to the managed devices. You cannot place them on a floor plan but you can locate them provided there is some data traffic from or to those devices. They can fall into any of the following categories: Authorized, Rouge, Guest, or External.
- Placed devices are managed devices (APs) that are placed on a floor plan.

If CVW can’t locate a device because there is no placed AP or because fewer than three APs are placed on the floor, then it displays the Proximity view for the device. The Proximity page shows an approximate distance of the device with respect to other APs.
23.2 Locate an AP or a Client in a Floor Plan

You can locate managed clients and devices using the Connected Clients and Failed Clients checkboxes. Use the Search option from the right panel to locate unmanaged and unplaced devices and clients, especially WIPS clients and devices. You can also use Search to see the Proximity views of clients that could not be located on the floor plan.

1. Click Floor Plans and expand the Navigator.
2. Select the location from the Location tree.
3. Click Locate Devices from the drop-down menu in the right panel.
4. Select the Connected Client checkbox to see the list of managed devices and clients in the floor plan.
23.3 Drill Down from a Device

You can drill down to the details page of an AP or client from a floor plan. Right-click an AP in a floor plan and then click View Access Point Details to see the details page of the device.
23.3.1 Locate a Specific Device

You can locate a specific device such as a managed placed AP, unmanaged placed AP, and a single client. For example, if you want to monitor a specific client that you suspect to be rogue, use this option to locate the client.

The following steps show how to locate an AP.

1. Click MONITOR > WiFi > Access Points.
2. Select the AP from the list and right-click.
3. Click Locate.

You are taken to the floor plan where the AP is placed. If the device can’t be located, then you are taken to the Proximity View page.

Note: The Locate menu is disabled for inactive devices or when multiple devices are selected.

Similarly, you can locate a client from MONITOR > WiFi > Clients.

23.3.2 What You Can See on the Floor Plan

- **Device name or User name**: Shows the user name for clients and device name for APs. To enable this feature, click the Show drop-down list and select **User/Device Name**.
- **Associations**: Shows which clients are associated with which AP. To enable Associations, click the **Show** drop-down list and select **Associations**.
- **Mesh Topology**: Shows the mesh links between APs.
• Connected clients and their connection health such as Low RSSI, Low Data Rate, and others.
• Failed clients and the reason of failure
Reports in CloudVision WiFi

CloudVision WiFi currently supports the following types of reports.

<table>
<thead>
<tr>
<th>Wireless Intrusion Prevention System (WIPS)</th>
<th>Compliance</th>
<th>Inventory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reports about the WiFi security posture.</td>
<td>Reports to meet federal or industry-based regulatory compliance for WiFi security.</td>
<td>Details of AP, clients, tunnels and networks for both WiFi and WIPS.</td>
</tr>
<tr>
<td>• Airspace Risk Assessment</td>
<td>• DoD Directive 8100.2 Compliance.</td>
<td>• WiFi Access Points</td>
</tr>
<tr>
<td>• Wireless Vulnerability Assessment</td>
<td>• HIPAA Wireless Compliance</td>
<td>• WiFi Tunnels</td>
</tr>
<tr>
<td>• Security Scorecard</td>
<td>• PCI DSS Wireless Compliance</td>
<td>• WIPS - Managed WiFi Devices</td>
</tr>
<tr>
<td>• Intrusion Prevention Summary</td>
<td>• SOX Wireless Compliance</td>
<td>• WIPS - Networks</td>
</tr>
<tr>
<td>• WIPS Alerts</td>
<td></td>
<td>• Managed WiFi Device Inventory</td>
</tr>
<tr>
<td>• AP Classification</td>
<td></td>
<td>• WiFi Clients</td>
</tr>
<tr>
<td>• Client Classification</td>
<td></td>
<td>• WIPS - Clients</td>
</tr>
<tr>
<td>• WIPS - Managed WiFi Devices</td>
<td></td>
<td>• WIPS - Access Points</td>
</tr>
<tr>
<td>• WIPS - Networks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Managed WiFi Device Inventory</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• WiFi Clients</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• WIPS - Access Points</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The reports can be accessed via the Reports tab on the left menu. You can view the definition and sections in each report, generate a report on-demand, or schedule one-time or recurring generation of a report.

24.1 Scheduling Reports

Report generation can be scheduled on a one-time or recurring basis. Users with Admin or Operator roles can schedule reports, while users with a viewer role can only view scheduled reports.

![Schedule Report](image)
Clicking on the Schedule Report icon opens a panel on the right-hand side of the screen, with a set of user-configurable parameters, as shown in the figure below.

The email that delivers the scheduled report contains the URL of the report and its JSON bundle. By default, the report URL is available for a limited period; once it expires, you can upload the JSON bundle to the report rendering application to view the report.
If the archival setting is set to Never Delete, then the URL sent in the email will always be valid until the report is manually deleted from the **REPORTS > Archived** page.

Once the report is successfully scheduled, it can be seen under **REPORTS > Scheduled**.

---

24.2 **On-Demand Generation of Reports**

Clicking on the Generate Report icon opens a panel on the right-hand side of a screen with a set of parameters to be configured as shown in the image below.
Sample HTML Report
24.3 Archive a Report

Reports can be archived so that they can be viewed at a later time. When the report archival quota of a user is consumed, no more reports can be archived unless older reports are deleted. You can define the date when an archived report should be deleted or you can also disable the auto-deletion for a report.

Archived reports can be viewed under REPORTS > Archived tab in CloudVision WiFi. Visibility of an archived report is not location-specific; it is based on a user's role. An archived report is always visible to a user who has previously generated the report. Role-based access is as follows:

- **Superusers** - can view all archived reports.
- **Administrators** - can view reports archived by them and for them.
- **Operators** - can view reports archived by them and for them.
- **Viewers** - cannot archive or view an archived report.
Chapter 25

Third-Party Servers

Integration of third-party servers with CloudVision WiFi is a system-level operation; it applies to the entire network.

Third-party servers supported are:

- Google
- ArcSight
- SMTP
- SNMP
- Syslog

25.1 Google Integration

You can integrate Google for Work with your network using CloudVision WiFi.

To configure Google integration:

1. Go to **System > Google Integration**.
2. Click **Upload JSON Key File** and .
   The file selection window opens.
3. Select the JSON key file you have downloaded from Google and click **Open**.
   The JSON file name shows up on the CloudVision WiFi screen.
4. Enter the **Admin Email Address**.
   This is the email address associated with the service account JSON key created in Google.
5. Click **Sync Client List** to sync the list of clients with the Google server.
   This updates the client list with the latest changes if any.

25.2 ArcSight Integration

Integration with ArcSight’s Enterprise Security Management (ESM) enables CVW to send events to the designated ArcSight server. The ArcSight server is configured to accept messages containing detailed event information in ArcSight’s Common Event Format (CEF). CVW needs the IP Address or the hostname and the port on which the ArcSight server receives events. Apart from events, you can also send audit logs from CVW to an ArcSight server.

To add an ArcSight server, perform the following steps:

1. Go to **System > Third-Party Servers > ArcSight Integration**.
2. Select **Enable ArcSight Servers**.
3. Click **Add** in the ArcSight Servers table to add an ArcSight server.
4. Enter the IP address or hostname of the Arcsight server.
5. Enter the port number to be used for communication between CVW and ArcSight.
6. Click **Select** next to the **Primary Cloud Integration Point (CIP)** and select the access point (AP) you want to designate as the primary CIP.

Note: Only CIP-enabled APs appear in the list. Make sure that you enable CIP mode on the APs you want to use as CIPs.
7. If you want to add a secondary CIP, click Select next to the Secondary Cloud Integration Point (CIP) and select the AP you want to designate as the secondary CIP.

8. Enable Forward Events and Forward Audit Logs to forward events and audit logs respectively from CVW to ArcSight servers.

9. Click Done.

10. Save the settings by clicking Save on the ArcSight Integration tab.

You can monitor the status of the ArcSight service from the ArcSight Integration tab. As shown in the following figure, the current status shows “Running” when the service is running, and “Stopped” when the service has stopped.

![ArcSight Integration Tab](image)

You can also enable and disable individual ArcSight servers using the three-dot menu in the table.

### 25.3 SMTP

The SMTP settings will be generic for the system and will be used for any email functionality. Although currently it is used for alerts, it will not be restricted for this use only. We must state that the SMTP settings will be used by CloudVision WiFi to notify users through email, for example notification of alerts.

**Note:** Only on-premises CVW deployments need an SMTP server to be set up. For cloud deployments, email notifications are sent by the Arista cloud services.

To configure SMTP, perform the following steps:

1. Go to **System > Third Party Server**.
2. Click the **SMTP** tab.
3. Configure the following parameters:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SMTP Server IP Address/Hostname</strong></td>
<td>IP Address or the host name of the SMTP server used by the system for sending e-mails. Default: 127.0.0.1</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>Port number of the SMTP server.</td>
</tr>
</tbody>
</table>
Option | Description
---|---
"From" Email Address | The source address from which e-mails are sent. Default: server@localhost.localdomain

4. Select **Enforce use of StartTLS (TLSv1)** to enforce the use of STARTTLS to send e-mails in an encrypted format.

STARTTLS is an extension to plain text communication protocols like SMTP that offers a way to upgrade a plain text connection to an encrypted (TLS or SSL) connection instead of using a separate port for encrypted communication.

5. Select **Verify SMTP Server's Certificate** to verify the certificate of SMTP server against a default built-in self signed CA certificate located on WM server or an uploaded CA certificate. If selected, and no certificate is uploaded then the certificate of SMTP server is verified against the built in certificate.

   a. Click **Set Certificate**.
   b. Browse and select the required certificate file, and click **Open**.

   If the certificate is imported successfully, the certificate file name and certificate details can be seen on the page.

   A **Set Certificate** option occurs.

   **Note:** If **Verify SMTP Server's Certificate** is selected, e-mails are sent only if the uploaded certificate matches with that on the SMTP server.

6. To authenticate with the SMTP sever, select **Authentication Required**, and enter the **Username** and **Password**.

7. Click **Save**.

### 25.4 SNMP

You can configure CloudVision WiFi to send information via SNMP traps to one or more SNMP servers. Depending on whether your network uses a cloud-based Arista WiFi server or an on-premises one, the following information can be sent to SNMP servers:

- For a cloud-based WiFi deployment, CloudVision WiFi can send alerts to your SNMP servers.
- For an on-premises WiFi server, CloudVision WiFi can send alerts and system health metrics to your SNMP servers.

#### 25.4.1 SNMP - Alerts

To add an SNMP server for alerts, go to **System > Third Party Servers > SNMP-Alerts** and click **Add** on the Destination SNMP Servers table. The SNMP server settings panel opens up.

The settings are described in the table below.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Select to enable communication between CloudVision WiFi and this SNMP server.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SNMP Trap Destination Server IP/Hostname</td>
<td>Enter the IP address or hostname of the SNMP server. Note: For a cloud-based Arista WiFi deployment, if the SNMP server uses a private IP address, you need to select a Cloud Integration Point.</td>
</tr>
<tr>
<td>Port Number</td>
<td>The port number for the SNMP server-CloudVision WiFi communication.</td>
</tr>
<tr>
<td>Primary Cloud Integration Point (CIP)</td>
<td><strong>Note</strong>: This field does not appear for an on-premises Arista WiFi server because it is needed only to integrate a cloud-based WiFi server. From the drop-down list, select an Arista device that you want to use as the primary Cloud Integration Point (CIP) for the SNMP server. Important: You must open port number 3852 in your network from the CIP to Arista cloud.</td>
</tr>
<tr>
<td>Secondary Cloud Integration Point (CIP)</td>
<td>From the drop-down list, select an Arista device that you want to use as the secondary Cloud Integration Point (CIP) for the SNMP server. If the primary CIP goes down, the secondary one ensures connectivity of your service to the cloud.</td>
</tr>
<tr>
<td>SNMP Version</td>
<td>Select SNMP V2 or V3 for the Arista server communication with the controller.</td>
</tr>
<tr>
<td>Community String</td>
<td>For SNMP v2, define a custom community string to authenticate with the SNMP server. The default value is &quot;public&quot;. Ensure that you change this community string.</td>
</tr>
<tr>
<td>Username</td>
<td>For SNMP V3, an auto-generated username for CloudVision WiFi to log in to the SNMP server.</td>
</tr>
<tr>
<td>Authentication Password</td>
<td>The password to authenticate with the SNMP v3 server.</td>
</tr>
<tr>
<td>Authentication Protocol</td>
<td>The authentication protocol used for SNMP v3. The options are MD5 (default) and SHA.</td>
</tr>
<tr>
<td>Privacy Password</td>
<td>The private key used to encrypt SNMP v3-based traps.</td>
</tr>
<tr>
<td>Privacy Protocol</td>
<td>The method used to encrypt SNMP v3-based traps. The options are DES (default) and AES.</td>
</tr>
</tbody>
</table>

**Note**: Make sure that the "Send Alerts using SNMP" checkbox is enabled. Even if all the individual SNMP servers are "Enabled", CloudVision WiFi will not send alerts unless the "Send Alerts using SNMP" checkbox is selected.
25.4.2 SNMP - Server Health

For an on-premises Arista WiFi server, CloudVision WiFi can send system health information to SNMP servers. To configure SNMP for system health, go to System > Third Party Servers > SNMP-Health and configure the settings shown in the figure below.

An SNMP Management Information Base (MIB) is a collection of definitions that define the properties of a managed object in a managed device. For example, the Arista WiFi server is a managed device, its disk memory is a managed object, and the Host Resource MIB contains information about the disk memory of the WiFi server.

The table below shows the SNMP Management Information Bases (MIBs) used for different system health metrics.

<table>
<thead>
<tr>
<th>MIB</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IF MIB</td>
<td>Select to send information about network interfaces such as eth0 and eth1.</td>
</tr>
<tr>
<td>MIB</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>AirTight MIB</td>
<td>Select to send information about the WiFi management specific processes running on the server.</td>
</tr>
<tr>
<td>Host Resource MIB</td>
<td>Select to send host resource information such as memory and CPU.</td>
</tr>
<tr>
<td>MIB-II</td>
<td>Select to send operational information such as System name, contact, and location. On the SNMP server, these fields are used to verify if the “SNMP GETs” option works.</td>
</tr>
</tbody>
</table>

To add SNMP servers, click Add on the Destination SNMP Servers table. As shown in the figure below, the SNMP server settings panel opens up.

The settings are described in the table below.
## Third-Party Servers

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Select to enable communication between CloudVision WiFi and this SNMP server.</td>
</tr>
<tr>
<td>SNMP Trap Destination Server IP/Hostname</td>
<td>Enter the IP address or hostname of the SNMP server.</td>
</tr>
<tr>
<td>Port Number</td>
<td>The port number for the SNMP server-CloudVision WiFi communication.</td>
</tr>
<tr>
<td>SNMP Version</td>
<td>Select one of the two options: a) SNMP V1,V2 or b) SNMP V3 for the the SNMP server-CloudVision WiFi communication.</td>
</tr>
<tr>
<td>Username</td>
<td>For SNMP V3, an auto-generated username for CloudVision WiFi to log in to the SNMP server.</td>
</tr>
<tr>
<td>Authentication Password</td>
<td>The password to authenticate with the SNMP v3 server.</td>
</tr>
<tr>
<td>Authentication Protocol</td>
<td>The authentication protocol used for SNMP v3. The options are MD5 (default) and SHA.</td>
</tr>
<tr>
<td>Privacy Password</td>
<td>The private key used to encrypt SNMP v3-based traps.</td>
</tr>
<tr>
<td>Privacy Protocol</td>
<td>The method used to encrypt SNMP v3-based traps. The options are DES (default) and AES.</td>
</tr>
</tbody>
</table>

**Note:** Make sure that the "Monitor System heath using SNMP" checkbox is enabled. Even if all the individual SNMP servers are "Enabled", CloudVision WiFi will not send system health information unless the "Monitor System heath using SNMP" checkbox is selected.

### 25.5 Syslog

You can configure a Syslog server from CloudVision WiFi to enable the underlying Wireless Manager service to send messages to be logged in the syslog server.

To configure a Syslog server, perform the following steps:

1. Go to **System > Syslog**.
2. The **Syslog Integration Status** indicates the status of the Syslog server.

   The Current Status displays the current status of the SNMP server. The applicable values are Running, Stopped and Error.
3. Select **Enable Syslog Servers** to enable integration of CloudVision WiFi with Syslog server.  
   A **Syslog Server** table appears.

4. Click **Add**
   An **Add Syslog Servers** window appears on the right pane.

5. Under **Add Syslog Servers** window, enter the following details:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syslog Server IP/Hostname</td>
<td>Specifies the IP address or the hostname of the Syslog server.</td>
</tr>
<tr>
<td>Port Number</td>
<td>Specify the port number of the Syslog server to which the system sends alerts. Default: 514</td>
</tr>
<tr>
<td>Primary Cloud Integration Point (CIP)</td>
<td>Note: This field does not appear for an on-premises Arista WiFi server because it is needed only to integrate a cloud-based WiFi server. Select a primary CIP to enable the integration of Arista Cloud with Syslog. The syslog server on which a CIP device is selected is termed as CIP destination and is listed as a CIP destination for the CIP enabled Arista device.</td>
</tr>
<tr>
<td>Secondary Cloud Integration Point (CIP)</td>
<td>From the drop-down list, select an Arista device that you want to use as the secondary Cloud Integration Point (CIP) for the Syslog server. If the primary CIP goes down, the secondary one ensures connectivity of your service to the cloud.</td>
</tr>
</tbody>
</table>
| Message Format                  | Specify the format in which an alert is sent. 
   Available options are:
   - **PLAIN**
   - Intrusion Detection Message Exchange Format (IDMEF). |
| Enabled                         | Sends the alerts to the Syslog server.                                      |
| Append BOM Header               | Appends the byte order mark to the syslog server entry. This is relevant in case of plain text files. |
| Forward Events                  | Forwards the main events to the Syslog server.                              |
| Forward Sub-events              | Forwards the sub-events along with the main events.                         |
| Forward Audit Logs              | Sends audit logs to the Syslog server. You can forward audit logs in plain text format only |

6. Click **Save**.
Advanced System Settings

Advanced system settings are system-level operations typically performed from the SYSTEM tab in CVW. The settings apply to the entire network.

You can perform the following advanced system-level settings in CVW:

- License settings for on-premises users
- Language settings

26.1 License Settings for On-Premises Users

You can apply licenses from CVW for on-premises users. After you upload the license file, you need to log out and then log in again for the license to be effective.

Follow these steps to apply the license:

1. Go to SYSTEM > Advanced Settings > License.
2. (Optional) Click Download License to download the existing license details in a text file format.
3. Click Select License File and select the license file from your local or shared drive. Licences must be in the json file format.
4. Apply the license.
5. When prompted, log out and then log in again to successfully activate the license.

26.2 Language Settings

You can define the system language that is used by CVW as a mode of communication. CVW uses the system language to send default messages from the application. For example, alerts and notifications are communicated using the system language. The default system language is English.

Follow these steps to configure the system language:

1. Go to SYSTEM > Advanced Settings > Language.
2. Select the system language and the SSID encoding language.
3. Save the changes.

26.3 High Availability Status

If you have enabled the High Availability (HA) service, you can see the HA status and configuration details of the servers. For example, you can see whether the HA service is running or stopped or disabled. If you have not configured the HA service, you will see the status as Disabled. This is a read-only page; you can’t configure anything on this page. Configure the HA service using the CLI.

To see the HA status from CVW, go to System > Advanced Settings > High Availability Status.
26.4  System Status

You can see the status of the WiFi server and other system-related information from **System > Advanced Settings > System Status**. You can also start and stop system services from the System Status page.

The following system-related information is displayed on this page:

- Server ID
- Server Access URL
- Managed Device Communication Port
- Maximum Managed Devices Allowed (Physical Devices)
- Allowed Mode of Operation — Indicates whether WiFi or WIPS or both services are enabled on the server.
- Software Version — Indicates the software version of CVW
- Software Build — Indicates the software build version of CVW
- Operating System
- Appliance Model
- IPv4 — Indicates the IPv4 address, if available
- IPv6 — Indicates the IPv4 address, if available

26.5  NTP Configuration

Network Time Protocol (NTP) is used to synchronize the time in servers and computers that are in different networks over the internet. You can add a maximum of three NTP servers.

1. Go to **System > Advanced Settings > NTP Configuration**.
2. Click the **Enable NTP** check box.
3. Add the NTP servers. You must add at least one NTP server.
4. Click **Check Drift** to check the time drift between NTP servers.
5. Sync and save the settings
Chapter 27

Client Connectivity Test Using a Tri-radio AP

With a tri-radio Arista access point (AP), you can turn its third radio into a client that can connect to another AP you want to test. This gives you the ability to proactively validate network assurance, the reachability of network services, and the quality of experience for critical applications such as VoIP. The AP being tested is called the Target AP. Acting as a client, the third radio of the tri-radio AP connects to the target AP and runs tests to assess network health and identify problems if any. With Arista CloudVision WiFi, you can select the applications you want to test and set up a recurring schedule.

For example, you could test VoIP applications at important meeting locations.

The tests, listed below, range from basic WiFi and Internet connectivity to application experience:

- Association
- Authentication
- DHCP
- Gateway
- DNS
- WAN Latency
- Application Test
- VOIP Test
- Throughput Test

Broadly, running tests using the third radio as a client consists of three steps: create a test profile, schedule a test or run it on demand using the profile, and analyze the test results.

27.1 Test Profile

A test profile comprises:

- The SSID being tested
- The frequency band being tested and
- The tests that you want to run on the SSID and that band.

A test profile allows you to test client experience based on the use case. For example, for a corporate SSID, you could define a test profile that includes VoIP test and productivity applications. For a Guest SSID, you could exclude VoIP from the test profile and include only some social and custom applications. If your VoIP WiFi clients are expected to primarily use the 5 GHz frequency band, then you could specify that in the test profile for testing VoIP quality of experience. The figure below shows an example of a test profile for a corporate SSID. A single test run carries out all the tests included in the test profile. Thus, for the corporate SSID test profile shown in the figure below, a single test run would consist of the Basic Connectivity Test, application tests for the Productivity applications chosen, the VoIP test, and the Throughput test.

You can run tests manually or on demand by selecting the AP to be tested, as shown below.

Alternatively, you can schedule tests for a location (see the Schedule section below for details).

Important things to remember about test profiles are:
• You must create a test profile before you run a client connectivity test.
• When you create a test profile, you can save it and use it multiple times. If multiple APs broadcast the same SSID, then a single test profile can be used to run tests on all the APs.
• To run a test on a target AP, make sure that the target AP is broadcasting the SSID that is in the selected test profile.

27.2 Schedule

Scheduling periodic tests can help you optimize network performance and proactively unearth any issues on an ongoing basis, thereby avoiding reactive network troubleshooting fire drills. A schedule can comprise a single test run or multiple test runs recurring every few days or weeks.

When you set up a schedule for client connectivity tests at a location, the schedule automatically applies to all its child locations. Note that the parent location and one or more child locations could be in different time zones. In such cases, the time you select is interpreted by each location as its local time.

Selecting APs for a Scheduled Test

When you schedule a test, a maximum of two target APs is tested for each folder. The selection of the target and tri-radio client APs is based on the considerations shown in the table below.

<table>
<thead>
<tr>
<th>Target AP</th>
<th>Tri-radio Client AP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target APs are selected at random to avoid testing the same AP repeatedly in a recurring schedule.</td>
<td>At least one tri-radio AP should be able to see the target AP with good RSSI, e.g., -70dBm or greater.</td>
</tr>
<tr>
<td>The SSID and frequency band of the target AP must match those in the selected test profile.</td>
<td>The third radio of the tri-radio AP must not be busy in other activities such as intrusion prevention, troubleshooting, or another test.</td>
</tr>
<tr>
<td>The target AP must not be busy with another test.</td>
<td>The tri-radio AP that sees the target AP with the best RSSI is chosen to act as the client, provided its third radio is not busy.</td>
</tr>
</tbody>
</table>

If a tri-radio client AP and target AP meeting the above criteria are found, then the test run starts per the schedule. Otherwise, the test run is not carried out and the appropriate reason is logged in the results.

27.3 Results

The Result Status column on the Results page shows a Green, Red, Orange or Grey dot against each test run. Note that a test run consists of multiple tests. The colors indicate the following:
• Grey: The test run could not be completed.
• Green: All tests in the test run succeeded.
• Red: One or more tests in the test run completely failed.
• Orange: Partial success (or failure) of a test. A partial success could mean, for example, that some of the applications in the application test failed but others succeeded (see the Application Test Results section below for a detailed explanation).
Application Test Results

Application Tests are grouped by the type of application - Productivity, Social, etc. The figure below shows an application test result.

Application tests send an HTTP GET request to the application being tested. If the HTTP GET fails, a Ping test is carried out to check connectivity to the application server. If the HTTP GET succeeds, the result captures the following parameters:

- Page Size
- HTTP Response Code (codes 100-399 represent a success)
- Page Loading Time. You can hover on the Page Loading Time to see the breakdown in terms of:
  - DNS Lookup Time
  - Initial Connection Time
  - SSL Connection Time

The logic for Application Test results is as follows:

- Green: All application tests succeeded.
- Red: All application tests fail.
- Orange: Anything other than Red or Green for a completed test run.

Thus, if even one of the applications fails, the application test result is Orange—a partial success—because the conditions for Red (all applications fail) or Green (all applications succeed) do not hold.
## Test Result Descriptions

Shown below are the descriptions of the fields in each test result.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **General information** | • Name of the target AP  
   • Name of the tri-radio AP  
   • Timestamp  
   • Start time - when the test started  
   • Stop time - when the test completed |
| **Access point acting as a client (tri-radio AP)** | • AP Name - Name of the tri-radio AP  
   • Radio Mac - MAC address of the tri-radio AP  
   • SSID - SSID being tested (as per the test profile)  
   • Frequency Band - Frequency band being tested (as per the test profile)  
   • Connectivity Test Profile - The name of the test profile used to run the client connectivity test. |
| **Association** | • Successful (Green)  
   • Failed (Red) |
| **Authentication** | • The authentication status:  
   • Successful (Green)  
   • Failed (Red)  
   • Security method: The security method used.  
   |\[\text{Note:}\text{ The latency is shown if the security mode is } 802.1x.\] |
| **DHCP** | • The DHCP status:  
   • Successful (Green)  
   • Failed (Red)  
   • IP address: The IP address used by the DHCP server if successful  
   • Latency: The DHCP latency in milliseconds if successful  
   • DNS Server Option  
   • DHCP Gateway |
| **Gateway** | • Reachable: The status of the gateway. The values are:  
   • Successful (Green)  
   • Failed (Red)  
   • Latency if successful |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| DNS        | • DNS Status: List of DNS servers with the status for each one:  
• Successful (Green)  
• Failed (Red)  
• Partial (Orange)  
• IP address and latency if successful.  
  Note: When any one of the DNS servers has a failed status, the overall status of the DNS server test is set to "Partial". If the overall the status of the DNS test is "Partial", the Client Connectivity test result is set to "Failed". |
| WAN Latency| • WAN Reachability:  
• Successful (Green)  
• Failed (Red)  
• WAN URL: The URL used to test the connectivity.  
  Note: The default URL is www.google.com which cannot be edited.  
• Latency if reachable |
| Ping Test  | • Ping Test:  
• Successful (Green)  
• Failed (Red)  
• Host: The host URL  
• Latency if successful |
| HTTP GET   | If successful, it captures the following:  
• Page Size  
• HTTP Response Code (codes 100-399 represent a success)  
• Page Loading Time. You can hover on the Page Loading Time to see the breakdown in terms of:  
• DNS Lookup Time  
• Initial Connection Time  
• SSL Connection Time |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **VoIP Test** | • VoIP call status:                                                                                                                  • Successful (Green)  
• Failed (Red)  
• Mean Opinion Score (MOS) between 0 to 5, shown as 5 stars.  
• When you hover the mouse over the MOS score, you can see values for:  
• Latency  
• Packet loss  
• Jitter |
| **Throughput Test** | • Internet/WiFi throughput test status:                                                                                                         • Successful (Green)  
• Failed (Red)  
• Internet Throughput Test  
• Upload and Download speeds.  
• WiFi Throughput Test  
• TCP Upload and Download speeds.  
• UDP Upload and Download speeds. |
A mesh network is typically used when it’s difficult to run a wired Ethernet connection to every access point (AP). In a mesh deployment, only some APs have a wired Ethernet connection—these APs are called “root nodes”. Other APs (called “non-root nodes”) form “mesh links” or “hops”—a chain of wireless links leading ultimately to the root node.

Thus, in a mesh, root nodes are directly connected to a switch, whereas the other APs connect to the wired network via one or more wireless hops to the root node. Each hop introduces a drop in the throughput, so a mesh network deployment requires careful planning.

CloudVision WiFi (CVW) supports mesh configuration via mesh profiles. The following sections describe key characteristics of Arista mesh networks, and the prerequisites and steps to set up a mesh.

### 28.1 Key Characteristics of Arista Mesh

- CloudVision WiFi supports mesh only for groups, and not for folders (locations). You cannot create a mesh profile in a folder.
- When setting up a mesh network for the first time, make sure that all participating APs are connected to the Wireless Manager (WM) server. This is because an [**AP must be connected to WM for a mesh profile to be enabled on it**](#).
• A root node must be active and available at all times for a mesh network to work.
• APs in a mesh automatically find the path and connect to the best root node. So once the individual APs are up, it takes some time for the mesh network to be up and running.
• A mesh AP periodically checks if its root node is reachable; if not, it automatically sets up a different path to a root node.
• We recommend that for mesh links you use the 5 GHz band because it has more non-overlapping channels and for 802.11ac APs, the mesh can leverage 802.11ac capabilities on the 5 GHz band.
• Only one AP radio can be configured in mesh mode.

28.1.1 Prerequisites for Mesh Access Points
Before setting up a mesh network, you need to make sure that the APs participating in the mesh meet the following prerequisites:
• Mesh APs must have Background Scanning turned off.
  Note: Background scanning is automatically turned off when you enable a mesh profile for a group. To manually turn background scanning off, go to Configure > Device Settings in the group where the mesh profile is defined and set Background Scanning to Off.
• For APs in a mesh, Channel Selection must be set to Manual on the band to be used for mesh links (we recommend that you use the 5 GHz band for mesh links). Under Configure > WiFi > Radio Settings > Channel Settings, set the Channel Selection to Manual and select the channel that APs will use to set up mesh links.
• Mesh cannot operate on Dynamic Frequency Selection (DFS) channels. When selecting a 5 GHz channel for mesh APs, make sure that it's not a DFS channel.
• A mesh profile is basically a special kind of SSID—one that has a mesh configuration. To join a mesh network, i.e., for a mesh profile to be enabled on it, an AP radio can run a maximum of six other (non-mesh) SSIDs. Thus, if AP1 is to be part of a 5 GHz band mesh, it can run a maximum of six other (non-mesh) 5 GHz SSIDs.
• Only one mesh profile can be enabled per group.

28.2 Features Affected By Mesh Mode
Because the mesh link must be kept up at all times, the following features are not supported in mesh mode:
• When you enable a mesh profile for a group, background scanning (including VoIP-aware scanning) is automatically turned off on the mesh radios of APs in that group.
• Automatic Channel Selection is not supported on the mesh radio of an AP; the other radios can select channels automatically.
• Link Aggregation (LAG) is not supported in mesh mode.

Note that the multi-function radio of an AP continues to scan (for WIPS, etc.) even if one of the other radios is a mesh radio.

28.3 Set Up Mesh Network
To set up a mesh network, you need to enable the mesh profile on all participating APs and define the root nodes before deploying the APs. You can then deploy them at their respective locations and connect the root nodes to the wired network.

The steps for the initial pre-deployment setup are as follows:
1. Connect all participating APs to the wired network and thereby to the Wireless Manager (WM) server.
As mentioned in the Prerequisites section, for a mesh profile to be enabled on an AP, it must be connected to the WM. Keep all the mesh APs connected to the wired network until you have enabled the mesh profile on them.

2. In the CloudVision WiFi (CVW) UI, go to System > Navigator > Groups and click on the “+” icon to create a group for the mesh network.

   **Note:** CVW supports mesh only for groups, and not for folders (locations). You cannot create a mesh profile in a folder. To create a mesh profile, you must first create a group, add the mesh APs to that group, and then create a mesh profile.

3. Under Monitor > WiFi, select the APs you want to add to the mesh, right-click and select Assign/Re-assign to a Group, and add the mesh APs to the group you created.

4. Decide which APs you want to use as root nodes. Note down the MAC addresses of these APs.

5. In the left-hand side navigator, go to the mesh group you created. Under Configure > WiFi > Mesh, click Add Mesh Profile. The following figure shows a mesh profile in a mesh group.

6. Configure the fields shown in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mesh SSID Name</td>
<td>The external name for the mesh link that APs use when setting up mesh links.</td>
</tr>
<tr>
<td>Mesh Profile Name</td>
<td>Internal to the system. It's used to identify a mesh profile.</td>
</tr>
<tr>
<td>Max Hop Counts</td>
<td>The maximum number of wireless hops between a non-root AP and its root node.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The maximum allowed value is 8.</td>
</tr>
<tr>
<td>Max Downlink</td>
<td>The maximum number of APs downlink of an AP, i.e., the maximum number of “child” APs an AP can have.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The maximum allowed value is 5.</td>
</tr>
<tr>
<td>Min RSSI</td>
<td>The minimum RSSI required for APs to form mesh links with each other.</td>
</tr>
</tbody>
</table>

7. Save the mesh profile.

8. Go back to Configure > WiFi > Mesh. Click Enable on the mesh profile. The Enable Mesh wizard opens up.
9. The Enable Mesh wizard takes you through the AP configuration steps needed to enable the mesh network. For example, it prompts you to select the frequency band and the channel to be used for mesh links (5 GHz is the better one). The exact steps in the wizard depend on the prerequisites that the mesh APs meet.

10. In the final step of the wizard, click Enable Mesh. This activates the mesh mode for APs in the group. To verify this, go to Monitor > WiFi > Access Points and confirm that the Mesh Mode column shows “Enabled” for these APs.

   **Note:** APs reboot when mesh is enabled on them. So it takes some time (could be a few minutes) for the Mesh Mode column to show “Enabled”. Once you have verified that the APs are in mesh mode, we recommend that you disconnect the non-root APs from the wired network to avoid VLAN congestion (but keep the root nodes connected to the network).

11. The next step is to select root nodes from the Select Root Node right panel. Select APs that have a wired connection and Save them as root nodes.

   **Note:** Do not disconnect the root node APs until you have saved them as root nodes.

The mesh APs are now ready to be deployed.

### 28.4 Deployment and Post-Deployment

If you have planned the mesh network properly (taking coverage and the number of mesh links per AP into account), the deployment process is straightforward. You can connect the root nodes to the wired network and place the non-root nodes within a Min RSSI radius from APs with which they are supposed to form mesh links. Make sure that no AP ends up having more “child” APs than the max downlink value. Arista mesh is self-actuating and self-healing: non-root APs automatically find the best path to a root node, both initially and in the event of a link failure.

For any post-deployment changes to the mesh group configuration, Wireless Manager pushes the configuration to the root nodes. The root nodes then push it to the non-root nodes, which in turn push it to their “child” APs, and so on.

**Note:** You need to add your service SSIDs (the ones you want WiFi clients to use) to the mesh group so that they get pushed to all the APs in the mesh.
User Accounts

For on-premises deployments, you can manage users from CVW. You can create new users, and then define LDAP and RADIUS configuration as applicable for the authentication of users. You can configure certificate-based authentication of users with the Superuser role. Similarly, you can set the password policy, and user account suspension criteria.

- Define and manage users from System > User Accounts > Users. You can specify the type of users such as local, LDAP, or RADIUS users.
- Configure the LDAP server parameters using System > User Accounts > LDAP.
- Configure the RADIUS server parameters using System > User Accounts > RADIUS.
- Configure the certificate-based authentication parameters using System > User Accounts > Certificate.
- Configure the password settings using System > User Accounts > Password Settings.
- Configure the account suspension criteria using System > User Accounts > Account Suspension.

The Users tab also serves as the dashboard where you see a snapshot of the user privileges. From the Users dashboard, you can edit individual user accounts, change the password, lock or unlock the user account, and delete the user. These actions are available for individual users; not for multiple users.

29.1 User Roles and their Privileges

CVW supports four types of users — Superuser, Administrator, Operator and Viewer. You must have the Superuser privileges to manage users in CVW.

The following table details the role-wise privileges in CVW.

<table>
<thead>
<tr>
<th>Privileges</th>
<th>Superuser</th>
<th>Administrator</th>
<th>Operator</th>
<th>Viewer</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Account Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set or modify identification and authentication option (Local, RADIUS, LDAP, and Certificate)</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Add and delete users</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>View and modify properties of any users (in Users tab)</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Privileges</td>
<td>Superuser</td>
<td>Administrator</td>
<td>Operator</td>
<td>Viewer</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------</td>
<td>-----------</td>
<td>---------------</td>
<td>----------</td>
<td>--------</td>
</tr>
<tr>
<td>Define password strength, account locking policy, maximum concurrent sessions for all users</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>View and modify preferences in Manage Account (email, password, language preferences, and time zone)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>User actions audit</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Download user actions audit log</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Modify user actions audit lifetime</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>System and operation settings</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modify system settings and operating policies</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Events, devices, and locations</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View generated events</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Modify and delete generated events</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>View devices</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Add, delete, and modify devices (APs, Clients, Sensors)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>View locations</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Add, delete, and modify locations</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Calibrate location tracking</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Reports</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Privileges

<table>
<thead>
<tr>
<th>Privileges</th>
<th>Superuser</th>
<th>Administrator</th>
<th>Operator</th>
<th>Viewer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add, delete, modify — Shared Report</td>
<td>Yes</td>
<td>Yes (only self created)</td>
<td>Yes (only self created)</td>
<td>No</td>
</tr>
<tr>
<td>Generate — Shared Report</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Schedule — Shared Report</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Add, delete, modify, generate, schedule — My Report</td>
<td>Yes (only self created)</td>
<td>Yes (only self created)</td>
<td>Yes (only self created)</td>
<td>No</td>
</tr>
</tbody>
</table>

### Manage Users

The Users tab serves as the dashboard where you see a snapshot of the user privileges. From the Users dashboard, you can edit individual user accounts, change the password, lock or unlock the user account, and delete the user. If a user account is temporarily suspended due to multiple unsuccessful password attempts, you can unlock such temporary suspensions from the Users dashboard. These actions are available for individual users; not for multiple users.

**Add Users**

To add a user, do the following.

1. Go to **System > User Accounts > Users**.
2. Click **Add User**.
3. The **User Name** page opens.
4. Provide the user details on the User Name page and then save the page.

The following table describes some of the fields on the User Name page. Some of the fields are not applicable for RADIUS and LDAP users.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Type</td>
<td>Specifies the type of user. You can define a local, LDAP, or RADIUS user.</td>
<td></td>
</tr>
<tr>
<td>Login ID</td>
<td>Specifies the login id of the user. For RADIUS and LDAP users, the login ID must be the same as defined in LDAP and RADIUS settings.</td>
<td></td>
</tr>
<tr>
<td>First Name</td>
<td>Specifies the first name of the user. Not applicable for LDAP users.</td>
<td></td>
</tr>
<tr>
<td>Last Name</td>
<td>Specifies the last name of the user. Not applicable for LDAP users.</td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td>Specifies the e-mail id of the user. Not applicable for LDAP users.</td>
<td></td>
</tr>
<tr>
<td>Language Preference</td>
<td>Specifies the language in which the user wants to view the UI text. The default value is English.</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Time Zone</td>
<td>Specifies the time zone in which the user operates.</td>
<td></td>
</tr>
<tr>
<td>Authorization</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>Specifies the role assigned to the user. Choose from Viewer, Operator, Administrator and Super User. For more information on what individual roles</td>
<td></td>
</tr>
<tr>
<td>Allowed Locations</td>
<td>Specifies the locations for which the user can operate. Click Change hyperlink to modify the list of allowed locations. A user can operate on one or more locations. For instance, a Superuser could have rights to multiple locations.</td>
<td></td>
</tr>
<tr>
<td>WiFi Access Management</td>
<td>Enables users to access the WiFi management settings and functions on CVW. Depending on the role, users have restricted access to the WiFi management operations.</td>
<td></td>
</tr>
<tr>
<td>WIPS Management</td>
<td>Enables users to access the WIPS management settings and functions on CVW. Depending on the role, users have restricted access to the WIPS management operations.</td>
<td></td>
</tr>
<tr>
<td>Password (Not applicable for LDAP and RADIUS users)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set Password</td>
<td>Specifies the password for the user.</td>
<td></td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Repeat the password for confirmation.</td>
<td></td>
</tr>
<tr>
<td>Force user to change password</td>
<td>Specifies that the user must change the password after the first login.</td>
<td></td>
</tr>
<tr>
<td>Password Expiry — Never Expires</td>
<td>Specifies that the password set by users after the first login never expires. Users can manually change the password any time but the system never forces users to change the password.</td>
<td></td>
</tr>
<tr>
<td>Password Expiry — Expires</td>
<td>Specifies that users must change the password after the specified duration. Configure the duration in the Expires After field, after which the password expires. The unit is calculated in days. The Warn Before field specifies that users will be warned before the specified days of the expiry day. For example, if you configure the Expires After as 90 days and Warn Before as 15 days, then the password will expire after 90 days and the user will be warned to change the password after 75 days, which is 15 days before the expiry of the password. Note that if users don’t change the password when intimated, they will be locked out of the application and the Superuser needs to reset their password.</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Password Expiry — Expires After</td>
<td>Specifies the duration in days from the time of change of the password after which the password expires.</td>
<td></td>
</tr>
<tr>
<td>Password Expiry — Warn Before</td>
<td>Specifies the time in days before the password expiry to prompt the user to change the password.</td>
<td></td>
</tr>
<tr>
<td>Session Timeout</td>
<td>Specifies the idle time interval after which the user's User Interface (UI) session should be timed out. Two options are available. Select Never Expires, if you don't want the session to timeout. Select Expires After and specify the time in minutes (between 10 and 120 minutes) after which the session should time out.</td>
<td></td>
</tr>
<tr>
<td>Additional User Fields (Not applicable for LDAP and RADIUS users)</td>
<td>Specifies some predefined and custom user fields that you can create for users. For example, you can assign a department to each user and assign them specific privileges. Use the Add/Remove Columns button in the Users tab to enable and view any of the additional user fields in the table.</td>
<td></td>
</tr>
</tbody>
</table>

**Edit a User**

You can edit only one user details at a time. To edit a user, do the following.

1. Go to **System > User Accounts > Users**.
2. Right-click the user and click **Edit**.
3. Edit the user details and save the changes.

   ☑️ **Note:** You cannot edit the **User Type** and **Login ID** fields.

**Change the Password of a User**

While creating the user, if you haven't assigned any password to the user, you can do so using the Change Password option. Also, you can also change any existing password of a user.

To change the password, follow these steps:

1. Go to **System > User Accounts > Users**.
2. Right-click the user and click **Change Password**.
3. In the **Change Password** right-panel, provide the new password.
4. Save the changes.

### 29.3 LDAP Server-based Authentication

For on-premises deployments, you can configure your LDAP server and map it to CVW to authenticate CVW users. After you have configured the LDAP server, users or groups defined in the LDAP server can log in to CloudVision WiFi. Based on the authentication and user role defined in CVW, users get restricted access to WiFi, WIPS, or both configuration pages.

You can configure the following attributes in LDAP:
• Connection Details: Connects CVW with your primary and secondary LDAP servers.
• LDAP Configuration Parameters: Allows access to the LDAP compliant directories.
• Privileges for LDAP Users: Specifies the role and locations assigned to LDAP users. The specified values apply to all users authenticated via LDAP.

You must have Superuser privileges to configure the LDAP server access parameters.

To configure LDAP server access parameters, do the following.

1. Go to **System > User Accounts > LDAP**.
2. Click the **LDAP Authentication** check box.
3. Configure the LDAP connection details as described in the Connection Details table.
4. If you have selected **Verify LDAP Server’s Certificate**, you must add a certificate. Click **Add Certificate** to add trusted root CA Certificate(s) for the LDAP server. Choose the certificate from your local drive.
5. Specify the LDAP configuration details as described in the LDAP Configuration Details table.
6. If the directory does not allow an anonymous search, you must configure user credentials to search the LDAP compliant directory. Click the **Authentication required to search LDAP** check box. Configure the user credentials as described in the User Credentials table.
7. Click **Start Test** to test the authentication options.
8. Configure user privileges as described in the Privileges for LDAP Users table.
9. Save the changes.

### Connection Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Server IP Address/Hostname</td>
<td>The IP address or hostname of the primary LDAP server.</td>
</tr>
<tr>
<td>(Primary Server) Port</td>
<td>The port number of the primary LDAP server. The default port is 389.</td>
</tr>
<tr>
<td>Backup Server IP Address/Hostname</td>
<td>The IP address or hostname of the backup LDAP server.</td>
</tr>
<tr>
<td>(Backup Server) Port</td>
<td>The port number of the backup LDAP server.</td>
</tr>
<tr>
<td>Enforce Use of SSL/TLS</td>
<td>Enable this option to ensure only the SSL/TLS connection to the LDAP server is allowed. If you don’t select this option, even Open connection to the LDAP server is allowed, besides SSL/TLS.</td>
</tr>
<tr>
<td>Verify LDAP Server’s Certificate</td>
<td>Enable this option to ensure that the CVW user cannot connect to the LDAP server unless the certificate check passes. When this option is not selected, the CVW user can connect to the LDAP server without verifying the LDAP server certificate.</td>
</tr>
</tbody>
</table>

### LDAP Configuration Details
### Field | Description
--- | ---
Base Distinguished Name | Specifies the base distinguished name (Base DN) of the directory to which you want to connect, for example, o=democorp, c=au.

Distinguished Name is a unique identifier of an entry in the Directory Information Tree (DIT). The name is the concatenation of Relative Distinguished Names (RDNs) from the top of the DIT down to the entry in question.

Filter String | This is a mandatory argument. It is a string specifying the attributes (existing or new) that the LDAP server uses to filter users. For example, IsUser=A is a filter string. By specifying a filter string, you can allow or deny login to a particular organizational unit (OU) or a group of users defined in the active directory (AD).

You can specify a DN (Distinguished Name) of any particular group to allow access to only those users who are members of that group. For example, memberOf=DC=GroupName,DC=com.

You can include members from multiple groups by using an OR condition. For example, to allow access to users under Base DN who are member of any of the two groups — Admins OR Reviewer, you must include the following filter string:

$$\{((\text{memberOf}=\text{CN}=\text{Admins,D}C=\text{ITShop,D}C=\text{Com})\text{OR}(\text{memberOf}=\text{CN}=\text{Reviewer,D}C=\text{ITShop,D}C=\text{Com}))\}$$

Similarly, to allow access to users under Base DN who are member of both Admins AND Reviewer groups, you must include the following filter string:

$$\{(\text{memberOf}=\text{CN}=\text{Admins,D}C=\text{ITShop,D}C=\text{Com})\text{AND}(\text{memberOf}=\text{CN}=\text{Reviewer,D}C=\text{ITShop,D}C=\text{Com})\}$$

You can have alternative configurations in the AD, such as, adding a new attribute named ATNWIFI to the users in AD that are granted access and then setting the filter string to allow users with that attribute only. For example, filter string = ATNWIFI

You can also create a new group of users in the AD with access granted and include that group in the filter string.

A common filter string that you can use is 'objectClass=*'. You can use this string when you do not want to filter out any LDAP entry.
### User ID Attribute

Specifies the string defined in the LDAP schema that the system uses to identify the user. (Default: `cn`)

#### User Credentials

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin User DN</td>
<td>Specifies the DN of the administrator user that is used for authentication in the LDAP server.</td>
</tr>
<tr>
<td>Password</td>
<td>Specifies the password for the administrator user.</td>
</tr>
<tr>
<td>Append Base DN</td>
<td>Indicates that when selected the base DN specified in the LDAP Configuration Details section is appended to the Admin User DN.</td>
</tr>
</tbody>
</table>

#### Privileges for LDAP Users

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Role Attribute</td>
<td>Specifies the user role attribute string that the system uses to identify a user’s role, as defined in the LDAP schema.</td>
</tr>
<tr>
<td>User Role</td>
<td>Specifies the default role for the new LDAP users. You can select one of the following four options — Superuser, Administrator, Operator, and Viewer.</td>
</tr>
<tr>
<td>User Location Attribute</td>
<td>Specifies the user location attribute string that the system uses to identify the locations where the user is allowed access, as defined in your LDAP schema.</td>
</tr>
<tr>
<td>Locations</td>
<td>The location to which a new LDAP user has access rights. You can select another location by clicking Change.</td>
</tr>
</tbody>
</table>

## 29.4 RADIUS-based Authentication

For on-premises deployments, you can use a RADIUS server to facilitate user authentication to access CVW. Configure the RADIUS server access parameters from the System > User Accounts > RADIUS tab.

You can configure the Authentication, Accounting, and Advanced Settings parameters for the RADIUS server.

Follow these steps to configure the RADIUS server:

1. Go to **System > User Accounts > RADIUS**.
2. Click the **Authentication** section.
3. Specify the IP address or hostname, port number, and shared secret for the primary RADIUS server. Configuring the secondary RADIUS server is optional.
4. Click **Test** to test the connection to the RADIUS server.
5. **In RADIUS users log in to the WiFi server using**, click **CLI** if you want users to access CVW using the command line. Click **UI** if you want the users to access CVW using the GUI.

6. Select vendor specific attributes as appropriate. The option you select here will be used when vendor specific attributes are not defined for the RADIUS server.

7. Select the Role of RADIUS users and the location that users can access in CVW. The user can access the selected location and all its child locations.

You have configured the RADIUS authentication.

The next steps are to configure the RADIUS accounting server and some advanced settings. If you don’t want to configure the RADIUS accounting server, you can save the page.

**Configure the RADIUS Accounting Server**

RADIUS accounting server is an optional configuration. You can use the accounting service of the RADIUS server independent of the RADIUS authentication services. The RADIUS accounting service is used to monitor the network and collect statistical data of the connected client.

1. Click the **Accounting** section.

2. Specify the IP address/hostname, port number and shared secret for the primary and secondary RADIUS accounting servers.

3. Click the **Advanced Settings** section.

4. Enter the realm or domain for CLI users.

5. Enter the realm or domain for GUI users.

6. Select the **Use Prefix Notation** check box to use the realm or domain as prefix. If you don’t select the check box, the realm or domain is used as a postfix notation.

7. Save the changes.

### 29.5 Certificate-based Authentication

In on-premises deployments, you can authenticate users using digital certificates. Configure the settings for user authentication from **System > User Accounts > Certificate** option.

There are three authentication criteria:

- Allow access with certificate only
- Allow access without certificate
- Users must provide password along certificate

**Authentication Criteria**

**Allow access without certificate:** The user authentication is performed using the password. The user has to enter the user name and the password at the login prompt. The password may be locally verified by the system or may be verified using the external LDAP or RADIUS authentication service, as appropriate.

**Allow access with certificate only:** The user authentication is performed using the client certificate (such as smart card). The system verifies the client certificate and obtains user identity (user name) from the certificate. Other attributes for the user are retrieved either locally or from the external authentication services such as LDAP or RADIUS, as appropriate.

**Users must provide certificate along with password:** Both client certificate and password are required for the user authentication. The user provides the client certificate and the password at the login prompt. The system verifies the password locally or using the external LDAP or RADIUS authentication service, as appropriate.

---

**Note:** In order to use the certificate-based authentication, ensure that the UI host can access the server using TCP port 4433. If there is a firewall between the UI host and the server, you must open the port 4433 from the host to the server.
Configure Certificate-based Authentication

To configure the certificate-based authentication, do the following:

1. Go to System > User Accounts > Certificate.
2. Enable the Certificate-Based Authentication check box.
3. Select one of the following values from the Use field in certificate as user identity drop down list:
   - CN — Indicates the common name or fully qualified domain name of the web server receiving the certificate.
   - EMAIL — Indicates the email ID of the user.
   - SAN RFC22 Name — Indicates a user identifier name, which include IP address, email address, URI, and other.
   - SAN Principal Name — Indicates the login ID of the user or server.
4. Specify your Authentication Criteria.
5. Click Add Certificate and select the certificate from your local drive. After adding the certificate, you can view the details of the certificate and even delete the certificate.
6. Click the Certificate Revocation checkbox to define the certificate revocation criteria. Note that you must select at least one option in the Certificate Revocation section.
7. Click Use Online Certificate Status Protocol (OCSP) check box to verify the revocation status of digital certificates.
8. Click the Check against Certificate Revocation Lists check box to verify the certificates that are revoked by the issuing certificate authority.
9. Select Valid or Invalid in Treat certificate as when certificate status cannot be confirmed. The default status is Valid.
10. Save the settings.

29.6 User Password Settings

For on-premises deployments, you can configure the minimum requirements for a password in the Password Settings tab. The password settings apply to all user roles - Superuser, Administrator, Operator, and Viewer. If you change the password settings, you can view the details of the certificate and even delete the certificate. Only those passwords that are created after you change the settings are subject to the new password settings. This setting applies only to local authentication and does not apply to LDAP and RADIUS authentication.

To configure password settings, follow these steps:

1. Go to System > User Accounts > Password Settings.
2. Specify the number of characters required for the password. Minimum number of characters is 4, maximum number of characters is 15.
3. Select the check boxes if you want numeric and special characters respectively in the password.
4. Save the changes.

29.7 User Account Suspension

For on-premises deployments, a Superuser can configure the account suspension criteria for other users. Account suspension protects the system from fake logins through dictionary attacks or from multiple failed login attempts. There are four roles available in CVW — Superuser, Administrator, Viewer, and Operator. You can configure different settings for each of these user roles.

Configure Account Suspension

To configure the Account Suspension settings for a user role, do the following:

1. Go to System > User Accounts > Account Suspension.
2. Expand each role and specify the number of failed login attempts and the duration for the account suspension to activate.

3. Specify a suspension time during which the consecutive failed login attempts happen. For example, Consecutive login failures are more than 4 [3 - 10] times in 5 [5 - 30] minutes. Suspension Time is 30 minutes. This indicates that if a user tries to log in 4 times in a duration of 5 minutes, then that user account will be suspended for 30 minutes.

4. Save the changes.
Chapter 30

Introduction to Migration Tool-2

The Migration tool phase 1 was already in use for the migration of model-specific configurations in a device template to universal configurations. Phase 1 had a few limitations. It dealt only with the migration of single, model-specific configurations in a device template to universal configurations.

With phase-2 of the Migration tool, you will be able to migrate all device templates with model-specific configurations to universal configurations. You will see a link to launch the migration tool on folders that have device templates that need migration. The migration link helps to migrate the device templates at a folder even if the default device template is migrated. On selecting a folder, you will see all the templates in that folder.

30.1 How to Launch the Migration Tool

There are two ways you can launch the tool:

1. When you attempt to configure a folder in CloudVision WiFi that is using an outdated template

2. Via the tool tip of the "bird" icon for folders that have outdated templates

30.2 Steps to use Migration Tool

Fixing a template means converting any model-specific configurations in the template to universal configurations. The main page shows templates in that folder that need fixing. The template cards also show details such as the number of devices using the template, configurations in the template, SSIDs using the template, etc.

Click a template to fix it. This opens up the template showing the configurations it contains. Discussed below are two scenarios for a template.
Scenario I - A Model-Specific Configuration is Default

- Consider two types of devices:
  - Type A Devices: Devices that are using this configuration because it is applied as default at their folder in the location tree.
  - Type B Devices: Devices to which this template is applied directly (not via their folder).

- When you fix a template:
  - You can select "Make Default" for one configuration. This makes it the default configuration for that folder (see first card from the left in the screenshot above, the C-60 Config). If this is a model-specific configuration, then fixing the template converts it to a Universal configuration with settings of the original model-specific config (C-60 in the screenshot above). For this configuration:
    - Type A devices using this configuration continue to use it as the default configuration for their folder in the location tree.
    - Type B devices using this configuration form a Group in CloudVision WiFi.
- Configurations that are not being used by any devices are discarded by default. If you uncheck the Discard box, this will create an empty Group for each such configuration.
- For all other configurations in the template, devices using the configuration form Groups regardless of whether they are of Type A or Type B.

**Scenario II - A Universal Configuration is Default**

- Shown above is the alternative scenario - when the second card from the left (Universal Config) is chosen as "Make Default"
- This card has 1 Type A device that continues to use this configuration as default at its location.
- The 2 devices on the C-60 card now go on to form a Group.

Click "Preview" to see the effect of your choices - i.e. to see which devices form groups and which ones continue to use the configuration you have chosen as Default.

Click 'Fix This Template' to confirm.

### 30.3 How to Analyze Location Tree

The migration of device templates can be done effectively by analyzing the entire location tree.

The "Analyze" option in the UI helps to determine which device templates have been fixed by coloring the folder icons with different colors. The "Analyze" option can be viewed in the left panel under the location tree.

1. Click the Auto Migrate option. The location tree will be displayed. You can see the Analyze button at the bottom most part of the tree.
Once you click on Analyze, it starts analyzing the folders. During the analysis, you will not be able to perform any other operations on the Migration Tool.

2. Once the Analysis is completed, you can see red, orange, or green folders depending on their status.
   a. Red - If the folder is colored Red, it means that none of the device templates under that folder has been fixed.
   b. Orange - If the folder is colored orange, it means that some templates have been fixed, while others still need to be fixed.
   c. Green - If the location folder is colored green, it means that all the templates for that folder are fixed.

3. When you click on the folder, you can see all the device templates under that folder that need to be fixed.
When you hover on a folder, it displays the status of the migration.

4. You can see the templates that need to be fixed if the color of the location folder is either red or orange. Click on the template and fix it. If the template was created at a parent folder, then it will throw a message asking you to navigate to the parent folder to fix it.

You will then be navigated to the parent folder and you can fix the template from there.
Appendix A: Configure AP Server Key

You can configure a key or passphrase for authentication and encryption between APs and the server. To configure this key or passphrase:

1. Go to System > AP-Server Key.
2. Select Key or Passphrase and enter a 32-digit hex key or a passphrase between 10 and 27 characters.
3. Save the settings.