User Guide

CloudVision Cognitive Unified Edge 18.0

Arista.com

Arista Networks

DOC-05152-11

Headquarters	Support	Sales
5453 Great America Parkway Santa Clara, CA 95054 USA +1-408-547-5500	+1-408-547-5502 +1-866-476-0000	+1-408-547-5501 +1-866-497-0000
www.arista.com/en/	support@arista.com	sales@arista.com

Contents

Chapter 1

What's New in this Release

This chapter describes features that are new in the 18.0 release of CloudVision Cognitive Unified Edge (CV-CUE).

1.1 Operations

LAN2 Port as Uplink Port

Access Points (AP) can also use LAN2, along with LAN1, as the Uplink Port. If LAN1 and LAN2 are connected and LAN1 fails to receive any packets, the AP can fail over to LAN2 as the Uplink Port and will continue to operate on the same uplink even if LAN1 is active again. The AP will switch to LAN1 again as the Uplink only when LAN2 is inactive or disabled.

AP Platforms Supporting this Feature: C-250/C-260, C-330, C-360, C-460, C-460E Series.

Customize SSID Attributes for Location Specific Overrides

Administrators can override certain attributes of an SSID at a child location without breaking the inheritance, so the entire SSID configuration remains the same except for the overridden attributes.

VLAN Pooling in SSID Settings

Network Administrators can define a VLAN Pool in SSID Settings, which is a list of VLAN IDs for Access Points (AP) to distribute to clients connecting to the SSID. VLAN Pooling offers better scalability and optimized load-balancing of traffic.

RADIUS Pooling in SSID Settings

RADIUS Pooling lets Network Administrators assign a pre-defined list of RADIUS Servers that Access Points (AP) can use to authenticate, authorize, and maintain clients' accounts. It offers better load-balancing capabilities and improved scalability.

Reject Clients Using Locally Administered MAC Addresses

Network Administrators can prevent clients that use locally administered MAC addresses from accessing your network. This feature ensures that only clients that use their device’s globally unique MAC addresses can connect to the network.

On-Demand Transmit Power Control and Auto-Channel Selection

Network Administrators can start the Auto-Channel Selection (ACS) Mode and Transmit Power Control (TPC) Mode for a radio on demand. In ACS Mode, the Access Point (AP) scans the network to select the best channel. In Auto-TPC Mode, the AP automatically adjusts its transmit power to minimize interference with neighboring Arista APs.

1.2 Monitoring and Troubleshooting

Timer-Based Window to Onboard Access Points After Changing the Communication Key

When Network Administrators change the AP-Server Communication Key, some APs may fail to connect to the server. Administrators can enable the onboarding window from CV-CUE and allow such APs to connect using the Default Key or the Old Key.

1.3 Third-Party Integrations

Google Chat and Microsoft Teams Webhook for Feed

Along with Slack, Network Administrators can configure Google Chat and Microsoft Teams Webhook to receive alerts whenever a network issue or anomaly is detected.

Forward Client DHCP Packets to Destination Servers

Send a copy of DHCP Packets from Access Points (AP) to Network Access Control (NAC) solutions for profiling clients and assigning appropriate network segments.

Chapter 2

What's New in CV-CUE 18.0 User Guide

The following table lists changes made in CV-CUE 18.0 User Guide:

Table 1: Guide Updates for 18.0 Release

Topic	Description
Customize SSID Attributes for Location-Specific Overrides	New topic. New feature introduced in this release.
Configure SSID Network Settings	Modified topic. Added information about DHCP Packet Forwarding setting.
SSID Network Settings	Modified topic. Added information about DHCP Packet Forwarding setting.
FEED	Modified topic. Added information about configuring Google Chat and Microsoft Teams webhook.
On-Demand Transmit Power Control and Auto-Channel Selection	New topic. New feature introduced in this release.
SSID VLAN Pooling	New topic. New feature introduced in this release.
SSID RADIUS Pooling	New topic. New feature introduced in this release.
Appendix A: AP Server Communication Workflow	New topic to explain the modified AP Server Communication Workflow.
SSID Security Settings	Modified topic. • Moved 802.11r setting to RF Optimization topic to reflect the updated navigation flow. • Added information about Deny Locally-Administered MAC Addresses setting.
Configure RF Optimization in SSID Profile	Modified topic. Removed Over the DS setting.
Configure 802.11be Enhancements	New topic. Feature introduced in 17.1 release.
SSID WiFi 7 Setting - Multi-Link Operation	New topic. Feature introduced in 17.1 release.

Chapter 3

Access CV-CUE

CloudVision Cognitive Unified Edge (CV-CUE) is a part of the Arista Cloud services. To access CV-CUE, you must log in to Launchpad.

You get the same user privileges in CV-CUE 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 CV-CUE as a Superuser.

Perform the following steps to access CV-CUE:

1. Log in to Launchpad. Refer the *Launchpad User Guide* for more information.

   Result: 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 CV-CUE tile under **Apps** to access CV-CUE.

This chapter contains the following topics:

- Get Details of CV-CUE Version, Build, and License Agreement
- Get Details of Logged In User
- Sign Out of CV-CUE
- View Open Source Software Licenses

3.1 Get Details of CV-CUE Version, Build, and License Agreement

The page displays the version number, build number, the terms and conditions, and the license agreement for CV-CUE.

To view the CV-CUE version number, build number, and license agreement:

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

Option	Description
Version	Version number of CV-CUE
Build	Build number of CV-CUE
Service Build	Build number of Wireless Manager

3.2 Get Details of Logged In User

You can view the basic information of the user who is logged in to CV-CUE.

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:

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

3.3 Sign Out of CV-CUE

You can sign out of CV-CUE and its services.

To sign out of CV-CUE, 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**.

   Result: You will be signed out and redirected to the Launchpad Sign In page.

3.4 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 CV-CUE and click the CV-CUE icon at the top-left corner.
2. Under OSS Licenses, click the link for each component. The license is downloaded to your local drive.

Chapter 4

Common Operations

This chapter contains the following topics:

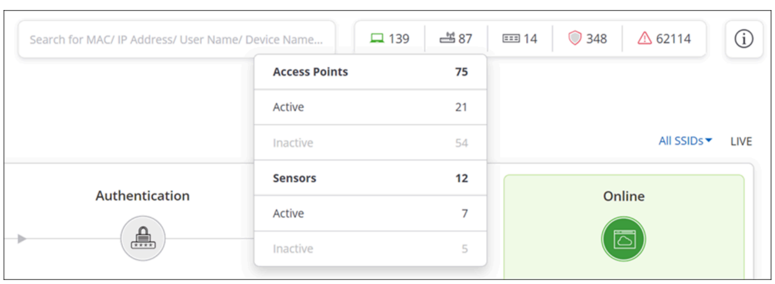
- Wi-Fi Network Counters
- Search
- Table level Operations
- Filters
- IPv6 Support in UI Fields

4.1 Wi-Fi Network Counters

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

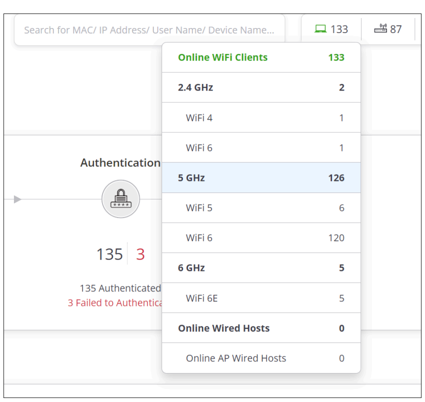
Managed Wi-Fi Devices 

Active and inactive status of managed Wi-Fi devices including Access Points (APs), sensors and network detectors, and if any of the devices are running an outdated firmware version or configuration.



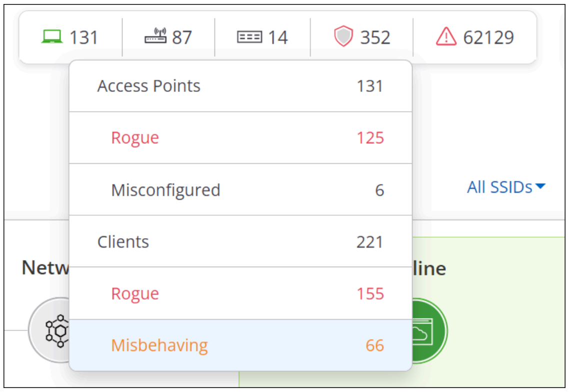
Wi-Fi Clients

Types of clients that are currently connected to the managed Wi-Fi network.



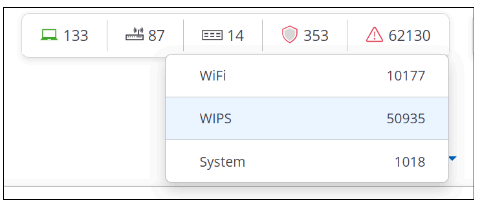
Threat-Posing Devices

Presence of threat-posing devices, such as, rogue, misconfigured APs, rogue clients, misbehaving authorized clients.



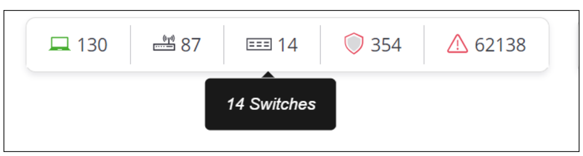
Alerts

Raised alerts related to Wi-Fi performance and security, and system health.



Switches

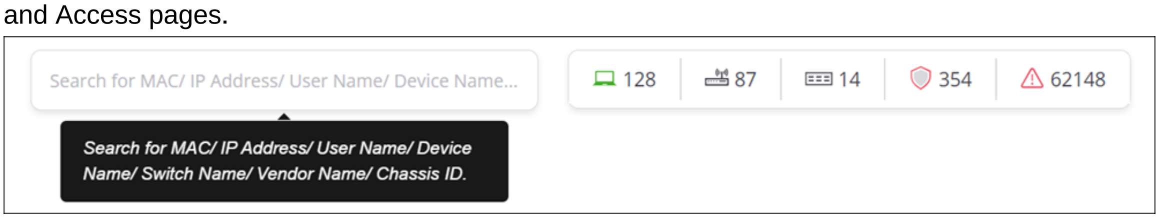
Total number of switches, active switches, inactive switches, and discovered switches.



4.2 Search

Global search helps to find a client, AP, or switches by typing the MAC or IP address, user name, switch 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, Switch Name, or the device name in the **Global Search** box, a detailed information of the device is displayed. Refer to Clients, Access Points or Switch 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, access points, managed switches and discovered switches. 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 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*`.

4.3 Table level Operations

CV-CUE 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.

4.3.1 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.

   List of all the columns with checkbox adjacent to their names appear.
2. Select or unselect the column you prefer to freeze or unfreeze.

4.3.2 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.

4.4 Filters

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

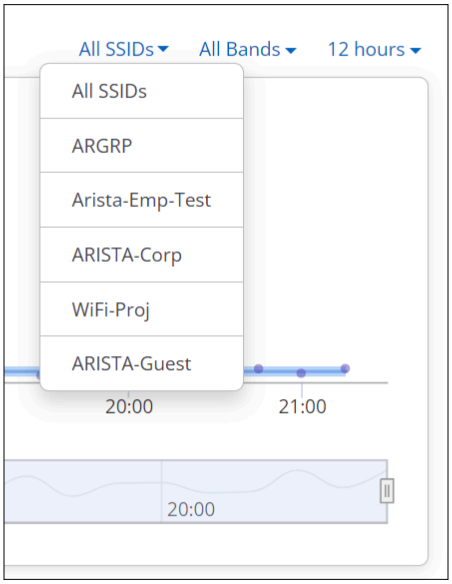
The available filters are:

- 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**.

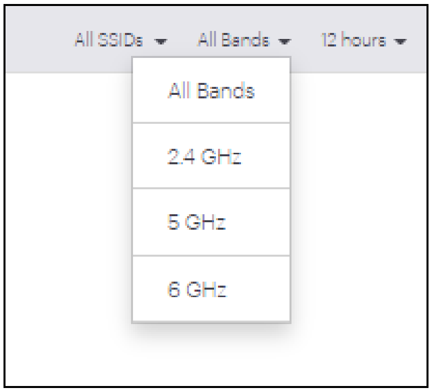


Frequency Band Filter

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
- 6 GHz
- All Bands

The default value is **All Bands**.



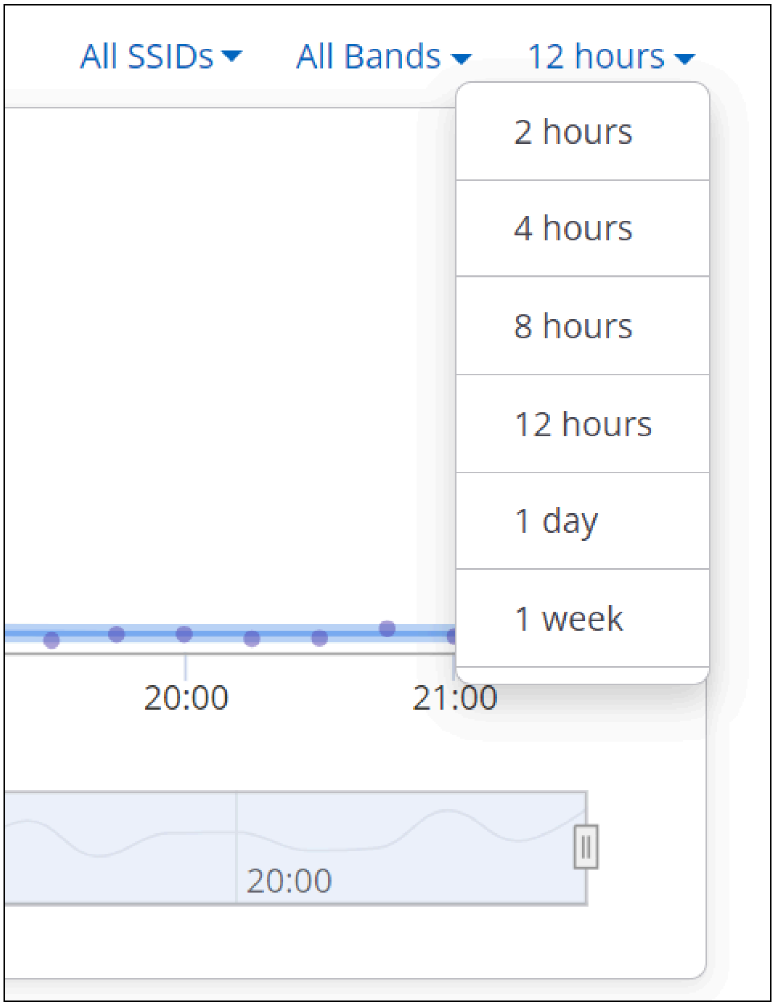
Duration Filter

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.

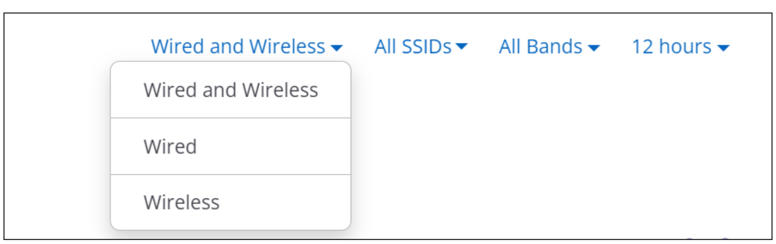
Note: All the provided time intervals may not be available for every widget.



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 and Wireless
- Wired
- Wireless



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

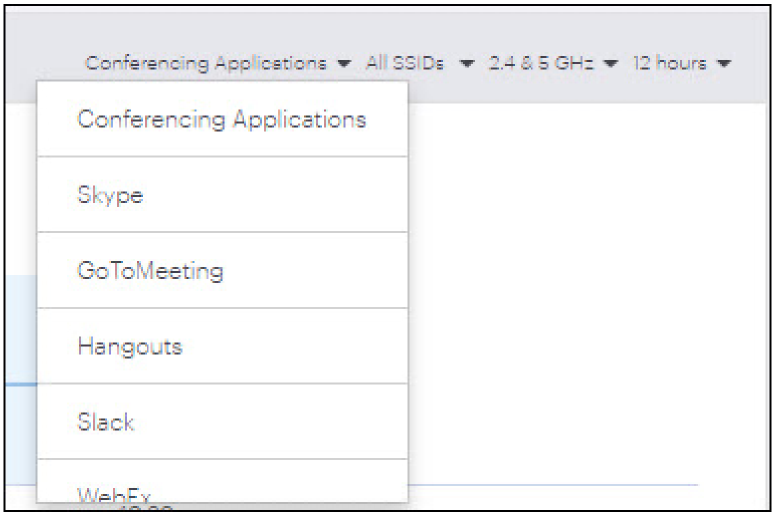
Conferencing Applications Filter

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.

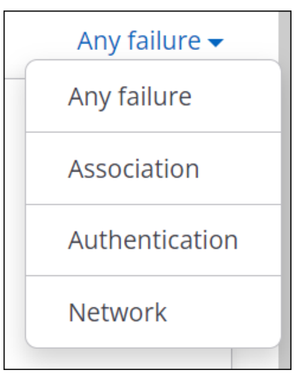


Any Failure

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**.



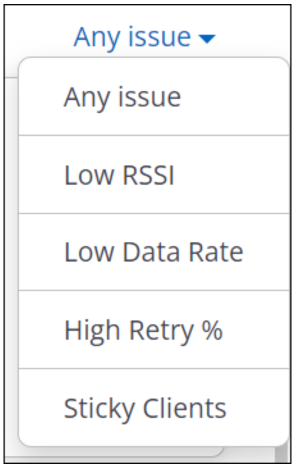
Any Issue

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

- Any issue
- Low RSSI
- Low Data Rate
- High Retry Percentage

- Sticky Clients

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



4.5 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.

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

UI Element		**Supports IPv4**	**Supports IPv6**
	IP Address/Hostname under Custom Application Test	Y	N
System Tab			
SMTP	SMTP Server IP	Y	N
SNMP-Alerts	SNMP Trap Destination Server IP/Hostname	Y	N
Syslog	Syslog Server IP/ Hostname	Y	N
WLAN Integration	Aruba Controller IP/ Hostname	Y	N
	Cisco Controller IP/ Hostname	Y	N

Chapter 5

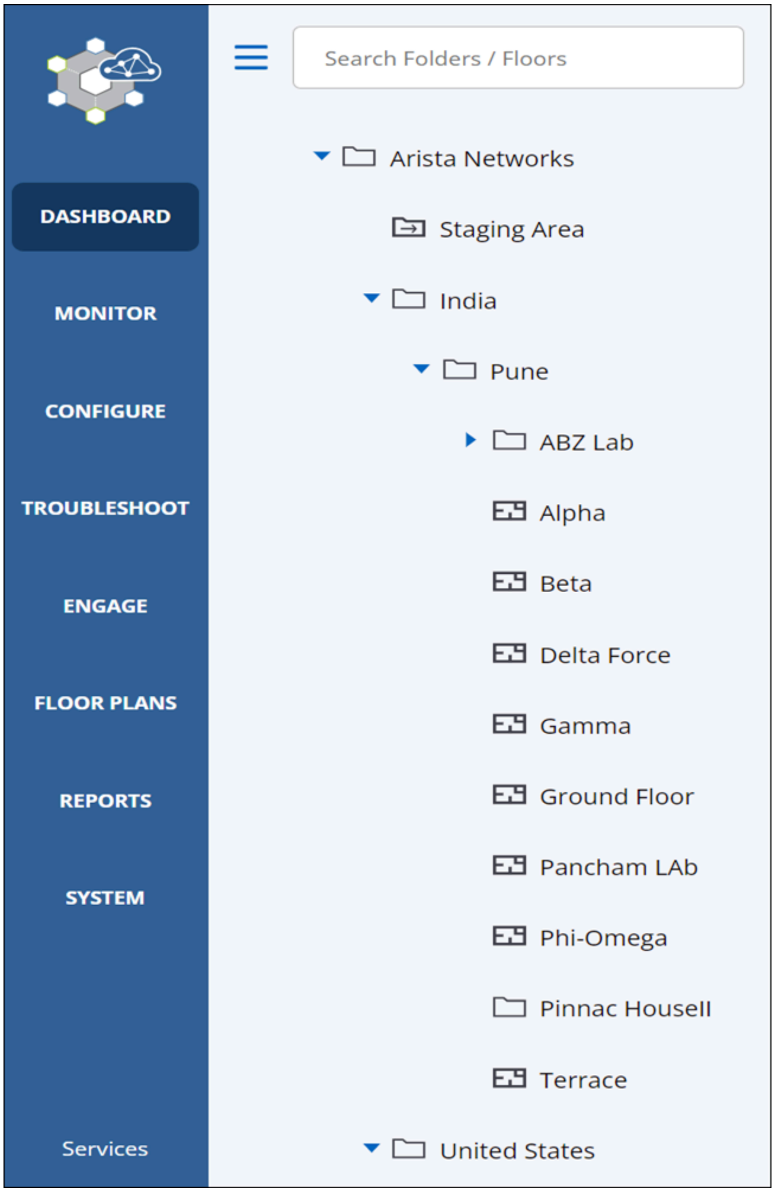
Managing Navigator

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.

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 Navigator. Users with the Viewer role can only view the Navigator.

The following figure shows the Navigator. Right-click on a folder or a floor to perform various tasks and edit the Navigator.



This chapter contains the following topics:

- Add a Folder or Floor
- Add Multiple Folders or Floors
- Delete Folders and Floors
- Rename Folder or Floor
- Search Folder or Floor
- Set Timezone for Folders
- Set Location Tag
- Introduction to Groups

5.1 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**.
2. Select a folder under which you want to add a new folder or floor. Right-click and select **Add a Folder/ Floor**.
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**.

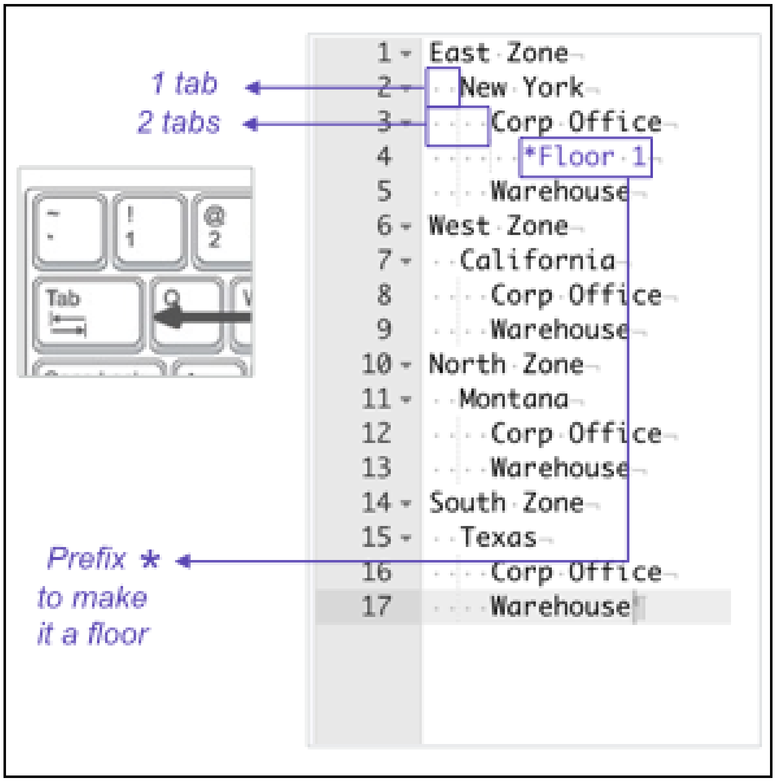
Important: You cannot add a folder or floor under a floor.

5.2 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**.
2. Right-click a folder under which you want to add multiple folders and floors and select **Add Multiple Folders/Floors**.
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**.

5.3 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**.
2. Select the folders and floors that you want to delete.
3. Right-click any of the selected folder or floor and select **Delete**.
4. Click **Delete** to confirm the deletion.

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

5.4 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**.
2. Select the folders and floors that you want to rename.
3. Right-click any of the selected folder or floor and select **Rename**.
4. Do the required changes and click **Rename** to save the changes.

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

5.5 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**.
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.

5.6 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**.
3. Select the appropriate timezone from the drop-down list and click **Set**.

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

5.7 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 Wi-Fi 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.

5.8 Introduction to Groups

Until now CV-CUE allowed users to configure only the Wi-Fi configuration for a selected location. You could not do custom configuration on a device or a set of devices. To overcome this restriction, Groups have been introduced in CV-CUE.

Groups will facilitate faster customization of Arista APs by allowing you to apply custom configuration (for example, 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**.

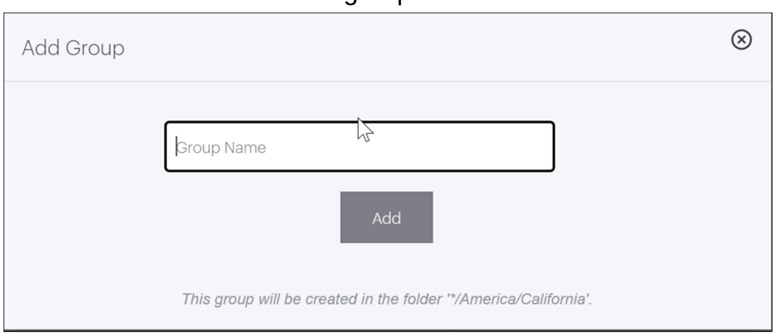
AP's in a configured group use the same configuration as the group. Moreover, each group has a single Wi-Fi configuration. APs which are not part of any group will continue to use the Wi-Fi configuration of the location on which they are created. When you delete a location, groups at the deleted location 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.

5.8.1 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.



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

Note: The group name should be unique across all the available groups and folders.CV-CUE 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.

5.8.2 Groups Actions

There are certain actions that can be performed on an individual group. The list of actions is:

- Show Assigned Devices
- Rename a Group
- Delete a Group

5.8.2.1 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.

5.8.2.2 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.

5.8.2.3 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 Wi-Fi 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 Wi-Fi configuration of their respective folders.

To delete a group, perform the following steps:

1. Go to **System > Navigator > Groups**.
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**.

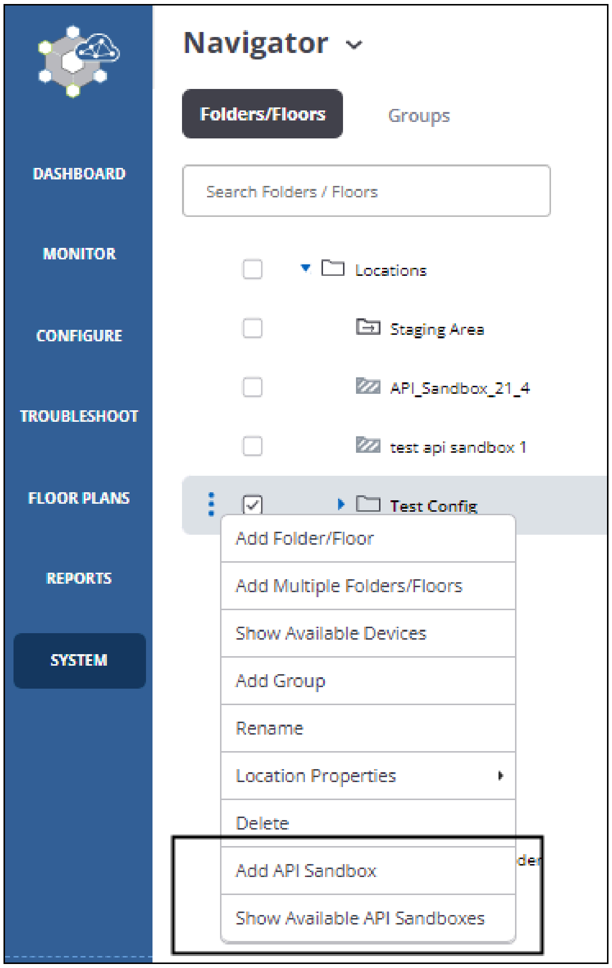
5.9 API Sandbox

API Sandbox allows you to try and test out APIs in the API sandbox without altering the data in your production environment. API Sandbox allows you to test the features programmatically by invoking APIs in a test environment for the selected location.

You can create an API sandbox for any location. The API sandbox provides an environment that is a clone of the selected folder location.

Creating an API Sandbox

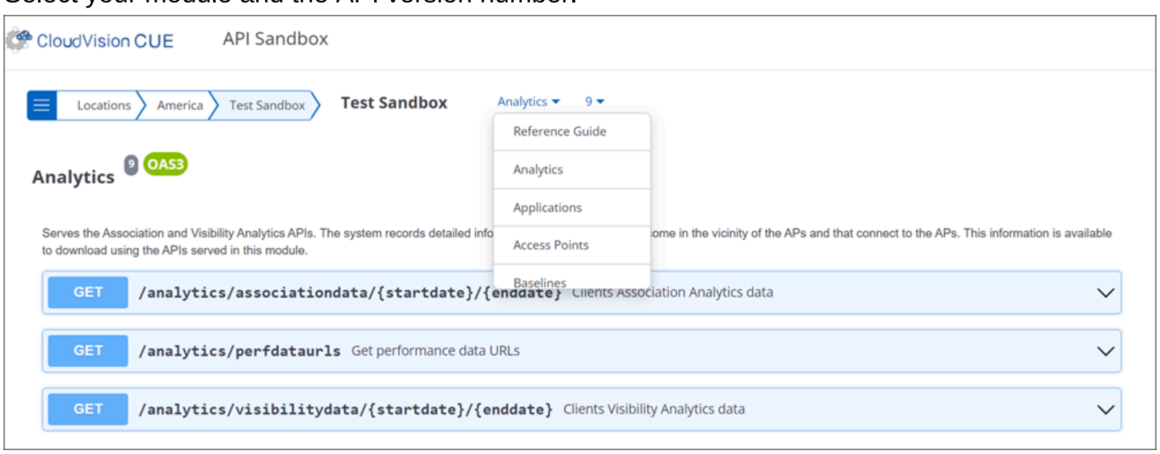
1. Navigate to **SYSTEM** > **Navigator** > **Folders/Floors** > **right-click a folder location** > **Add API Sandbox.**
2. Provide a name and description for the API Sandbox and click **Create.**



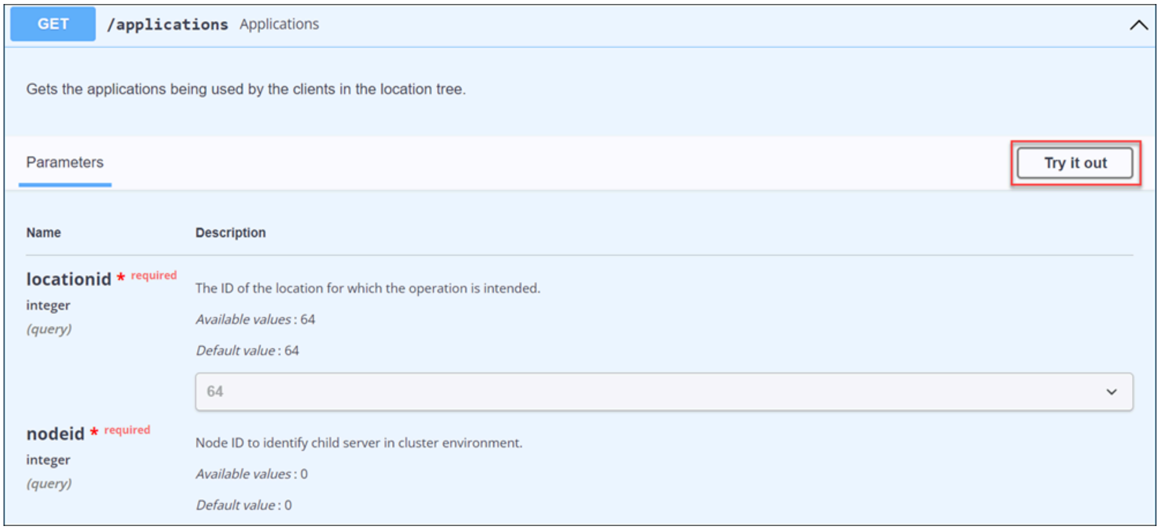
Executing APIs in the Sandbox

To try out the APIs in the sandbox:

1. Navigate to your location and click **Show Available API Sandboxes.**
2. Click your API sandbox. The API Sandbox portal opens.
3. Select your module and the API version number.



4. Click the **Try it Out** button next to the API you want to try.



5. Provide the required request parameters and click **Execute.**

Chapter 6

Baselines

CV-CUE 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.

This chapter contains the following topics:

- Baselines versus Thresholds
- How to Read a Baseline Graph?
- CV-CUE Baselines
- Data Reporting and Retention
- Data Point Drill Down

6.1 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%.

CV-CUE 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.

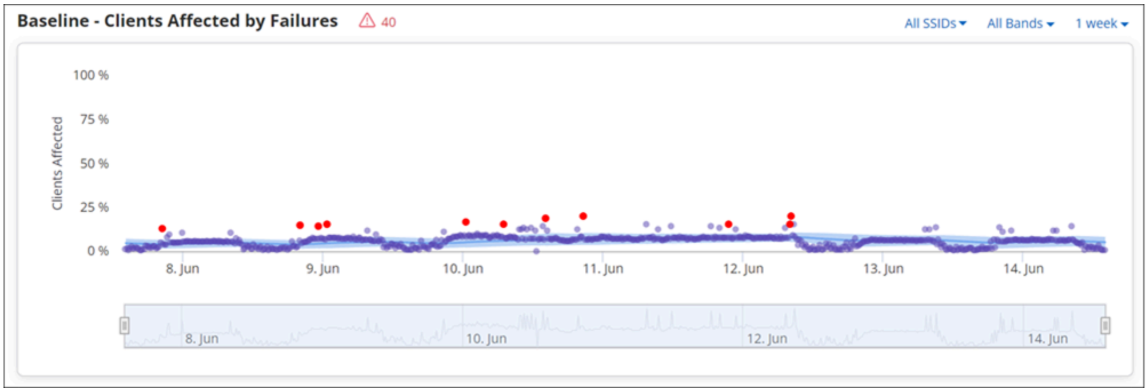
Thresholds are good for monitoring information where there is a clear, non-arbitrary delineation between acceptable and not acceptable. Thresholds are static. They do not adjust to changing conditions. Wireless networks are dynamic and change over time. The normal level of retry rates may be very different today and a month from now. Clients change, environments change, applications change, and usage changes rapidly. A static threshold is a challenge because it does not 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.

6.2 How to Read a Baseline Graph?

CV-CUE 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 Wi-Fi is first set up with only a few clients. Later, when many more clients are added to the Wi-Fi 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 graphs 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.

6.3 CV-CUE Baselines

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

Note: Wherever applicable, CV-CUE shows separate baselines for IPv4 and IPv6.

Type	Baseline Chart	Per	Location on CV-CUE UI
Connectivity	Clients Affected by Failures	Location	DASHBOARD > Connectivity
		AP	MONITOR > Access Points > AP Drill Down
	Baseline - AAA Latency	Location	Dashboard > Performance > Avg. Latencies Chart > AAA Drill Down
	Baseline - DHCP Latency	Location	Dashboard > Performance > Avg. Latencies Chart > DHCP Drill Down
	Baseline - DNS Latency	Location	Dashboard > Performance > Avg. Latencies Chart > DNS Drill Down
Performance	Data Rate	Client	MONITOR > Clients > Clients Drill Down
	RSSI	Client	MONITOR > Clients >Clients Drill Down
	Retry Rate %	AP	MONITOR > Access Points > AP Drill Down
	Client Affected by Poor Performance	Location	Dashboard > Performance
		AP	MONITOR > Access Points > AP Drill Down
	Clients Affected by Poor App Experience	AP	MONITOR > Access Points > AP Drill Down
	Clients Affected	Location	Dashboard > Applications
	% Poor Application Experience	Location	Dashboard > Applications
	Baseline - Application Latency	Location	Dashboard > Performance > Avg. Latencies Chart > Application Drill Down

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

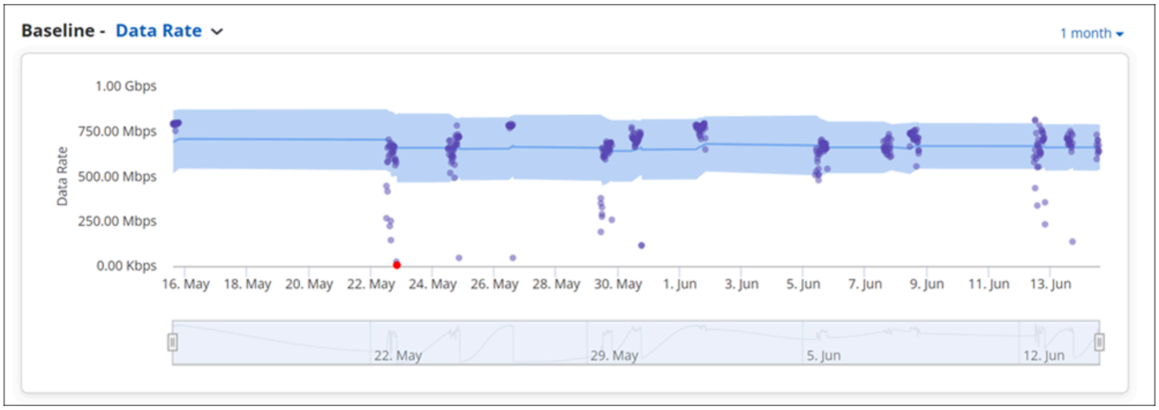
Example 1: Baseline - Clients Affected by Failures (AP Based)

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.

6.4 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 CV-CUE.

Data Type	AP Reporting Interval	Cloud Storage Duration
Client Connection Attempts	Immediately	1 week
AAA, DHCP, DNS. & TCP Latencies	Soon after detection	1 week
Client Application Data	15 minutes	12 hours
Client Performance Metrics	15 minutes	1 week
BSSID Performance Metrics	15 minutes	1 week
SSID Application Data	15 minutes	1 week
Baseline Data	15 minutes	1 week

6.5 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.

Option	**Description**
Name	Name of the client.
User Name	User name of the client.
MAC Address	A unique 48-bit IEEE format address of the client assigned to the network adapter by the manufacturer.
Last Failure Time*(Available for Baseline - Clients affected by failure)*	The latest date and time when the client failed to connect to the network.
Associated SSID	SSID of the WLAN to which the client is connected.
Associated Access Point	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.
Location	Location of the client.
IP Address	IP address of the client.
Protocol	Indicates the 802.11 protocol used.
Channel	Operating channel of the AP to which the client attempted to connect
OS	Name of operating system running on the client.
Average RSSI(dBm)	The observed RSSI (Received Signal Strength Indicator) value for the client.
Up/Down Since	The latest date and time since when the client is up or down.
Connected/Disconnected Since *(Available for Baseline - Clients Affected by Poor Performance graphs)*	
First Detected At	The date and time when the client was first detected.
Role	The role assigned to the client on associating with an SSID.
Google Authorized	A boolean value indicating whether the client is in the authorized list of clients imported through Google Integration.
Vendor Name	Indicates the vendor name.
Uplink Data *(Available for Baseline - Clients Affected by Poor Performance graphs)*	The amount of data transferred by the client.

Option	Description
Downlink Data *(Available for Baseline - Clients Affected by Poor Performance graphs)*	The amount of data received by the client.
Retry Rate *(Not available for Baseline - Clients affected by failure)*	The retry rate in percentage.
Sticky *(Not available for Baseline - Clients affected by failure)*	A boolean value indicating if the client is a "sticky client", i.e., if it is connected to an AP even though it sees better signal strength from a neighboring AP.
Application Name *(Available for Baseline - Poor Application Experience)*	Name of an application.
Application Usage Time *(Available for Baseline - Poor Application Experience)*	The time duration for which a client has accessed an application.
Poor Application Experience *(Available for Baseline - Poor Application Experience)*	The poor application usage experience for a client connection.
Uplink Bitrate *(Available for Baseline - Poor Application Experience)*	The rate at which the client transmits data (in bits).
Downlink Bitrate (Available for Baseline - Poor Application Experience)	The rate at which the client receives data (in bits).
Downlink Jitter *(Available for Baseline - Poor Application Experience)*	Variation in the delay of packets received by a client. It is used to measure the quality of VoIP applications.
Uplink Jitter *(Available for Baseline - Poor Application Experience)*	Variation in the delay of packets transferred by a client. It is used to measure the quality of VoIP applications.

Chapter 7

Dashboards

CV-CUE 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.

This chapter contains the following topics:

7.1 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

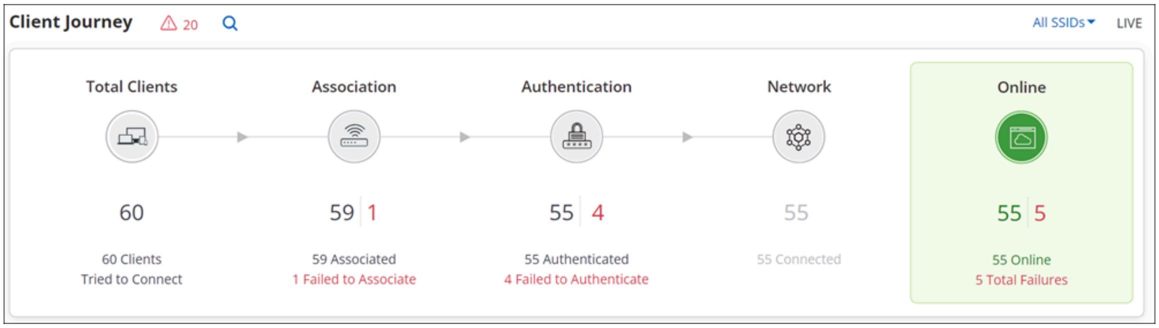
Displays the top five locations which are affected by association, authentication or network failure. The locations are listed in decreasing order based on the percentage of connection failures.

Baseline - Clients Affected by Failures

CV-CUE 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.

7.1.1 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 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

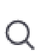
The **Authentication** section displays the total number successfully authenticated clients and the clients that failed to authenticate through the Wi-Fi network.

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.

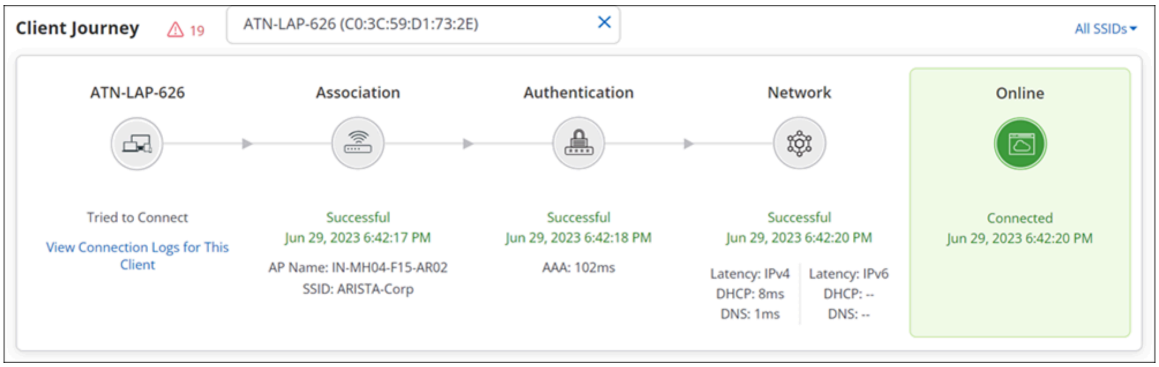
Search Icon on Client Journey

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:

Option	Description
Tried to connect	Name of the client and a link that redirects you to the Connection log for the searched active client.
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.

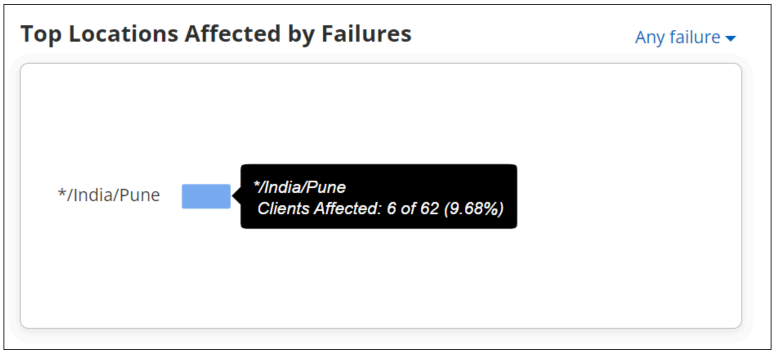
7.1.2 Top Locations Affected by Failures

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.

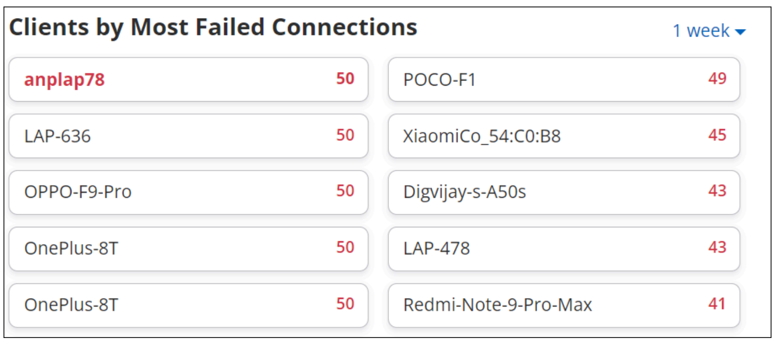
You can select the failure type from the drop-down list given on the top-right corner of the widget. To know more about the **Any failure** filter refer Filters on Widgets.



7.1.3 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.



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.

7.2 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:

Client Health

Displays the total number of clients for the selected folder or floor, with Low RSSI, Low Data Rate, High Retry %, and Sticky Clients.

Avg Latencies

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.

Baseline - Clients Affected by Poor Performance

Displays the baseline for the percentage of clients affected by poor performance for all the clients over a period of time.

Clients by Avg. Data Rate

Displays a bar graph that shows the average data rate of the clients on a selected folder or floor.

Clients by RSSI

Displays a bar graph showing the total number of clients and the RSSI values.

Clients With Most Traffic

Displays a horizontal bar graph of clients with highest data usage.

Top Locations Affected by Poor Performance

Displays a horizontal bar graph of locations with highest performance issues, in a decreasing order.

Network Usage

Displays a line graph showing the number of client association and and a bar graph that shows the traffic volume.

7.2.1 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. CV-CUE ensures that such clients are not 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.

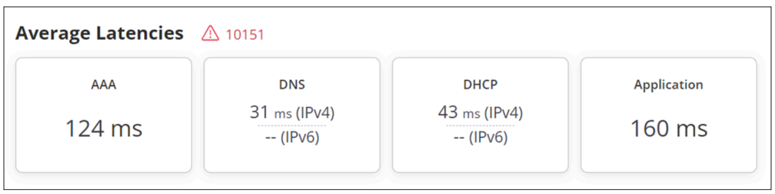
Note: For more information on setting threshold values, refer Set Threshold for a Folder or Floor.

7.2.2 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

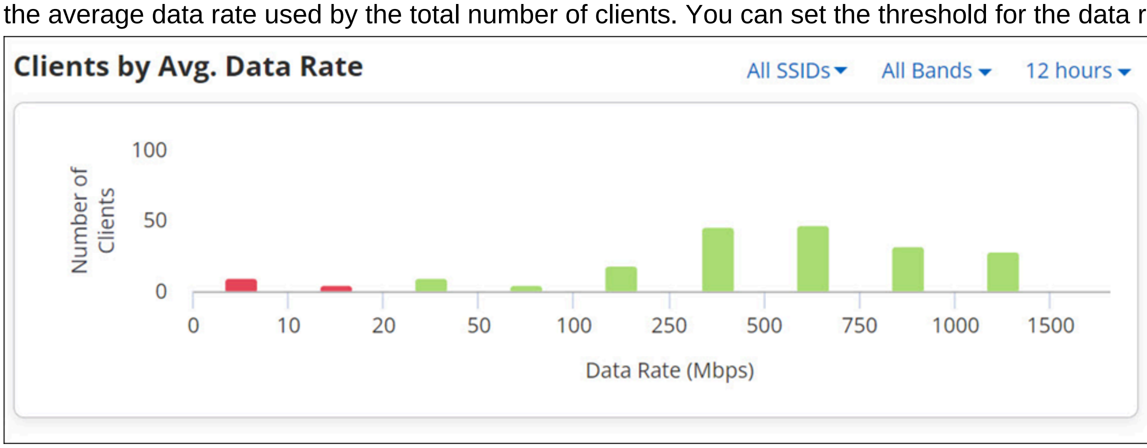


When you click on a latency, you can view the baseline graph for that latency.

7.2.3 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.

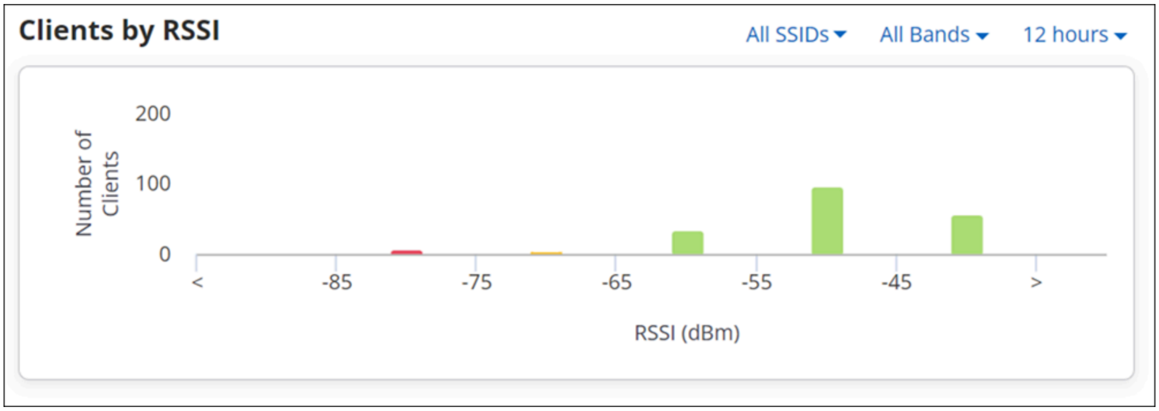
Refer to Set Threshold for a Folder or Floor for more information on how to set a threshold value.

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 to Filters on Widgets.

7.2.4 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:

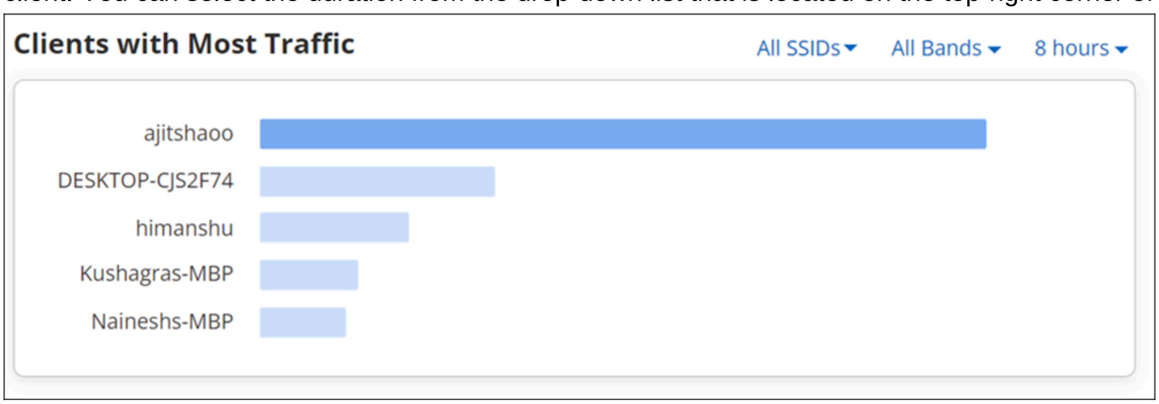
- The clients with RSSI, below the set threshold value are in red.
- The clients with RSSI above the set threshold value are in green.
- The clients that are in the bucket where the threshold value falls, are in yellow. For example, in the above image, a threshold value that is set as -60 dBm, falls 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 to Set Threshold for a Folder or Floor for more information on how to set a threshold value.

7.2.5 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 to Filters on Widgets.

7.2.6 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.

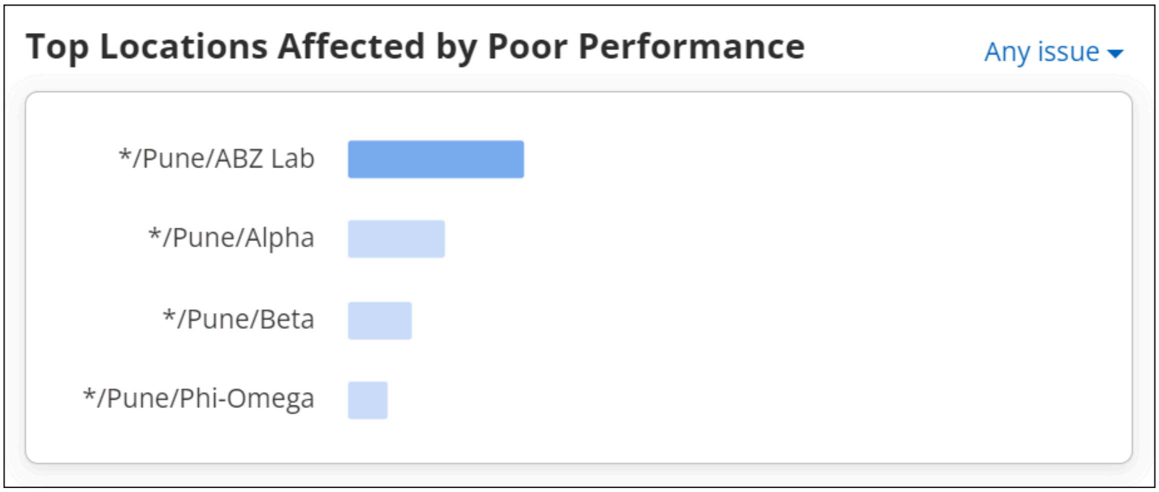
The poor performance is calculated based on the following factors:

- 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.

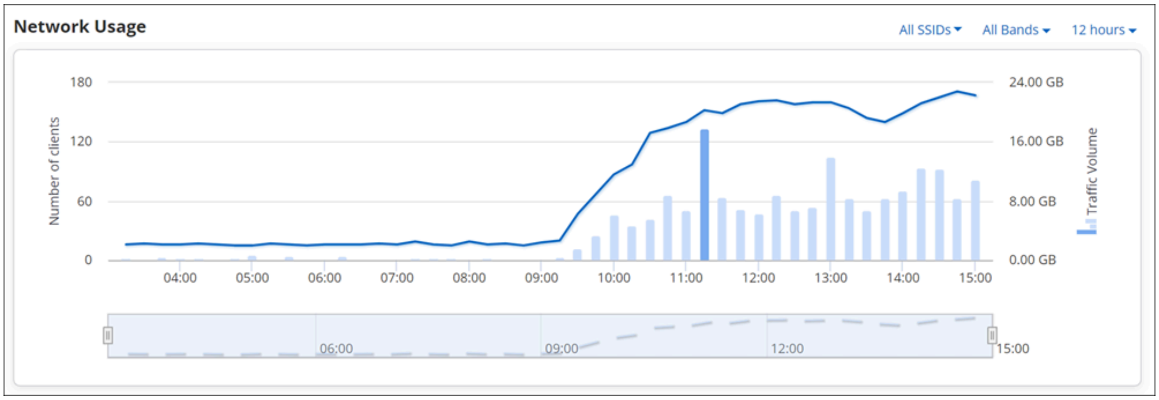


The data on the widget can be filtered using the available filters on the top right corner of the widget. To know more about the filters refer to Filters on Widgets.

7.2.7 Network Usage

You can access the Network Usage chart in two different ways from CV-CUE 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 to 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 to 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.

7.2.8 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:

Threshold Name	Values
Data Rate	20 Mbps to 100 Mbps For example, if the threshold value is 80, clients below the set Data Rate threshold will be classified as Low Data Rate clients.
RSSI	-45 dBm to -75 dBm For example, if the threshold value is -60, the clients below the set RSSI threshold will be classified as Low RSSI clients

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.

7.3 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.

7.3.1 Application Experience

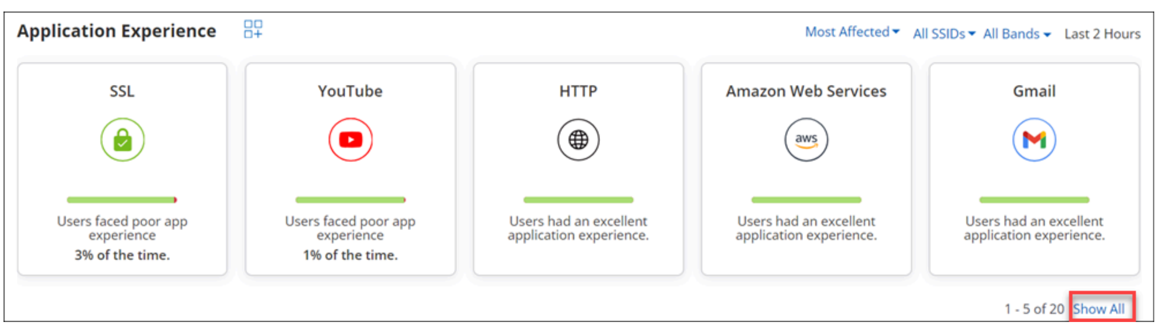
Navigate to **Dashboard** > **Applications** to view the Application Experience chart. You can monitor the performance of web-based enterprise applications (such as Email applications, HR and Project Management applications, Intranet, Online Drive, and others) along with VOIP-based applications such 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, CV-CUE 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 does not inspect the user's data in the process.
- Only Wi-Fi 5 and higher 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 is 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
- 6 GHz
- All Bands

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 - Sessions
- Application Traffic - Clients
- Application Traffic - Quality of Experience
- Clients with Most Application Traffic
- Clients using this Application

7.3.2 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 not have a different Web QoE setting for each folder in the Navigation tree.

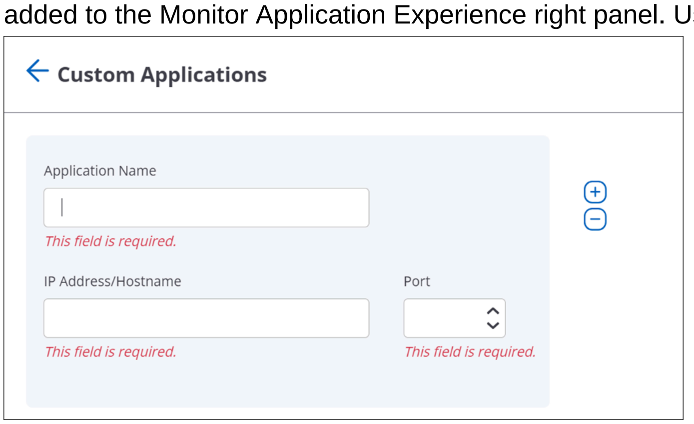
1. Go to **DASHBOARD** > **Applications** tab. Ensure that you are at the root folder.
2. On the Application Experience widget, click the **Monitor Application Experience** icon.
3. On the Monitor Application Experience right panel, click **Add** to monitor the applications. You can add up to 25 applications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

7.3.3 Monitor Custom Applications

Your organization may use applications that are not predefined in CV-CUE. 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:

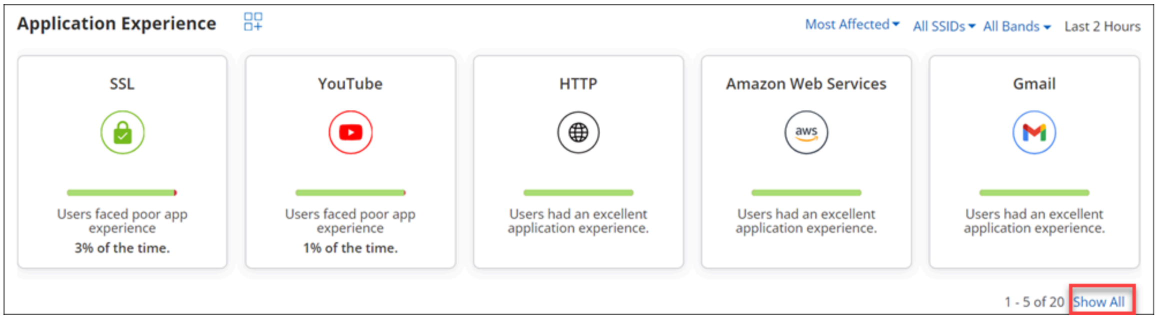
1. Go to **DASHBOARD** > **Applications** tab. Ensure that you are at the root folder.
2. On the Application Experience widget, click the **Monitor Application Experience** icon.
3. On the Monitor Application Experience right panel, click **Custom Applications**.
4. Provide the Application Name, IP address 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.



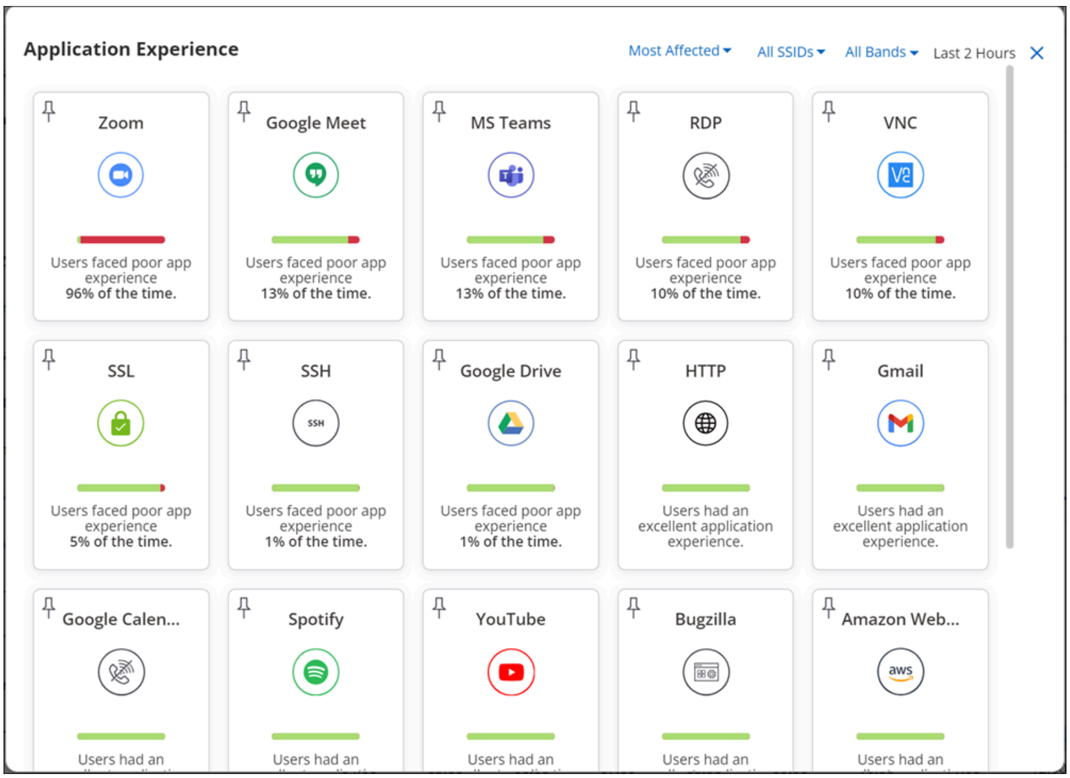
5. Save the applications.
6. On the Monitor Application Experience right panel, search the custom application and click **Add**.

7.3.4 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 20 applications, click **Show All**.



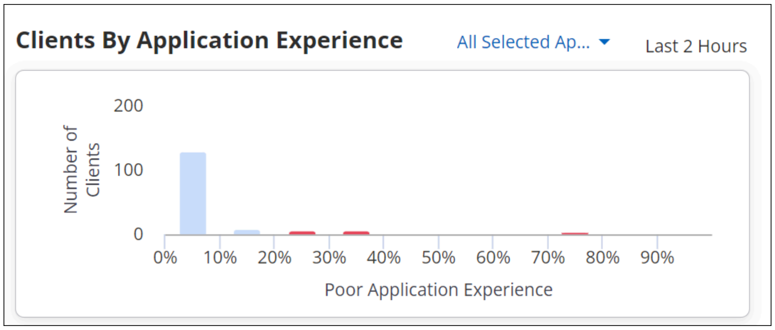
You can choose which applications you want to view on the landing page by pinning your desired applications. To pin the applications on the Dashboard landing page for default view, click **Show All** in the Application Experience widget. Pin the application using the **Pin** button.



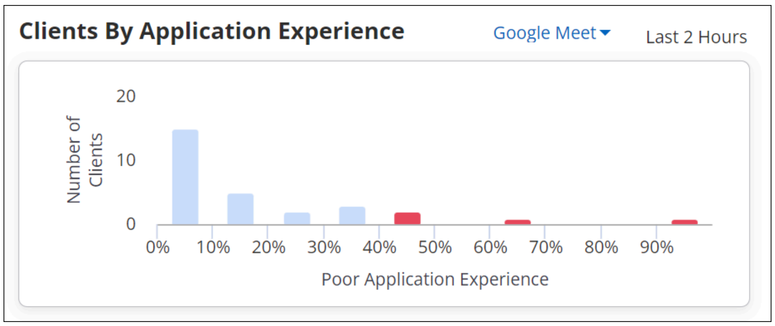
If you don not pin any applications, then CV-CUE displays the applications based on its usage or application experience. Use the **Most Affected** or **Most Used** filter to view the applications without pining them.

7.3.5 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 Meet application in the last 2 hours. So, from the image you can infer that in the past 2 hours, 1 client faced poor application experience between 90 to 100 percent of the time, which indicates a bad user experience. Similarly, around 15 clients faced poor application experience between 0 to 10 percent of the time, which indicates a good user experience.



7.4 Logical Categorization of Clients and Failures

CV-CUE creates logical categories of clients, grouping them based on properties such as their band of operation (2.4, 5, or 6 GHz), 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.

CV-CUE 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.

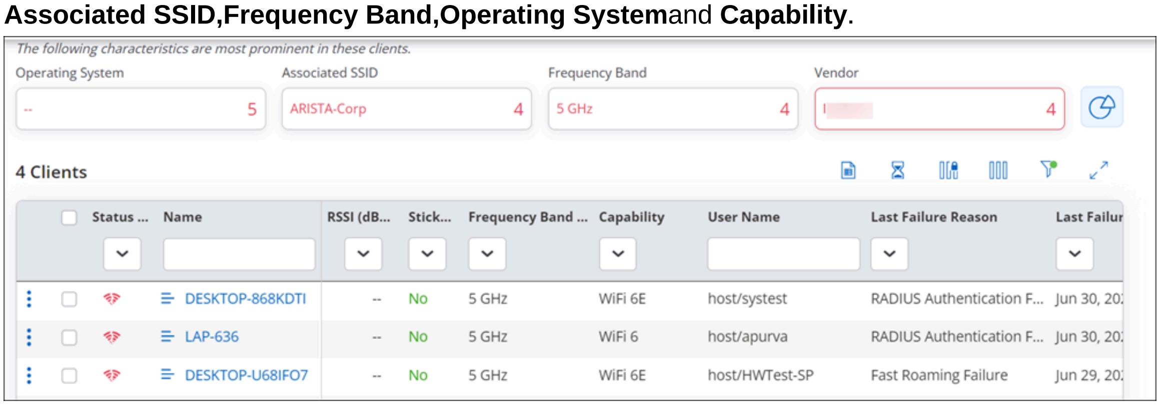
7.4.1 Drill-Down by Logical Client Category

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**.

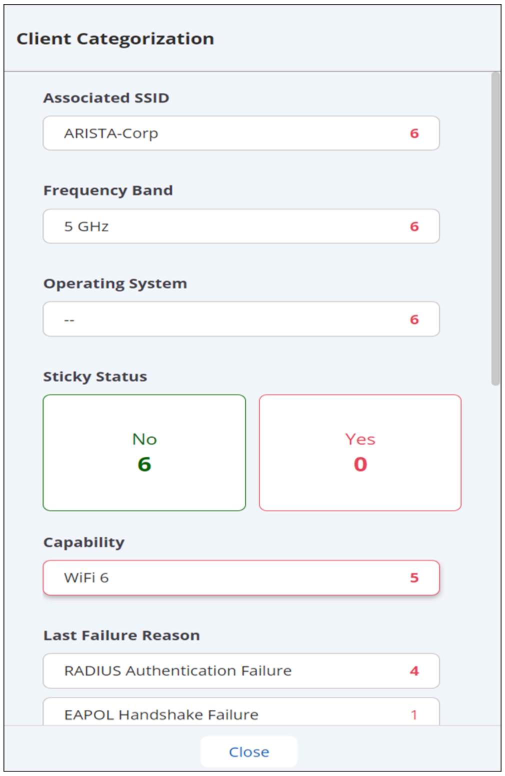
   You will see the list of clients that failed authentication, with filter tabs for the most prominent characteristics, i.e., logical groupings. For example, the following figure shows tabs for **Associated SSID,Frequency Band,Operating System**and **Capability**.



3. Select the characteristic (for example, logical category) by which you want to filter the list of clients. For example, to see the list of clients with WiFi 6 Capability that failed authentication, click the **Capability** filter tab.

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.



7.5 Infrastructure Dashboard

The Infrastructure Dashboard that provides an overview of the health of all managed access points (APs).

Navigate to **Dashboard** > **Infrastruture** to view the Infrastuture Dashboard.

Infrastructure Dashboard charts consider the CPU Utilization and Memory Utilization of all the APs present at a server to calculate the average CPU Utilization and Memory Utilization based on the different selected criterias. The average is used as the threshold to point out the APs that have higher than average CPU and Memory Utilization.

Note: You must have Aeris enabled on your server to leverage this feature.

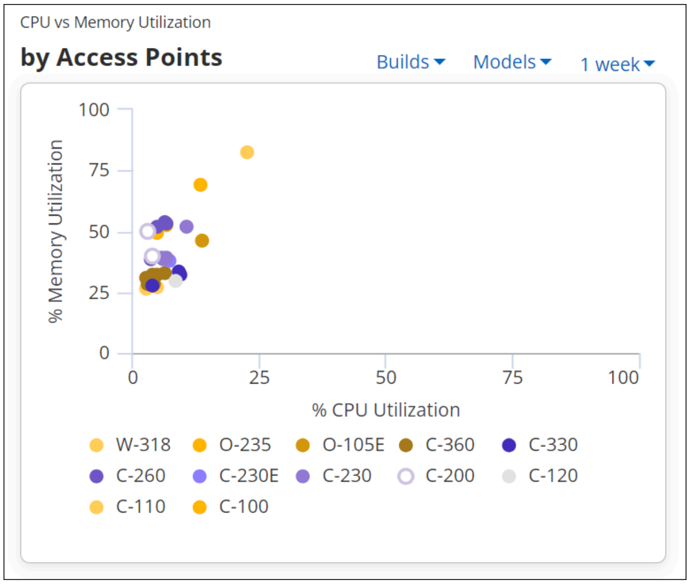
With the Infrastructure Dashboard, network administrators can get the health check of all the APs installed at a particular location. In case of network failure, network administrators can use the dashboard to identify APs showing anomalous behavior. Infrastructure Dashboard also allows network administrators to take preventative and corrective actions based on the health insights. It helps them identify APs that have high CPU or memory utilization which might lead to network downtime because of reboot or panic due to high utilization.

Infrastructure Dashboard consists of the following charts:

- CPU vs Memory Utilization by Access Point
- CPU vs Memory Utilization by Location
- Access Points by CPU Utilization
- Access Points by Memory Utilization
- Trend - CPU Utilization/Memory Utilization

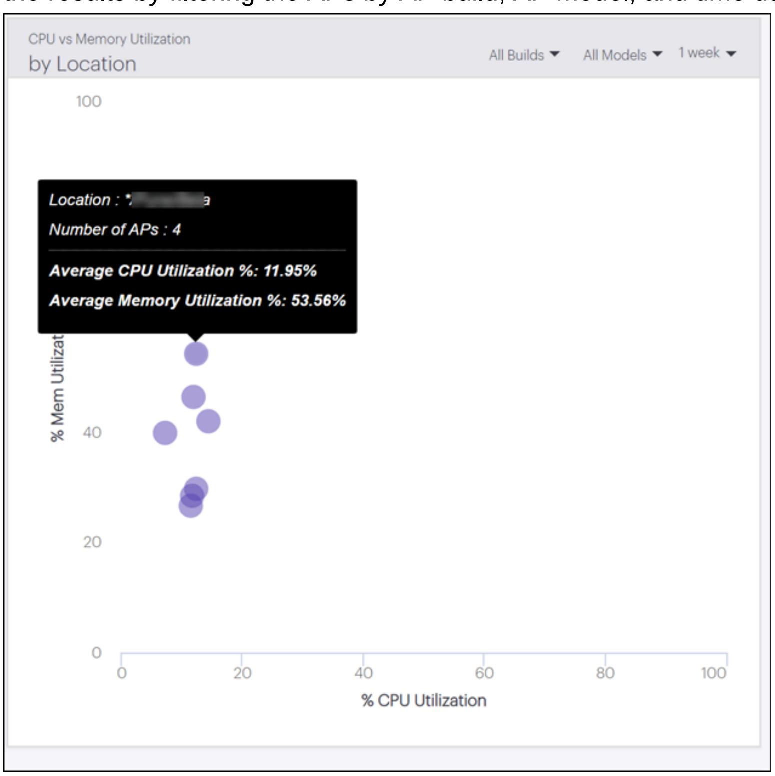
7.5.1 CPU VS Memory Utilization by Access Point

CPU vs Memory Utilization by Access Point graph represents the cpu vs memory utilization data of all the access points on the server. Each data point on the scatter plot represents data for each AP. Hover over each AP to get more details and click the plotted data point to view the AP detail page. You can also narrow down the results by filtering the APs by AP build, AP model, and time duration.

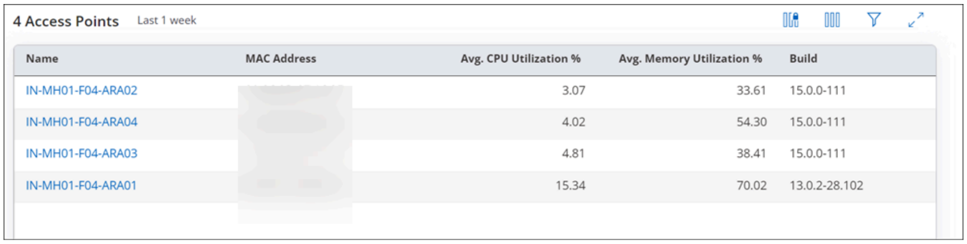


7.5.2 CPU VS Memory Utilization by Location

CPU vs Memory Utilization by Location chart groups the APs by location. All the APs at the selected location and its child location are considered in this chart. Hover over each location to get more details about the number of APs, their average CPU utilization and their average memory utilization. You can also narrow down the results by filtering the APs by AP build, AP model, and time duration.



Click the plotted data point to view the AP list with their average CPU and Memory Utilization details.

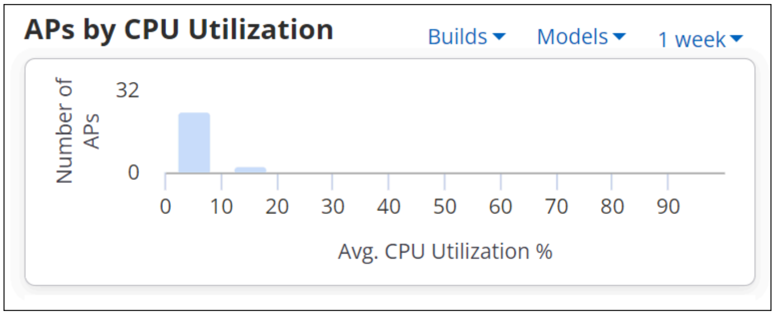


4 Access Points Last 1 week

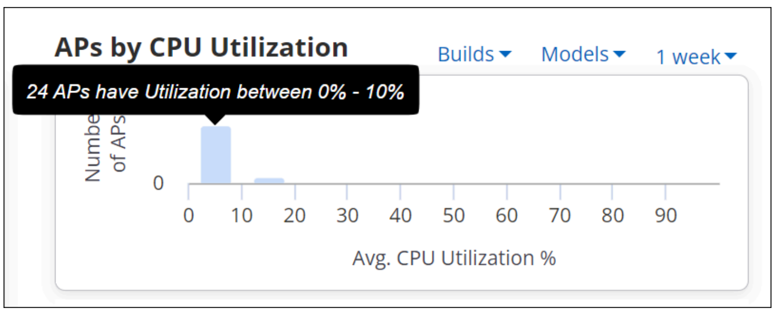
Name	MAC Address	Avg. CPU Utilization %	Avg. Memory Utilization %	Build
IN-MH01-F04-ARA02		3.07	33.61	15.0.0-111
IN-MH01-F04-ARA04		4.02	54.30	15.0.0-111
IN-MH01-F04-ARA03		4.81	38.41	15.0.0-111
IN-MH01-F04-ARA01		15.34	70.02	13.0.2-28.102

7.5.3 Access Points by CPU Utilization

Access Points by CPU Utilization chart depicts the number of APs based on their utilization range.



Hover over the bar to get the number of APs in a particular range. You can also click the bar to view more details about the APs.



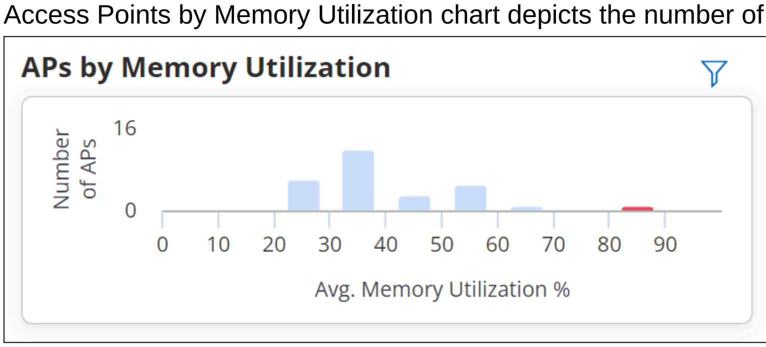
A yellow bar denotes APs having utilization more than the threshold. The threshold is calculated by the following formula.

Threshold = (mean utilization of all the APs + standard deviation *2)

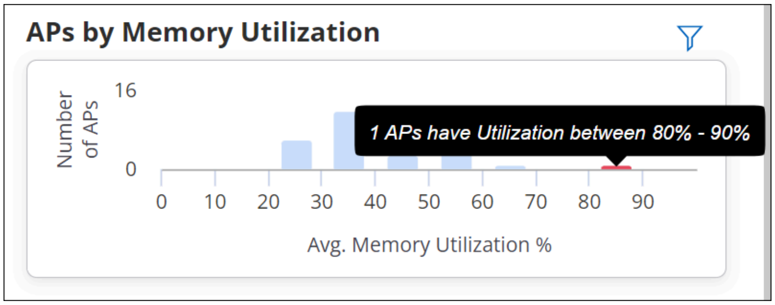
APs with utilization higher than the calculated threshold are marked with the yellow bar. And all the APs with utilization of more than 80% are marked with red bar.

7.5.4 Access Points by Memory Utilization

Access Points by Memory Utilization chart depicts the number of APs based on their utilization range.



Hover over the bar to get the number of APs in a particular range. You can also click the bar to view more details about the APs.



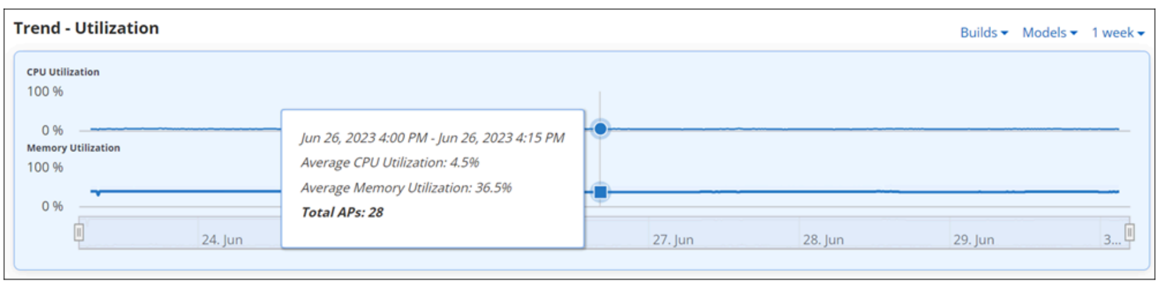
A yellow bar denotes APs having utilization more than the threshold. The threshold is calculated by the following formula.

Threshold = (mean utilization of all the APs + standard deviation *2)

APs with utilization higher than the calculated threshold are marked with the yellow bar. And all the APs with utilization of more than 80% are marked with red bar.

7.5.5 Trend Utilization

Trend Utilization chart depicts the trend of average CPU and Memory Utilization of all APs installed at the selected location. The trend chart shows 25, 50 and 75 percentile utilization of the APs. The trend chart uses comparative data and not the absolute data to depict percentile utilization.



A change in the trend during a particular time duration can help administrators identify network issues or time frames when network congestion is highest.

Chapter 8

FEED

FEED is a network dashboard that presents a timeline view of all the detected anomalies in the network. CV-CUE curates the feed by continuously monitoring and proactively detecting anomalies in the network. It also analyzes the cause of the anomaly and provides dynamic suggestions to mitigate the issue. The administrator can analyze the issue, the AI-based recommended action, and then decide on the best approach to mitigate the issue. Feed also lets administrators go back in time and understand anomalies that occurred in the past.

Administrators can also configure a Slack, Google Chat, or Microsoft Teams webhook to get a notification whenever an anomaly is detected.

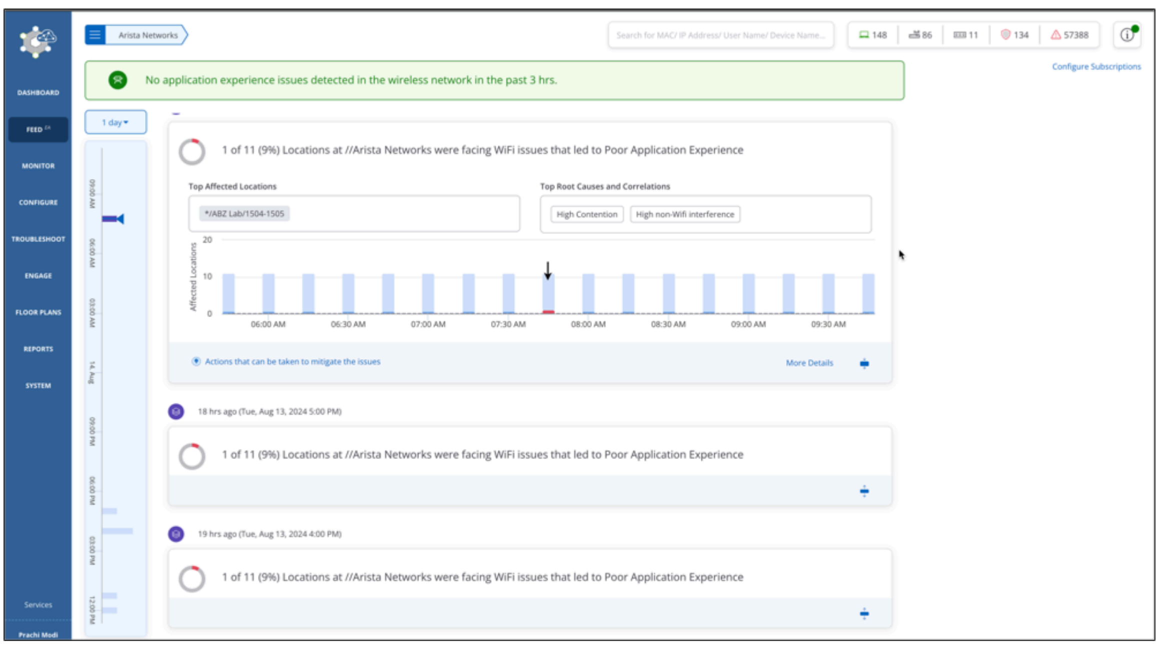
Note: This is a BETA feature. Reach out to your Arista account manager to enable it.

This chapter contains the following topics:

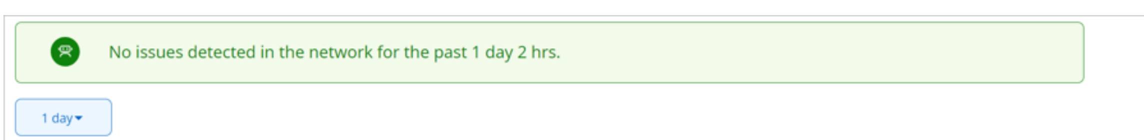
- FEED Dashboard
- Configure Subscriptions

8.1 FEED Dashboard

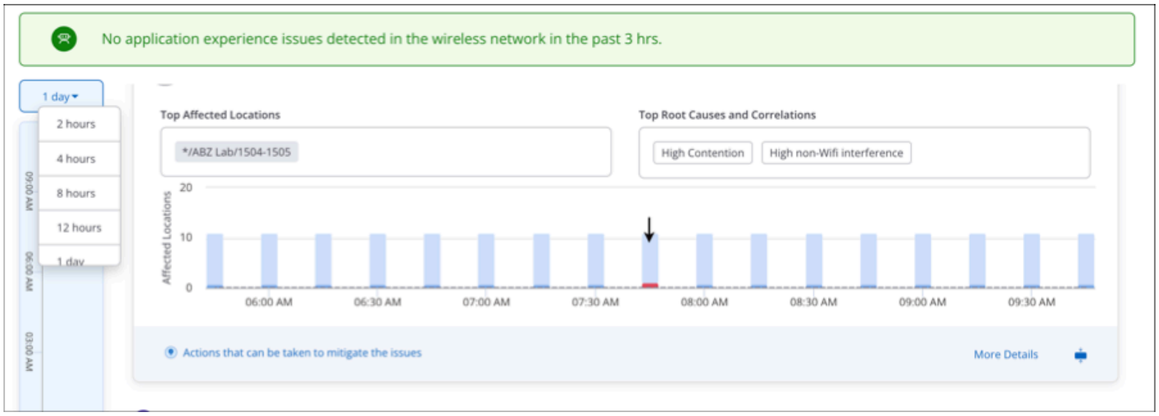
To view detected anomalies, navigate to FEED.



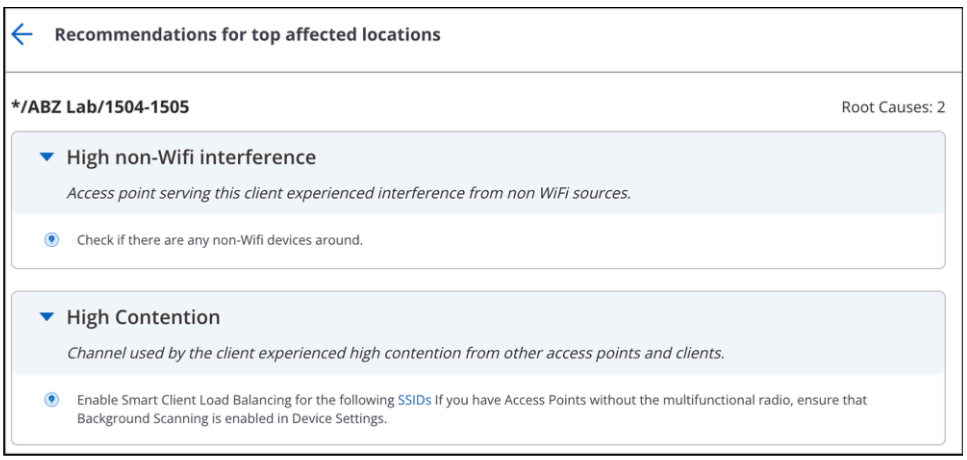
At the top of the feed dashboard is the anomaly highlight widget. The anomaly highlight shows the number of anomalies detected in the last 2 hours. If no anomaly was detected in the last 2 hours, it shows when the last anomaly was detected.



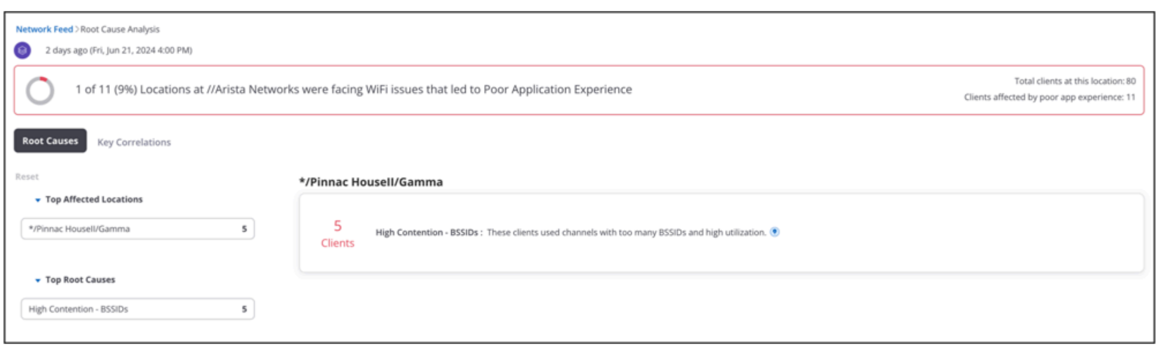
Following the analogy highlight, the Feed displays the network timeline of detected anomalies within the chosen time frame. You can select the time frame using the time slider on the left.



For each detected anomaly, the dashboard shows the top affected locations, root causes and correlations, and actions you can take to mitigate the anomaly.



Click the **Actions that can be taken to mitigate the issues** link to view the recommend actions. Click **More Details** to view a detailed Root Cause Analysis of the detected anomaly.



8.2 Configure Subscriptions

You can configure a Slack, Google Chat, or Microsoft Teams webhook to send alert notifications to your configured channel anytime a network anomaly is detected.

To configure a subscription:

1. Go to **FEED.**

2. Click **Configure Subscription.**
3. Click **Add Subscription.**
4. Add the following details:
    a. **Subscription Name:** Enter a name for the subscription.
    b. **Type:** Select **Slack, Google Chat, or Microsoft Teams.**

       Add the webhook link configured for your channel. For information on adding an incoming webhook, refer to:

       Slack: https://api.slack.com/messaging/webhooks
    c. **Webhook Link:** Add the webhook link configured for your channel. For information on adding an incoming webhook, refer to
        - **Slack:** https://api.slack.com/messaging/webhooks
        - **Google Chat:** https://developers.google.com/workspace/chat/quickstart/webhooks
        - **Microsoft Teams:** https://learn.microsoft.com/en-us/microsoftteams/platform/webhooks-and-connectors/how-to/add-incoming-webhook?tabs=dotnet
    d. Select **Webhook Enabled.**
    e. Click **Test-Webhook Link** to send a test message to your configured channel.
    f. Click **Save.**

Anytime an anomaly is detected, CV-CUE sends an alert message to your configured channel. The message contains information about the number of affected clients, their location, root cause, and key co-relations.

Chapter 9

Monitor Wi-Fi

The **Monitor** tab in CV-CUE is primarily used for monitoring the Clients, APs, Radios, WLANs, Applications, and Tunnels in the network. You can perform troubleshooting operations based on the information collected for each of the components in the **Monitor** tab.

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 2.4, 5, and 6 GHz frequencies.

Active SSIDs (WLANs)

Lists the SSID profiles.

Application Visibility

Lists the applications with details about their data usage for a specific SSID.

Tunnels

Lists the tunnels used by the SSIDS to traffic the data between endpoints.

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 managed devices (access points and sensors)
- Total active access points
- Total inactive access points
- Total currently online clients
- Total switches

This chapter contains the following topics:

9.1 Clients

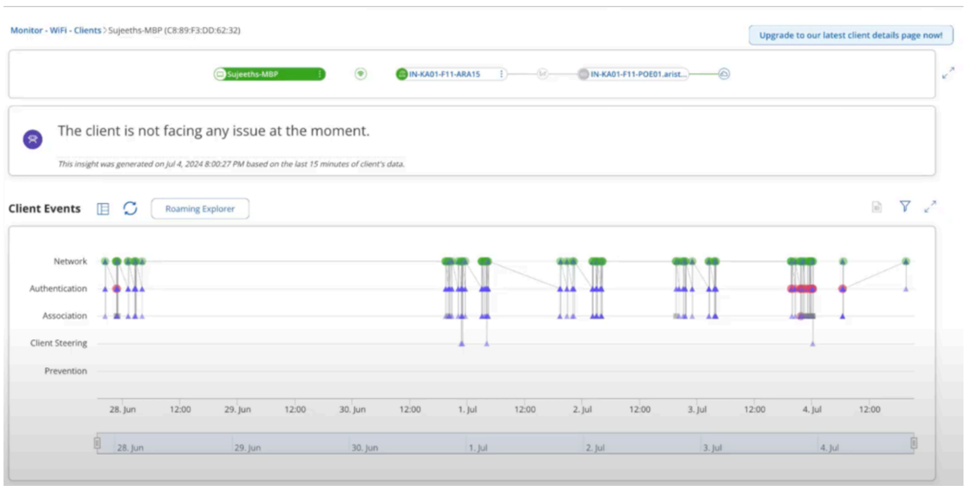
The Clients tab displays the clients that are connected to APs. The type of Clients differ depending on their association with the AP.

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:

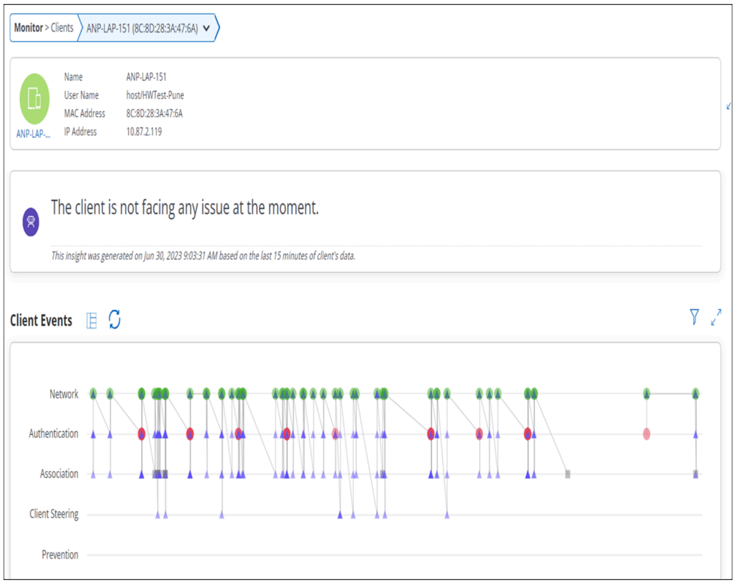
- If you select Live: A list of clients with the following status are displayed:
  - Clients that are successfully connected to Arista APs.
  - Clients that failed to connect.
- If you select All: A list of clients with the following status (including Live clients) are displayed:
  - Clients that are 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 Events widget with a Graph view. You can view the client detail dashboard by clicking, **Upgrade to our latest client details page now!**.



Graph View (Old view)

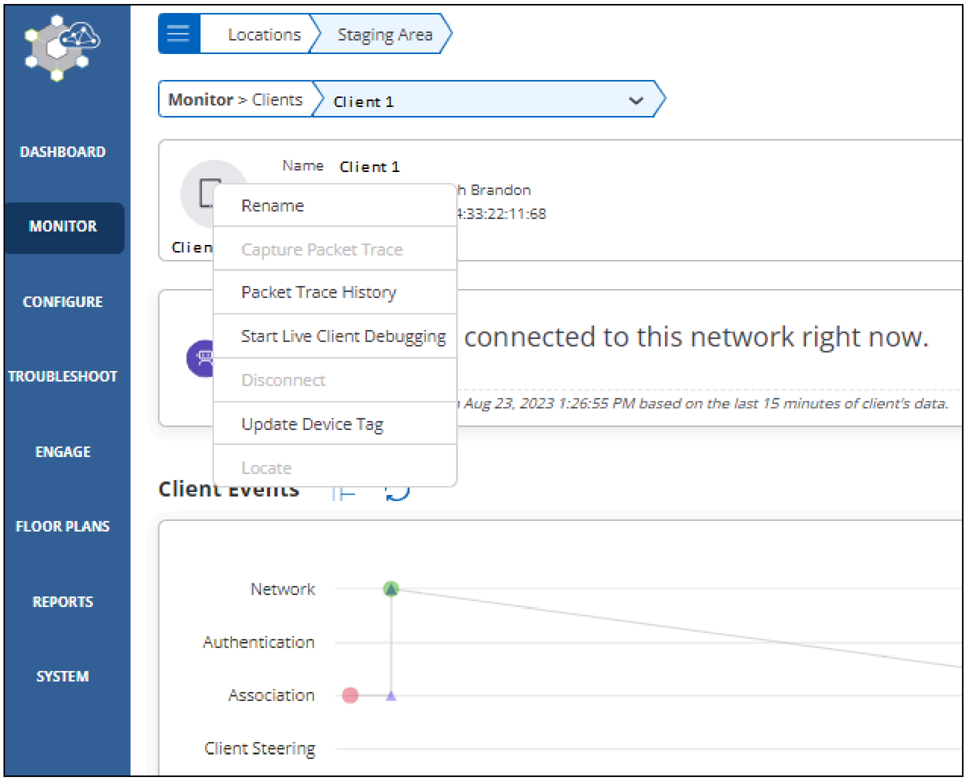


Click **Switch to Table View**, and you can see the following properties of clients displayed in the tabular format:

Property	Description
Status	Indicates if the client is successfully associated or failed to connect.
Name	Specifies the user-defined name of the client.
User Name	Provides Username of the client
Role	After client is connected via any SSID, it is assigned with Role configured in SSID profile.
Google Authorized	It is boolean value to represent whether client is authorized using google integration.
Location	Location of the client.
MAC Address	Specifies the unique 48-bit IEEE format address of the client assigned to the network adapter by the manufacturer.
IP Address	IP address of the client.
OS	Name of Operating System running on the client.
Associated AP	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.
Associated SSID	Specifies the operating SSID of the AP with which the client is associated.
Avg. data rate	Refers to the average amount of data transferred per unit of time
RSSI(dbm)	Displays the observed RSSI (Received Signal Strength Indicator) value for the client.
Uplink Data	Indicates the amount of data transferred by the client.
Downlink Data	Indicates the amount of data received by the client.
Protocol	Indicates the 802.11 protocol (with or without 802.11n or 802.11ac capability) used.
Up/Down Since	Date and time since the client is up or down.
First Detected At	Indicates the time and day when the client was first detected
Retry Rate (%)	Indicates the retry rate in percentage
Sticky	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.

The client icon also supports a context menu. Right-click the client icon to view the context menu.

Figure 9-1: Context menu in Client Details



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:

Action	Description
Rename a Client	To change the name of a client.
Capture Packet Trace for a Client	Responsible for intercepting a data packet that is crossing or moving over a specific computer network
View Packet Trace History for an Access Point	Displays packet traces captured in the last 30 minutes
Start Live Client Debugging	Displays live client logs of a client.
Disconnect	Disconnects the client.

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

- Client Connection Logs
- Client Events Logs
- Baselines
- Top Locations Affected by Poor Performance
- Client Traffic Volume
- Application Session Logs
- Devices Seeing This Client

9.1.1 Client Explorer

Client Explorer helps you view the distribution of clients that are connected to Arista devices.

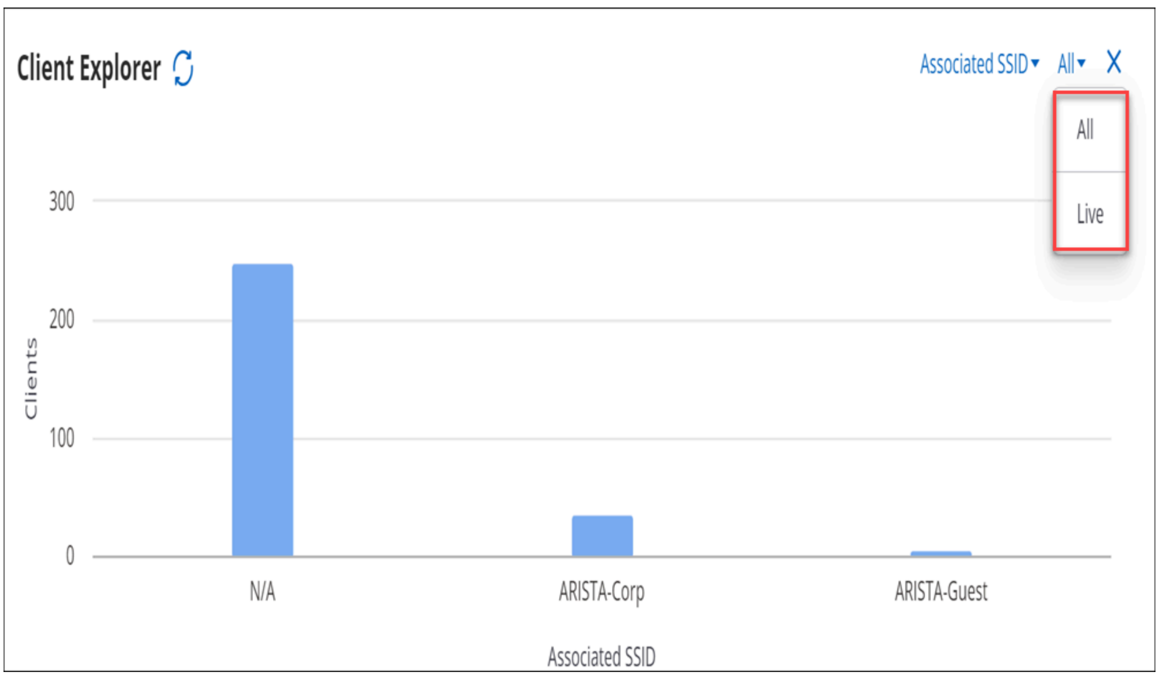
It provides a summary view of all the clients and provides an easy way for the network administrators to understand client distribution for each attribute. For example, network administrators can use the Client Explorer to understand client distribution for different versions of Wi-Fi and determine the percentage of legacy clients at a location.

To view the Client Explorer,

1. Navigate to **MONITOR** > **WiFi** > **Clients.**
2. Click **Client Explorer**

On the Client Explorer chart, you can filter the clients based on their association attributes such as SSID and with AP as well as a range of Client properties. You can use the client connection status drop-down menu to view graphical client distribution based on the selected attribute.

Connection Status



If you select **Live**, the chart shows data corresponding to clients with the following status:

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

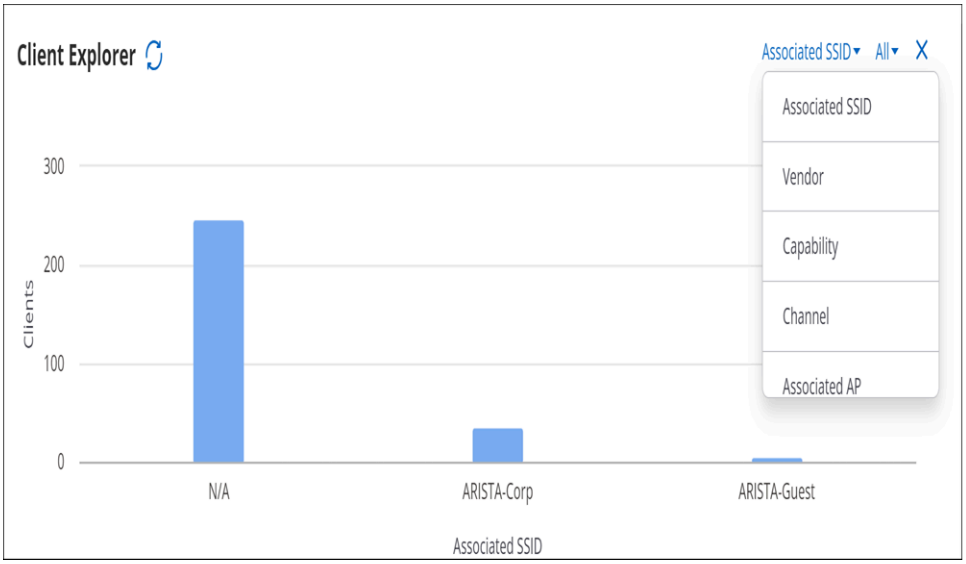
If you select **ALL,** data for clients with the following status is displayed in the chart:

- 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.

Hover over the Status icon to view the current selection for client connection status filter.

Client Attributes



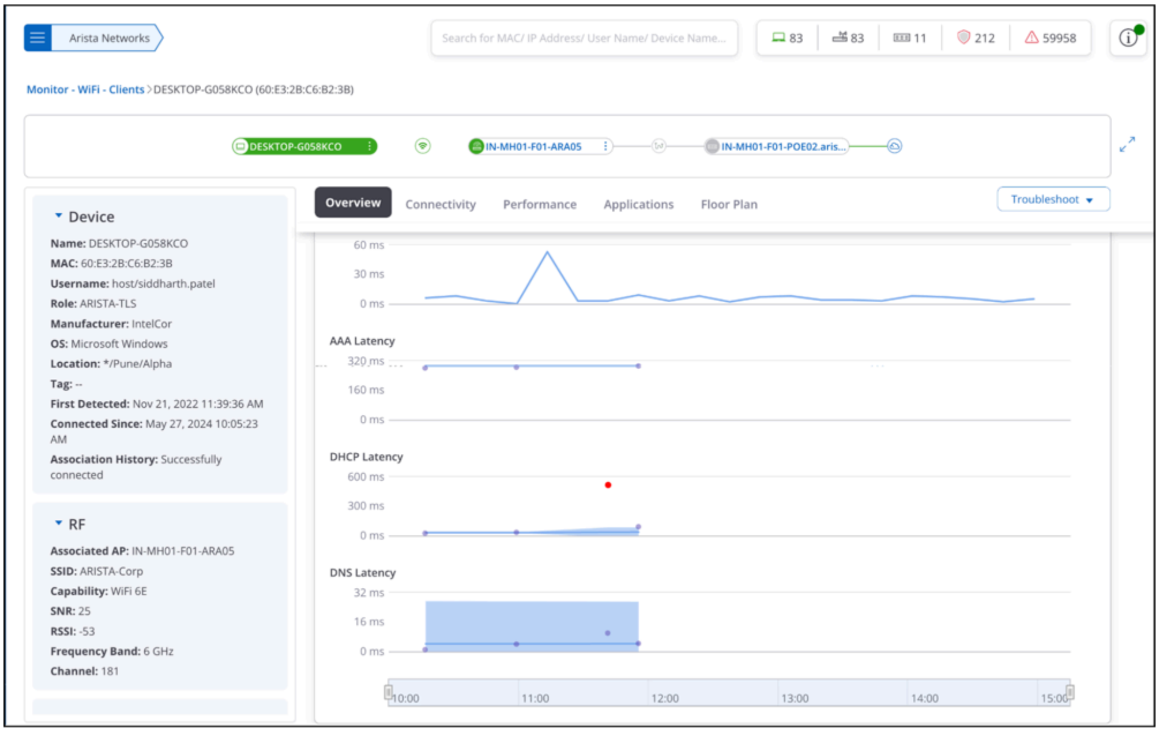
You can further filter the clients by the following attributes:

- Associated SSID
- Vendor
- Capability
- Channel
- Associated AP
- Connection Failure Type
- Protocol
- Google Auth Status
- Role Operating Status

You can select and deselect a particular bar in the bar graph to filter the tabular data in the client list.

9.1.2 Client Dashboard

Along with client and network details, the client details dashboard also contains multiple data points regarding client connectivity, performance, and application experience. From a single dashboard, you can conduct live troubleshooting, and review past data to identify and troubleshoot past issues, thus resulting in a faster resolution.



The Client Details Dashboard contains a client connection widget, a client properties widget, and multiple tabs containing different charts and graphs showcasing client details.

Client Connection Widget

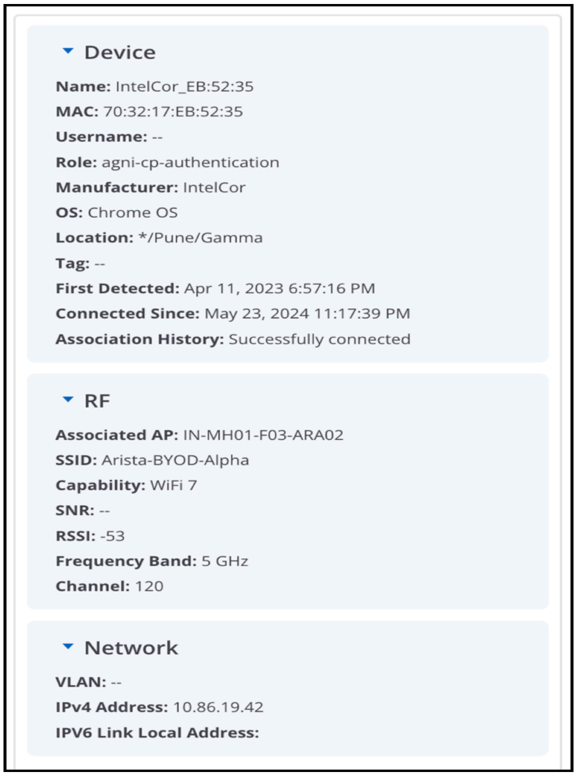
The top section of the dashboard has the client connection widget, which visually shows the selected client's network connectivity path. It shows the **Client > AP > Switch** association.

Hover over any device to view more information about it or click the three-dot menu next to the device icon to see the available actions for that device.

Client Properties Widget

The left side of the dashboard contains the following sections that display client properties:

- Device Details
- RF Details (Radio Frequency)
- Network Details - Only available for connected clients.



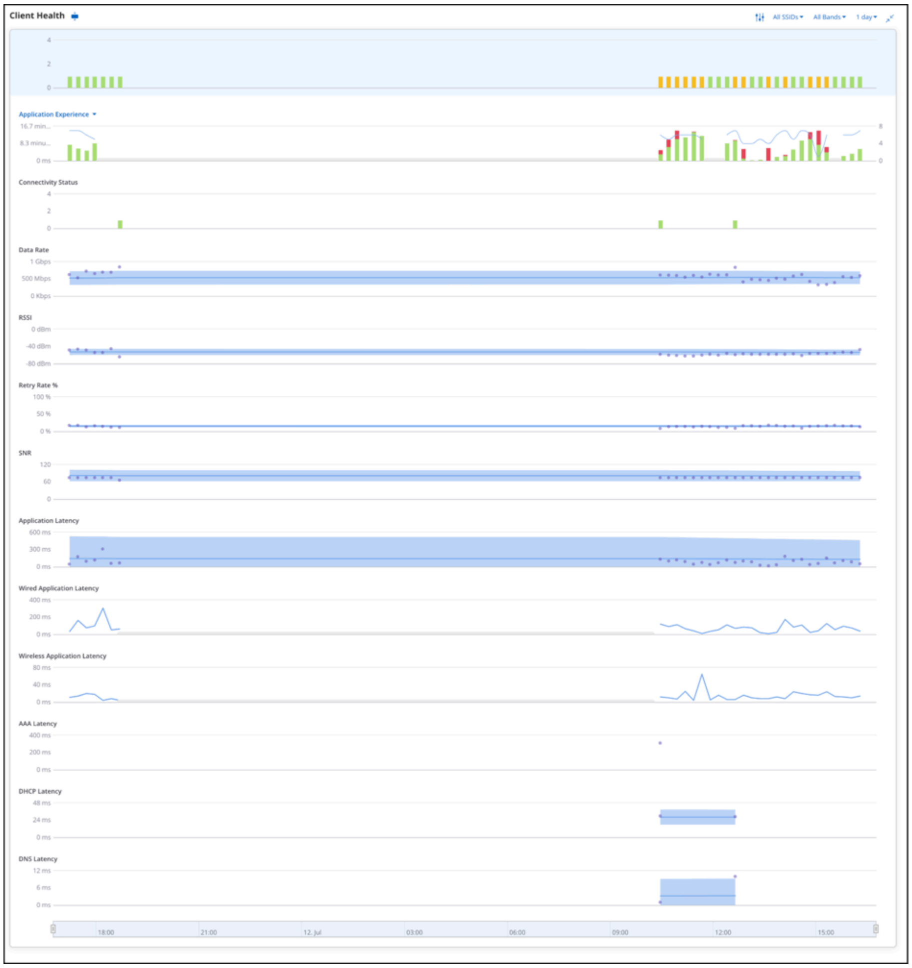
Client Dashboard Tabs

Client Dashboard is divided into the following tabs:

- Overview
- Connectivity
- Performance
- Application
- Floor Plan

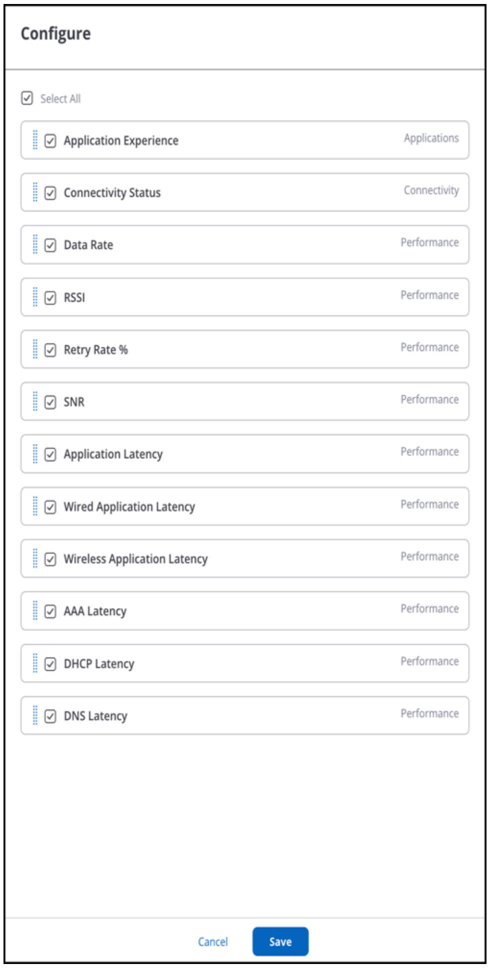
Overview Tab

At the very top of the Overview tab is the RCA widget, which shows the Root Cause Analysis for the symptoms faced by the client and the reason, along with the possible solution for the issues.



The **Client Health Widget** contains multiple charts related to client health, such as % Poor application experience, Connectivity Failures, RSSI, Data Rate, Wired Application Latency, Wireless Application Latency, Retry Rate %, etc. It is an interactive widget that you can customize according to your preferences. You can customize it to add or remove certain charts and change the order of visible charts. You can also hover over any data point to view more information.

To configure the widget, click the **Customize**  icon next to the chart filters to open the Configure panel. The following image shows the Configure panel for the Client Health widget:

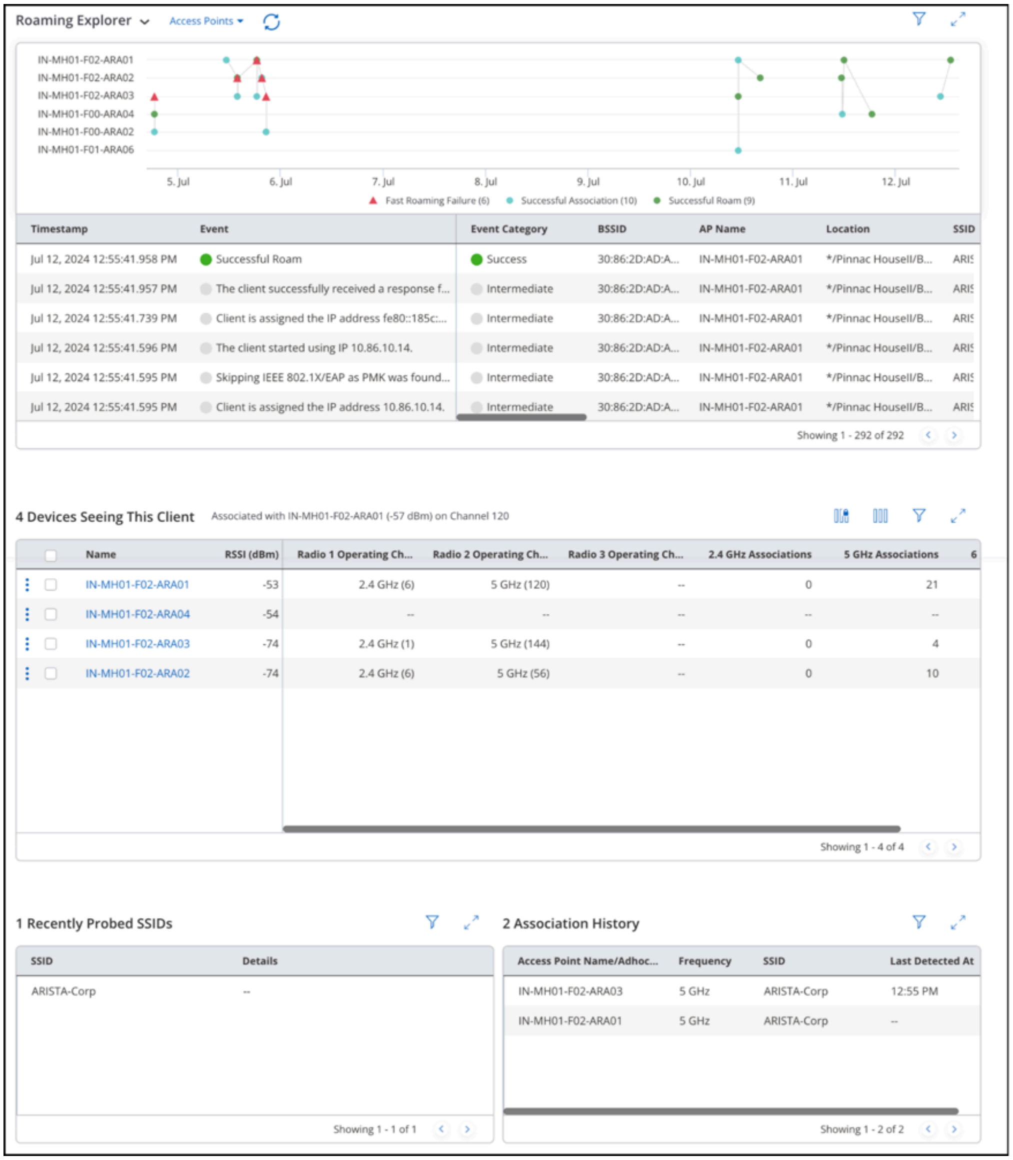


Connectivity Tab

The connectivity tab contains charts that display the client’s connection attempts, the client’s roaming events from one AP to another, and a list of APs watching this client.

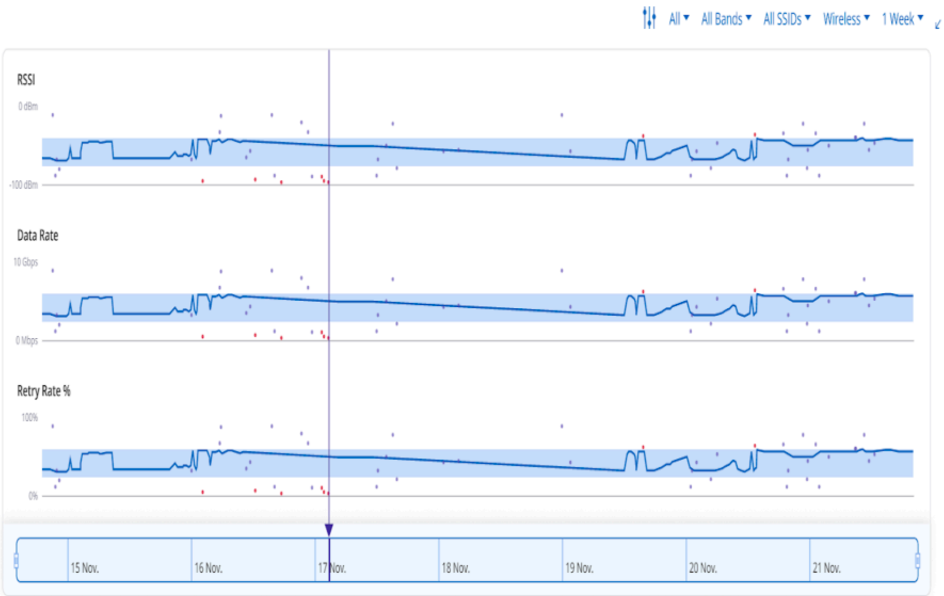
The connectivity tab shows the following charts:

- Client Events / Roaming Explorer
- Devices Seeing This Client
- Recently Probed SSIDs
- Association History



Performance Tab

The performance tab contains RSSI, Data Rate, Retry Rate %, and Traffic Volume charts.



Application Tab

The application tab displays charts that provide details about the applications used by the client such as the number of applications, application latency, poor application experience, etc.

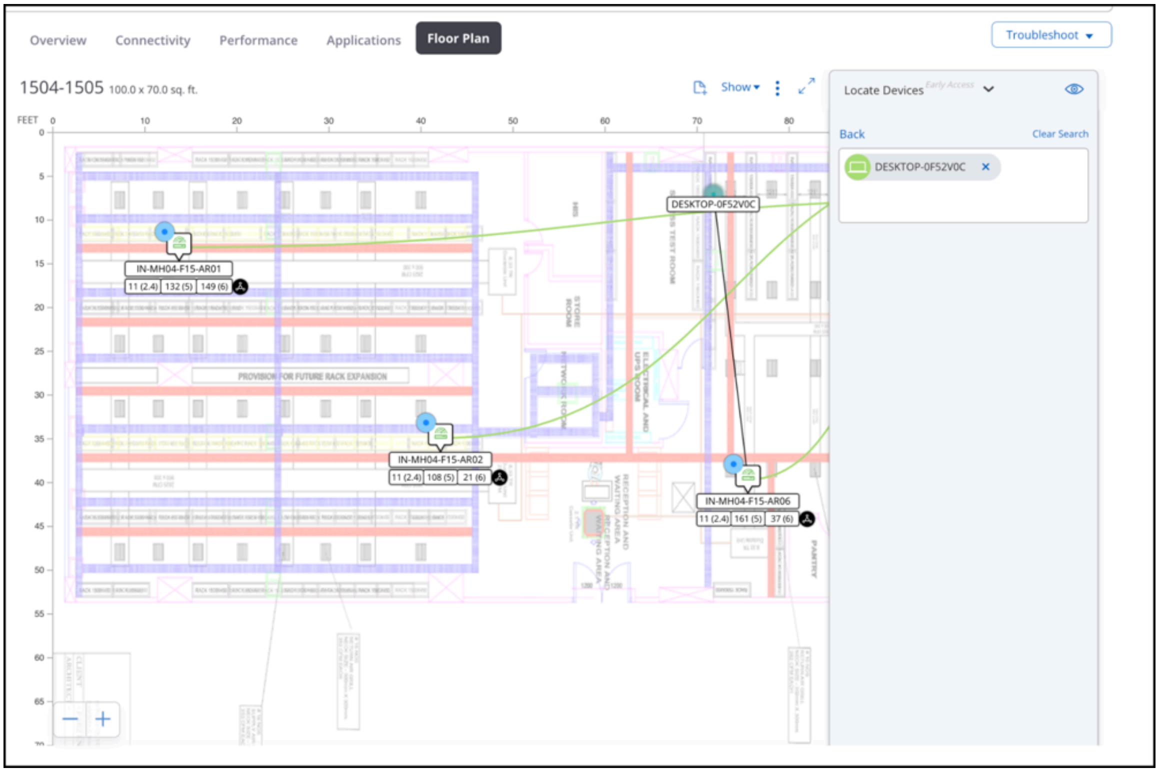
It contains the following charts:

- Application Explorer
- Top Applications by Traffic
- Application Experience

Floor Plan Tab

The floor plan shows the location of the client on the floor. For the client to be located on the floor plan, it must be visible to at least three APs operating in the same frequency band. At least three APs must report the device and the APs must be placed on the floor.

If the client cannot be located on the floor plan, the proximity view is displayed.



Troubleshooting a Client

You can perform the following actions on each client. These actions are available under the Troubleshoot menu.

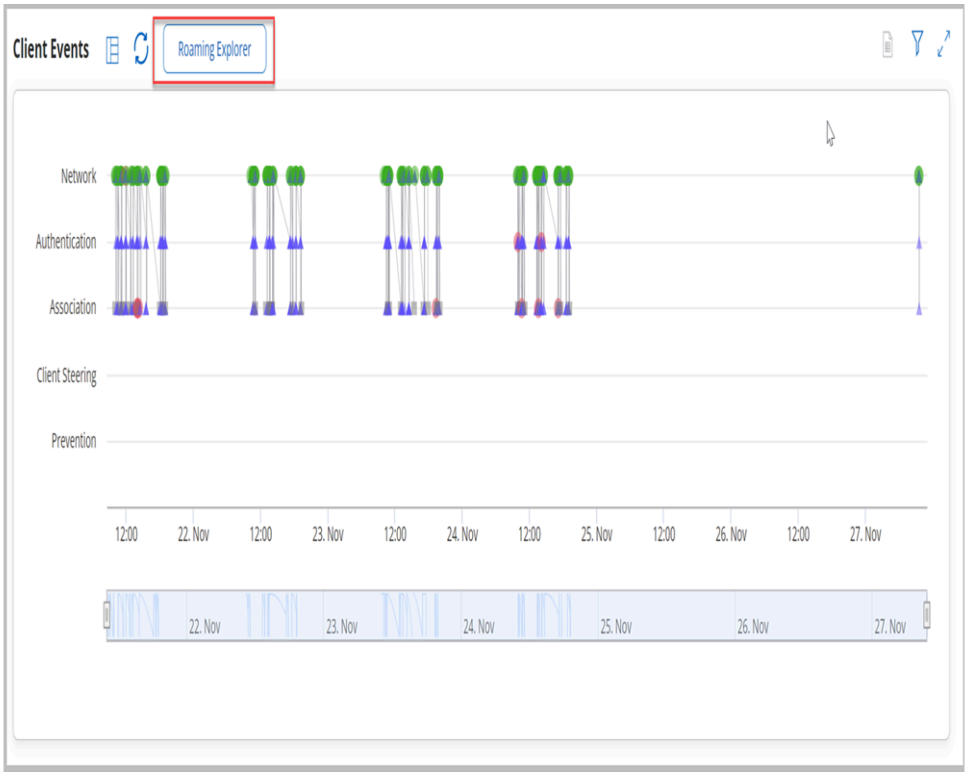
- **Rename:** To change the name of a client.
- **Capture Packet Trace:** To intercept a data packet that is crossing or moving over a specific network. The captured packet is stored temporarily for analysis. The packet is inspected to help diagnose and solve network problems.
- **Packet Trace History:** To view the Packet Trace History for the selected client. The packet traces captured only during the last 30 minutes are displayed in the history.
- **Start Live Client Debugging:** Displays live client logs of a client connection.
- **Disconnect:**Disconnects the client.
- **Update Device Tag:** Update the device tag of the client.

9.1.3 Roaming Explorer

Roaming Explorer provides a graphical and tabular view of a client's roaming events from one access point (AP) to another AP.

To view the Roaming Explorer,

1. Navigate to **MONITOR** > **WiFi** > **Clients.**
2. Click **Roaming Explorer** next to the Client Events widget.



Roaming Explorer consists of a graph view and a split view.

Graph View

The graph view appears as follows:

It is a line graph denoting the client's roaming activities on different APs. The APs are listed based on the number of events logged for each AP, with the AP having the highest number of roaming events listed on top.

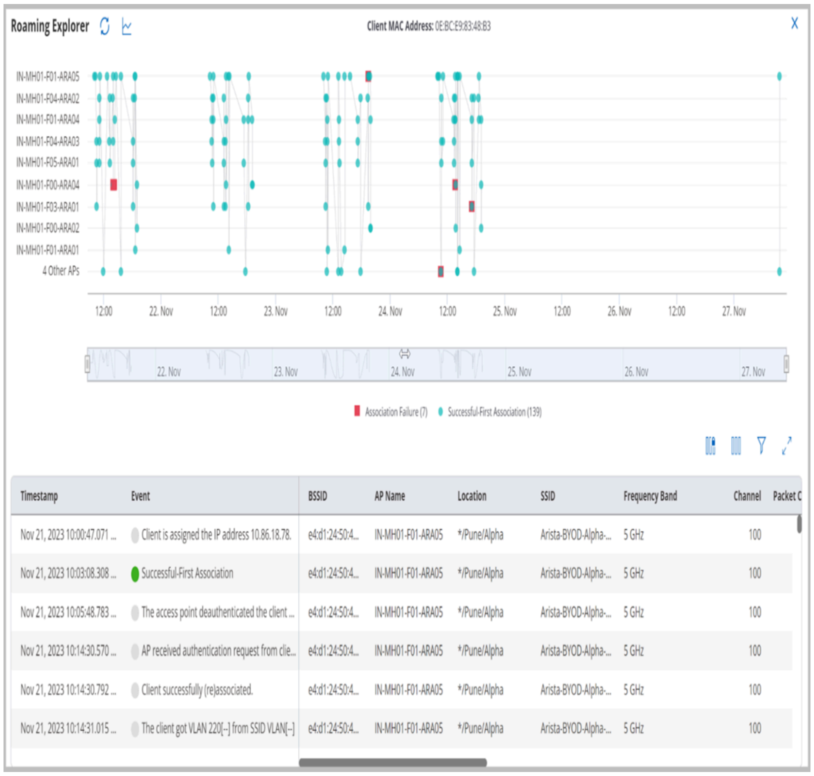
The Y-axis shows the APs, and the X-axis shows the timeline of the roaming event. You can hover over any event to view more details about it.

Graph view considers the following roaming events only:

- Association Failure
- Fast Roaming Failure
- Successful-Fast Roam
- Successful-First Association

Split View

The split view consists of a graph view and tabular data that lists all the clients' events along with the event timestamp and further details such as BSSID, AP Name, Location, Frequency Band, and more.



9.1.4 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

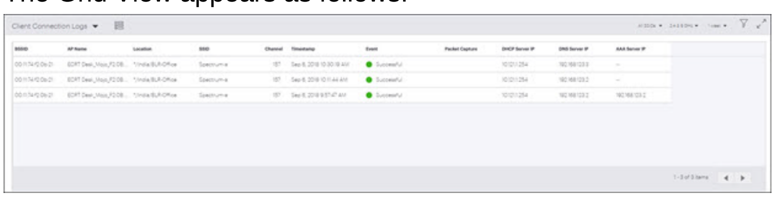
- Grid View

The Timeline View appears as follows:

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

Field	Description
Timestamp	Indicates the date and time when the client connected to an AP.
Average Latencies	Average latencies of various stages and their sub-stages in the Wi-Fi connection for the client.
BSSID	BSSID is the MAC address of the AP to which the client attempted to connect.
AP Name	Name of the AP to which the client attempted to connect.
SSID	SSID of the WLAN to which the client is connected.
Channel	Operating channel of the AP to which the client attempted to connect.
Disconnect	Disconnects client from AP.

The Grid View appears as follows:



The Grid View contains detailed information in a tabular format:

Field	Description
BSSID	BSSID is the MAC address of the AP to which the client attempted to connect.
AP Name	Name of the AP to which the client attempted to connect.
SSID	SSID of the WLAN to which the client is connected.
Channel	Operating channel of the AP to which the client attempted to connect.
Timestamp	Indicates the date and time when the client connected to an AP.
Event	Indicates if the client successfully connected.

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:

Failure Categories	**Main Failure Type**
Association Failure	AP association limit exceeded
	Capability mismatch
	Association failure
Authentication Failures	Eapol 4-way handshake failed
	RADIUS authentication failure
	Radius server not responding
	Incorrect Pre-Shared Key
	Fast roaming failed
Network Failures	Captive portal - shared secret mismatch
	Captive Portal authentication failed
	Captive portal - client in blackout period
	DHCP failed
	DNS failure

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:

Column	**Filtering Criteria**	**Description**
Event	All	Retrieves all the event logs.
	Successful	Retrieves only successful event logs.
	Failed	Retrieves only unsuccessful event logs.

Filtering Criteria	**Description**
Enter the From and To dates.	Retrieves client connection logs between the From and To dates.
Check the Long Time Ago check box and enter the To date.	Retrieves all client connection logs till the To date.
Enter the From date and check the Now check box.	Retrieves client connection logs between the From date and the current date.
Check the Long Time Ago and Now check boxes.	Retrieves all the available client connection logs.

9.1.5 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
- Consolidated View

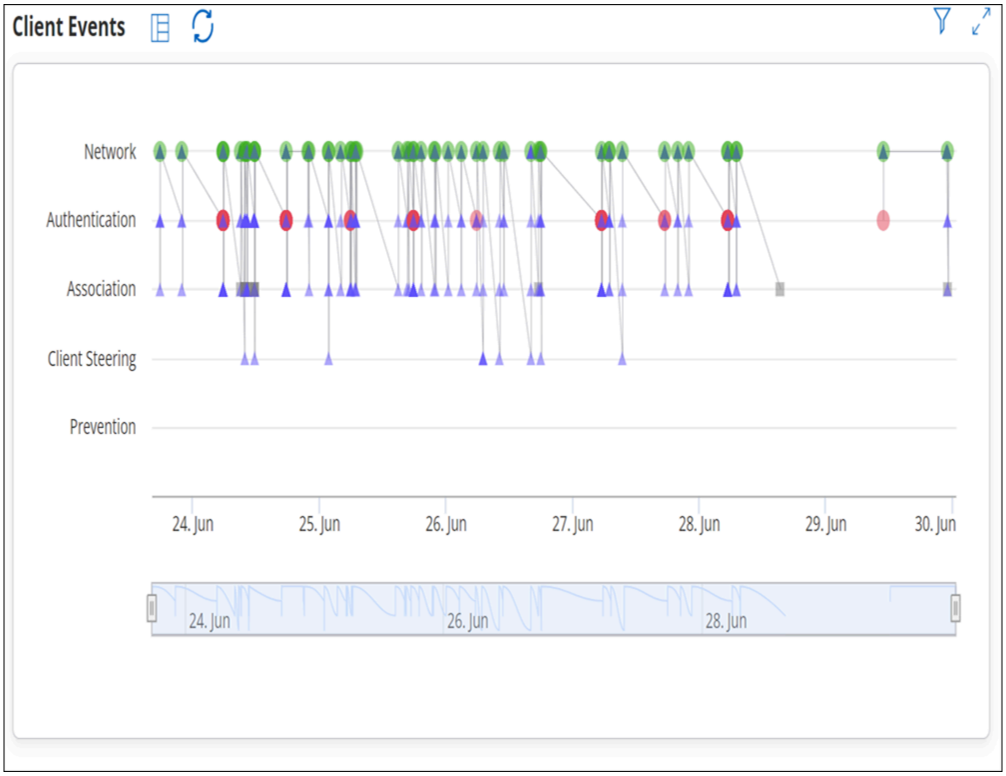
Graph View

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:

Field	Description
Timestamp	Indicates the date and time when the client connected to an AP.
Average Latencies	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.
BSSID	BSSID is the MAC address of the AP radio for that SSID.
AP Name	Name of the AP to which the client attempted to connect.
SSID	SSID of the WLAN to which the client is connected.
Channel	Operating channel of the AP to which the client attempted to connect.
Location	Location of the AP to which the client is connected.
Frequency Band	Frequency band of the client connected to the AP.

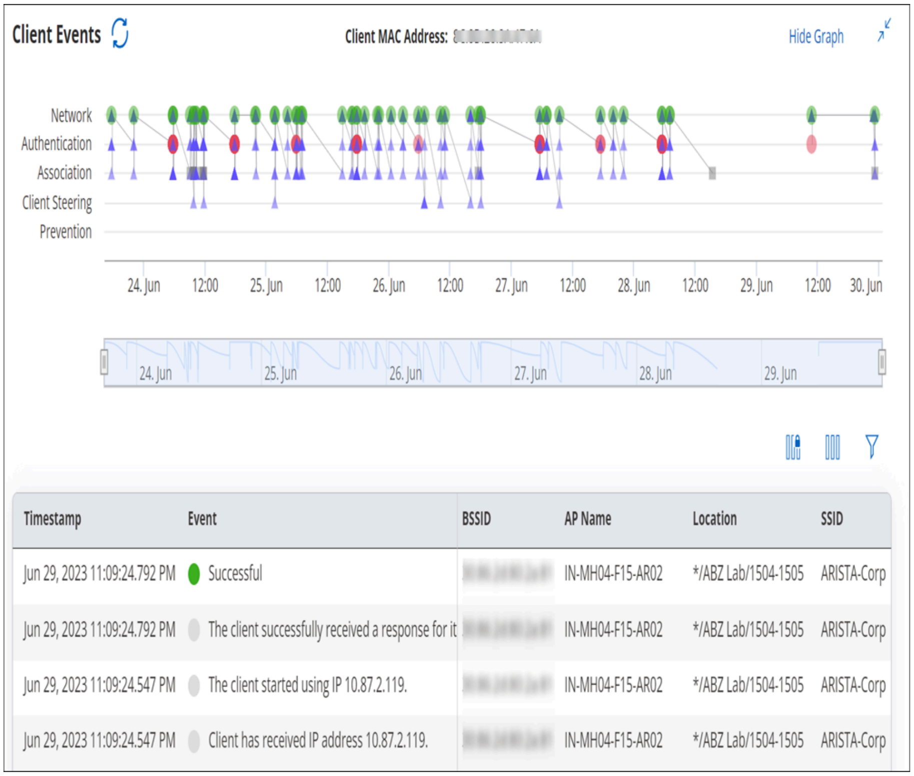
Graph View

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 not 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.



You can click a specific event in the graph and the corresponding event detail is highlighted in the table.

Grid View

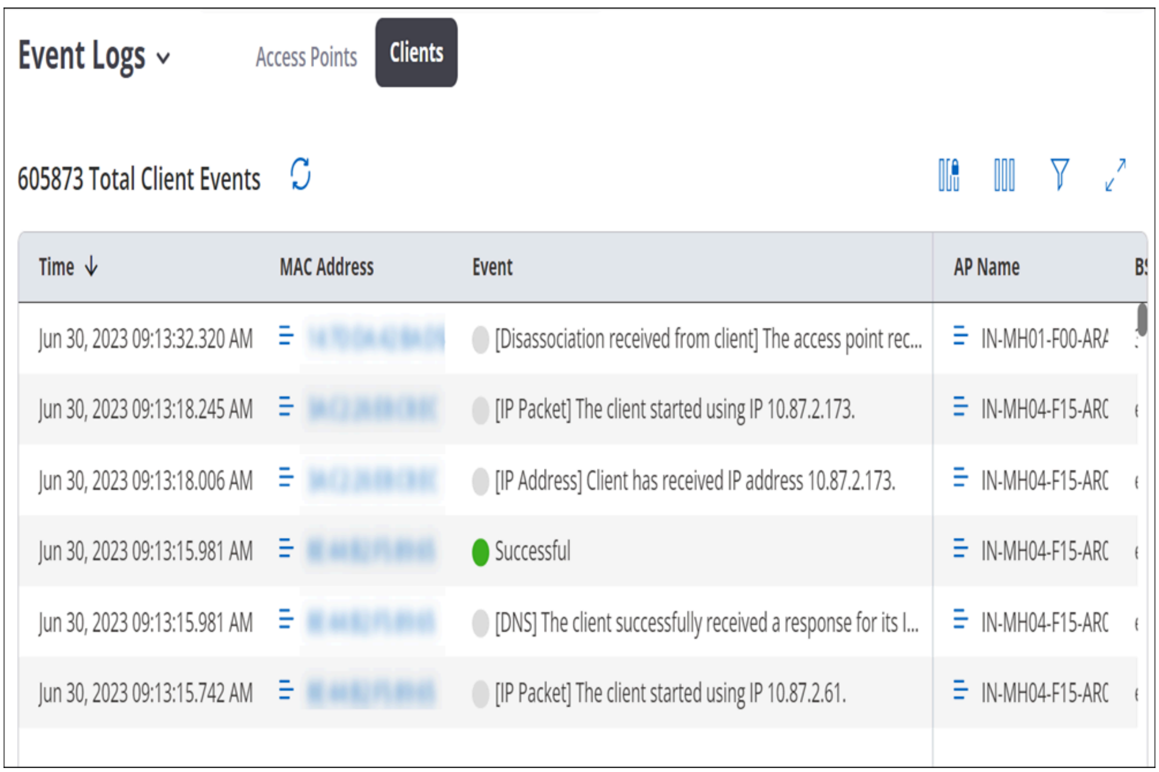
The Grid View appears as follows. The red, green and grey colored symbols in event column of the client event logs denotes unsuccessful, successful and intermediate events respectively. Hover on each text to know about type of event occurred.

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

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

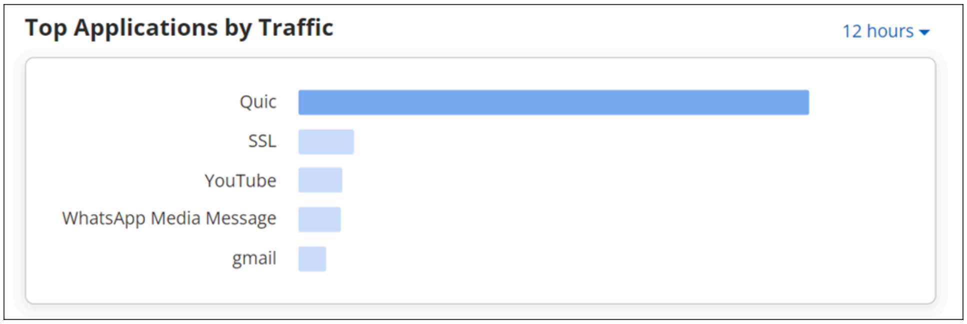
Consolidated View

Consolidated view captures client event logs of all clients connected to Arista devices. To view all client event logs, navigate to **TROUBLESHOOT** > **Event Logs** and click the **Clients** tab. The consolidated view appears as follows.



9.1.6 Top Applications by Traffic in Client Tab

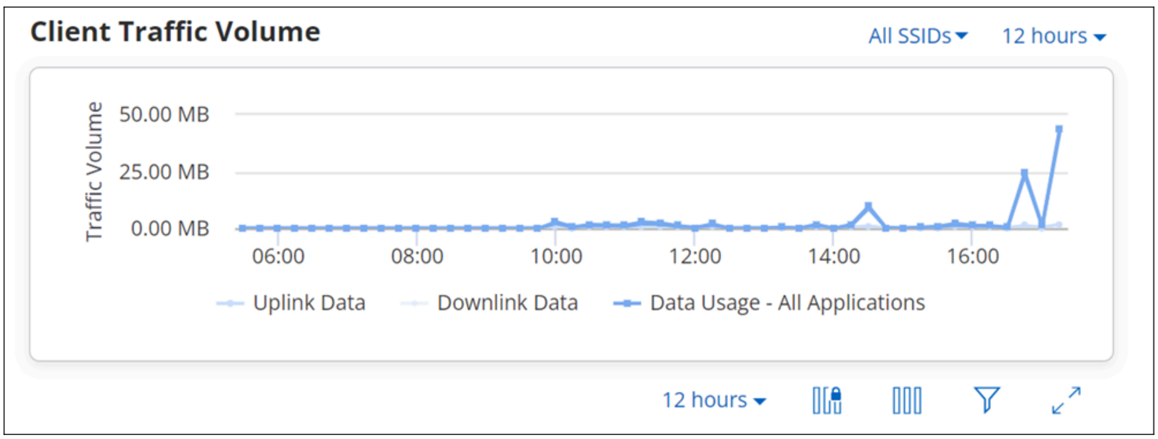
Top Applications by Traffic chart graphically represents data usage for applications. It always represents data for top five applications, with highest traffic. To view exact data usage, hover on the specific bar in the graph.



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.

9.1.7 Client Traffic Volume

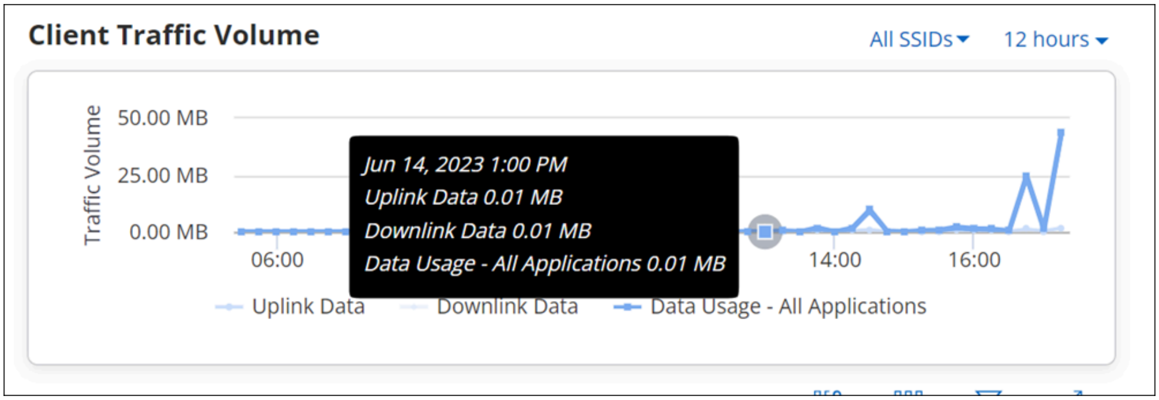
The **Client Traffic Volume** graph represents the data traffic sent and received by the client every 15 minutes. X-axis in the graph denotes the time period for which the Data Usage is plotted and Y-axis denotes the Traffic Volume.



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.



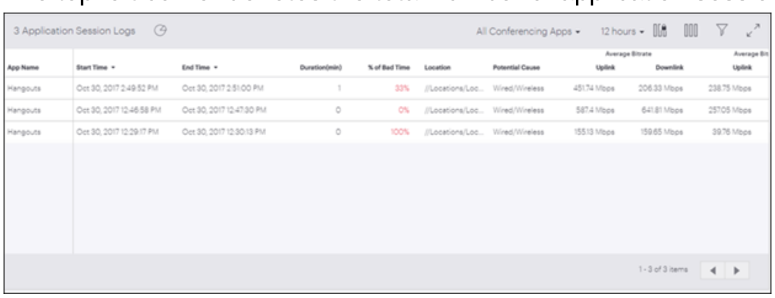
The graph contains the following details about the data:

- 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.

9.1.8 Application Session Logs

Application Session Logs provides details of the applications used by the client. Select a client from **MONITOR** > **WiFi** > **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.

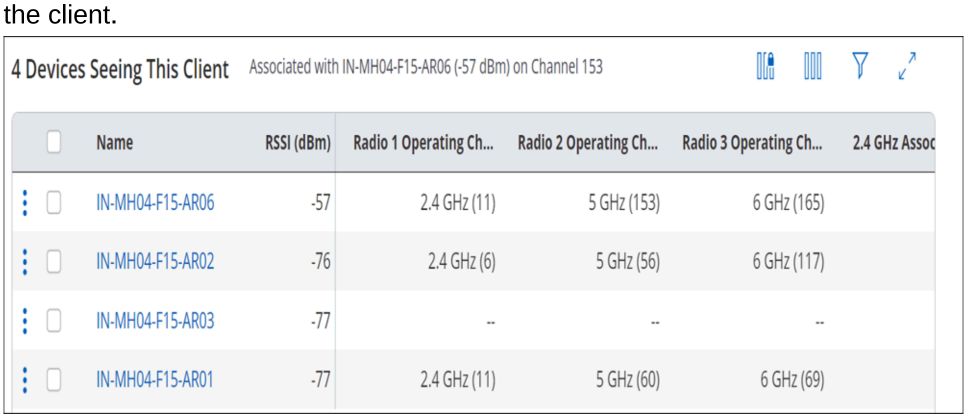
Detailed information about session logs is displayed in tabular format:

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

9.1.9 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.



The detailed information is as follows:

Field	Description
Name	Name of APs seeing the client.
RSSI (dbm)	RSSI states signal strength of an AP as seen by the client.
Radio 1 Operating Channel	Shows the band and channel operating on radio 1. Channel is shown in brackets.
Radio 2 Operating Channel	Shows the band and channel operating on radio 2. Channel is shown in brackets.
Radio 3 Operating Channel	Shows the band and channel operating on radio 3. Channel is shown in brackets.
2.4 GHz Associations	It states number of clients associated with 2.4 GHz radio.
5 GHz Associations	It states number of clients associated with 5 GHz radio.
6 GHz Association	It states number of clients associated with 6 GHz radio.

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

9.1.10 Rename a Client

You can change the name of a client.

Perform the following tasks to rename a client:

1. Go to **MONITOR** > **WiFi** > **Clients** or **MONITOR** > **WIPS** > **Clients**.
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**.
3. Change the name of the client and click **Done** to save the changes.

9.2 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.

Note: An AP's status is set as **Inactive** after 10 minutes of Inactivity.

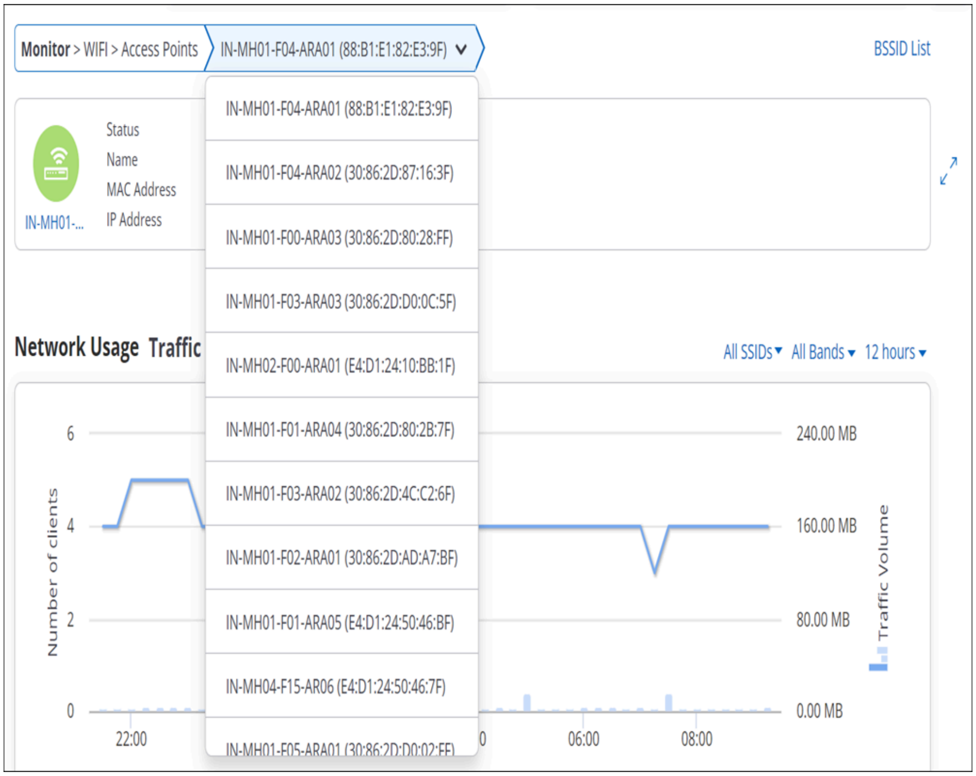
You can view ongoing activities on an AP using View Ongoing Activities option available to the right top corner on the AP table. The list of live activities that can be viewed for AP are:

- **Packet Trace:** Capture Packet Trace action on an AP captures the packet and inspectes 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 tis 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:

Action	Description
Update Firmware	Using this option you can update the firmware on the AP to the latest or any previously released version.
Access Point Event Logs	A log table that maintains event logs of APs.
Run Client Connectivity Test	Runs the Client Connectivity Test.
View RF Explorer	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.
Capture Packet Trace	This option helps troubleshoot Arista devices operating in AP or AP/Sensor mode.
Packet Trace History	You can view the Packet Trace History for a selected AP.
View on Floor Map	This option redirects you to the location on the floor map where the AP is placed.
Customize Transmit Power or Channel	Transmit Power Selection enables you to control the transmission power of the AP.
Move	Using Move operation you can change location of an AP.
Reboot	This operation Reboot's the AP.
Rename	Renames the AP.
Delete	Deletes the APs from the list of available APs.

Click on an AP in the list on the **MONITOR** > **WiFi** > **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 - Averge Data Rate

The graph calculates the data rates for 2.4 GHz, 5 GHz, or 6 GHz 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 has 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.

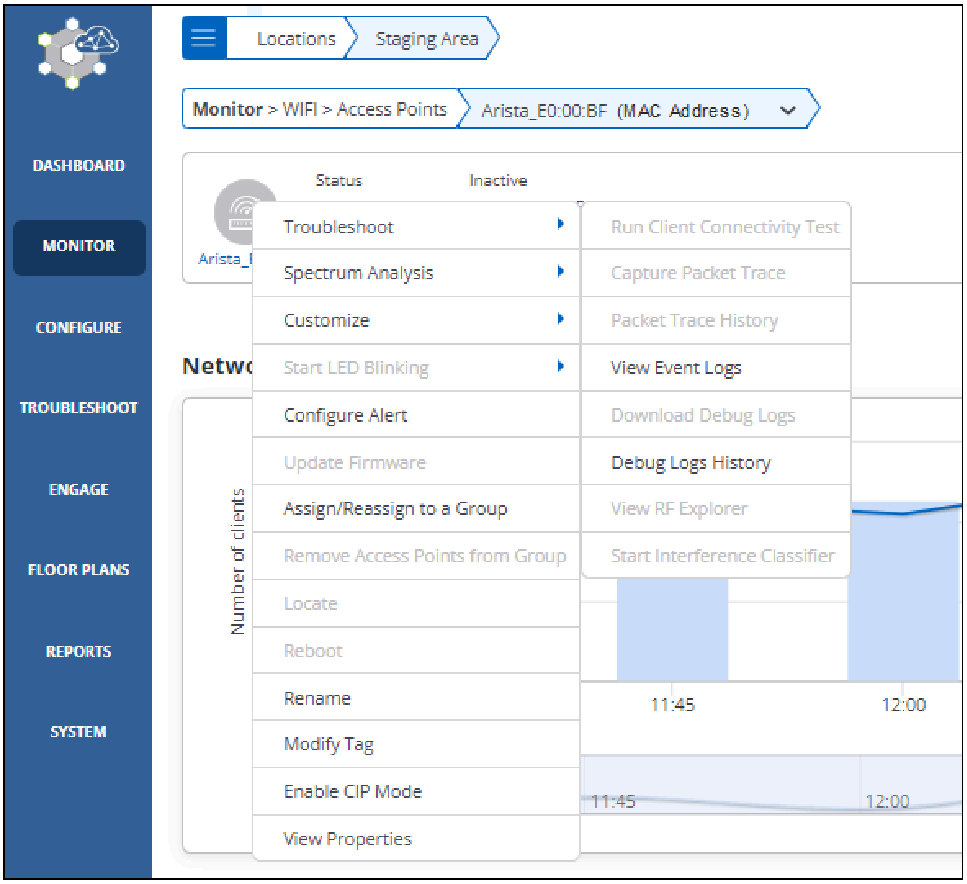
Note: Views and charts that show information about channels other than the operating channels of the AP work best when the AP has a dedicated scanning radio. APs that do not have a dedicated scanning radio use background scanning, where typically an AP goes off-channel once every 60 seconds to scan one 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 managed APs also support a context menu from the AP Details page. Right-click the managed AP icon to view the context menu. T

Figure 9-2: Context menu in AP Details page



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 are 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.

AP State	Switch Properties			VLANs Detected	IPv4 or IPv6 Properties	Link Speed	Health Stats
	Switch Name	**Switch Vendor**	**Switch Port**				
Active	Current	Current	Current	Current	Current	Current	Current
Inactive or Offline	Last Known	Last Known	Last Known	Last Known	Last Known	Last Known	Last Known with a note in the right panel: "*Values when AP was last active*" (shown "--" in the Managed Devices and AP listing)
Mesh Root	Current	Current	Current	Current	Current	Current	Current
Mesh Non-Root (Powered by DC or PoE brick)	Not Displayed ("--")	Not Displayed ("--")	Not Displayed ("--")	Current	Current	Not Displayed ("--")	Current
Mesh Non-Root (Used for network extension and connected to a switch)	Current	Current	Current	Current	Current	Current	Current
Link Aggregation: eth0 Up (regardless of whether eth1 is Up or Down)	Current	Current	Current	Current	Current	Current	Current
Link Aggregation: eth0 Down and eth1 is Up	Last known	Last known	Last known	Last known	Current	Last known	Current

Failsafe	Last Known	Last Known	Last Known	Last Known	Last Known	Last Known	Last Known with a note in the right panel: "*Values before AP entered failsafe mode*" (shown "--" in the Managed Devices and AP listing)
LLDP Disabled on Switch	Last Known	Last Known	Last Known	Current	Current	Current	Current

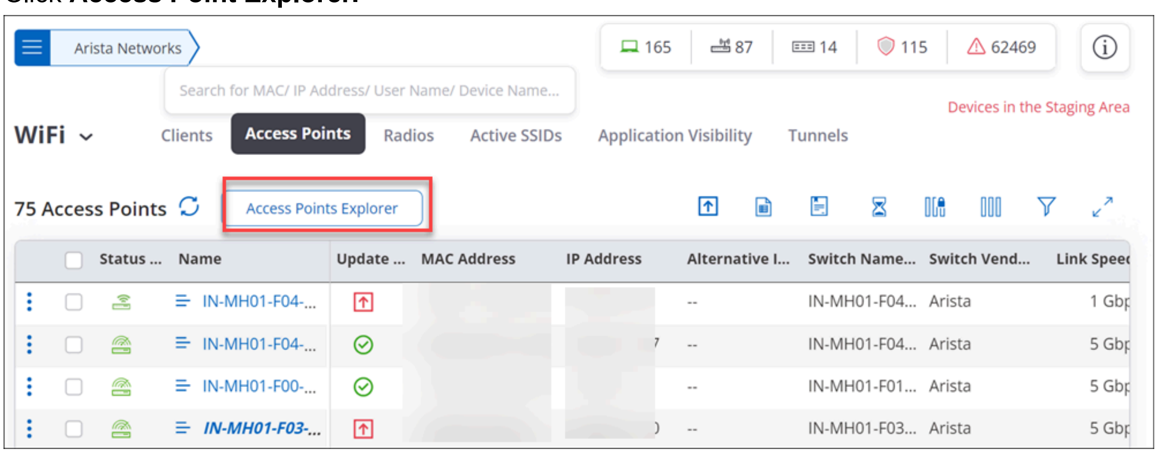
The wired properties of only the primary interface (eth0) of the AP are shown. Thus, when using link aggregation, the switch and VLAN wired properties reflect the information available on the primary interface only; their values do not depend on the state of the secondary interface (eth1). The IP and 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.

9.2.1 Access Point Explorer

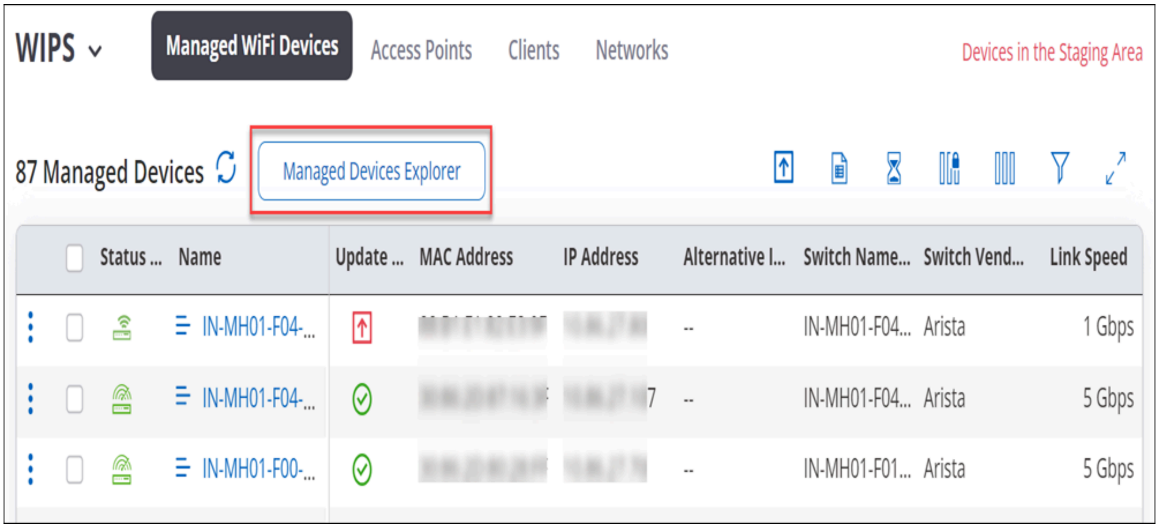
AP Explorer provides a holistic view of all the APs at a location and provides an easy way for the network administrators to understand AP distribution for each attribute.

To view the AP Explorer,

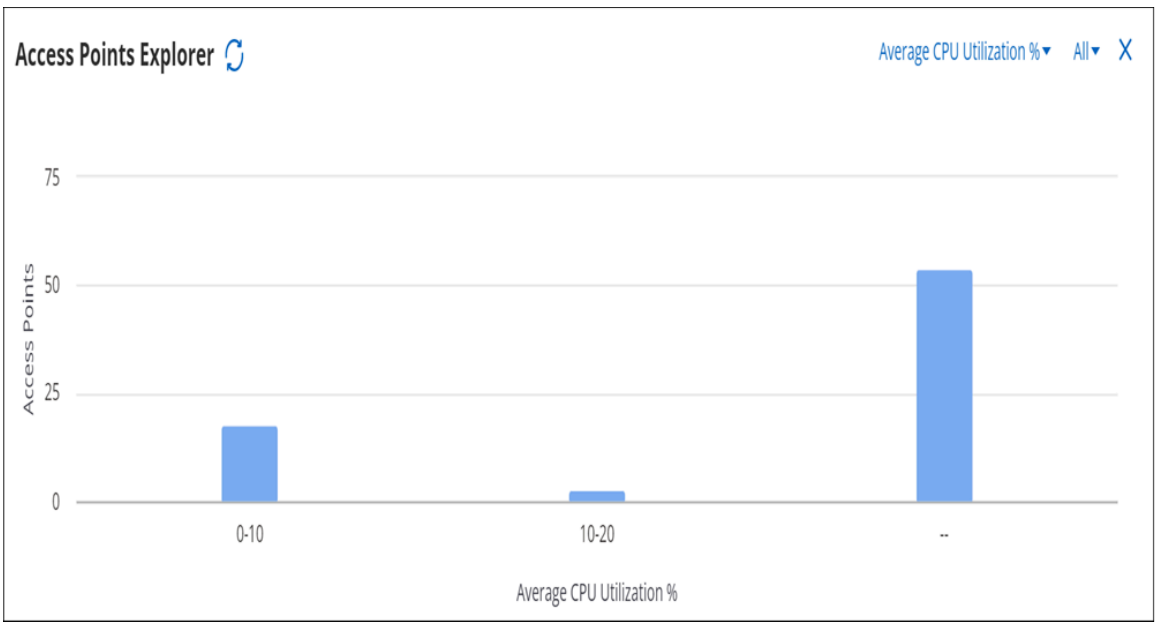
1. Navigate to **MONITOR** > **WiFi** > **Access Points.**
2. Click **Access Point Explorer.**



Alternatively, you can also navigate to AP Explorer from **MONITOR** > **WIPS** > **Managed Device Explorer.**

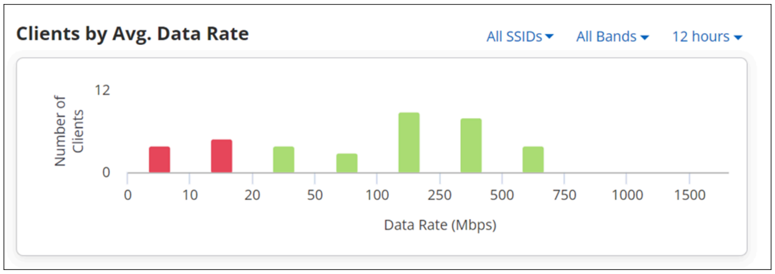


On the AP Explorer chart, you can filter the devices based on the **Device Status** (All, Active, or Inactive). You can use the attribute drop-down menu to view graphical AP distribution based on the selected attribute. For example, you can the AP Explorer chart to get a summary view of AP Health by looking at the APs based on CPU Utilization or Memory Utilization.



9.2.2 Clients by Avg. Data Rate for an Access Point

The Clients by Avg. Data Rate graph displays clients classified based on data rate. CV-CUE 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:

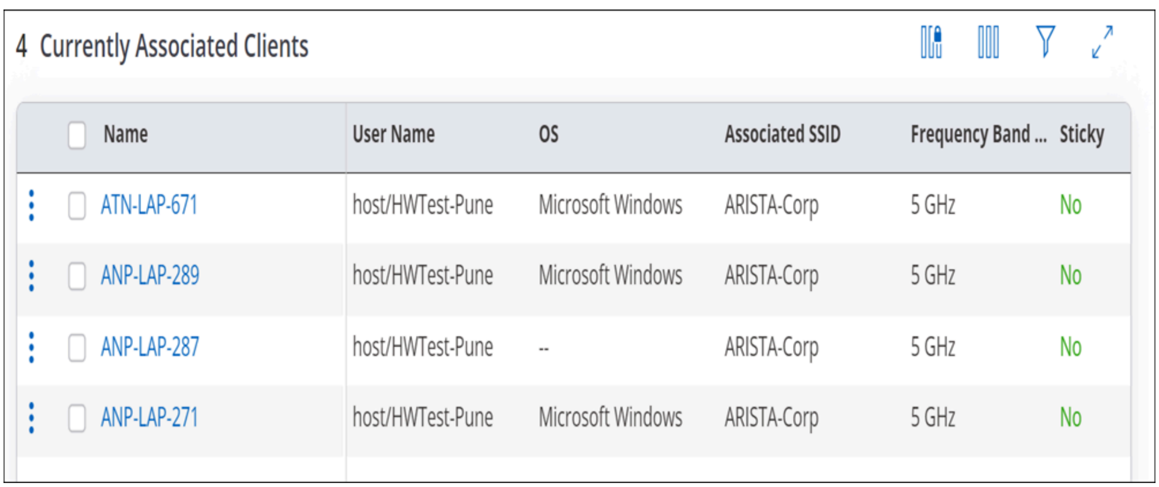
- If all values in the “50 to 100 Mbps” bucket are below 75 Mbps, then the bar in the “50 to 100 Mbps” bucket is red.
- If all values in the “50 to 100 Mbps” bucket are above 75 Mbps, then the bar in the “50 to 100 Mbps” bucket is green.
- If some values in the “50 to 100 Mbps” bucket are above and below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

The chart can be observed for the following bands:

- 2.4 GHz
- 5 GHz
- 6 GHz
- All Bands

9.2.3 Currently Associated Clients for an Access Point

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



4 Currently Associated Clients

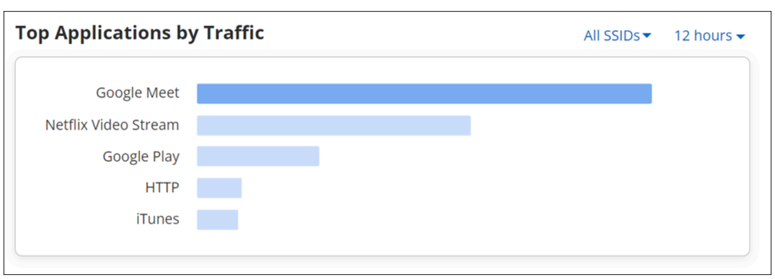
Name	User Name	OS	Associated SSID	Frequency Band ...	Sticky
ATN-LAP-671	host/HWTest-Pune	Microsoft Windows	ARISTA-Corp	5 GHz	No
ANP-LAP-289	host/HWTest-Pune	Microsoft Windows	ARISTA-Corp	5 GHz	No
ANP-LAP-287	host/HWTest-Pune	--	ARISTA-Corp	5 GHz	No
ANP-LAP-271	host/HWTest-Pune	Microsoft Windows	ARISTA-Corp	5 GHz	No

The graph displays the following information:

Column	Description
Name	Name of a device to which AP is connected.
User Name	Name of a user.
MAC Address	Unique 48-bit address of the AP/ 802.11 PHY modes used by the AP.
IP Address	IP address of the AP
Associated SSID	Name of a SSID to which client is connected.
OS	Operating System running on the client.
UP/Down Since	Up since time or Down since time
RSSI (dBm)	Received Signal Strength Indicator.
Sticky	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.
Tx Data Rate	Tx Data Rate is Transmission Data Rate of a client.
Rx Data Rate	Rx Data Rate is Received Data Rate of a client.
Avg Data Rate	Avg Data Rate is Average Data Rate of a client
Retry Rate (%)	Retry Rate (%) is Retransmission rate of a client.

9.2.4 Top Applications by Traffic for an Access Point

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.



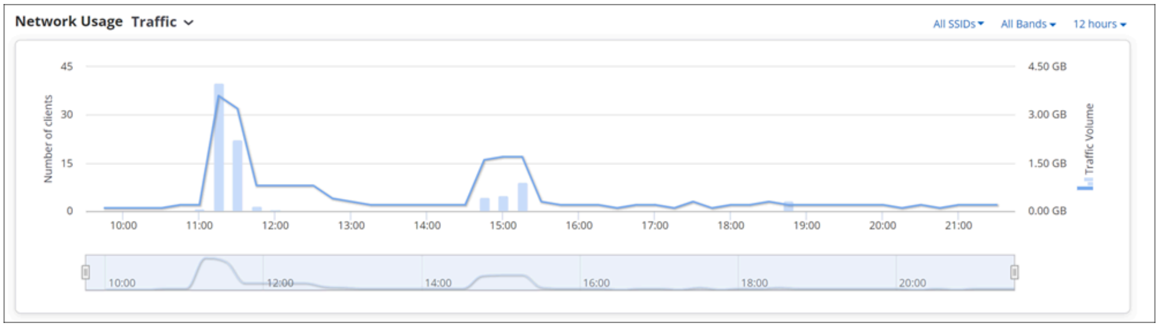
You can choose to view the top applications by traffic for the following time intervals:

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

9.2.5 Network Usage

You can access the Network Usage chart in two different ways from CV-CUE 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.

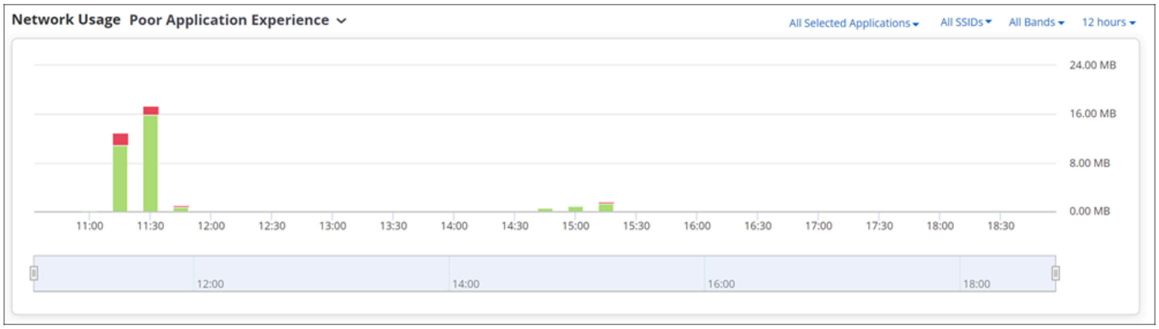
9.2.6 Network Usage - Poor Application Experience

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.



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
- 6 GHz
- All Bands

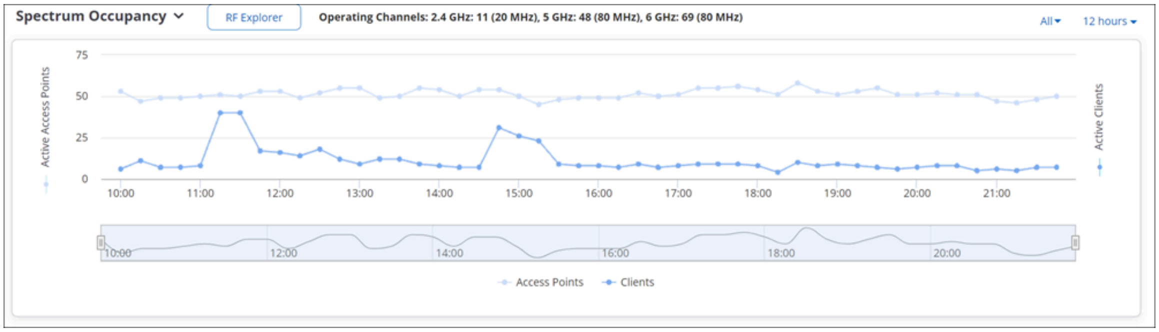
Time Filter

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

9.2.7 Spectrum Occupancy

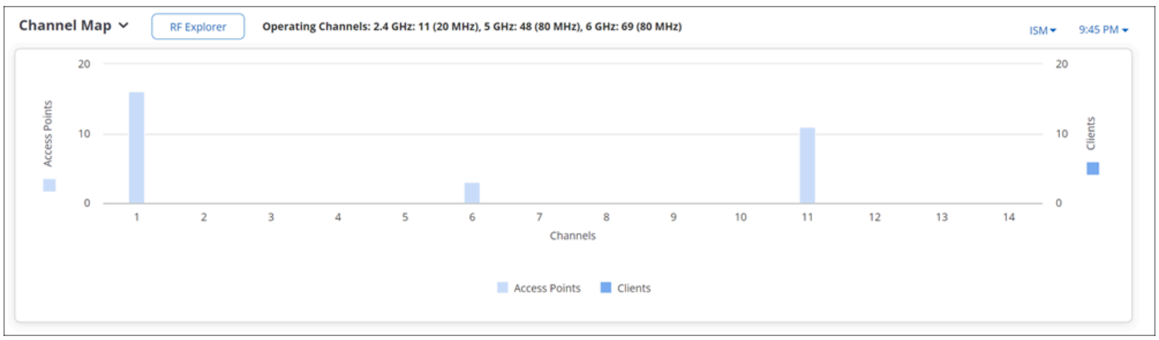
As shown in the following figure, you can filter on a band and duration to see the number of radios and clients that were active in that band in that duration. This can help you identify congested or under-utilized bands.



9.2.8 Channel Map

Channel Map displays the number of clients and Access Points (APs) visible to the managed device at a time on a given channel. Network administrators can use this information to identify congested or underutilized channels in a given band.

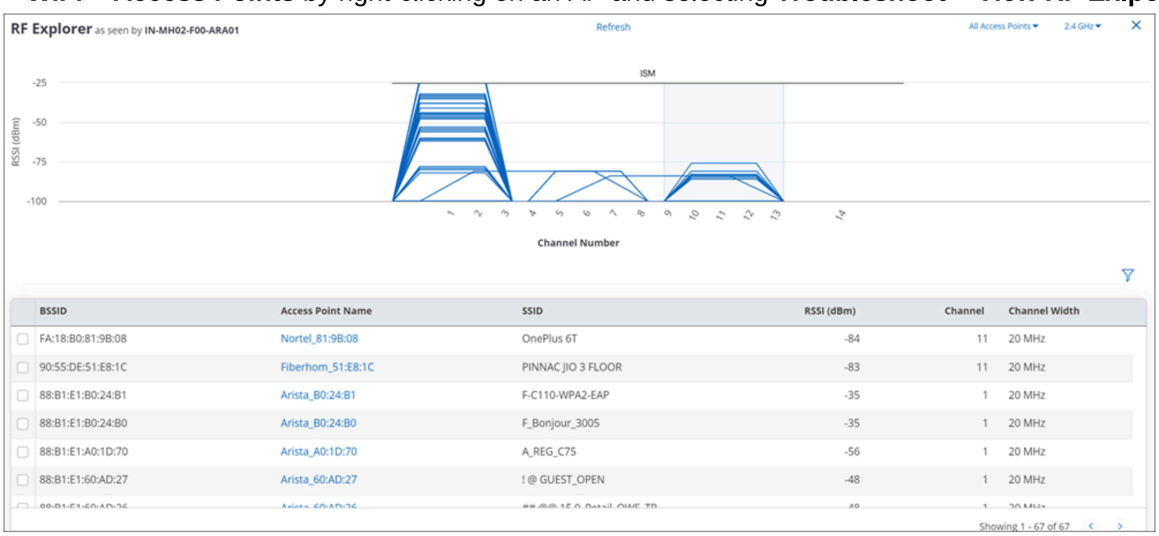
To view Channel Map, select **Channel Map** from the drop-down menu in Specturm Occupancy chart.



In the Channel Map chart, from the right-hand drop-down menu, select the band and use the time slider to select your time interval to view the number of visible clients and APs. You can view the Channel Map upto 12 hours in the past from the current time. Hover over the chart to view the exact count of APs and clients on a given channel.

9.2.9 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 Exlporer**.



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.

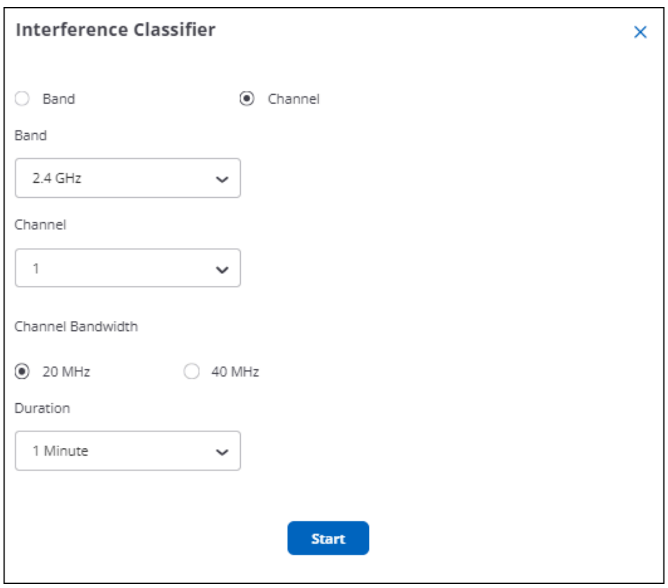
You can use the RF Explorer to identify issues such as co-channel and adjacent channel interference, and DFS channels occupied by APs. The grey rectangle stretching across the RSSI axis represents the operating channel of the AP itself; the heights of the other channel trapezoids indicate the RSSI values 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).

9.2.10 Interference Classifier

One of the reasons why Wi-Fi clients encounter RF issues is non-Wi-Fi interference. All Wi-Fi 6 and above APs can perform interference classification. CV-CUE classifies interference into four categories — Wi-Fi, Microwave Oven (MWO), Frequency Hopping Spread Spectrum (FHSS), and Continuous Wave (CW).

You can run the interference classifier for a specific band or for a specific channel. The results are shown in a separate tab as a read-only information. To launch Interference Classifier from the AP listing, click **MONITOR** > **WiFi** > **Access Points**. Right click an AP and select selecting **Troubleshoot** > **Start Interference Classifier**.

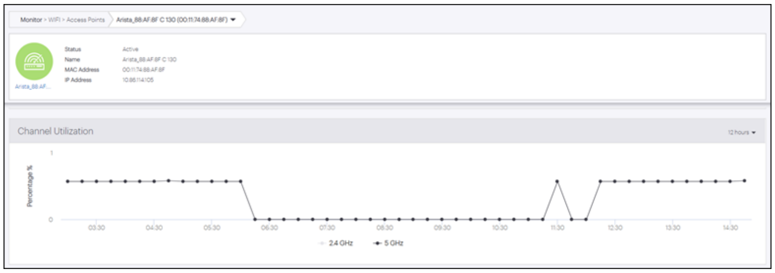
Figure 9-3: Interference classifier



The interference classification opens in a separate tab. Hover your pointer over a data point to see more details about the interference source for a specific channel.

9.2.11 Channel Utilization

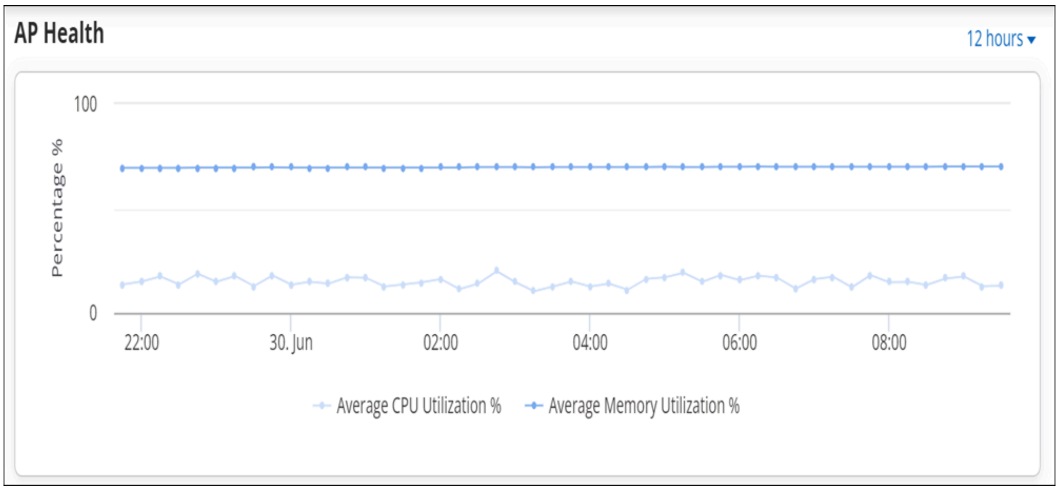
As shown in the following figure, the channel utilization chart shows the AP channel utilization (as a percentage value) averaged over 15-minute intervals for both the 2.4 GHz and 5 GHz bands, for the selected duration.



The channel utilization chart is available for 2.4, 5, and 6 GHz bands.

9.2.12 Access Point Health

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



9.2.13 Visible BSSIDs

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

Visible BSSIDs - Managed

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

Visible BSSIDs - Managed

BSSID	AP Name	Associated SSID	RSSI (dBm)	Channel	Clients	Channel Wi...	Frequency ...
30:86:2D:D0:0C:40	[illegible]	ARISTA-Guest	-77	1	--	20 MHz	2.4 GHz
30:86:2D:B0:02:D0	[illegible]	Arista-Emp-Test	-72	144	--	80 MHz	5 GHz
30:86:2D:B0:02:D1	[illegible]	ARISTA-Corp	-72	144	2	80 MHz	5 GHz
30:86:2D:B0:02:D2	[illegible]	ARISTA-Guest	-72	144	--	80 MHz	5 GHz
30:86:2D:B0:02:D3	[illegible]	ARGRP	-72	144	--	80 MHz	5 GHz
30:86:2D:87:16:00	[illegible]	Arista-Emp-Test	-76	140	--	80 MHz	5 GHz

Visible Access Points - Un-managed

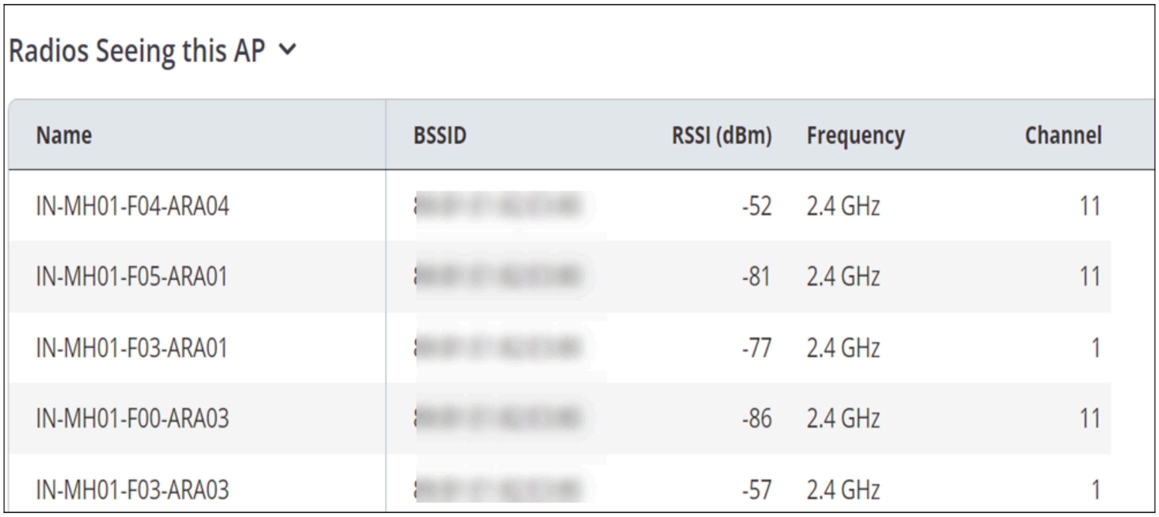
Selecting un-managed from the drop-down list displays the Access Points that do not belong to your network but are in the vicinity of the selected AP.

Visible BSSIDs - Unmanaged

BSSID	AP Name	Associated SSID	RSSI (dBm)	Channel	Clients	Channel Wi...	Frequency ...
[illegible]	[illegible]	Omega-Support.b,	-42	6	--	20 MHz	2.4 GHz
[illegible]	[illegible]	SCALE-SSID-Remote	-55	11	--	20 MHz	2.4 GHz
[illegible]	[illegible]	SCALE-SSID-WPA3-...	-55	11	--	20 MHz	2.4 GHz
[illegible]	[illegible]	SCALE-SSID-WPA2-...	-55	11	--	20 MHz	2.4 GHz
[illegible]	[illegible]	SCALE-SSID-WPA3-...	-55	11	--	20 MHz	2.4 GHz

9.2.14 Radios Seeing this Access Point

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

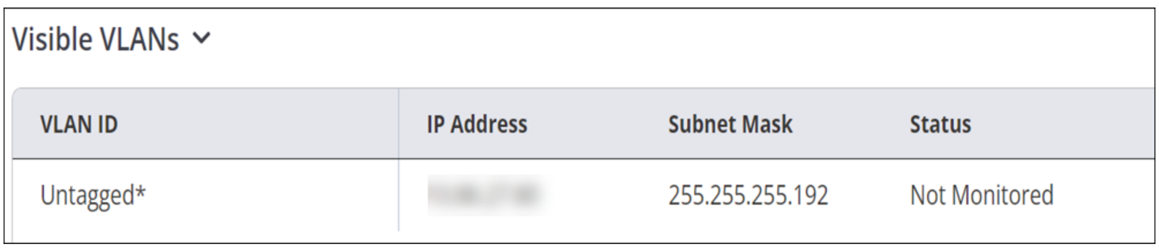


Radios Seeing this AP

Name	BSSID	RSSI (dBm)	Frequency	Channel
IN-MH01-F04-ARA04	[illegible]	-52	2.4 GHz	11
IN-MH01-F05-ARA01	[illegible]	-81	2.4 GHz	11
IN-MH01-F03-ARA01	[illegible]	-77	2.4 GHz	1
IN-MH01-F00-ARA03	[illegible]	-86	2.4 GHz	11
IN-MH01-F03-ARA03	[illegible]	-57	2.4 GHz	1

9.2.15 Visible VLANs

The visible VLANs widget is available on drilling down from any managed Wi-Fi 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.

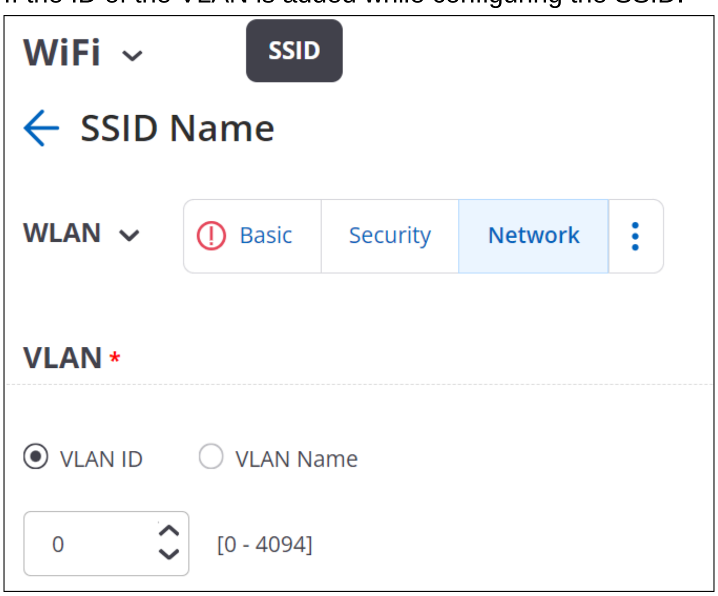


Visible VLANs

VLAN ID	IP Address	Subnet Mask	Status
Untagged*	[illegible]	255.255.255.192	Not Monitored

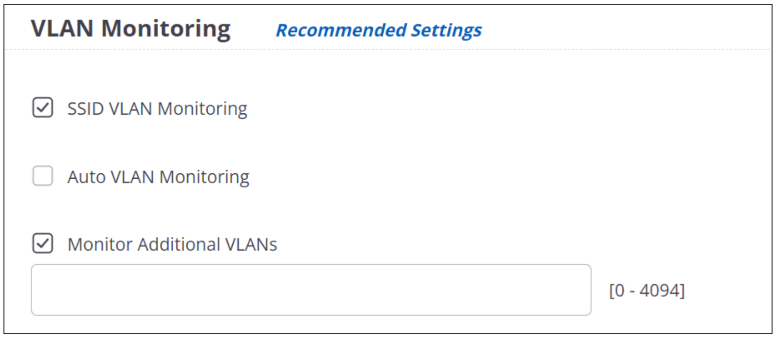
The VLANs that can be seen by the selected device are populated depending on the following:

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.



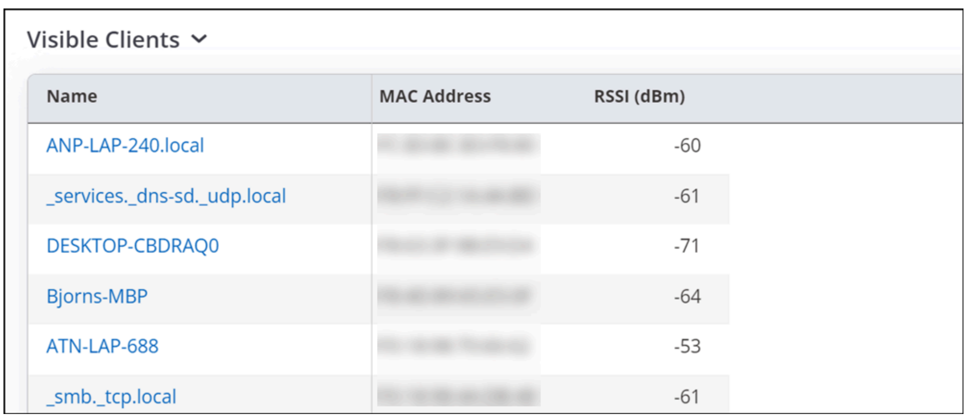
3. If you enable Auto VLAN monitoring from **CONFIGURE** > **Device** > **Access Points** > **Security,** the active VLAN is monitored by the device with the highest MAC address.

   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**.



9.2.16 Visible Clients

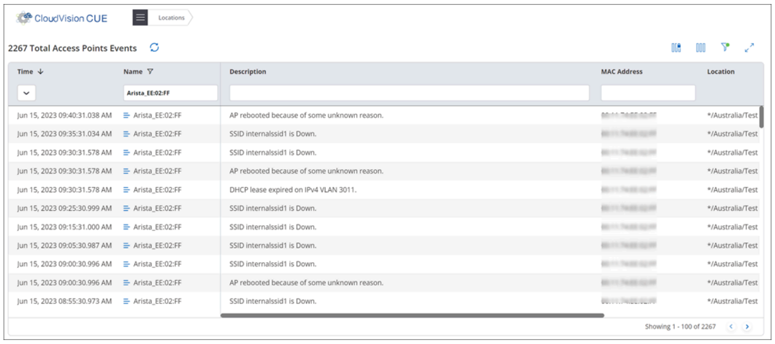
The Visible Client widget provides the list of clients visible to the selected AP. It also provides the total number of visible clients on the top left corner of the widget.



9.2.17 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**Troubleshoot** > **View Event Longs.** with a right-click on any AP.



The detailed information about the event logs is as follows:

Column	Description
Category	It is a category of event.
Type	It is a type of event.
Description	It is description of event.
Date	Timestamp at which event occurred.

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.

9.2.18 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** > **WiFi** > **Access Points** or **MONITOR** > **WIPS** > **Access Points.**
2. Right click on the AP, you wish to locate on the Floor Map.
3. Select **Locate**. These option is enabled only if the selected AP is placed on any of the floor maps. Else it is disabled.

9.2.19 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.

CV-CUE 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** > **WiFi** > **Access Points.**
2. Right click on the AP, for which you wish to customize the settings.
3. Select **Customize Transmit Power or Channel**.
4. Select appropriate frequency for which you wish to customize the settings.
5. Select **Customize Transmit Power** for transmit power settings. Select **Auto** or **Manual** option.
6. Select **Customize Channel Settings** for channel settings. Select **Operating Channel**as either **Auto** or **Manual**.
7. Click **Save**.

9.2.20 Customize VLANs to Monitor per Access Point

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

1. Go to **MONITOR** > **WiFi** > **Access Points** or **MONITOR** > **WIPS** > **Managed WiFi Devices**, 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 Wi-Fi server over the Communication VLAN. So the Communication VLAN must be one of the VLANs that the AP monitors.
6. Save the configuration.

9.2.21 Move an Access Point

CV-CUE provides the facility to change the location of an AP using the **Move** option.

To move an AP:

1. Go to **MONITOR** > **WiFi** > **Access Points** or **MONITOR** > **WIPS** > **Access Points.**
2. Right-click on the name of the AP that you want to move and select **Move**.
3. Select the new location, where you wish to move the AP.
4. Click **Move**.
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.

9.2.21.1 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.

Source		Destination	
Is the device in a group?	**Does the group have a config?**	**Is the same group available at the destination location?**	**Behavior**
Yes	Yes	Yes	All devices become part of the destination group but retain their configuration.
Yes	Yes	No	All devices are removed from their respective groups and start using the default configuration of the destination folder.
Yes	No	Yes	All the devices are removed from their respective groups and become part of the destination group. They start using the configuration of the destination group.
Yes	No	No	All devices are removed from their respective groups and start using the default configuration of the destination folder.

9.2.22 Reboot Access Points

You can reboot an AP, with the help of CV-CUE.

Perform the following tasks to reboot an AP:

1. Go to **MONITOR** > **WIPS** > **Access Points.**
2. Right-click on the name of the AP that you want to reboot and select **Reboot**.
3. Click **Yes** to reboot the AP.

9.2.23 Rename Access Points

You can change the name of the AP.

Perform the following tasks to rename an AP:

- Go to **MONITOR** > **WiFi** > **Access Points** or **MONITOR** > **WIPS** > **Access Points.**
- Right-click on the name of the AP that you want to rename and select **Rename**.
- Change the name of the AP and click **Done** to save the changes.

9.2.24 Delete Access Points

You can delete the access points (APs) from the list of APs available on the Access Points tab.

Deleting APs from **MONITOR** > **WiFi** > **Access Point** or **MONITOR** > **WIPS** > **Managed Devices** deletes the BSSIDs (the properties) of the AP but doesn't remove the AP from the listing. To permanently remove the APs fromthe listing, unassign them from Arista Launchpad.

MONITOR > **WIPS** > **Access Point**shows all the APs (BSSIDs) visible to the managed access points in the vicinity; the BSSIDs could be the Managed AP's BSSID, another managed AP's BSSID, or neighboring company's BSSIDs.Deleting the neighboring company’s AP removes it from the list. Deleting a Managed AP resets its properties but doesn't remove it from the AP list.

Follow these steps to delete an AP:

1. Go to **MONITOR** > **WiFi** > **Access Points** or **MONITOR** > **WIPS** > **Managed Devices.**
2. Right-click on the name of the AP that you want to delete and select **Delete**.
3. Click **Yes** to confirm the deletion.

Important: If the AP is physically active on the network after deletion, then:

- CV-CUE marks the AP to the Unknown location.
- The default Device Settings of the Unknown location is applied.
- The default SSIDs are pushed on the active AP, if the AP is configured in the Device Settings.
- No SSIDs are applied, if the AP is not configured.

9.2.25 View Ongoing Activities on Access Point

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 CV-CUE 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:

   Choose From:

   - 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.

9.2.26 View Access Point Uptime

Access Point (AP) Uptime indicates how long the AP has been up and running. To view AP Uptime, navigate to **MONITOR** > **WIPS** > **Managed WiFi Device.** The *Last Booted At* column shows the AP Uptime.

9.2.27 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 Wi-Fi configuration to multiple devices across different locations. If a group has no configuration, then the assigned devices will use the default Wi-Fi configuration of their respective locations. On the other hand, suppose an AP already has custom Wi-Fi configuration applied to it. Then if you assign such an AP to a group it will start using the Wi-Fi configuration of the group.

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

- Assign a Device to a Group from Access Points tab
- Assign a Device to a Group from the Folders/Floors Page

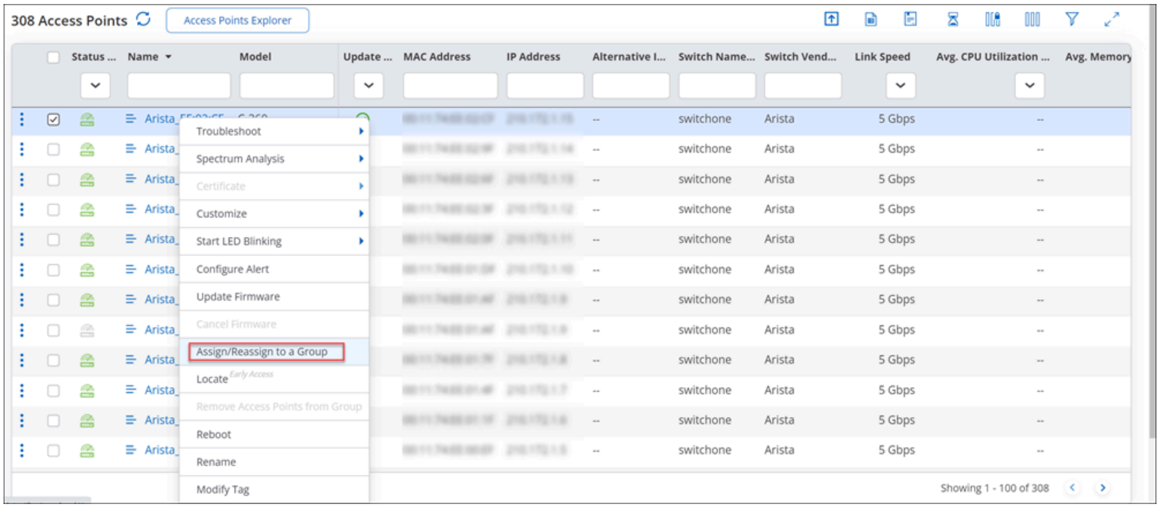
9.2.27.1 Assign a Device to a Group from Access Points tab

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** > **WiFi** > **Access Points.**

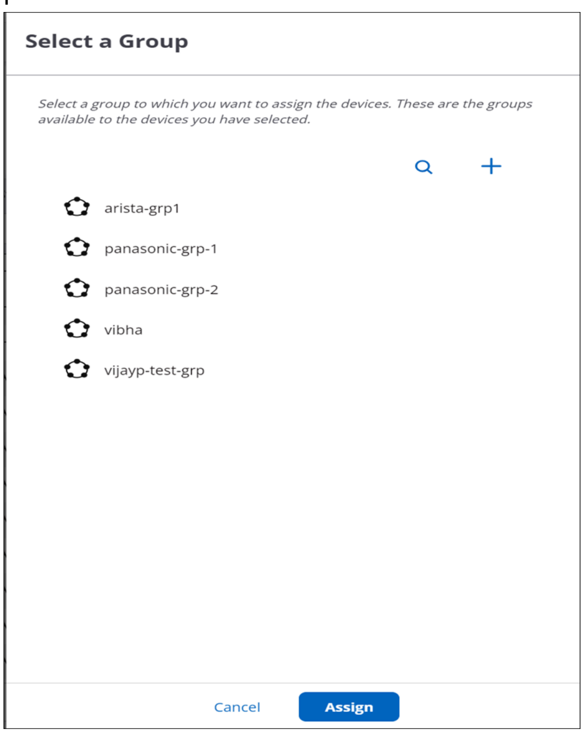
2. Right-click on the name of a single AP, that you want to assign to a group or click on the menu icon (three vertical dots) and select **Assign/Reassign to a Group.**



3. Select the group to which you want to assign the selected AP.

   Info: 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**.

9.2.27.2 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.
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**.
4. Select the group to which you want to assign to the selected AP.

   Info: 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**.

9.2.28 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 Wi-Fi configuration. If the target group does not have Wi-Fi configuration applied to it, access points will use their location's default Wi-Fi 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 does not have any configuration , then such devices will use the default Wi-Fi configuration of the respective folder.

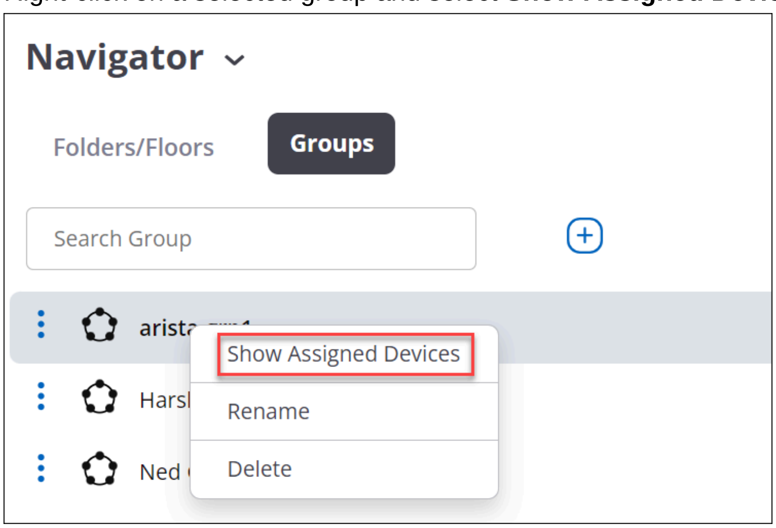
Re-assigning a device to a group can be done from three different tabs:

- Assign a Device to a Group
- Assign a Device to a Group from the Folders/Floors Page
- Groups

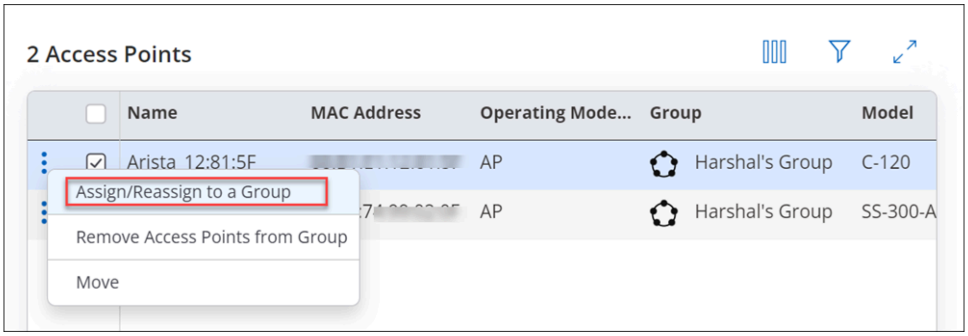
The first two methods are the same as for assigning a device to a group. The third one is applicable only to re-assigning devices.

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

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



3. Right-click on the name of the AP you want to reassign and click **Assign/Reassign to a Group**.



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

9.2.29 About Device Firmware Update in CV-CUE

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.

9.2.29.1 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** > **WiFi** > **Access Points.**
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.
4. Click **Update**.

9.2.29.2 Update Firmware for Multiple Access Points

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** > **WiFi** > **Access Points.**
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.

9.2.29.3 Schedule Firmware Update of a Single AP

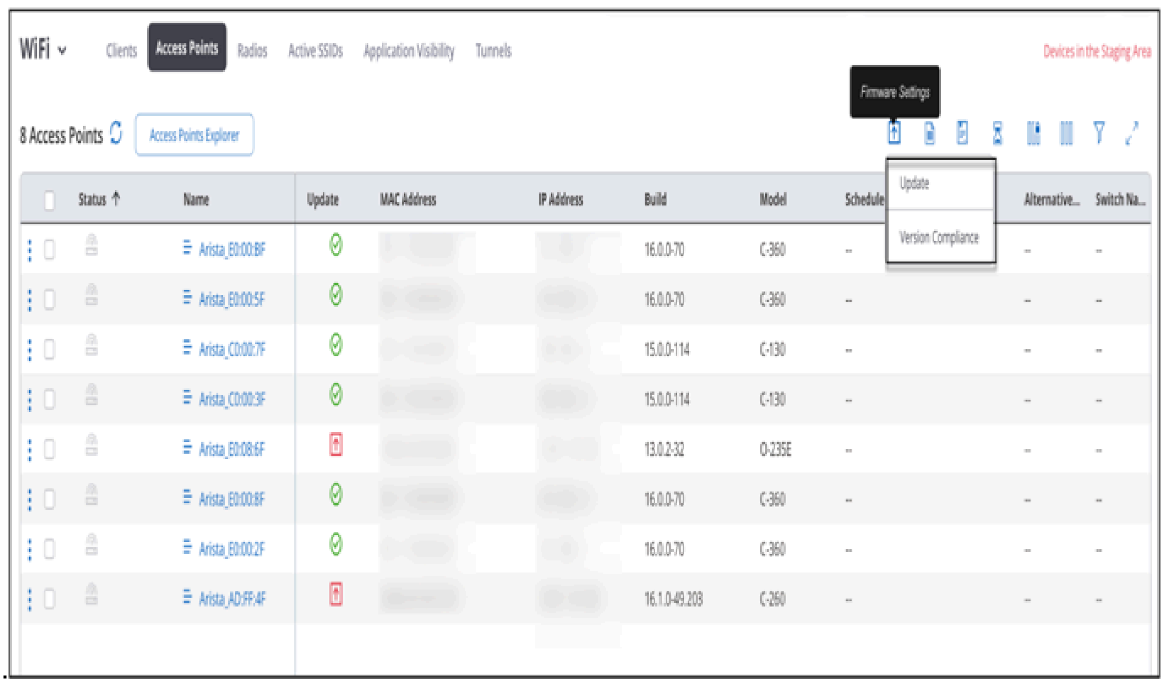
Follow these steps to create a recurring or one-time schedule to update the AP firmare:

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

9.2.29.4 Schedule Firmware Update of Multiple Access Points

Follow these steps to create a recurring or one-time schedule to update the AP firmare:

1. Go to **MONITOR** > **WiFi** > **Access Points.**
2. Click **Update** under **Firmware Settings**



icon.

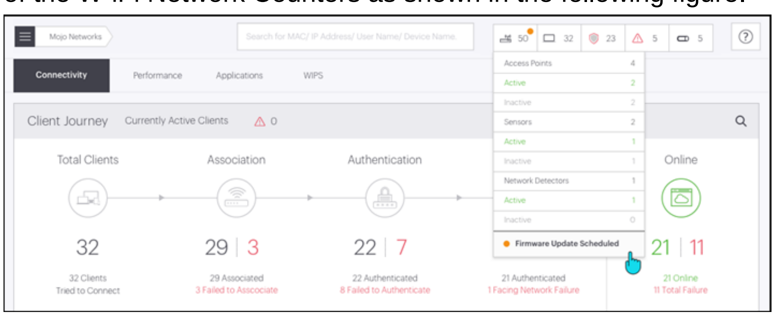
3. Provide the schedule for update in the Firmware Update Settings right panel.

   The following table provides additional information for some of the options the Firmware Update Settings panel:

Table 2:

UI Option	Description
Apply Update Settings Recursively to Subfolders	Applies the update settings to the selected folder location and also to all its subfolders, if any.
Hitless Update	Updates access points with minimum impact to Wi-Fi 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 Wi-Fi will be impacted.
Update Window	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.

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 W-iFi Network Counters as shown in the following figure.



9.2.29.5 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** > **WiFi** > **Access Points.**
2. Right-click the AP for which you want to cancel the firmware update and select **Cancel Update**.
3. Click **Yes** to cancel the update.

9.2.29.6 Configure Firmware Version Compliance

Organizations may have multiple access points (APs) of different models operating with various firmware versions. As an organization, you may want to designate a specific version as a compliant firmware version for a certain model. Assigning a compliant firmware version helps network administrators identify non-compliant AP models by generating notification alerts.

Firmware Version Compliance is a location-based setting and is applicable for all access points placed at the location.

Note: Configure the firmware version compliance before you update the AP firmware version.

Assign a Compliant Firmware Version

Follow these steps to assign a firmware version as the compliant version across the organization:

1. Select **MONITOR** > **WiFi** > **Access Points**
2. Select **Firmware Settings** > **Version Compliance.**
3. Select the **Compliant Version** checkbox.
4. Select one of the two options:
    - **Latest Version for all Models:** Indicates that the latest firmware version is the compliant version across your organization. CV-CUE will raise an alert if any AP model doesn't have the latest firmware version.
    - **Customize:** Specify the AP model number and the firmware version you want to standardize across your organization. After you have made the selection, if any AP doesn't have the compliant version, CV-CUE will raise an alert.
5. Save the settings.

Configure Alerts

The compliant firmware detection alert notifies you whenever CV-CUE detects non-compliant firmware. To configure alerts for compliant firmware, go to **CONFIGURE** > **Alerts** > **Device**and select **Access Point with non-compliant firmware version detected.**For more information on this alert, refer to Configure System Alerts

9.2.30 Access Point Web Shell

Web Shell is an online interface to remotely log into an access point (AP) via SSH. An administrator or a superuser can open Web Shell for a specific AP from CV-CUE. 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 CV-CUE.

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**

9.2.30.1 Open Access Point Web Shell

You can open the Access Point (AP) web shell from CV-CUE for an individual AP and perform basic operations using CLI commands.

To open the AP Web Shell:

1. Got 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.

9.3 Custom Certificates for Access Points

Manage custom certificates and CA certificates for access points from a central location.

Access points (AP) can authenticate themselves to the network using respective certificates. With AP VPN, an AP uses the EAP-TLS protocol for authentication. Since EAP-TLS requires the client and network to authenticate themselves using respective certificates, the protocol is considered robust compared to exchanging shared secret and Xauth password. Therefore, the AP VPN solution requires the AP to use a unique certificate per AP or per tunnel. APs can use the default certificate or a custom certificate for the authentication.

Caveats

Note the following points before you create certificates:

- You can upload the Device and CA certificate in the PEM encoded format.
- You can upload a certificate with a maximum of five CA chain length.
- You need to upload the device certificate and root CA chain separately at two different places.
- When you regenerate a CSR, the existing certificates on the APs are not deleted until the new signed certificates are installed on the AP.
- When you regenerate a CSR, the existing certificates on the APs are not deleted until the new signed certificates are installed on the AP.

9.3.1 Certificate Flow Overview

High level process flow for managing certificates.

Here’s a high level process flow on how you manage certificates in CV-CUE:

1. Generate CSR.
   a. Create a new tag and assign it to a CSR from the global certificate menu. Note that you cannot a create a new tag for an individual AP.
   b. Use an existing tag to generate a CSR. You can use an existing tag for an individul AP or for all APs.
2. Download the generated CSR and get it signed manually/offline.
3. Upload Device Certificate.
4. Upload CA Certificates.

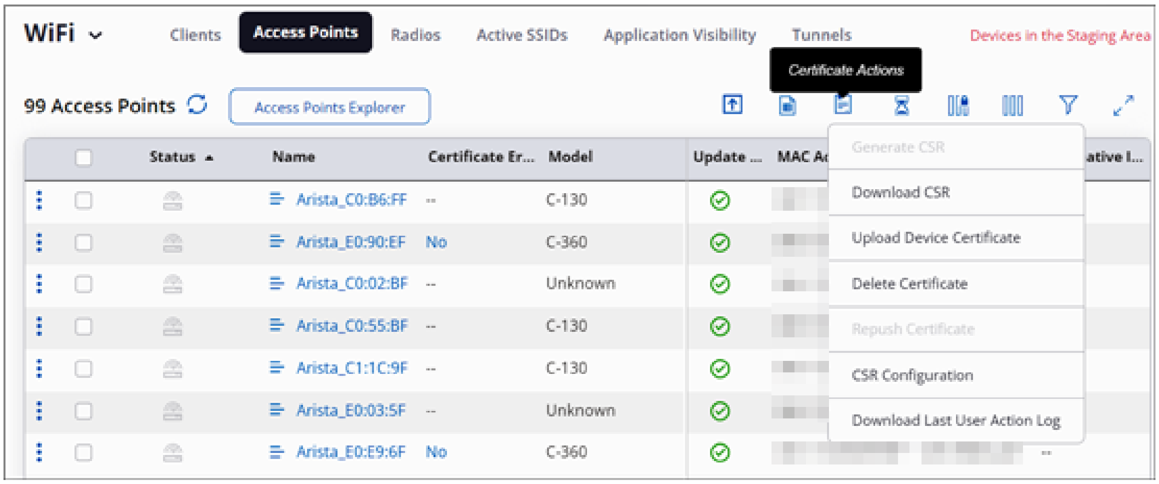
9.3.2 Certificate Actions and Tags

Describes different actions available for certificates from the global toolbar as well as per AP.

You can take actions related to certificates for each AP or for all the APs seen in the **Monitor > Access Points** tab. When you use the global menu to perform your certificate-related actions, it applies to all APs in that location. For individual APs, you can perform the certificate actions from the three-dot menu per AP.

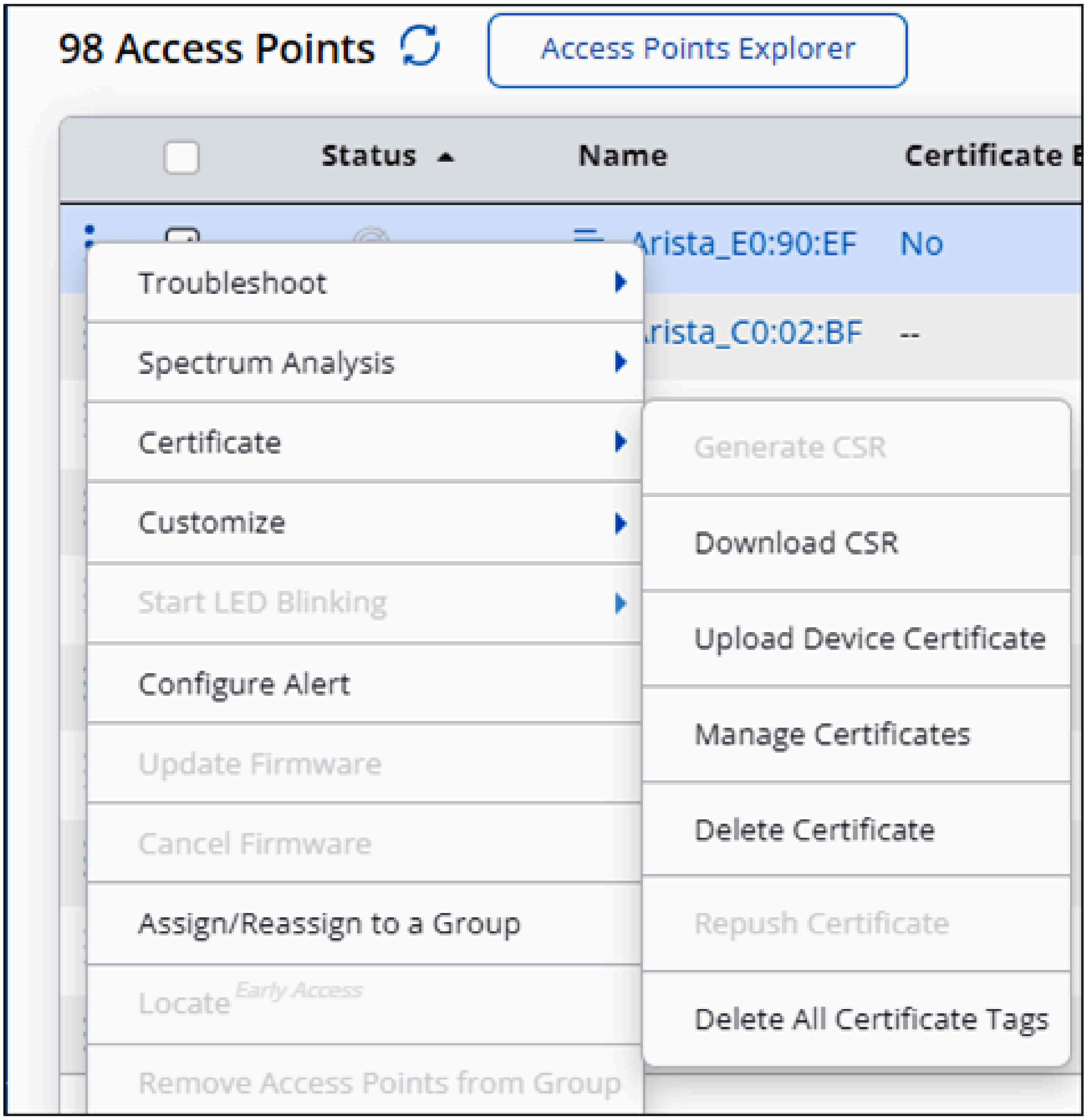
The following image shows the certificate actions from the toolbar:

Figure 9-4: Certificate actions from the global toolbar



The following image shows the certificate actions per AP:

Figure 9-5: Certificare actions per AP

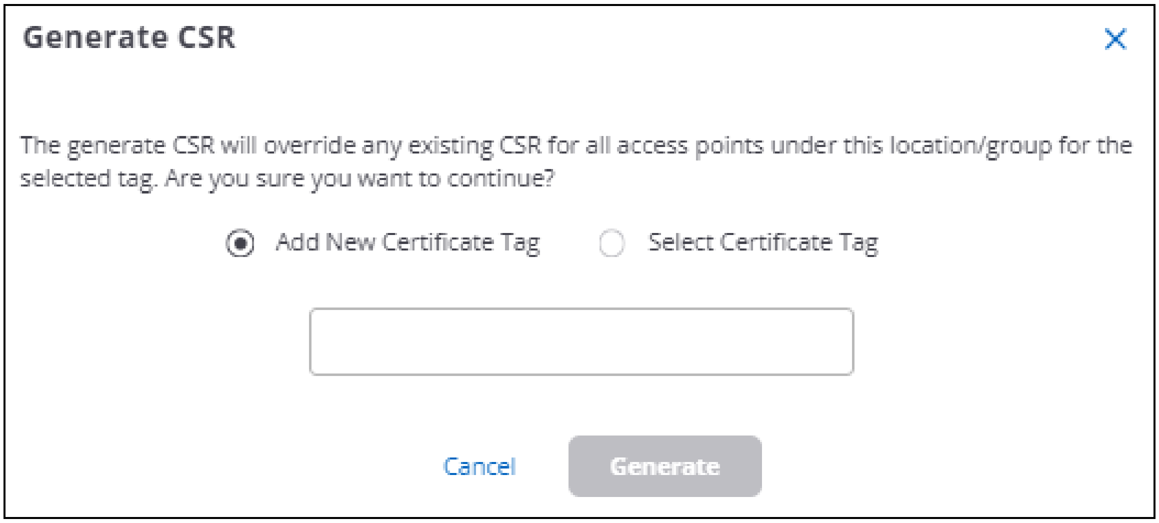


Certificate Tags

Each certificate must have a tag associated with it. Typically, you assign tags for a specific function or you could keep a generic tag and use it for all purposes. For example, you could use a tag named IPsec and assign it to all the APs that use the IPsec protocol. You can also use a tag named Generic and use it for all purposes. This makes handling of certificates easier through tags. Note that after you update the certificate, you still need to manually upload the new certificates to APs.

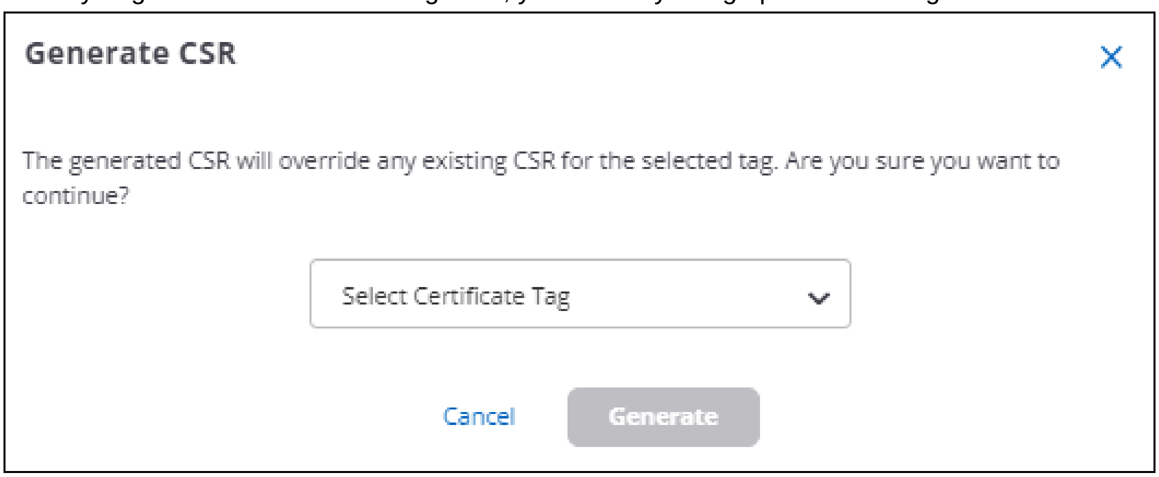
When you manage certificates for the first time, you do not have any predefined tags. In such cases, you have to create a tag first and then generate a CSR.

Figure 9-6: Create a new certificate tag



You can create a new tag from the global certificate actions only. You cannot create a new tag for an individual AP.

When you generate a CSR for a single AP, you can only assign pre-created tags.



9.3.3 CSR Configuration

Configure CSR properties for access points.

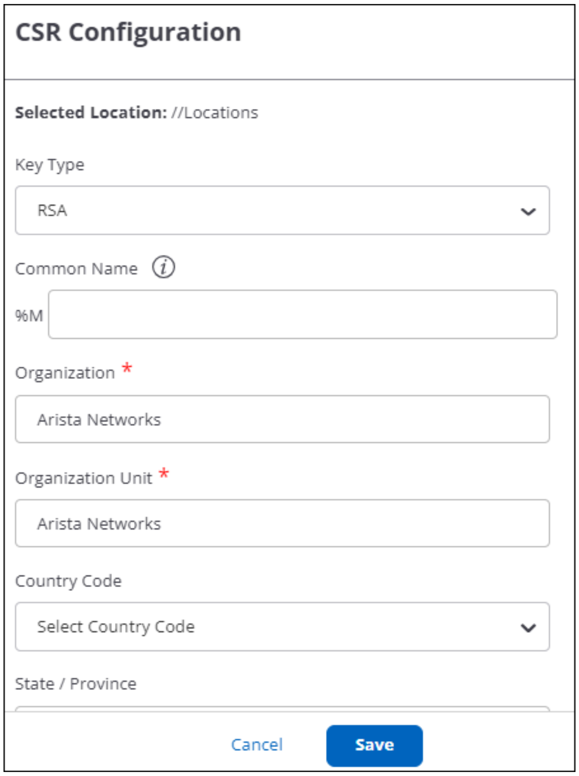
CSR Configuration allows you to configure CSR properties for your AP. This is a location-based configuration.

To configure CSR for your AP:

1. Go to **MONITOR** > **WiFi** > **Access Points**
2. Click the **Certificate Action** button from the global toolbar and click **CSR Configuration**.

3. In the rght panel, provide the values for each field.

Figure 9-7: CSR configuration



4. Save the configuration.

9.3.4 Generate CSR

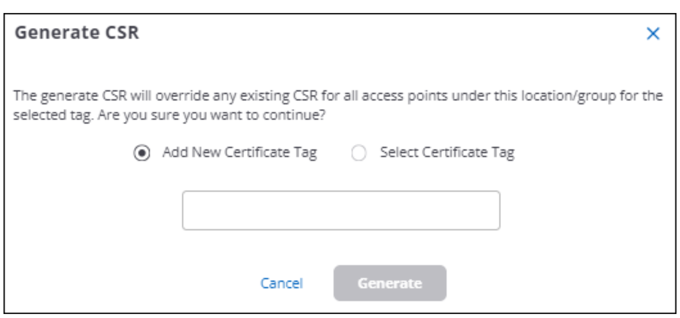
Generate CSR for your access points.

You can generate CSR for individual APs or all the APs at the selected location. When you generate CSR for all the APs, you can create a new tag and assign it to the CSR. However, if you generate a CSR for an individual AP, you cannot create a new tag. You have to use an existing tag.

To generate CSR for all the APs at a specific location:

1. Go to **MONITOR** > **WiFi** > **Access Points**.
2. Click the **Certificate Action** button and click **Generate CSR**.
3. Assign a new tag or use any existing tags if you have.

Figure 9-8: Add new tag and generate CSR



4. Click **Generate**.

9.3.5 Manage Certificates

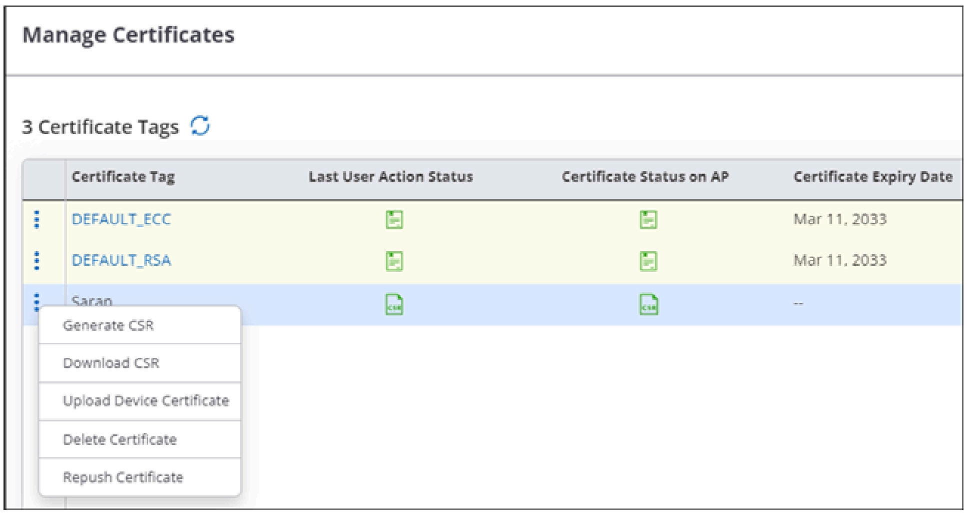
Manage certificates for each access point.

You can see all the certificates for a location from the Manage Certificates page. It is a per-AP feature. Right-click an AP, then click **Certificate** > **Manage Certificates**. You can view the current status of certificates based on the tags. Refresh the page to get the latest certificate status.

For each certificate tag, you can perform the forllowing actions:

- Generate CSR
- Download CSR
- Upload Device Certificate
- Delete Certificate
- Repush Certificate

Figure 9-9: Manage certificates per AP



The **Last User Action Status** column shows the latest action performed by the user. For example, if you regenerate the certificate, this column shows the status of your action. The **Certificate Status on AP** column shows whether the AP already has a certificate or if it's in the process of obtaining a certificate.

The actions on the Manage Certificate page are already associated with a tag. Therefore, you do not have to provide a new tag when you perform any action from this page.

9.3.6 Upload Device Certificate

Upload device certificate for one or all access points.

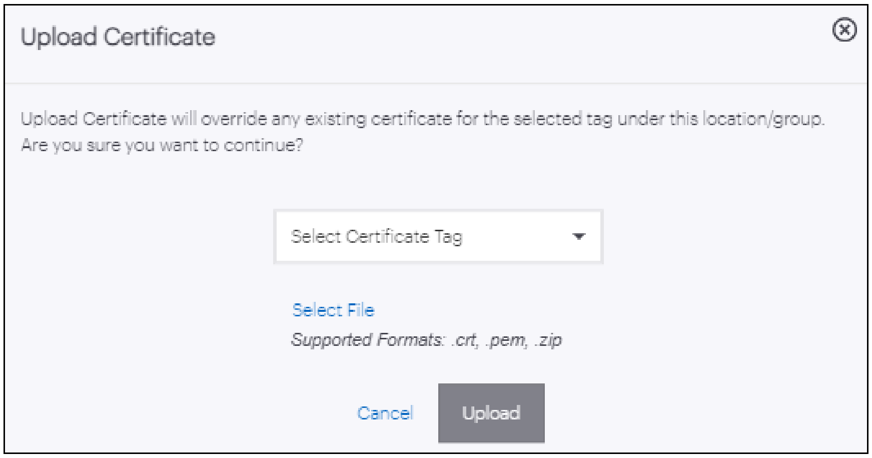
After the certificates are signed by the signing authority, you can upload the device certificate either from the global toolbar or individually for each AP. You must upload the device certificate first before uploading the CA certificates.

To upload the device certificate for each AP:

1. Go to **MONITOR** > **WiFi** > **Access Points**.
2. Select the APs for which you want to upload the signed certificates.

3. Click the three-dot menu and click **Certificate** > **Upload**.

Figure 9-10: Upload certificate for a single access point



4. Select the certificate tag and click **Upload**.

9.3.7 Upload CA Certificate

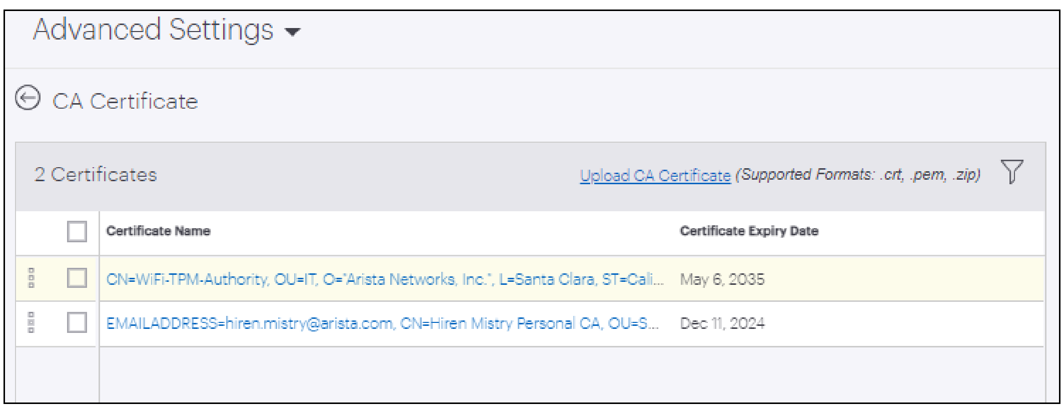
Upload CA certificate in Advanced Settings.

You can upload the CA certificates from the global settings and the CA certificates get automatically applied to the respective APs that have the device certificate installed.

To upload CA certificates:

1. Go to **SYSTEM** > **Advanced Settings** > **CA Certificate**.
2. Click **Upload CA Certificate**.

Figure 9-11: Upload CA certificate



3. Select the certificate or the certificate chain zip file from your local drive.
4. (Optional) Select a certificate and click the three-dot menu icon to **Delete** or **Download** the CA certificate.
5. (Optional) Click the certificate to view the certificate details in the right panel.

Note that the default certificate is grayed out and you cannot delete it.

9.3.8 Delete Certificate

When you delete a certificate, the tag is also deleted from the AP. When you delete certificates from an AP, you delete both the device certificate and CA certificates associated with the respective tag.

To delete certificates from an AP:

1. Go to **MONITOR** > **WiFi** > **Access Points**.
2. Select the APs for which you want to delete the certificates.
3. Click the three-dot menu and click **Certificate** > **Delete**.

However, if you want to update a certificate and not delete it, you can use the **Upload** option and it will update the certificate.

1.

9.3.9 Repush Certificate

Repush a certificate to reupload an existing but corrupt certificate.

When you repush a certificate, the server tries to reupload the device and CA certificates to the AP. Use this option when the AP malfunctions and stops associating with the installed certificates.

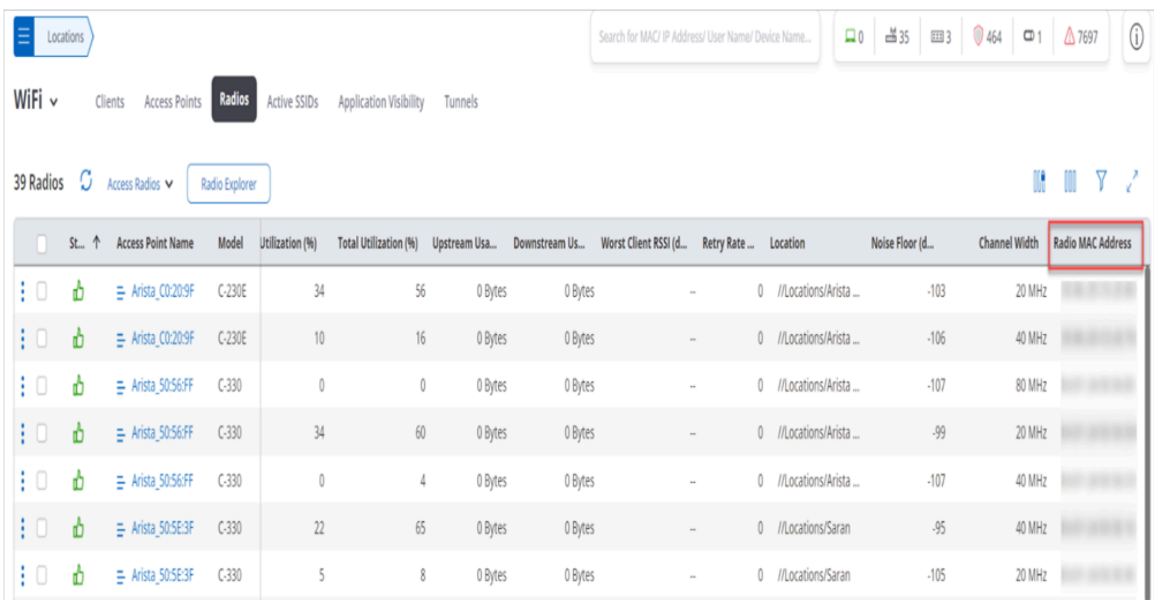
When you initiate the Repush action, the server automatically identifies the certificate that was previously available and tries to reinstall the certificate. Note that when you delete a certificate from an AP, the Repush action will not be effective to reinstall the certificate. You need to manually reupload certificates then.

9.4 Radios

The Radios tab under **MONITOR** tab has Access Radio Grid and Multifunctional Radio Grid.

Access Radio Grid

Access Radio Grid contains a list of all the radios operating on 2.4 GHz, 5 GHz, and 6 GHz 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.



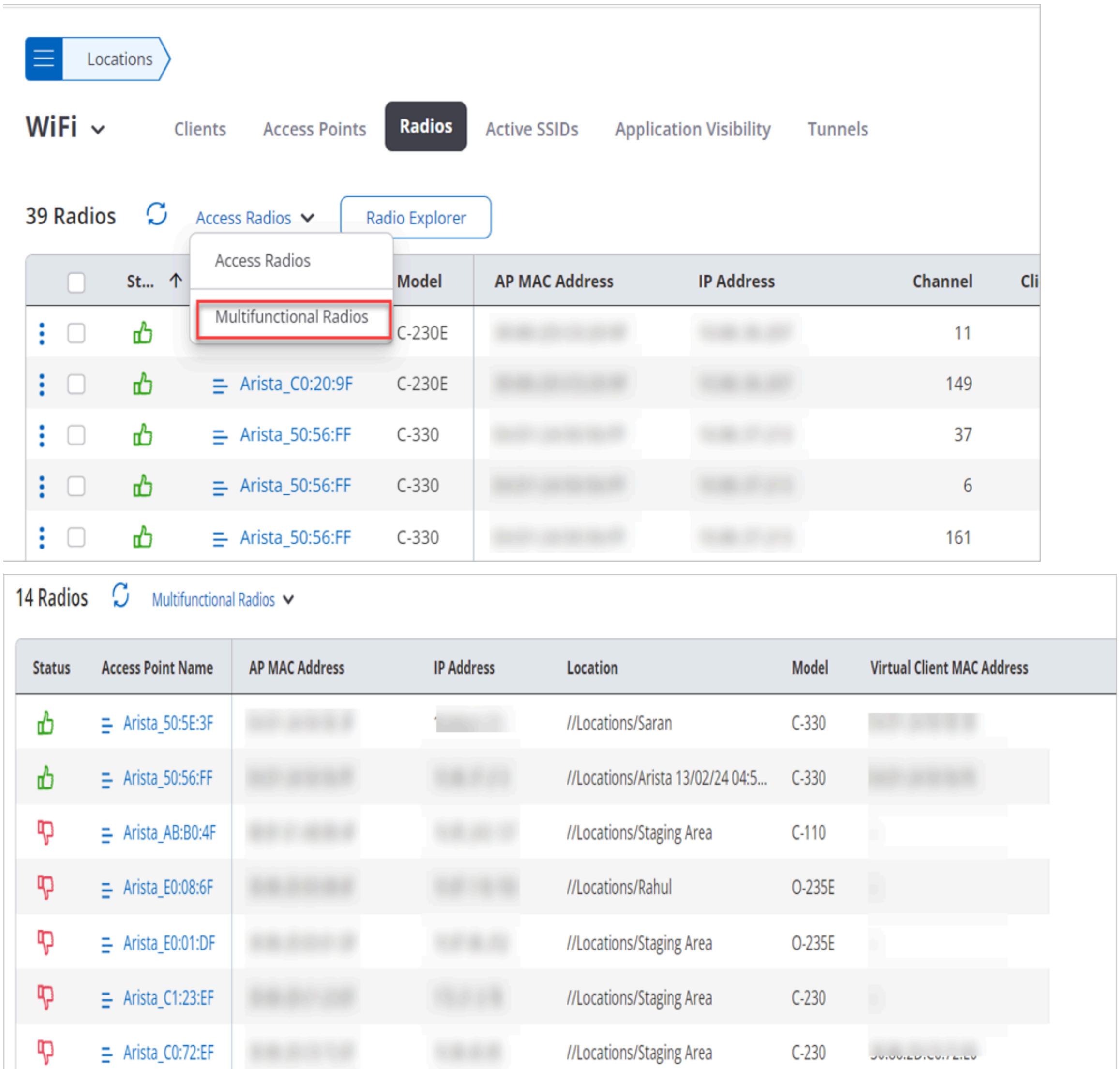
The Radios tab displays the following information about radios:

Field	Description
Status	Indicates whether the radio is on or off.
Access Point Name	Name of the AP.
Channel Width	Displays the width of the operating channel of the radio such as 80 MHz or 40 MHz.
MAC Address	Unique 48-bit address of the AP.
IP Address	Displays the IP address.
Device Template	Indicates the device template applied to the device.
Channel	Displays the Channel number on which the AP radio operates.
Clients	Displays the number of clients connected to the radio.
Tx. Power(dBm)	Indicates the transmission power.
Frequency	Indicates the frequency on which radio is operating.
RF Utilization (%)	Indicates the percentage of transmit and receive time on the radio.
Upstream Usage	Indicates upstream data usage.
Downstream Usage	Indicates downstream data usage.
Worst Client RSSI (dBm)	Displays the worst client signal strength.
Retry Rate (%)	Indicates the re-transmission rate in percentage.
Location	Displays the radio location.
Model	Displays the name of the device model.
Noise Floor (dBm)	Indicates the measure of the signal created from the sum of all the noise sources and unwanted signals within a measurement system.
Channel Width	Shows the width of the operating channel of the radio.
Radio MAC Address	Displays the MAC Address of the radio.

Multifunctional Radios

Multifunctional radios are radios present on Arista APs that do not broadcast SSIDS. Multifunctional radios can be used to perform actions such as Client Connectivity Tests (CCT), Packet Capture, Spectrum Analysis, etc.

To view Multifunction Radios, click **Multifunction Radios** from the Radios view drop-down menu.



The Multifunctional Radio grid displays the following information:

Table 3:

Field	Description
Status	Indicates whether the radio is on or off.
Access Point Name	Name of the AP on which the radio is present.
IP Address	Displays the IP address of the AP on which radio is present.
Location	Displays the location of the AP on which the radio is present.
Model	Displays the AP model of the connected radio.
Virtual Client MAC Address	Virtual MAC Address used by the radio to connect as a client to another AP while performing Client Connectivity Test.

9.4.1 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 Wi-Fi 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 Wi-Fi 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.

9.4.2 Freeze and Unfreeze Transmit Power Control and Auto-Channel Selection

You can freeze the channel and transmit power in the Auto mode to operate a specific radio at a specific channel number and transmit power. You can perform this action per radio. To switch to other channels, unfreeze the settings and make your own channel and power selection, or enable the Auto mode to select the optimum channel and transmit power.

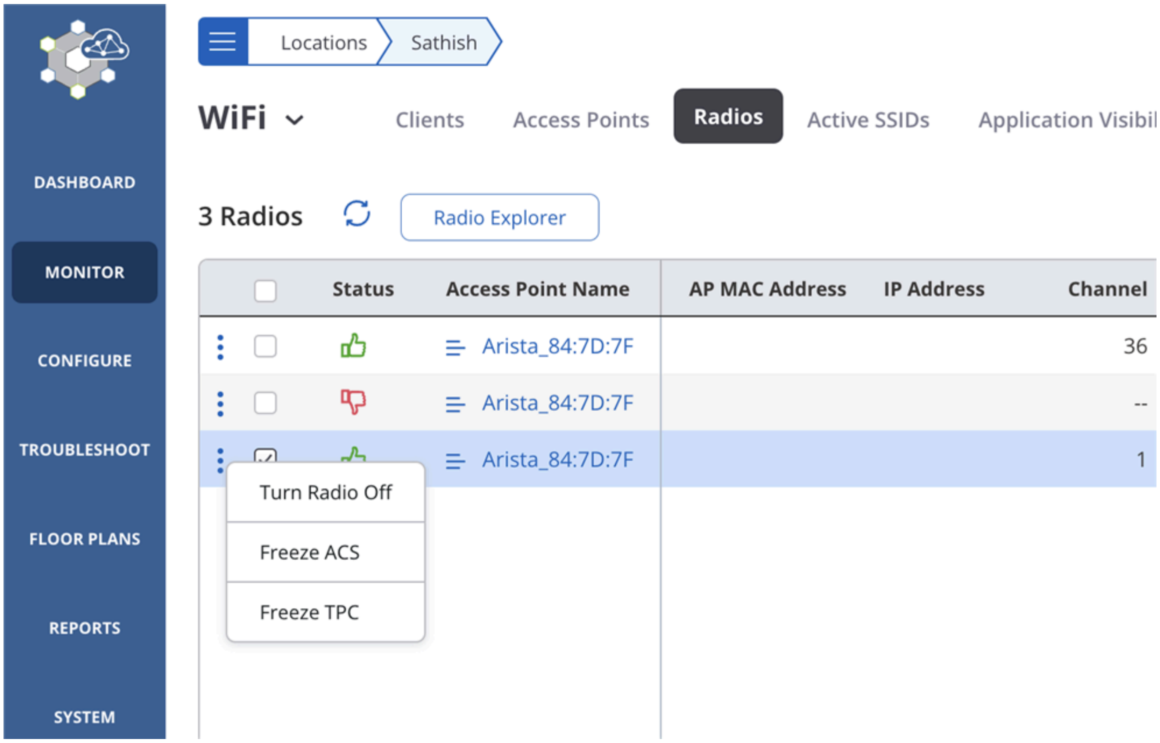
Note: You can freeze and unfreeze ACS and TPC only when you have enabled the Auto option. Both these options won’t work with the Manual mode.

Use Case

When you customize the Transmit Power and Channel Settings, and select the Auto mode, you let the access point decide and select the best channel and transmit power according to the current conditions. The AP reviews the channel and transmit power periodically and depending on the conditions, it may change the channel and power to best suit the existing conditions. For operational needs, you may want to freeze the channel and transmit power in the Auto mode. The Freeze ACS and Freeze TPC options let you easily achieve this result.

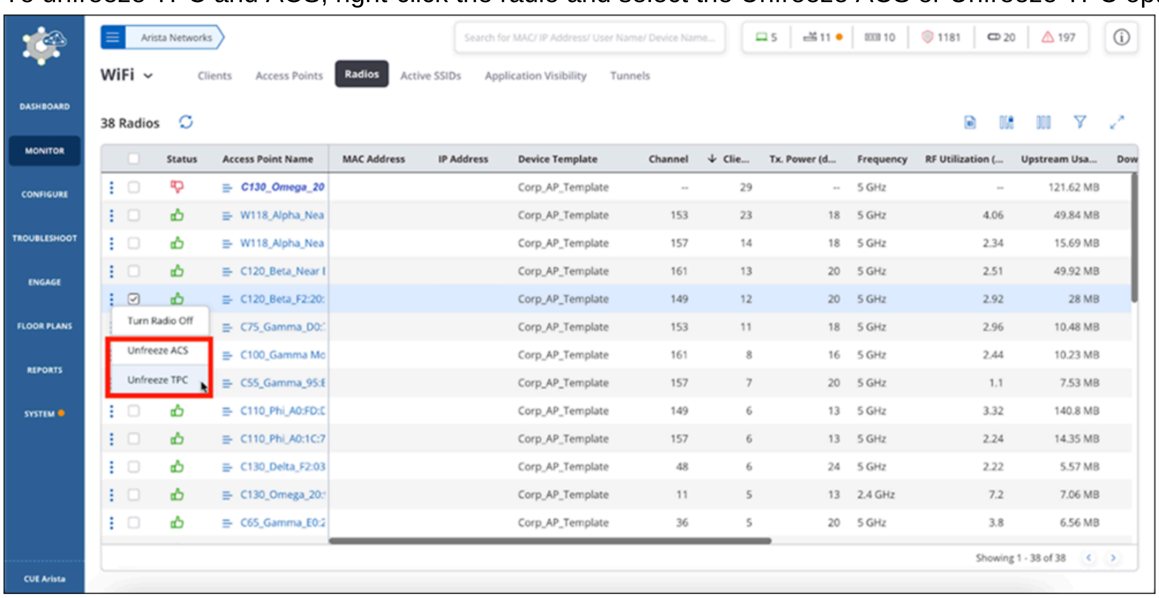
To Freeze or Unfreeze Transmit Power Control and Auto-Channel Selection:

1. Navigate to **MONITOR** > **WiFi** > **Radios**
2. Select the radio of the access point and click the three-dot menu to open the context menu.

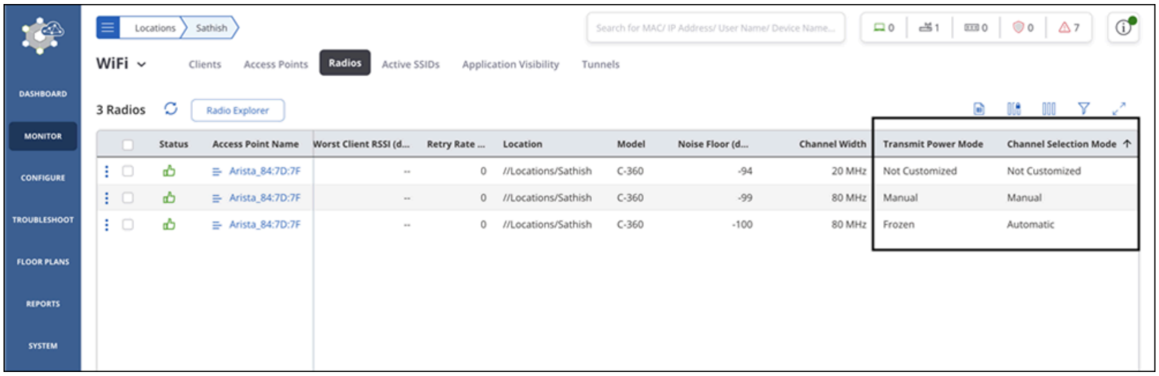


3. Select **Freeze ACS** or **Freeze TPC.**
4. Click Confirm in the confirmation dialog box.

To unfreeze TPC and ACS, right-click the radio and select the Unfreeze ACS or Unfreeze TPC options.



To verify whether the access points have the channels and transmit power frozen, go to the **MONITOR** > **WiFi** > **Radios**page and check the status on the Transmit Power Mode column.



9.4.3 On-Demand Transmit Power Control and Auto-Channel Selection

You can trigger the Auto-Channel Selection (ACS) Mode and Transmit Power Control (TPC) Mode for a radio on demand. In ACS Mode, the Access Point (AP) scans the network to select the best channel. In Auto-TPC Mode, the AP automatically adjusts its transmit power to minimize interference with neighboring Arista APs.

You can trigger ACS and TPC only when you have enabled the **Auto** option. Both these options do not work in the Manual mode.

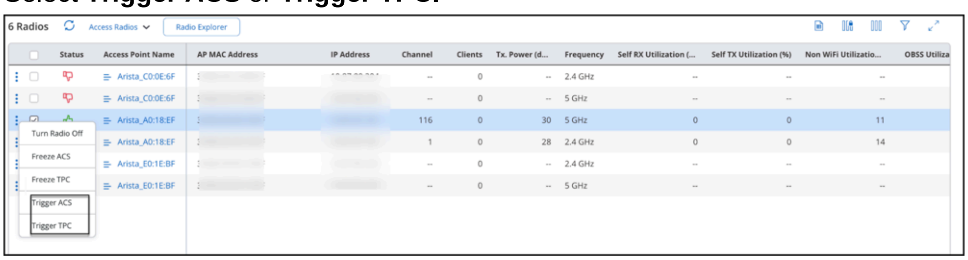
Note: Trigger ACS and Trigger TPC work even if ACS or TPC is in freeze mode.

Use Case

When you customize the Transmit Power and Channel Settings, and select the Auto mode, the access point decides and selects the best channel and transmit power according to the current conditions. When you are facing high interference in your network, Triggering ACS and TPC allows the AP to review the channel and transmit power and change the channel and power to best suit the existing network conditions. Network administrators can use this functionality to switch to the best conditions without changing network configurations.

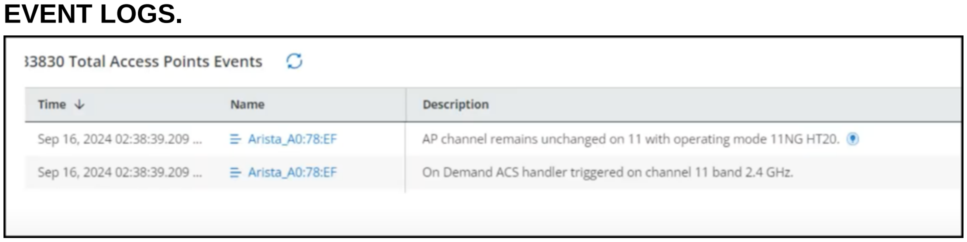
To Trigger ACS or TPC:

1. Navigate to **MONITOR** > **WiFi** > **Radios**
2. Select the radio of the access point and click the three-dot menu to open the context menu.
3. Select **Trigger ACS** or **Trigger TPC.**



4. Click **Confirm** in the confirmation dialog box.

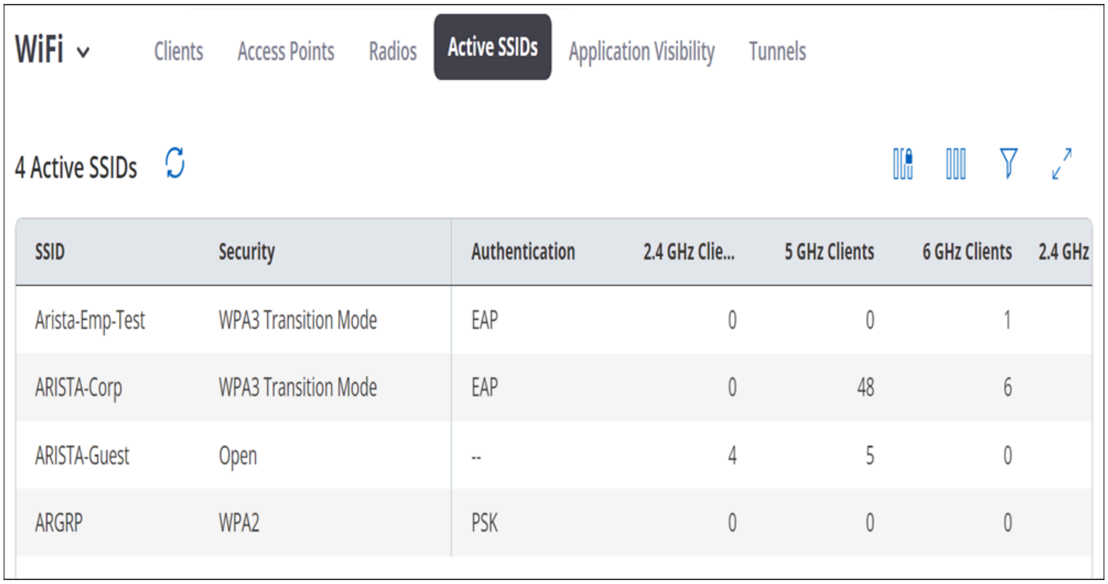
To verify whether the access points have the ACS and TPC triggered, go to **TROUBLESHOOT > EVENT LOGS.**



9.5 Active SSIDs

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

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



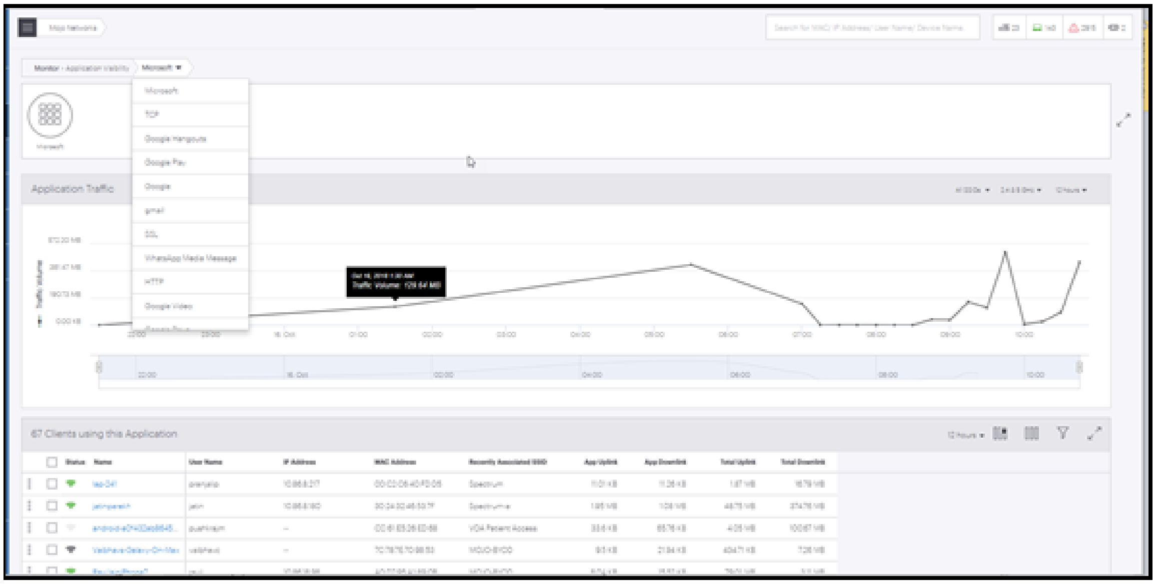
The Active SSIDs page displays the following information:

Field	Description
SSID	Name of the SSID profile.
Security	The mode of security used.
Authentication	The authentication method used.
2.4Ghz Clients	The number of clients connected on the 2.4 GHz frequency.
5 GHz Clients	The number of clients connected on the 5 GHz frequency.
6 GHz Clients	The number of clients connected on the 6 GHz frequency.
2.4 GHz Radios	The number of 2.4 GHz radios on which the SSID is being broadcasted.
5 GHz Radios	The number of 5 GHz radios on which the SSID is being broadcasted.
6 GHz Radios	The number of 6 GHz radios on which the SSID is being broadcasted.
Uplink Data	The uplink data usage.
Downlink Data	The downlink data usage.

9.6 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:

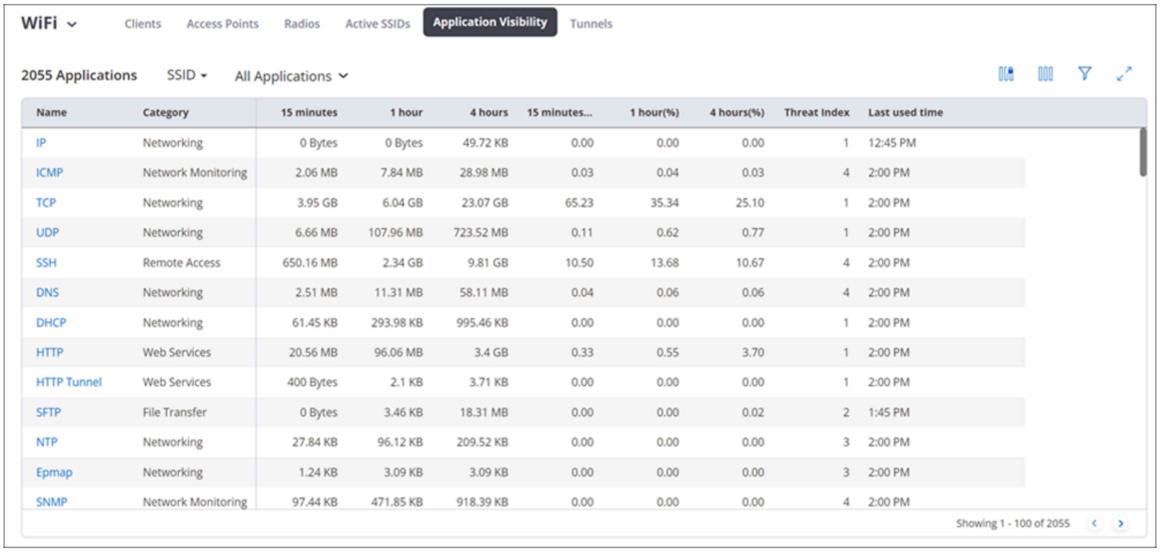
- Baseline - Clients Affected
- Baseline - % Poor Application Experience
- Application Traffic: It displays the usage of data of the selected application, over a period of time. Refer Application Traffic section for more information.
- Application Traffic - Clients
- Application Traffic - Sessions
- 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.

9.6.1 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** > **WiFi** > **Application Visibility.**



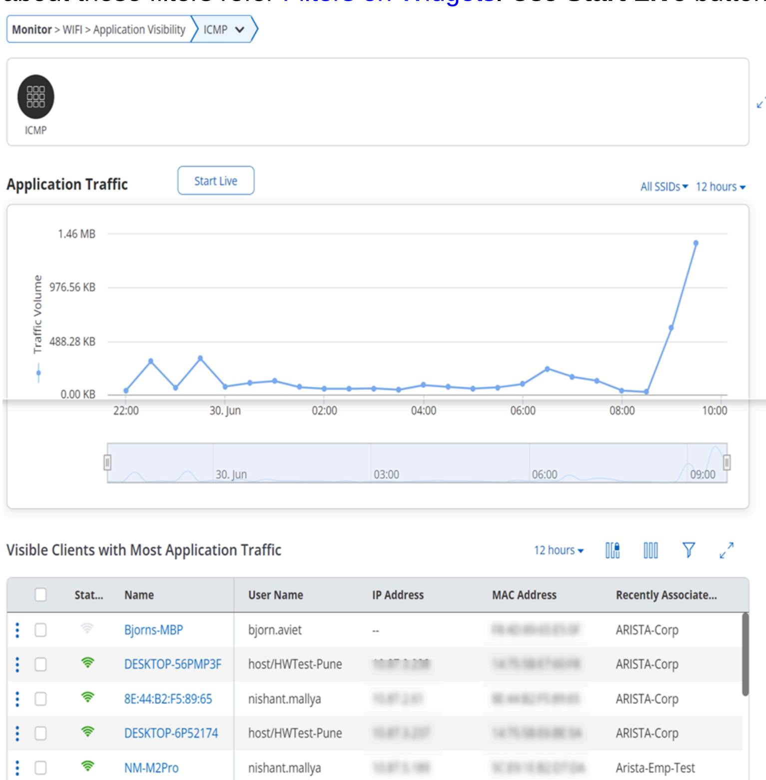
Name	Category	15 minutes	1 hour	4 hours	15 minutes...	1 hour(%)	4 hours(%)	Threat Index	Last used time
IP	Networking	0 Bytes	0 Bytes	49.72 KB	0.00	0.00	0.00	1	12:45 PM
ICMP	Network Monitoring	2.06 MB	7.84 MB	28.98 MB	0.03	0.04	0.03	4	2:00 PM
TCP	Networking	3.95 GB	6.04 GB	23.07 GB	65.23	35.34	25.10	1	2:00 PM
UDP	Networking	6.66 MB	107.96 MB	723.52 MB	0.11	0.62	0.77	1	2:00 PM
SSH	Remote Access	650.16 MB	2.34 GB	9.81 GB	10.50	13.68	10.67	4	2:00 PM
DNS	Networking	2.51 MB	11.31 MB	58.11 MB	0.04	0.06	0.06	4	2:00 PM
DHCP	Networking	61.45 KB	293.98 KB	995.46 KB	0.00	0.00	0.00	1	2:00 PM
HTTP	Web Services	20.56 MB	96.06 MB	3.4 GB	0.33	0.55	3.70	1	2:00 PM
HTTP Tunnel	Web Services	400 Bytes	2.1 KB	3.71 KB	0.00	0.00	0.00	1	2:00 PM
SFTP	File Transfer	0 Bytes	3.46 KB	18.31 MB	0.00	0.00	0.02	2	1:45 PM
NTP	Networking	27.84 KB	96.12 KB	209.52 KB	0.00	0.00	0.00	3	2:00 PM
Epmap	Networking	1.24 KB	3.09 KB	3.09 KB	0.00	0.00	0.00	3	2:00 PM
SNMP	Network Monitoring	97.44 KB	471.85 KB	918.39 KB	0.00	0.00	0.00	4	2:00 PM

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 to Clients with Most Application Traffic for more details.
   - Application Data Usage Over Time. Refer to Application Traffic for more information.

9.7 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.



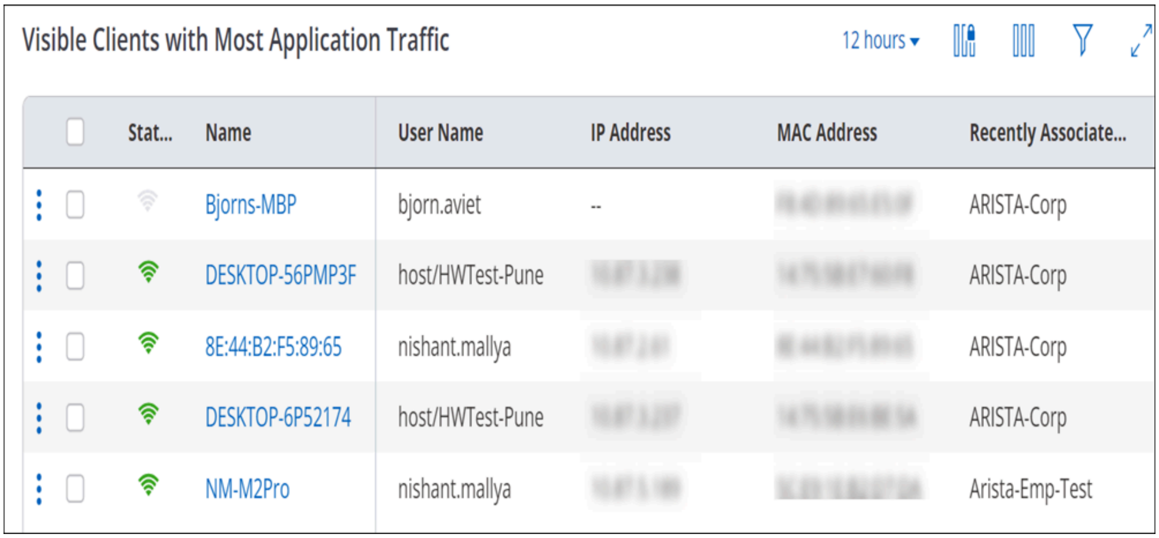
The graph is plotted at a time interval of 15 minutes. If its live data it is plotted every 3 seconds. If you hover the mouse over the graph, you can get a quick view of the timestamp and the data consumption by the selected application, at the given time.

9.7.1 Visible Clients with Most Application Traffic

The **Visible Clients with Most Application Traffic** widget displays a list of the visible 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.



9.8 Automated Root Cause Analysis

CV-CUE eliminates the need to manually troubleshoot some commonly occuring network issues. Its powerful Root Cause Analysis (RCA) engine identifies the root causes of network issues for a single client or total clients, and recommends solutions to those problems.

The RCA 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.

The RCA 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 does not support the latest 2.4 GHz, 5 GHz, or 6 GHz protocol

- Band Issues such as client does not 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 RCA 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 Wi-Fi configuration settings that might have caused the issue. For example: is transmit power set to "Auto"?, is Dynamic Channel Selection enabled?

Note: The RCA 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.

9.8.1 Root Cause Analysis for a Single Client Vs Total Clients

CV-CUE performs root cause analysis on single clients as well as on the total number of clients facing problems.

For single clients, you do not have to run the Inference Engine. You can view the recommendations from **MONITOR** > **WiFi** > **Clients** .

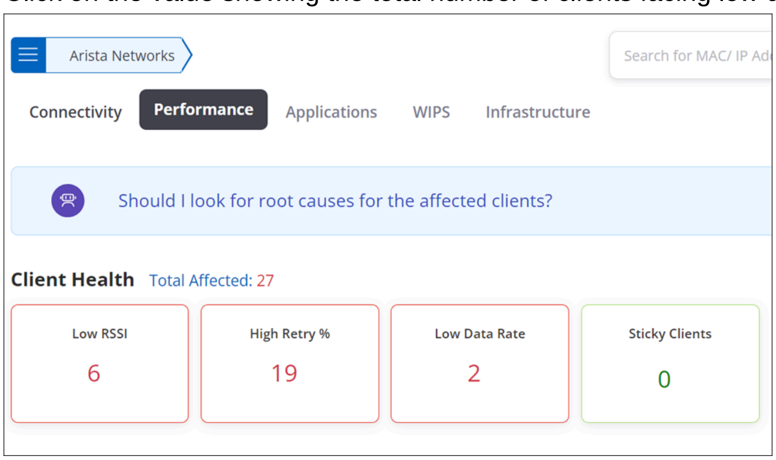
For total clients, you have to run the Inference Engine in the Client Health widget and the root cause analysis runs based on the locations. You run it from **Dashboard** > **Performance** > **Client Health** > **Total Affected.**

9.8.2 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:

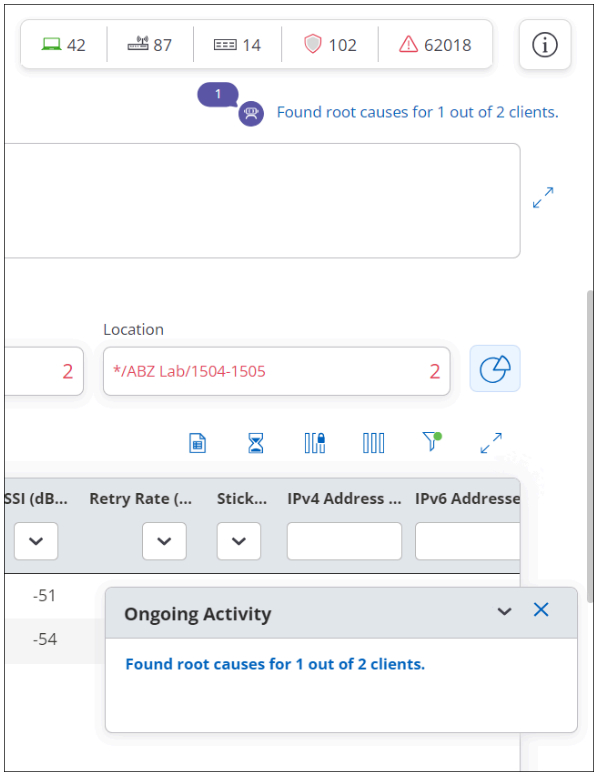
1. Go to **DASHBOARD** > **Performance** > **Client Health.**
2. Select a parameter (Low RSSI,Low Data Rate, High Retry) that you want to analyze. For example, let us consider "Low Data Rate".
3. Click on the value showing the total number of clients facing low data rate.



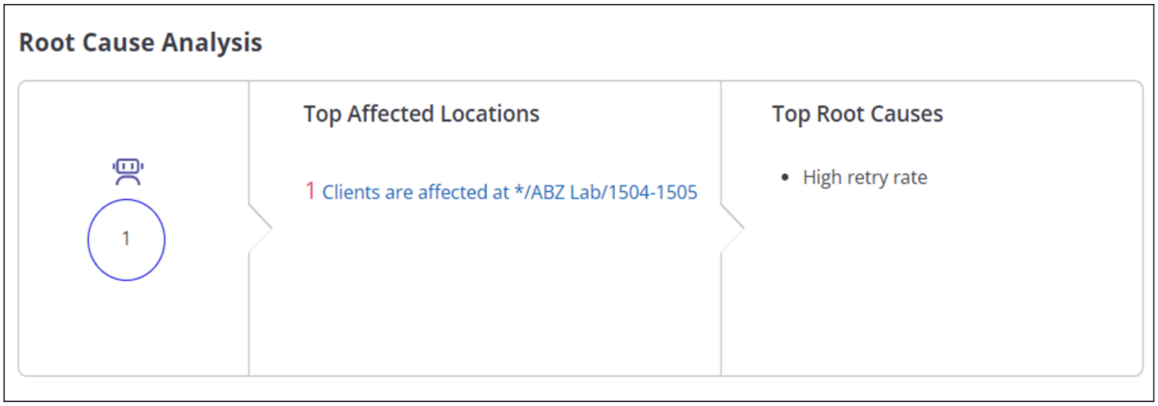
4. Click **Should I look for root causes?** This will start the root cause analysis in the background. You can continue navigating to other parts of CV-CUE while it is generating the intelligent view.

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."

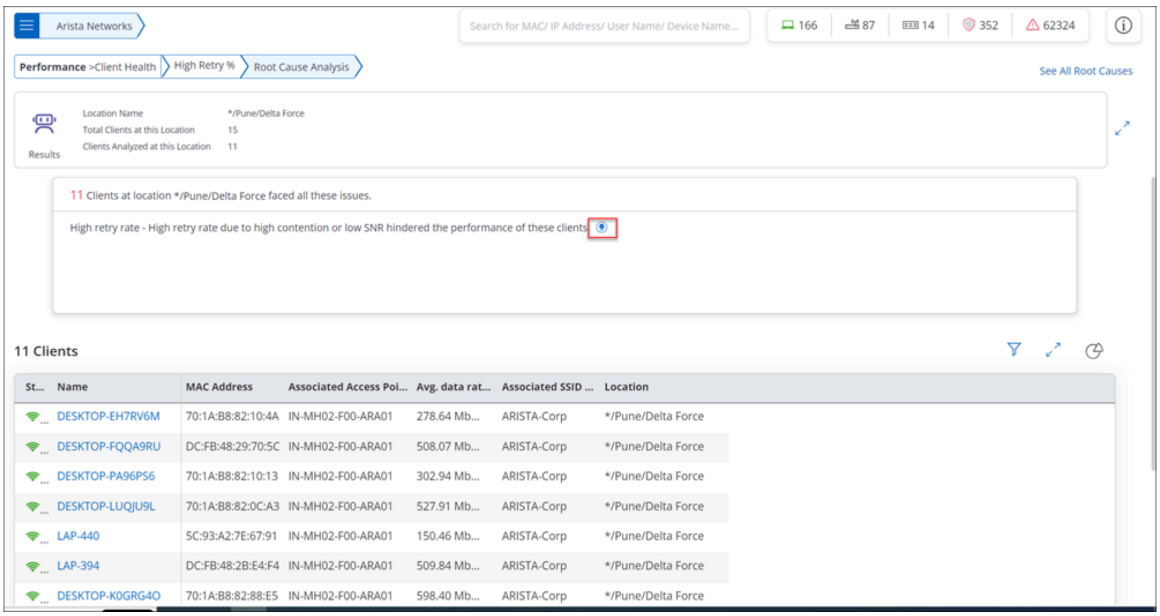
5. Click **Should I look for root causes?** Or click on the link in the **Outgoing Activity**message box to view the result of the root cause analysis.



The RCA Engine displays the results of the analysis at one glance.



6. Click a location to view the list of affected clients.
7. To view recommendations, click the bulb icon next to the root cause.



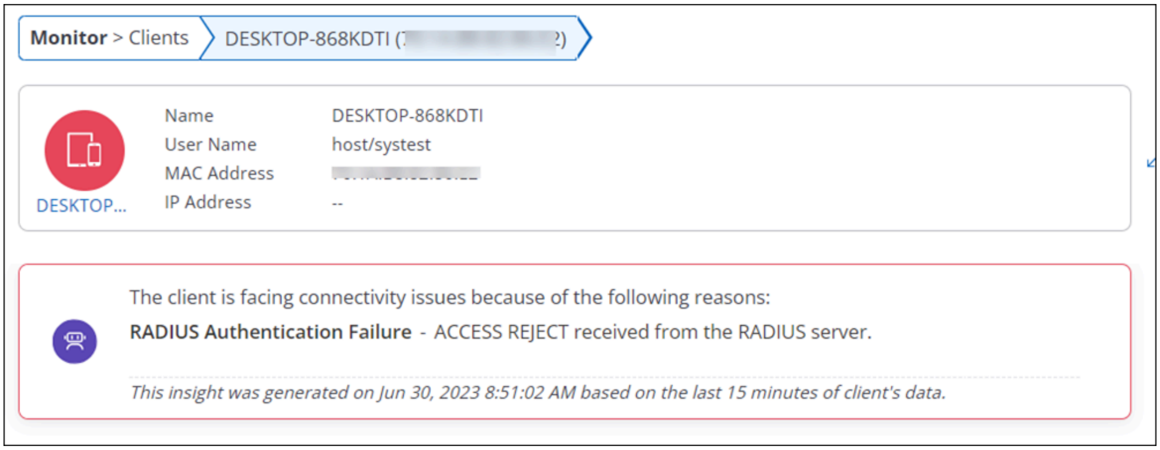
8. To go back to the normal view, first close the recommendation panel.

9.8.3 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.

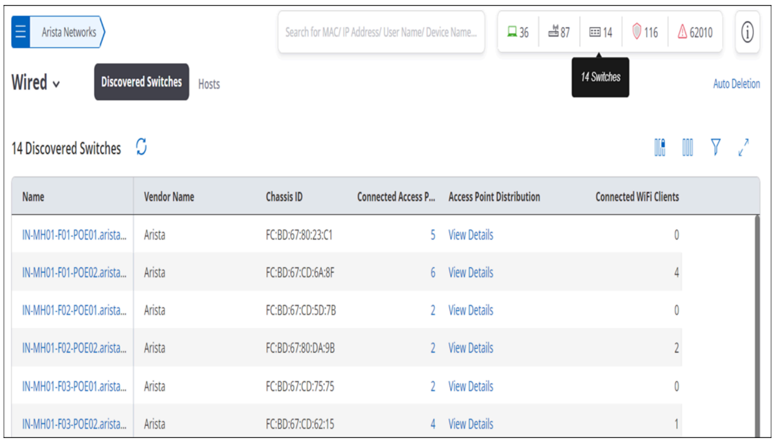
Chapter 10

Monitor Wired Devices

You can access the switch listing page from **MONITOR** > **Wired**.

The Wired page displays the list of discovered switches, managed switches, and hosts. There is no separate configuration needed to display the list of switches. APs collect and analyze the Link Layer Discovery Protocol (LLDP) packets to obtain switch information. The data is then displayed on the UI.

You can also view the switch information from the global counter. The switch counter shows the number of active switches, inactive switches, and discovered switches depending on the selected location. For a parent location, the counter would show the total count of active switches available in the parent and its child location.



Note: This is a Beta feature.

This chapter contains the following topics:

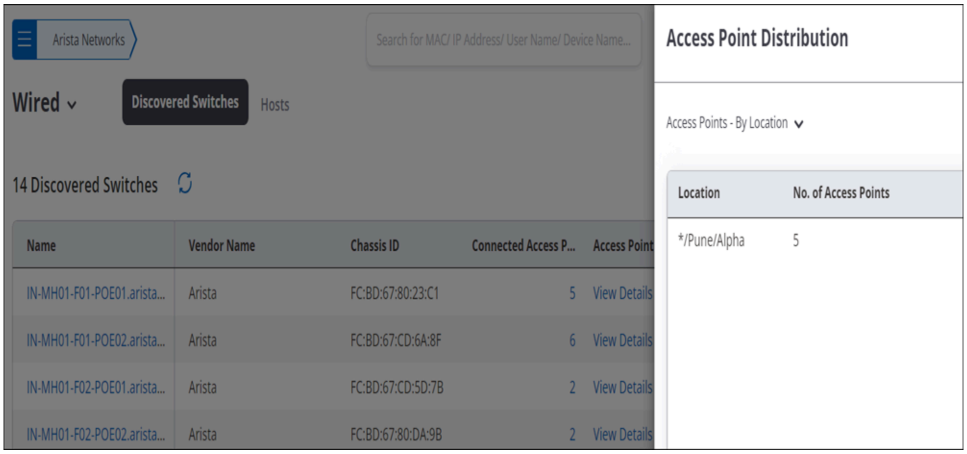
- Discovered Switches
- Managed Switches
- Hosts
- Onboard Switches
- Configure Switches
- VXLAN Endpoints

10.1 Discovered Switches

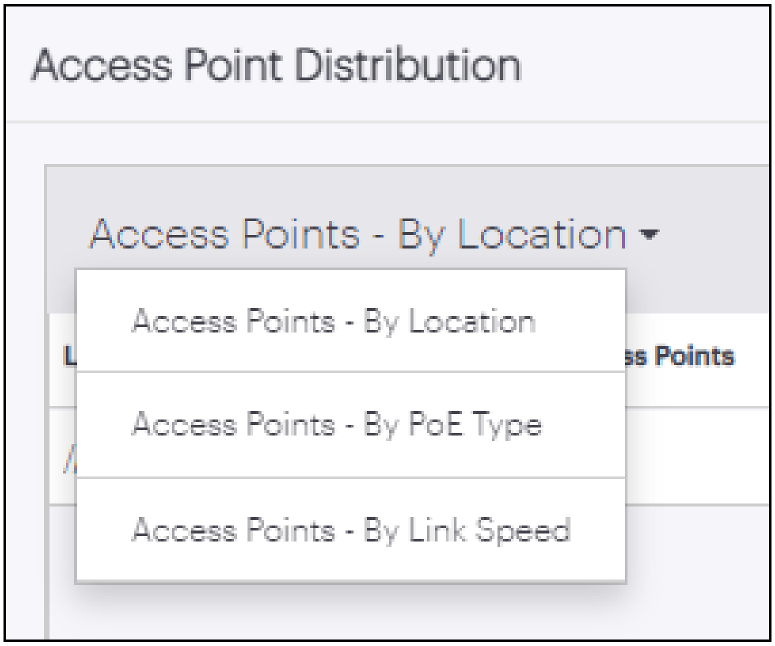
Discovered Switches are switches discovered by Arista's Managed APs.

The Discovered Switch listing page displays the vendor name, number of APs managed by that switch, the AP distribution, and the number of connected WiFi clients. The Access Point Distribution column has a link to view all the APs connected to the switch. Since the APs are tied to the location hierarchy, if you do not have access to a particular location, you may not see the APs managed by the switch.

The following image shows the AP distribution in the right panel on clicking the View Details link:



In the AP Distribution view, you can filter the APs by location, PoE type, or link speed.



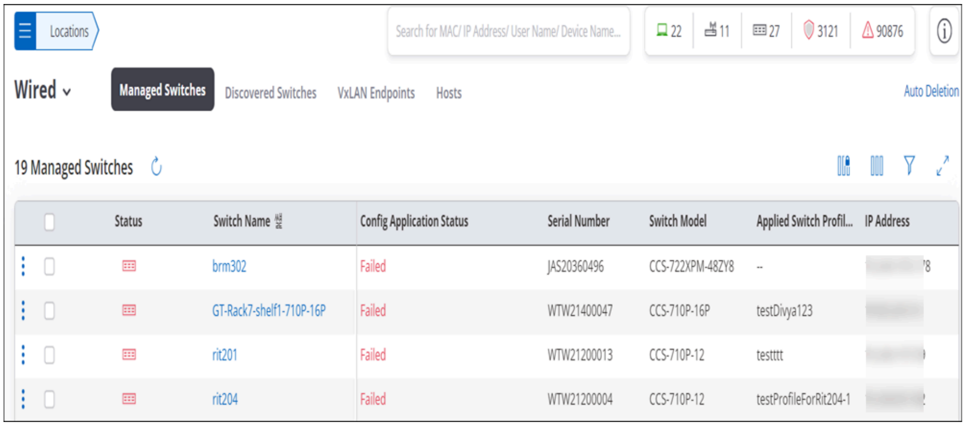
- The categories for PoE Type are PoE, PoE+, andPoE++.
- The categories for link speed are 10Gbps, 5Gbps, 2.5Gbps, 1Gbps, 100Mbps, and 10Mbps.

10.2 Managed Switches

The Managed Switches listing shows all the managed switches deployed in your network. You will see the Manged Switches tab if you have enabled CVaaS.

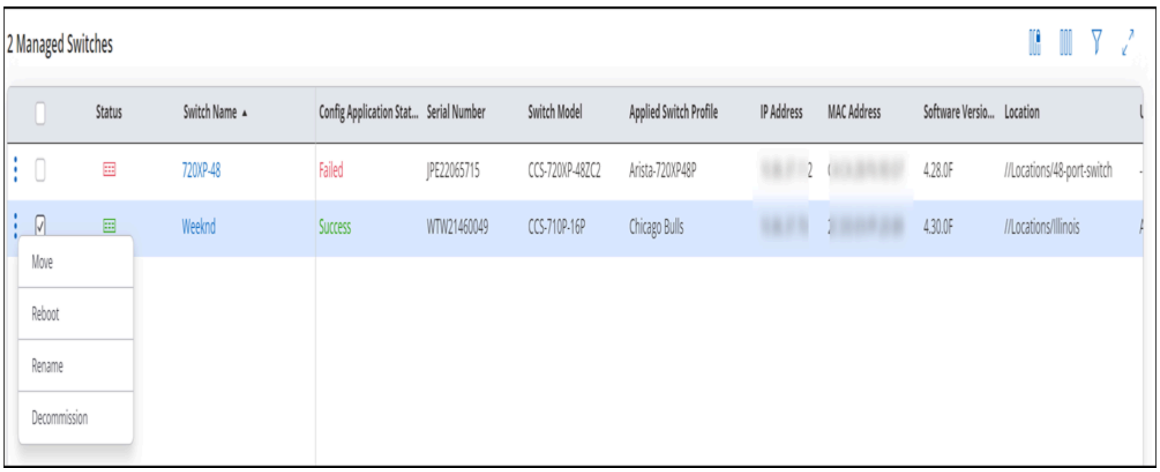
CV-CUE displays the switch details for the following switch models — 710P, 720XP, 720D, and 722XP. It contains information about the switch such as Software Version, MAC Address, Location, Status, Total Ports, Available Ports, Available PoE Power, etc.

Note: Managed Switches features are available for cloud deployments only. They are not available for on-premises deployments.



You can perform the following operations on Managed switches:

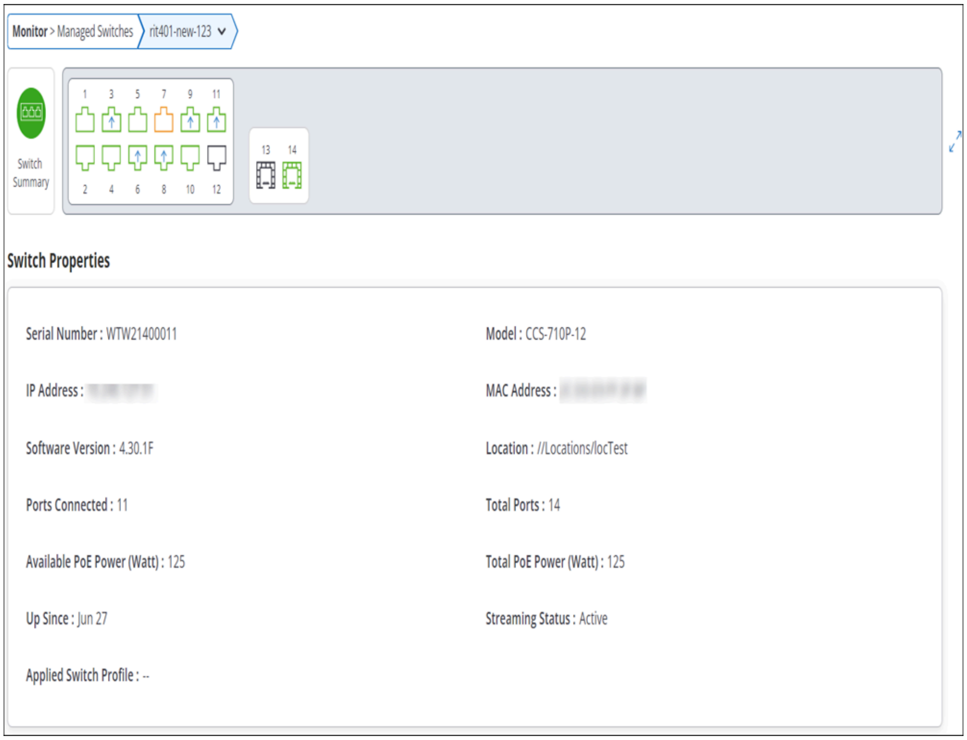
- **Move:** Move to switch to a different location.
- **Rename:** Rename the switch.
- **Decommission :** You can decommission a switch and remove it from CV-CUE. Once you decommission a switch, it is deleted from CV-CUE and you need to onboard the switch again.
- **Reboot:** Reboot the switch.



Switch Details

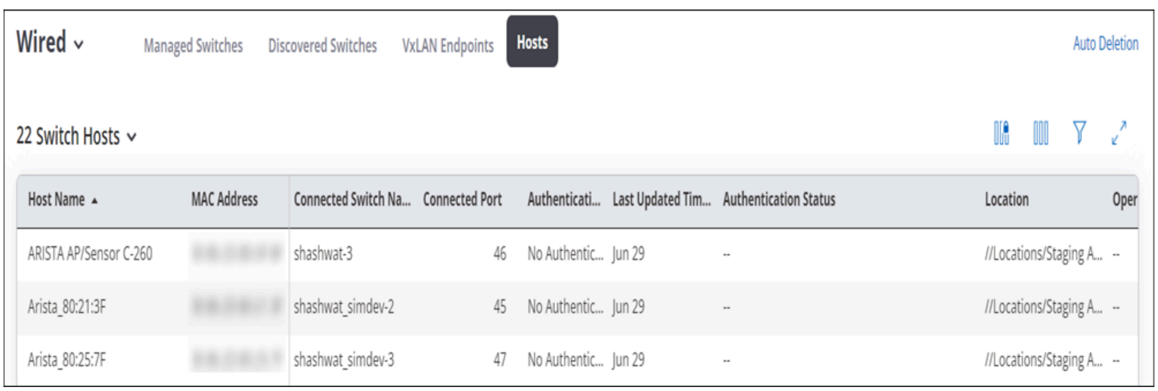
Click the switch name to view complete details of the switch. Switch details contain Switch Summary, Switch Properties and Switch Layout, Switch Topology. Hover over a port in the Switch layout to view its status. You can also click a particular port to view more details about the port. To go back to summary, click the Switch Summary icon.

The following image shows the switch details page:



10.3 Hosts

Host tabs contain information about devices connected to switches.



10.4 Onboard Switches

You can onboard switches manually or use Arista's Zero Touch Provisioning (ZTP) to onboard your switches to CV-CUE.

Onboarding Switches using ZTP

You can use ZTP to onboard a switch without user intervention. ZTP leverages the power of Arista's Extensible Operating System (EOS) to onboard switches.

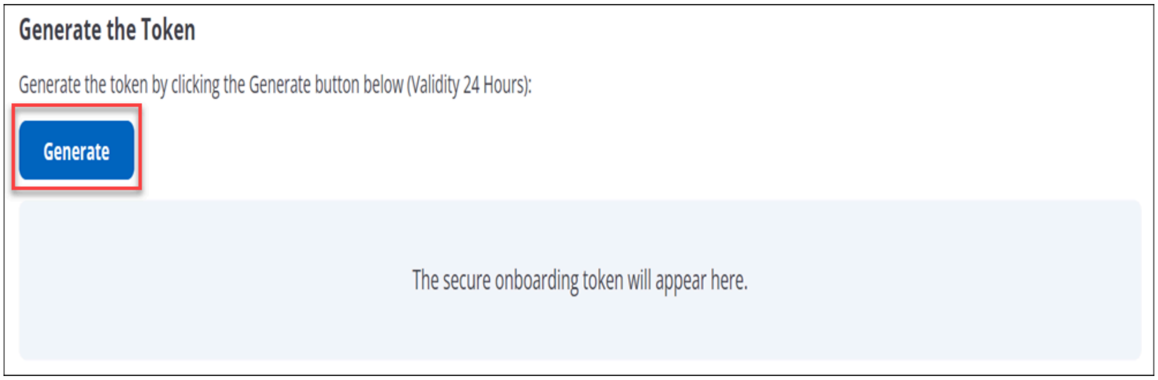
Prerequisites:

- **DHCP Server:** Switch should be able to reach arista.io by obtaining valid IP settings from a DHCP server.
- **EOS Version:** The device should be running EOS version 4.25.5 or 4.26.1 or newer.

You can enable ZTP using a custom bootstrap script and use a DHCP server option to point to that bootstrap script.

To enable ZTP using a bootstrap script:

1. Log in to the CV-CUE and generate a token from **System** > **Advanced Settings** > **Switch Onboarding** and click **Generate.**



2. Prepare a bootstrap script and host it on an HTTP server. You can get a sample script from https://github.com/aristanetworks/cloudvision-ztpaas-utils.
3. Provide the updated token information and other information in the bootstrap script.

```
############## USER INPUT #############
cvAddr = "www.cv-staging.corp.arista.io"
enrollment_token = "eyJhbGciOiJSUzI1Nixxx..."
############## USER INPUT #############
Note: If the device is behind a non-transparent proxy, use the following
 cvproxy option:
# Add proxy url if device is behind proxy server, leave it as an empty
 string otherwise
cvproxy = ""
Note: You can start an HTTP server using python (python3 -m http.server 8000
 &),
and host the bootstrap.py file, and then point the DHCP server to download
 from this server location.
```

4. Host the script on a TFTP server locally and direct the DHCP server to point to the bootstrap script via option-67/bootfile-name option:

```
For example:
subnet 10.10.1.1 netmask 255.255.255.0 {
range 10.10.1.1 10.10.1.253;
option domain-name "dev.aristanetworks.com";
option routers 10.10.1.250;
option domain-name-servers 10.10.1.5;
option ntp-servers time.google.com;
host leaf-1A {
hardware ethernet fc:bd:67:aa:22:33;
fixed-address 10.10.1.180;
option host-name "leaf-1A";
option bootfile-name "http://10.10.1.10:8000/bootstrap.py";
}
```

Note: Make sure the ntp-servers option is set in your DHCP configuration.

5. Boot up the switch into ZTP provisioning mode.

The onboarding process begins and the successfully onboarded switches are displayed under **Monitor** > **Wired** > **Managed Switches** tab.

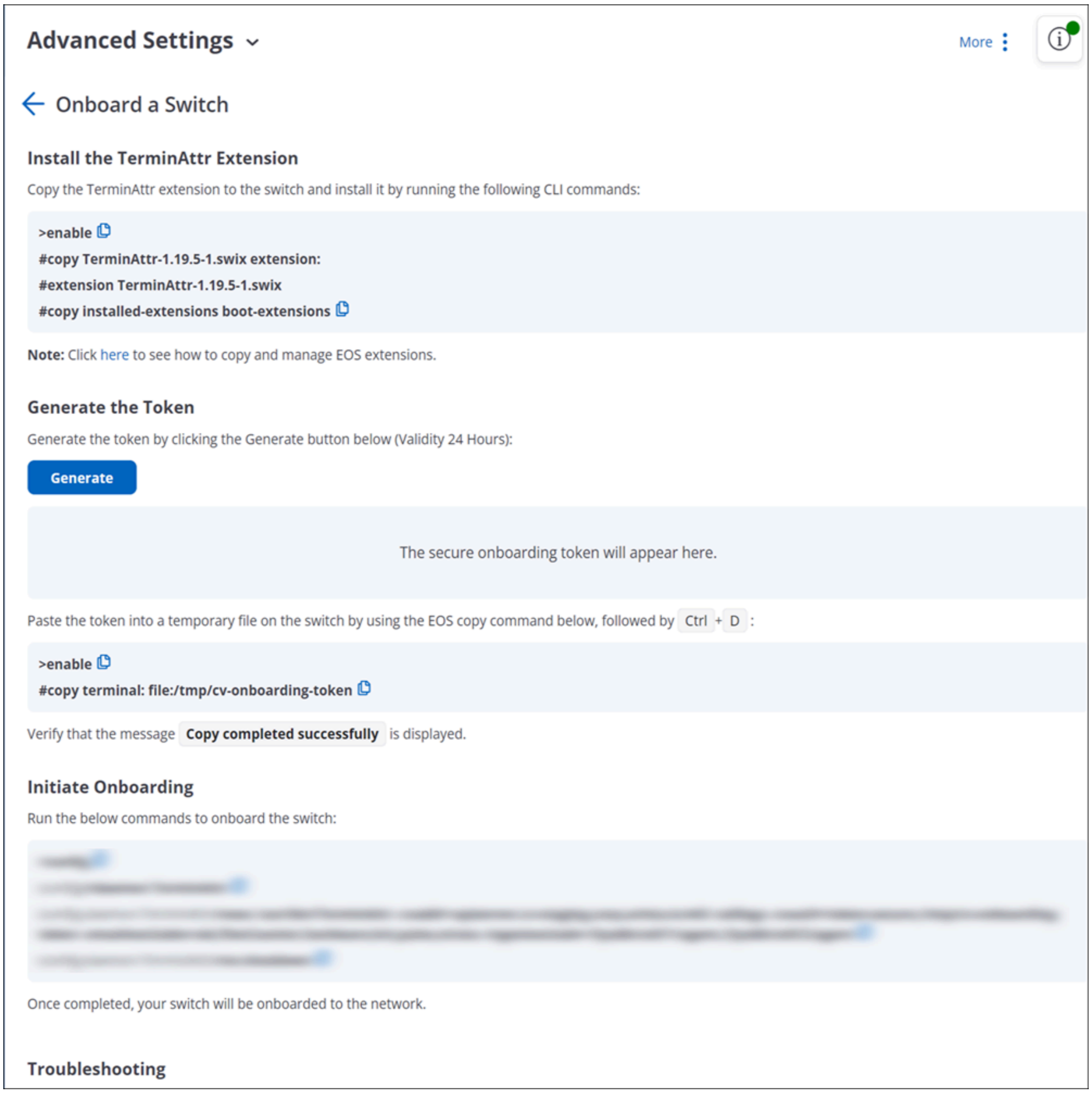
Note: You can use the same bootstrap script and token to onboard multiple switches. Ensure that the token has not expired before proceeding.

Onboarding Switches Manually

You can onboard switches manually to CV-CUE. The onboarded switches show up as Managed Switches in CV-CUE.

To onboard switches manually:

1. Go to **SYSTEM** > **Advanced Settings.**
2. Click **Switch Onboarding.**
3. Follow the instructions shown.



Note: You can use the same token to onboard multiple switches in one go.

Onboarded switches are available under **Monitor** > **Wired** > **Managed Switches** tab. All the managed switches when first identified are deployed in the staging environment.

10.5 Configure Switches

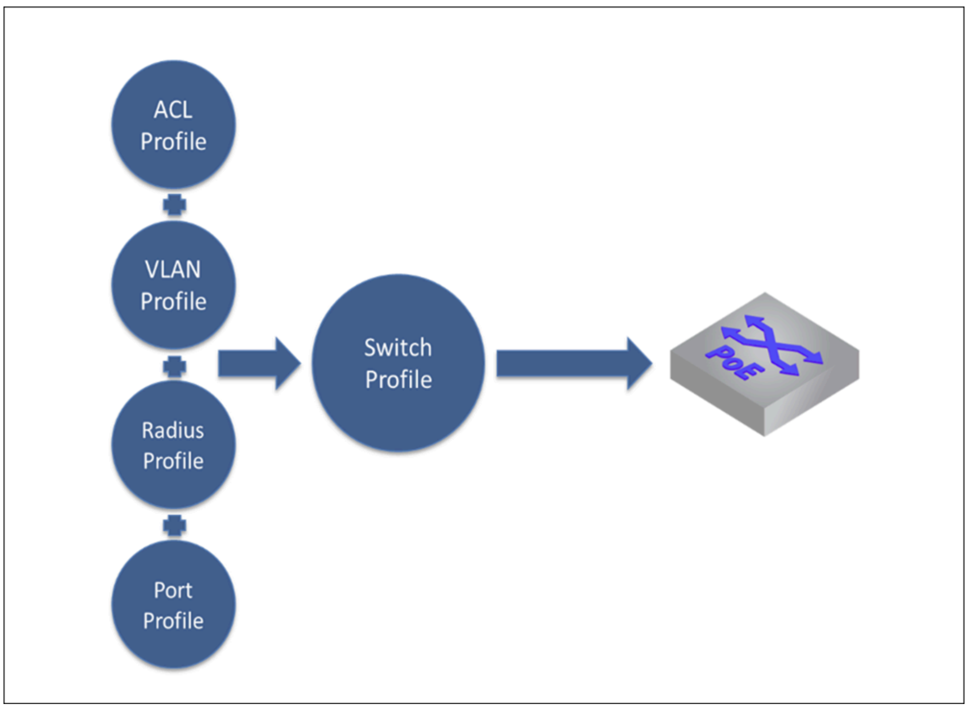
To configure an onboarded switch, perform the following steps:

1. Create Network Profiles
2. Create Switch Profiles
3. Apply Switch Profile to a Switch
4. Configure Device Settings

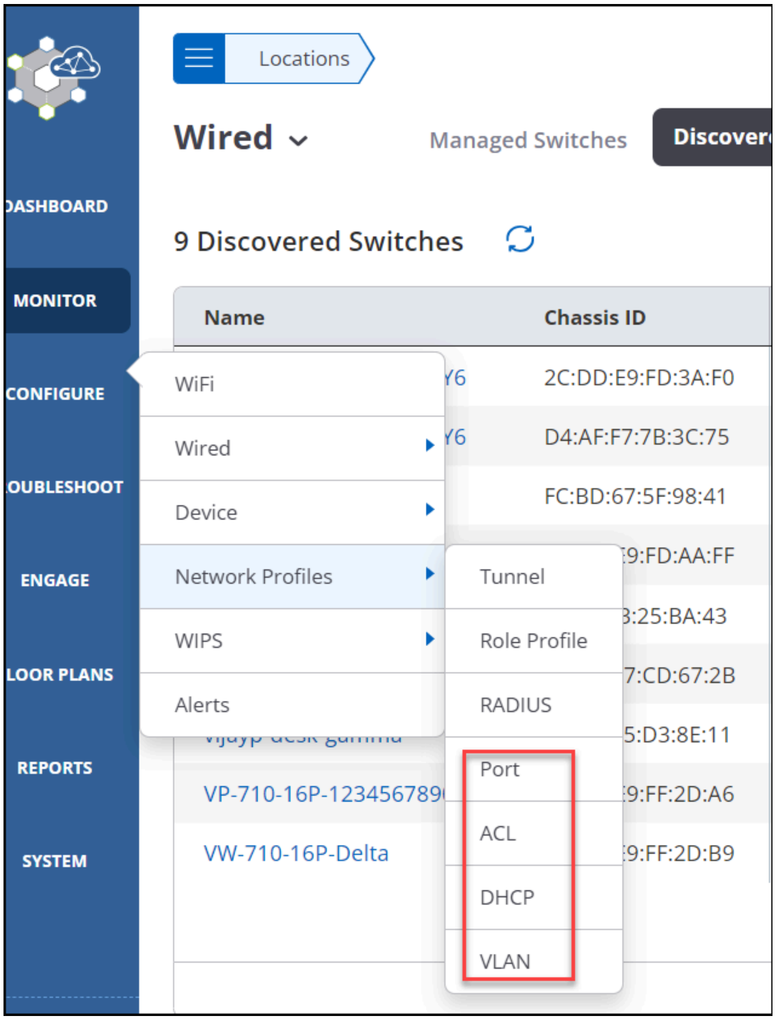
10.5.1 Create Network Profiles

To configure a switch, you need to create the following network profiles:

- Port Profile
- ACL Profile
- DHCP Profile
- VLAN Profile



You can create network profiles by navigating to **CONFIGURE** > **Network Profiles.**

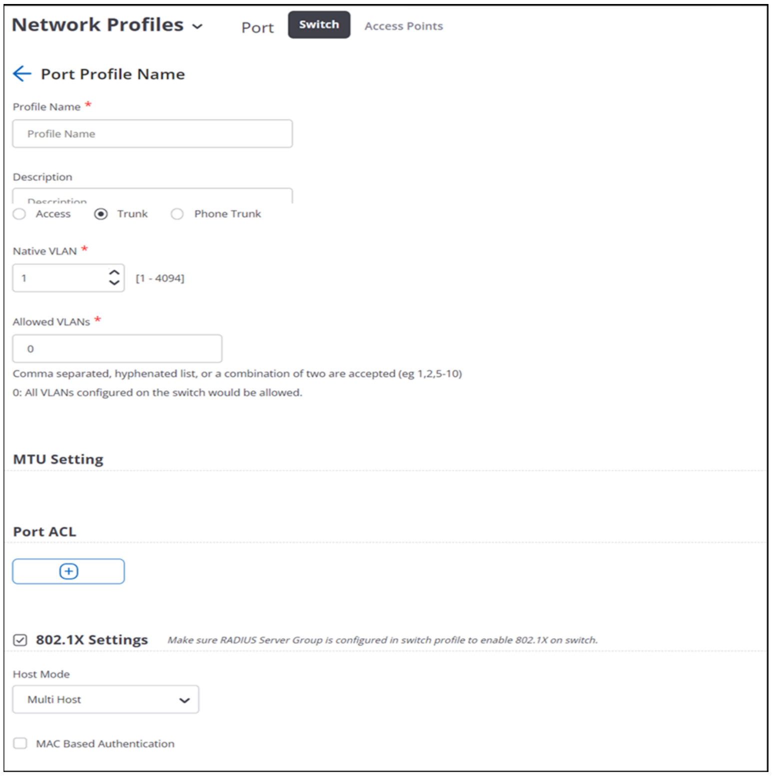


10.5.1.1 Port Profile

With Port Profile, you can configure all the settings of a switch port.

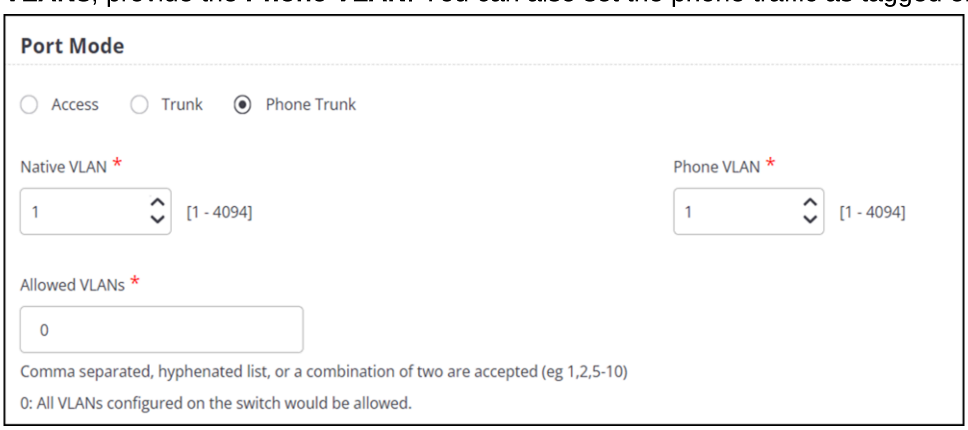
To create a Port Profile:

1. Go to **Configure** > **Network Profiles** > **Port.**
2. Click **Add Switch Port Profile.**



3. Provide the port profile name and description.
4. Select **Enable PoE** and select the power mode.
5. Select the **Port Mode.** You can select:

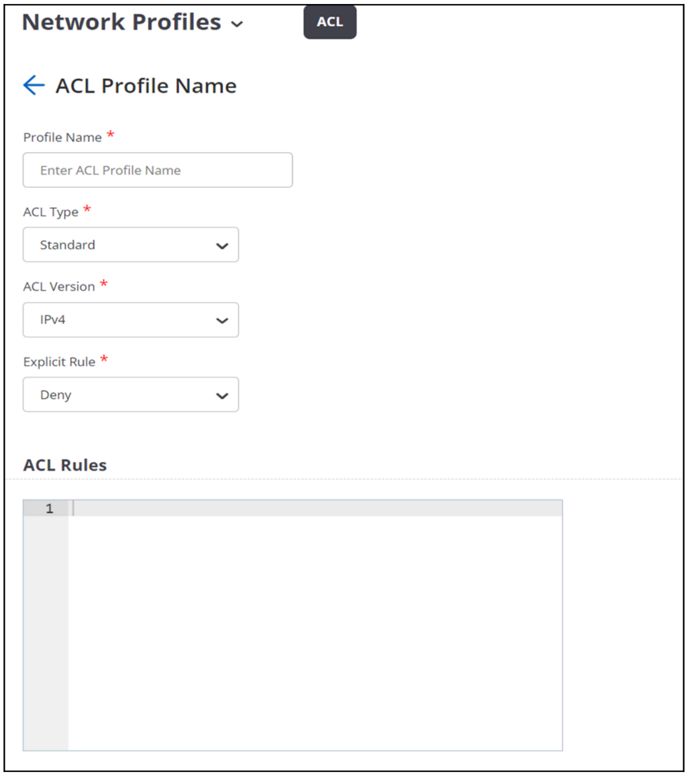
- **Access Mode:** Provide the access VLAN.
- **Trunk Mode:** Trunk mode allows you to connect multiple VLANs. Provide the **Native VLANs** and **Allowed VLANS.**
- **Phone Mode:** Phone mode allows you to connect a phone. Along with **Native VLAN** and **Allowed VLANs**, provide the **Phone VLAN**. You can also set the phone traffic as tagged or untagged.



6. Select the **MTU Settings.**
7. Enable **Port Security** to define the maximum number of MAC Addresses. You can also select the action to take if the MAC Addresses exceed the allowed value.
8. Click **Add Port ACL** to add and define ACL Profile for this port.
9. Select **802.1X Settings** to apply RADIUS Group Configuration to this port.
10. Click **Save.**

10.5.1.2 ACL Profile

Access Control List (ACL) Profile allows you to define rules that control the traffic flow to and from the switch.



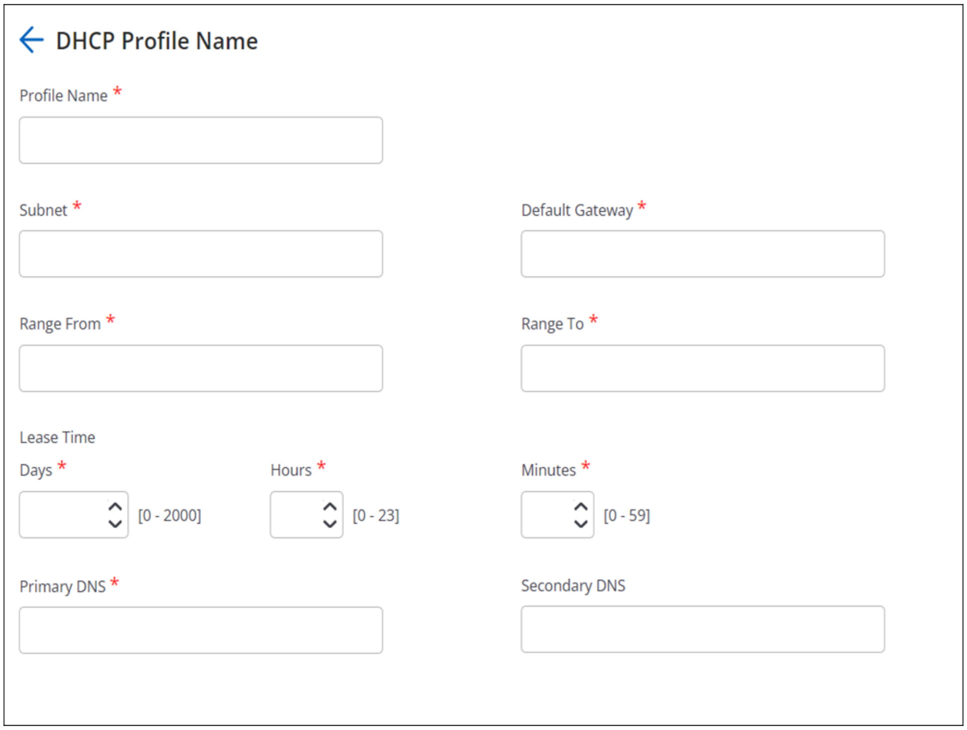
To create an ACL Profile:

1. Go to **CONFIGURE** > **Network Profiles** > **ACL.**
2. Click **Add ACL Profile.**
3. Select the **ACL Type:**
   - Standard
   - Extended: Along with the source and destination address, you can provide the protocol as well.
   - MAC
4. Select either **IPv4** or **IPv6** as **ACL Version**.
5. Select either **Permit** or **Deny** for the **Explicit Rule.** An explicit rule is applied if none of your defined ACL rules are applicable.
6. Provide the ACL Rules. For example, permit host 1.1.1.1

   You can also check the rule syntax.
7. Click **Save.**

10.5.1.3 DHCP Profile

With DHCP Profile, you can configure DHCP server for a particular VLAN on the switch.

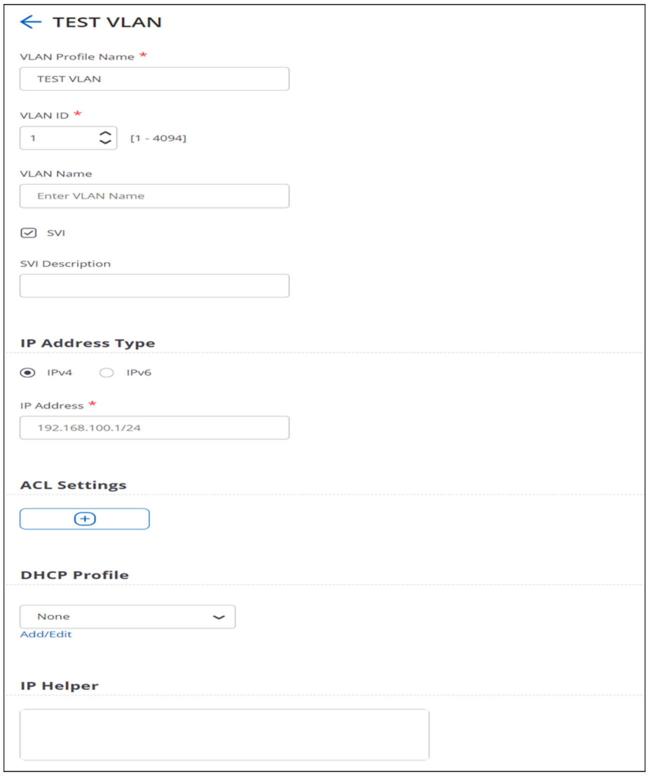


To create DHCP Profile:

1. Go to **CONFIGURE** > **Network Profiles** > **DHCP.**
2. Click **Add DHCP Profile.**
3. Provide the **Profile Name**, **Subnet,** and **Default Gateway** of the DHCP server. The IPv4 address for the subnet has to be in the CIDR notation. For example, 192.168.100.1/24.
4. Provide the **DHCP Range** and define the **Lease Time.**
5. Provide the **Primary DNS** and **Secondary DNS.**
6. Click **Save.**

10.5.1.4 VLAN Profile

With VLAN Profile, you can configure VLAN and virtual interface. One VLAN profile corresponds to one VLAN.



To create a VLAN Profile:

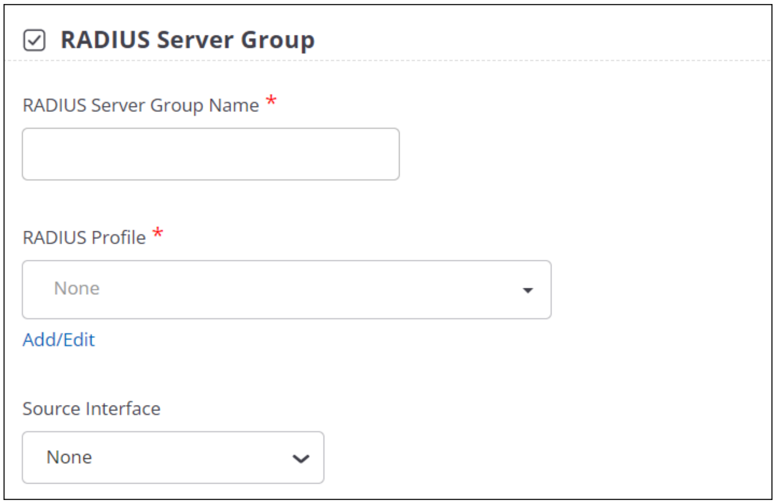
1. Go to **CONFIGURE** > **Network Profiles** > **VLAN.**
2. Click **Add VLAN Profile.**
3. Provide the **Profile Name**, **VLAN ID**, and **VLAN Name.**
4. Select **SVI** to enable the virtual interface.
5. Provide the following details for SVI:
   - IP Address Type
   - IP Address
   - IP Helper
   - ACL Profile
   - DHCP Profile
6. Click **Save.**

10.5.2 Create Switch Profiles

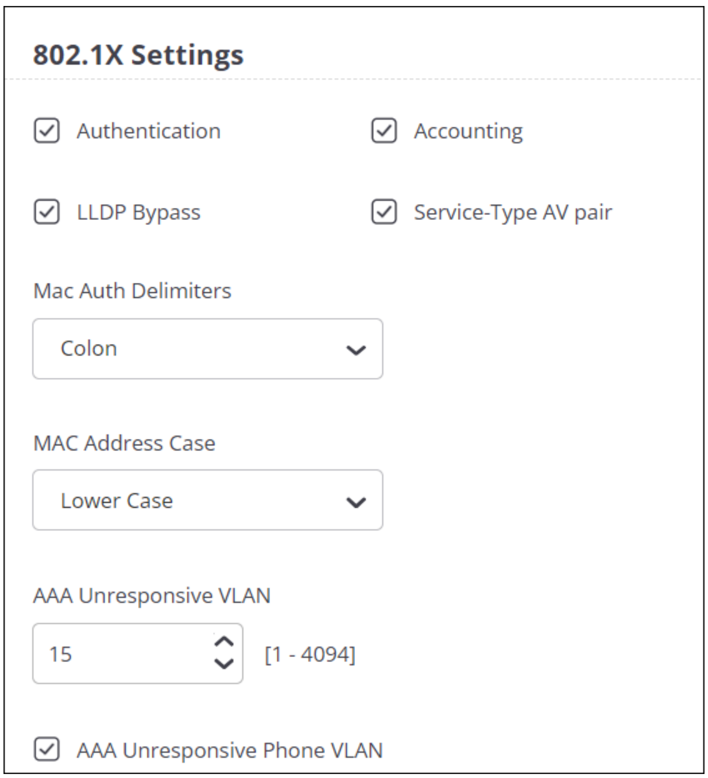
Switch profile consists of switch configuration, RADIUS server settings, mapping switch ports to port profile, and SNMP server details.

To create a switch profile:

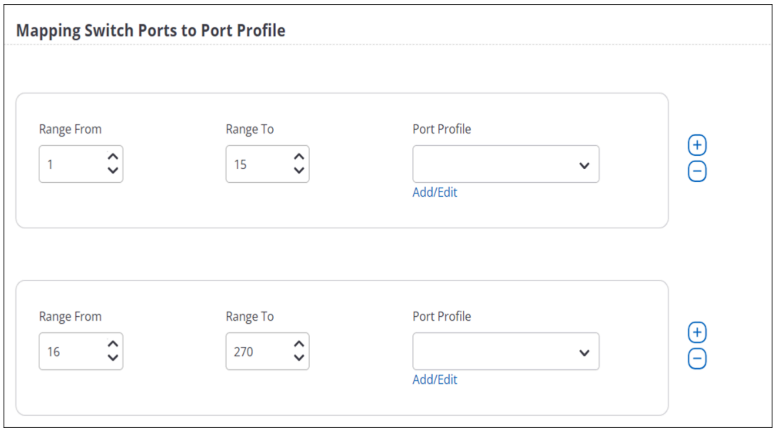
1. Navigate to **CONFIGURE** > **Wired** > **Switch Profiles**
2. Click **Add Switch Profile.**
3. Provide the switch name.
4. Select **Enable LLDP** and **Enable STP.**
5. Select the **VLAN Profile.**
6. Select **Enable RADIUS Server Group** to enable RADIUS server. Select the source interface to use to communicate with the RADIUS server and provide the interface number.



7. Specify the 802.1X Settings. You can also specify the **Unresposnvie VLAN** to use if the RADIUS server is unresponsive.



8. Select the **ACL Profile.**
9. Select **Enable IGMP Snooping** and select the **IGMP version.**
10. Provide **Static Route Configuration.** Static routes are typically used when dynamic protocols are unable to establish routes to a specified destination prefix. Static routes are also useful when dynamic routing protocols are not available or appropriate.
11. Select **DHCP Relay** and provide the DHCP server IP address.
12. Click **+** under the **Mapping Switch Ports to Port Profile** section.



13. Provide port ranges and select the port profile to apply to that entire port range. Ensure that port values do not overlap. A port can have only one port profile mapped to it.

    Note:

    Provide the same port value number in the **From** and **To** field to map a port profile to a single port.

14. Click **+** under **SNMP Servers** to send information to the SNMP server using SNMP Traps.
15. Click **Save.**

10.5.3 Apply Switch Profile to a Switch

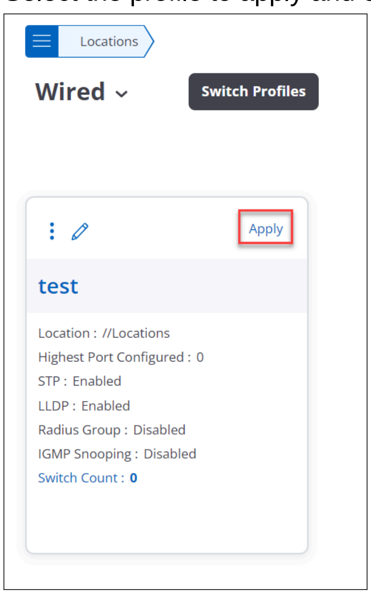
Once you have defined the switch configurations in a switch profile, you can apply those configurations to individual switches.

Note:

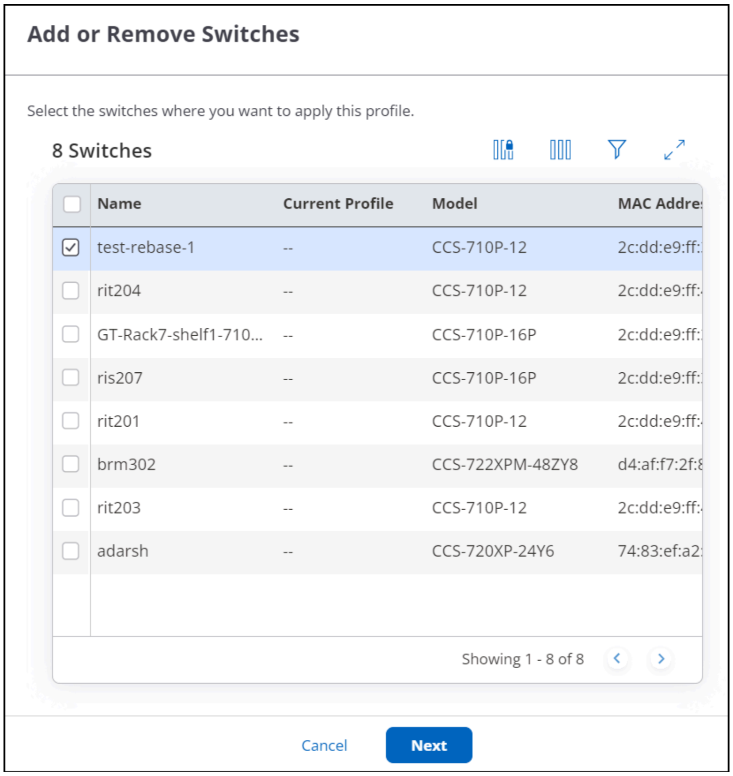
You can apply only one switch profile per switch.

To apply a switch profile to a switch:

1. Navigate to **CONFIGURE** > **Wired** > **Switch Profiles.**
2. Select the profile to apply and click **Apply.**

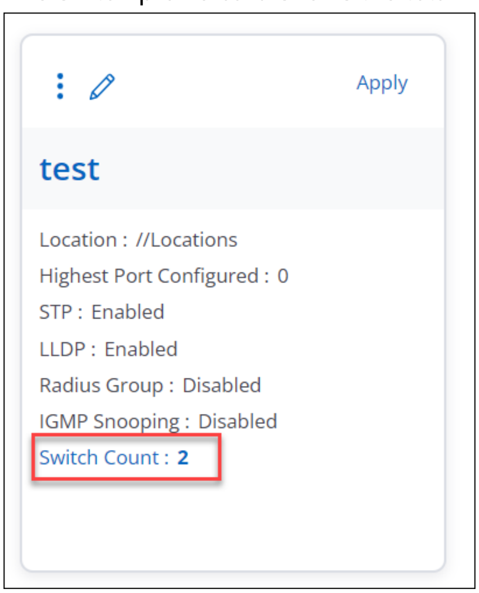


3. The switch pane opens and displays all the available switches. Switches that already have this profile are preselected. You can uncheck the selection to remove the profile from those switches. Select the switches that you want to apply the profile to and click **Next.**

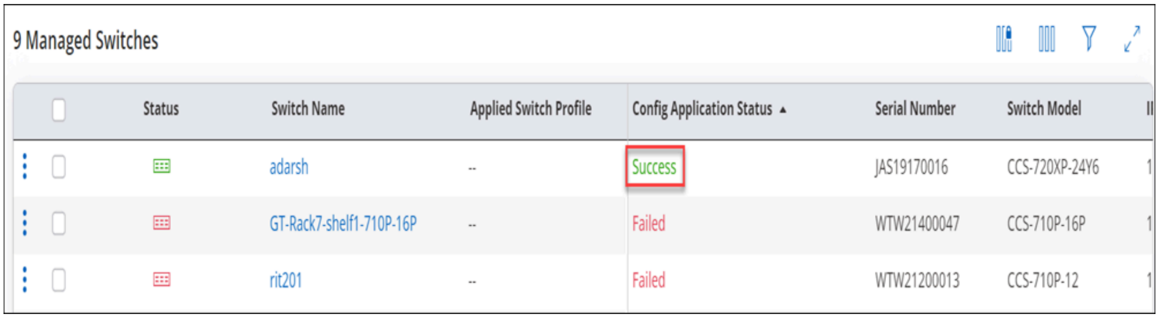


4. Verify the switches where the profile will be applied. If you have unchecked a switch in the previous pane, confirm that the switch doesn't appear here. Click **Apply.**

   The switch profile card shows the total number of switches using the particular profile.



You can verify that the profile is applied to the switch by checking the **Config Application Status** column in the **MONITOR** > **Wired**. Once the profile is applied to a switch and the configuration is applied successfully, the value on the Config Application Status column changes to **Success.**



10.5.4 Configure Device Settings

Under **CONFIGURE** > **Device** > **Switches,**, you can configure general switch-related settings such as NTP Server, Syslog Server, and security-related settings such as User Access Levels.

Note: By default, Device Settings applied to a location are automatically inherited by its child locations.

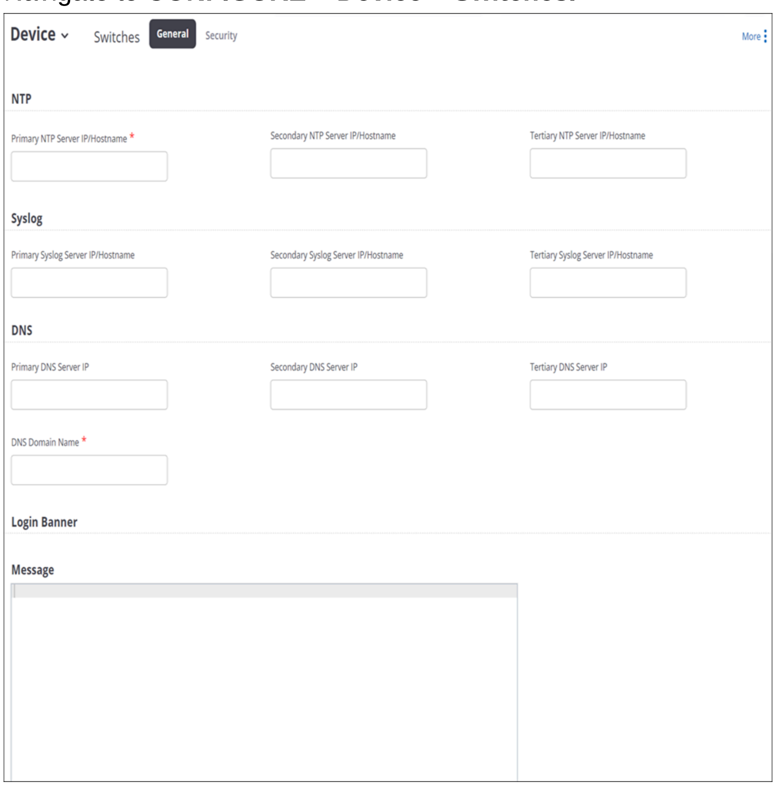
Switch device settings are divided into two tabs:

- General
- Security

General Switch Settings

To configure general switch settings:

1. Navigate to **CONFIGURE** > **Device** > **Switches.**



2. Under the **General** tab, provide the following details:

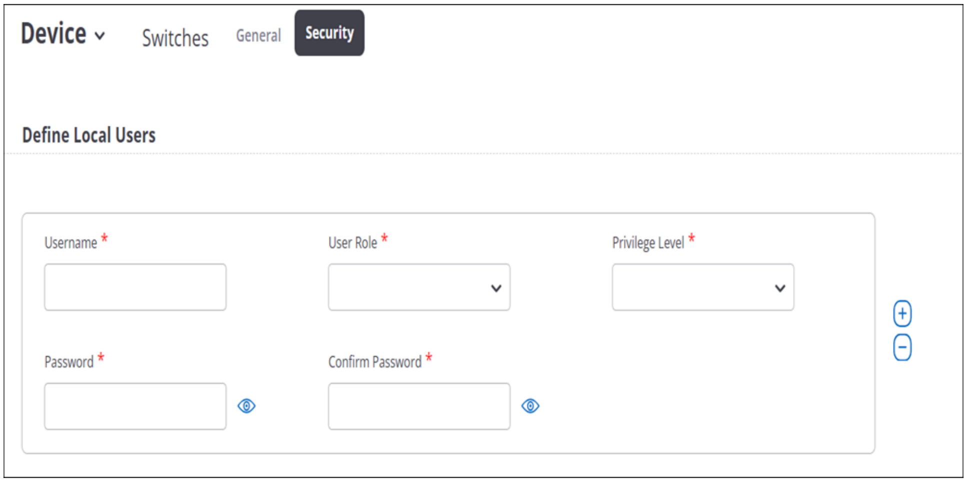
   - **NTP -** Provide details of the NTP server to ensure that the timestamp on the logs reflects the correct date and time by synchronizing the Arista device system clock with an NTP server.
   - **Syslog -** Provide details of the Syslog server to send messages and alerts to the Syslog server.

- **DNS** - Provide details of the DNS server to fetch the DNS information.
- **Login Banner** - Provide a text message to display on the switch CLI.

3. Click **Save.**

Security Settings

Under **Switches** > **Security** tab, you can define **Local Users** to enable your users to access the switch CLI. Along with the user credentials, you can define the user role and their privilege level.



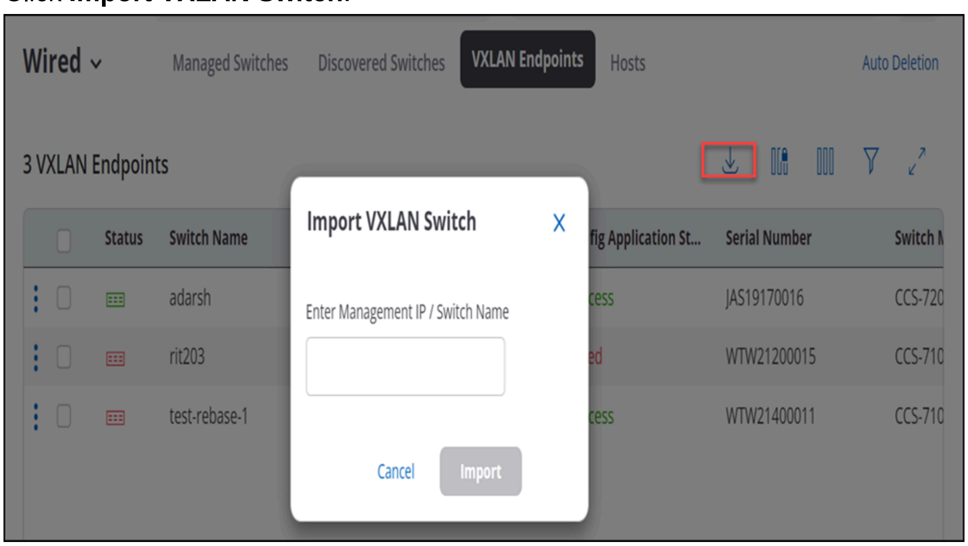
10.6 VXLAN Endpoints

VXLAN tunneling requires that the switch where the tunnel terminates is configured with a VTEP that matches the configuration on the AP. By having the same VXLAN configuration for APs and switches, you can aggregate all wireless traffic from the same VXLAN to a single wired destination for better traffic management and visibility.

To configure the switches from CV-CUE, the first step is to import the switches to the **VXLAN Endpoints** tab. You can import one switch at a time and up to a maximum of 10 switches to CV-CUE. Only those switches that you import, get listed in the VXLAN Profile.

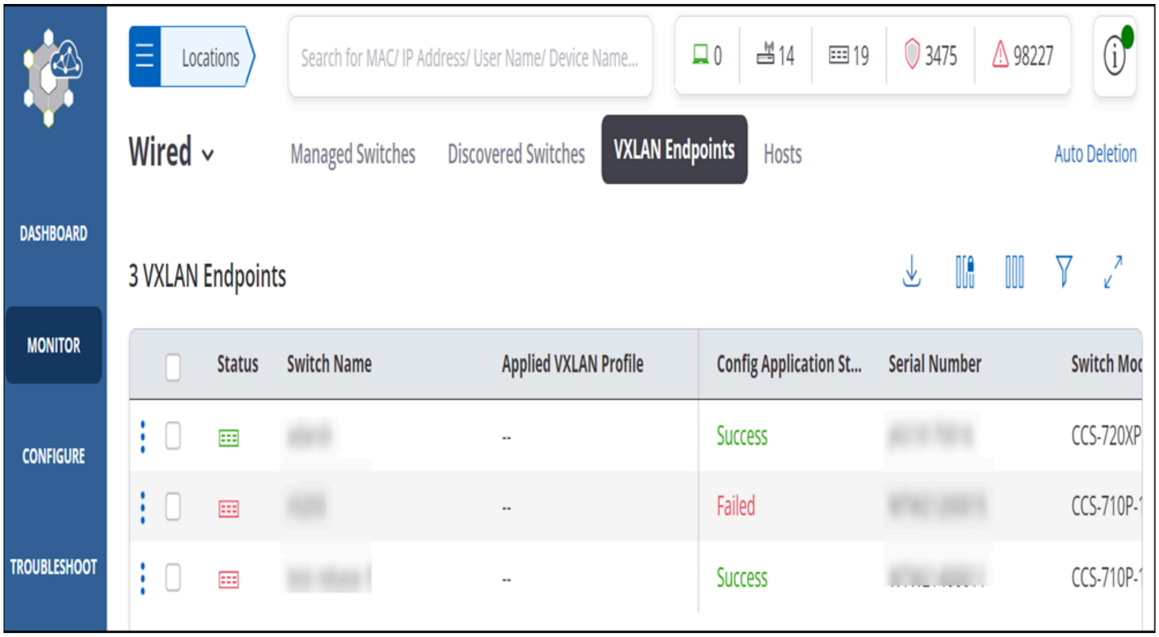
Follow these steps to import the switches:

1. Go to **MONITOR** > **Wired** > **VXLAN Endpoints**.
2. Click **Import VXLAN Switch**.



3. Provide the Management IP address of the switch or the name of the switch and click **Import**.

The switches are immediately imported to the **VXLAN Endpoints** tab.



Once imported, you can delete the switch listing from the page, rename switches, and reboot switches. You can rename and reboot active switches.

Chapter 11

Configure Wi-Fi

CV-CUE provides a convenient way to configure your Wi-Fi network via the Configure tab.

All configuration in CV-CUE 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 Configure tab allows you to configure the following:

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

Service Impact of Configuration Changes

CV-CUE warns a user of any service impact caused by settings changed on the UI. In general, the configuration changes affect the Wi-Fi 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 Wi-Fi service.

Tab and Action	Settings	Impact of Setting Change
SSID	Client Isolation Hide SSID SSID Profile Name	No impact.
	Any other setting	SSID restarts.
Role Profile	Profile Name	No impact.
	Any other setting	SSIDs using these settings restart.
Tunnel Interface	Profile Name	No impact.
	Any other setting	SSIDs using these settings restart.
RADIUS Profile	Profile Name	No impact.
	Any other setting	SSIDs using these settings restart.
Radio Settings	Wi-Fi Regulatory Domain	APs using these settings reboot.
	Any other setting	SSIDs using these settings restart.
Device Settings	- Access Radio Exceptions - Scanning - Wi-Fi Scan Duration - Wi-Fi Access Duration - Inter-Access Point Sync for Client Steering - Inter AP Sync Period	SSIDs using these settings restart.
	- SSID VLAN Monitoring - IPv4/IPv6 Dual Stack - Turn Access Points into Dedicated WIPS Sensors - Link Aggregation - Transmit Hash Policy	APs using these settings reboot.
Mesh Profile	Mesh Profile Enabled Mesh Profile Disabled	Mesh APs reboot. **Note**: When you edit an “enabled” mesh profile, mesh links are re-established, which may disrupt Wi-Fi service to clients.
Monitor > WiFi > Access Points > Customize VLANs	Any setting	AP reboots.

Tab and Action	Settings	Impact of Setting Change
Monitor > WiFi > Access Points > Customize Transmit Power or Channel	Any setting	SSIDs on the AP restart.
Monitor > WiFi > Access Points > Assign/Reassign to Group OR Remove Access Points from Group Other screens from which you can change AP-group assignment: • System > Navigator> Show Available Devices • Floor Plan	The service impact depends on which settings at the current location change because of the operation.	APs or the SSIDs on these APs may restart.
Get Configuration from another folder/group.	The service impact depends on which settings at the current location change because of the operation.	APs or the SSIDs on these APs may restart.
Monitor > WiFi > Radios > Turn Off Radio	-	All SSIDs on the radio are turned off.
Customize or Inherit Configuration at a Location	The service impact depends on which settings at the current location change because of the operation.	APs or the SSIDs on these APs may restart.
Move AP to another location	The service impact depends on which settings at the current location change because of the operation.	APs or the SSIDs on these APs may restart.
Troubleshoot > Packet Trace	Enable or disable packet trace on an SSID.	SSIDs for which auto packet trace is enabled or disabled will restart.

11.1 Checkpoints

You can create checkpoints to save your current configurations, profiles and settings. Creating and restoring a checkpoint is possible for all configuration settings available in CV-CUE. You can create a checkpoint for location based configurations, group configurations, or global configurations. For all the configurable settings that are available for a network, you can create a checkpoint to save it.

A checkpoint is a snapshot of your current settings and configurations.You can use this checkpoint to view your configuration details, compare your current configurations with a previous instance, or to restore your configurations to a particular set of settings. In case of a network failure or performance degradation, you can restore a previously created checkpoint to go back to the previous working state.

Note: This is a Beta Feature.

This chapter contains the following topics:

- Types of Checkpoints

- Create Checkpoints
- View Checkpoints
- Compare Checkpoints
- Restore Checkpoints

11.1.1 Types of Checkpoints

There are 3 kinds of checkpoints:

- **Location Checkpoint**

  Location checkpoint saves all your SSID configurations, network policies, device configurations, WIPS policies, Mesh profile, and other settings of the selected location.
- **Group Checkpoint**

  Group checkpoint captures the device configurations, custom device settings, and enabled SSID and Mesh profiles for a group.

  Note:

  Group checkpoint only captures which SSIDs and Mesh profiles have been enabled for the group, the actual SSIDs and Mesh profiles are not part of the checkpoint. Thus, restoring a group checkpoint restores the Enabled or Disabled state of SSIDs and Mesh profiles for that group. However, if the configuration of the SSID or Mesh profile was changed, the changed configurations are not restored.
- **Global Checkpoint**

  Global checkpoints save configurations for all locations and groups, along with global policies such as WIPS, Advanced Settings, and third-party server policies.

11.1.2 Create Checkpoints

The ability to create a checkpoint is available on the following UI screens:

- Configure > WiFi
- Configure > Device
- Configure > Network Profile
- Configure > WIPS
- Configure > Alerts
- System > Navigator
- System > Third Party Server
- System > WIPS
- System > Logs
- System > User Accounts

Create a Location or Group Checkpoint

The option to create a location or group checkpoint is available in all configuration options under the **Configure** menu.

To create a location or group checkpoint:

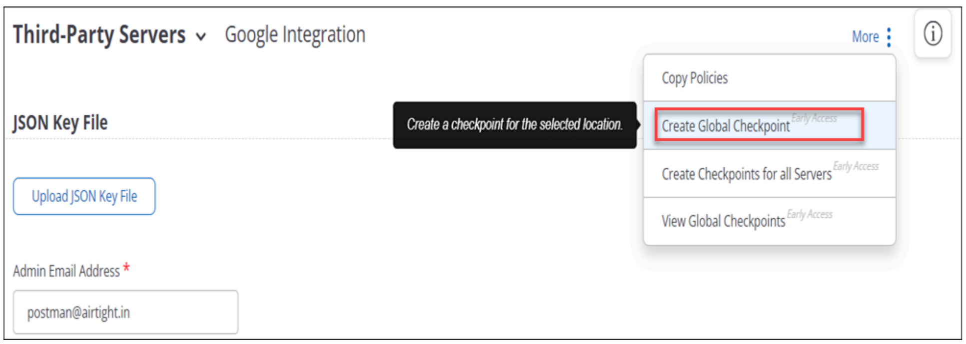
1. Select your location or group from the Navigator.
2. Go to **Configure > WiFi** or any Configure option.

   Note: Note: You cannot create a location checkpoint at the root location.
3. Click **Create Checkpoint** from the three-dot more menu.

4. Provide a name and a brief description for the checkpoint and click **Create.**

Create a Global Checkpoint

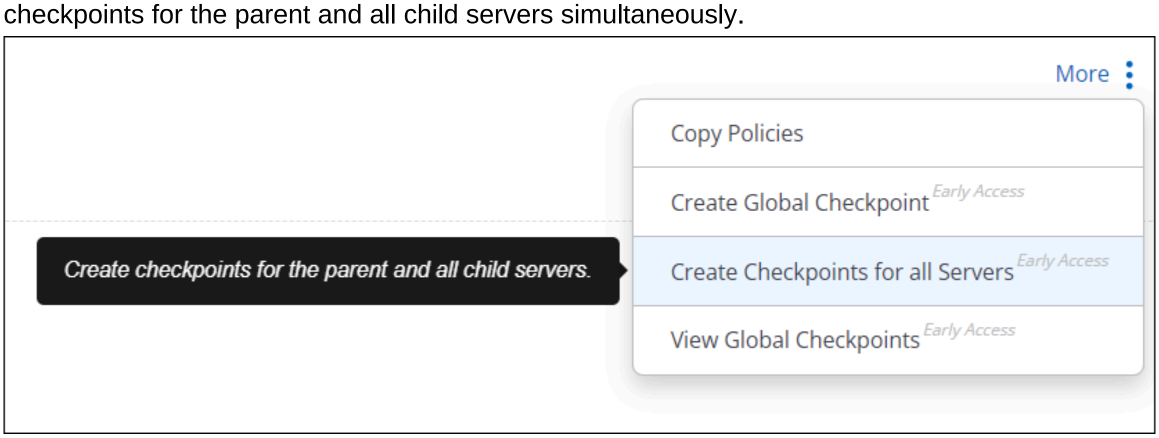
The option to create global checkpoint is available in all screens available under the **System** menu. You can create a global checkpoint by clicking **Create Global Checkpoint** from the three-dot more menu.



You can also create a global checkpoint from any CONFIGURE screen by selecting the root location in the location tree.

Create Global Checkpoint in MSU Setup

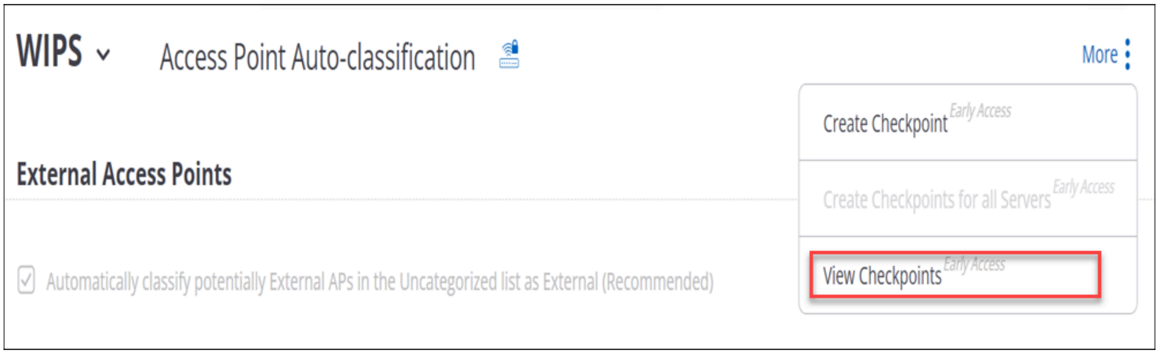
For MSU setups, navigate to the parent server and click **Create Checkpoints for all Servers** to create checkpoints for the parent and all child servers simultaneously.



Note: For MSU setups, global checkpoints are server specific. You need to create a separate global checkpoint for each server.

11.1.3 View Checkpoints

Just like Create Checkpoint, the option to view your created checkpoints is available on all **Configure** screens in the three-dot more menu. Navigate to your location or group to view all the checkpoints available for that particular location or group. You can view your global checkpoints from any of the screens available under the System menu or by selecting the root location in the location tree.

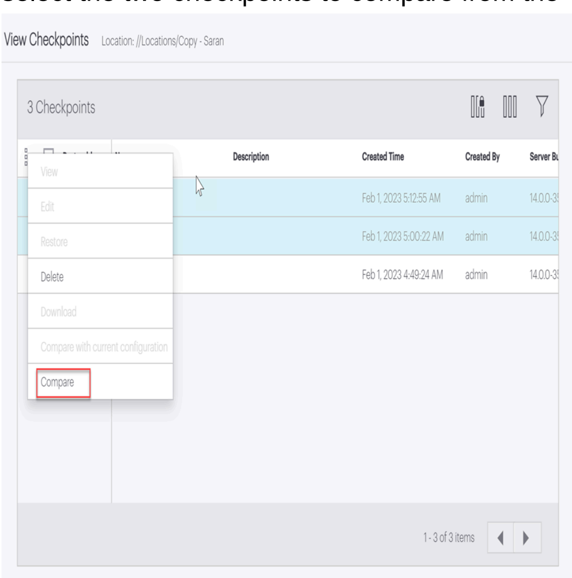


You can perform the following actions on your created checkpoints:

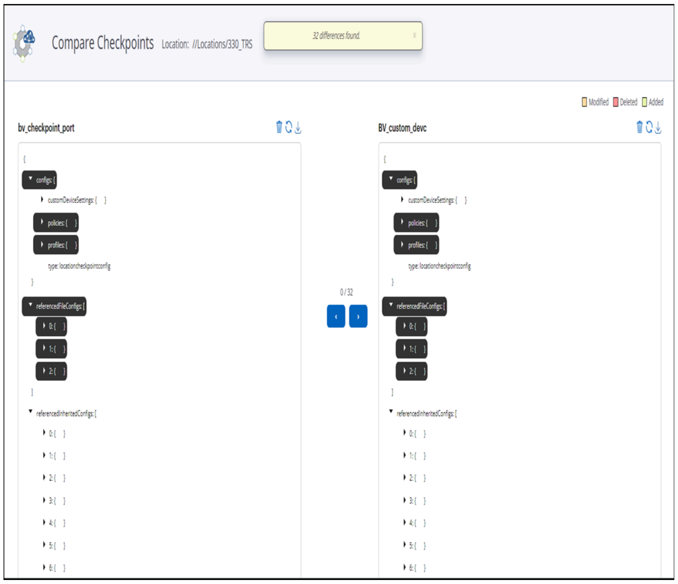
- Edit
- Delete
- Download - Displays a downloadable json file of your configuration details
- Compare
- Restore

11.1.4 Compare Checkpoints

You can compare two checkpoints to identify the delta in the configurations. To compare the checkpoints, select the two checkpoints to compare from the **View Checkpoint** table and click **Compare.**



A new tab displaying the differences in the JSON files of both the checkpoints opens.



You can also compare the checkpoint with your current configuration.

11.1.5 Restore Checkpoints

You can restore your configurations and settings to an earlier created checkpoint. When you restore a checkpoint, all the settings and configurations are changed to that of the saved checkpoint. If a location is inheriting a policy from its parent or is using an inherited profile, the checkpoint only captures the inheritance information and not the actual profile or policy. When you restore such a checkpoint, the policy is inherited again from the parent. If the inherited policy or profile is changed, the changed settings are not restored.

Non-restorable checkpoints

You cannot restore global checkpoints. Checkpoints also become non-restorable if any of the referenced configurations are deleted. For example, consider an SSID profile inherited by a child location. If you delete the SSID profile from the parent location, the checkpoint created on the child location becomes non-restorable.

You can use global and non-restorable checkpoints to perform view and compare operations.

Chapter 12

SSID Settings

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

The **SSID** tab shows all the SSIDs configured on your Wi-Fi 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.

This chapter contains the following topics:

12.1 SSID Basic Settings

The **Basic** tab is the first of the three mandatory 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:

- **SSID Profile Name:** 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 "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)". You can modify the profile name.
- **SSID Type:** This could be a **Public** or a **Guest** SSID. If you select **Guest**, then on the UI you can see the **Captive Portal** tab next to the **Network** tab, since Guest SSIDs typically use captive portal logins.
- **Hide SSID:** If you select this, the SSID will be hidden, i.e., it will not be broadcast on the wireless link.
- **Include AP Name in Beacon:** Select this option to include the name of the access point (AP) in the beacon.

12.1.1 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.

12.2 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.
- **Enhanced Open (OWE):** 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), **UPSK**(Unique PSKs), **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), **UPSK**(Unique PSKs), **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.

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 does not support 802.11w and 802.11r.

RADIUS Settings

See 802.1X or RADIUS Settings for details.

Deny Locally-Administered MAC Addresses

You can prevent clients using locally-administered MAC addresses from accessing your network. You can ensure that only clients using their device's globally unique MAC addresses are able to connect to the network. By making sure that only devices with globally unique MAC addresses connect to the network, you can mitigate potential security threats associated with spoofing or unauthorized access by having control over device identification.

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 mangement frames. Arista uses the AES-128-CMAC algorithm, so that is 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 is not 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.

12.2.1 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** > **WiFi** > **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**, **UPSK**, 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** or **WPA2** and **UPSK**, 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.
  - Enable **Send DHCP Options and HTTP User Agent** if you want the AP to send client profiling attributes such as DHCP Options 12, 15, and 60, and HTTP User Agent to the RADIUS server in the RADIUS accounting packets.
  - 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. Select **VLAN IDs** and manually enter the RADIUS VLANs. Select **Auto VLAN** to dynamically assign VLANS to clients and send the VLAN to the access point (AP) when the client connects. For more information on creating dynamic VLANs from RADIUS server, refer to **Create Dynamic VLANS from RADIUS Server.**
  - **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 does not 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 Wi-Fi client. The choice depends on whether your network 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**.
  - 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 does not happen too soon, allowing time for the primary server to stabilize if it had been flapping.

- If you select **WPA2**, you can configure **802.11w** for Management Frame Protection (MFP). If you select **PSK**, you can enable Group PSK. To enable Group PSK, select **Group PSK** and enter the passphrase. If you select **UPSK**, you must configure the RADIUS server.

  Note: 802.11w is not supported in Open, OWE, and WPA/WPA2 Mixed Mode security levels.

- If you select **WPA/WPA2 Mixed Mode**, you need to select **PSK**, **UPSK**, 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**.
- If you select **WPA3**, you need to select either **WPA3 Personal**, **UPSK**, 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. If you select WPA3 or WPA3 Transition Mode, you can select one of the following **SAE Mechanism for PWE Derivation:**
  - Hunting-and-Pecking only
  - Hash-to-Element only
  - Hunting-and-Pecking and Hash-to-Element

3. Select **Deny Locally-Administered MAC Addresses** to prevent clients using locally-administered MAC addresses from accessing your network.
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 **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.

12.2.2 Group PSKs

A single SSID can support up to 64 Group PSKs, each for a group of Wi-Fi clients. To appreciate Group PSKs, consider the following use cases:

- An enterprise might require IoT devices to connect to the Wi-Fi 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.

12.2.3 Unique PSKs

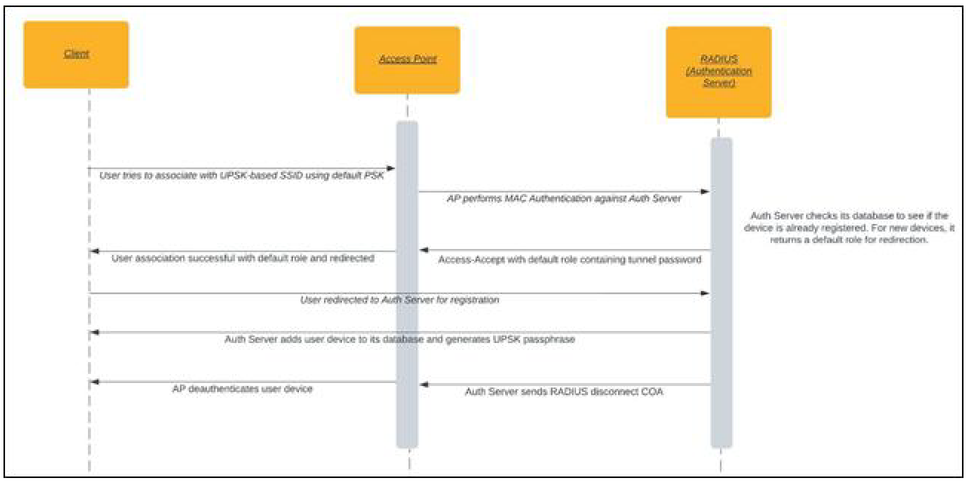
UPSKs allow users to connect to the same SSID using a unique PSK which is user specific. UPSK provides added security as compared to single PSK because single PSKs are easily compromised.

UPSK is useful for large campuses that have huge numbers of BYOD/IOT devices, for example, college campuses or universities. The advantages of UPSK are:

- Increased security by using individual PSKs per student and MAC authentication. When a user leaves the organization, administrators can deactivate their account so their PSK will no longer be valid to connect to the university network.
- Easily managing a group of devices. For example, consider an enterprise having multiple categories of IOT devices such as cameras and printers. The administrator can assign different PSK to different categories of devices and manage the group of devices easily.
- Easily managing a group of devices. For example, consider an enterprise having multiple categories of IOT devices such as cameras and printers. The administrator can assign different PSK to different categories of devices and manage the group of devices easily.
- Monitoring of devices. One user may have multiple devices. In such cases, RADIUS assigns each device a specific PSK making it unique. Network administrators can easily track individual devices.

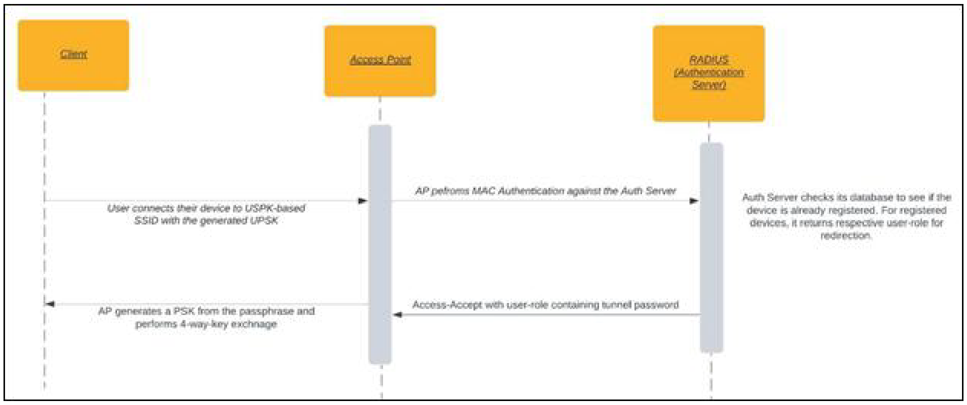
Note: You cannot disable **RADIUS MAC Authentication** if you have enabled UPSK.

UPSK New User Onboarding Flow



1. New user logs in and connects its clients using the default PSK (shared by admin).
2. Access Point (AP) initiates the MAC-Auth with the RADIUS server. As the MAC address is not registered, the RADIUS server assigns a default role to the client.
3. Client gets redirected to a portal for registration.
4. After registration, the user gets an auto-generated or admin-configured Unique PSK. The user can use this UPSK to connect other devices after MAC registration in the RADIUS server. This PSK remains unique to that user.
5. Once the device is registered, the RADIUS server can now send COA-Disconnect to the client.

UPSK Registered User Onboarding Flow



1. The user connects the registered device to the UPSK enabled SSID and enters the assigned PSK.
2. AP initiates the MAC-Auth with the RADIUS server. As the MAC address is already registered, RADIUS server sends an access-accept containing RADIUS Tunnel-Password attribute, which carries the assigned PSK.
   - Attribute Name: Tunnel-Password
   - Attribute ID: 69
3. AP matches the hash of the PSK entered by the user and the hash of the PSK received in the access-accept packet. If it's a correct match, the user device is onboarded.

Use Case

Consider a new student trying to connect to the university network. The student first connects to the SSID using the default credentials provided by the network administrator. The student is connected to the network using the default role and is redirected to the registration portal. The student can then provide their device information and register their device. The registration portal assigns a user-specific PSK and the client is disconnected. Post registration, the student can log into the network using the unique PSK assigned to them.

Unique-PSK User Private Network and Identity Lookup

Along with UPSK, you can also enable User Private Netwtoks and Identity Lookup.

UPSK User Private Networks

You can enable UPSK User Private Networks option to generate UPSK with isolation between multiple users' devices. After you enable this setting, User-A's devices onboarded using UPSK-A cannot reach or communicate with devices onboarded using User-B's UPSK-B.

This setting further enhances the security provided by UPSK.

UPSK Identity Lookup

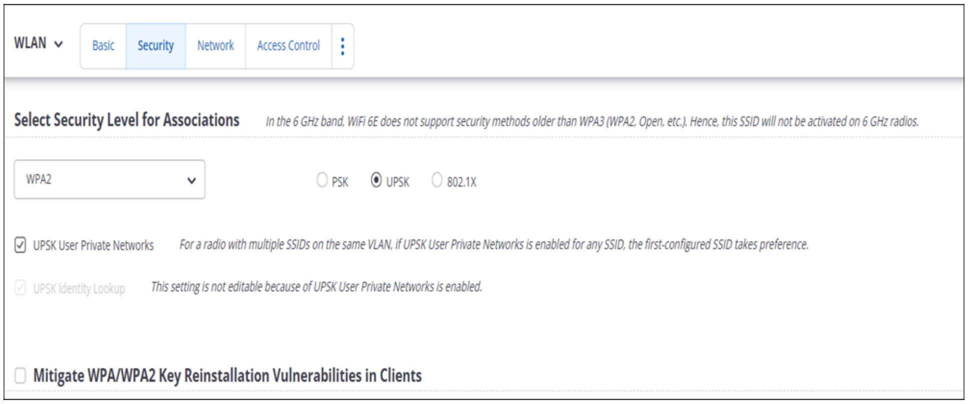
You can enable UPSK Identity Lookup to auto-register a new client using the generated UPSK Password. This feature lets you onboard a new client without the need of manual intervention.

Enabling UPSK

To enable UPSK:

1. Go to **WiFi** > **Configure** > **SSID.**
2. Under the **Security** tab, select your security level for associations.

   Note: UPSK is unavailable for Open, OWE, and Hotspot 2.0 OSEN security levels.
3. Select the **UPSK** radio button.



4. Select **UPSK User Private Network** to enable isolation between client devices.

   Note: For WPA2 and WPA/WPA2 Mixed Mode, UPSK Identity Lookup is auto-enabled. For WPA3 and WPA3 Transition Mode, you cannot enable UPSK Identity Lookup.

5. Under the **Access Control** tab, provide details for the **RADIUS** Settings.
6. Save the settings.

Supported AP Platforms and Security Methods

- AP Platforms - WiFi 6 and above
- Supported Security Methods
  - WPA2
  - WPA3
  - WPA/WPA2 Mixed
  - WPA3 Transition mode

Note: For WPA3 and WPA3 Transition Mode, you cannot enable **UPSK Identity Lookup**.

12.2.4 Local Authentication of Wireless Clients

Local Authentication (also known as authentication survivability) is the ability of access points (AP) to authenticate and onboard clients to the network using CA certificates through the integrated EAP server of the AP. Use Local Authentication when the RADIUS servers are not reachable to authenticate the clients. It is typically a temporary authentication mechanism; avoid using it as a primary authentication.

When the AP cannot reach the RADIUS server, it goes into authentication survivability mode. While the AP is in this mode, if any client tries to connect to the AP, the AP uses certificate-based authentication to on-board the AP and connect to the network. As soon as the RADIUS servers are reachable, the client gets reauthenticated by the RADIUS server.

Workflow

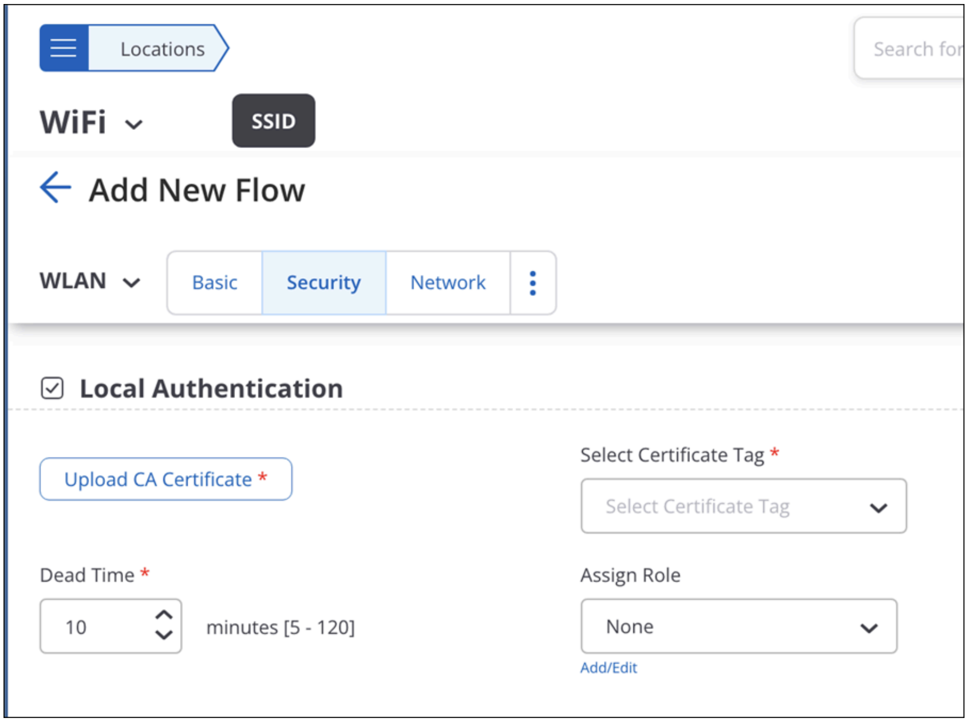
You can define up to four RADIUS servers in CloudVision Cognitive Unified Edge (CV-CUE) for 802.1X authentication. When the Primary RADIUS server computer is unreachable, the AP retries connecting to the Primary RADIUS server a certain number of times before switching to the next RADIUS server. When all the RADIUS servers are unreachable, the AP falls back to the local authentication mode. While the AP is in this mode, if any client tries to connect to the AP, the AP uses certificate-based authentication to on-board the client and connect to the network. Such clients are called locally authenticated clients.

The AP remains in the local authentication mode for the duration defined in the Dead Time configuration. After the dead time is over, the AP repeats the cycle of connecting to the RADIUS servers. If it successfully connects to the RADIUS server, it disconnects all locally authenticated clients. The clients reauthenticate using the RADIUS server.

Enable Authentication Survivability

To enable Authentication Survivability:

1. Go to **CONFIGURE** > **WiFi** > **Add SSID** or edit an existing SSID.
2. Click the Security tab and navigate to the **Local Authentication** section.

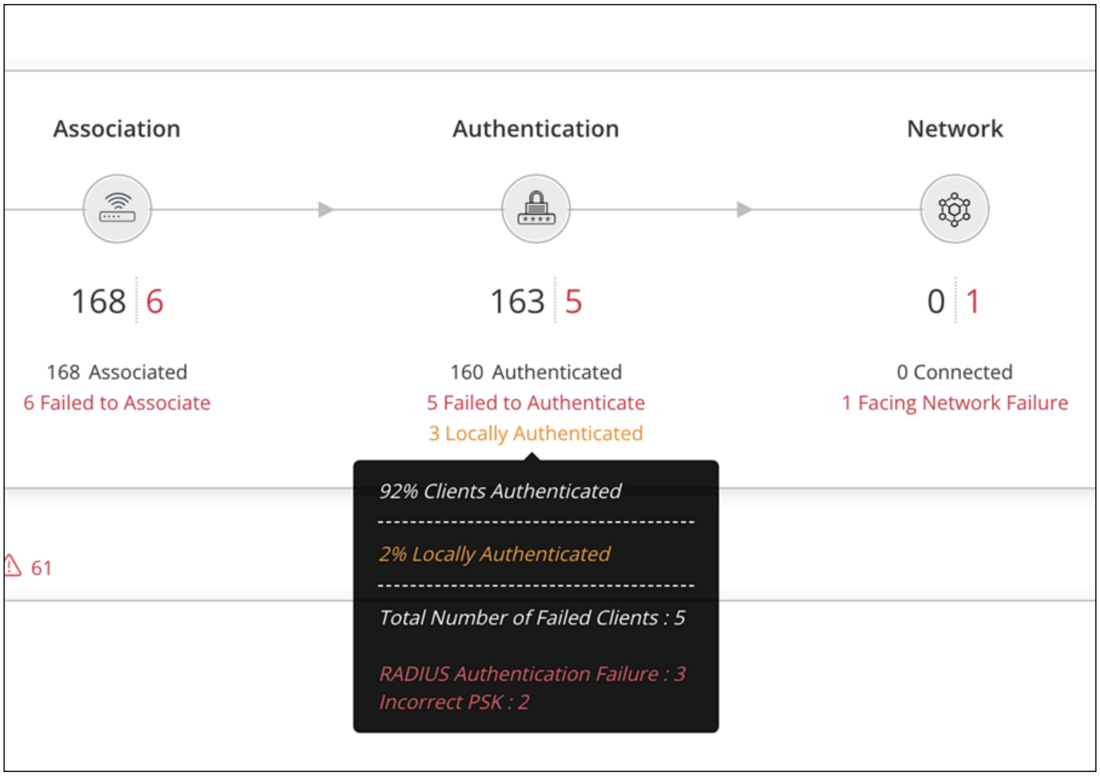


3. Select **Local Authentication** and provide the CA Certificate.
4. Upload the CA Certificate and then select a certificate tag.
5. Select the **dead time.** Dead Time indicates the duration for which the AP remains in the Local Authentication mode before connecting to the RADIUS server.
6. (Optional) Select a role for the clients from Assign Role for locally authenticated clients

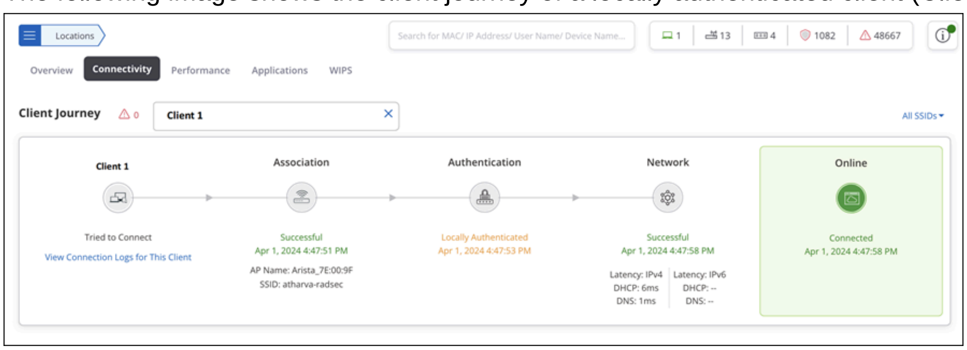
You can verify locally authenticated clients and APs from the following pages:

- Connectivity Dashboard — Client Journey
- Client Details — Client Journey
- Client Listing: Locally Authenticated column in client listing (MONITOR > WiFi > Clients)
- AP Listing: Locally Authenticated column in AP listing (MONITOR > WiFi > Access Points)

The following image from the Connectivity Dashboard shows 3 locally authenticated clients:



The following image shows the client journey of a locally authenticated client (Client 1):



Configure and Monitor Alerts

You can configure and monitor alerts related to Local Authentication by navigating to **CONFIGURE** > **Alerts** > **Device** > **Local Authentication.** . For more information, refer to Configure System Alerts

12.2.5 SSID RADIUS Pooling

RADIUS Pooling lets you assign a pre-defined list of RADIUS Servers that Access Points (AP) can use to authenticate, authorize, and maintain clients' accounts. It offers better load-balancing capabilities and improved scalability.

You do not have to specify the order of the RADIUS servers as Primary or Secondary. Every AP randomly chooses the RADIUS servers from the pool, and then independently decides the sequence of the RADIUS servers and follows the order. Two APs sharing the same RADIUS pool may not share the same order for the RADIUS servers. APs automatically distribute the client load based on an intelligent algorithm.

Also, there is no separate list of RADIUS servers for Accounting and Authentication. The AP uses the same active RADIUS for accounting and authentication. If the AP doesn't receive any Accounting messages from the active RADIUS server, it switches to the next RADIUS in the order. If all the RADIUS servers are disconnected and Local Authentication (Authentication Survivability) is enabled, the AP goes into the Local Authentication mode.

RADIUS Pooling is an SSID setting in the **Security** and **Access Control** tabs.

Configure RADIUS Pooling

Follow these steps to configure VLAN Pooling in SSID settings:

1. Go to **CONFIGURE > WiFi > Add SSID**.
2. Select the **Security** tab and select any 802.1X Authentication security level association, such as WPA3, WPA3 transition Mode, or WPA2.
3. Select **Enable RADIUS Pooling** and select a maximum of four RADIUS servers from the drop-down list. If you have not configured any RADIUS servers, they won't be visible in the drop-down list.

4. (Optional) Click **Add/Edit** to add RADIUS servers or edit existing RADIUS servers.
5. Save the settings.

Note: On enabling **RadSec**, only the RadSec-capable RADIUS servers will be displayed in the drop-down list. On disabling RadSec, the RadSec-capable RADIUS servers are not displayed in the drop-down list.

Event Logs

When the AP decides the order of the RADIUS server, it generates an event log that displays the order of the RADIUS Server. You can view the event logs from **TROUBLESHOOT > Event Logs > Access Points**.

12.3 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 additional Ethernet ports 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 additional Ethernets 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 additional Ethernet ports are available only on some Arista AP models. For more information, see the AP Datasheet.

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 have not 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**, CV-CUE tunnels RADIUS messages between the AP and the RADIUS server. Key characteristics are:

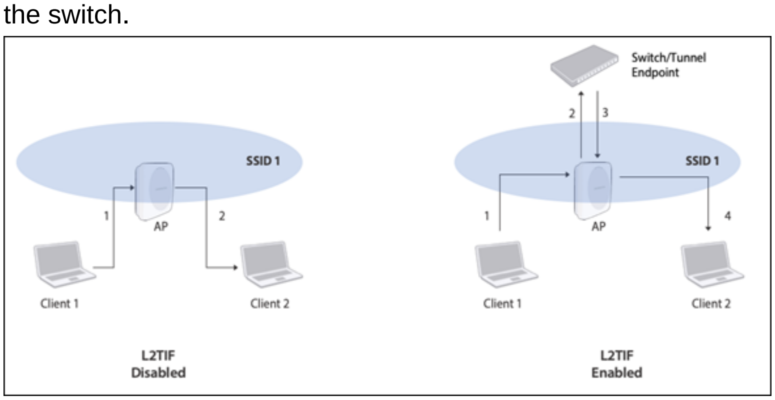
- All types of tunnel interfaces support tunneling of RADIUS messages between APs and a RADIUS server located behind the tunnel endpoint.
- For tunnel types other than the RAP VPN tunnel, an AP obtains its IP address from the DHCP server in the remote network on the SSID VLAN. A RAP running an SSID with 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:

- 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 Wi-Fi 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**, CV-CUE 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.

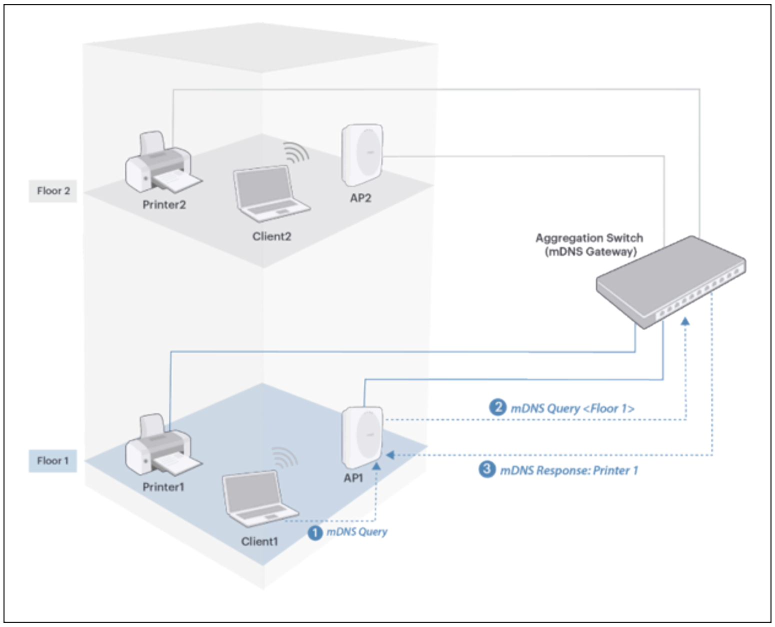
DHCP Option 82 (DHCP Agent Information Option) is generally used in a distributed DHCP server environment to assign IP addresses to clients based on their location. The AP inserts DHCP Option 82 in all DHCP packets, such as DHCP Discover and DHCP Request, thereby providing additional information to identify 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.

DHCP Packet Forwarding is used to send a copy of DHCP Packets from Access Points (AP) to Network Access Control (NAC) solutions for profiling clients and assigning appropriate network segments. When you enable the packet forwarding option on the UI, the AP forwards a copy of the DHCP packets to Port 67 of the destination server.

The destination server can be an IPv4 or IPv6 address, not a hostname. You can provide a maximum of eight IP addresses for the destination server. You also have the option to send the DHCP packets through a tunnel if the Network Mode is **L2 Tunnel** or **L3 Tunnel**. However, you cannot send the DHCP packets to IPv6 addresses if the network mode is L3 Tunnel.

Note: Forwarding of DHCP packets is applicable only for wireless clients.

Multicast DNS (mDNS) Packet Tagging helps Wi-Fi clients discover network services such as printers or conference room displays. A Wi-Fi 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.



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.

12.3.1 Example Use Case

Let us 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

12.3.2 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** > **WiFi** > **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 messags 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.
    - 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. Select **DHCP Packet Forwarding** to send a copy of DHCP Packets from Access Points (AP) to Network Access Control (NAC) solutions for profiling clients and assigning appropriate network segments.
9. Click **Save** or **Save & Turn SSID On**.If you select **Save & Turn SSID On**, see Turn an SSID On for details.

12.3.3 SSID VLAN Mapping

To enable SSID VLAN mapping:

1. Go to **CONFIGURE** > **WiFi** > **SSID.**Click **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**.
6. Add the VLAN name and ID and save the settings.
7. Save and turn on the SSID.

12.3.4 SSID VLAN Pooling

VLAN Pooling is a list of VLAN IDs defined by the Network Administrator. The Access Point (AP) distributes the VLAN IDs from this pool of VLAN to the clients connecting to the SSID. VLAN Pooling offers better scalability and optimized load-balancing of traffic.

VLAN Pool can be Static or Dynamic. Static VLAN Pool is manually defined by Network Administrators in the SSID. Dynamic VLAN Pool is assigned by RADIUS servers depending on the device identity.

VLAN Pooling also supports MVRP.

Rules and Restrictions for VLAN Pool

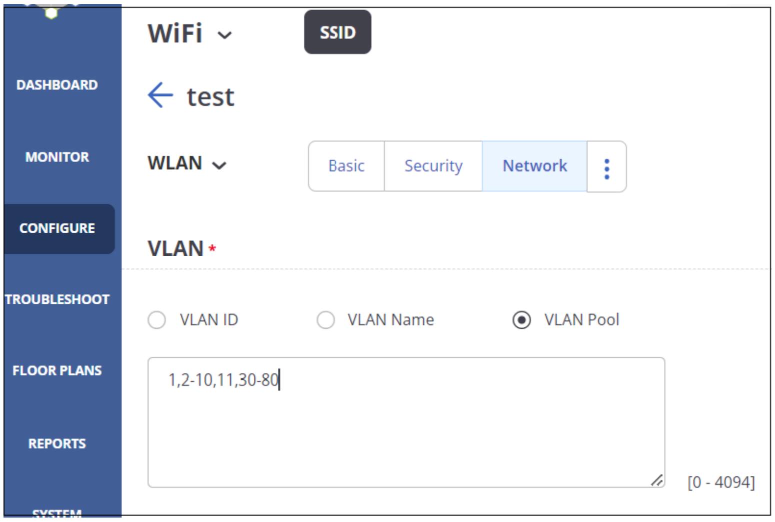
The following VLAN rules and restrictions apply to VLAN Pool:

- You can provide a maximum of 128 VLAN IDs in the VLAN Pool.
- VLAN IDs must be in the range of 0-4094.
- You can provide a VLAN range separated by a hyphen. Example, 10-20
- Duplicate VLAN IDs are not allowed.
- Inverse or decreasing VLAN range is not allowed. For example, 20-10 is not allowed.

Configure VLAN Pooling

Follow these steps to configure VLAN Pooling in SSID settings:

1. Go to **CONFIGURE > WiFi > Add SSID**.
2. Select the **Network** tab and then select the **VLAN Pool** option.



3. Specify the **VLAN IDs.**
4. Save the settings.

Alternatively, to configure the VLAN Pool from the Role profile, navigate to **CONFIGURE > Network Profile > Role** and specify the VLAN Pool.

12.4 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, CV-CUE 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 Wi-Fi. 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 Authentication, Authorization and Accounting (AAA) 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 us 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.

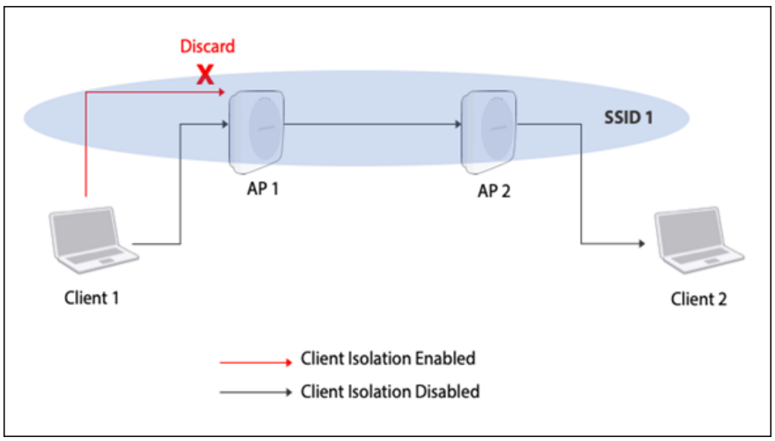
It could happen that you have different settings in the SSID tabs and different ones in the Role Profiles tab. What happens then? For the answer, see Role Profile.

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, Wi-Fi 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 Wi-Fi 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.



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 CV-CUE grays out the **RADIUS MAC Authentication** option, since 802.1X already is a RADIIUS-based mechanism.

Some Wi-Fi 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 Sopt 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.

12.4.1 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 Wi-Fi 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.

12.4.2 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 us 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 4: Example Rules Table for Retail Store

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

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 do not 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.

12.4.3 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. CV-CUE prompts you to enable Application Visibility from within the Application Firewall Settings, so you do not 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 5: Example Rule for Enterprise Corporate SSID

Rule Name	Category	Application Name	Action
Block Facebook and Twitter	Social Networking	Facebook, Facebook Apps, Facebook Event, Facebook Messages, Facebook Post, Facebook Search, Facebook Video, Facebook Video Chat, Twitter	Block
Default			Block

12.4.4 L3-4 versus Application Firewall Decision Table

Table 6: Decision Table for L3-4 Firewall versus Application Firewall

L3 Firewall Action	Application Firewall Action	Final Action
Deny	Any	Deny
Allow	Deny	Deny
Allow	No Match	Allow
No Match	Deny	Deny
No Match	Allow	Allow
No Match	No Match	Default
Allow and Mark	Allow and Mark	Allow with App Mark
Allow and Mark	Allow	Allow with L3 Mark
Allow and Mark	No Match	Allow with L3 Mark
No Match	Allow and Mark	Allow with App Mark
No Match	No Match	Default Mark

12.4.5 Configure Firewall in SSID

You can configure both L3-4 and Application firewalls.

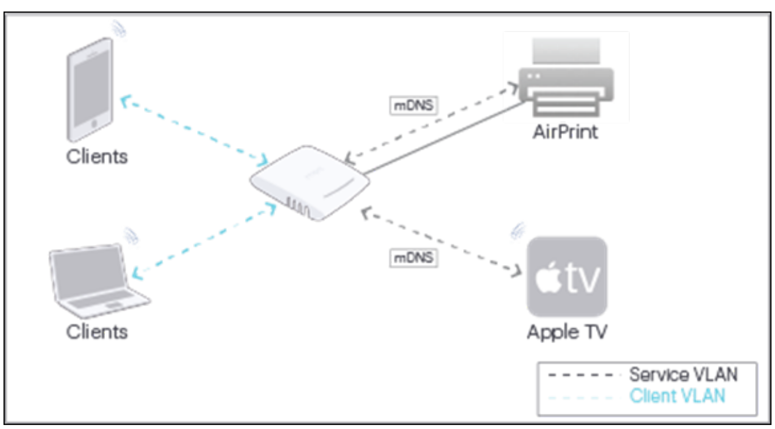
To configure firewalls:

1. Go to **CONFIGURE** > **WiFi** > **SSID** > **Access Control.**
2. Click **Firewall**.
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.
5. Click **Save** or **Save & Turn SSID On**. If you select **Save & Turn SSID On**, see Turn an SSID On for details.

12.4.6 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).

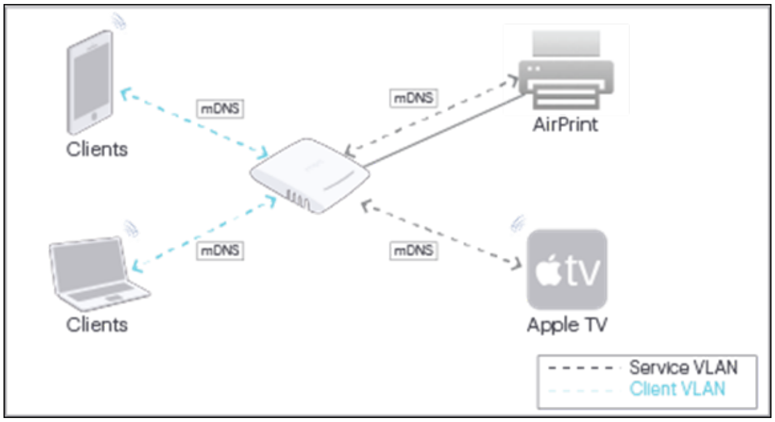
Generally, Bonjour devices run on local networks and the Bonjour service advertisements do not cross network boundaries. They are restricted to the broadcast domain of a single VLAN / Subnet. Clients that are connected on a different VLAN than the one on which the Bonjour devices are connected, cannot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



12.4.7 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 us 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, 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.

12.4.8 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** > **WiFi** > **SSID** > **Access Control.**
2. Select **Bonjour Gateway**.

   Note: Bonjour Gateway does not work when the Network is set to **NAT** mode. If you have set the Network to NAT mode, CV-CUE 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**.

12.4.9 DHCP Fingerprinting-based Access Control

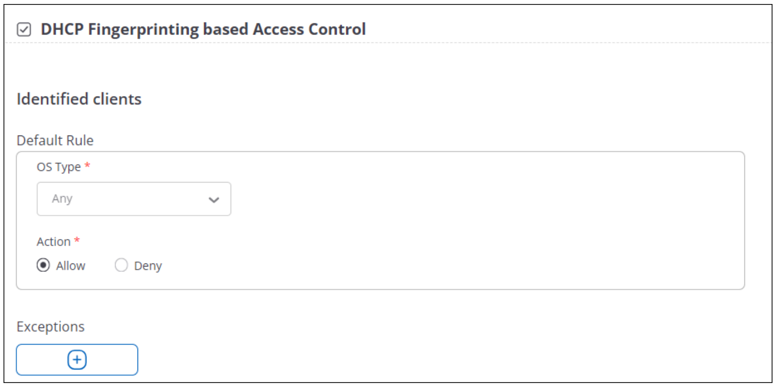
Using DHCP Fingerprinting-based access control, you can allow or deny clients getting connected to an SSID.

The AP can identify the Operating System (OS) of the client based on the DHCP exchange packets between the client and the DHCP server. DHCP has many request parameters; in this case, DHCP uses Option 55 to capture and exchange client OS (Macintosh, Windows, and others). Leveraging this client-specific information, you can restrict certain types of clients from connecting to the network.

As a network administrator, you can use DHCP fingerprinting to allow or deny a client from associating with an Access Point (AP), put clients in a specific VLAN, apply bandwidth control or firewall rules, and apply other network policies.

Note that DHCP fingerprinting-based access control is not a per-client configuration. This configuration applies to all clients matching a particular profile, using a specific OS. So, all clients of a specific OS can be allowed or denied to access the network.

1. Navigate to **CONFIGURE** > **WiFi** > **SSID** > **Access Control.**
2. Enable the **DHCP Fingerprinting based Access Control** check box.
3. For **Identified Clients**, first specify the **Default Rule**. The **OS Type** is **Any** and you cannot change it. Select either **Allow** or **Deny** for **Action**. The default rule applies to all identified clients.
4. (Optional) Specify the exceptions to your default rule, if any. You can add multiple exceptions.
5. Click **Allow** or **Deny** for **Unidentified clients**.



6. Save the settings.

12.4.9.1 Identified and Unidentified Clients

The AP categorizes clients into identified and unidentified based on client information captured from DHCP exchange request.

When the client tries to connect to the AP the next time, the client data is matched with the fingerprint database. If the data matches, the client is classified as identified. If not, the client is considered as unidentified.

How the Rules Work for Identified and Unidentified Clients

For unidentified clients, you can specify whether to Allow or Deny such clients to connect to the network. For identified clients, you can specify a default rule and exceptions to the default rule. Exceptions are given priority over the default rule.

In a default rule, the OS type is **Any** for clients and you cannot change it. You can change the action as **Allow** or **Deny** for such clients. In exceptions, you can specify only the OS type. The action will be the opposite of what you select in the default rule. For example, if the default rule for an identified client is Allow for Windows OS, and in the exceptions you have added Android as the OS type, then Windows clients will be allowed to connect to the network but Android clients will be denied connection to the network.

When a client successfully connects to the network, you can see the status of the client as **Successfully connected** in **MONITOR** > **WiFi** > **Clients**. For clients that failed to connect, the status is seen as **Failed client. DHCP Fingerprinting Failure**. The client events are also captured in the client event logs.

12.4.10 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** > **WiFi** > **SSID** > **Access Control.**
2. Select **Redirection**.
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.

Info: 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.

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**.

12.4.11 What is a Walled Garden?

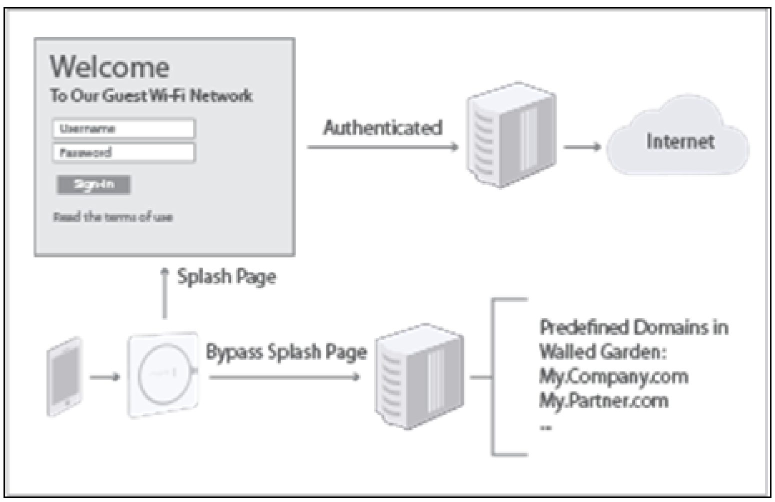
Let us understand the concept of a "walled garden" and its typical applications within Arista Wi-Fi. A walled garden allows Wi-Fi providers to control which destinations users can or cannot access on a wireless network.

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 Wi-Fi network.

When a captive portal is enabled on an SSID, a splash page is presented to the users before allowing them Wi-Fi access. The splash page serves as a gatekeeper for allowing Wi-Fi 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 Wi-Fi 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.



12.4.12 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 is 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.

12.4.13 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

12.4.14 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.

12.4.15 Configure Client Authentication

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

To configure client authentication:

1. Go to **CONFIGURE** > **WiFi** > **SSID** > **Access Control.**
2. Select **Client Authentication**.
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 RADIIUS-based mechanism.
4. Click **Save** or **Save & Turn SSID On**. If you select **Save & Turn SSID On**, see Turn an SSID On for details.

12.4.16 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.

Prerequisites

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

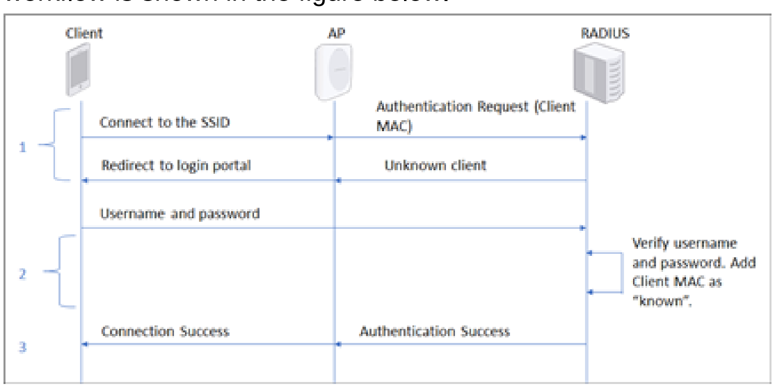
You do not have to leave the SSID Access Control tab to configure Google or RADIUS. Just click **Change Settings?** under **Role Based Control**. CV-CUE opens a right-pane window, allowing you to configure and save the relevant settings and continue with Role Based Control.

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 do not 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**.

12.4.17 Typical RADIUS MAC Authentication Flow

You can configure RADIUS MAC Authentication in CV-CUE to assign roles to clients both before and after authentication. Let us 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. The RADIUS server notifies the AP that the client MAC is unknown. The AP then redirects the client to a login portal.
2. 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.
3. 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 CV-CUE using any of the following:

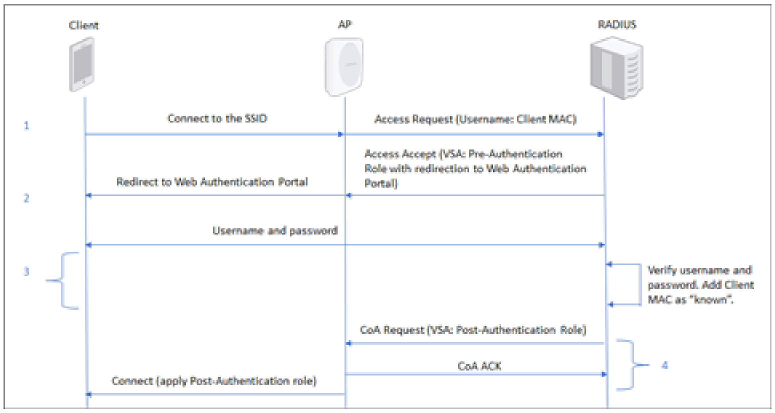
- Role Profiles

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

CV-CUE supports integration with Forescout, ISE and ClearPass.

12.4.18 Implementation Using Role Profiles

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



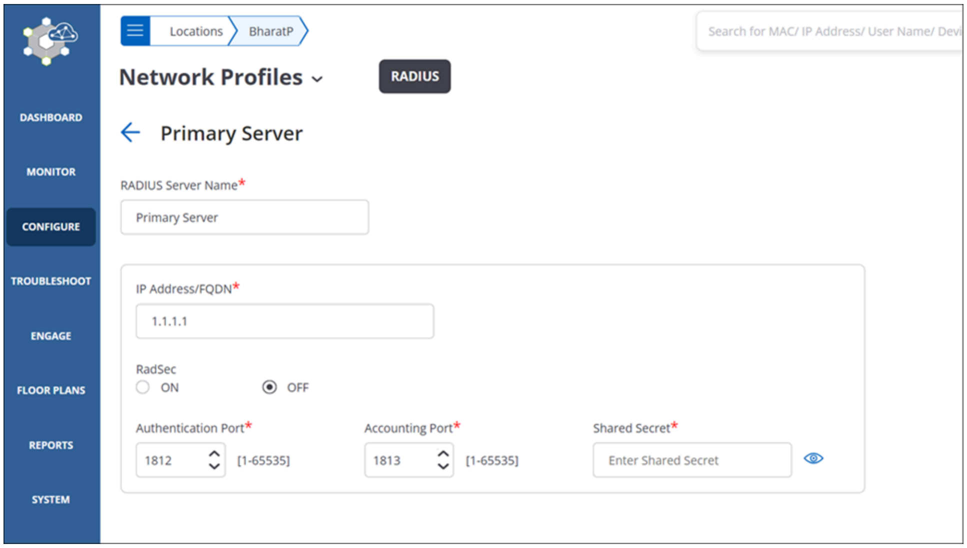
1. When the client first connects to the SSID, the WiFi Access Point (AP) sends an Authentication Request containing the client's MAC address to the RADIUS server.
2. The RADIUS server responds with an Access-Accept message containing the Pre-Authentication role. The Pre-Authentication role redirects 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.

12.4.18.1 Configure Roles with RADIUS MAC Authentication

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

RADIUS Profile

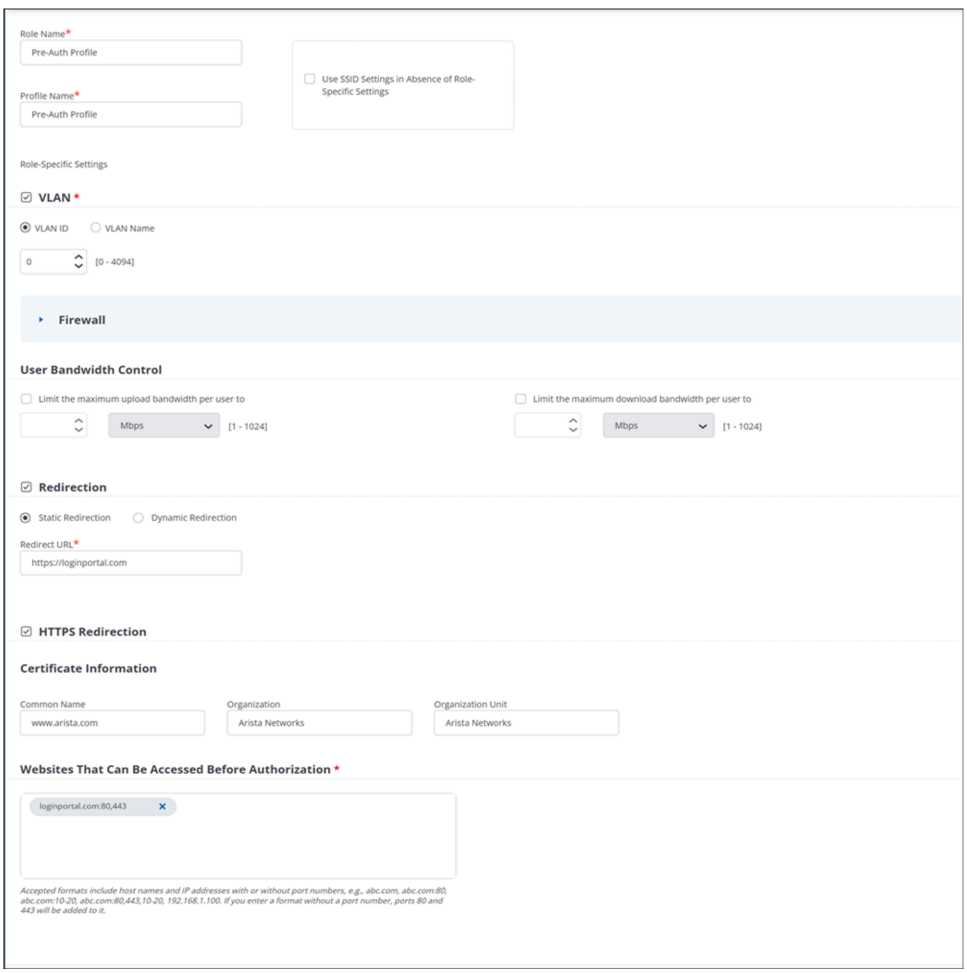
Under **CONFIGURE** > **Network Profiles** > **RADIUS,** click **Add RADIUS Server** and enter the RADIUS server details as shown below:



Pre-Authentication Role

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

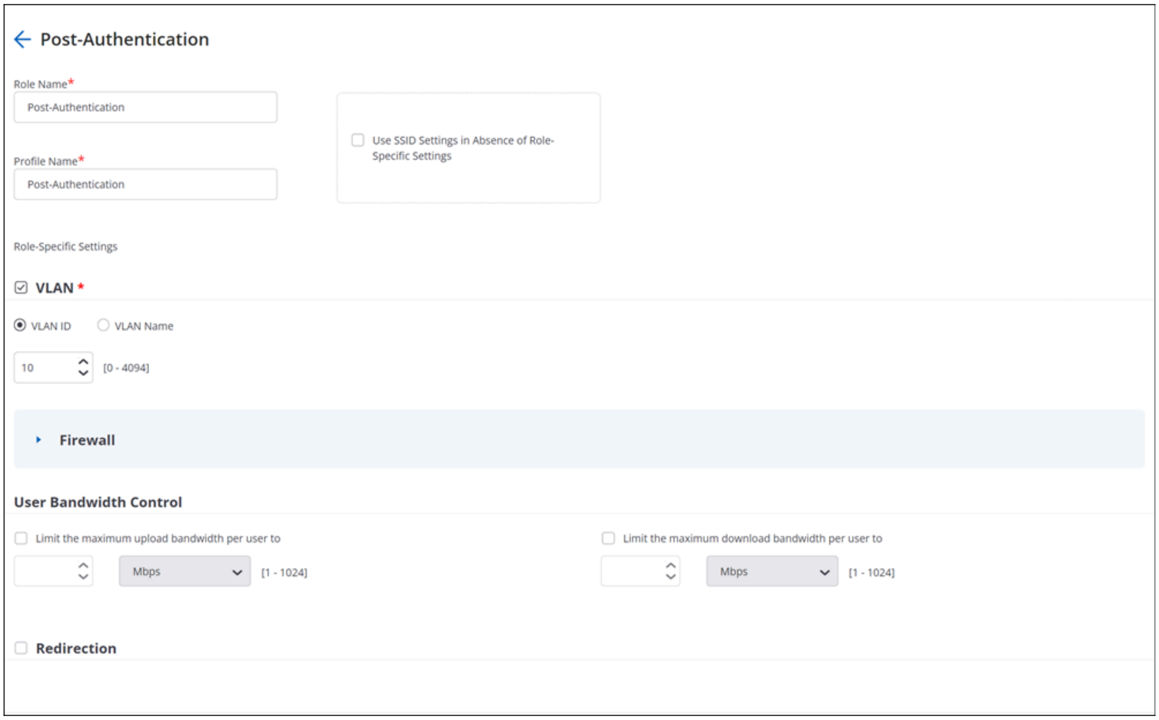
Note: You must add the web authentication portal URL and ports 80 and 443 to the “Websites That Can Be Accessed Before Authorization” list.



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.



You need to configure the RADIUS server to return this role in the Change Of Authorization (CoA) message it sends to the AP.

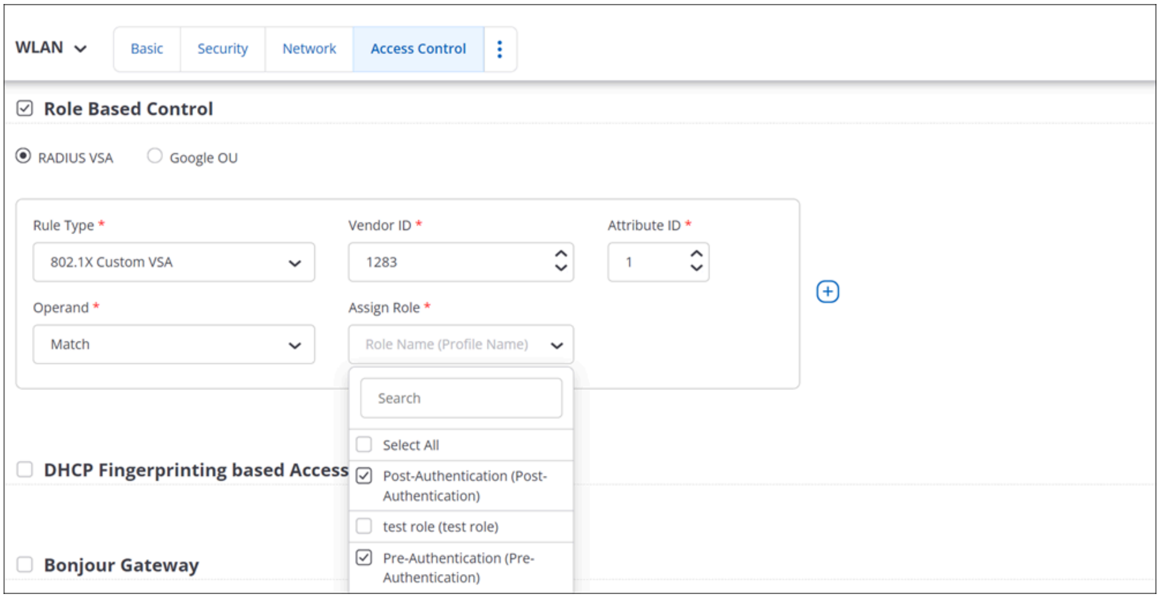
RADIUS MAC Authentication and Role-Based Control

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.

12.5 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 and neighboring APs that are visible to the AP. 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)
- 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
- RSSI data of connected clients as well probing clients without the local MAC address
- RSSI data of neighboring Arista APs
- Channel information with each RSSI record

If you select **Association**, you can also select **Website URLs accessed by WiFi userst** 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 CV-CUE either on a per-Client basis or on a per-Application basis.

Note: Application Visibility is not supported on 802.11n devices (AP Feature Matrix). 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.

12.5.1 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>

12.5.2 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** > **WiFi** > **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**.

12.5.3 Analytics Parameter

Fields	Description
Store Analytics on This Server	
Application Visibility	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 > 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.
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

Fields	Description
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	
Server URL	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.
Send Interval	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.
HTTP Fields	
HTTP Content	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.
Post Request Body	If checked then include the POST method request body in the JSON file.
User Agent	If checked then include the user agent (browser) in the JSON file.
Referer	If checked then include the HTTP referrer in the JSON file.

12.6 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 Wi-Fi 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 CV-CUE 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 Wi-Fi.
- **Social Media Plug-Ins**: Users authenticate using their social media login credentials to access the Wi-Fi. 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 Wi-Fi, Paid Wi-Fi, 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 Wi-Fi free for some time and then start charging. For example, many airports offer free Wi-Fi for the first half an hour and charge users after that. **Host Approval** is for enterprise setups, where you want to authorize the guest Wi-Fi access. The host, whom the guest has come to visit in the enterprise, can be the authorizer. Host-approved Wi-Fi 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 Wi-Fi with guest user account credentials that you have defined. The guestbook can include other user-specific information. When you enable this in CV-CUE, 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 Wi-Fi. 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 Wi-Fi, 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. CV-CUE 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**, CV-CUE automatically disables the other plugins.

Important Notes on Payment Gateway

If you use the **Paid** or the **Free + Paid** option, you are 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 do not 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 Wi-Fi 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 Wi-Fi connection, some Operating Systems (e.g. iOS) try to reach some sites — let us call them "test sites" — to detect if the user is behind a captive portal. If they are 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 have not spent using the Wi-Fi. To avoid such problems, it is 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 Wi-Fi 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 Wi-Fi users of an organization see the same e-mail and use the same SMS account, no matter what location they are 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 Wi-Fi. Or, if you are organizing an event and want to provide Wi-Fi 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 Wi-Fi by using these account credentials.

Another use case is to give users the option to access Wi-Fi without any authentication. Say, you have configured the social media plug-ins on your portal. But you also want to provide Wi-Fi 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 Wi-Fi 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

12.6.1 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 are 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 do not 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.

Content Type	Walled Garden Entries
Vimeo	vimeo.com vimeocdn.com google-analytics.com
PollDaddy	polldaddy.com
YouTube	youtube.com googlevideo.com ytimg.com google.com googleusercontent.com (for thumbnail images) lh5.googleusercontent.com (for thumbnail images)

12.6.2 Configure Access Point Hosted Captive Portal

To configure AP Hosted Captive Portal settings:

1. Navigate to **CONFIGURE** > **WiFi** > **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.
5. Click **Upload Custom Splash Page Bundle** to upload the bundle.

   Info: 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.

12.6.3 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 **CONFIGURE** > **WiFi** > **SSID** > **Captive Portal.**
2. Select **Captive Portal**.
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:

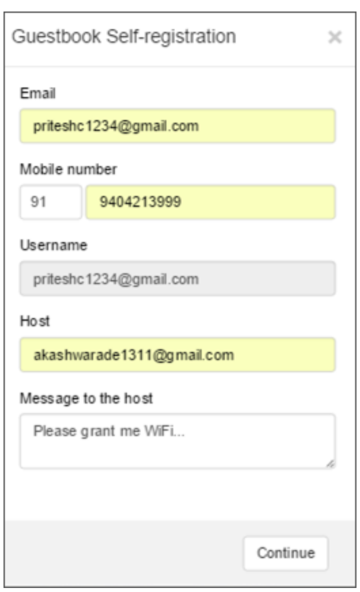
- Configure Clickthrough Plugin
- Configure Username Password Plugin
- Configure Social Media Plugins
- Configure Passcode Through SMS Plugin
- Configure Webform Plugin
- Configure External RADIUS Plugin

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 are 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.
   - **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.

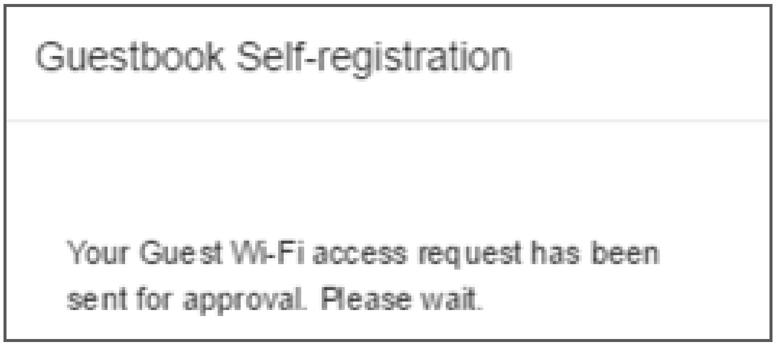
12.6.4 Guest Wi-Fi User Authentication with Host Approval

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.

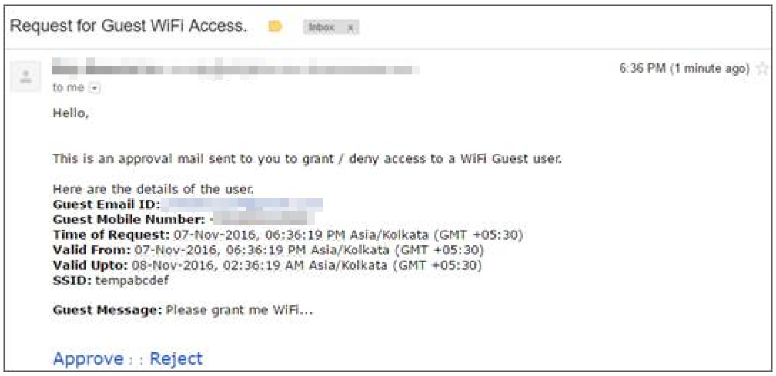


2. The user is shown a message that the request has been sent for approval.

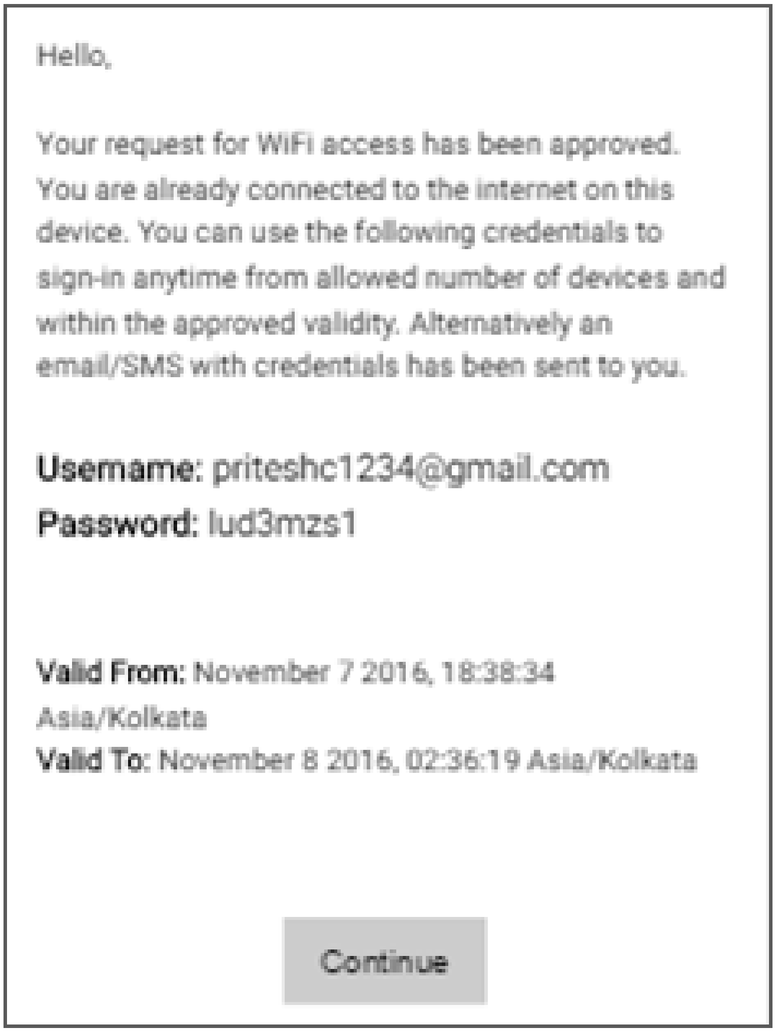


3. The host receives an email for the registration performed by the guest user.

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.

12.6.5 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 **CONFIGURE** > **WiFi** > **SSID** > **Captive Portal.** to edit the splash page.

To edit the splash page:

1. Click the "pen" (edit) icon on the Splash Page section.
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.
   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 Wi-Fi") and your copyright info.
   a. Enter the **Plugin Title**. This is your caption or welcome message.
   b. Enter the **Copyright** text.
8. Click **Save**.

12.6.6 Configure Common Settings for Plugins

Common settings are system wide — they are 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 Wi-Fi users.

You must select **Cloud Hosted** captive portal under **SSID** > **Captive Portal** to configure common settings.

- Configure Email Account Settings
- Configure SMS / MMS Account Settings
- Configure Payment Gateway Settings

12.6.7 Configure Email Account Settings

This is the email account used to communicate with your Wi-Fi 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 **CONFIGURE** > **WiFi** > **SSID** > **Captive Portal** tab, click **Select login method for guest WiFi users**.
2. Click the "gear" icon for Common Settings.
3. Click the "envelope" icon for **Email Account**.
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.
6. Click **Save** to save the configuration.

12.6.8 Configure SMS/MMS Account Settings

This is the SMS / MMS account used to communicate with your Wi-Fi users.

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**.
2. Click the "gear" icon for Common Settings.
3. Click the "message" icon for **SMS / MMS Account**.
4. Under the **Account** option, select an existing account or select **Add New** to add a new account.
5. Provide an account name.
6. Select a **Service Provider**.

   Info: 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. Enter a **Test Account** number, provide the **DLT Template ID**, and **Test SMS Settings** to verify that the configuration works.
8. Click **Save** to save the configuration.

12.6.9 Configure Payment Gateway Settings

This is the payment gateway used to bill users when you select Paid or Free + Paid Wi-Fi.

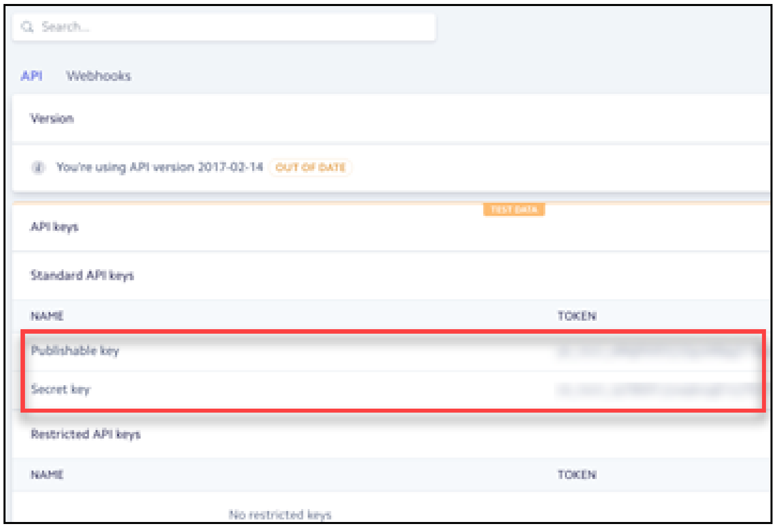
You must select **Cloud Hosted** captive portal under **SSID** > **Captive Portal** to configure common settings.

Note: When using Paid or Free + Paid Wi-Fi, 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 is not 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**.
2. Click the "gear" icon for Common Settings.
3. Click the "two coins" icon for **Payment Gateway**.
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 CV-CUE.
9. Click **Save** to save the configuration.



12.6.10 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 Wi-Fi.

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**.
2. Select **Clickthrough** and click the edit icon (pencil) to edit settings.
3. Configure the Common Plugin Settings.
4. Click **Save**.
5. Click **Save** on the **Plugin & QoS** page to save the clickthrough settings.
6. Save the SSID.

12.6.11 Configure SAML

You can integrate SAML SSO with a captive portal for authentication.

Note: The SAML integration functionality is only available for captive portals hosted on the Arista Cloud. It is not available if the captive portal is hosted on third-party servers or on the access point.

To configure SAML:

1. Navigate to **CONFIGURE** > **WiFi** > **SSID** > **Captive Portal** tab.
2. Select the **Captive Portal** checkbox and select **Cloud Hosted** from the dropdown list.
3. In **Authentication Plugins and Quality of Service**, click **SAML** in Custom.
4. From the right panel, click the **Custom > SAML** checkbox and click the SAML logo. You can add your custom logo or keep the default logo. The SAML Settings right panel opens.
5. Provide the display name. Users will see this name on the splash page. A maximum of 15 characters, including spaces, is allowed for the display name.
6. (Optional) Upload a logo for the SAML icon. Once uploaded, you will see this logo appear in the previous screen.
7. Click the **Download SP Metadata XML** link and share the downloaded metadata with the identity provider.
8. Provide the metadata information received from your IDP Vendor. You can add the metadata manually or upload an XML with all the metadata details. To add metadata manually, provide these information:

   - **Entity ID** — The ID of the SAML SSO identity provider (IDP).
   - **Login URL** — The URL of the IDP application.
   - **Hash Algorithm**

- **Upload Certificate** — Certificate used by the IDP to sign or encrypt the data.

9. To upload the metadata, click Upload XML and upload the XML file from your local or shared drive.
10. Provide a mapping between SAML attribute and target attribute. The SAML attributes are predefined attributes that users see on the UI. The Target attributes are attributes defined by the identity service provider.
11. Define the Quality of Service parameters:
    - Login Timeout
    - Blackout Time
    - Limit the maximum download bandwidth to
    - Limit the maximum upload bandwidth to
12. Specify the redirect URL. Users will be redirected to this URL after authentication.

    Note: There is another redirect URL field in the Post Login section in Captive Portal settings. If both the fields have different redirect URLS, then the URL defined in the SAML settings page takes precedence over the general Captive Portal redirect URL settings.
13. Save the SAML settings and then save the Captive Portal settings.

12.6.12 Configure OpenID Connect

You can integrate OpenID Connect with a captive portal for authentication. .

Note: The OpenID Connect integration functionality is only available for captive portals hosted on the Arista Cloud. It is not available if the captive portal is hosted on third-party servers or on the access point.

To configure OpenID:

1. Navigate to **CONFIGURE** > **WiFi** > **SSID** > **Captive Portal** tab.
2. Select the **Captive Portal** checkbox and select **Cloud Hosted** from the dropdown list.
3. In **Authentication Plugins and Quality of Service**, click **Custom**.
4. From the right panel, click the **Custom > OpenID Connect** radio button and click the OpenID Connect logo. You can either keep the default logo or add your custom logo in the next screen. The **OpenID Settings** right panel opens.
5. Provide the display name. Users will see this name on the splash page. A maximum of 15 characters, including spaces, is allowed for the display name.
6. (Optional) Upload a logo for the OpenID Connect icon. Once uploaded, you will see this logo appear in the previous screen.
7. Specify the login details for the OpenID Connect account:
    - **Client ID** — The client ID or login ID of your OpenID Connect account. It is used to identify your application on IDP.
    - **Client Secret** — The password of your OpenID Connect account. Client secret ensures that the access tokens are granted to authorized applications only. By adding the client secret in SSID settings, we ensure that our application is considered as authorized by the IDP.
    - **Issuer URL** — The URL of the OpenID server. This is the landing page url of the IDP. The user gets to the sign-in page through this URL.

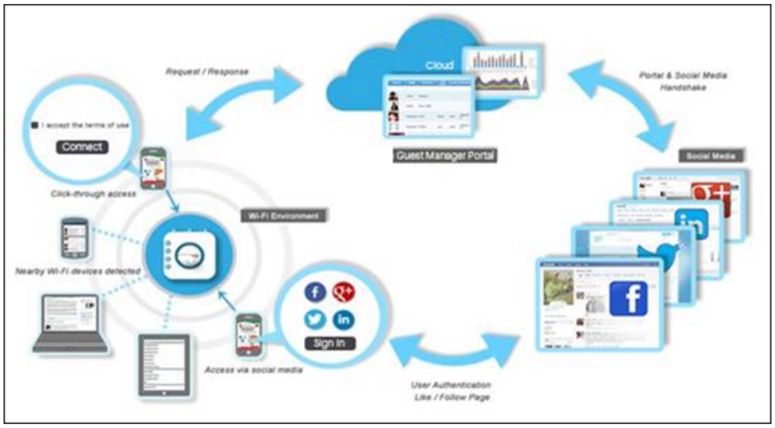
    Note: The maximum character limit for all the three fields is 200 characters.
8. Define the Quality of Service parameters:
    - Login Timeout
    - Blackout Time
    - Limit the maximum download bandwidth to
    - Limit the maximum upload bandwidth to
9. Specify the redirect URL. Users will be redirected to this URL after authentication.

Note: There is another redirect URL field in the Post Login section in Captive Portal settings. If both the fields have different redirect URLS, then the URL defined in the SAML settings page takes precedence over the general Captive Portal redirect URL settings.

10. Save the OpenID settings and then save the Captive Portal settings.

12.6.13 Access Wi-Fi Using Social Media Plug-Ins

The figure below explains how Arista authenticates the guests using social media plug-ins.



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.

12.6.14 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

12.6.15 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** > **WiFi** > **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**.

5. Select **Display Like Page** if you wish the guests must Like your Facebook page when they authenticate using their Facebook account credentials.
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.

   Info: 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 Commom Social Media Plugin Settings for **Quality of Service** and **Redirect URL** configuration.
9. Click **Save**.

12.6.16 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** > **WiFi** > **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**.
5. Select **Display Follow Page** if you wish the guests must Follow you on Twitter when they authenticate using their Twitter account credentials.
6. Enter the **Follow Page URL** for the Twitter page that the guests can see and 'Follow'.
7. Refer Configure Commom Social Media Plugin Settings for **Quality of Service** and **Redirect URL** configuration.
8. Click **Save**.

12.6.17 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** > **WiFi** > **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**.
5. Select **Display Follow Page** if you wish the guests must Follow you on LinkedIn when they authenticate using their LinkedIn account credentials.
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.

   Info: 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 Commom Social Media Plugin Settings for **Quality of Service** and **Redirect URL** configuration.

9. Click **Save**.

12.6.18 Configure Foursquare Plug-In

To configure the Foursquare plug-in:

1. Navigate to **CONFIGURE** > **WiFi** > **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**.
5. Refer Configure Commom Social Media Plugin Settings for **Quality of Service** and **Redirect URL** configuration.
6. Click **Save**.

12.6.19 Configure Google+ Plug-In

To configure the Google+ plug-in:

1. Navigate to **CONFIGURE** > **WiFi** > **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**.
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.

   Info: 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 Commom Social Media Plugin Settings for **Quality of Service** and **Redirect URL** configuration.
8. Click **Save**.

12.6.20 Configure Instagram Plug-In

To configure the Instagram plug-in:

1. Navigate to **CONFIGURE** > **WiFi** > **SSID** > **Captive Portal** > **Authentication Plugins & Quality of Service** > **Social.**
2. Select **Instagram**.
3. Enter **Client ID** provided by Instagram to communicate with the Instagram application that uses OAuth 2.0 protocol to call Instagram APIs.
4. Enter **Client Secret**.
5. Refer Configure Commom Social Media Plugin Settings for **Quality of Service** and **Redirect URL** configuration.
6. Click **Save**.

12.6.21 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 CV-CUE, 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 drop-down 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 Commom Social Media Plugin Settings for **Quality of Service** and **Redirect URL** configuration.
8. Save the Okta configuration and then save the SSID configuration.

12.6.22 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**.
5. Enter **Limit the maximum upload bandwidth to**.
6. Enter **Custom** URL in **Redirect URL** section.

12.6.23 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**.
2. To let users self-register, select **Allow Guest Users to Self-Register**.
3. Select the option you want to use for self-registration.

    - Select **Free Wi-Fi** to allow free Wi-Fi access to users. Click on the "gift" icon to configure the free Wi-Fi. With free Wi-Fi 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 Wi-Fi access. Click on the "$" icon to configure paid Wi-Fi. With paid Wi-Fi, you can do all of the things listed in free Wi-Fi 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 Wi-Fi welcome message.
- Enter the **SMS Content** you want to include as part of the paid Wi-Fi 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 Wi-Fi and the paid Wi-Fi cases. The only additional task is that you need to define the initial period for which the Wi-Fi 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 do not 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 vie 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.

5. Click on the Guestbook icon.

   Info: This opens a new Guest Manager tab in your browser, where you can define new guest Wi-Fi accounts. For details on how to configure Guestbook, see the *Guest Manager User Guide*.
6. Click **Save**.
7. Click **Save** on the **Plugin & QoS** page to save the plugin settings.
8. Save the SSID.

12.6.24 Configure Passcode Through SMS Plugin

In this method, users provide their mobile numbers and receive a passcode for Wi-Fi 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**.
2. Select **Passcode through SMS** and click the edit icon (pencil) to edit settings.
3. Select the limit for the maximum number of devices per user.
4. Select the **Passcode Length** and the **Passcode Validity**.

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. Enter the **DLT Template ID**. The DLT Template ID is provided by the SMS service provider.
8. Configure the **Quality of Service** settings and the **Redirect URL**. See Common Plugin Settings.
9. Click **Save**.
10. Click **Save** on the **Plugin & QoS** page to save the clickthrough settings, and then save the SSID.

12.6.25 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**.
2. Select **Webform** and click the edit icon (pencil) to edit settings.
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**.
6. Click **Save** on the **Plugin & QoS** page to save the clickthrough settings.
7. Save the SSID.

12.6.26 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**, CV-CUE 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**.
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).

   Info: The **External RADIUS Settings** window appears. For details on these settings, see Common Plugin Settings.
4. Select the **Authentication Server**.

   Info: 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 sever and Secondary Authentication and Accounting servers as well.
5. Select the **Accounting Server**.

   Info: 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**.
9. Click **Save** on the **Plugin & QoS** page to save the plugin settings, and then save the SSID.

12.6.27 QoS Settings for Plugins

Field	Description
Login Timeout	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 Wi-Fi service. "0" 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.
Blackout Time	The time period for which a user cannot log in to the portal after the last successful login has timed out. "0" 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.
Redirect URL	The URL of the page to which the guest user must be redirected to on successful login from the portal using the plug-in.
Max Download Bandwidth	Maximum download bandwidth, in Kbps or Mbps, for this plug-in on the portal.
Max Upload Bandwidth	Maximum upload bandwidth, in Kbps or Mbps, for this plug-in on the portal.

12.6.28 Configure Third-Party Hosted Captive Portal

To configure Third-Party Hosted Captive Portal settings:

1. Navigate to **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**.
4. To configure basic settings within Third-Party Hosted do the following:
   a. Select **With RADIUS Authentication**.

      Info: 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**.
   d. Enter a **Shared Secret** for SSID-external portal communication.
   e. Select **HTTPS Redirection** if you wish to move to secure version of HTTP.

Info: 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**.

   Info: 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**.

   c. Specify **Login Timeout**, in minutes, for which a wireless user can access the guest network after submitting the portal page.

   Info: 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.

   Info: 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**.

12.6.29 Request and Response Parameters

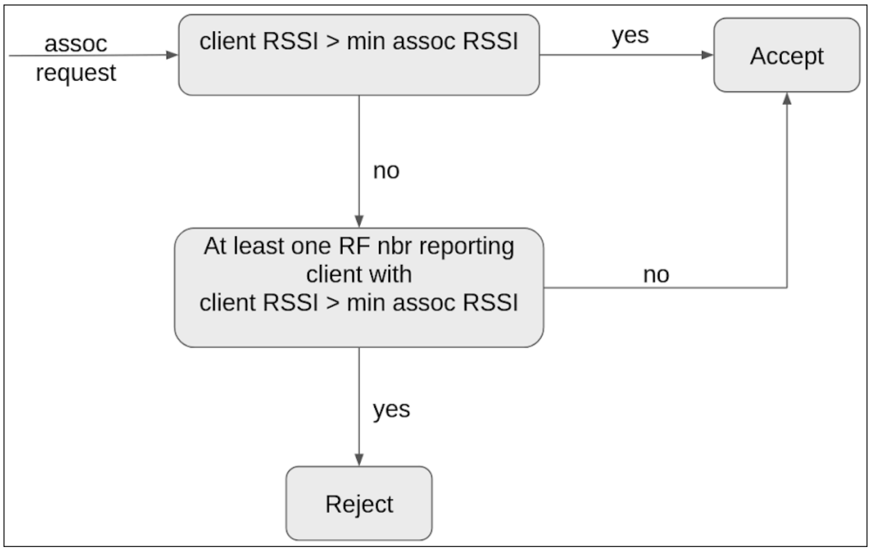
Request Attributes	Description
Request Type	Field name for request type field.
Challenge	Field name for random text used for authentication.
Client MAC Address	Field name for the MAC address of the client.
Access Point MAC Address	Field name for MAC address of the access point that is communicating with the external portal.
Access Point IP Address	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.
Access Point Port Number	Field name for the AP port number on which the AP and external server communicate.
Failure Count	Field name for the count of the number of failed login attempts.
Requested URL	Field name for the requested URL that is the URL requested by the client through the AP, to the external server.
Login URL	Field name for the login URL.
Logoff URL	Field name for the logoff URL.
Remaining Blackout Time	Field name for the remaining blackout time.
Service Identifier	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.
Response Attributes	
Challenge	Field name for the challenge
Response Type	Field name for the response type.
Challenge Response	Field name for the challenge response.
Redirect URL	Field name for the redirect URL
Login Timeout	Field name for login timeout.
User name	Field name for user name.
Password	Field name for password.

12.7 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.

Figure 12-1: Minumim RSSI-based Association



The flowchart depicts the logic for minimum RSSI-based association. When an AP receives an association request, it first checks if the client RSSI is more than te minimum association RSSI. If it is more, then the AP accepts the association request from the client. However, if the client RSSI is less than the minimum association RSSI, then the AP checks if any neighbor AP is reporting the a higher RSSI for the same client. If yes, the AP rejects the association request because the neighbor AP is reporting a better RSSI for the client. If the neighboring AP is not reporting a better RSSI for the client, then the AP accepts the association request.

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.

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 does not 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**.

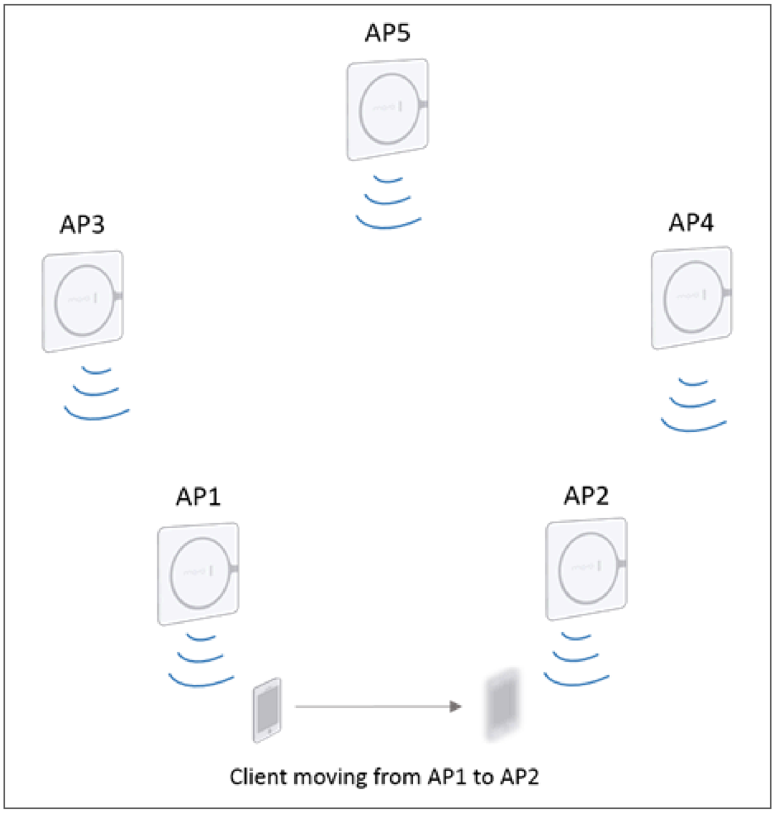
Bonjour is an Apple protocol designed to make Bonjour-enabled devices and services easy to use and configure over the network. Bonjour makes heavy use of broadcast and is essential for Apple products. You can select **Allow Bonjour** to automatically apply an exemption.

IGMP Snoopingis 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.

Target Wake Time (TWT) is one of the advanced features of Wi-Fi 6. It enables access points (AP) and stations (STAs) to negotiate schedules for active and sleep durations.

12.7.1 802.11k - Use Case

Consider a client moving from one AP (AP1 in the figure) 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.

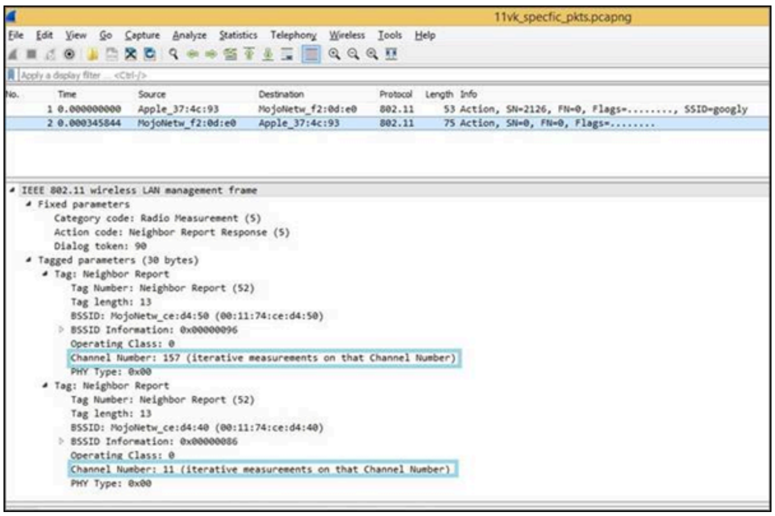


The IEEE 802.11k amendment, also called Radio Resource Measurement (RRM), defines methods allowing stations to inform each other about their respective radio frequency (RF) environments. That way, they can make faster and better informed decisions on roaming. With 802.11k, a client can request an Arista AP to send a Neighbor Report. In case of the client in the above figure, it requests a Neighbor Report from AP1. It is 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 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 7: Scan Times with and without 802.11k

5GHz (w DFS)	All Channels	11k Neighbors
Channels to scan	21	4
Scan Time	2.1s	400ms

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.



12.7.2 802.11v - 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 is 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 is the client saying, “60 seconds is too short. Let us 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.

12.7.3 Configure RF Optimization in SSID Profile

To enable RF related optimizations navigate to **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**, **802.11v BSS Transition** and **802.11r** (Fast Transition). By default these 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 all bands - Both 2.4 GHz, 5 GHz, and 6 GHz**.
   - 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 does not disconnect the client (but waits for the client to disconnect on its own).
   - If you enable 802.11r, you can optionaly enable **Mixed Mode**. By enabling Mixed Mode, you allow both 802.11r capable and incapable clients (clients that do not support 802.11r) to connect to this SSID.
3. Select **Proxy ARP and NDP**.

   Info: 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**.

   Info: It is applicable only for Hotspot 2.0. If you enable this option, 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. Select **Target Wake Time**, **Broadcast/Multicast Control**, **IGMP Snooping**.
6. Click **Save**.

12.7.4 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

Feature	Description	Default	Range
IGMP Snooping	Enables IGMP Snooping	Enabled	
IGMP Snooping Exception List	Allow multicast to be delivered without client sending an IGMP Report (Join)		30 Max

Table 3 – IGMP Snooping Restrictions

Feature	Restrictions
IGMP Snooping	Enabled by default Based on client IGMP Report (Join) Enable – blocks multicast, Disable – forwards all multicast Applies to multicast going from Ethernet to wireless Independent of multicast/unicast conversion Snoop table forwarded when client roams AP does not send IGMP Query
IGMP Snoop Protected Address	Max 30 multicast addresses Internal protected addresses 224.0.0.1/24 – query for all systems 224.0.0.22/24 – IGMP v3 addresses Not converted to unicast even if **Convert Mulicast to Unicast** is enabled. All packets forwarded on match even if no client sends an IGMP Report to join

12.7.5 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 **SSID** > **RF Optimization.**
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**.

   Info: 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**.

12.7.6 Target Wake Time

Target Wake Time(TWT) is one of the advanced features of Wi-Fi 6. It enables access points (AP) and stations (STAs) to negotiate schedules for active and sleep durations.

TWT is beneficial for the following reasons:

- Pre-defined schedules allow STAs to manage their power consumption more effectively, thus helping conserve energy. STAs need to wake up only during the designated Service Periods (SP) to transmit and receive data.
- TWT can help reduce contention by time slicing. Individual STAs or STA groups can be assigned different SPs by the AP to ensure that contention within a BSS is limited to only the clients that have overlapping SP.

TWT Modes

TWT can be deployed in two modes: **Individual** and **Group**. Individual TWT allows each STA to independently negotiate one or more TWT sessions with its AP.

In Group TWT, the AP creates a set of schedules and multiple STAs can be assigned to the same schedule. For example, there can be a ‘VoIP schedule’ and STAs with VoIP sessions can join it.

Note: The Individual TWT mode is mandatory for Wi-Fi 6 certification of APs and STAs.

To understand more about TWT protocol, refer to TWT Help Article.

Enable TWT in CV-CUE

To enable TWT:

1. Go to **CONFIGURE** > **WiFi.**
2. Navigate to your SSID and go to the **RF Optimization** tab.
3. Select **Individual** under the **Target Wake Time** setting and click **Save.**

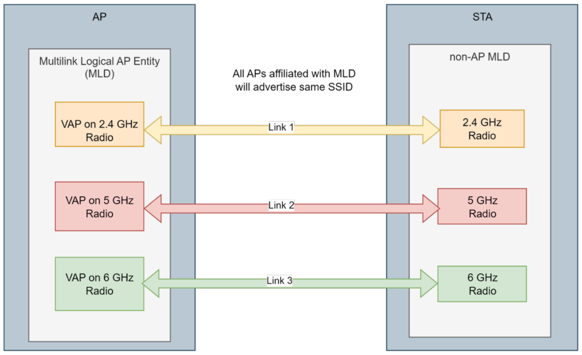
12.8 SSID WiFi 7 Setting - Multi-Link Operation

The **WiFi 7** tab contains MLO setting.

Multi-Link Operation

Until now, a multi-band client (for example, a phone with 2.4, 5, and 6 GHz radios) could connect to an AP using only one of the bands. Therefore, only one connection link formed between the client and the AP. Multi-link Operation (MLO) is the capability of the client and the AP to connect to more than one band simultaneously establishing multiple links. The clients that are capable of communicating with each other over multiple radio links at the same time are called Multi-Link Devices (MLD).

Establishing multiple links of communication reduces access latency and enables bandwidth aggregation for increased throughput. With MLO, Wi-Fi 7 APs broadcast the same SSID on all radios (2.4, 5, and 6 GHz), and MLO-capable clients can connect to all bands or a combination of bands simultaneously.



Enable MLO

MLO is a per-SSID configuration.

To enable MLO for the selected SSID:

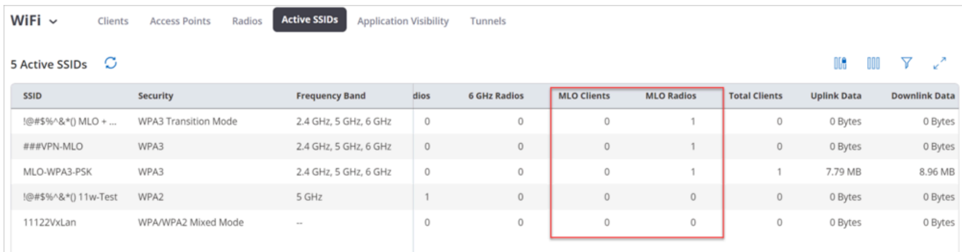
1. Go to **CONFIGURE > WiFi > SSID.**

2. Open a new SSID or edit an existing one.
3. Select the WiFi 7 tab and select the **Mutli-Link Operation** checkbox.

4. Save the settings.

Verification

You can verify active MLO radios and MLO clients by navigating to **MONITOR > WIFI > Active SSIDs.**



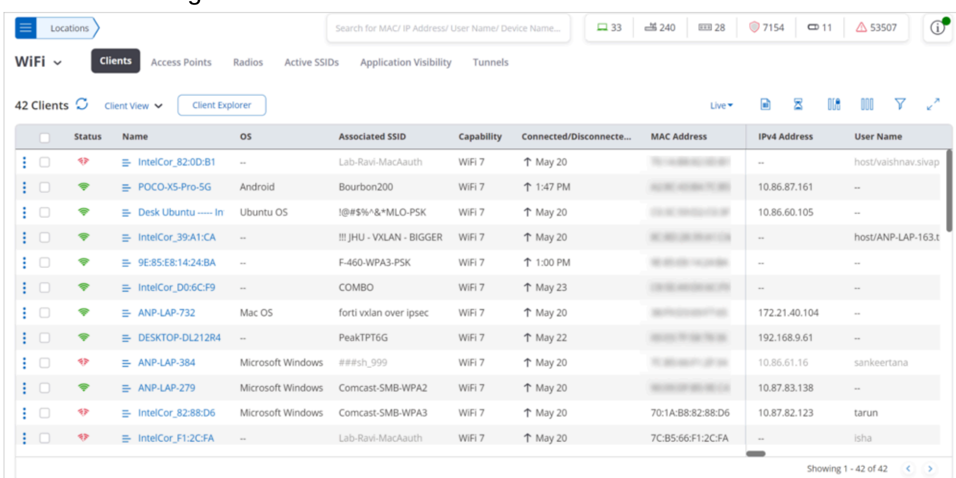
SSID	Security	Frequency Band	dios	6 GHz Radios	MLO Clients	MLO Radios	Total Clients	Uplink Data	Downlink Data
!@#$%^&*() MLO + ...	WPA3 Transition Mode	2.4 GHz, 5 GHz, 6 GHz	0	0	0	1	0	0 Bytes	0 Bytes
###VPN-MLO	WPA3	2.4 GHz, 5 GHz, 6 GHz	0	0	0	1	0	0 Bytes	0 Bytes
MLO-WPA3-PSK	WPA3	2.4 GHz, 5 GHz, 6 GHz	0	0	0	1	1	7.79 MB	8.96 MB
!@#$%^&*() 11w-Test	WPA2	5 GHz	1	0	0	0	0	0 Bytes	0 Bytes
11122VxLan	WPA/WPA2 Mixed Mode	--	0	0	0	0	0	0 Bytes	0 Bytes

MLO Client Details

The client view tab is divided into 2 grids, client view and link view.

Client View

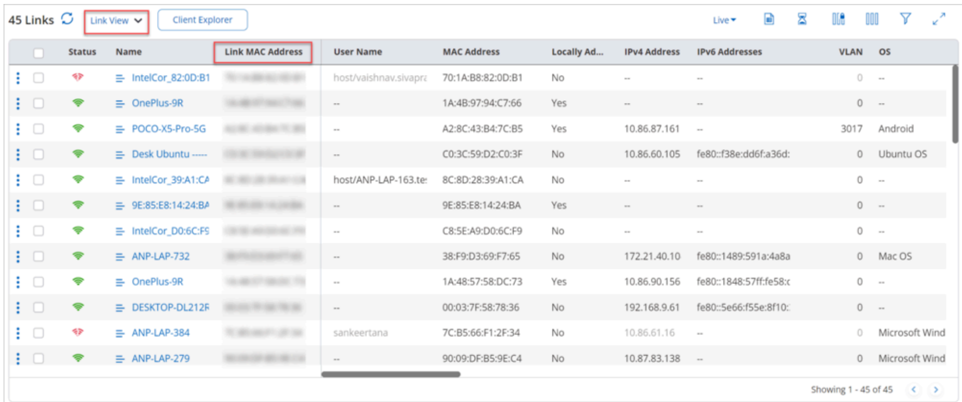
The client view grid contains information about the clients connected to the AP.



Status	Name	OS	Associated SSID	Capability	Connected/Disconnecte...	MAC Address	IPv4 Address	User Name
	IntelCor_82:0D:B1	--	Lab-Ravi-MacAauth	WiFi 7	May 20	[illegible]	--	host/vaishnav.sivap
	POCO-X5-Pro-5G	Android	Bourbon200	WiFi 7	1:47 PM	[illegible]	10.86.87.161	--
	Desk Ubuntu ----- In	Ubuntu OS	!@#$%^&*MLO-PSK	WiFi 7	May 20	[illegible]	10.86.60.105	--
	IntelCor_39:A1:CA	--	!!! JHU - VXLAN - BIGGER	WiFi 7	May 20	[illegible]	--	host/ANP-LAP-163.t
	9E:85:E8:14:24:BA	--	F-460-WPA3-PSK	WiFi 7	1:00 PM	[illegible]	--	--
	IntelCor_D0:6C:F9	--	COMBO	WiFi 7	May 23	[illegible]	--	--
	ANP-LAP-732	Mac OS	forti vxlan over ipsec	WiFi 7	May 20	[illegible]	172.21.40.104	--
	DESKTOP-DL212R4	--	PeakTPT6G	WiFi 7	May 22	[illegible]	192.168.9.61	--
	ANP-LAP-384	Microsoft Windows	###sh_999	WiFi 7	May 20	[illegible]	10.86.61.16	sankeertana
	ANP-LAP-279	Microsoft Windows	Comcast-SMB-WPA2	WiFi 7	May 20	[illegible]	10.87.83.138	--
	IntelCor_82:88:D6	Microsoft Windows	Comcast-SMB-WPA3	WiFi 7	May 20	70:1A:B8:82:88:D6	10.87.82.123	tarun
	IntelCor_F1:2C:FA	--	Lab-Ravi-MacAauth	WiFi 7	May 20	7C:B5:66:F1:2C:FA	--	isha

Link View

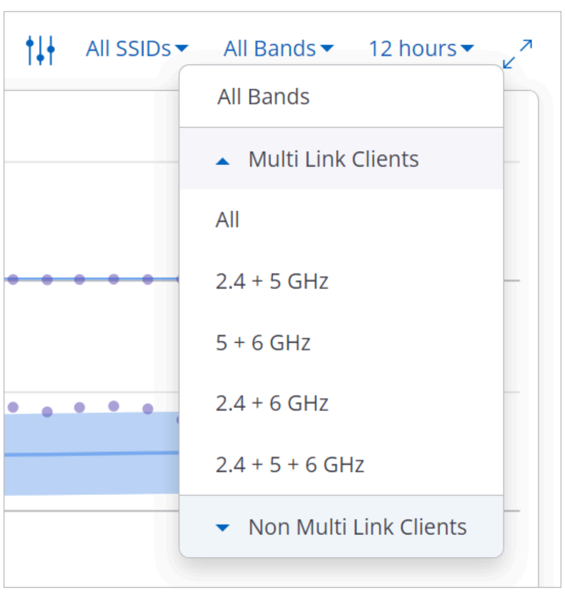
The link view contains information about the links established between client and AP. Each MLO link is denoted by an entry in the link view grid. The link view grid contains the Link MAC Address, which is a unique identifier for each link, along with other client details.



You can view the same information in a graphical format through the Link Explorer.

Wi-Fi Analytics for MLO Clients

The **Frequency Band Filter** on all analytics charts and widgets is enhanced with filters for **Multi Link Clients** and **Non Multi Link Clients.** You can filter the analytics data on the basis of MLO Clients and non-MLO clients. Within MLO Clients, you can further drill down the data on the basis of All Bands or a combination of selected bands.



The following analytics widgets are enhanced with MLO filters:

- Overview Dashboard
- Connectivity Chart:

- Baseline - Clients Affected by Failure
- Performance Charts:
    - Baseline - Clients Affected by Poor Performance
    - Clients by Avg. Data Rate
    - Clients by RSSI
    - Clients by Retry Rate %
    - Network Usage
- Application Charts:
    - Application Experience
    - Baseline - % Poor Application Experience

12.9 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 have 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 does not 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 8: Arista to RADIUS-Mapping of Bandwidth Control Attributes

Arista Attribute	RADIUS Attribute
Per-user download limit	5
Per-user upload limit	6

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 Wi-Fi 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, Wi-Fi Multimedia (WMM) is mandatory. For 802.11n APs, if you do not 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**, CV-CUE 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 Wi-Fi 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.

DSCP / TOS / 802.1p Class of Service	802.11e/WMM access category
0 (Background)	1 (Background)
1 (Best Effort)	0 (Best Effort)
2 (Excellent Effort)	3 (Best Effort)
3 (Critical Apps)	4 (Video)
4 (Video)	5 (Video)
5 (Voice)	6 (Voice)
6 (Internetwork Ctrl)	7 (Voice)
7 (Network Ctrl)	7 (Voice)

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.

802.1p Class of Service	DSCP	802.11e/WMM Access Category
1	0	0
0	10	1
0	18	2
2	0	3
3	26	4
4	34	5
5	46	6
6	48	7

12.9.1 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** > **WiFi** > **SSID** > **Traffice 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 bandwith 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 bandwith 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. Maximum threshold for minimum as well as maximum data rate is 54 Mbps.
   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**.

12.9.2 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** > **WiFi** > **SSID** > **Traffice Shaping and QOS.**
2. Scroll down and Select **QoS** to define your own QoS settings for Wi-Fi multimedia on the SSID profile.
3. Select **Enforce WMM Admission Control**.

   Info: 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**.

   Info: 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.

   Info: 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.

Info: 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**.

12.10 SSID Scheduling

If you want to limit the duration for which the SSID is active, you can define a schedule for the SSID.

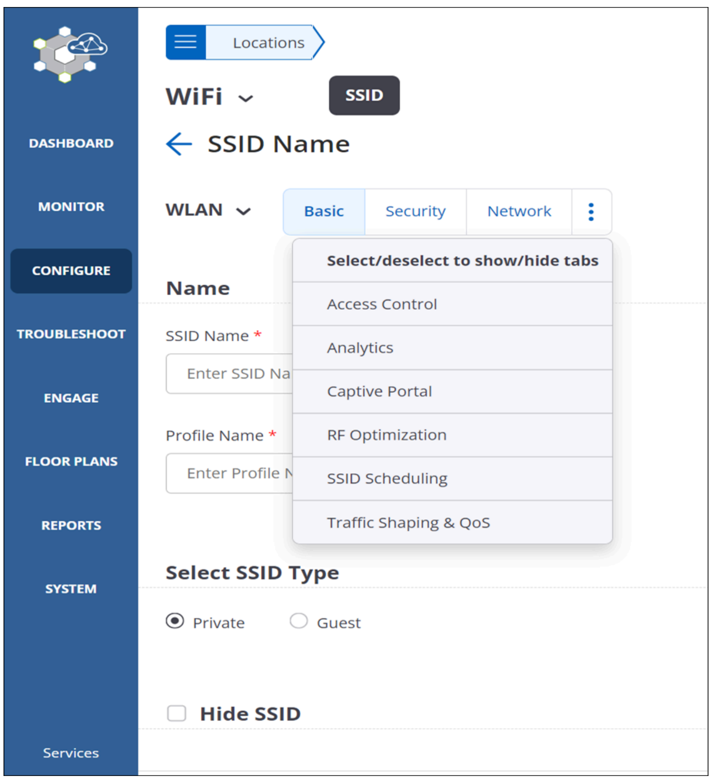
You can also specify if an SSID is to be permanently active or valid for only a limited time duration. This could be useful if, for example, you have an event coming up for which you want to use a special Guest SSID with a different splash page. Another use case might be to restrict employee SSID use to office hours. When you enable **Select Timeslot**, CV-CUE 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**.

12.10.1 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** > **WiFi** > **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.

   Info: 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.

7. Select **Select Timeslot**.
8. Select the active timeslots for the SSID.

   Info: 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**.

12.11 Hotspot 2.0

Hotspot 2.0 is a standard for public-access Wi-Fi that enables seamless roaming among Wi-Fi networks and between Wi-Fi and cellular networks. With Hotspot 2.0, Passpoint-certified mobile devices such as laptops and smartphones can automatically discover and connect to Wi-Fi networks without the need of signing in manually. It is based on IEEE 802.11u standard for Interworking with External Networks.

Hotspot 2.0 works only with WPA2 802.1x, WPA3 Enterprise or WPA3 Transition Mode. Ensure that you have configured the RADIUS Server and 802.11w Management Frame Protection is set as Required or Optional.

12.11.1 Hotspot 2.0 Settings

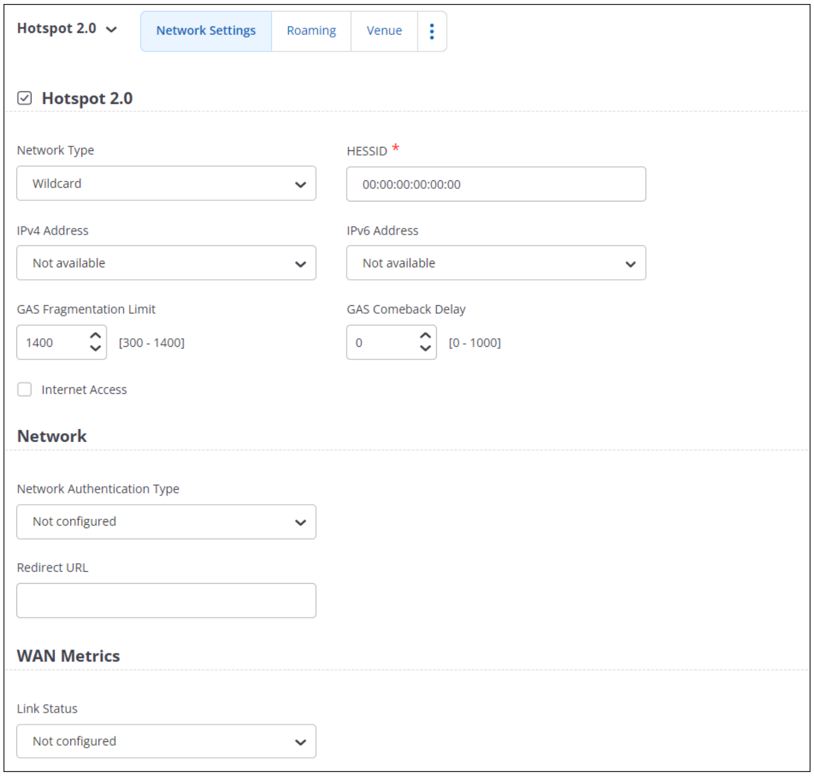
The Hotspot 2.0 settings for an Arista AP are divided into Network Settings, Roaming, Venue, Domain, NAI Realms, Friendly Names, Connection Capabilities and QoS Mapping.

This topic contains the following subtopics:

- Hotspot 2.0 Network Settings
- Hotspot 2.0 Roaming Settings
- Hotspot 2.0 Venue Settings
- Hotspot 2.0 Domain Settings
- Hotspot 2.0 NAI Realms Settings
- Hotspot 2.0 Friendly Name Settings
- Hotspot 2.0 Connection Capabilities Settings
- Hotspot 2.0 QoS Mapping Settings

12.11.1.1 Hotspot 2.0 Network Settings

Network setting tab consists of settings related to network configuration.



Provide the following details for the network settings:

- **Network Type:** The type of the network.
- **HESSID:** HESSID stands for Homogenous Extended Service Set Identifier. It is used to identify hotspot AP. APs with the same HESSID have the same hotspot configuration.
- **IPv4 Address:** Select the appropriate IPv4 Address from the available options.
- **IPv6 Address:** Select the appropriate IPv6 Address from the available options
- **GAS Fragmentation Limit:** The maximum allowed size, in bytes, for the GAS response frame above which frame fragmentation needs to be done. Default value is 1400 bytes.
- **GAS Comeback Delay:** The comeback delay, in milliseconds, between initial GAS response and first comeback request.
- **Internet Access:** Select this checkbox if the network provides internet access to the client through the AP.
- **Network Authentication Type:** Select the network authentication type from one of the following options:
  - Terms and conditions - Select this option if the network requires the user to accept terms and conditions.
  - Online enrollment - Select this option if you want the user to enroll online.
  - Https redirection- Select this option if the user is redirected for authentication.
  - DNS redirection- Select this option if the network supports DNS redirection.
  - Not configured- Select this option if you don't want to provide specific information when the client queries about network authorization type.

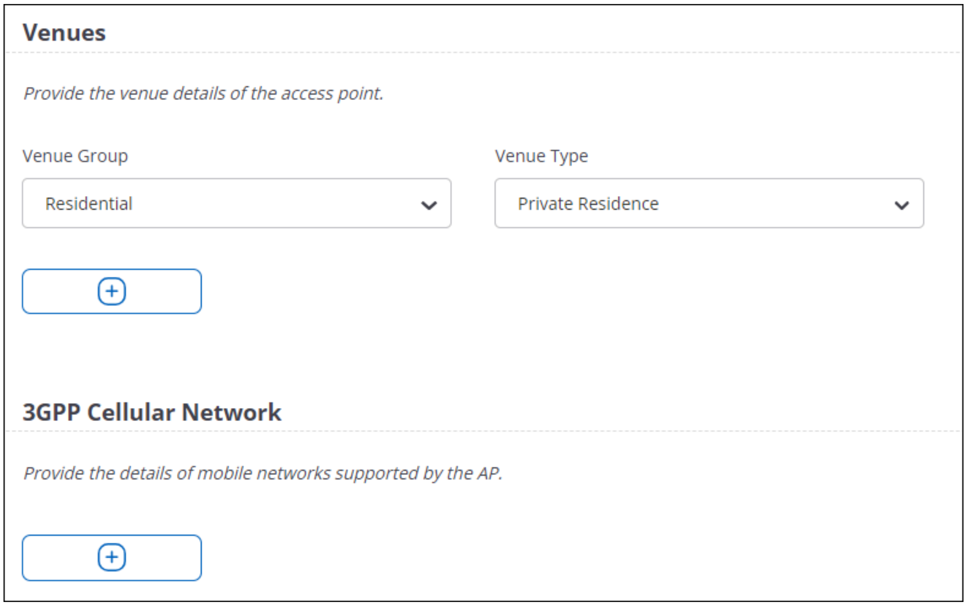
  You can also provide the **Redirect URL** if you want the client to be redirected after connecting to the access point.
- **Link Status:** Select the status of the link
- **Symmetric Link Status:** Select the Same option if the uplink and downlink speeds are the same. Select the Different option if the uplink and the downlink speeds are different.
- **Uplink Speed:** Enter the uplink speed in Kbps or Mbps.
- **Downlink Speed:** Enter the downlink speed in Kbps or Mbps.

12.11.1.2 Hotspot 2.0 Roaming Settings

Enter the roaming consortium list using hex characters. Roaming consortium consists of one or more organization identifiers that are unique hexadecimal strings.

12.11.1.3 Hotspot 2.0 Venue Settings

Under the **Venue** tab, provide the venue details and 3GPP Cellular Network Details of the access point.



Venue Details

Venue details consist of venue groups and venue types. Select the venue group from the available options and based on the venue group, select your venue type.

3GPP Cellular Network

Provide the list of mobile networks supported by the access point.

12.11.1.4 Hotspot 2.0 Domain Settings

Under the **Domain tab**, provide the list of Hotspot 2.0 operator domain names.

12.11.1.5 Hotspot 2.0 NAI Realms Settings

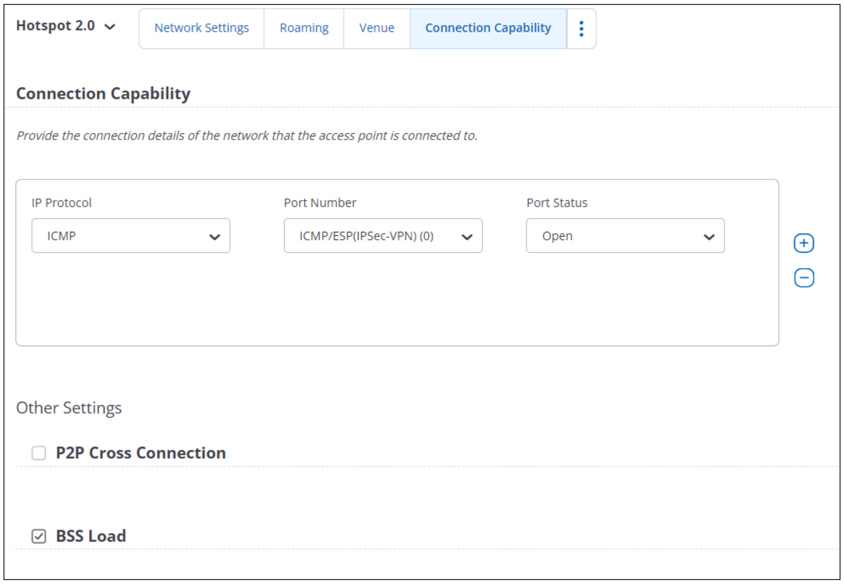
The NAI Realm List corresponds to the NAI realm element. The NAI realm element provides a list of network access identifier (NAI) realms corresponding to service providers whose networks are accessible through the AP. A list of one or more **EAP** Methods is optionally included for each NAI realm.

12.11.1.6 Hotspot 2.0 Friendly Name Settings

Under **Friendly Name**, enter the friendly name of the Hotspot 2.0 operator in different languages along with their language code. You can provide up to 32 operator friendly names.

12.11.1.7 Hotspot 2.0 Connection Capabilities Settings

Under connection capability, enter the connection capability details of the network. Connection capability settings signify the capabilities of the wired network the AP is connected to.



Specify the protocols supported by the network connection and the corresponding port numbers and the port status.

P2P Cross Connection

Enable P2P Cross Connection to allow the client to bridge the Wi-Fi direct network and the infrastructure network.

BSS Load

Enable BSS Load to include BSS Load element in the beacons and probe responses. The BSS Load element contains information on the number of currently associated stations and traffic levels in the BSS.

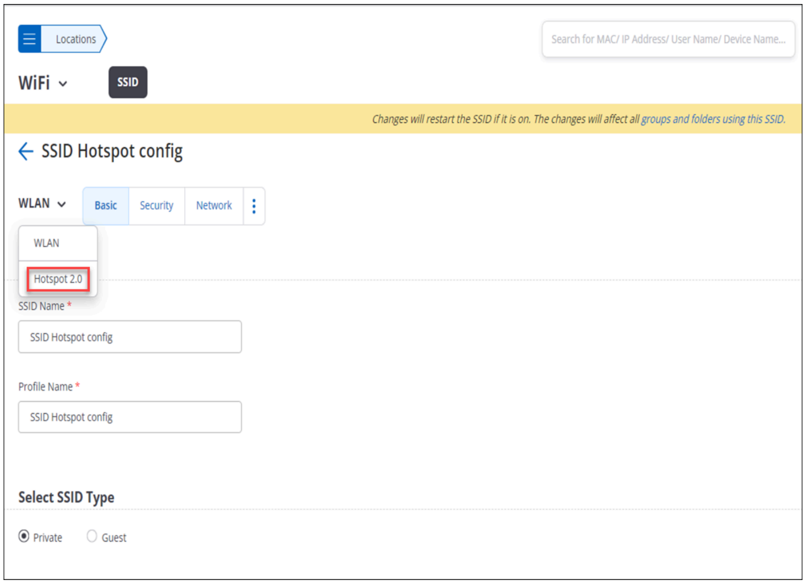
12.11.1.8 Hotspot 2.0 QoS Mapping Settings

Enter the **QoS Mapping**, only if required. The DSCP exception indicates the priority to be assigned when the specified DSCP value is detected in data packets. The value 255 indicates that the row is ignored.

12.11.2 Configuring a SSID with Hotspot 2.0

To configure a SSID profile with Hotspot 2.0:

1. Click **CONFIGURE** > **WiFi** > **SSID.**
2. Click **Add SSID.**
3. Enter the **Profile Name** and **SSID Name.**
4. Under the Security section, select **WPA2, WPA3 or WPA3 Transition Mode** as the Security Level for Association.
5. Select **802.1X** and configure the RADIUS Settings.
6. Set **802.11w Management Frame Protection** as **Optional** or **Required.**
7. Configure the required Network, Captive Portal, Firewall, and Traffic Shaping & QoS settings.
8. Click **Hotspot 2.0** from the WLAN drop-down menu.



9. Enable **Hotspot 2.0.**
10. Configure all the Hotspot 2.0 settings.
11. Save and turn on the SSID.

12.11.3 Configuring a Wi-Fi Profile for an AP Connecting to Online Sign-up Servers

A Hotspot 2.0 compatible mobile client can subscribe to online sign up servers from various service providers through a Hotspot 2.0 compliant Arista AP. The mobile client can choose an online service from the list of available online services and sign up for the chosen service through the Arista AP.

To configure a Wi-Fi Profile for an AP connecting to Online Sign-up Server:

1. Click **CONFIGURE** > **WiFi** > **SSID.**
2. Click **Add SSID.**
3. Enter the **Profile Name** and **SSID Name.**
4. Under the **Security** section, select **Hotspot 2.0 OSEN.**
5. Configure the **RADIUS Settings.**
6. Save the SSID settings.

Note: Proxy ARP and **Disable DGAF** must be selected when you select Hotspot 2.0 OSEN.

12.12 Managing SSID

This chapter contains the following topics:

- Turn an SSID On
- Edit an SSID
- Delete an SSID
- Create a Copy of an SSID

12.12.1 Turn an SSID On

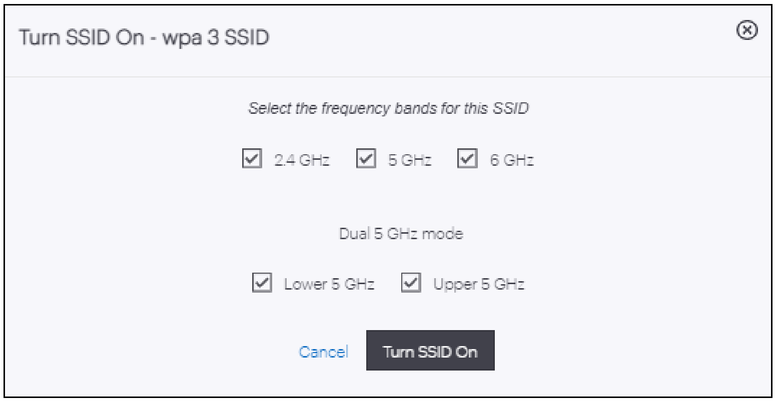
You need to turn an SSID on before it becomes available for access to users.

1. You can turn on a new SSID once you are done configuring it, or you can turn an existing SSID on.

   Choose from:

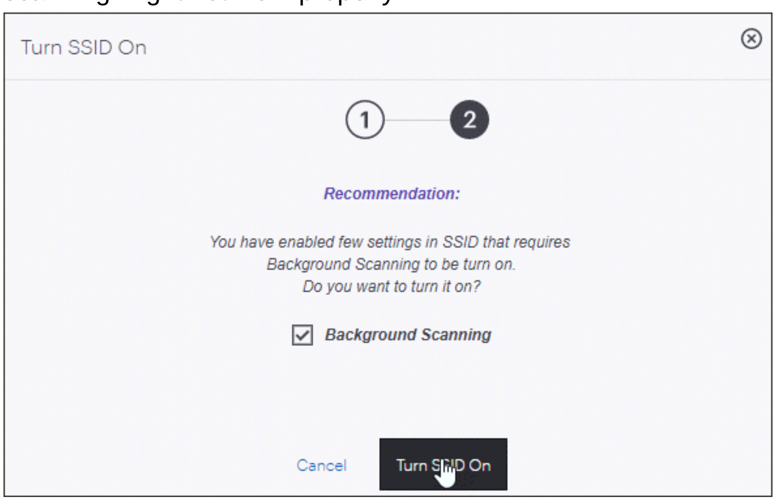
- If you are adding a new SSID, you can click **Save & Turn SSID On** after you are done configuring at least the three mandatory SSID tabs (Basic, Security and Network).
- If you are turning an existing SSID on, just go to **Configure** and click the **OFF / ON** switch on the SSID you want to turn on.

2. Select whether you want the SSID on the **2.4 GHz**, **5 GHz** , or **6 GHz** bands and click **Turn SSID On**. You will also see the Dual 5 GHz mode option with Lower 5 GHz and Upper 5 GHz options in the Turn SSID On page if you have enabled Dual 5 GHz in the Radio Settings tab.



Choose from:

- 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 CV-CUE 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.



12.12.2 Edit an SSID

You can modify an existing SSID.

To edit an existing SSID at a location:

1. Go to **CONFIGURE** > **WiFi** > **SSID.**
2. On the SSID you want to edit, click **Edit** (the pencil icon).
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.

12.12.3 Delete an SSID

You can delete an SSID from a location

To delete an SSID at a location:

1. Go to **CONFIGURE** > **WiFi** > **SSID.**
2. On the SSID you want to delete, click the **Menu** icon (three vertical dots) and select **Delete**.
3. Click **Delete**.

12.12.4 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** > **WiFi** > **SSID.**
2. On the SSID you want to duplicate, click the Menu icon (three vertical dots) and select **Create a Copy**.
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**.

   Choose From:

   - 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.

12.13 Location Based VLAN Mapping

Location-based VLAN mapping takes precedence over SSID VLAN mapping. As VLAN mapping is not inherited, you must map the VLAN ID to VLAN Name for each floor in a location hierarchy.

To enable location-based VLAN mapping:

1. Go to **CONFIGURE** > **WiFi** > **SSID.**
2. Navigate to your SSID and click **Location Based VLAN Mapping** from the three-dot more menu.
3. Add the VLAN name, ID, and provide the location for the mapping.
4. Save the settings.

12.14 Customize SSID Attributes for Location-Specific Overrides

Network Administrators can create SSIDs at any location in CV-CUE, and the same SSID can be inherited from a parent to a child location. The inherited SSIDs, by default, share the same attributes as the parent location. Administrators can override certain attributes of SSID at a child location without breaking the inheritance, so that the entire SSID configuration remains the same, except for the overridden attributes.

Overriding SSID attributes is useful if you want to have the same SSID configurations across your organization but want to have specific attributes for specific locations. For example, you can have the same corporate SSID across your geography but want a different RADIUS server for each location.

Note: Overriding SSID attributes is not supported for floors; it is available only for folders.

Attributes You Can Edit

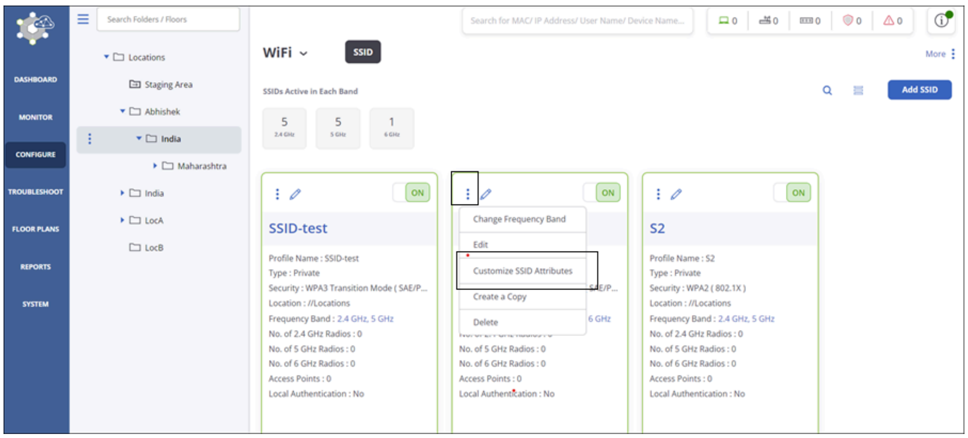
- L2 Tunnel Interface in the Network tab

- VLAN Name
- VLAN ID
- Fallback VLAN ID
- SSID VLAN Mapping
- VLAN Pool
- RADIUS Pool
- RADIUS Authentication and Accounting Servers (Primary and all additional servers)

Override SSID Attributes

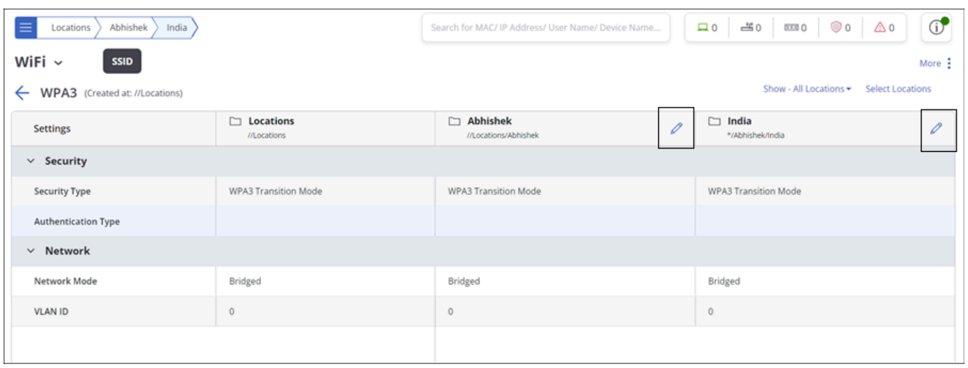
To override any SSID attribute:

1. Select the location and then select **Configure > WiFi.**
2. From the SSID list, select the three-dot menu for the SSID and select **Customize SSID Attributes.**

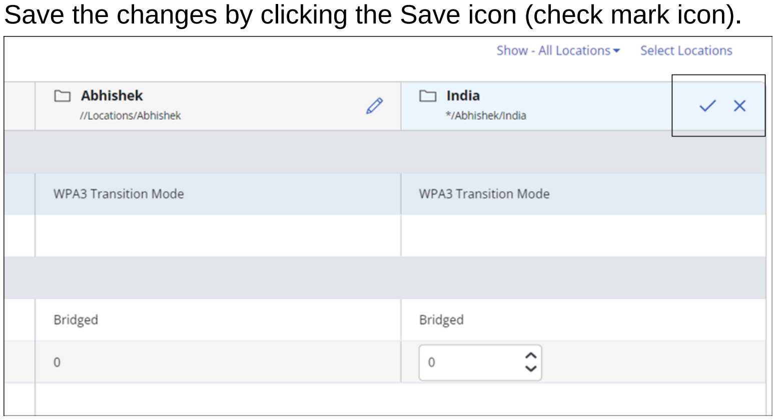


You see a table comparing the SSID attributes of the current folder and its parent folders side-by-side.

3. Select the **Edit** icon to edit the SSID's attributes. You can edit one folder at a time.



4. Save the changes by clicking the Save icon (check mark icon).



Compare Attributes Across Locations

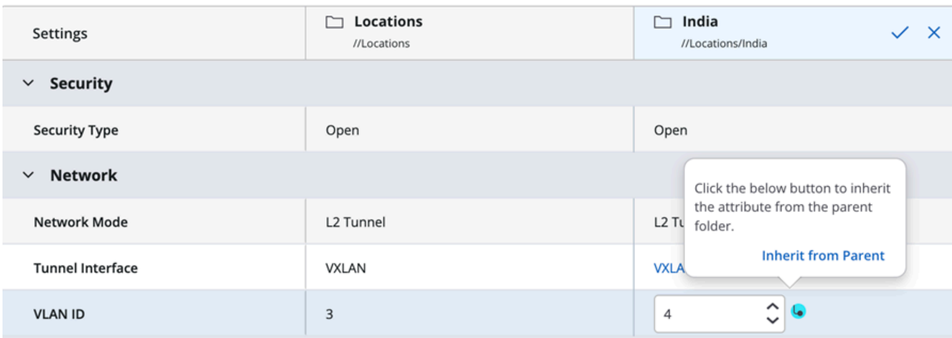
You can select up to 10 locations to compare SSID attributes. To compare attributes across locations:

1. Select the location and then select **Configure > WiFi.**
2. From the SSID list, select the three-dot menu for the SSID and select Customize SSID Attributes.

   You see a table with a side-by-side comparison of the SSID attributes between the current folder and its parent folders. The farthest column towards the right is the current folder. All its parent folders, up to the root folder where the SSID was created, are displayed towards the left of the current folder.
3. Select the Edit icon to edit the SSID's attributes. You can edit one folder at a time.
4. Save the changes by clicking the Save icon (checkmark icon).

Inherit from Parent Vs. Manually Providing the Parent Value

When you click Inherit from Parent, the overridden value is deleted, and the parent value is restored. However, manually entering the same value as the parent folder without using the Inherit from Parent button is treated as an override.



Chapter 13

LAN Port Profile

You can configure LAN Port Profile from **CONFIGURE** > **Network Profile** > **Port** tab.

You can authenticate wired hosts connected to the LAN ports of access points (W-118 and W-318) using 802.1X or MAC-based authentication. You can configure the authentication parameters for each downlink port on the access point (AP) using the LAN Port profile in CV-CUE. The communication happens either through a bridged network or transferred using L2 tunnels.

This chapter contains the following topics:

13.1 Use Case

Consider a home office or a remote office with APs such as W-318 and W-118. Earlier, whatever wired hosts were connected to the AP through the downlink port, they were onboarded to the network without any authentication. It was a security loophole as these external devices could breach into the corporate network as the downlink ports were not secure. Now, the entire office L2 network, including the security perimeter, extends to your AP using VXLAN over IPSec. The network configuration in your office is broadcast in the same VLAN through the internet to your AP. You will have access to the same VLAN and resources that you had in the office. Devices are first authenticated, given a respective VLAN, and then connected to the network.

APs support 802.1x and MAC-based authentication. Administrators can configure each port and control which device gets connected to each port and which authentication will happen on each port.

If users connect any unauthorized device to the downlink port, such devices will not be onboarded to the network. Also, the entire traffic is bridged through the same tunnel to the corporate data center. For example, if you connect a laptop to Port 1 and that port in the AP is configured for a printer, then you cannot connect a laptop to that port. The AP will onboard only the printer through that port.

13.2 Configure Wired LAN Ports

Configure LAN ports to authenticate and manage wired hosts connected through W-118 and W-318 access points. You can create multiple port profiles with different confgurations and apply one profile per port. You can apply one profile to one port and another profile to another port in the same AP.

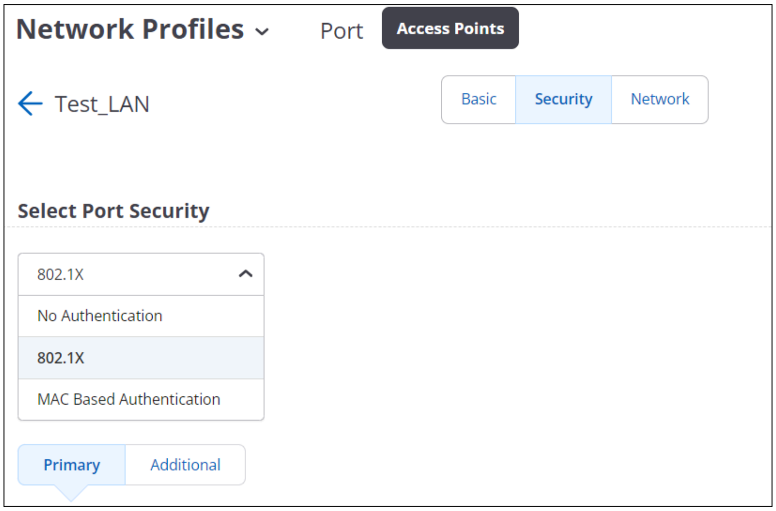
Administrators can manage per-port configuration and shut down each port remotely when needed. CV-CUE displays a view-only information for all the devices connected to the downlink ports in the AP. Only one wired host can connect per port. The wired ports support CoA.

Follow these steps to configure the LAN port profile:

1. Go to **CONFIGURE** > **Network Profile** > **Port**.
2. Click **Add LAN Ports**.
3. Provide a profile name in the **Basic** tab.

4. Click the **Security** tab and select the port security type.

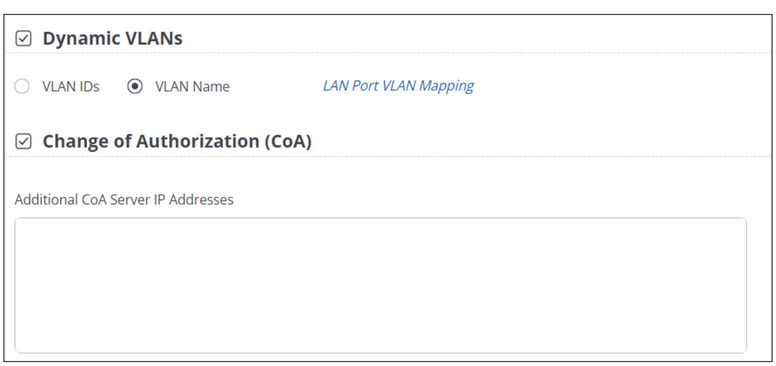
Figure 13-1: LAN Port Security



5. For MAC Based Authentication, provide the username and password.
6. Provide the details of the RADIUS server. You can add one Primary RADIUS server and three additional servers.
7. Configure the other parameters in the **Security** tab:

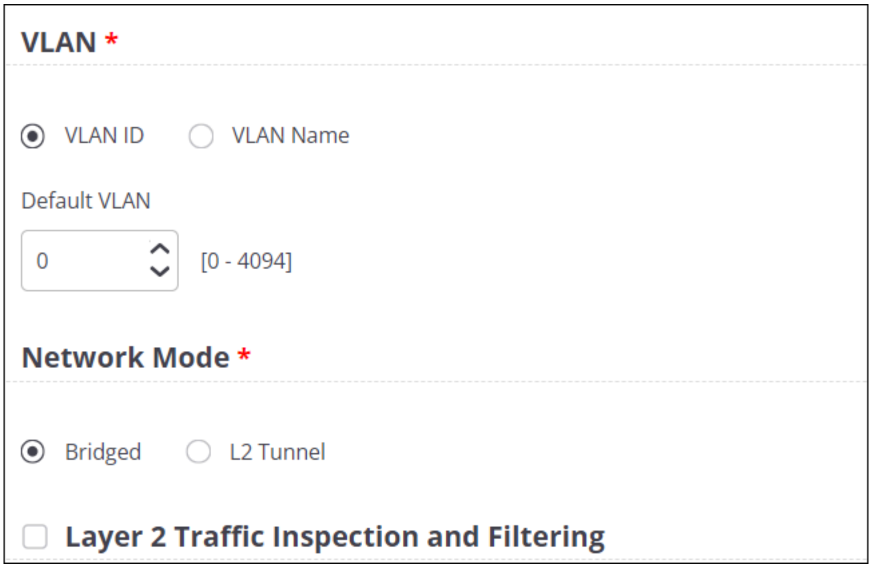
- Retry Parameters: Indicates the frequency of retries to establish connection with a server before switching to the alternative (secondary) server.
    - Attempts
    - Timeout
- Dynamic VLAN: Indicates the VLAN assigned by the RADIUS server. Specify the VLAN name or VLAN ID.
- Change of Authorization (CoA): Indicates the IP addresses of the CoA servers in load-balancer deployments. Specify the IP address of the CoA servers.
- Prefer Primary RADIUS Server: Indicates the fallback to Primary RADIUS Server when it's detected in the network.
    - Dead Time — The time interval for which the primary RADIUS server is marked unreachable after a failover. For example, if the dead time is 30 minutes, the AP will not try to connect with the primary RADIUS server for 30 minutes after failover. The AP will try to connect with the primary RADIUS server after the 30 minutes dead time is over.

Figure 13-2: VLAN Assignment



8. Click the Network tab and provide the VLAN details and the network mode.

Figure 13-3: Network tab configuration



9. Save the settings.

13.3 Assign Port Profile to Ports

After you configure the port profile, you need to manually apply the port profile to each port. Although you can create multiple port profiles, you can apply only one profile per port.

Follow these steps to assign port profiles to ports:

1. Go to **CONFIGURE** > **Device** > **Access Points**.
2. Click the **LAN Ports** tab and then select the **Configure LAN Ports** check box.

Figure 13-4: Assign LAN port profile

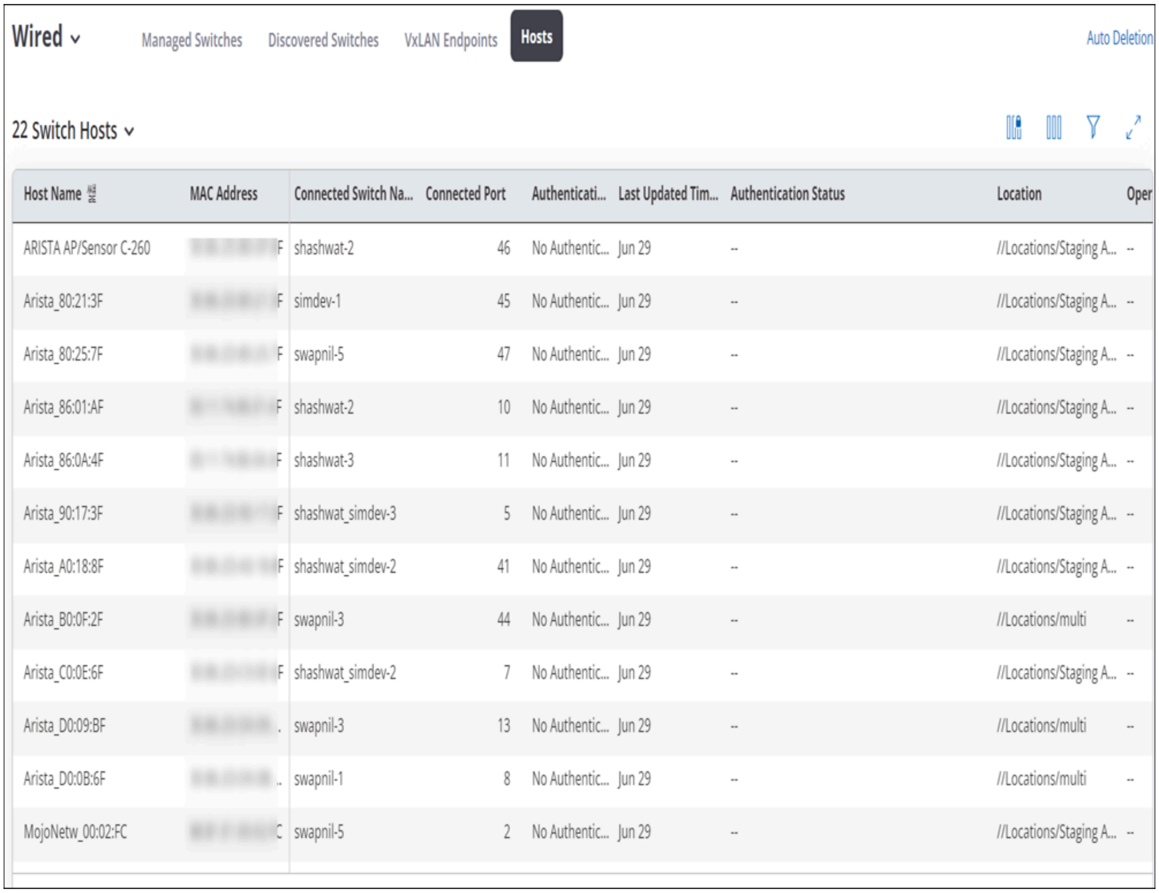
3. Select a port number and apply a profile from the dropdown list.

13.4 Monitor Wired Hosts

You can monitor hosts or clients connected to the wired ports from **MONITOR** > **Wired** > **Hosts**.

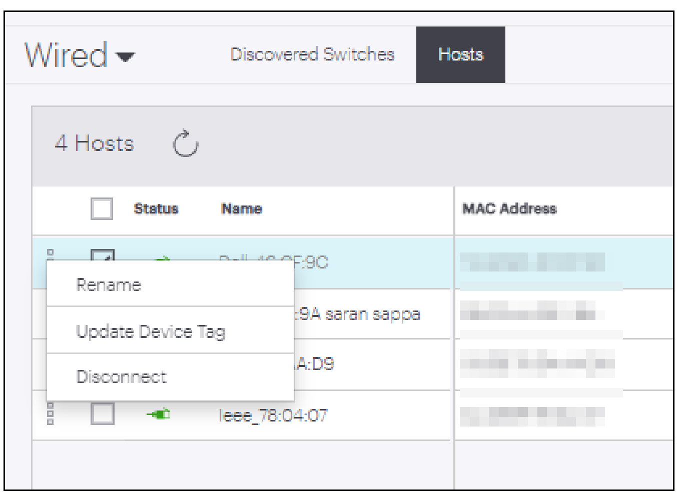
You can view details such as name and MAC address of the host, current connection status, authentication type and others.

Figure 13-5: Wired host listing



For each host, you can perform limited functions such as rename the host, update the device tag, and disconnect the host.

Figure 13-6: Actions for wired hosts



Chapter 14

RADIUS

You can create, edit and delete RADIUS servers on the RADIUS tab.

Enterprise networks often use Remote Authentication Dial-In User Service (RADIUS) 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.

The chapter contains the following topics:

14.1 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** > **Network Profiles** > **RADIUS.**
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 **RadSec** as **ON** to enable the RadSec protocol.
6. 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.
7. 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.
8. Specify a **Shared Secret** key. The primary RADIUS server and the AP identify themselves using the shared secret key.
9. Save the settings.

14.2 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.

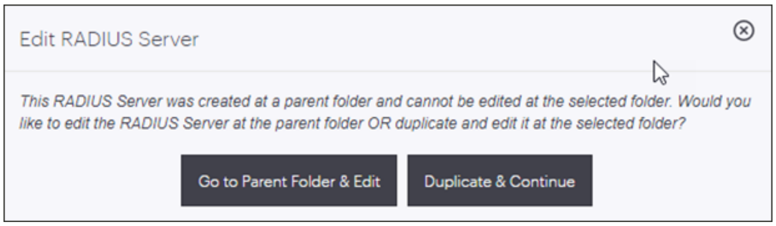
To know more about parameters required in editing RADIUS Settings refer RADIUS Settings Parameters

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**.

   Choose from:

   a. If you are on the location where profile was created, then directly go to step 3.
   b. If you are on the child location and the profile is a inherited profile, then choose the appropriate option.



Option	Description
If you select **GO to Parent Folder and Edit**.	Then perform the Step 2 again and then perform step 3.
If you select **Duplicate & Continue**.	Then a ready to edit duplicate profile gets created on the child location.

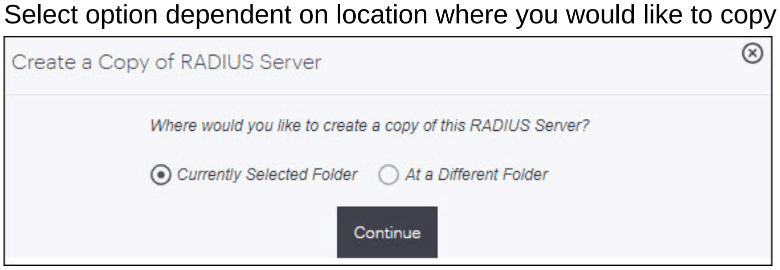
3. Make the necessary changes and click on **Save**.

14.3 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.



4. Click on **Copy**.

14.4 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.

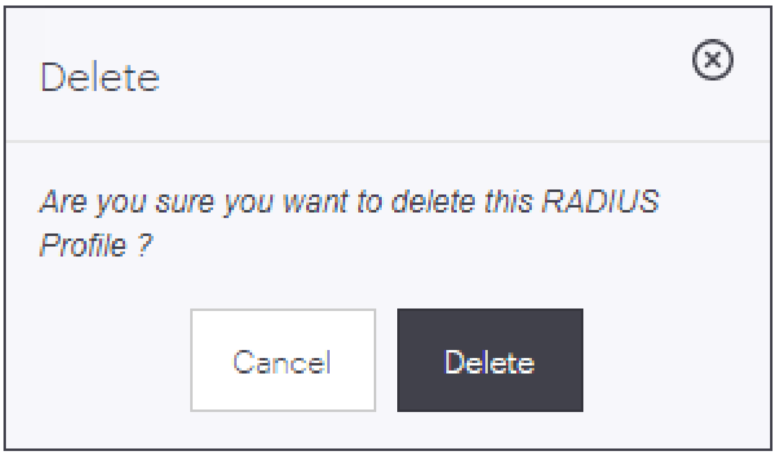
Note: You cannot delete a RADIUS profile that is currently in use on an SSID. You need to disable/ remove the RADIUS profile from the SSID configuration before you delete it.

To delete the RADIUS profile:

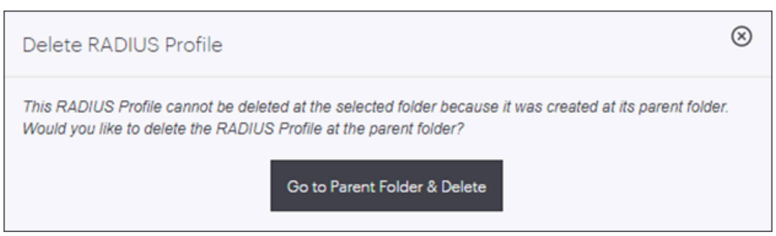
1. Click on the options tab (three vertical dots), of the RADIUS profile that is to be deleted.
2. Select **Delete**.
3. Perform the below location dependent actions:

   Choose from:

   - If you are on the location where you had created the RADIUS profile, then select **Delete**.



   - 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 all the above steps again.

14.5 RADIUS Setting Parameters

The below table provides information related to **RADIUS Settings** parameters.

Field	Description
RADIUS Name	Name for the RADIUS profile.
IP Address/Hostname	IP / Hostname address of accounting RADIUS server.
Authentication Port	The port number at which RADIUS server listens for authentication requests. The value can be between 1 to 65535. The default value is 1812.
Accounting Port	The port number on which to contact the RADIUS accounting server. The value can be between 1 to 65535. The default value is 1813.
Shared Secret	The secret shared between the primary RADIUS server and the AP.

Chapter 15

Role Profile

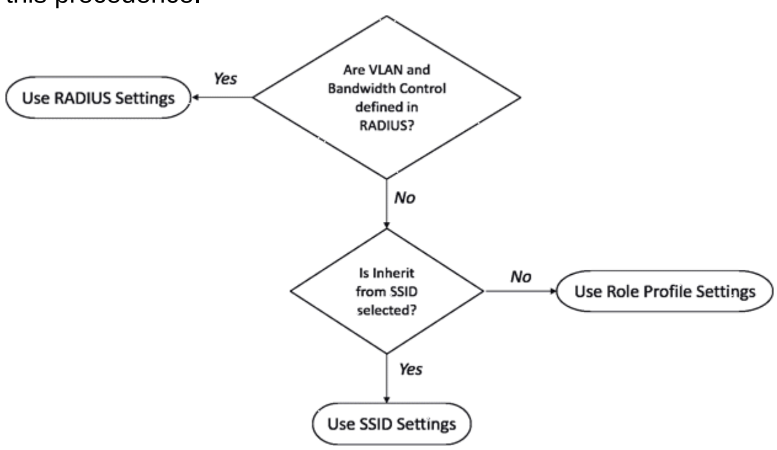
This chapter contains the following topics:

15.1 About 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:

- RADIUS settings, if configured, always trump both Role Profile settings and SSID settings
- 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:

- **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 is 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 do not select the **Inherit from SSID** option and you do not 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.

Setting	SSID Profile	Role Profile	Inherit from SSID	Precedence
VLAN	Yes/No [1]	Yes	Yes/No	Role Profile
VLAN	Yes	No	Yes [2]	SSID Profile
Bandwidth Control	Yes/No	Yes	Yes/No	Role Profile
Bandwidth Control	Yes	No	Yes	SSID Profile
Bandwidth Control	Yes	Yes [3]	Yes	Role Profile/ SSID Profile [3]
Bandwidth Control	Yes	Yes/No [4]	No	Role Profile
Firewall Rules	Yes/No	Yes	Yes/No	Role Profile
Firewall Rules	Yes	No	Yes	SSID Profile
Firewall Rules	Yes	Yes [5]	Yes	Role Profile/ SSID Profile [5]
Firewall Rules	Yes	Yes/No [6]	No	Role Profile
Redirection	Yes	Yes	Yes/No	Role Profile
Redirection	Yes [7]	No	Yes	SSID Profile
Redirection	Yes	No	No	Role Profile

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 do not 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.

15.2 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** > **Network Profiles** > **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**.

15.3 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** > **Network Profiles** > **Role Profile.**
2. For a particular Role Profile, select **Use SSID Settings in absence of Role-Specific Settings** 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**.

15.4 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.

Note: If you do not configure this setting in the Role Profile, then you must select the Inherit from SSID option.

SSID Profile	Role Profile	Inherit from SSID	Precedence	Notes
Yes / No	Yes	Yes / No	Role Profile	If no VLANs are configured in the SSID, the default value of 0 indicating untagged VLAN is set.
Yes	No	Yes	SSID Profile	If Inherit from SSID is not enabled in the role profile, then VLAN settings must be configured in the role profile.

To configure VLAN:

1. Navigate to **CONFIGURE** > **Network Profiles** > **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.

   Info: 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**.

15.5 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.

SSID Profile	Role Profile	Inherit from SSID	Precedence	Notes
Yes / No	Yes	Yes / No	Role Profile	-
Yes	No	Yes	SSID Profile	-
Yes	Yes	Yes	Role Profile / SSID Profile	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.
Yes	Yes / No	No	Role Profile	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.

To configure Firewall Rules:

1. Navigate to **CONFIGURE** > **Network Profiles** > **Role Profile.**
2. Scroll down to **Firewall** section.

Info: 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.

   Note: If you enable Application Firewall, you must select Application Visibility in the SSID profile.
5. In **Default Rule** section provide an **Action**.

   Info: Action can be one of the following, **Allow**, **Block** and **Allow and Mark**.
6. Click **Save**.

If the configuration is correct and saved successfully, CV-CUE displays a success message.

15.6 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.

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.

SSID Profile	Role Profile	Inherit from SSID	Precedence	Notes
Yes / No	Yes	Yes / No	Role Profile	-
Yes	No	Yes	SSID Profile	-
Yes	Yes / No	No	Role Profile	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.
Yes	Yes	Yes	Role Profile / SSID Profile	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.

To configure User Bandwidth Control:

1. Navigate to **CONFIGURE** > **Network Profiles** > **Role Profile.**
2. Scroll down to **User Bandwidth Control** section.
3. Select **Limit the maximun upload bandwith 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 maximun download bandwith 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**.

15.7 Configure Redirection in Role Profile

You can specify whether a user to whom the profile is assigned must be redirected to a static or dynamic 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.

SSID Profile	Role Profile	Inherit from SSID	Precedence	Notes
Yes / No	Yes	Yes / No	Role Profile	-
Yes	No	Yes	SSID Profile	Redirection in Role Profile maps to BYOD or Captive Portal configuration on the SSID Profile. You can configure eith 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.
Yes	No	No	Role Profile	-

To configure redirection,

1. Navigate to **CONFIGURE** > **Network Profiles** > **Role Profile.**
2. Navigate to a role profile and enable **Redirection.** Select **Static 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.
   - Organization: Name of an organization.

- Organization Unit: Name of an organizational unit.

Dynamic URL Redirection

You can redirect onboarding clients to a dynamic URL defined by the RADIUS. If the RADIUS access-accept request has a role and a redirection URL for a client, access points (AP) can redirect such client's HTTP or HTTPS requests.

Prerequisites:

- The access-accept request for a client must contain the URL along with the role that is configured with the dynamic redirection option. The RADIUS must send the URL in the given VSA:
  - Vendor -id : 16901 Arista WiFi
  - Attribute-Id: 8
  - Data-type: string
  - Attribute Name: arista-portal-url
- Add all the hostnames and IP addresses to **Websites That Can Be Accessed Before Authorization.** The website address must include the IP or hostname of the host hosting the Portal.

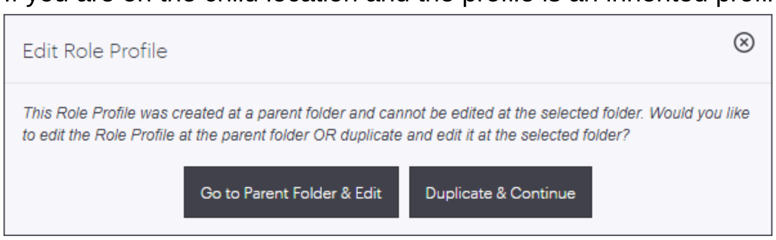
To configure the Dynamic URL, select **Dynamic Redirection** option under **CONFIGURE** > **Network Profiles** > **Role Profile** and add the list of websites that the client can access before authorization.

15.8 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**. Choose from:
   - 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.



Option	Description
If you select **GO to Parent Folder and Edit**	Then perform the Step 2 again and then perform step 3
If you select **Duplicate & Continue**	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

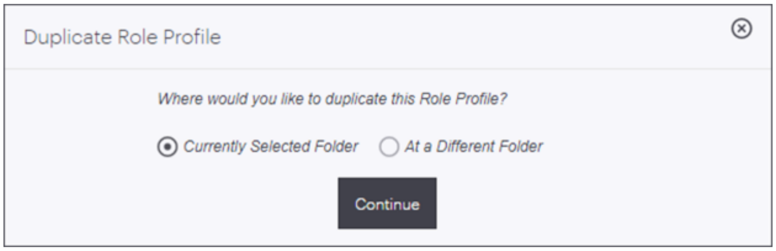
3. Make the necessary changes.
4. Click **Save**.

15.9 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.



Choose from:

- 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**.

15.10 Delete a Role Profile

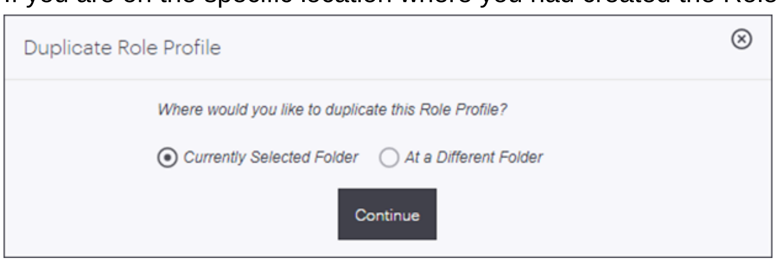
An existing Role profile and a duplicate Role profile both can be deleted using the delete option. The profile once deleted is removed permanently from its specific location and its child location as well. Inherited profiles can not be deleted from the child location. Profiles can be deleted only on the location, where they were created.

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.

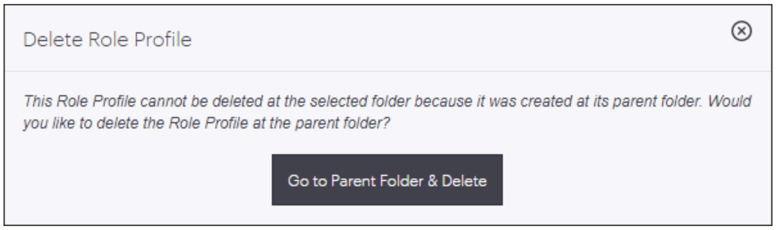
To delete the Role profile:

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**



- 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.

Chapter 16

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 Wi-Fi traffic from remote locations to the enterprise HQ for inspection, applying policies, and regulatory compliance.

CV-CUE supports the following types of tunneling protocols:

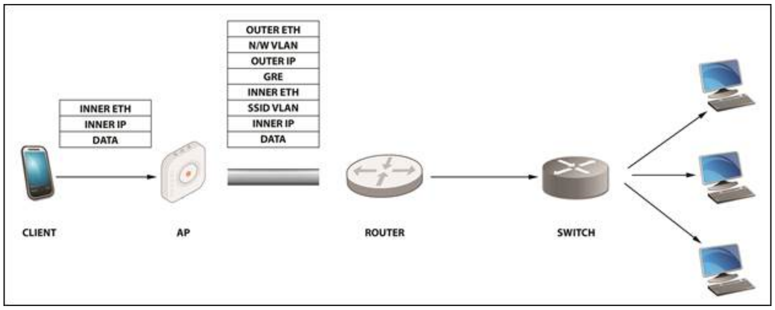
- **EoGRE**: Ethernet over GRE. See EoGRE for details.
- **EoGRE over IPsec**: Ethernet over GRE over IPsec where Ethernet frames are encapsulated using GRE and then encrypted using IPsec. See EoGRE over IPsec for details.
- **VXLAN (Virtual Extensible LAN)**: Virtual Extensible LAN (VXLAN) was originally developed to overcome the limited scalability of VLANs in large network deployments such as datacenters. See VXLAN for details.
- **VxLAN over IPSec**: VXLAN creates a virtual network and IPSec adds a layer of security to the SSID traffic using different encryption methods.

This chapter contains the following topics:

- What is EoGRE?
- What is EoGRE over IPsec?
- What is VXLAN?
- What is VXLAN over IPSec?
- MSS Clamping
- Configure Tunnel Interface
- Tunnel Interface Parameters
- Configure an IPSec Tunnel
- Configure an IPSec Tunnel with EAP-TLS Authentication
- How Failover Works in a Tunneled Network
- Configure VXLAN Profile for Wired-Wireless Tunnel

16.1 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.



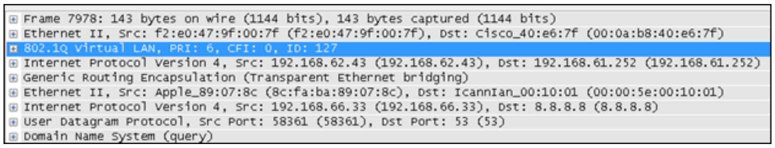
The packet sent by the client contains the following:

- **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.

A packet layout as seen in Arista Packets is shown below:



16.2 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 CV-CUE UI when you set up an IPSec tunnel.

16.3 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 Wi-Fi Access Points (APs) also support VXLAN to allow tunneling of data from Wi-Fi APs to a central aggregation point, e.g., an Arista switch. This allows enterprises to migrate their existing controller-based Wi-Fi networks to Arista's controller-less cloud architecture without having to change the design of their underlying campus network.

16.4 What is VXLAN over IPSec?

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 Ethernet frames traveling over the VXLAN tunnel are encapsulated in IP and UDP headers at the source host and decapsulated at the remote endpoint.

VXLAN creates a virtual network and IPSec adds a layer of security to the SSID traffic using different encryption methods. Using IPSec, an extra layer of security is added to the VXLAN packets in order to protect client's sensitive information against eavesdropping or any modification.

16.5 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 Wi-Fi 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.

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 Wi-Fi 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 Access Point Calculates the MSS based on the tunnel MTU.)

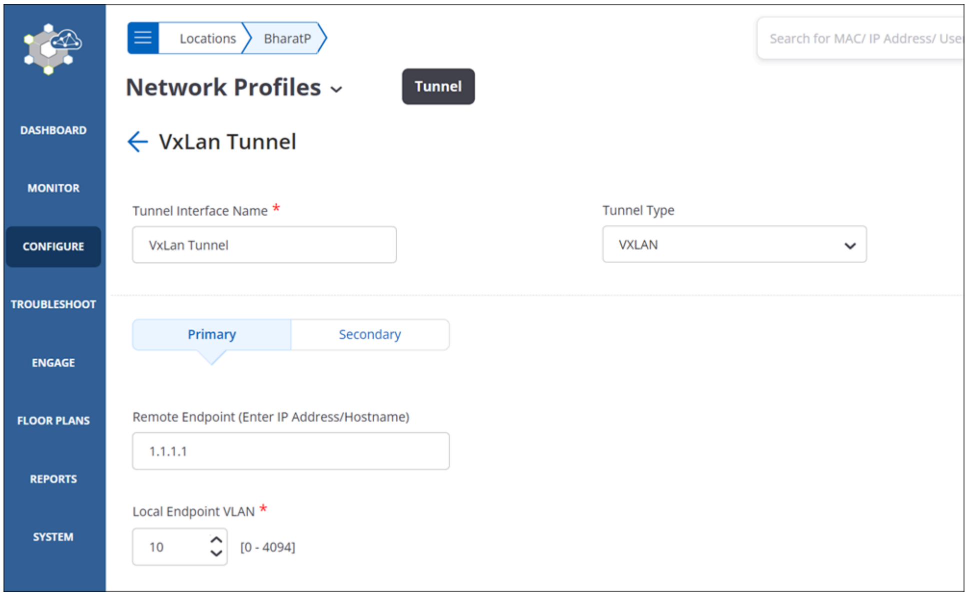
16.6 Configure Tunnel Interface

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 Ethernet over Generic Routing Encapsulation (EoGRE), EoGRE over Internet Protocol security (IPsec), or Virtual Extensible Local Area Network (VXLAN) tunnel.

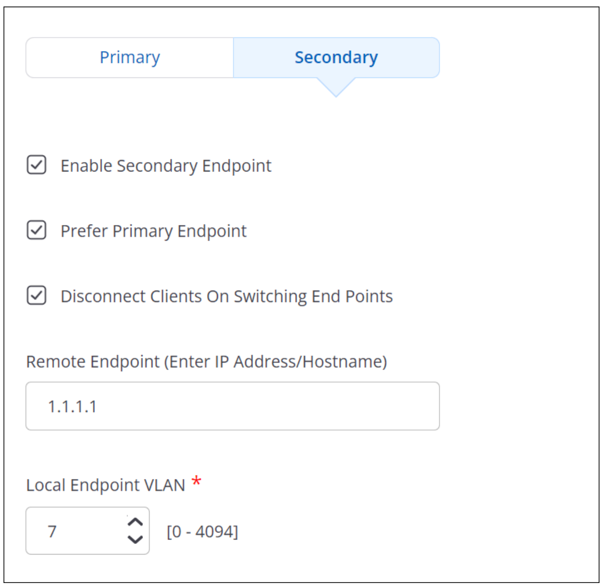
Multiple such tunnels can be configured. The tunnel Interface configuration is location hierarchy specific. Tunnel Interface Profile defined at a specific location is visible at all its child locations.

Let us configure a VXLAN tunnel, to understand the process of creating a tunnel interface profile through CV-CUE.

1. To create a network interface profile navigate to **CONFIGURE** > **Network Profiles** > **Tunnel.**
2. Click **Add Tunnel Interface**.
3. Configure primary endpoint as shown below:



4. You can optionally configure a secondary endpoint as shown below:

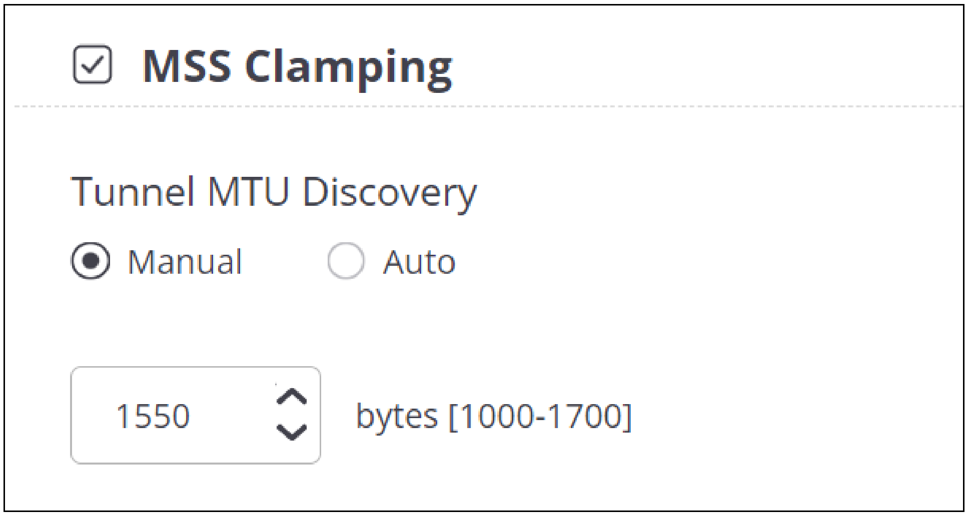


5. Create an SSID Profile with a valid VLAN ID (e.g. 10 as discussed above) and add the recently created Remote-vxlan-bridging network profile to it.

16.6.1 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 CV-CUE are:

1. Navigate to **CONFIGURE** > **Network Profiles** > **Tunnel.**
2. Click **Add Tunnel Interface**.
3. Select the**Tunnel Type**.
4. Enable **MSS Clamping**.
5. Select **Auto** or **Manual** under **Tunnel MTU Discovery**. For the Manual case, set the appropriate tunnel MTU value.



6. Add this tunnel interface to the SSID by selecting **Tunneled** under the **SSID > Network** tab.

16.6.2 How an Access Point 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.

16.7 Tunnel Interface Parameters

The table below provides information required to configure a Tunnel Interface Profile.

Field	Description
Tunnel Interface Name	Name of the tunnel interface profile.
Tunnel Type	Select appropriate network tunnel type: EoGRE, EoGRE over IPSec, VXLAN, or VXLAN over IPSec.
Primary Endpoint Parameters	
Remote Endpoint (IP/Hostname)	The IP address or hostname of the primary remote server or endpoint.
Local Endpoint VLAN	This is the VLAN ID with which the tunneled traffic is tagged. A value between 0 and 4094 should be entered here.
Secondary Endpoint Parameters	
Enable Secondary Endpoint	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.
Remote Endpoint(IP/Hostname)	The IP address or hostname of the secondary remote server or endpoint.
Local Endpoint VLAN	This is the secondary VLAN ID that the tunneled traffic is tagged with. A value between 0 and 4094 should be entered here.
Prefer Primary Endpoint	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.
Retry Parameters (They govern how the AP pings the remote endpoint to check for connectivity)	
Network Probe Interval	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.
Network Ping Retry Count	Count of ping request packets that the AP sends to the remote endpoint. The default value is 2.

Field	Description
Network Ping Timeout	Time, in seconds, till which the AP waits for a ping reply. The default value is 10 seconds.
Ethernet over GRE Parameters	
GRE Primary Key	This is an optional setting. If configured, the same key should be used at both ends of the tunnel.
GRE Secondary Key	This is an optional setting. If configured, the same key should be used at both ends of the tunnel.

16.8 Configure an IPSec Tunnel

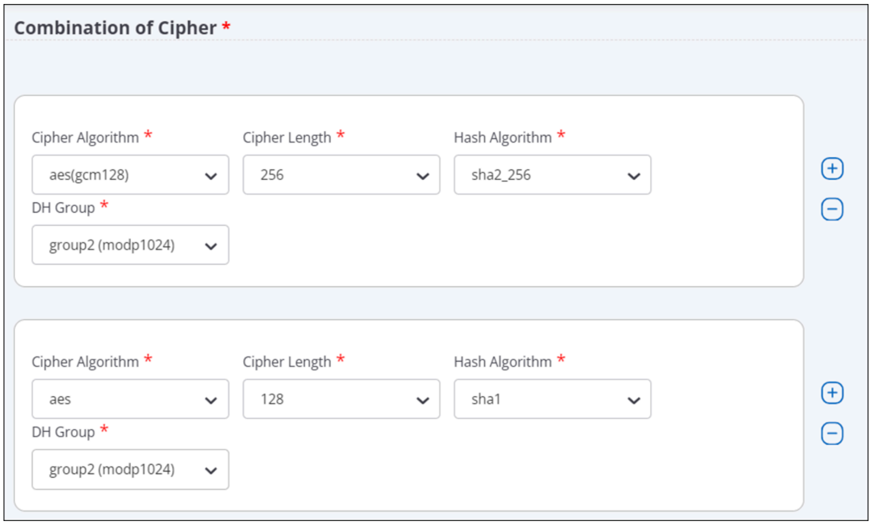
The configuration considers the Tunnel Mode with IKE Version 2 Security Association (SA) protocol and ESP IPSec protocol. Refer to IPSec Parameters to know more about the IPSec configuration parameters.

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.

1. Navigate to **CONFIGURE** > **Network Profiles** > **Tunnel**
2. Click **Add Tunnel Interface**.
3. Select the **Tunnel Type** as **EoGRE over IPSec**.
4. Specify the primary endpoint details such as the remote endpoint, GRE primary key, and VLAN ID.
5. 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.
6. Click **Configure IPSec**.
7. Select the mode as **Tunnel**.
8. Enter the IP address or the hostname of the remote endpoint of the GRE tunnel.
9. Select the Virtual IP address support checkbox. On selecting this field, the remote endpoint assigns a virtual IP address for incoming packets.
10. Click **Phase 1 Parameter**. Phase I Parameter consists of IKE Settings and cipher configuration.
11. 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.
12. 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**.
13. Select the cipher, hash algorithm, and DH group values.

Note: Use one 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



14. Click **Phase 2 Parameter**. Phase 2 Parameter has cipher configurations.
15. Specify the **Lifetime/Phase 2 keepalive** value.
16. Select **ESP** (Encapsulating Security Payloads) or **AH** (Authentication Header) protocol, and then select cipher, hash algorithm, and DH group values.
17. Specify the values for **MSS Clamping**.
18. Save the configuration.

16.9 Configure an IPSec Tunnel with EAP-TLS Authentication

Configure IPSec Tunnel for certificate-based authentication.

When you configure an IPsec Tunnel with IKE Version 2, you can configure the Local (Left) to use the certificate-based authentication to form the tunnel with the Remote (Right). It is mandatory for you to upload the CA certificate for the Remote (Right) endpoint.

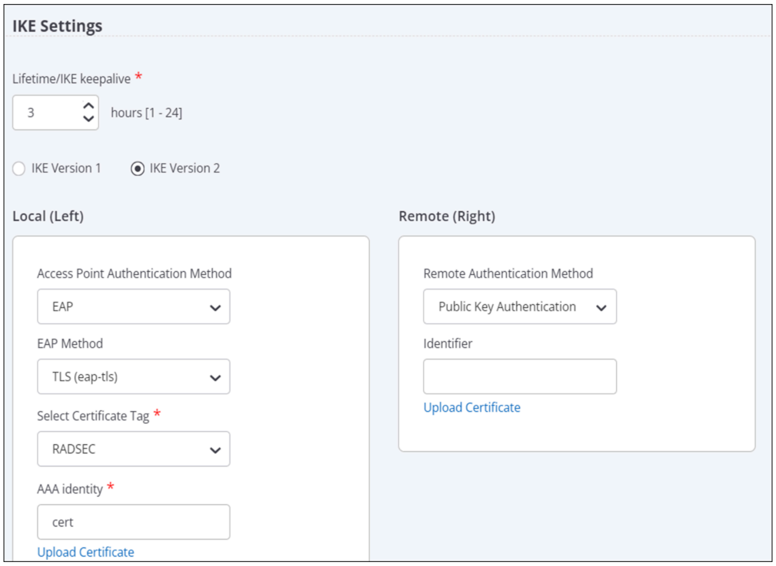
To configure the certificate-based authentication in IPsec tunnels:

1. Go to **CONFIGURE** > **Network Profile** > **Tunnel**.
2. Select any IPSec tunnel type. For example, select the Tunnel Type as EoGRE over IPSec.
3. Specify the primary and secondary endpoint details.
4. Click Configure IPSec.
5. Select the mode as Tunnel and provide the details.
6. In the Phase 1 Parameters > IKE Version 2, specify the Local (Left) settings. The following settings are required for the certificate-based authentication:

    - Access Point Authentication Method: EAP
    - EAP Method: TLS (eap-tls)
    - Select Certificate Tag: Select the certificate tag from the drop-down list.
    - AAA Identity: The address of the AAA server (RADIUS).

- (Optional) Upload Certificate: Upload the CA certificate of the RADIUS server, if the certificate issuer is different for AP and RADIUS. The AP needs the certificate of the RADIUS for mutual authentication.

Figure 16-1: EAP-TLS selection in IPSec configuration



7. Specify the Remote (Right) settings. The following settings are required for the certificate-based authentication:

- Remote Authentication Method: Public Key Authentication
- (Optional) Identifier: The address of the remote endpoint.
- Upload Certificate: Upload the CA certificate of the remote endpoint.

8. Save the configuration.

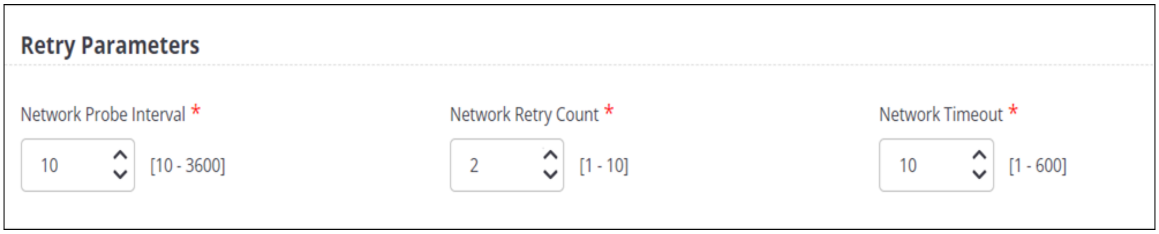
16.10 How Failover Works in a Tunneled Network

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 not 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 does not 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 does not 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 not establish the connection with the primary endpoint, it switches over to the secondary endpoint.

For example, using defaut 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.

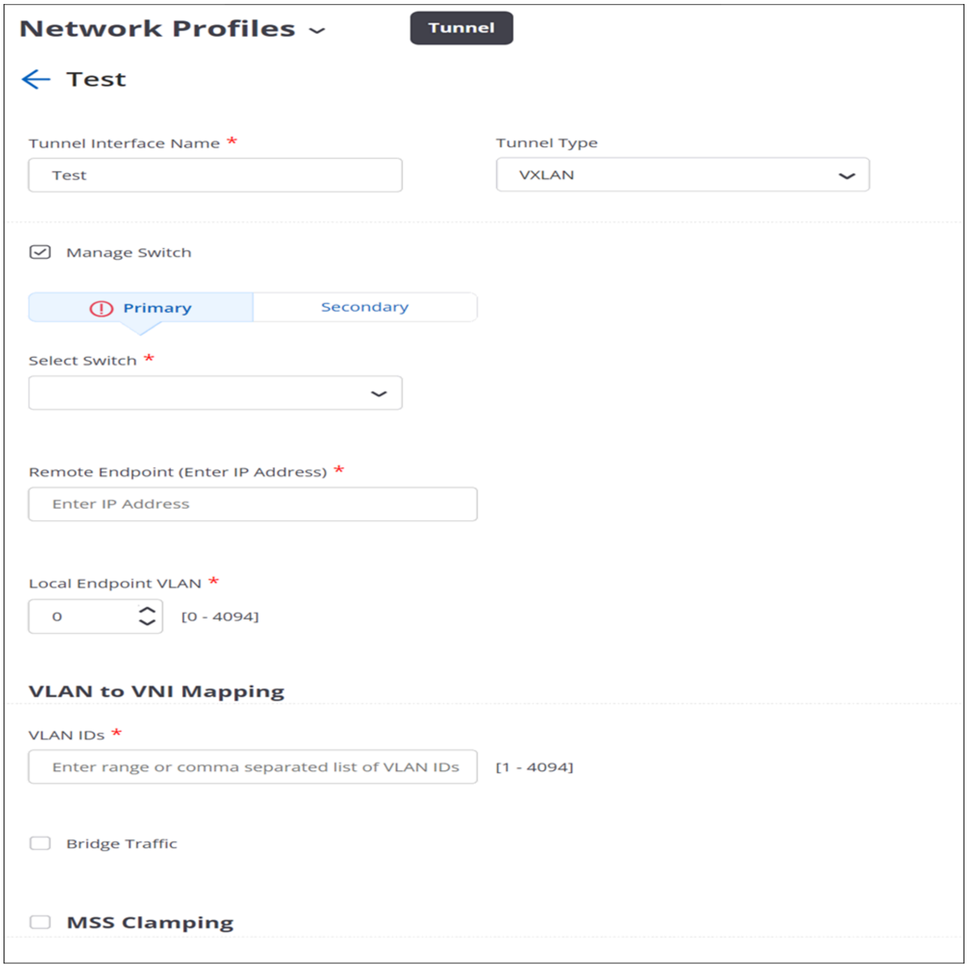
Note that the above calculation is applicable only after the receiver increment counter stops. So, with the default values, it takes around 35 seconds for the tunnel to failover from one endpoint to the other.

16.11 Configure VXLAN Profile for Wired-Wireless Tunnel

You can create a VXLAN profile and use it in your SSID to form a VXLAN tunnel between AP and switch.

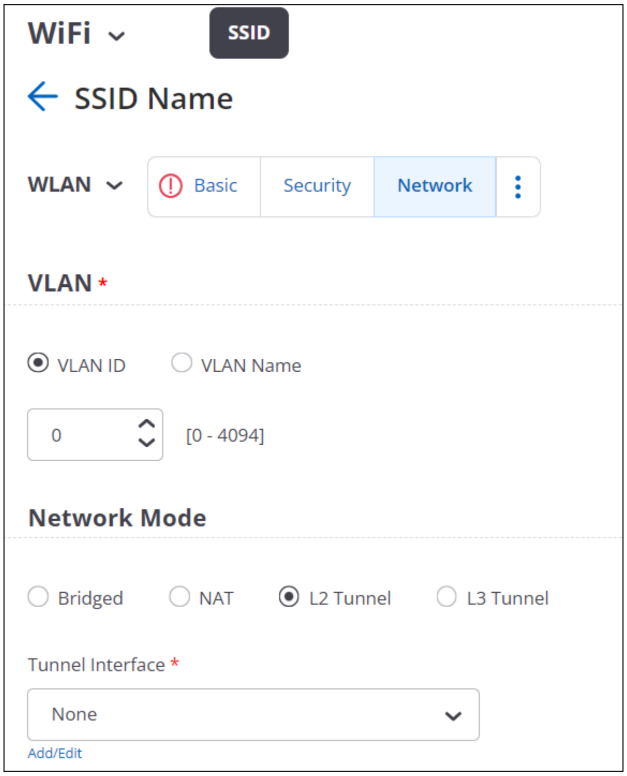
Follow these steps to configure the VXLAN tunnel profile:

1. Navigate to **CONFIGURE** > **Network Profiles** > **Tunnels.**
2. Click **Add Tunnel Interface.**
3. Select the Tunnel Type as **VXLAN** for L2 Tunnels.
4. Provide a tunnel name.
5. Enable the **Manage Switch** check box.



6. For the Primary switch, select the switch name from the drop-down list. Only the available switches are listed in the menu. You will see only those switches that you have imported earlier and if they are not already applied to a different VXLAN profile.
7. Specify the **Remote Endpoint IP** address. This is the loopback address that gets created on the switch.
8. (Optional) Configure the Secondary switch.
9. Specify the **Local Endpoint VLAN** where the AP creates the tunnel with the remote endpoint. Ensure that the remote endpoint is reachable from the local endpoint VLAN.
10. Specify the **VLAN IDs** which are mapped to the VNI of the switch. As a best practice, create the VNIs on the switch and then map them here with respective VLAN.
11. Enable **Bridge Traffic.**
12. Enable **MSS Clamping.**
13. Select **Auto** or **Manual** under Tunnel MTU Discovery. For the Manual case, set the appropriate tunnel MTU value.
14. Save the settings.

Once you have created a VXLAN tunnel profile, you can add it to your SSID in the **Network** tab. Click **SSID** > **Network** > **L2 Tunnel** under the Network Mode and select the VXLAN tunnel from the drop-down list.

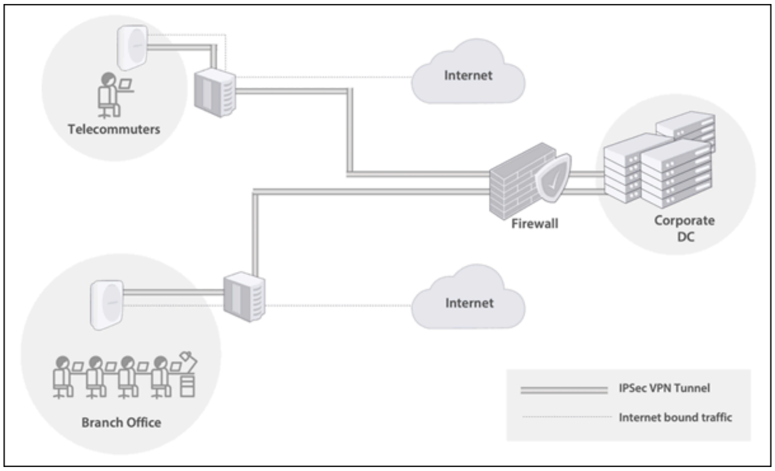

WiFi
SSID
SSID Name
WLAN
Basic
Security
Network
VLAN *
VLAN ID
VLAN Name
0
[0 - 4094]
Network Mode
Bridged
NAT
L2 Tunnel
L3 Tunnel
Tunnel Interface *
None
Add/Edit

Chapter 17

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.



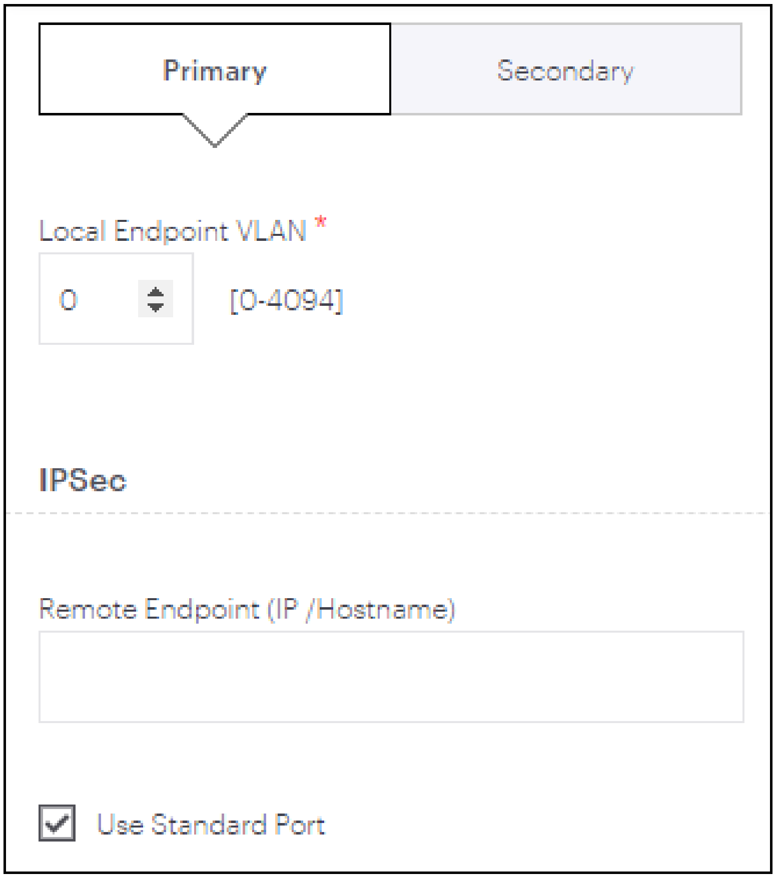
This chapter contains the following topics:

- Configure a Remote Access Point
- Configure IPSec Credentials for Each Remote Access Point

17.1 Configure a Remote Access Point

You can configure all Wave 2 and Wi-Fi 6 Arista access points, except C-100 and C-110, to function as a remote AP using CV-CUE. 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 CV-CUE, 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

   Info: 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.

   .

17.2 Configure IPSec Credentials for Each Remote Access Point

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 CV-CUE, 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 18

Radio Settings

This chapter contains the following topics:

18.1 About Radio Settings

The Radio Settings tab allows you to configure settings related to the Wi-Fi 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. The newer Wi-Fi 6E APs have four radios, where three radios are dedicated access raios and the fourth radio is a multifunction radio. For more information on AP models and radios, see the AP matrix under AP Platforms in https://www.arista.com/en/products/cloudvision-cue.

You also have two new tabs to configure the 6 GHz band and Dual 5 GHz band. In the 6 GHz tab, the channels are arranged based on the UNII bands (UNII-5, UNII-6, etc.) because the number of allowed 6 GHz UNII bands varies depending on the regulatory domain. Rest of the options are the same as the 5 GHz or 2.4 GHz bands. Dual 5 GHz is hidden by default, but you can access it from the three-dots menu. 6 GHz and Dual 5 GHz configurations are applicable only for Wi-Fi 6E APs (such as C-360).

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.

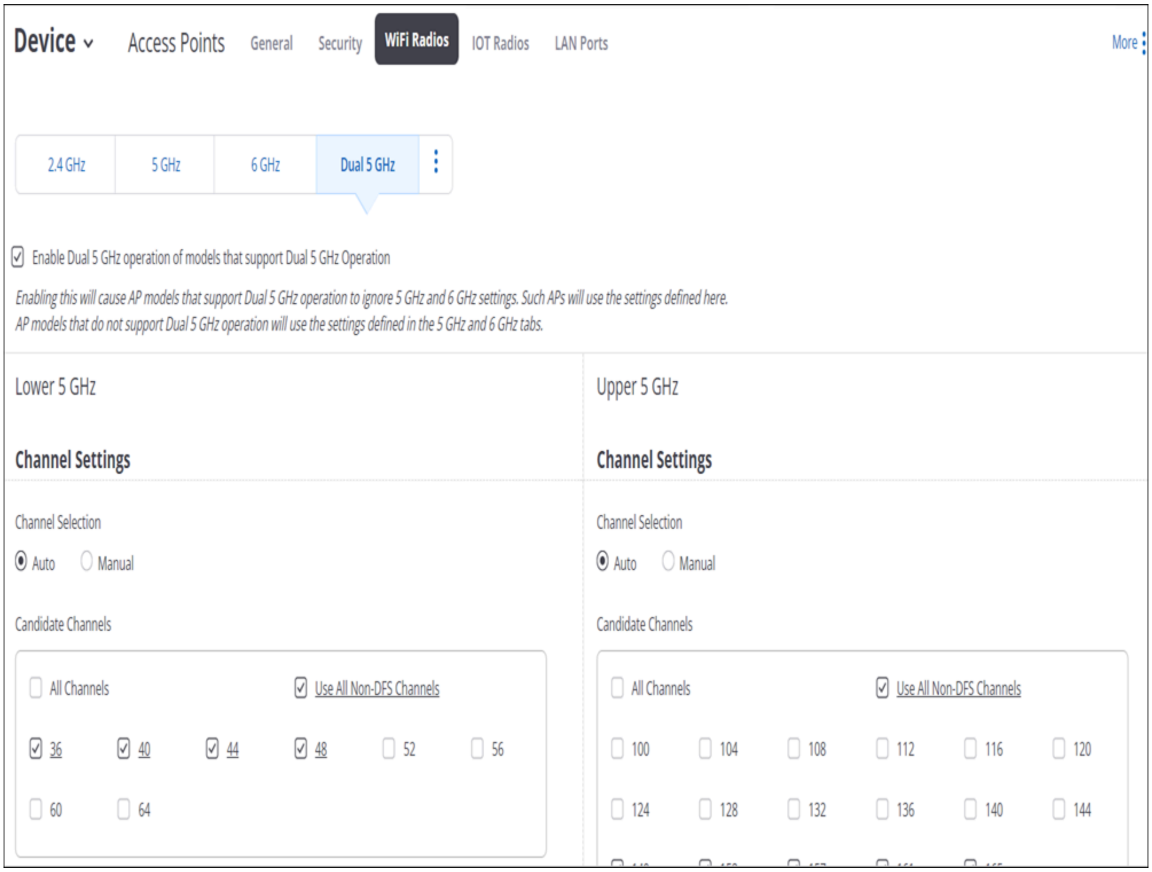
In case of the 2.4GHz (i.e. 802.11 b/g/n) radio , you can select some or all of the available candidate channels. Similarly, for the 5GHz (i.e. 802.11 a/n/ac) and 6 GHz radios, you can select some or all of the available DFS channels and/or non-DFS channels as candidate channels. DFS stands for dynamic frequency selection. It is a mechanism using which interference by RADAR signals in 5GHz and 6 GHz are 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.

Dual 5 GHz

In a dual 5 GHz band configuration, radio 2 operates in the lower 5 GHz band and radio 3 operates in the upper 5 GHz band. The 5 GHz band has 25 non-overlapping 20 MHz channels, which allows operation in the Dual 5 GHz mode without the lower and upper 5 GHz bands interfering with each other.



When Dual 5 GHz is enabled, those configurations will be given preference over 6 GHz configurations. That is, if you configure all the three radios — 2.4, 5, and 6 GHz, and then configure Dual 5 GHz as well, then the AP will ignore the configurations defined in 5 GHz and 6 GHz tabs, for C-360 APs.

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 Effective Isotropic Radiated Power (EIRP). 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 does not 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 are on a voice or a video call.

18.2 How Unified Client Steering Works

The following table 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 Indicator (RSSI), load or band).

Table 9: Types of Client Steering

Stage	Method	Short Description
Pre-Association	Min Association RSSI	Rejects association request if client's RSSI is less than the configured threshold
	Band Steering	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.
	Smart Client Load Balancing	Rejects association request if the client load on an AP is high and less loaded neighbor APs are available
Post-Association	Smart Steering	Disconnects client if RSSI drops below a certain threshold
	Band Steering	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

Note: Unified Client Steering works only on 11ac Arista devices. It is not supported for 11n Arista devices.

18.2.1 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

18.2.2 Inter Access Points Sync

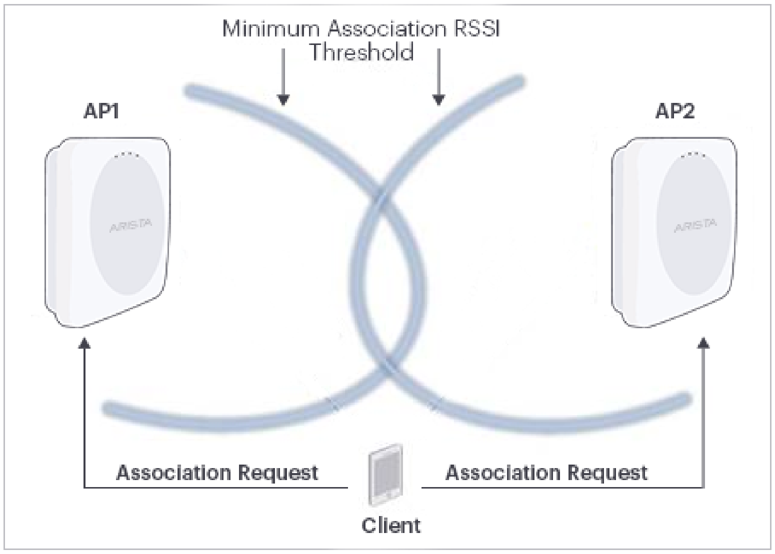
An AP must have a unified, client-aware view of the network. That is, it must know how the network looks to its neighboring APs and to clients – both its own clients and those of the neighbors. The AP can then make informed steering decisions to ensure optimum client QoE.

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 CV-CUE 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.



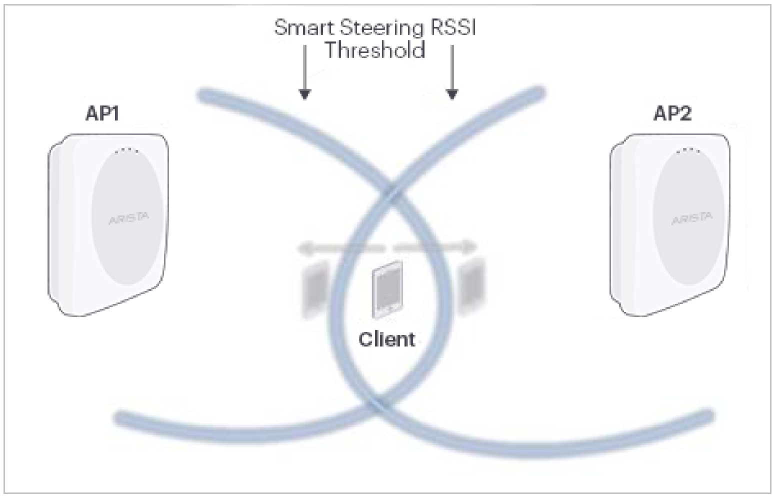
18.2.3 Frequency of Client Steering

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.



18.3 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** > **Device** > **Access Points** > **WiFi Radios.**
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**.

18.3.1 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.

18.3.2 Client Steering Parameters

Field	Description
Client Steering Common Parameters	
Client Steering Common Parameters	Client Steering Common Parameters can be configured only on11ac devices.
Steering RSSI Threshold	The steering RSSI threshold can be between -60 to - 85 dBm. Default value is -70 dBm.
Steering Attempts Threshold	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.
Steering Blackout Period	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.

18.4 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** > **Device** > **Access Points**
2. Select the **RF Regulatory Domain**.
3. Select the frequency band under **Wi-Fi Radios** tab.
4. Configure the **Operating Channel** section.
5. Choose **Auto** or **Manual Channel Selection**. Choose from:
    - If **Channel Selection** is **Auto**, then provide appropriate values for the fields below.
        - Channel Width
        - Selection Interval in hours
        - Selection Mode - Select **Scheduled** to run ACS at a specific time of the day and minimize service disruption. Select **Periodic** to run ACS at defined time intervals.
        - **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**.

18.4.1 Basic Radio Settings Parameters

Field	Description
Operating Region	Contains list of region or country, default it United States. User is allowed to change it **if he has an entitlement or license.**
Frequency Band	The radio frequency band. You can configure the radio frequency for 2.4 GHz, 5 GHz, 6 GHz, and Dual 5 GHz. Default value is 2.4 GHz.
Channel	
Operating Channel	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.
Channel Width	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+80 MHz and 20/40/80/160 MHz options are available. The options are enabled for 2.4 GHz, 5 GHz, and 6 GHz modes.
Selection Interval	This field is visible only when the Operating Channel is set to **Auto**. 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.
Dynamic Channel Selection	This field is visible only when the Operating Channel is set to **Auto** . 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.

Field	Description
Candidate Channels	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.
Auto Channel Selection(ACS) Mode	ACS has two selection modes, Scheduled and Periodic. In Scheduled ACS, you can define the duration in hours and minutes. The AP radio checks for interference and contention every day during the scheduled time. You can also specify a secondary time to run the ACS. The duration between the two scheduled ACS must be at least 60 minutes. Else, you will receive an error message and you will not be able to schedule the ACS. The Scheduled ACS is a per-radio setting. So, you need to define the ACS schedule for each band. In Periodic ACS, you can specify the time duration in hours, to run ACS at pre-defined time intervals.

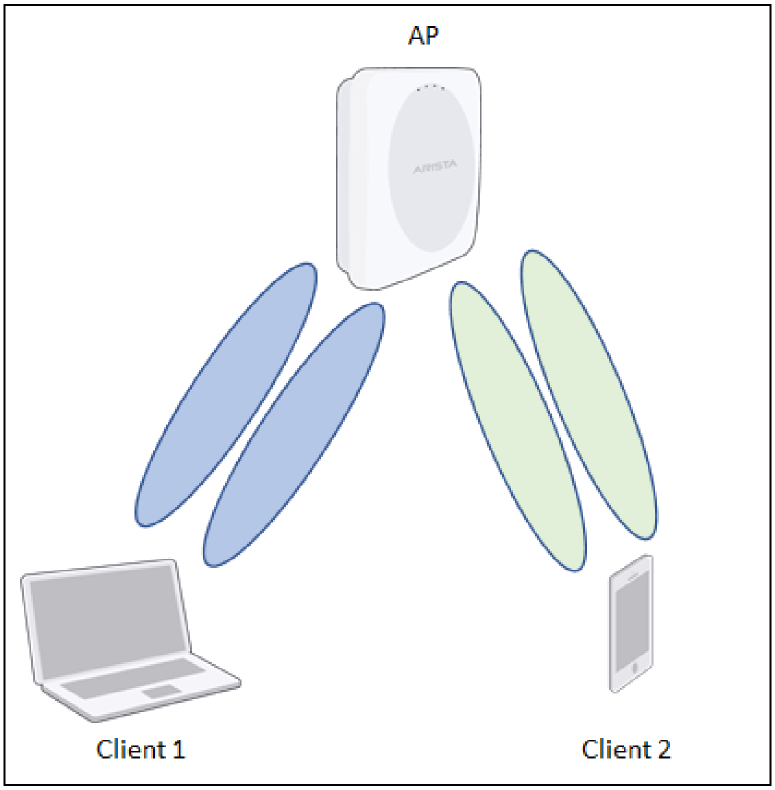
18.5 Configure 802.11ax Settings

Until 802.11ac, Wi-Fi standards focussed on increasing peak data rates. With 802.11ax, although the data rates increase, the focus is on improving Wi-Fi capacity—a must for high-density environments. Given the large number and variety of Wi-Fi 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, MU-MIMO, and Spatial Reuse 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 Wi-Fi Help Portal.

18.5.1 MU-MIMO

Multiple Input Multiple Output (MIMO) refers to the use of multiple antennas on Wi-Fi 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

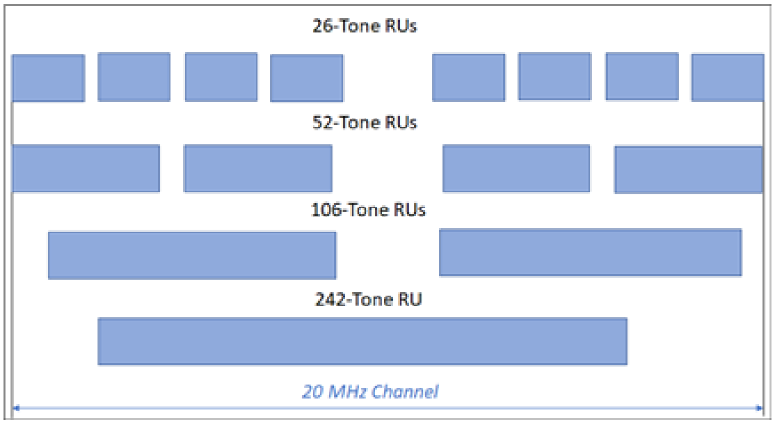
Depending on the channel conditions of a client, an AP can use Single User MIMO (SU-MIMO) to improve the client's data rates or reduce its error rates. Both, however, are per-link improvements. Since dense environments are about capacity and not just individual user data rates, downlink MU-MIMO can help 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 Wi-Fi 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.

18.5.2 OFDMA

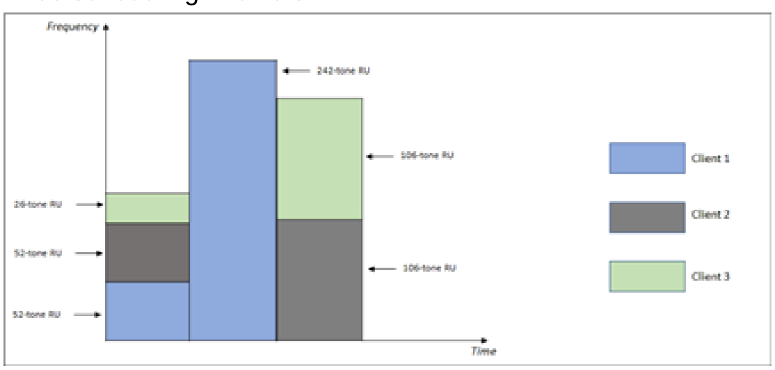
Orthogonal Frequency Division Multiple Access (OFDMA) divides the Wi-Fi channel into subcarriers, also called "tones", each 78.125 KHz wide. Tones are combined to form Resource Units (RUs) of different widths. As shown in the representation below, an RU can consist of 26, 52, 106, or 242 tones—corresponding 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

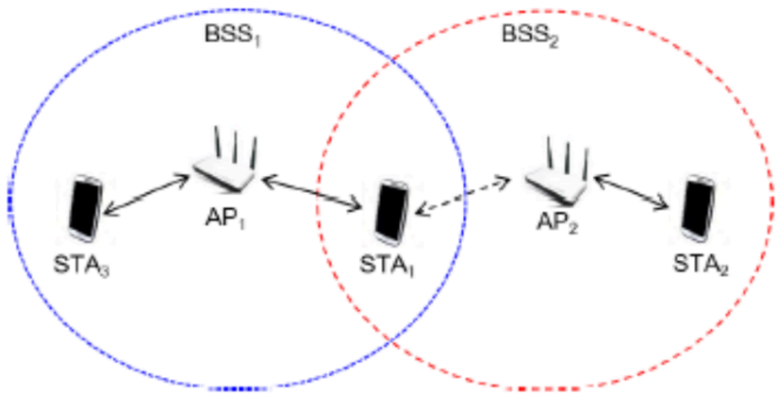
The Wi-Fi uplink is a distributed form of communication because the transmitters (i.e., clients) cannot coordinate their schedules (unlike the downlink, where the AP is both the transmitter and the scheduler). Until 802.11ac, Wi-Fi uplink was uncoordinated: clients contended for the medium and, based 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 Wi-Fi 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 Wi-Fi 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.

18.5.3 Spatial Reuse

With spatial reuse, two or more Wi-Fi devices (AP or client) that support 802.11ax protocols can send transmissions simultaneously without any significant data loss. Spatial Reuse helps in improving the spectral efficiency and optimal allocation of resources to meet the Quality of Service (QoS).

How Spatial Reuse Improves Efficiency?

To understand spatial reuse, consider the two co-channel BSSs as shown in figure below.



BSS1 and BSS2 operate on the same channel and can hear each other with an RSSI higher than the Clear Channel Access Signal Detection (CCA-SD) level, the threshold that Wi-Fi devices use to decide if the channel is clear to transmit or if they need to wait for the . A co-channel BSS that can be heard at an RSSI greater than the threshold is called an overlapping BSS (OBSS). Thus, BSS2 is an OBSS for BSS1, and vice versa.

Before Wi-Fi 6, if a Wi-Fi device detected an ongoing transmission with RSSI higher than CCA-SD on a specific channel, all other devices on the same channel had to back off and they would wait for the ongoing transmission to get over. With Wi-Fi 6, a device can leverage spatial reuse to transmit in parallel with an ongoing OBSS transmission, provided the spatial reuse transmission is at an acceptably low transmit power.

BSS Color

A Wi-Fi device that wants to transmit using spatial reuse needs to distinguish the transmissions of its own BSS from those of the OBSS. To enable this, Wi-Fi 6 introduces BSS color, an integer between 1 and 63 to identify a BSS. An AP radio automatically assigns a BSS color to each transmission. When two radios transmit on the same channel, BSS color helps an AP to differentiate between an inter-BSS transmission and intra-BSS transmission.

Typically, every 802.11ax HE (High Efficiency) frame contains a BSS color value that a Wi-Fi device can use to identify the frame as its own BSS or an OBSS. The BSS color is signaled in the 802.11ax PHY preamble, allowing for early detection of an OBSS transmission. Since a Wi-Fi 6 device instantly decodes the HE preamble, the device can identify an OBSS transmission well in advance to transmit in parallel.

As long as BSSs in vicinity of each other use distinct BSS colors, a device can distinguish the transmissions of its own BSS from those of an OBSS.

Enabling Spatial Reuse

To enable spatial reuse,

1. Click the **WiFi Radio** tab.
2. Select a frequency band and scroll down to 802.11ax Enhancements.
3. Click the **Spatial Reuse (SR)** checkbox.
4. Specify your OBSS Packet Detection Threshold. If the RSSI of an ongoing BSS transmission is below the specified level but within the range of -81 to -62 dBm, the OBSS device can transmit in parallel.

5. Save the settings.

18.6 Configure 802.11be Enhancements

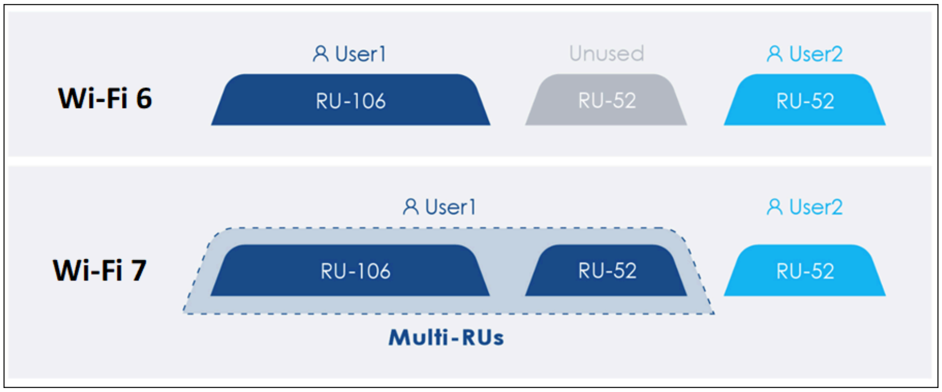
The 802.11be standards build on 802.11ax by providing ultra-high throughput, improved resource utilization, and interference mitigation. The 320 MHz support increases the throughput and performance in the 6GHz band. The improved resource utilization is attributed to the introduction of Multiple Resource Units (MRU) in Orthogonal Frequency Division Multiple Access (OFDMA) transmission and Multi-Link Operation (MLO).

Key features supported by Arista 802.11be access points (AP) include:

- Multiple Resource Units (MRU)
- Preamble Puncturing
- Multi-Link Operation
- Support for 320 MHz Channel Bandwidth

18.6.1 Multiple Resource Units

Multiple Resource Units (MRU) is an enhancement to RU introduced in 802.11ax. With MRU, the AP can allocate multiple, non-contiguous resource units (RU) to a single client device. This feature significantly improves resource utilization when used with the puncturing of RU.



Enabling Multiple Resource Units

To enable MRU:

1. Click the **WiFi Radio** tab.
2. Select a frequency band and scroll down to **802.11be Enhancements.**

Note: As a prerequisite, select **Downlink OFDMA** and **Uplink OFDMA**.

3. Click the **Multiple Resource Units** checkbox.
4. Save the settings.

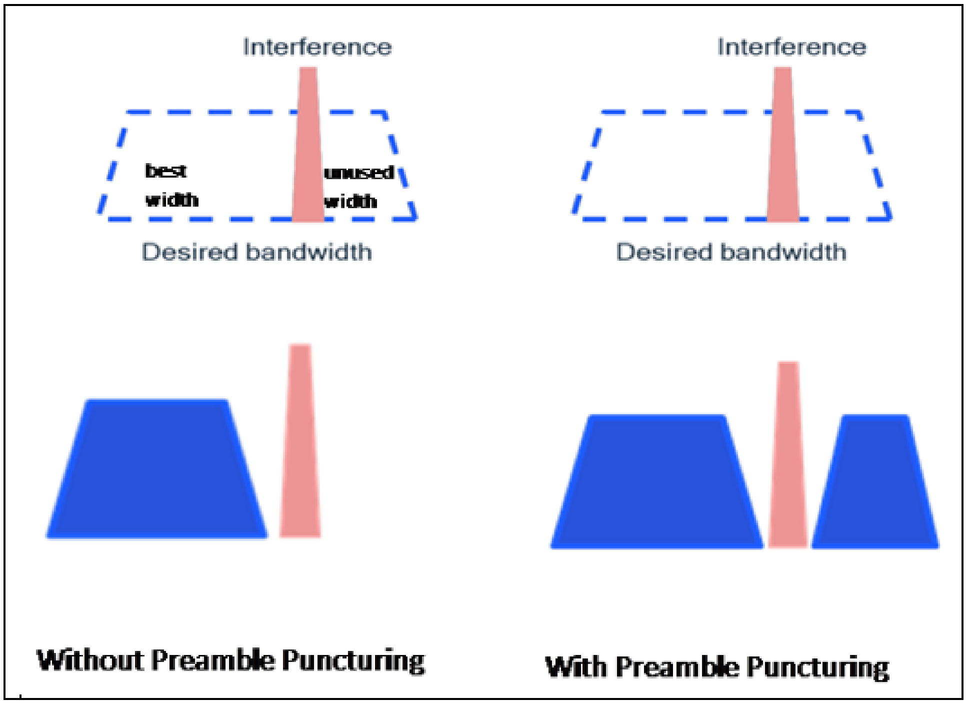
Verification

To verify MRU, check the AP logs. You can also see the status on the SSID card view.

18.6.2 Preamble Puncturing

Preamble Puncturing is the ability to not send the preamble for a given 20 or 40 MHz channel, indicating that the ensuing data will not be present in that 20 or 40 MHz channel. Except for the primary 20 MHz or 40 MHz channels, the AP can puncture the secondary or other channels. Preamble Puncturing is not supported in the 2.4 GHz band because the AP cannot puncture 20 MHz and 40 MHz channels.

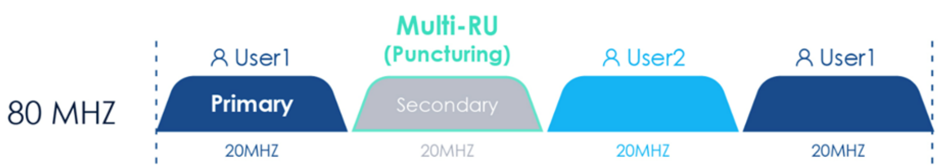
Until 802.11ax, if the AP discovered interference on any of the secondary channels, the AP had to use the best, complete width for data transmission; the remaining width would remain unused. With Preamble Puncturing, the AP can puncture only the affected width and use the remaining width for data transmission.



When you enable Preamble Puncturing, the AP uses proprietary algorithms to identify interference in the 5 GHz or 6 GHz band and punctures the interfering RU. It transmits data with the punctured RU for 30 minutes. After 30 minutes of transmission, the AP scans for interference again, and if it doesn’t find any, it stops the puncturing.

Preamble Puncturing improves clients' overall bandwidth utilization by utilizing all available RUs for data transmission. With Preamble Puncturing, APs can puncture the worst-performing RUs, and therefore, administrators can allocate 80 or higher MHz RUs depending on demand. You do not have to restrict yourself to allocating just 20 or 40 MHz RUs.

The following image shows data transmission in an 80 MHz channel. The AP efficiently transmits data to two clients or users despite noticing interference in a 20 MHz width (Punctured).



The AP uses the puncturing resolution of 20 MHz in 80 MHz and 160 MHz. The puncturing resolution in a 320 MHz channel is 40 MHz.

Enabling Preamble Puncturing

To enable preamble puncturing:

1. Click the **WiFi Radio** tab.
2. Select a frequency band and scroll down to **802.11be Enhancements.**
3. Click the **Preamble Puncturing** checkbox.
4. Save the settings.

Verification

To verify the punctured width from the RF Explorer:

1. Go to **MONITOR > WiFI > Radios.**
2. Scroll down to the **Channel Map** widget and select RF Explorer.

You can see the RF Explorer chart and the table.

You can also verify if a radio has Premable Puncturing enabled from the Radio listing or from the Radio Properties right panel.

18.7 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** > **Device** > **Access Points.**
2. Click **WiFi Radios** tab,
3. Move to **Transmit Power Selection Settings**.
4. Select **Auto** option.
5. Enter the appropriate values for the following fields.
    - Loudness RSSI
    - Neighbor Count
    - Minimum Transmit Power
    - Maximum Transmit Power
6. Select **Manual** option.
7. For access points that use an external antenna, select **Use External Antennas** and enter the **External Antenna Gain** in dB.
8. Click **Save**.

18.7.1 Transmit Power Selection Parameters

Field	Description
Advanced Radio Settings	
Transmit Power Selection (Auto and Manual radio buttons)	This field enables you to control the transmission power of the AP. It is a mandatory field. • Manual - Select the **Manual** option to manually specify the transmission power of the AP in dbm. • 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.
Loudness RSSI	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.
Neighbor Count	Maximum number of allowed loud neighbor APs. Allowed range is 1 - 10. The Default value is default 3.
Minimum Transmit Power	Minimum transmission power. Allowed range is 4 - 30 dBm. The Default value is 4 dBm.
Maximum Transmit Power	Maximum transmission power. Allowable range is 4 - 30 dBm. The Default value is 30 dBm.

18.8 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** > **Device** > **Access Points** > **WiFi Radios.**
2. In the **Smart Steering** section enter the time interval, in seconds for **Roam Initiation Interval**.

   Info: 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.
3. Enter the RSSI threshold to disconnect a client in **Roam Initiation Packet Threshold** field.

   Info: 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.
4. Click **Save**.

18.9 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** > **Device** > **Access Points** > **WiFi Radios.**
2. In the **Smart Client Load Balancing** section enter the minimum number of clients that can connect to an AP in **Minimum Client Load** field.

   Info: 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.
3. Enter The minimum difference between the number of clients connected on neighboring APs in **Minimum Client Load Difference** field.

   Info: This minimum difference is considered to balance client load. Default value is 5 and range varies from 2 to 10.
4. Click **Save**.

18.10 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** > **Device** > **Access Points** > **WiFi Radios.**
2. Scroll down to **Band Steering** section.
3. Enter the value for **Band Steering Client Load Difference**.

   Info: 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.
4. Click **Save**.

18.11 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** > **Device** > **Access Points** > **WiFi Radios.**
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.

Info: 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.

   Info: 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.

   Info: 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.

   Info: 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.

   Info: The range for percentage share is from 0 to the percentage share specified in **Maximum Share Of Medium Time** field.

10. Click **Save**.

Chapter 19

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 CV-CUE 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 Wi-Fi Server. The server pushes the changes onto the AP when the AP reconnects with the server.

This chapter contains the following topics:

- Device Tab
- Turn Access Point into a WIPS Sensor
- Configure Scanning
- Configure Inter Access Point Sync for Client Steering in Device Settings
- Configure Client RSSI Update Interval in Device Settings
- Configure VLAN Extension in Device Settings
- Configure Link Aggregation in Device Settings
- Configure AeroScout Integration
- Configure Antenna Settings in Device Settings
- Configure Device Password in Device Settings
- Configure Device Access Logs in Device Settings
- Configure IPv4/IPv6 Dual Stack in Device Settings
- Enable SSH IP Allow List

19.1 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, CV-CUE permanently erases Wi-Fi 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 specific APs (AP Feature Matrix) and only when it is in AP mode (i.e. not configured as a sensor). VLAN Extension allows you to map a LAN port to a VLAN ID. It is 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.

Link Aggregation applies only to specific Arista APs (AP Feature Matrix). 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 Wi-Fi 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.

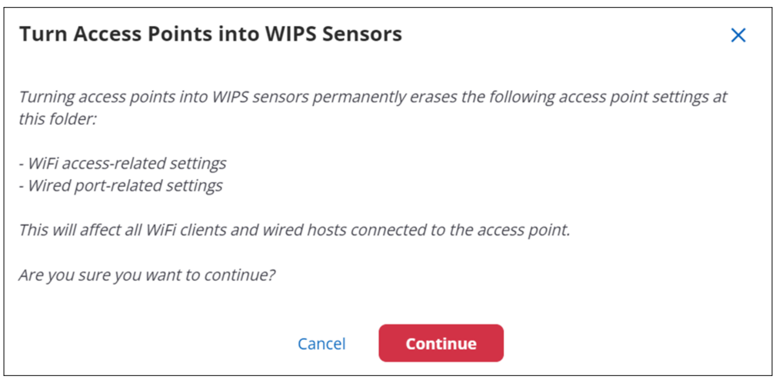
Access Radio Exceptions apply to Single Radio devices or to dual-radio devices that can operate in a "combo" mode with one radio in access mode and the other one in WIPS mode. For Single Radio devices, you can select the band you want the device to operate on. For Dual Radio AP-Sensor Combo devices, you can select the band of operation of the access radio.

19.2 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** > **Access Points** > **General**.
2. Select **Turn Access Point into Dedicated WIPS Sensor**.



3. Click **Continue** to turn APs into WIPS sensor.
4. Click **Save**.

19.3 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 Do not enable background scanning if the radio is being used for Voice over IP (VoIP). 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 Wi-Fi 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 disrupts 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 10sec spent on the service channel to serve Wi-Fi clients will make a visit to a single off-service channel for 30 ms.

To configure Scanning:

1. Navigate to **CONFIGURE** > **Device** > **Access Points.**
2. Under **Background Scanning** in **General** tab, 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**.

19.3.1 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.

Field	Description
Wi-Fi Scan Duration	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.
Wi-Fi Access Duration	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.

19.4 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** > **Access Points** > **WiFi Radios.**
2. Click **Client Steering Common Parameters** from the bottom panel.
3. Select **Inter-Access Point Sync for Client Steering**.
4. Enter **Sync Period** in seconds.

   Info: Sync Period is the time interval specified to broadcast periodic Sync messages. The time interval can be minimum 10 seconds and maximum 60 seconds.

5. Click **Save**.

19.5 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** > **Access Points** > **General**.
2. Scroll down to **Client RSSI Update Interval** section.
3. Enter the interval value in seconds.
4. Click **Save**.

19.6 Configure VLAN Extension in Device Settings

Enabling VLAN Extension takes precedence over the Wired Extension configured in the Network Profile in SSID settings.

To configure VLAN Extension:

1. Navigate to **CONFIGURE** > **Device** > **Access Points** > **LAN Ports**.
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. Save the settings.

19.7 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.

To configure Link Aggregation:

1. Navigate to **CONFIGURE** > **Device** > **Access Points** > **LAN Ports**.
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. Save the settings.

19.8 Configure AeroScout Integration

Configuring CV-CUE 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 Wi-Fi APs. You can set up SSIDs under **CONFIGURE** > **WiFi.**
2. To enable integration with AeroScout, go to **CONFIGURE** > **Device** > **Access Points** > **General** tab. In the **Integrations** section, seable 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 Wi-Fi APs. You can configure Channel Settings under **CONFIGURE** > **Device** > **Access Points** > **WiFi Radios.**

19.9 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** > **Access Points** > **General.**
2. Scroll down to **Legacy Model Features**.
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**.

19.10 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** > **Access Points** > **General.**
2. In the **Device Password** section, enter **username**.
3. Enter Password. The password should be at least 8 characters long and it cannot contain your login ID.
4. Confirm the new password by entering again the same password in **Confirm Password** field.
5. Click **Save**.

19.11 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** > **Access Points** > **General.**.
2. Select **Send Device Logs to a Syslog Server** in the **Network** section.
3. Enter **Syslog Server IP/Hostname**.
4. Click **Save**.

19.12 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** > **Access Points** > **General.**
2. Select **IPv4/IPv6 Dual Stack** in the **Network** section.
3. Click **Save**.

19.13 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** > **Access Points** > **General** tab.
2. Select **Enable SSH IP Allow List** in the **Network** section.
3. Enter an IPv4 IP address in the **IP Address** field.
4. Enter a Wildcard Mask. in the **Wildcard Mask** fileld.
5. Click **Add**.

Note: 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.

19.13.1 SSH IP Allow List Parameters

Field	Description
IP Address	A valid IP address.
Wildcard Mask	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 does not 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.

19.14 Enable Multiple VLAN Registration Protocol

Multiple VLAN Registration Protocol (MVRP) is a Layer 2 protocol. The protocol allows access points to propagate the VLAN created on CV-CUE to the connected Switches. The real-time propagation of configuration allows you the flexibility of configuring your wired and wireless network in one interface and distributing it to other active interfaces. You do not have to worry about managing and maintaining the configurations in all interfaces.

Note: Untagged VLANs are not automatically propagated to Switches. You need to manually configure the Untagged VLANs on Switches.

Considerations:

- Before enabling MVRP on CV-CUE, ensure that MVRP is enabled on the Switch interface. Refer to the vendor-specific Switch documentation for more information on enabling MVRP on Switches.
- The AP reboots every time you update the MVRP configuration in CV-CUE.
- MVRP is not supported for non-root AP in a Mesh network.

To enable MVRP:

1. Navigate to **CONFIGURE** > **Device** > **Access Points** > **General** tab and scroll-down to Network section.
2. Select the **Enable MVRP** checkbox.
3. Save the settings.

19.15 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** > **Access Points** > **-General** tab.
2. Scroll down to **NTP Configuration** in **Network** section.
3. Enter **Primary NTP Server IP/Hostname**.

   Info: 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**.

19.16 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** > **Access Points.**
2. Scroll down to **Legacy Model Features**.
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**.

19.17 Device Security Settings

On the Security tab under Device Settings, you can configure VLAN Monitoring and WIPS.

CV-CUE 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 is really easy to set up an unauthorized Wi-Fi network. Small plug-and-play devices can act as access points. Smart phones and tablets can act as Wi-Fi 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 Wi-Fi 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 Wi-Fi 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.

19.17.1 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 **CONFIGURE** > **Device** > **Access Points** > **Security,** 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 Wi-Fi 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.

19.17.2 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 10: Maximum number of VLANs monitored

Model	AP Mode	Sensor Mode	ND Mode
C-50	12	16	50
Other Arista devices	20	20	100

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 us 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. *Number of automatically monitored VLANs = Max – User-Defined VLANs*

19.18 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 CV-CUE:

- **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 Wi-Fi Help portal.

19.18.1 Example Use Case for BLE

Let us 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.

19.18.2 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** > **Access Points.**
2. Click **IOT Radios** tab.
3. 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**.
4. 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.

19.18.3 Customize the BLE Minor of an Access Point

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.

19.19 Configure Bluetooth Scanning

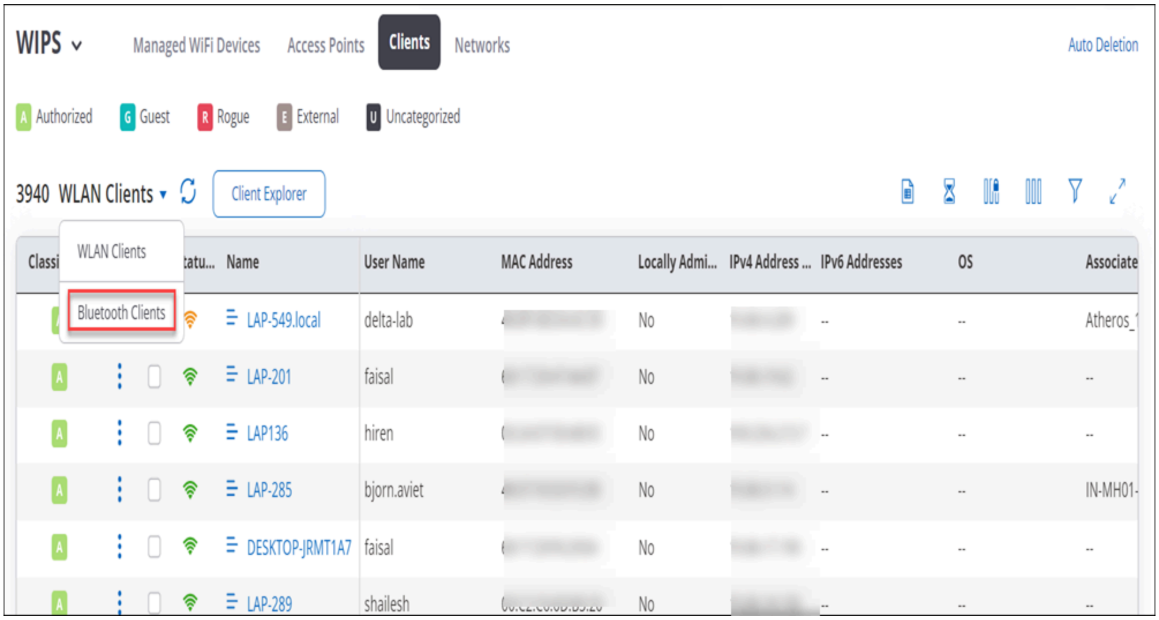
You can configure Bluetooth scanning to detect nearby Bluetooth devices.

To enable Bluetooth Scanning,

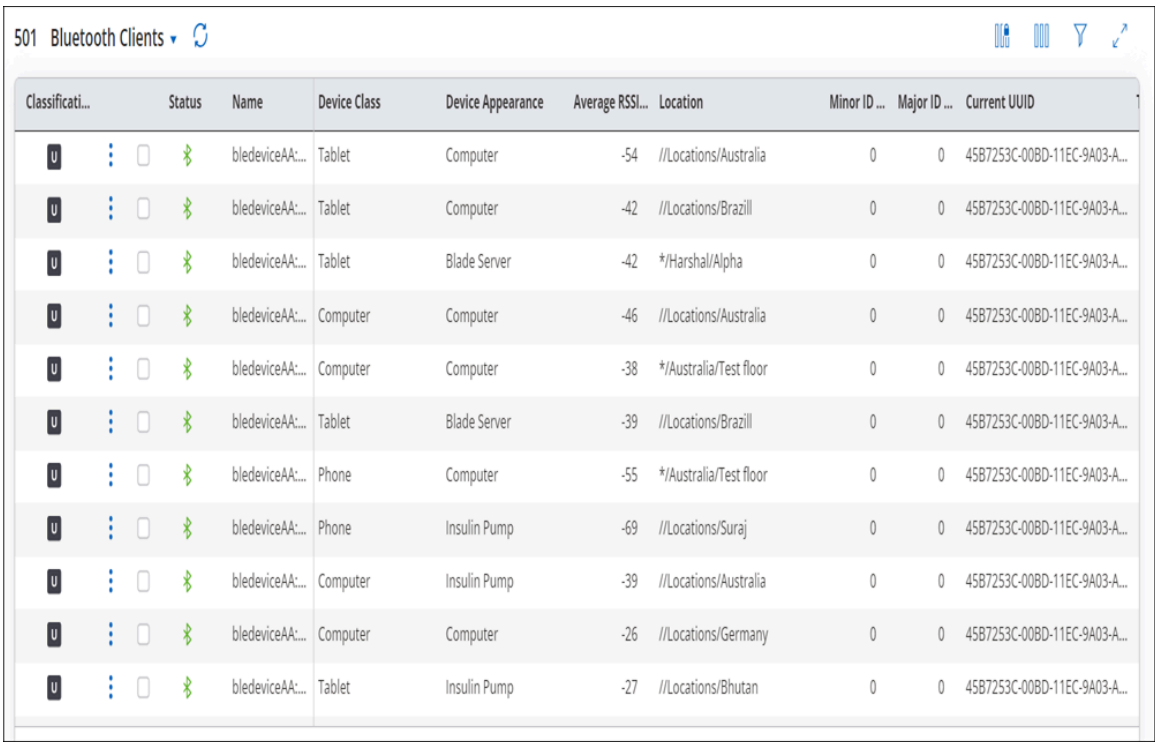
1. Navigate to **CONFIGURE** > **Device** > **Access Points.**
2. Under the **IOT Radios** tab, select **Bluetooth Scanning** checkbox.

Scanned Bluetooth Devices

Scanned and detected Bluetooth devices are available under **Monitor > WIPS > Clients.** To view Blueooth devices, click **Bluetooth Clients** from the drop-down menu.



Detected Bluetooth devices are displayed in a grid as follows:



You can perform the following actions on the visible Bluetooth devices:

- **Classification:** By default, Bluetooth devices are classified as **Uncategorized.** You can authorize a Bluetooth client by classifying it as **Authorized.**
- **Rename:** You can rename Bluetooth devices. You can also rename multiple Bluetooth devices at once. **Note:** You can rename authorized devices only.
- **Delete:** You can delete identified Bluetooth devices. **Note:** You can delete authorized and inactive devices only. When the deleted device is detected next time, it will be classified as Uncategorized.

Send Analytics to Third-Party Server

You can send information about visible Bluetooth devices such as MAC address and RSSI, and timestamp to third-party servers. This may be used by 3rd party systems, e.g. to determine client location using RSSI triangulation.

To send data to third-party servers,

1. Select **Push Analytics to Third-Party Server** checkbox under Bluetooth Scanning.
2. Enter values for the following fields and save your device settings.
    - Visibility Analytics Format: You can send the data as a CSV file or a JSON file.
    - Server URL: Enter the URL of the third-party server to send data.
    - Send Interval: Enter the time interval to send the data.
    - Authorization: Enter the authorization details for the third-party server. You can enter the Key or User Name and Password.

Bluetooth client's data will be sent to the configured server in regular time intervals.

19.20 Configure Uplink Port Authentication for Access Point

You can authenticate edge devices from a centrally managed network access control server using the 802.1X authentication. As a network administrator, you want to authenticate the access points (APs), before the APs connect to the network. To enable the authentication, you need to first configure the uplink port on the AP using CV-CUE.

Note:

The uplink port authentication is supported only on the eth0 port of the AP.

Supported Platforms:

- All switches supporting the 802.1X protocol (multi-host mode)
- All Wi-Fi 6 and higher version APs

Workflow

A new access point (AP) does not have the 802.1X configuration. When you connect a new access point to the switch via the uplink (eth0) port, the switch assigns a Guest VLAN (temporary VLAN) to the AP for that particular location. The AP uses the Guest VLAN to connect to the Wireless Manager and download the necessary configurations. Once the AP receives the configuration for uplink port authentication, the AP becomes capable of sending EAPOL frames. It comes out of the Guest VLAN and does uplink port authentication.

Further, the RADIUS server assigns a Native VLAN or Auth-Fail VLAN based on the authentication result.

The uplink port authentication is location-specific. If you change the location of the AP, it goes through a re-authentication process. The 802.1X network uses the EAP-TLS protocol for digital authentication.

For more information on Configuring 802.1X on the Switch Port, refer to Uplink Port Authentication for Access Point.

Prerequisites

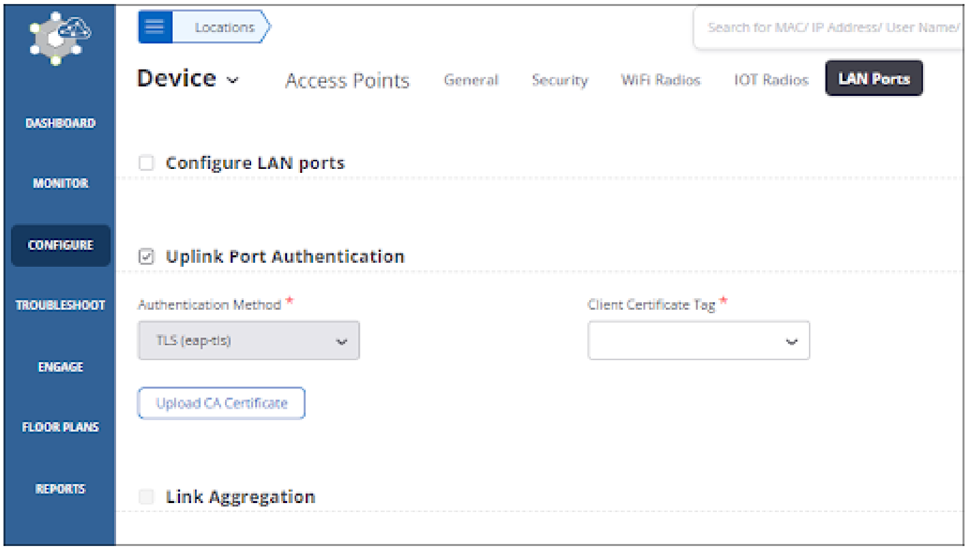
Ensure that you have already configured the necessary certificates in CV-CUE before you configure the uplink port authentication settings.

- CA certificate of the RADIUS server
- Device certificates, which are managed using tags

To Configure Uplink Port Authentication

1. Navigate to **CONFIGURE** > **Device** > **Access Points** > **-LAN Ports** tab.
2. Enable the **Uplink Port Authentication** check box.
3. Select the **Authentication Method** as **TLS (eap-tls).**

4. Select the certificate tag from the **Client Certificate Tag** drop-down list.

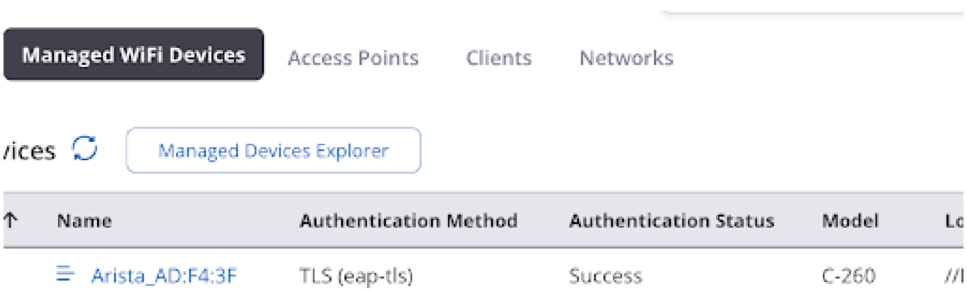


5. Click **Upload CA Certificate** and upload the CA certificate of the RADIUS server from your local drive.
6. Save the settings.

When Uplink Port Authentication is enabled, the Link Aggregation check box is disabled. That's because link aggregation is not supported for uplink port authentication. Similarly, if you have enabled Link Aggregation for a location, you cannot enable Uplink Port Authentication.

Verify Configuration

You can verify whether the uplink port authentication is enabled successfully from the **Managed WiFi Devices** tab in **MONITOR** > **Wired.**



You can also configure alerts to notify you for any authentication failure. You can view the alerts from **MONITOR** > **Alerts** > **System.**

19.21 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 VLAN Monitoring Parameters.

To configure VLAN Monitoring:

1. Navigate to **CONFIGURE** > **Device** > **Security.**
2. In the **VLAN Monitoring** section, select**Auto VLAN Monitoring** to automatically monitor the VLANs.
3. Select **Monitor Additional VLANs** to enable the device to monitor additional VLANs.
4. Enter the additional VLANs to be monitored as a comma-separated list.
5. Click **Save**.

19.21.1 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.

Field	Description
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.
Comma separated list of VLAN IDs	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. **Important:** If a VLAN is configured with a static IP address, then configure the VLAN from the CLI.

19.22 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.

To configure WIPS Settings:

1. Navigate to **CONFIGURE** > **Device.**
2. Go to **Security** tab.
3. Select **Offline Mode**.
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.

   Info: 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**.

19.22.1 WIPS Settings Parameters

The below table contains detail information about the parameters included in **WIPS Settings**.

Field	Description
Offline Mode	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).
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 allowed channels
Additionally, select intermediate channels	

Channel	Protocol	Frequency (GHz)
1	b/g/n	2.412
2	b/g/n	2.417
3	b/g/n	2.422
4	b/g/n	2.427
5	b/g/n	2.432
6	b/g/n	2.437
7	b/g/n	2.442
8	b/g/n	2.447
9	b/g/n	2.452
10	b/g/n	2.457
11	b/g/n	2.462
12	b/g/n	2.467
13	b/g/n	2.472
14	b/g/n	2.487
184	a/n/ac	4.92
188	a/n/ac	4.94
192	a/n/ac	4.96
196	a/n/ac	4.98
208	a/n/ac	5.04
212	a/n/ac	5.06
216	a/n/ac	5.08
34	a/n/ac	5.17
36	a/n/ac	5.18
38	a/n/ac	5.19
40	a/n/ac	5.2
42	a/n/ac	5.21
44	a/n/ac	5.22
46	a/n/ac	5.23
48	a/n/ac	5.24
50	a/n/ac	5.25
52	a/n/ac	5.26
56	a/n/ac	5.28
56	a/n/ac	5.28
58	a/n/ac	5.29

Channel	Protocol	Frequency (GHz)
60	a/n/ac	5.3
64	a/n/ac	5.32
100	a/n/ac	5.5
104	a/n/ac	5.52
108	a/n/ac	5.54
112	a/n/ac	5.56
116	a/n/ac	5.58
120	a/n/ac	5.6
124	a/n/ac	5.62
128	a/n/ac	5.64
132	a/n/ac	5.66
136	a/n/ac	5.68
140	a/n/ac	5.7
149	a/n/ac	5.745
152	a/n/ac	5.76
153	a/n/ac	5.765
153	a/n/ac	5.765
157	a/n/ac	5.785
160	a/n/ac	5.8
161	a/n/ac	5.805
161	a/n/ac	5.805
165	a/n/ac	5.825

19.23 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 Wi-Fi 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, 5, or 6 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 CV-CUE 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**.

3. Scroll down and select the **Push Visibility Analytics to Third-Party Server** check box.
4. Configure the fields shown in the following table:

Field	Description
Visibility Analytics Format	You can view the analytics data in CSV or JSON format.
Server URL	The URL of the third-party server.
Authorization	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.
Send Interval	The interval in seconds at which the AP sends RSSI values to the server.

5. Save the settings.

Chapter 20

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.

This chapter contains the following topics:

- Apply configuration to a Group by Switching on the SSID
- Copy Configuration from a Folder or Group

20.1 Apply configuration to a Group by Switching on the SSID

To configure a group by switching on the SSID:

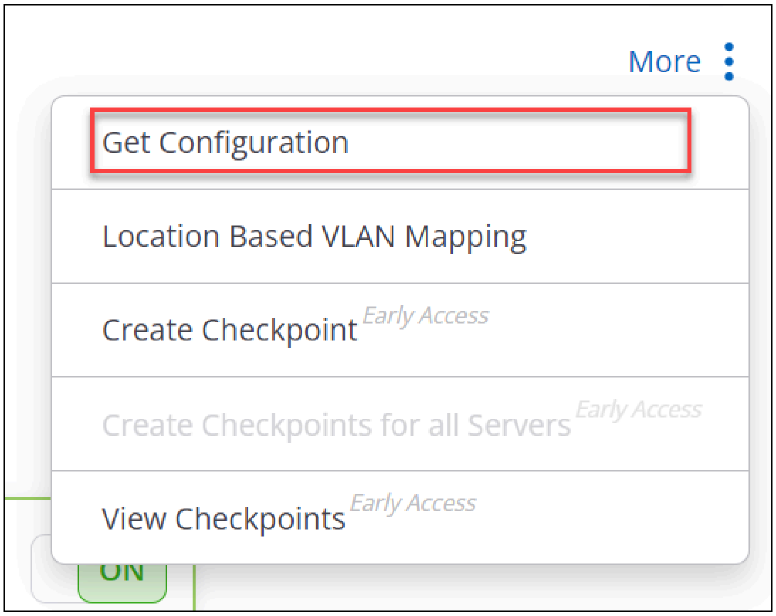
1. Navigate to **CONFIGURE** > **WiFI** > **SSID.**
2. Click on the hamburger icon (three horizontal lines) on the top left corner of the page.
3. Expand the list of groups, available at the bottom of the location pane.
4. Select the group to which you would like to apply the configuration. **Info:**On 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.

20.2 Copy Configuration from a Folder or Group

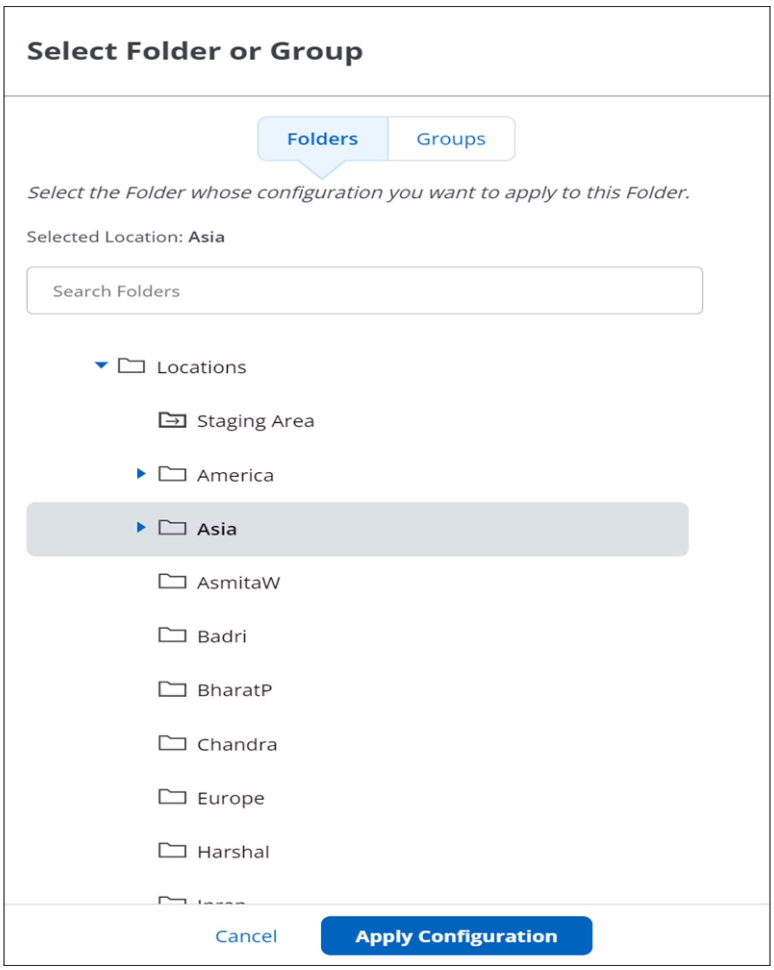
This option allows you to copy Wi-Fi configuration settings from a folder/group to an another folder/group.

To copy the settings to a different location or group, perform the following steps:

1. Go to **CONFIGURE** > **WiFi.**
2. Select the location where you want to copy the Wi-Fi settings and click **Get Configuration** from the more menu.



3. Under the **Select Folder** tab, select the location whose settings you want to copy.



4. Click **Apply Configuration**.
5. Click **Continue** in the pop-up dialog to copy the Wi-Fi configuration to the selected location.

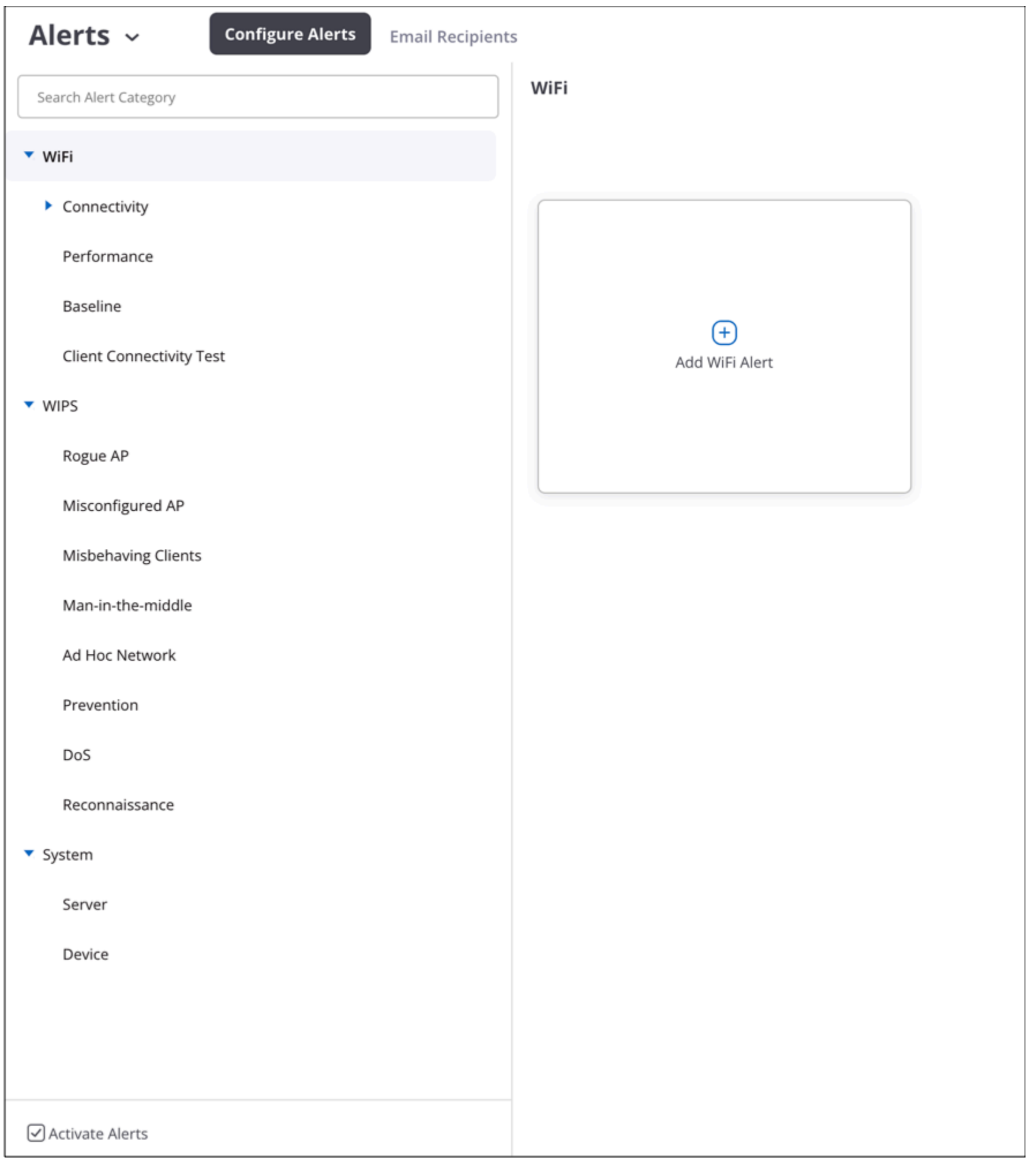
Similarly, you can copy the settings of a group at a location to an another group at a different location using Groups Navigator.

Chapter 21

Configure Alerts

CV-CUE 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.



This chapter contains the following topics:

- Configure Wi-Fi Alerts
- Configure WIPS Alerts

- Configure System Alerts
- Alerts Auto-Deletion

21.1 Configure Wi-Fi Alerts

You can define when Wi-Fi 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 Wi-Fi alerts can be configured.

Example 1: Poor Client Performance Alert

Suppose that you want CV-CUE 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 Wi-Fi.
- 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 CV-CUE 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 Wi-Fi.
- 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.

The following sections describe the various Wi-Fi alerts and the actions you can take to mitigate or counter them:

Table 11: Connectivity Alerts

Alert	Alert Description	Recommended Action	Default Setting Display | Email | Notify
Connection Failure	Connection Failure Alerts are triggered when clients experiencing connectivity issues exceed a certain number. You can configure an alert for the following connectivity issues: • Association • Network • Authentication To set a threshold for all connectivity issues, select Any from the drop-down menu.	Investigate the reason behind respective connection failures from Client Event Logs.	Disabled | Disabled | Disabled
Associated Clients by Location or Access Point (AP)	This alert is raised when the number of associations on AP exceeds the set threshold or the number of associations on location exceeds the set threshold.	Increase the number of APs at the location	Disabled | Disabled | Disabled

Table 12: Performance Alerts

Alert	Alert Description	Recommended Action	Default Setting Display | Email | Notify
Average Latency Exceeded	This alert is raised when the average latency for a particular SSID and frequency band exceeds the set threshold.	Check for network issues and take corrective actions according to the alert details.	Disabled | Disabled | Disabled

Table 13: Baseline Alert

Alert	Alert Description	Recommended Action	Default Setting Display | Email | Notify
Baseline Threshold Exceeded	This alert is raised when the Wi-Fi baseline for an SSID and frequency band exceeds the set threshold.	Take corrective actions according to the alert details.	Disabled | Disabled | Disabled

Table 14: Client Connectivity Test Alerts

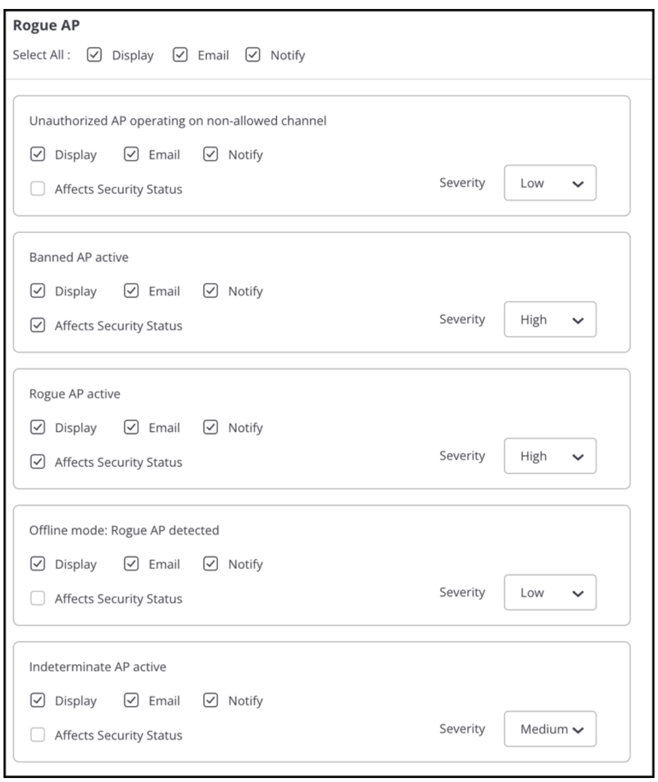
Alert	Alert Description	Recommended Action	Default Setting Display | Email | Notify
Client Connectivity Test Fail	This alert is raised when a scheduled client connectivity test fails.	Investigate the result behind the client connectivity failed test.	Disabled | Disabled | Disabled

21.2 Configure WIPS Alerts

WIPS alerts are related to Wi-Fi vulnerabilities and attacks that may pose a security threat to your network.

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.

WIPS Alert Type	Description
Rogue AP	Alerts for any potentially rogue APs. Examples: Unauthorized AP connected to the enterprise wired network, Banned AP, Unauthorized AP on non-allowed channels.
Misconfigured APs	Alerts for any AP behavior that deviates from the authorized Wi-Fi policy. Examples: Change in an authorized AP's SSID, No encryption on an authorized AP.
Misbehaving Clients	Alerts for any client behavior that could compromise network security. Examples: Authorized client association with an external AP, Unauthorized client association with an authorized AP.
Man-in-the-middle	Alerts for potential man-in-the-middle type attacks. Examples: Honeypot/evil twin active, PS-poll attack.
MAC Spoofing	Alerts for AP and client MAC spoofing.
Ad-hoc Network	Alerts for an authorized client participating in an ad-hoc network.
Prevention	Intrusion prevention related alerts. Examples: Device reached maximum prevention capacity, AP/client needs to be prevented.
DoS	Alerts for potential DoS type attacks. Examples: Disassociation flood attacks, Deauthentication flood attacks.

WIPS Alerts

The following sections describe the various WIPS alerts and the actions you can take to mitigate or counter them:

Table 15: Rouge AP Alerts

Alert	Alert Description	Recommended Action	Default Setting Display | Email | Notify | Affects Severity Status
Banned AP active	This alert is raised when a banned AP gets active.	Locate the banned AP and remove it from the network. You can use the location tracking feature to locate this device. You can configure Intrusion Prevention to automatically prevent banned APs. You can also manually prevent an AP from the list of monitored APs.	Disabled | Disabled | Disabled | Disabled
Rogue AP active	This alert is raised when a rogue AP gets active. This is a serious security violation. Unauthorized users can gain access to the network if they are within the radio coverage of this AP.	You can use the location tracking feature to locate this AP on the floor map. If you have enabled the corresponding setting in the Intrusion Prevention Policy, WIPS will automatically prevent rogue APs. You can also manually prevent the AP from the list of monitored APs. However, note that prevention is not a permanent solution.	Enabled | Enabled | Enabled | Enabled
Offline mode: Rogue AP detected	This alert is raised when a Rogue AP is detected in the offline mode operation of an Arista device. This AP is not one of your authorized APs and is plugged into the network. This AP could have been used to gain unauthorized access to the network.	As mitigation against this threat, configure the policies to automatically prevent Rogue APs.	Enabled | Disabled | Disabled | Disabled

Alert	Alert Description	Recommended Action	Default Setting Display | Email | Notify | Affects Severity Status
Indeterminate AP active	This alert is raised when an indeterminate AP becomes active.	WIPS cannot determine if this AP is connected to your network. If you know this AP, mark it authorized or external as appropriate. Otherwise, locate the AP and investigate if it poses a security threat to your network. You can use the location tracking feature to locate this AP on the floor map. You can configure Intrusion Prevention to automatically prevent either authorized or all clients from connecting to indeterminate APs. You can also manually prevent an AP from the list of monitored APs. However, note that prevention is not a permanent solution.	Disabled | Disabled | Disabled | Disabled
Unauthorized AP operating on non-allowed channel	This alert is rasied when an unauthorized AP starts operating on an non-allowed channel.	Operation on non-allowed channels amounts to a violation of the country's wireless communication laws. You can use the location tracking feature to locate the device.	Enabled | Disabled | Disabled | Disabled

Table 16: MAC Spoofing Alerts

Alert	Alert Description	Recommended Action	Default Setting Display | Email | Notify | Affects Severity Status
Client MAC Spoofing	This alert is raised when the spoofing of MAC address of an authorized client is in progress. With MAC spoofing, an attacker imitates an authorized client by advertising the same identity as the latter. This is a serious security violation.	Locate the attacker client and remove it immediately from the network. You can also manually prevent the client from the list of monitored clients. However, note that prevention is not a permanent solution.	Disabled | Disabled | Disabled | Disabled
AP MAC Spoofing	This alert is raised when spoofing of the MAC address of an authorized AP is in progress. The same MAC is visible to two devices. With MAC spoofing, an attacker AP imitates an authorized AP by advertising the same identity as the latter. This is a serious security violation.	Locate the fake AP and remove it from the network.If you have enabled the corresponding Intrusion Prevention setting, WIPS will automatically prevent APs with the same MAC address. You can also manually prevent the AP from the list of monitored APs. However, note that prevention is not a permanent solution.	Disabled | Disabled | Disabled | Disabled

Table 17: Misbehaving Client Alerts

Alert	Alert Description	Recommended Action	Default Setting Display | Email | Notify | Affects Severity Status
Offline mode: Authorized client association with rogue AP detected	This alert is raised when an authorized client association with rogue AP is detected. Authorized Client connecting to Rogue AP may be due to misconfiguration of the Client.	Rogue APs must be located and removed. As mitigation against this threat, configure Intrusion Prevention to automatically quarantine rogue APs.	Disabled | Disabled | Disabled | Disabled
Offline mode: Authorized client association with external AP detected	This alert is raised when an authorized client association with an external AP is detected. Such associations pose a security threat to the client and the network.	Configure authorized clients to prevent such associations. For example, ensure that the client connects to only those APs that advertise your corporate network SSID. As mitigation, configure Intrusion Prevention to automatically prevent authorized clients that connect to APs categorized as external.	Disabled | Disabled | Disabled | Disabled
Offline mode: Authorized client association with Honeypot AP detected	This alert is raised when an authorized client association with Honeypot AP is detected. This can happen if Intrusion Prevention has not been configured to automatically prevent authorized clients from associating with Honeypot/ Even Twin APs. It can also happen if a managed WiFi device is unable to prevent the association due to overload or limited visibility. Such connections pose a security threat as Authorized Clients may unwittingly provide confidential information (e.g. passwords) to the External AP over these connections. The External AP can also insert itself as a man-in-the-middle for authorized communications using this connection. It can also perform port scanning on the Client to discover its vulnerabilities.",	Locate and remove such APs. If this cannot be done, change the SSIDs of your authorized APs. As mitigation against this threat, configure Intrusion Prevention to prevent authorized clients from associating with Honeypot/Evil Twin APs.	Disabled | Disabled | Disabled | Disabled

Alert	Alert Description	Recommended Action	Default Setting Display | Email | Notify | Affects Severity Status
Offline mode: Unauthorized/ Uncategorized client association with authorized AP detected	This alert is raised when unauthorized or uncategorized client association with authorized AP is detected. Such associations pose a security threat to the network.	Use either WPA or 802.11i on authorized APs. Also, use SSIDs different from those used by neighboring networks. As mitigation, configure Intrusion Prevention to prevent Unauthorized/Uncategorized clients from associating with authorized APs.	Disabled | Disabled | Disabled | Disabled
Offline mode: Unauthorized/ Uncategorized client association with rogue AP detected	This alert is raised when unauthorized or uncategorized client association with rogue AP is detected. Such associations allow unauthorized clients to access your network. This is a serious security violation.	Locate and remove the rogue AP. As mitigation against this threat, configure Intrusion Prevention to automatically prevent rogue APs.	Disabled | Disabled | Disabled | Disabled
Offline mode: Soft AP detected	This alert is raised when a wireless client is operating as a Soft AP. A Soft AP is a wireless client operating as an access point. If this client is connected to the enterprise network (over the Ethernet, for example), unauthorized users can access the network through it.	Recommended action: Locate the client and shut it down.	Disabled | Disabled | Disabled | Disabled
Authorized client connection to guest SSID of authorized AP	This alert is raised when an authorized client gets connected to the guest SSID of an authorized AP. Guest SSIDs provide wireless access to guests. They are usually less secure than enterprise SSIDs. Authorized clients should not be connecting to guest SSIDs.	Remove SSID of Guest AP from the wireless profiles in the client. Instruct Authorized users to not connect to Guest APs. You can also configure layer-2 encryption such as static WEP on Guest APs to prevent accidental connection of Authorized Clients to Guest APs.	Enabled | Disabled | Enabled | Enabled

Alert	Alert Description	Recommended Action	Default Setting Display | Email | Notify | Affects Severity Status
Banned client active	This alert is raised when a banned client gets active.	Locate the banned client and remove it from the network. You can use the location tracking feature to locate this device. You can configure Intrusion Prevention to automatically prevent banned clients from connecting to your APs. You can also manually prevent a client from the list of monitored clients.	Enabled | Enabled | Enabled | Enabled
Client in Bridging/ICS configuration	This alert is raised when a client is bridging its wireless interface and other network interface(s). If the other network interface(s) is connected to your enterprise network, the enterprise network will become accessible to unauthorized users via the wireless interface of this client.	Check the client configuration and disable the bridging or Internet Connection Sharing (ICS) option. Until then, if you have enabled the corresponding Intrusion Prevention setting, WIPS will automatically prevent such devices from engaging in wireless communication.	Disabled | Disabled | Disabled | Disabled
Rogue client active	This alert is raised when a rogue client is active. A client is marked as rogue if it falls under any of the following conditions: • An authorized client that connects to a rogue AP. • An external or Uncategorized client that connects to an authorized AP when the relevant automatic client authorization policies are not in force. • A client bridges its wireless interface to a monitored enterprise wired network. A rogue client poses a threat by allowing unauthorized access to the enterprise network.	The rogue client will be automatically disrupted if the relevant Intrusion Prevention setting is enabled. Locate the rogue client using the location tracking feature. If this is a client connecting to a rogue AP or an external/ Uncategorized client connecting to an authorized AP, shut the client down. If this client is bridging its wireless interface to the enterprise wired network, correct its wireless configuration settings.	Disabled | Disabled | Disabled | Disabled

Alert	**Alert Description**	**Recommended Action**	**Default Setting** **Display | Email | Notify | Affects Severity Status**
Guest client mis-association	This alert is raised when a guest client gets connected to an unauthorized AP. The AP may not be malicious but such connections pose a security threat to the client and the network.	Configure the guest client to avoid such connections. For example, ensure that the client connects only to APs broadcasting your guest or corporate network SSID. If you enable the corresponding Intrusion Prevention setting, WIPS can prevent such connections.	Disabled | Disabled | Disabled | Disabled
Unauthorized client connection to guest SSID	This alert is raised when an unauthorized client gets connected to a guest SSID. Such connections can degrade the performance of your guest clients as they have to share the guest network bandwidth.	Ensure that you do not use commonly used SSIDs as your Guest SSID or the Guest SSID is not the same as one of your neighbors' SSIDs. Also, consider setting up WEP or WPA/WPA2 with PSK authentication on your guest network to prevent such associations. You can also set up an intrusion prevention policy to automatically disrupt such associations.	Disabled | Disabled | Disabled | Disabled
Authorized client mis-association	This alert is raised when an authorized client gets connected to an unauthorized AP. The AP may not be malicious but such connections pose a security threat to the client and the network.	Configure authorized clients to avoid such connections. For example, ensure that authorized clients connect only to APs broadcasting your corporate network SSID. You can enable the corresponding Intrusion Prevention settings to disallow authorized client mis-associations.	Enabled | Disabled | Enabled | Enabled

Alert	Alert Description	Recommended Action	Default Setting Display | Email | Notify | Affects Severity Status
Soft Mobile Hotspot AP or Windows 7 Virtual AP Active	This alert is raised when a soft Mobile Hotspot AP or Windows 7 Virtual AP gets detected on a client. Clients running the Soft Mobile Hotspot AP or Windows 7 Virtual AP pose a serious security threat to the enterprise. If such a Client is also connected to the wired network, it can expose the Enterprise network to anyone who connects to the Soft Mobile Hotspot AP or Windows 7 Virtual AP.	Locate such clients and change their settings to stop this AP. Operating Systems like Windows 7 make it easy for users to create such APs. Several smart mobile device platforms such as Apple iOS and Android also natively provide hotspot AP features. Hence users must also be educated about the security threats from such settings.	Disabled | Disabled | Disabled | Disabled
Client authenticated using a non-compliant authentication type	This alert is raised when a client associated with an authorized AP uses the non-compliant authentication type instead of the allowed authentication type.	Ensure that the authentication server, the AP, and the WLAN infrastructure policy are all correctly configured. Use the location of the event and the details of the participating AP device to reach the AP to check its settings.	Disabled | Disabled | Disabled | Disabled
Unauthorized client connection to authorized AP	This alert is raised when an unauthorized client gets connected to an authorized AP. Such connections pose a security threat to the network.	Ensure that your network is not using an SSID being used on neighboring networks. Enforce an authentication policy between authorized APs and authorized clients. Until then, if you have enabled the corresponding Intrusion Prevention settings, WIPS will automatically prevent unauthorized clients. You can manually prevent the client from the list of monitored clients. Note: You might be preventing a client on a neighboring network.	Disabled | Disabled | Disabled | Disabled

Table 18: Man-in-the-middle Alerts

Alert	Alert Description	Recommended Action	Default Setting Display | Email | Notify | Affects Severity Status
Honeypot/Evil Twin active	This alert is raised when a Honeypot/Evil Twin AP is active. A potentially external AP is advertising an SSID used in your authorized WiFi Policy. This can lure your authorized clients into connecting to the external AP. Such connections pose a security threat because authorized clients may unwittingly provide confidential information (e.g. passwords) to the external AP. The external AP can also insert itself as a man-in-the-middle for authorized communications using this connection. It can also perform port scanning on the client to discover its vulnerabilities.	Locate the Honeypot AP and remove it from the vicinity of your network. Until then, if you have enabled the corresponding Intrusion Prevention setting, WIPS will prevent authorized clients from connecting to Honeypot APs. You can use the location tracking feature to locate this AP. Note: Location tracking might be inaccurate if the attacker is not on your premises.	Enabled | Enabled | Enabled | Enabled
Offline Mode: Honeypot AP detected	This alert is raised when a Honeypot AP is detected. The AP is advertising an SSID used in your WiFi network. This may lure your authorized clients into connecting to the AP.	Locate and remove the AP. If this cannot be done, change the SSIDs of your authorized APs. As mitigation against this threat, configure Intrusion Prevention to prevent authorized clients from associating with Honeypot/Evil Twin APs.	Enabled | Disabled | Disabled | Disabled
PS-Poll attack in progress	This alert is raised when a PS-Poll attack is in progress against an authorized AP and client. In a PS-Poll attack, an attacker sends spoofed PS-Poll messages to the AP in order to steal the victim client's data. A flood of PS-Poll packets can even be used to starve a client when the client is in power-saving mode.	Locate the attacker device and shut it down immediately. You can use the event location tracking feature to locate the attacker on the floor map. Note: Location tracking might be inaccurate if the attacker is not on your premises.	Disabled | Disabled | Disabled | Disabled

Table 19: MAC Spoofing Alerts

Alert	**Alert Description**	**Recommended Action**	**Default Setting** **Display | Email | Notify | Affects Severity Status**
Client MAC Spoofing	This alert is raised when the spoofing of MAC address of an authorized client is in progress. With MAC spoofing, an attacker imitates an authorized client by advertising the same identity as the latter. This is a serious security violation.	Locate the attacker client and remove it immediately from the network. You can also manually prevent the client from the list of monitored clients. However, note that prevention is not a permanent solution.	Disabled | Disabled | Disabled | Disabled
AP MAC Spoofing	This alert is raised when spoofing of the MAC address of an authorized AP is in progress. The same MAC is visible to two devices. With MAC spoofing, an attacker AP imitates an authorized AP by advertising the same identity as the latter. This is a serious security violation.	Locate the fake AP and remove it from the network.If you have enabled the corresponding Intrusion Prevention setting, WIPS will automatically prevent APs with the same MAC address. You can also manually prevent the AP from the list of monitored APs. However, note that prevention is not a permanent solution.	Disabled | Disabled | Disabled | Disabled

Table 20: Ad-hoc Network Alerts

Alert	**Alert Description**	**Recommended Action**	**Default Setting** **Display | Email | Notify | Affects Severity Status**
Offline mode: Authorized client detected in ad-hoc connection mode	This alert is raised when an authorized client is detected in an ad-hoc connection. Ad-hoc connections pose a security threat because unauthorized wireless clients can connect to authorized clients in ad-hoc mode.	Reconfigure such clients to not advertise or participate in ad-hoc networks. As mitigation, configure Intrusion Prevention to automatically prevent authorized clients that participate in any ad-hoc network.	Disabled | Disabled | Disabled | Disabled
Authorized client participating in ad-hoc network	This alert is raised when an ad-hoc network involving one or more authorized clients is active. Ad-hoc connections pose a security threat. Unauthorized clients can launch attacks on authorized clients via ad-hoc connections. Ad-hoc connections among authorized clients are also undesirable because enterprise security policies cannot be enforced on these connections.	See the sub-events of this event for information on clients participating in this ad-hoc network. Locate the authorized client(s) involved in the ad-hoc network and configure these clients to not use ad-hoc connections. You can use the location tracking feature to locate these clients on the floor map. Until then, if you have enabled the corresponding Intrusion Prevention settings, WIPS will prevent authorized clients from communicating over ad-hoc connections.	Disabled | Disabled | Disabled | Disabled

Table 21: Prevention Alerts

Alert	Alert Description	Recommended Action	Default Setting Display | Email | Notify | Affects Severity Status
AP reached maximum prevention capacity	WIPS raises this alert when AP reaches the maximum prevention capacity.This access point will no longer be able to prevent unwanted communication on a new channel. The Intrusion Prevention Level is a trade-off between prevention strength and the number of channels prevented simultaneously.	If you want to configure the AP to simultaneously quarantine on more channels, you must reduce the Intrusion Prevention Level. However, doing so will weaken the prevention and some packets might go through.	Enabled | Disabled | Disabled | Disabled
AP needs to be prevented	This alert is raised when an AP needs to be prevented.	Identify the reason for AP prevention. See the sub-events and the help for details. If the necessary conditions are satisfied (for example, the device is operating on a legal channel, and resources are available for prevention), then this AP will be prevented. Eliminate the condition that caused WIPS to prevent this AP.	Enabled | Disabled | Disabled | Disabled
Client needs to be prevented	This alert is raised when a client needs to be prevented.	Identify the reason for client prevention. See the sub-events and the help for details. If the necessary conditions are satisfied (for example, the device is operating on a legal channel, resources are available for prevention), then this client will be prevented.	Enabled | Disabled | Disabled | Disabled

Table 22: DoS Alerts

Alert	Alert Description	Recommended Action	Default Setting Display | Email | Notify | Affects Severity Status
Offline mode: DoS attack detected	This alert is raised when WIPS detects a DoS attack on a device. DoS attacks try to disrupt authorized communication.	Locate the device and shut it down or disconnect it from the network.	Disabled | Disabled | Disabled | Disabled
Disassociation flood attack in progress	This alert is raised when a disassociation flood attack is in progress against an authorized AP and client. A disassociation flood attack is a DoS attack wherein an attacker sends spoofed disassociation messages to break or prevent a connection between the victim AP and a client.	Locate the attacker device and shut it down immediately. You can use the event location tracking feature to determine the physical location of the attacker on the floor map.	Disabled | Disabled | Disabled | Disabled
Disassociation broadcast attack in progress	This alert is raised when a disassociation broadcast attack is in progress against an authorized AP. A disassociation broadcast attack is a DoS attack wherein an attacker sends spoofed broadcast disassociation messages to break or prevent all client connections to the victim AP. While this attack is in progress, no client will be able to connect to the AP.	Locate the attacker device and shut it down immediately. You can use the event location tracking feature to determine the physical location of the attacker on the floor map.	Disabled | Disabled | Disabled | Disabled
Association flood attack in progress	This alert is raised when an association flood attack is in progress against an authorized AP. An association flood attack is a DoS attack wherein an attacker overwhelms the victim AP with connection requests (usually with spoofed source MAC addresses in them). This can quickly fill up the association table of an AP and prevent it from accepting any new connection requests from legitimate clients.	Locate the attacker device and shut it down immediately. Then reset the AP so that its association table frees up. You can use the event location tracking feature to determine the physical location of the attacker on the floor map.	Disabled | Disabled | Disabled | Disabled

Alert	Alert Description	Recommended Action	Default Setting Display | Email | Notify | Affects Severity Status
Association table overflow	This alert is raised when WIPS detects an overflown association table at an authorized AP. The association table keeps track of successful associations to the authorized AP. Association table overflow happens when the number of successful associations exceeds 127 clients as a result of the AP receiving a large number of connection requests in a short period of time. This could happen due to a large number of legitimate connection requests or due to a DoS attack such as an association flood attack in which the attacker deliberately generates a large number of connection requests. The AP cannot accept new connection requests when its association table is full.	If you suspect that a DoS attack is in progress, locate the attacker device and shut it down immediately. If there is no DoS attack in progress, then the table could have overflowed due to high client density in this area. In any case, reset the AP so that its association table frees up. If the client density remains high in this area, then consider adding more APs.	Disabled | Disabled | Disabled | Disabled
Fake client detected	This alert is raised when WIPS detects the use of a fake client tool near an AP. Fake client tool generates a large number of bogus Probe Requests with different MAC addresses. This can fill up the databases of WiFi security and management systems with bogus client records.	Locate the device running the fake client tool and shut it down immediately or disconnect it from the network.	Disabled | Disabled | Disabled | Disabled

Alert	Alert Description	Recommended Action	Default Setting Display | Email | Notify | Affects Severity Status
Deauthentication flood attack in progress	This alert is raised when a de-authentication flood attack is in progress against an authorized AP and client. A de-authentication flood attack is a DoS attack wherein the attacker sends spoofed de-authentication messages to break or prevent a connection between the victim AP and a client. While this attack is in progress, the client cannot connect to the AP.	Locate the attacker device and shut it down immediately. You can use the event location tracking feature to locate the attacker on the floor map. Note: Location tracking might be inaccurate if the attacker is not on your premises.	Disabled | Disabled | Disabled | Disabled
Deauthentication broadcast attack in progress	This alert is raised when a de-authentication broadcast attack is in progress against an authorized AP. A deauthentication broadcast attack is a DoS attack wherein the attacker sends spoofed broadcast de-authentication messages to break or prevent all client connections to the victim AP.	Locate the attacker device and shut it down immediately. You can use the event location tracking feature to determine the physical location of the attacker on the floor map.	Disabled | Disabled | Disabled | Disabled
Authentication flood attack in progress	This alert is raised when an authentication flood attack is in progress against an authorized AP. An authentication flood attack is a DoS attack wherein the attacker overwhelms the victim AP with connection requests, usually with spoofed source MAC addresses in them. This can quickly fill up the connection table of an AP and prevent it from accepting any new connection requests from legitimate clients.	Locate the attacker device and shut it down immediately. Then reset the AP so that its connection table frees up. This event could be accompanied by another DoS attack that actively disconnects clients from APs. This is because some clients aggressively try to reconnect to the AP and flood the wireless medium with Authentication Requests. You can use the event location tracking feature to determine the physical location of the attacker on the floor map.	Disabled | Disabled | Disabled | Disabled

Alert	Alert Description	Recommended Action	Default Setting Display | Email | Notify | Affects Severity Status
EAPOL Logoff flood attack in progress	This alert is raised when a EAPOL Logoff flood attack is in progress against an authorized AP and client. EAPOL Logoff flood attack is a DoS attack wherein an attacker sends spoofed EAPOL Logoff messages to an AP to break the connection between the AP and its client. While this attack is in progress, the client cannot connect to the AP.	Locate the attacker device and shut it down immediately. You can use the event location tracking feature to determine the physical location of the attacker on the floor map. Note: Location tracking might be inaccurate if the attacker is not on your premises.	Disabled | Disabled | Disabled | Disabled
EAPOL Start flood attack in progress	This alert is raised when an EAPOL Start flood attack is in progress against an authorized AP. EAPOL Start flood attack is a DoS attack wherein an attacker overwhelms an AP with EAPOL Start requests (usually with spoofed source MAC addresses in them). This can quickly fill up the association table of the AP and prevent it from accepting any new connection requests from legitimate clients. An EAPOL Start flood is always accompanied by an Authentication flood and an Association flood because authentication and association are prerequisites for an EAPOL Start request.	Locate the attacker device and shut it down immediately. Then reset the AP. You can use the event location tracking feature to determine the physical location of the attacker on the floor map. Note: Location tracking might be inaccurate if the attacker is not on your premises.	Disabled | Disabled | Disabled | Disabled

Alert	**Alert Description**	**Recommended Action**	**Default Setting** **Display | Email | Notify | Affects Severity Status**
Premature EAP Success attack in progress	This alert is raised when a Premature EAP Success attack is in progress against an authorized AP and client. Premature EAP Success attack is a DoS attack wherein the attacker sends spoofed EAP Success messages to a client to confuse its EAP state machine. This can result in repeated restarting of the client's EAP state machine, preventing the client from connecting to an AP.	Locate the attacker device and shut it down immediately. You can use the event location tracking feature to determine the physical location of the attacker on the floor map. Note: Location tracking might be inaccurate if the attacker is not on your premises.	Disabled | Disabled | Disabled | Disabled
Premature EAP Failure attack in progress	This alert is raised when a Premature EAP Failure attack is in progress against an authorized AP and client. Premature EAP Failure attack is a DoS attack wherein the attacker sends spoofed EAP Failure messages to a client to confuse its EAP state machine. This can result in repeated restarting of the client's EAP state machine, preventing the client from connecting to an AP.	Locate the attacker device and shut it down immediately. You can use the event location tracking feature to determine the physical location of the attacker on the floor map. Note: Location tracking might be inaccurate if the attacker is not on your premises.	Disabled | Disabled | Disabled | Disabled
Fake AP detected	This alert is raised when WIPS detects the use of fake AP tool. The Fake AP tool generates a large number of bogus beacon frames with different MAC addresses. This confuses wireless clients. It can also fill up the databases of WiFi security and management systems with bogus AP records.	Locate the device running the fake AP tool and shut it down immediately or disconnect it from the network.	Disabled | Disabled | Disabled | Disabled

Alert	Alert Description	Recommended Action	Default Setting Display | Email | Notify | Affects Severity Status
RTS/CTS flood	This alert is raised when WIPS detects an RTS/CTS flood on a particular channel near an AP. RTS/CTS flooding is a DoS attack wherein an attacker sends requests to reserve the wireless channel for large durations (usually with spoofed source MAC addresses in them). These requests can block legitimate devices operating on that channel from accessing the wireless medium.	Locate the attacker device and shut it down immediately.	Disabled | Disabled | Disabled | Disabled

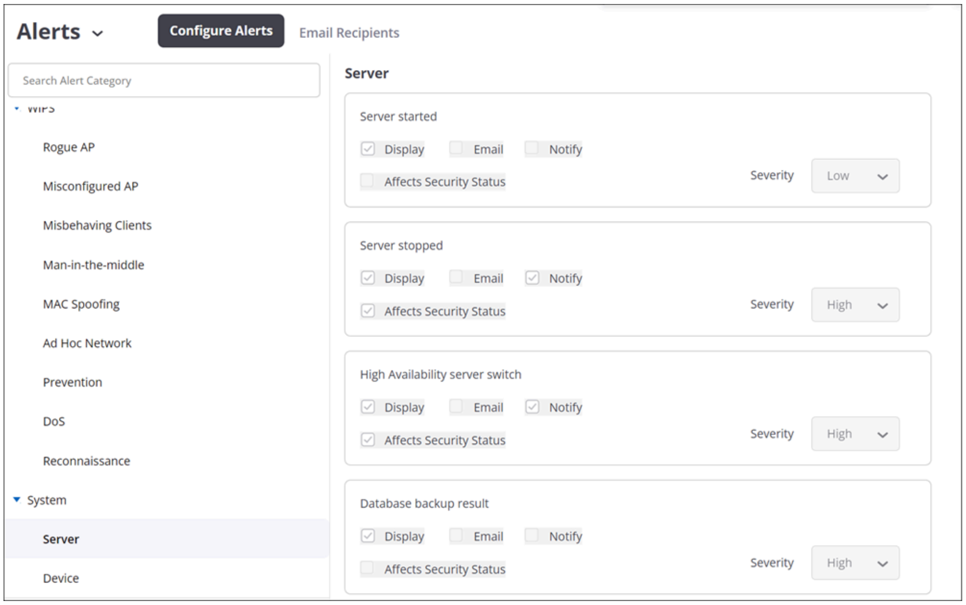
Table 23: Reconnaissance Alerts

Alert	Alert Description	Recommended Action	Default Setting Display | Email | Notify | Affects Severity Status
Cellular activity detected	This alert is raised when WIPS detects cellular activity near one or more managed Wi-Fi devices. One or more cellular connections are active within 40 feet of the device.	Move the cellular device away from the Wi-Fi device.	Disabled | Disabled | Disabled | Disabled
Excessive NULL probes detected	This alert is raised when WIPS detects Excessive NULL Probe Requests detected near an access point. Typically, NULL probes come from a harmless Windows/Linux laptop when it is not able to associate with an AP in its vicinity. However, the NULL probes could be from a client running a network scanning tool such as Netstumbler, Wellenreiter. Such tools gather information about the wireless network.	Track the location of the client and check if this client is able to associate to any AP in the vicinity. If the Client is not engaged in network scanning or malicious activity, no action is required.	Disabled | Disabled | Disabled | Disabled

21.3 Configure System Alerts

System alerts are triggered by events related to the Wi-Fi server (e.g., the active server switches to the standby server) or the AP/Sensor (for example, a new network is detected or the memory utilization exceeded a certain threshold). 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, CV-CUE 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.

The following section describes the various System alerts and the actions you can take to mitigate or counter them:

Table 24: Server Alerts

Alert	Alert Description	Recommended Action	Default Setting Display | Email | Notify | Affects Severity Status
Server started	This is an informational alert raised when a server instance starts or boots up.	This is an information alert. No action is required.	Enabled | Disabled | Disabled | Disabled
Server stopped	This is an informational alert raised when a server instance stops.	If this is not a planned shutdown, investigate why the server stopped.	Enabled | Disabled | Disabled | Enabled
Database backup result	This alert is raised when the server takes a backup of the database. This alert captures the remote server IP address and the remote file details.	If the database backup failed, verify the following: • Connectivity with the backup server. • The credentials to authenticate on the backup server. • The account provided has write permissions on the backup server. • The backup server has enough disk space.	Enabled | Disabled | Disabled | Disabled
Database restore result	This alert is raised when the server restores the database.	If the restore operation is successful, the current server database is overwritten with the restored database. This is an informational alert. Ensure that this action was performed by authorized personnel.	Enabled | Disabled | Disabled | Disabled
Automatic deletion done	This alert is raised when a scheduled automatic deletion job is completed on a server. This job deletes old and inactive access points, clients, unmonitored networks, device prevention history, old events, and user action logs.	This is an information alert. No action is required.	Enabled | Disabled | Disabled | Disabled
Device connection rejected; licensed limit reached	This alert is raised when you attempt to connect a device to a server after the number of devices connected has already reached the number of devices per your license.	To connect more devices, apply for a new license allowing more devices. Contact Technical Support for information on procuring the license.	Enabled | Disabled | Enabled | Disabled

Alert	Alert Description	Recommended Action	Default Setting Display | Email | Notify | Affects Severity Status
High Avaibility Server Switch	This alert is raised when the server switches to standby server. After the HA failover, the server that was on standby becomes the Active server. When the server that was the Active one before the failover recovers, it becomes the Standby server.	If this event is raised when Failover mode is set to Automatic, the Active server may be down or its connectivity with the Standby server over the network interface may be down. Unless both appliances are ON and connected, the HA feature will not work.	Enabled | Disabled | Disabled | Enabled
Data synchronization link is up	This alert is raised when The connection between the Active and Standby servers is done. Active and Standby servers are now connected	This is an information alert. No action is required.	Enabled | Disabled | Disabled | Disabled
Data synchronization link is down	This affects server availability because the Standby server is no longer connected to the Active server. Data synchronization with the Active server is essential in case the Standby server needs to take over from the Active server.	Restore the link between the Active and Standby servers.	Enabled | Enabled | Enabled | Enabled
Data synchronization is lagging	This alert is raised when database synchronization between Active and Standby servers is slow.	Check the Data Sync link between the two servers. If it is up, then the lag may be temporary. Wait for few minutes and then check if 'Data Synchronization State' is 'Complete' in the 'get ha' CLI. If it is not 'Complete', contact Technical Support.	Enabled | Enabled | Enabled | Disabled
Inactive Clients Detected	This alert is raised when server detects inactive clients that are eligible for deletion.	Enable Auto Deletion for Inactive Clients. To enable Auto Deletion, go to Monitor>WIPS>Clients, and click Auto Deletion..	Enabled | Disabled | Disabled | Disabled

Table 25: Device Alerts

Alert	Alert Description	Recommended Action	Default Setting Display | Email | Notify | Affects Severity Status
CPU utilization exceeds X for X minutes	This alert is raised when the AP's CPU utilization exceeds your configured threshold for the configured time duration.	Configure optimal utilization threshold values.	Enabled | Enabled | Enabled| Disabled
Memory utilization exceeds X for X minutes	This alert is raised when the AP's memory utilization exceeds the configured threshold for the configured time duration.	Configure optimal memory utilization threshold values.	Enabled | Enabled | Enabled| Disabled
Access point is not reachable by the server for at least X minutes	This alert is raised when the AP is not reachable by the server since the last configuration time duration.	Investigate why the AP device is not reachable by the server. It could be due to network issues, power issues with the device, or a planned disconnection of the device from the network.	Enabled | Enabled | Disabled| Disabled
The number of access points with failed firmware update exceeds X	This alert is raised when a certain number of APs with failed firmware update exceeds the configured threshold.	Check for network connectivity issues. Contact Technical Support if the problem persists.	Disabled | Disabled | Disabled | Disabled
Authorized AP inactive	This alert is raised when an authorized AP becomes inactive. Clients cannot connect to an inactive AP and it can create a coverage gap in your Wi-Fi network.	If this is not a planned shutdown, investigate why the AP was shut down. Restart the AP.	Disabled | Disabled | Disabled | Disabled
Authorized AP disconnected from network	This alert is raised when an authorized AP gets disconnected from the network. A disconnected AP can create a gap in the WLAN coverage of your Wi-Fi network as it prevents authorized clients from accessing the network. how	Investigate why the disconnection happened. It could be due to a physical disconnection or due to failure of the AP's wire side interface. Connect the AP back to the network.	Disabled | Disabled | Disabled | Disabled

Alert	Alert Description	Recommended Action	Default Setting Display | Email | Notify | Affects Severity Status
Access Point Reboot	An alert is raised when the AP gets rebooted.	No action is required if the reboot was because of a configuration change or an upgrade. Otherwise, check the AP power source and port connectivity, and the configuration of the AP. For details, check the AP logs for problems that might have caused the reboot.	Enabled | Disabled | Enabled | Disabled
VAPs down for network profile	This alert is raised when VAPs for a Network Profile are down because both tunnel interfaces are unreachable.	Investigate and fix any network connectivity issues between the device and the tunnel endpoints.	Enabled | Enabled | Enabled | Disabled
VAPs up for network profile	This alert is raised when VAPs for Network Profile are brought up because the tunnel interface, primary or secondary, becomes reachable.	This is an informational alert. No action is required.	Disabled | Disabled | Disabled | Disabled
Authentication RADIUS server switched	This alert is raised when the authentication RADIUS server is switched.	Investigate and fix any network connectivity issues between the device and the RADIUS server.	Enabled | Enabled | Enabled | Disabled
RADIUS server not responding	This alert is raised when the RADIUS server stops responding.	Investigate and fix any network connectivity issues between the device and the RADIUS server.	Enabled | Enabled | Enabled | Disabled
Tunnel endpoint down (Applicable to AP build 13.0 and higher)	This alert is raised when the tunnel endpoint is down for a particular network profile.	Investigate and fix any network connectivity issues between the device and the tunnel endpoint.	Enabled | Enabled | Enabled | Disabled
Tunnel endpoint down (Applicable to AP build lower than 13.0)	This alert is raised when the tunnel endpoint is down for a particular network profile.	Investigate and fix any network connectivity issues between the device and the tunnel endpoint.	Enabled | Enabled | Enabled | Disabled

Alert	Alert Description	Recommended Action	Default Setting Display | Email | Notify | Affects Severity Status
Tunnel endpoint switched	This alert is raised when the tunnel endpoint is switched.	Investigate and fix any network connectivity issues between the device and the tunnel endpoint.	Enabled | Enabled | Enabled | Disabled
Device firmware version unavailable	This alert is raised when an attempted scheduled update or auto-update of a device fails because the firmware version is not available.	Change the scheduled update or auto-update policy and configure an available version.	Enabled | Disabled | Enabled | Disabled
Device firmware update failed	This alert is raised when an attempted firmware update of a device fails. This could be because of network connectivity problems between the device and the server.	Investigate and fix any network connectivity issues between the device and the server, and then re-attempt the firmware update. Contact Technical Support if the problem persists.	Enabled | Disabled | Enabled | Disabled
Device with old firmware version detected	This alert is raised when the device firmware is lower than the latest available firmware version This device may not have some of the features from the latest version.	Update the device firmware. Arista recommends that you upgrade the device firmware to the latest version. Contact Technical Support if you have any questions..	Disabled | Disabled | Disabled | Disabled
Device disconnected from server	This alert is raised when a device gets disconnected from the server.	The device can get disconnected when it is rebooting, which takes a few minutes. If the device stays disconnected for more than 10 minutes, investigate the reason.	Enabled | Enabled | Enabled | Enabled
New device connected to server	This alert is raised when a new device gets connected to the server.	Move the device from the staging area to your required location.	Disabled | Disabled | Disabled | Disabled
Device operating in fail-safe mode	This alert is raised when a device starts operating in fail-safe Mode. This could be because of configuration changes or a firmware update on the device.	Undo any recent configuration changes and reboot the device from the UI. If the issue persists, try upgrading the device or contact Technical Support.	Enabled | Enabled | Enabled | Disabled

Alert	Alert Description	Recommended Action	Default Setting Display | Email | Notify | Affects Severity Status
Authentication failed for managed WiFi device	This alert is raised when a managed Wi-Fi device fails authentication.	This alert provides the reason behind failed authentication. If the communication key on the device does not match the one on the server, log in to the device and set the correct communication key. If the device uses legacy authentication, turn on the legacy authentication method on the server and upgrade the device. After the upgrade, the device will connect to the server if the server is using the factory default communication key. If you have changed the communication key on the server, log into the device and set the correct key.	Enabled | Enabled | Enabled | Disabled
AP with incompatible version detected	This alert is raised when an AP is running an incompatible version. An AP with an incompatible version cannot connect to the server.	Upgrade the AP to the recommended version.	Enabled | Enabled | Enabled | Disabled
New network detected	This alert is raised when a device detects a new network. You can configure the SSID (under the authorized WiFi Policy) to ensure that the SSID to network/VLAN mappings are enforced. A managed WiFi device in WIPS mode can then detect APs connected to its own network.	Review the authorized WiFi Policy to ensure that the SSIDs are configured with the correct SSID to network/VLAN mapping.	Disabled | Disabled | Disabled | Disabled
Authentication failed for access point uplink port	This alert is raised when a device fails to authenticate its uplink port.	Investigate the device.	Enabled | Enabled | Enabled | Disabled
Maximum VLAN limit reached	This alert is rasied when the AP reaches Maximum VLAN limit.	This is an informational alert.	Enabled | Enabled | Enabled | Disabled

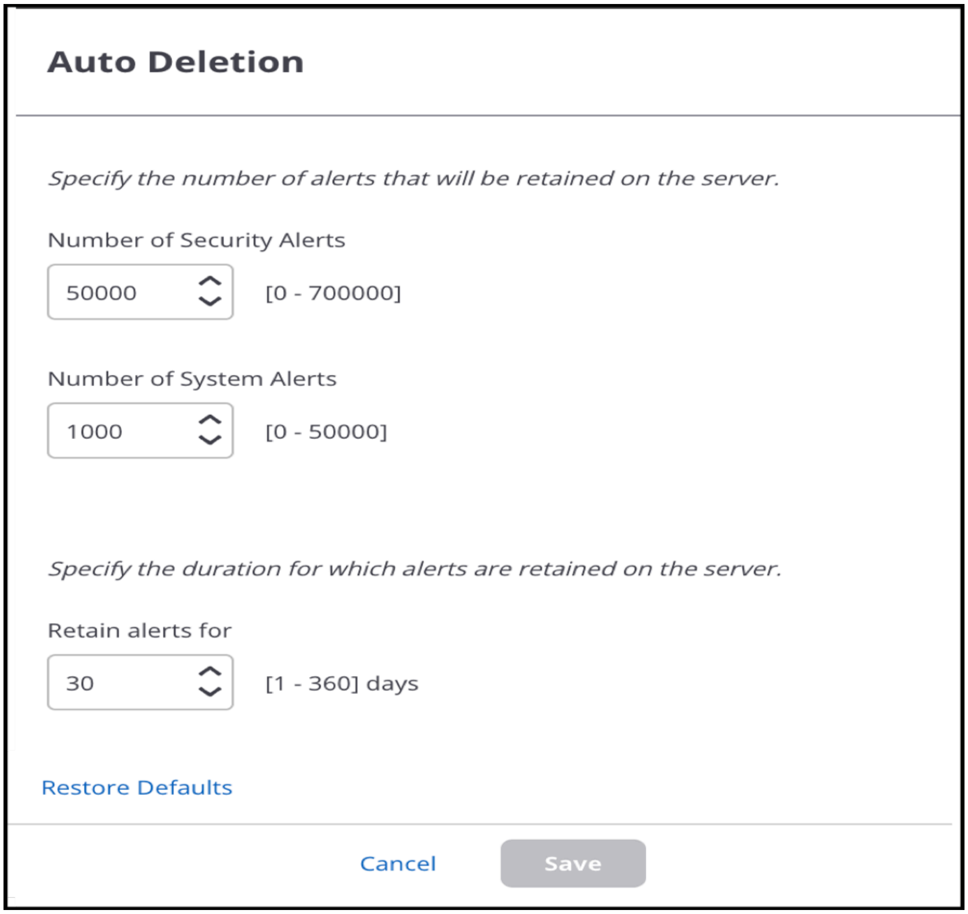
Alert	Alert Description	Recommended Action	Default Setting Display | Email | Notify | Affects Severity Status
Access Point with non-compliant firmware version detected	This alert is raised when the current version of the access points do not match with the compliant version configured for the selected location	Upgrade your AP builds to the complaint versions. You can upgrade the access point from Monitor > WiFi > Access Points or Monitor > WIPS > Managed WiFi Devices	Enabled | Enabled | Enabled | Enabled
Local Authentication	This alert is raised when a BSSID enters Local Authentication mode.	Investigate and fix any network connectivity issues between the device and the RADIUS server.	Enabled | Disabled | Disabled | Disabled

21.4 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. Got 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.

Chapter 22

Monitor Alerts

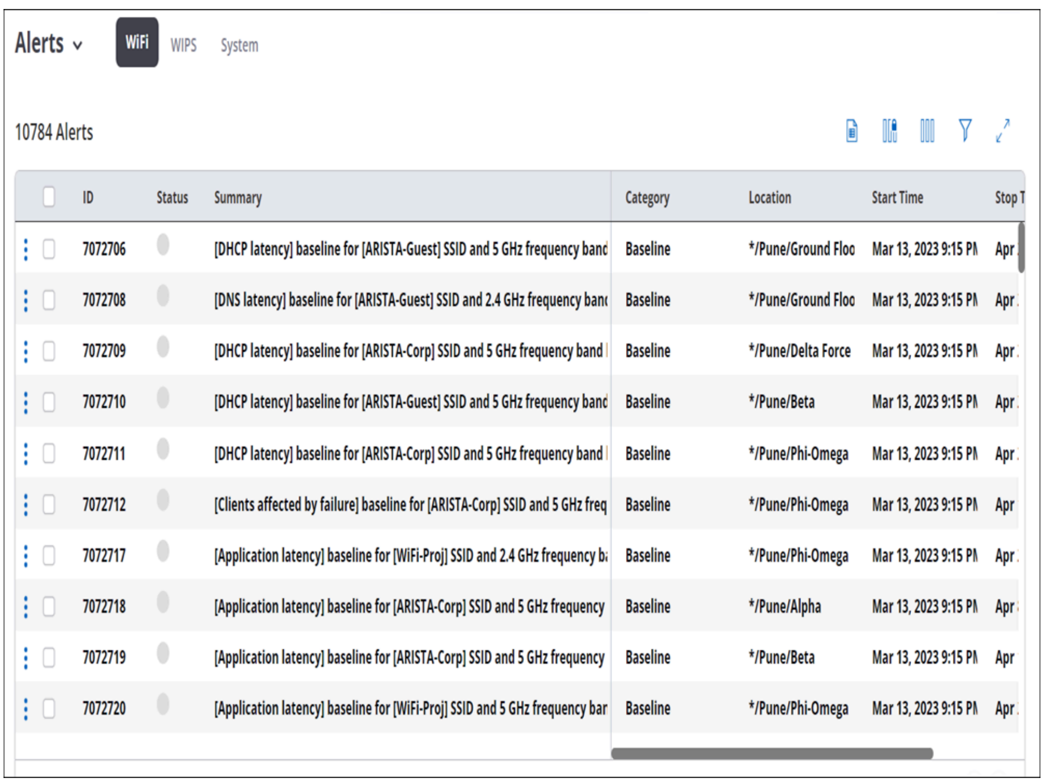
Alerts are categorized into three types: Wi-Fi, System, and WIPS (see the sections below for details) and are further classified as follows, based on the nature of events that trigger the alerts.

- **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 Wi-Fi 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 Wi-Fi 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.

The chapter contains the following topics:

22.1 Monitor Wi-Fi Alerts

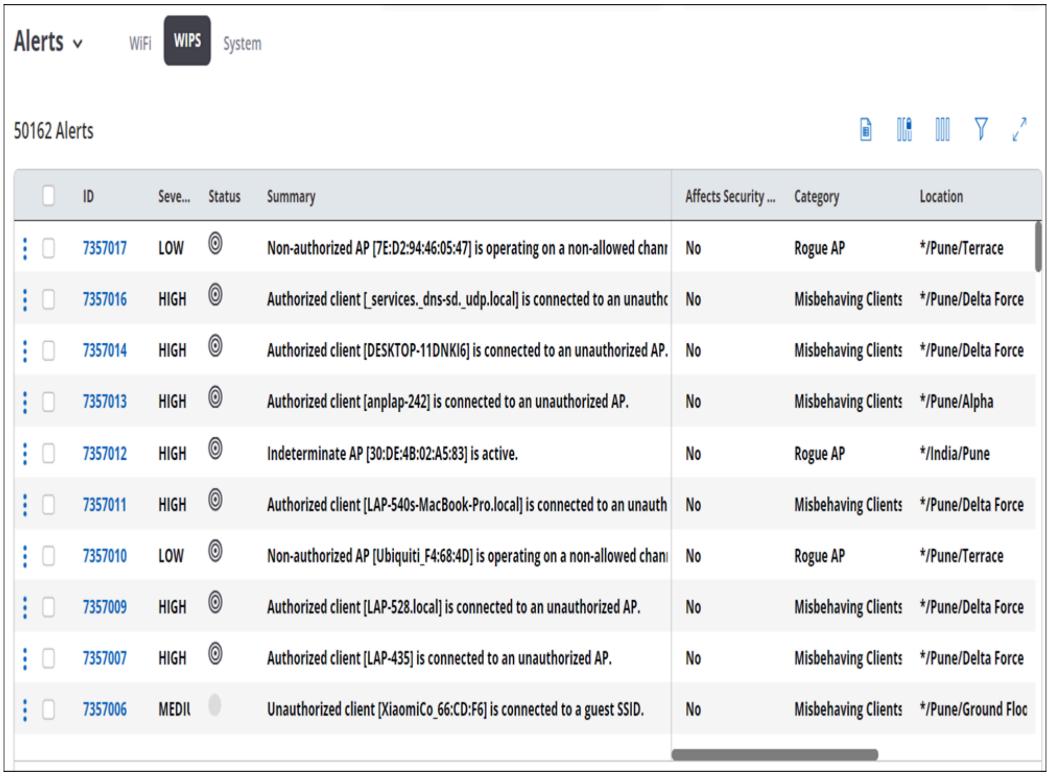
Under **MONITOR** > **Alerts** > **WiFI**, you can review Wi-Fi alerts that have been configured to be displayed on the UI.



Wi-Fi 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 Wi-Fi network that they pertain to-for example, client connectivity test or connection failure. You can mark a Wi-Fi alert as "Read" or "Unread" and you can delete it.

22.2 Monitor WIPS Alerts

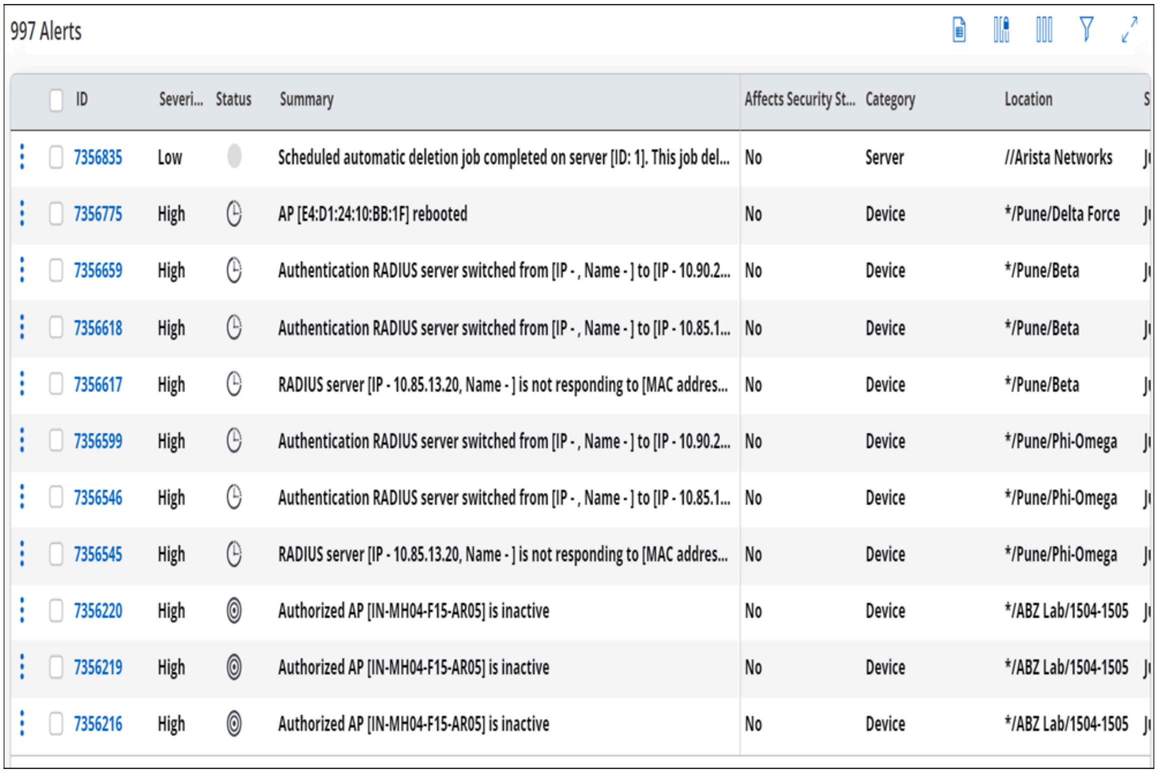
Under **MONITOR** > **Alerts** > **WIPS,** you can review WIPS alerts that have been configured to be displayed on the UI.



WIPS alerts are related to Wi-Fi 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.

22.3 Monitor System Alerts

Under **Monitor** > **Alerts** > **System**, you can review System alerts that have been configured to be displayed on the UI.



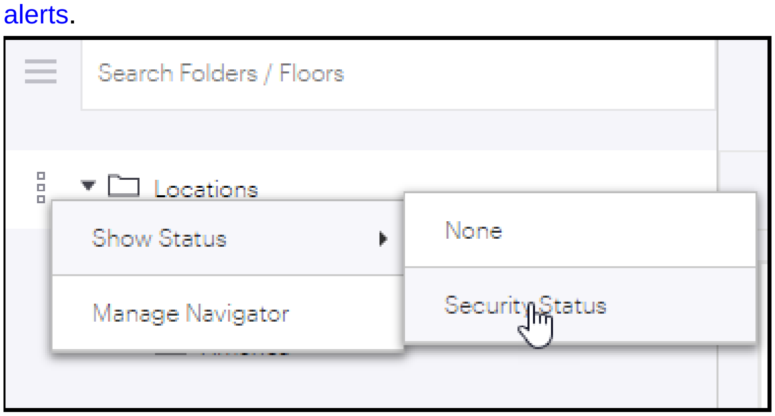
997 Alerts

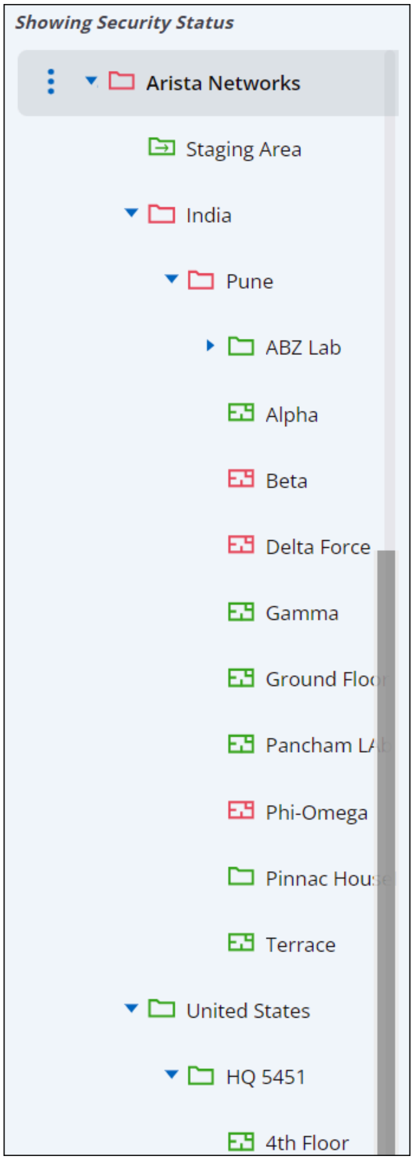
ID	Severi...	Status	Summary	Affects Security St...	Category	Location	S
7356835	Low		Scheduled automatic deletion job completed on server [ID: 1]. This job del...	No	Server	//Arista Networks	J
7356775	High		AP [E4:D1:24:10:BB:1F] rebooted	No	Device	*/Pune/Delta Force	J
7356659	High		Authentication RADIUS server switched from [IP - , Name -] to [IP - 10.90.2...	No	Device	*/Pune/Beta	J
7356618	High		Authentication RADIUS server switched from [IP - , Name -] to [IP - 10.85.1...	No	Device	*/Pune/Beta	J
7356617	High		RADIUS server [IP - 10.85.13.20, Name -] is not responding to [MAC addres...	No	Device	*/Pune/Beta	J
7356599	High		Authentication RADIUS server switched from [IP - , Name -] to [IP - 10.90.2...	No	Device	*/Pune/Phi-Omega	J
7356546	High		Authentication RADIUS server switched from [IP - , Name -] to [IP - 10.85.1...	No	Device	*/Pune/Phi-Omega	J
7356545	High		RADIUS server [IP - 10.85.13.20, Name -] is not responding to [MAC addres...	No	Device	*/Pune/Phi-Omega	J
7356220	High		Authorized AP [IN-MH04-F15-AR05] is inactive	No	Device	*/ABZ Lab/1504-1505	J
7356219	High		Authorized AP [IN-MH04-F15-AR05] is inactive	No	Device	*/ABZ Lab/1504-1505	J
7356216	High		Authorized AP [IN-MH04-F15-AR05] is inactive	No	Device	*/ABZ Lab/1504-1505	J

System alerts are for events related to the overall health of the Wi-Fi server and infrastructure, e.g., when a Wi-Fi 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.

22.4 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 are not. Whether or not a WIPS or System alert contributes to the security status can be set while configuring those alerts.




Showing Security Status
Arista Networks
Staging Area
India
Pune
ABZ Lab
Alpha
Beta
Delta Force
Gamma
Phi-Omega
Terrace
United States
HQ 5451
4th Floor

Chapter 23

Wireless Intrusion Prevention Techniques

This chapter contains the following topics:

23.1 About Wireless Intrusion Prevention Techniques

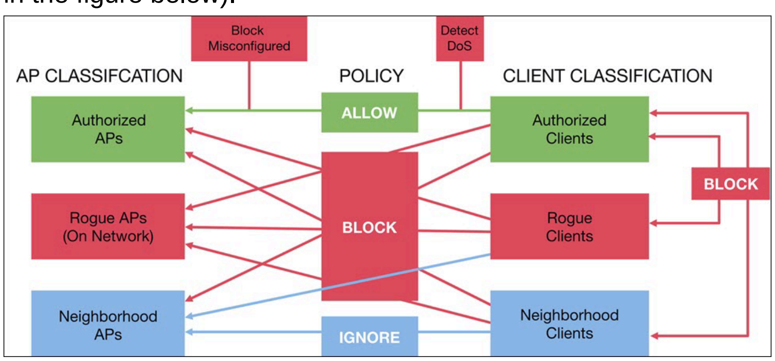
A large number of Wi-Fi devices Access Points (APs) and clients-are commonly present in the vicinity of an enterprise. While most are legitimate devices, belonging either to the enterprise or businesses around it, manually tracking the presence of any threat-posing devices among them or Wi-Fi connections violating the enterprise security policy is impractical.

Arista Wireless Intrusion Prevention System (WIPS) can automate that process and protect enterprise networks from Wi-Fi-based vulnerabilities and attacks. It can also track the physical location of Wi-Fi devices on enterprise premises.

Arista WIPS uses a variety of patented techniques to classify Wi-Fi devices automatically and accurately as follows.

- Authorized: Owned and officially deployed by the enterprise,
- External: Legitimate Wi-Fi devices in the enterprise vicinity, and
- Rogue: Unauthorized Wi-Fi devices on the enterprise network.

This serves as the foundation for enforcing Wi-Fi security policies. Based on the accurate device classification, Arista WIPS can automatically block threat-posing Wi-Fi devices and connections (shown in red in the figure below).



You can enable automatic intrusion prevention using Arista CV-CUE, 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 Wi-Fi connections, e.g., an authorized client could be blocked from connecting to an external AP that is a Wi-Fi 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 Wi-Fi-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 Wi-Fi 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 multipot) 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 Wi-Fi frames or frames that consume a significant amount of airtime, starving legitimate APs and clients from transmitting, thus, disrupting the Wi-Fi 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:

- **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.
- **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.
- **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.
- **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 unicasted to the authorized client, thus, not affecting the other connections.

- **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.
- **Cell Splitting**: Cell splitting is used to prevent encrypted ad hoc Wi-Fi 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.

23.2 Intrusion Prevention Level

Arista WIPS offers four levels of automatic intrusion prevention, listed below.

Level	Number of channels-per-radio prevented
Block	1
Disrupt	2
Interrupt	3
Degrade	4

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 does not 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 Wi-Fi environment. By default, the intrusion prevention level is set to "Disrupt".

23.3 Authorized Wi-Fi Policy

Arista Wireless Intrusion Prevention System (WIPS) uses a variety of patented techniques to automatically and accurately classify Wi-Fi Access Points (APs) and clients as follows.

- Authorized: Owned and officially deployed by the enterprise,
- External: Legitimate Wi-Fi devices in the enterprise vicinity, and
- Rogue: Unauthorized Wi-Fi devices on the enterprise network.

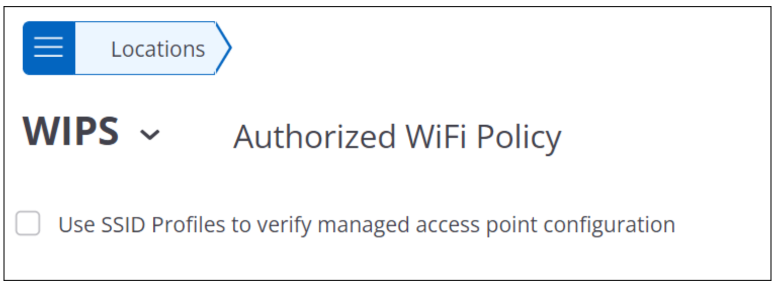
An Authorized Wi-Fi Policy forms the basis of this automatic device classification; it can be defined in terms of:

- The characteristics of the official enterprise Wi-Fi 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.
- A pre-classification of Wi-Fi 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 Received Signal Strength Indicator(RSSI) with which those APs are visible to Arista WIPS.

You can implement an authorized Wi-Fi policy in two ways: either using the SSID Profile settings to validate the configuration running on your Arista Wi-Fi APs or by creating an Authorized Wi-Fi Profile for each SSID. Each method is described below.

Using SSID Profile Settings

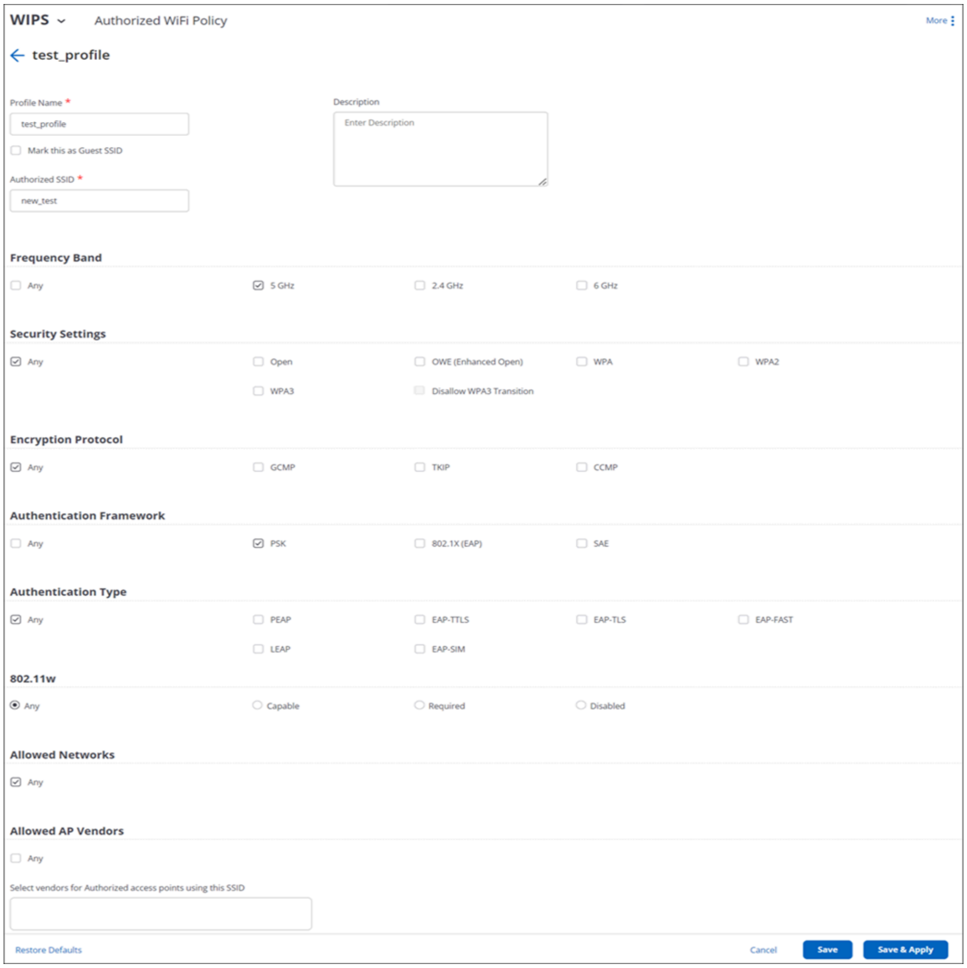
You may choose to simply leverage the settings of the SSID Profiles in use to validate the configuration running on the enterprise Wi-Fi APs; this can be done by enabling the **Use SSID Profiles to verify managed access point configuration** option as shown below.



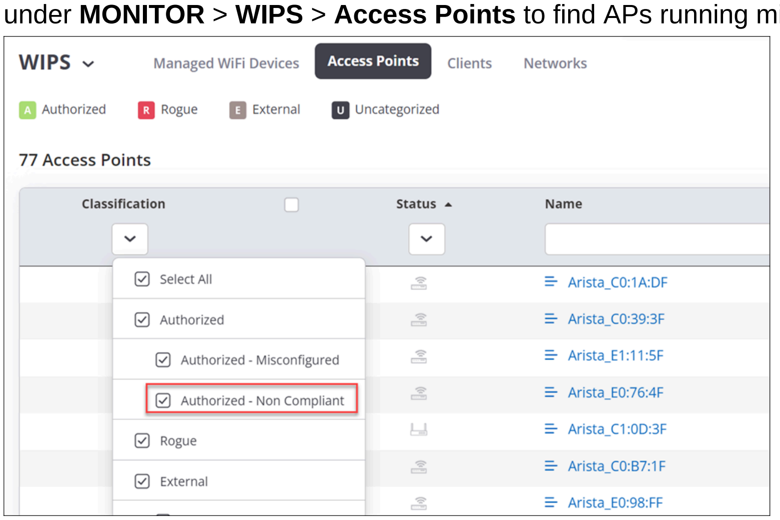
Note: This option is enabled by default. You will have to disable it if you choose to define your enterprise authorized Wi-Fi policy in terms of Authorized Wi-Fi Profiles.

Authorized Wi-Fi Profile per SSID

The figure below shows an Authorized Wi-Fi 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 is the only allowed AP vendor; similarly, it must use PSK authentication.



When an SSID configuration does not match the authorized Wi-Fi policy, the SSID is marked as a Misconfigured SSID. When an SSID configuration does not follow the security policies of Wi-Fi 6 and 6E, the SSID is marked as Non Compliant. As shown in the figure below, you can filter on the **Classification** column under **MONITOR** > **WIPS** > **Access Points** to find APs running misconfigured SSIDs.

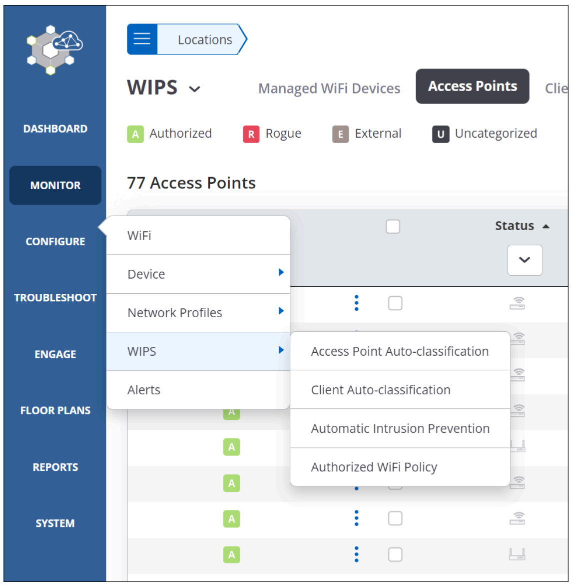


You can select an AP to see the SSIDs that are misconfigured and to view the reasons for the configuration mismatch. Active APs running misconfigured SSIDs are marked orange on the **MONITOR** > **WIPS** and **MONITOR** > **WiFi** tabs.

23.4 Access Point Auto Classification

Arista Wireless Intrusion Prevention System (WIPS) continuously scans the Wi-Fi frequency spectrum to detect other Wi-Fi devices present in the vicinity.

Whenever a new Wi-Fi 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 Wi-Fi 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.

23.5 Client Prevention

Client prevention allows you to choose the types of Wi-Fi client communication you want to prevent.

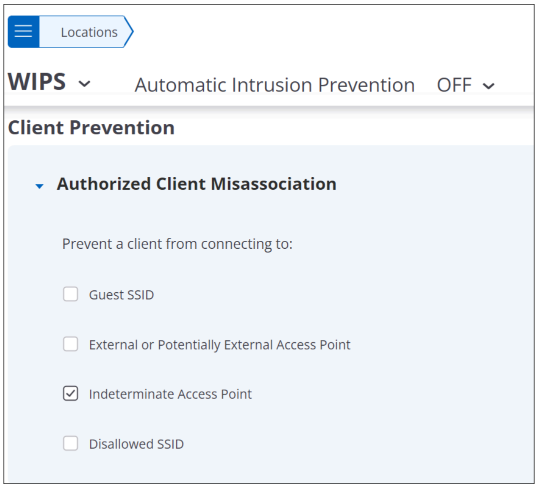
The types of client communication are based on two factors:

- 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 Wi-Fi client could attempt to associate with access points in the vicinity of your enterprise. To protect authorized clients on an enterprise Wi-Fi network, you might want to prevent them from associating with any non-authorized APs as shown below.

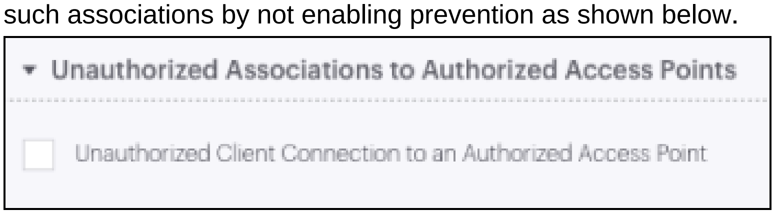


Client Bridging/ICS

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 Wi-Fi 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.



23.6 Client Auto-Classification

Classifying Wi-Fi clients can help you automatically enforce your Wi-Fi 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 Wi-Fi 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 Wi-Fi network for Internet access and have limited or no access to the internal network.
- **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.

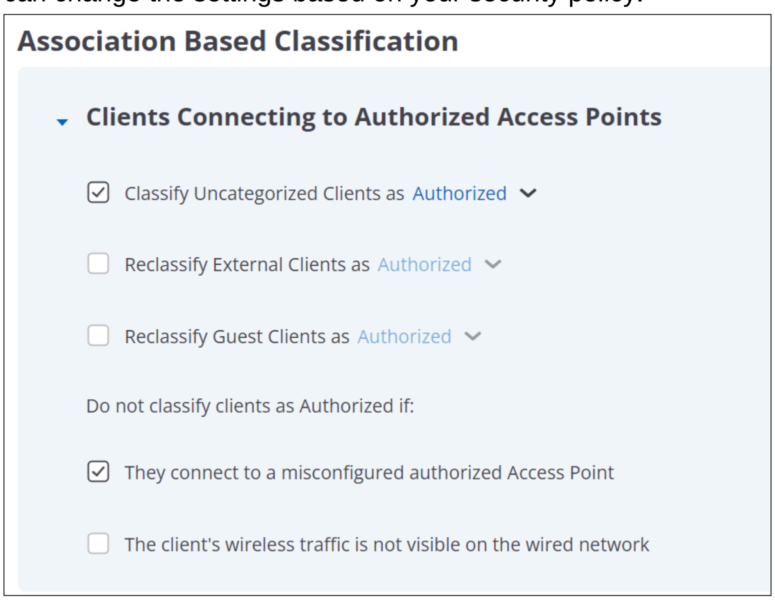
Manually keeping track of the list of clients that are authorized to access your enterprise Wi-Fi network is not scalable and is prone to errors, especially in large organizations. Arista CV-CUE provides a simpler way to automatically classify clients. The client auto-classification policy settings are available under **CONFIGURE** > **WIPS** > **Client Auto-Classification.**

By default, clients are left uncategorized initially and classified based on the type of AP or Wi-Fi 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.

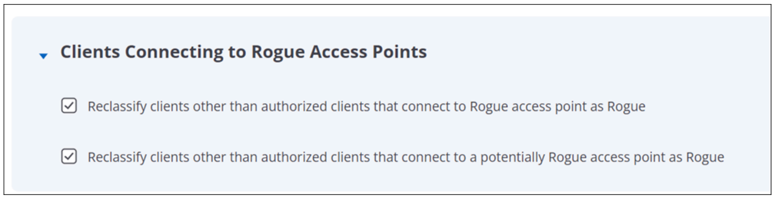
Clients Connecting to Authorized Access Points

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 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.

23.7 Banned Device List

You can ban certain Wi-Fi 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 Wi-Fi 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. Wi-Fi connectivity with a banned access point or client can also be prevented automatically by configuring the relevant intrusion prevention policy.

23.8 WLAN Integration

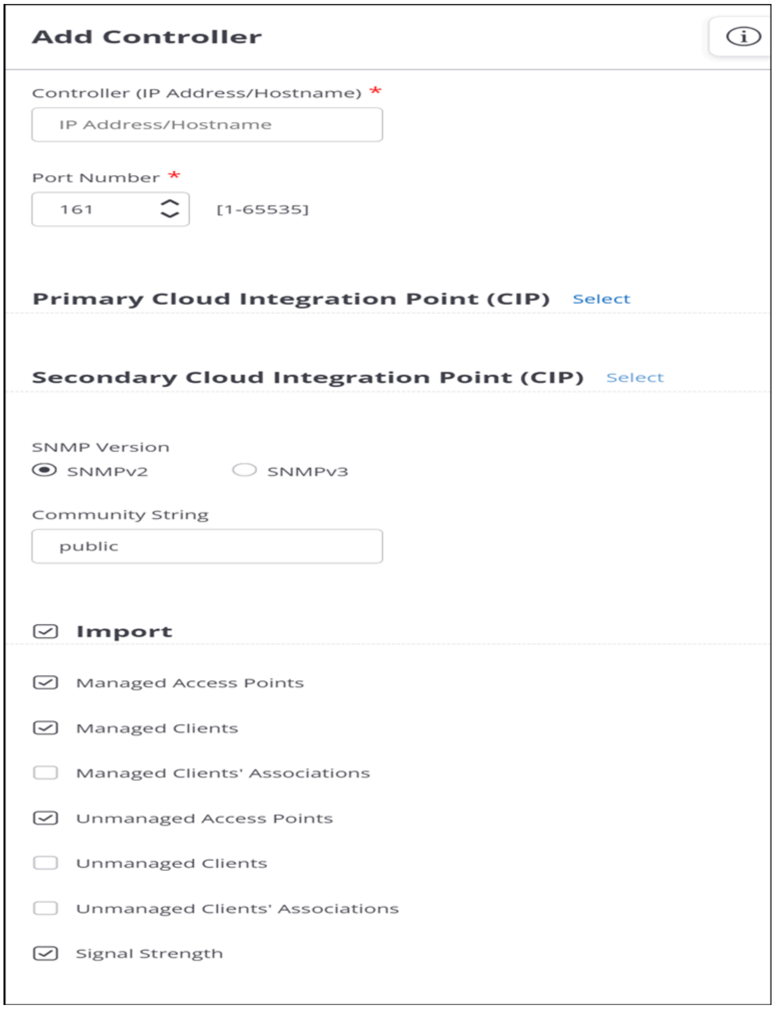
Whether you are using Arista WIPS or transitioning to cloud-based Wi-Fi, integrating the Arista Cloud Wi-Fi server with your on-premises WLAN controller allows you to leverage key advantages of the cloud server while continuing to use your controller-based WLAN.

The Arista cloud-based Wi-Fi 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 Wi-Fi client locations.

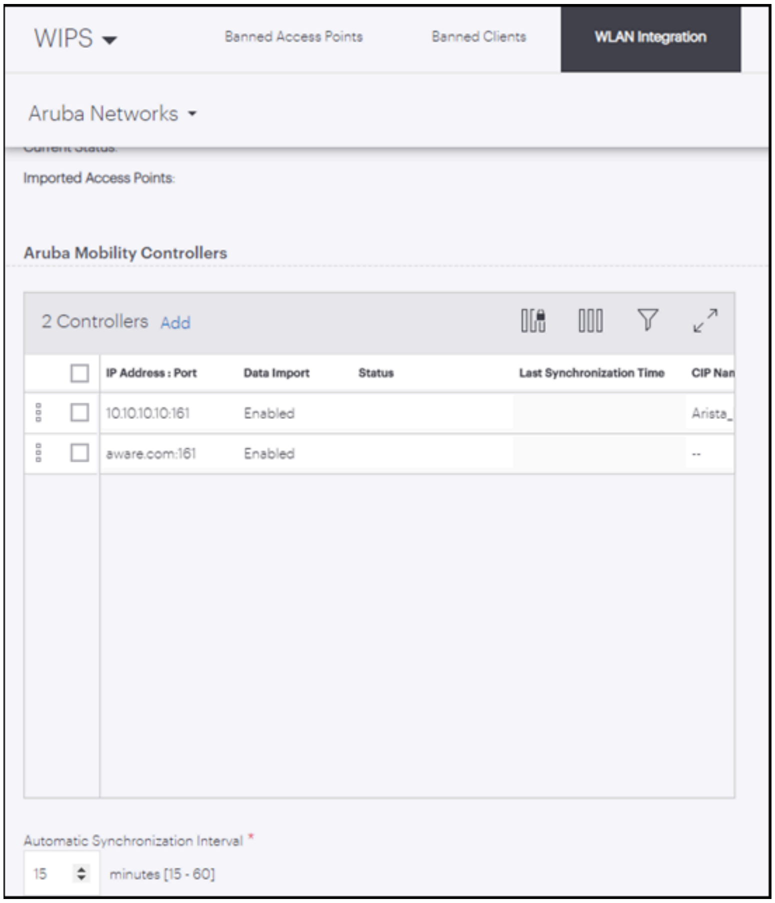
Arista supports integration with Aruba Mobility Controllers and Cisco WLC.

23.8.1 Configure WLAN Integration

To add WLAN controllers, go to **SYSTEM** > **WIPS** > **WLAN Integration** in CV-CUE. 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.



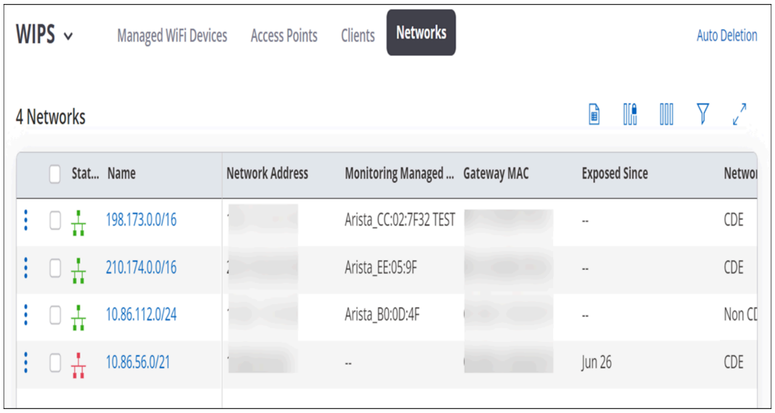
WIPS
Banned Access Points
Banned Clients
WLAN Integration
Aruba Networks
Imported Access Points:
Aruba Mobility Controllers
2 Controllers Add
IP Address : Port
Data Import
Status
Last Synchronization Time
CIP Nan
10.10.10.10:161
Enabled
Arista_
aware.com:161
Enabled
--
Automatic Synchronization Interval *
15
minutes [15 - 60]

23.8.2 Controller Settings

Field	Description
Controller (IP Address/Hostname)	Enter the IP address or hostname of the controller. **Note:** If the controller uses a private IP address, you need to select a Cloud Integration Point.
Port Number	The controller port number from which data is imported.
Primary Cloud Integration Point (CIP)	From the drop-down list, select an Arista device that you want to use as the primary Cloud Integration Point (CIP) for this controller. **Important:** You must open port number 3852 in your network from the CIP to Arista cloud.
Secondary Cloud Integration Point (CIP)	From the drop-down list, select an Arista device that you want to use as the secondary Cloud Integration Point (CIP) for this controller. If the primary CIP goes down, the secondary one ensures connectivity of your service to the cloud.
SNMP Version	Select SNMP V2 or V3 for the Arista cloud communication with the controller.
Community String	User-defined community string using which Arista cloud communicates with the controller. The default value is 'public'.
Import	Select to enable the import of data from the controller.
Managed Access Points	Select to import managed access point information from the controller.
Managed Clients	Select to import information about clients associated with access points managed by the controller.
Unmanaged Access Points	Select to import information about access points not managed by the controller.
Unmanaged Clients	Select to import information about clients associated with access points not managed by the controller.
Signal Strength	Select to import signal strength information from the controller.

23.9 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.

23.10 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
- Network
- Clients
- Alerts
- Inactive Authorized APs

You must have superuser, administrator, or operator privileges to use auto-deletion settings.

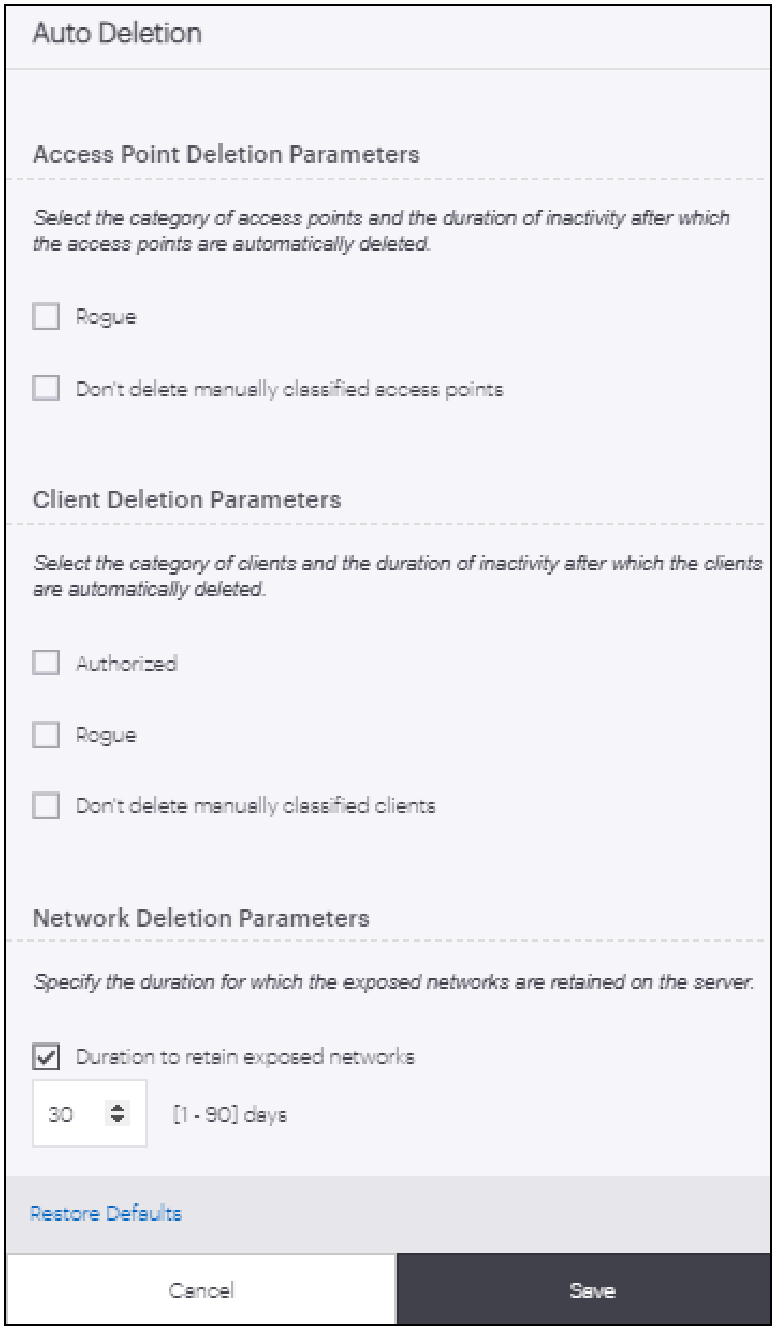
23.10.1 Auto-Delete Access Points, Clients, and Network

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. Got 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.

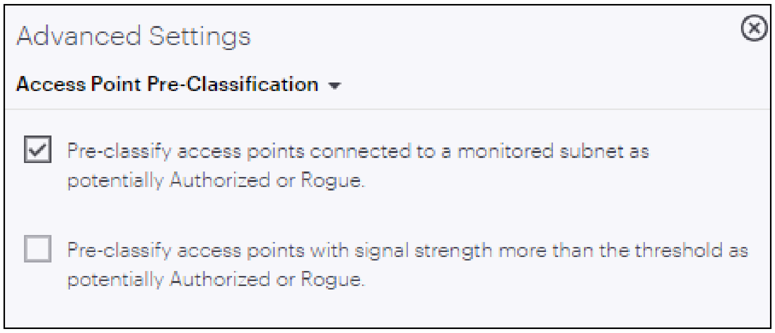
23.11 WIPS Advanced Settings

Under **CONFIGURE** > **WIPS** > **Authorized WiFi Policy,** you can define Advanced Settings that allow you to pre-classify **Access Points** (APs) and define No-Wi-Fi networks.

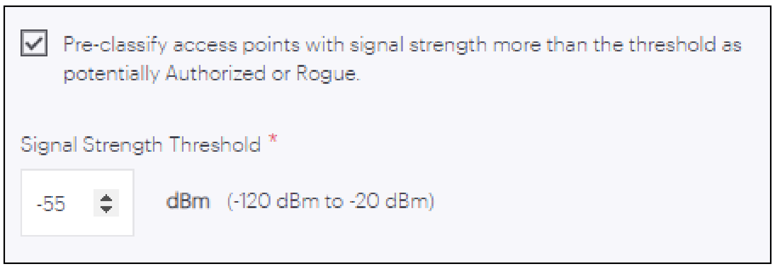
Access Point Pre-Classification

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.



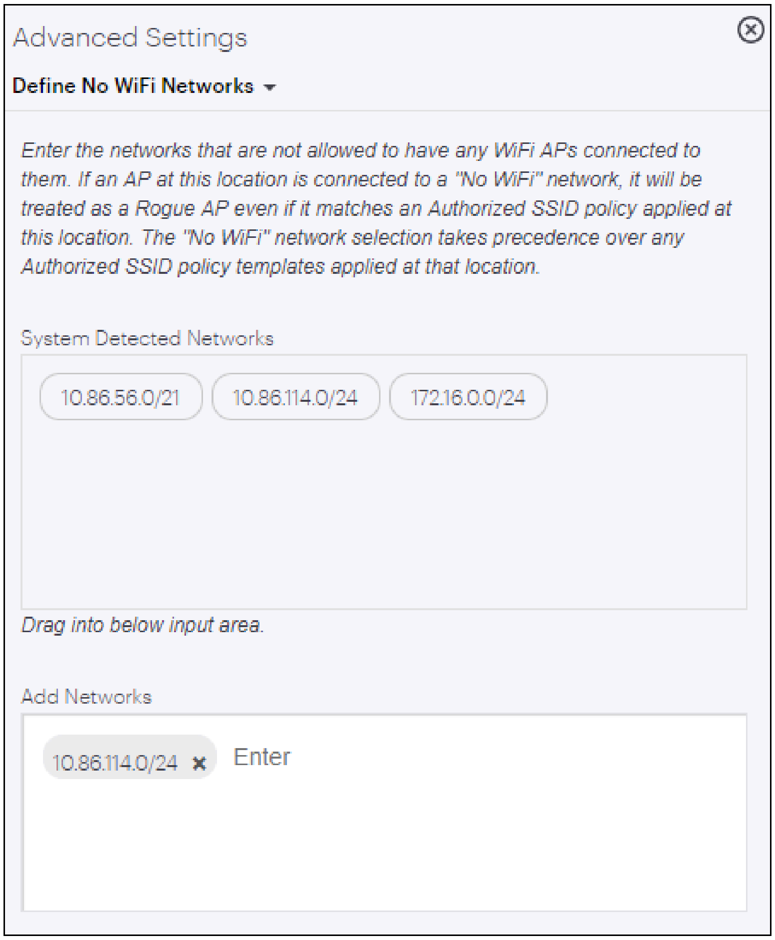
You can also have WIPS pre-classify APs based on the signal strength with which they are visible. As shown in the figure below, if you enable signal strength based pre-classification, CV-CUE allows you to define a signal strength threshold. APs with signal strength greater than the threshold are automatically 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 Wi-Fi connections to the AP. Therefore, use this classification only if you are sure that no unauthorized Wi-Fi 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 Wi-Fi hotspots, for example).

Define No-Wi-Fi Networks

Security-sensitive environments might need to ensure that no Wi-Fi network operates at certain locations. As shown in the figure below, you can define "No-Wi-Fi" networks for a location, i.e., specify subnets where no Wi-Fi 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.


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

Chapter 24

Engage

With the Engage functionality, network administrators or Guestbook operators can configure and manage guest user accounts from CloudVision Cognitive Unified Edge (CV-CUE). Engage functionality also lets network administrators analyze the various statistics and demographic profiles of guest users who access your Wi-Fi setup. You can obtain the user profiles by using custom plug-ins, except Clickthrough, or through entries from a private guest book.

Users access the Wi-Fi through custom captive portals created in CV-CUE. These portals can be configured to enable users to access the Wi-Fi by using their credentials or by using user accounts that you have created in the portal guest book.

Engage offers the following functionalities:

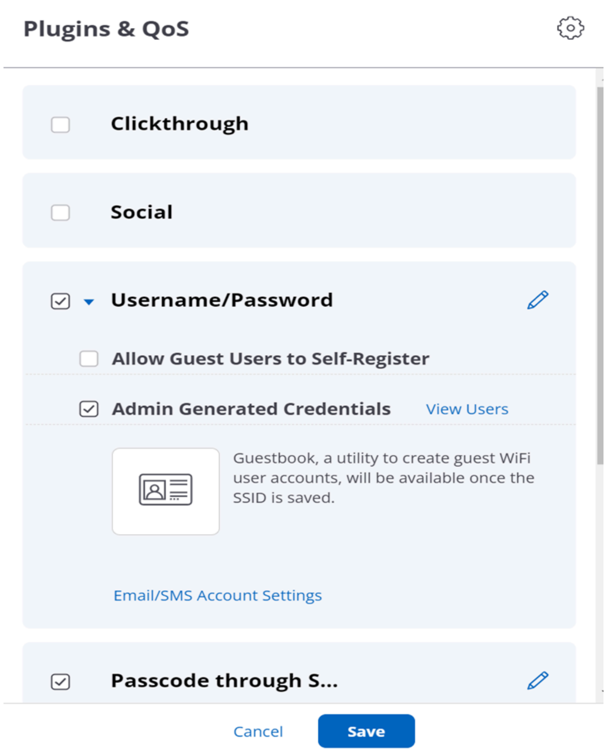
- Manage Guest Users
- View Guest Insights and Profiles
- Create and Schedule Reports
- Admin Settings
    - Third-Party Integration
    - View Logs

24.1 Manage Guest Users

Network administrators or Guestbook operators can configure and manage guest user accounts using the **Engage** > **Users** tab. As a network administrator, you can create multiple user accounts, set their credentials, and share the account details with the guest users over email. You can create individual user accounts or create user accounts in bulk. Guest users can use these administrator-generated credentials to access the internet through your Wi-Fi setup.

Note: Engage functionality is applicable for cloud-hosted captive portals only. Ensure that you have enabled either of the options for **Username / Password:** while configuring the captive portal:

- **Allow Guest Users to Self-Register:** Users can self-register directly from the splash page. Administrators can modify the user account settings once the user successfully registers.
- **Admin Generated Credentials:**Administrators can create users or user batches and share the account credentials and details with the guest users.



This chapter contains the following topics:

- Use Case
- Create Users
- Create User Batches

24.1.1 Use Case

Consider a scenario where you are conducting a seminar or an event for a large number of users. You want to allow these users to access your Wi-Fi network for a short period of time and once the event is done, you need to revoke the access. You can achieve this by creating a batch of users or by importing a large number of users. You can set the validity of the user accounts, login-limits, device limits, and also specify Quality of Service Setting parameters to ensure smooth connectivity.

24.1.2 Create Users

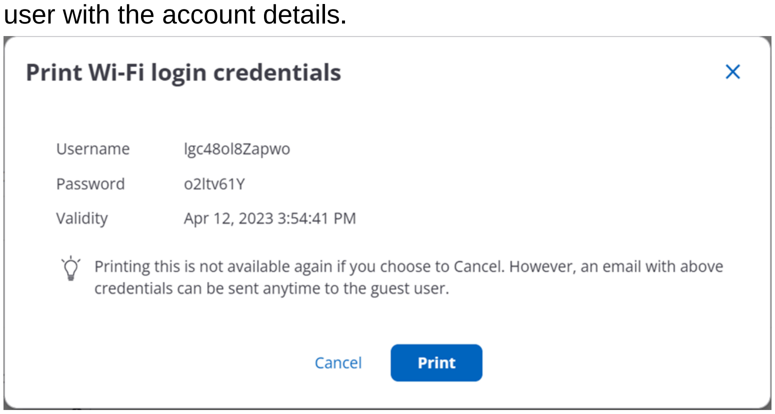
To create a user account:

1. Go to **Engage** > **Users.**
2. From the drop-down menu, select the **SSID profile** with the configured captive portal.
3. Click **Add** and provide the following details:

Field	Description
User Name	Name of the guest user account.
Password	Password for the guest user account.
Email	Email address of the guest user to send notifications.
User Status	Set it as Unlocked to enable the user to access the network.
Validity	Set the time duration for which you want the user to be able to access the network. Guest users will not be able to access the network once the validity expires.
SSID Name	SSID Name on which the user is available.
SSID Key	SSID Key to get access to the SSID on which the user is available.
Device Limit	The maximum number of devices a guest user can simultaneously log in.
Login Limit	The number of times the guest user can log-in from the splash page using these credentials. If the account is valid and the user has crossed the login count limit,the user will not be allowed to log-in.
Quality of service settings	
Login Timeout	The time period after which the guest user session expires. The user must re-authenticate with their login credentials to continue using the Wi-Fi service. If you leave this setting blank, the user session does not timeout and the user must explicitly log out from the portal.
Blackout Time	The time period during which a user cannot log in to the portal after the last successful login has timed out.
Max Download Bandwidth	The maximum download bandwidth, in Kbps, for the guest user.
Max Upload Bandwidth	The maximum upload bandwidth, in Kbps, for the guest user.

4. Save the settings.

When you save the user details, you have an option to print the user details. You can print the account details or save a .pdf file to share with your guest users. You can click Save and Send Notification to email the guest user with the account details.

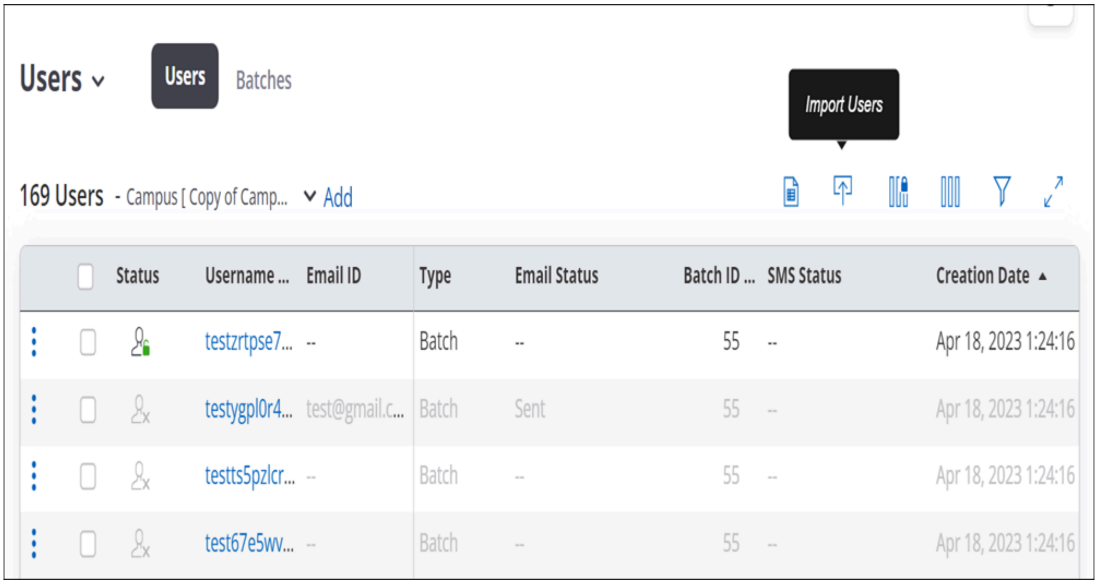


Importing Users

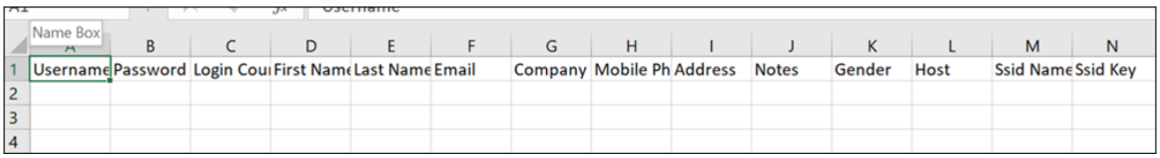
You can also import multiple users by providing the user details in a .csv file.

To import Users,

1. Go to**Engage** > **Users tab**and click **Import Users.**



2. Upload a .csv file with the user details.



You can view the imported users in the User tab. Users imported from .csv file are tagged as batch users and a batch is created for every imported .csv file. The username prefix is left blank for imported users.

24.1.3 Create User Batches

You can also create multiple users simultaneously by creating a batch of users. Creating a batch of users is useful when you need to create a large number of guest user accounts.

To create a user batch:

1. Go to **Engage** > **Users** > **Batches**
2. From the drop-down menu, select the **SSID Profile** with the configured captive portal.
3. Click **Add** and provide the following details:

Field	Description
Username Prefix	Prefix for the guest user accounts batch. This is applied to all the users in the batch.
Batch Type	• Select **Random Users** to generate users with random user names with the specified prefix in the guest user batch. • Select **Incrementing Users** to generate usernames with the specified prefix and an incremental index in the batch.
Username Length	The length of the user name. This setting is available only for Random Users.
Start Index	The numerical index to start the user names. This setting is available only for Incrementing Users.
Password Length	Length of the password.
Number of Users	The number of users to create in this batch.
Expires At	Set the time to expire the validity of all the users in this batch.

4. Specify the Login Limit, Device Limit, and Quality of service setting parameters applicable to all users in this batch.
5. Save the settings.

You can export the created user batch to retrieve the usernames and passwords and share them with your guest users.

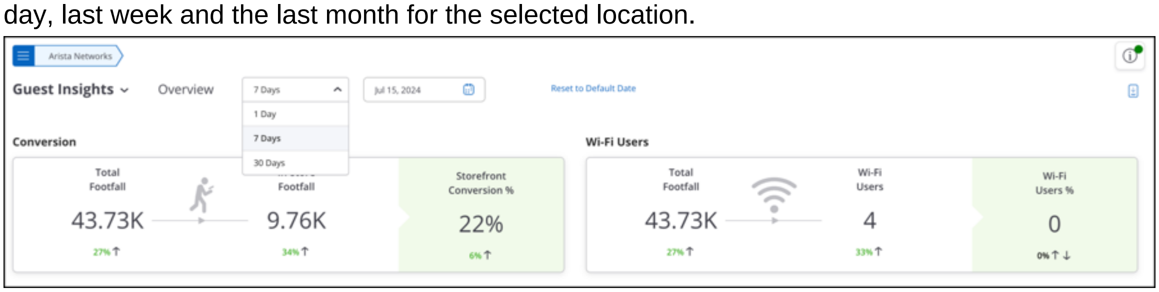
24.2 Guest Insights

Guest Insights menu contains the following tabs:

- Overview
- Presence
- Demographics
- Profiles
- WiFi Usage

24.2.1 View Guest Overview

The overview dashboard provides a quick overview of the statistics related to demographic data about visitors using guest Wi-Fi, male users vs female users, dwell time, new users versus repeat users , etc for the last day, last week and the last month for the selected location.

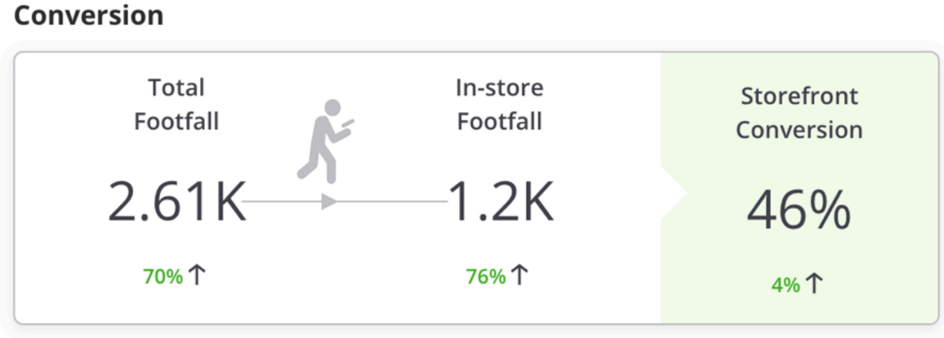


All charts on the Overview tab display data for Today’s date. To view overview-related data for a specific date, select the date from the date picker at the top.

The Overview tab contains the following charts:

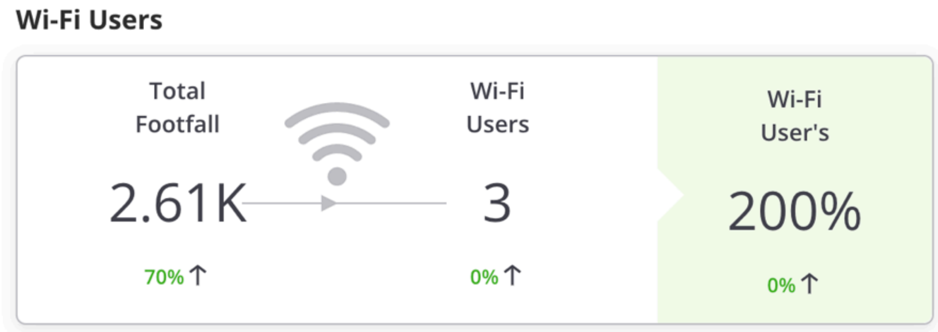
Conversion

Conversion data indicates the number of visitors entering the store to use the Wi-Fi compared to visitors accessing Wi-Fi from outside the store. Conversion shows the data for the converted customers. Converted customers means the visitors who were visible around the store but chose to enter and use the Wi-Fi.



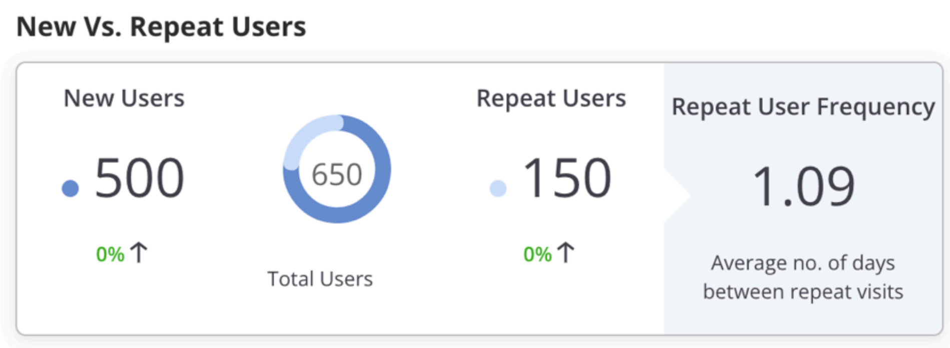
Wi-Fi Users

The Wi-Fi Users widget presents the total visible visitors inside and outside the store, the total users who have used Wi-Fi, and the percentage of the visitors using the guest Wi-Fi out of the total users.



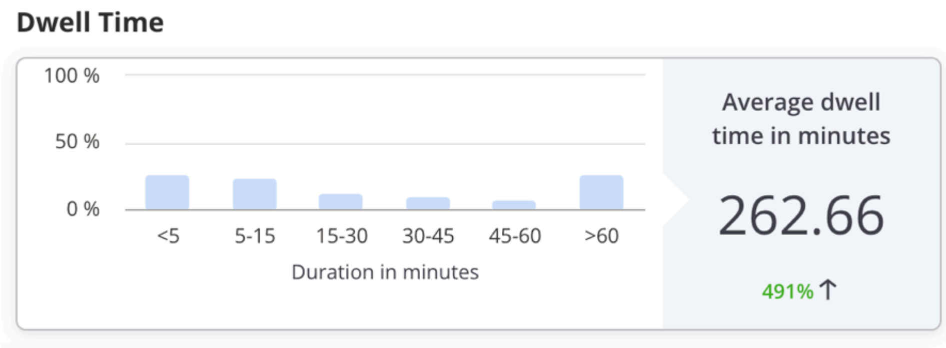
New vs. Repeat Users

The New Vs Repeat Users widget indicates the total number of users using the guest Wi-Fi, along with the percentage of new and repeat users. It also presents the average number of days between visits for repeat users.



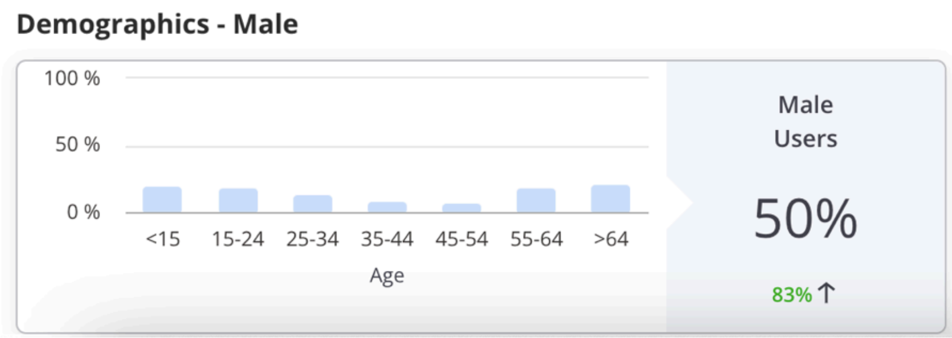
Dwell Time

Dwell time is the time for which a user is visible to the access points installed in the store. The dwell time widget displays a bar graph of the percentage of visitors for different time ranges. The unit of measurement for the time range is minutes. The widget also displays the average dwell time in minutes.



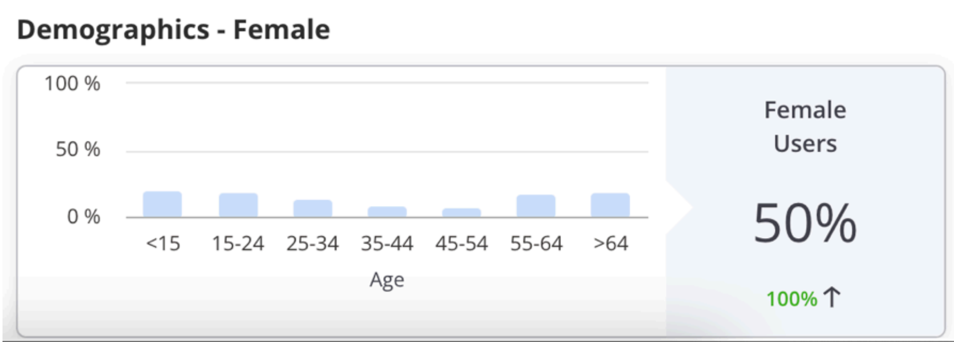
Demographics - Male

The Demographics - Male widget displays the percentage of male users using the guest Wi-Fi through a social media plugin. This data is derived from the social media sites used by the guest Wi-Fi users to log in to CV-CUE.



Demographics - Female

The Demographics - Female widget displays the percentage of female users using the guest Wi-Fi through a social media plugin. This data is derived from the social media sites used by the guest Wi-Fi users to log in to CV-CUE.



24.2.2 View Guest Presence

To view Guest Presence data, navigate to **Engage** > **Guest Insights** > **Presence.**

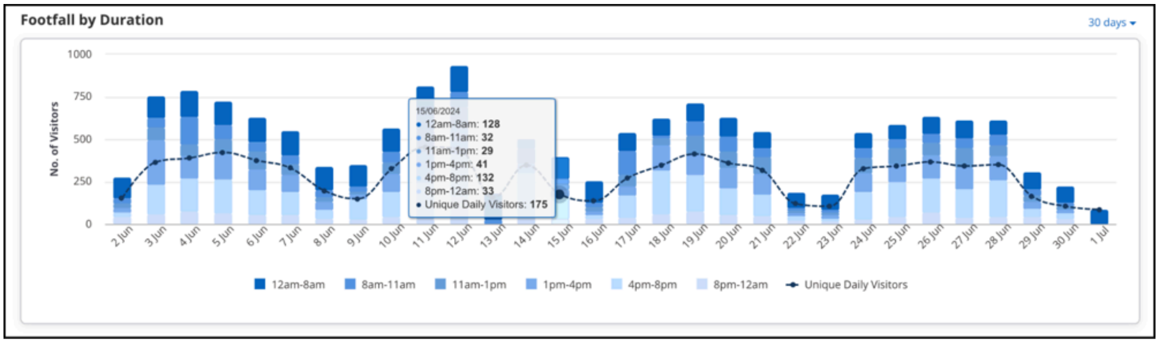
Presence Tab contains the following charts:

- Footfall by Duration
- Footfall by Location
- Dwell Time by Duration
- Dwell Time by Location

All charts on the Presence tab display data for Today's date. To view presence-related data for a specific date, select the date from the date picker at the top.

Footfall by Duration

This is a bar graph that shows the number of visitors during different time splices of a day for the specified duration and at the selected location. The graph also plots the total number of visitors for each day at the selected location for the specified duration. The number even includes the guest users who haven't even accessed the Wi-Fi but were duly visible. The data displayed on the graph for each time splice is based on the time zone set for the location selected in the tree. That is to say, you select a node with multiple locations under it. The graph plots the total number of visitors for each day (based on the duration selected). The graph also plots the total number of visitors during a specific time period of the day (time splice). The total number of visitors for a specific time splice is calculated by aggregating the visitor count during the said time splice for each location based on the time zone of the location. We can access their presence for a span of 7 days, 30 days, 60 days, 180 days or 365 days.

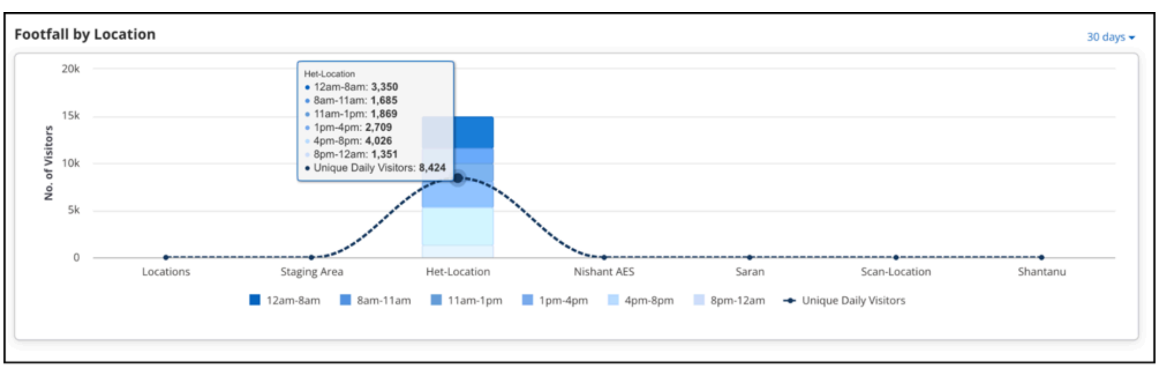


When you need a 7 day chart, you will easily be able to track the per day data of the visitors in and around the store from Monday to Sunday. But when you go for >60 days slot you will be able to see per week data for 60 days. And for 365 days you can view the per month data. The granularity changes as per the data distribution for the duration. If a user accesses the Wi-Fi in a particular time slot like 8 am-12 pm multiple times, it will be counted as one visit for that time slot. But if the user logs in under different time slots, the user will be counted different for each time but for an overall view for the parent location, the guest user will be counted as one visitor.

Similarly, If a user logs in through different devices in the same time slot or different slot, the user will be counted as a different visitor each time as that login depends on the MAC address of the device. Different MAC addresses will count as different visitors.

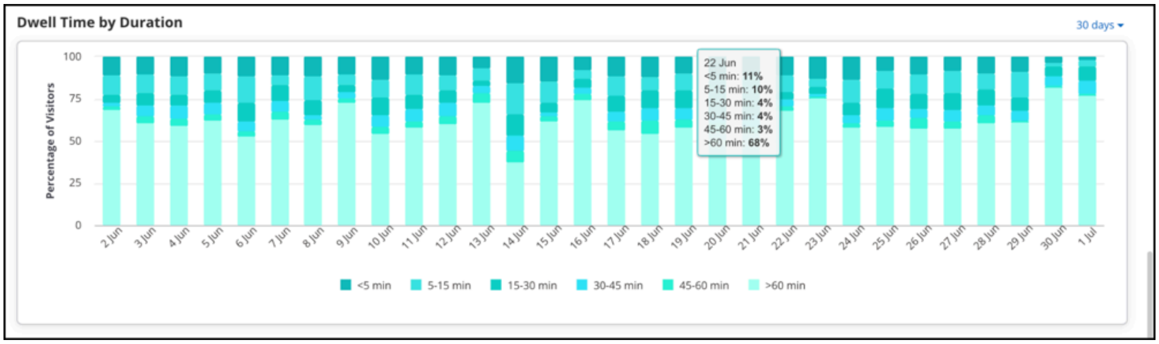
Footfall by Location

This is a location-wise bar graph depicting the total number of visitors during different time periods of the day (time splice) aggregated for the specified duration. The data is plotted for the selected location and its immediate child locations.



Dwell Time by Duration

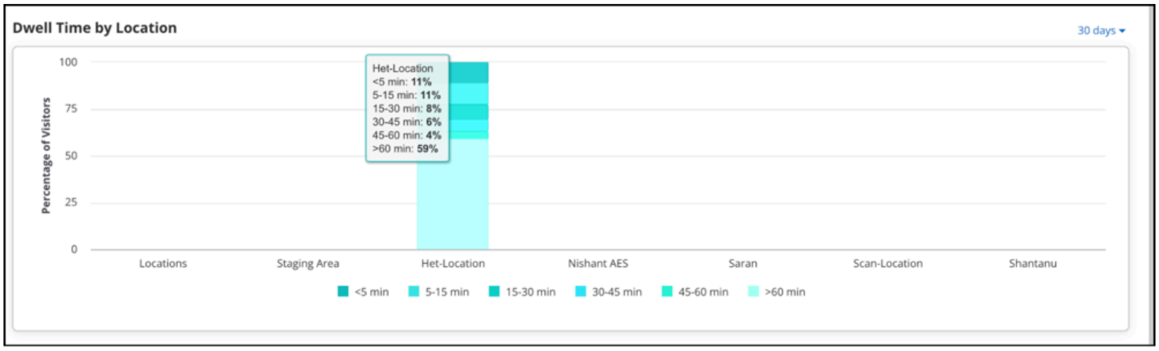
This is a bar graph showing total number of users who have accessed the Wi-Fi for different time periods during each visit for the specified duration and at the selected location.



The Dwell time depends on the received RSSI value. The relative signal strength of the Wi-Fi is considered to be good the more its value is close to 0. So, when a client connects for a particular time slot its duration is mapped. This is again an aggregated data. Suppose, in the time slot of 8-11 am, a client logs in at 8-9 am for 4 minutes and again logs in from 9-10 am for 3 minutes. The total time slot of the client will be 4+3= 7 minutes and will be depicted on the chart, accordingly.

Dwell Time by Location

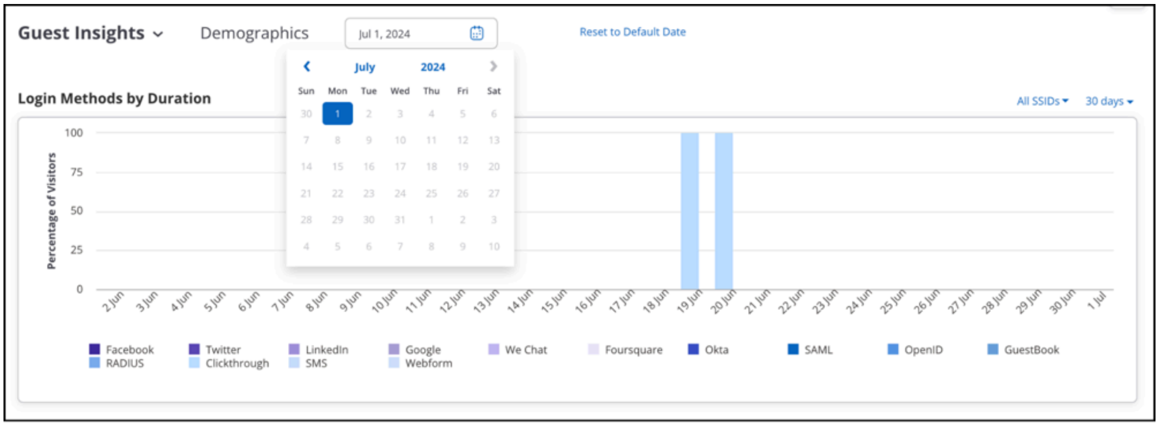
This is a location-wise bar graph depicting the total number of users who have accessed the Wi-Fi for different time periods during each visit. The data is aggregated for the specified duration and plotted for the selected location and its immediate child locations.



24.2.3 View Guest Demographics

To view Guest Demographics data, navigate to **Engage** > **Guest Insights** > **Demographics.**Demographic charts provide social analytic information for guest users who use Wi-Fi by authenticating with their social media accounts.

To view demographic data for a specific date, select the date from the date-picker at the top. The default is today’s date.

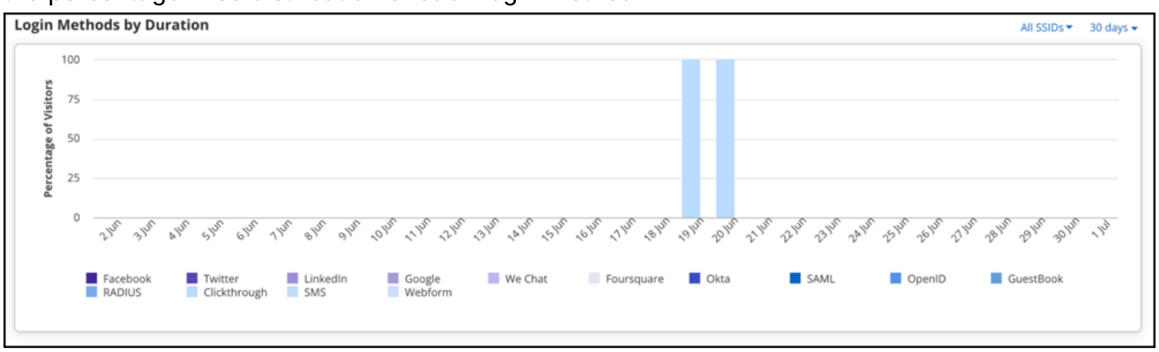


The demographics tab contains the following charts:

- Login Methods by Duration
- Login Methods by Location
- Social Engagement by Duration
- Social Engagement by Location

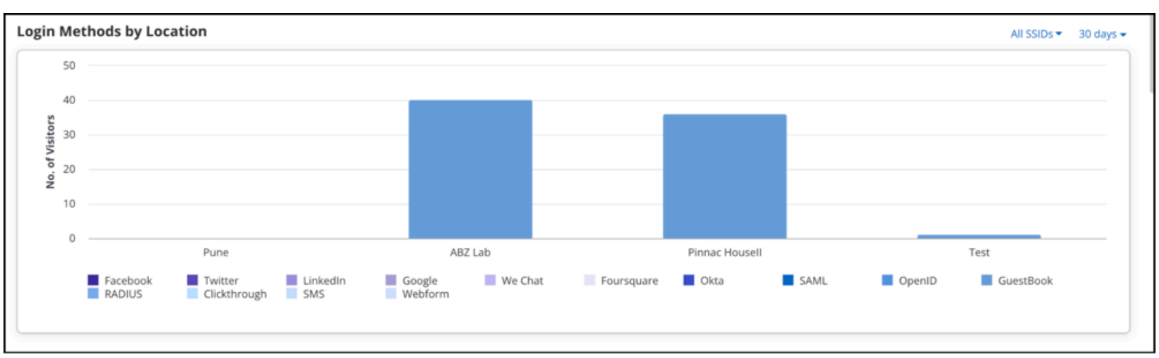
Login Methods by Duration

It is a bar graph charting login method-wise visitors (guests) accessing the Wi-Fi. For the selected location, the chart shows the number of visitors for each plug-in (social media, guest book, and click-through) during the specified duration for the selected SSID based on the selected date. You can hover over the bar to view the percentage-wise distribution of each login method.



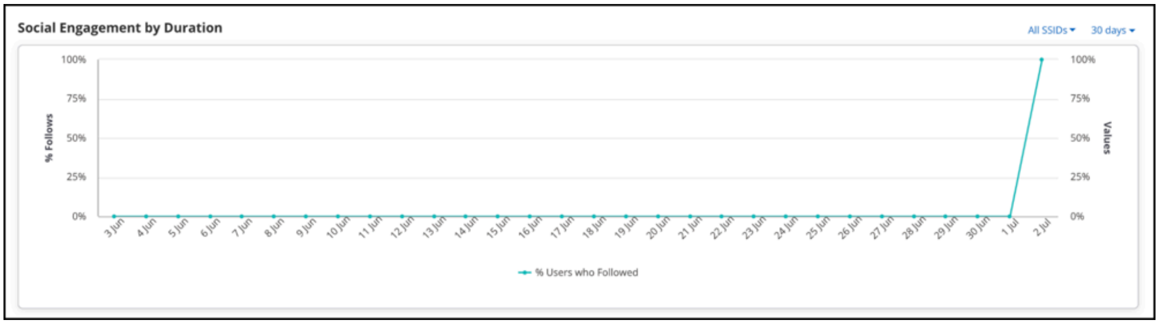
Login Methods by Location

This is a bar graph showing the login method-wise percentage of guests for the selected location and its child locations who have accessed the Wi-Fi during the specified time duration for the selected SSID.



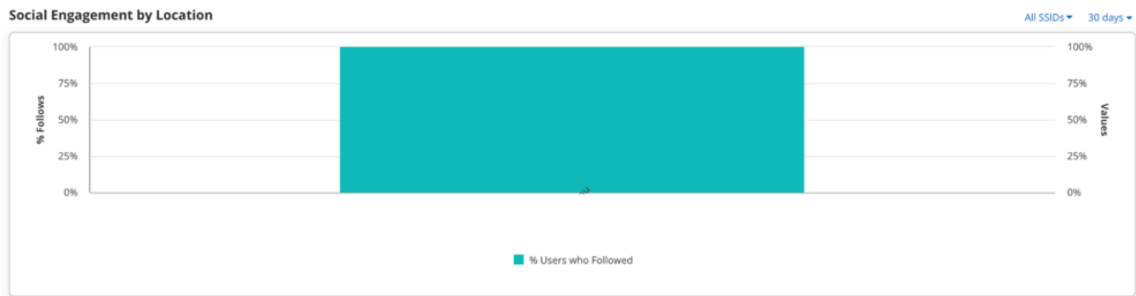
Social Engagement by Duration

This is a chart showing the number of guest users who logged in using a social media application and engaged with the platform for a selected duration.



Social Engagement by Location

This is a chart showing the number of guest users who logged in using a social media application and engaged with the platform for a selected location.



24.2.4 View Guest Profiles

To view Guest Profiles, navigate to **Engage** > **Guest Insights** > **Profiles.**The Profiles tab displays the guest profile information available for each location in the location tree.

The profile information of guests or visitors is presented in a tabular format. The information displayed is the information that the guest user has allowed to be displayed. When a user logs in to Wi-Fi, he logs in through a plugin, such as a Social plugin, Guestbook, or Webform. While logging in through the plugin, the user is asked to fill in various fields. Those fields, such as profile picture, portal, plugin, gender, or location, are displayed in the Profile tab.

Some of the information is visible by default. You can view additional fields by selecting them from the **Add/ Remove Column** button.

The following table provides a description of the fields seen in the profile information:

Table 26: Guest Profiles

Field	Description
Profile Picture	The photograph of the guest. This is retrieved from the social media site based on the respective social media account the user uses to access the Wi-Fi.
Portal	The name of the portal used to access the Wi- Fi.
Plugin	Name of the plug-in used to authenticate.
User Name	Login name of the guest as mentioned on the social media account.
First Name	First name of the guest as mentioned on the social media account.
Last Name	Last name of the guest as mentioned on the social media account.
Gender	Gender of the guest as mentioned on the social media account.
Number of Visits	Number of visits by the guest to the portal.
Location	Location of the guest as mentioned on the social media account.
Login Location	Location of the AP to which the guest connected. This is the location defined in the Wireless Manager.
Email ID	The E-mail ID of the guest as mentioned on the social media account.
Last Authentication Time	Date and time of the last visit by the guest to the portal.
Client MAC	MAC Address of the client.
Age Range	Age range of the guest.
Phone Number	Phone number of the guest as mentioned on the social media account.
Languages	Languages known to the guest as mentioned on the social media account.
Friends Count	Number of friends the user has on the social media account.
Followers Count	Number of followers as mentioned on the social media account.
DOB Day	Day of birth of the guest as mentioned on the social media account.
DOB Month	Month of birth of the guest as mentioned on the social media account.
DOB Year	Year of birth of the guest as mentioned on the social media account.
Date Created	Date of account creation.
Last Skip Time	Date and time of the last splash page skipped by the guest user.
Skip Visit Count	Number of time the guest user skipped the splash page.

Field	Description
Membership ID	Membership ID of the guest user.
Marketing Opt-in	Marketing Opt-in if used by guest user.

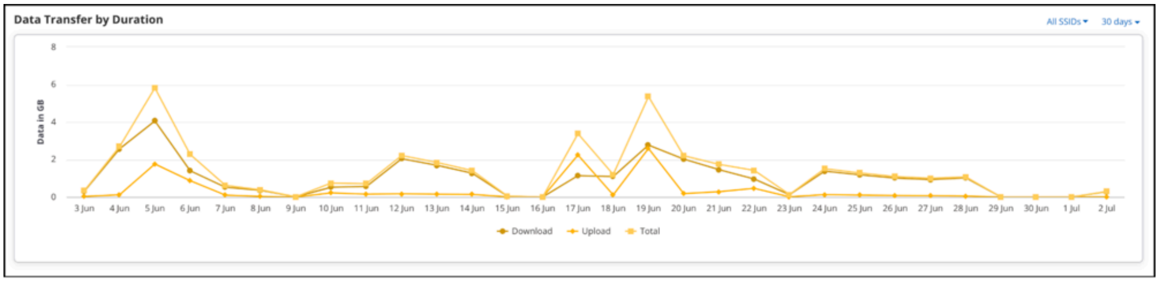
24.2.5 View Wi-Fi Usage

To view Wi-Fi Usage data, navigate to **Engage** > **Guest Insights** > **WiFi Usage**WiFi Usage tab contains the following charts:

- Data Transfer by Duration
- Data Transfer by Location

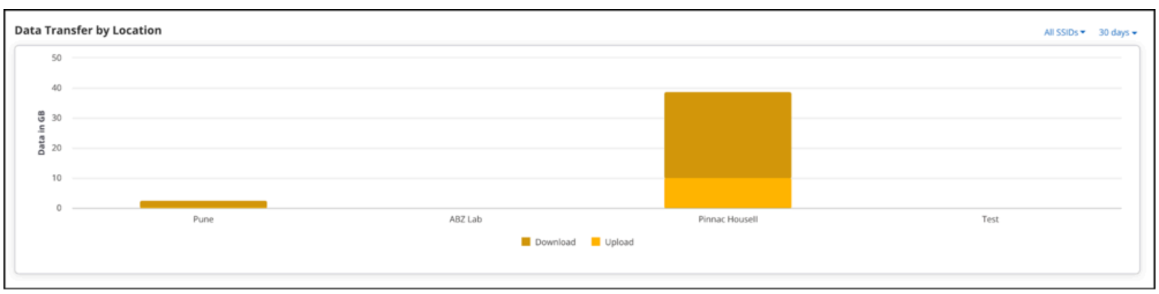
Data Transfer by Duration

This is a line graph that plots the data received and transmitted and the total data exchange over the specified duration at the selected location for the selected SSID.



Data Transfer by Location

This is a bar graph that plots the data transmitted and received for the specified duration at the selected location and its immediate child locations for the selected SSID. When you select a particular location from the root folder, the chart depicts the total Wi-Fi usage done in that particular location. The line data shows the data that is being transferred from AP to the client(download data) and from the client to the AP(upload data). The data transferred can be chosen for a particular location along with its child locations, SSID or duration. An aggregated data for the location is presented.

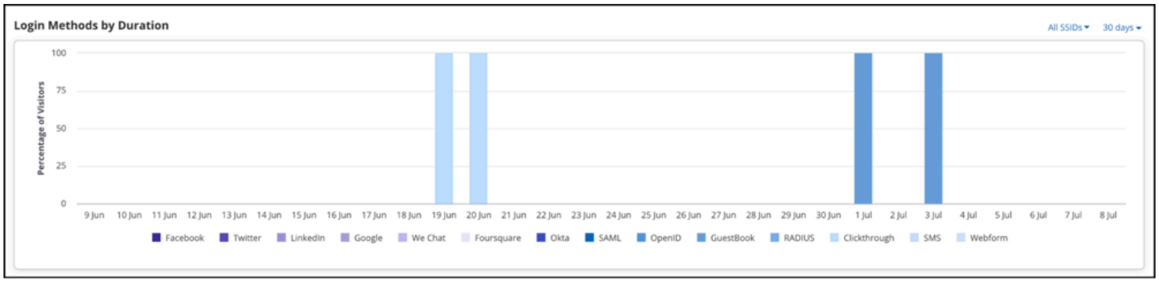


24.2.6 Guest Insights for Clients with Random MAC Addresses

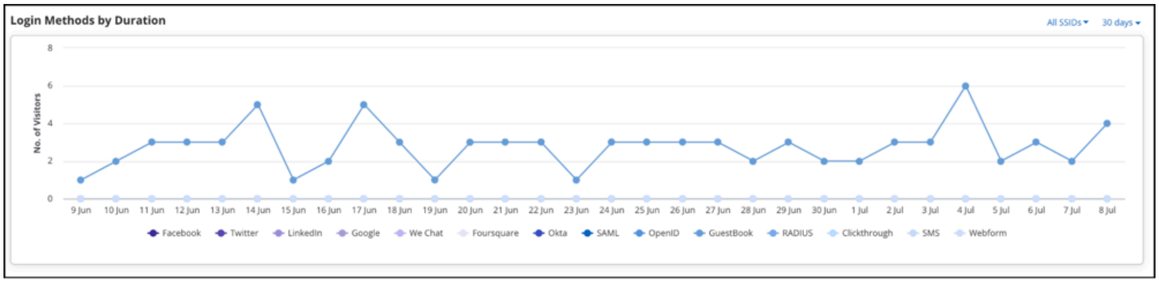
iOS, Android, and Windows OS have introduced the use of randomly generated, locally-administered MAC addresses for Wi-Fi clients. It is done to hide the hardware MAC for security reasons. As a result, identifying such devices by its MAC is not possible because the MAC address keeps changing with time.

When clients with random MAC addresses connect to an AP, the actual count and the absolute count of the clients are vastly different. Due to MAC Randomization, the same client can connect multiple times with an AP using MAC addresses in a shorter duration. The AP will consider such clients as different clients as the MAC addresses are different in every association. When clients with randomly assigned MAC addresses connect to CV-CUE, CV-CUE uses an approximation algorithm to identify such clients. GM then displays a percentage approximation of such clients in all the client-association charts, instead of displaying the actual count.

Login Method by Duration with MAC Randomization Enabled:



Login Method by Duration with MAC Randomization Disabled:



The following charts are different or have changes when you enable the MAC Randomization feature:

- **Overview > Conversion:** Shows only the total footfall.
- **Overview > Wi-Fi Users:** Shows only the percentage change in footfall instead of the absolute count.
- **Overview > New us Repeat Users:** Not available if MAC Randomization is enabled. Instead, a widget displaying Repeat Users is shown.
- **Overview > Dwell Time:** Shows approximate number.
- **Overview > Demographics - Male:** Not affected by MAC Randomization.
- **Overview > Demographics - Female:** Not affected by MAC Randomization.
- **Presence > Footfall by Duration:** Shows an approximate number instead of total count.
- **Presence > Footfall by Location:** Shows an approximate number instead of total count.
- **Presence > Dwell Time by Duration:** Converted the Y-axis into an approximate percentage count instead of an absolute count.
- **Presence > Dwell Time by Location:** Converted the Y-axis into an approximate percentage count instead of an absolute count.
- **Demographics > Login Methods by Duration:** Y-axis shows the approximate percentage count instead of the absolute count of visitors.
- **Demographics > Login Methods by Location:** Y-axis shows the approximate percentage count instead of the absolute count of visitors.
- **Demographics > Social Engagement by Duration:** Y-axis shows the approximate percentage count instead of the absolute count of visitors.
- **Demographics > Social Engagement by Location:** Y-axis shows the approximate percentage count instead of the absolute count of visitors.

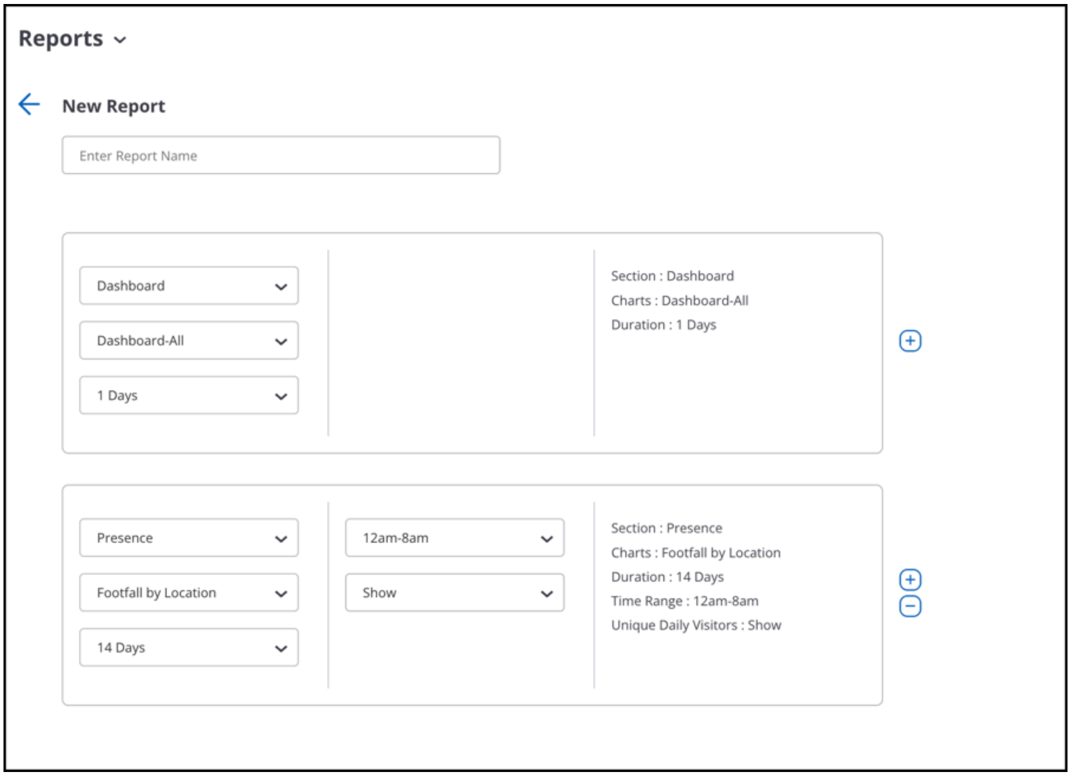
24.3 Create Reports

You can create one or more custom reports for a location floor. Each report can have segments with different filter criteria. A custom report can have one segment with a Dashboard section, one segment with a Floor Maps section, and one or more segments with the remaining sections.

The Demographics, Presence, Engagement, and Wi-Fi Usage sections can be repeated in a custom report with different filters applied to each of the repeating sections.

To generate a report:

1. Navigate to **Engage** > **Reports** tab.
2. Select the location for which you want to create the report.
3. Click **New Report.**
4. Enter the report name.
5. Click the **Add** icon to add a new segment.
6. Select the section, chart, and duration.
7. Select the appropriate option from any other filters that appear.
8. Repeat steps 5 through 7 to add new segments to the report.

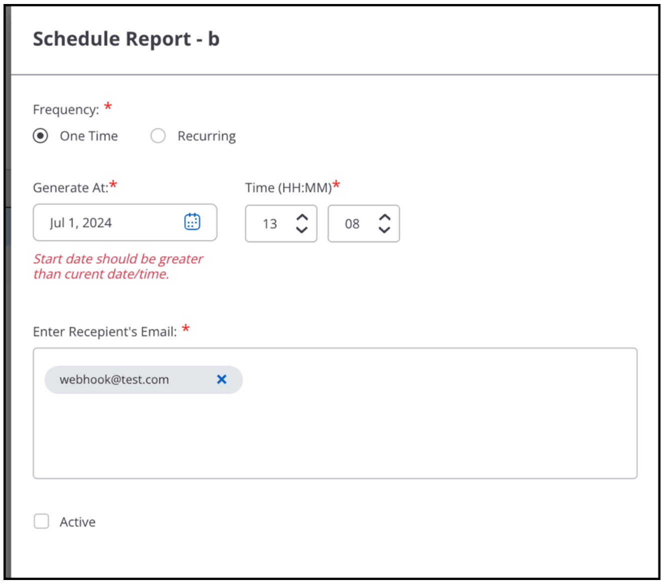


9. Click **Save.**

Once a report is saved, you can schedule it from the **Reports Listing** page.

To schedule a report:

1. Go to **Engage** > **Reports.**
2. Select **Schedule** from the three-dot menu next to your saved report.
3. Provide schedule details.



4. Click **Save.**

You will receive the generated report in the provided recipient's email. To generate a report in pdf format instantly, click **Download** from the three-dot menu and provide the date for the report.

24.4 Admin Settings

The following settings are available for administrators:

- Third-Party Integration
- View Logs

24.4.1 Third-Party Integration

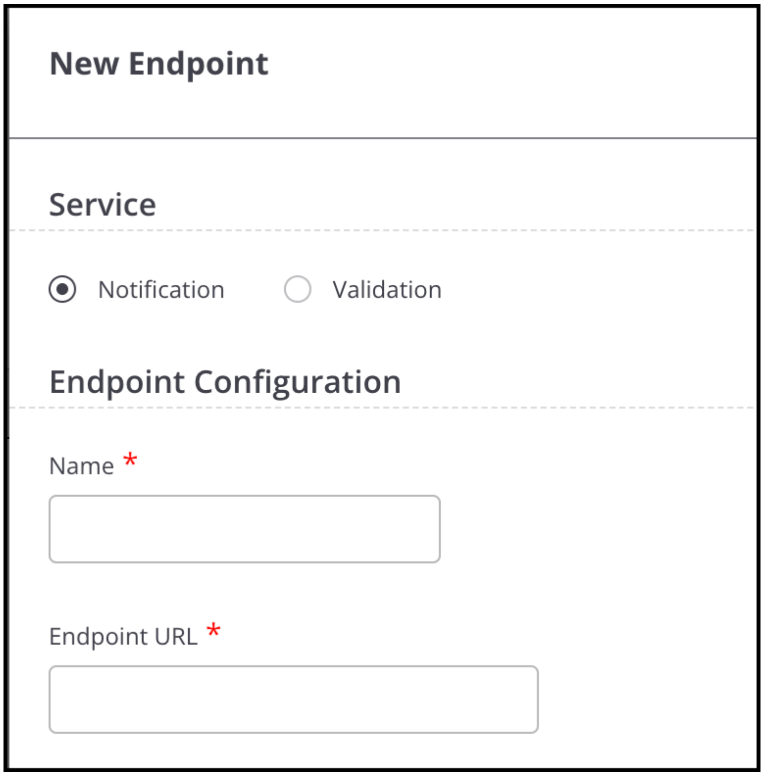
You can configure Third-Party Endpoints to receive **Notifications** when a guest user connects to the Wi-Fi or to **Validate** the request for accessing the guest Wi-Fi. An endpoint is a destination, say a service running on a server, to which the guest profile information is to be sent. When you configure the endpoint, you specify the destination URI, the HTTP method to use for data transfer, and the information (key-value pairs) to be sent to this endpoint.

CV-CUE provides a predefined set of values for a guest profile based on the information it captures. The individual fields in the guest profile information can be mapped to relevant keys or field names in a third-party application. Keys are the identifiers derived from the third-party application to which you want to associate this information to form a key-value pair.

After you define the endpoints, you must configure them in the respective plug-in QoS on the portal. This helps in sending the requested key-value pairs to the appropriate endpoint when a user authenticates from the portal splash page using the plug-in.

You can configure the endpoint for the following services:

- Notification Service
- Validation Service



The notification service occurs after the user logs in to the server, while the validation service happens when the user tries to connect to the server to gain access to the guest Wi-Fi.

Notification Service

By configuring an endpoint with a Notification service, you can send real-time guest profile information to third-party applications as soon as a guest user accesses a portal and successfully authenticates using one of the plug-ins defined on the portal.

This works for all the plug-ins like SMS, Guestbook, Facebook, LinkedIn, Google, Twitter, Foursquare, Instagram or Clickthrough. The third-party application can store it for future use. This information is sent in the form of key-value pairs and can be stored in any desired format, JSON, XML, or in a database by the third-party application. The information sent to the third-party plugins can be different for different plugins.

Validation Service

By configuring an endpoint with a Validation service, you can add an extra step for validation to secure the Wi-Fi access granted to guest users. The validation is needed to allow only authenticated users to have access to the Wi-Fi.

How does validation work?

The authentication process is done by specifying certain primary parameters which will perform the authentication process. In case of the SMS plugin, we need a valid phone number of the user which will receive an OTP or any authenticated code that will validate the user. This can be a combination of two or more than two parameters.. It depends on the customer and its customized splash page.

For example, if a user logs in to the portal and needs to access the guest Wi-Fi in a particular office area. He is then asked to provide a valid phone number and an insurance id. These two unique primary factors define the user and the information is sent to the server. The server then sends an OTP via SMS plug-in to the user's phone number. Once the details have been put in, the authentication process takes place and a corresponding success or failure message is sent based on which the guest user can log in.

Configuring an Endpoint for Third-Party Integration

You can add endpoints for third-party integration. The guest profile information can be sent to the endpoint using the HTTP GET and HTTP POST methods or the redirect method. You can send guest profile information that is collected by Guest Manager and custom data where you can specify your own key and corresponding value for the key.

When adding an endpoint, you must enter at least one notification parameter for the endpoint. If you select the parameter type as Guest Manager, you must select a value from the predefined list of values.

If you select the HTTP GET method or redirect, the key-value pairs are appended to the endpoint URL. If you select HTTP POST, the key-value pairs are sent as encoded form-data. A Notification Preview is presented on the bottom of the page as you enter the key-value pairs. This is a preview of the actual form in which the data will be sent to the third-party application using an HTTP request. The Validation Preview has a header tab and request body. The request body parameter generates only when the call is POST Call and for SMS plugin specifically.

To configure a new endpoint:

1. Navigate to **Engage** > **Admin Settings** > **Third Party Integration.**
2. Click **New Endpoint.**
3. Provide the endpoint details:

Table 27: End Point Details

Field	Description
Service	The service type can be either Validation or Notification.
Name	A user-defined name of the endpoint.
End Point URL	The URL of the endpoint. This is URL to which the key-value pairs will be sent. This could be a service listening for requests and handling the incoming key-value pairs.
Description	An optional description of the endpoint.
Method Type	You can select only one method for an endpoint. Select GET, POST, or Redirect option. If you select the HTTP GET method or redirect, the key value pairs are appended to the endpoint URL. If you select HTTP POST, the key-value pairs are sent as encoded form-data. If you select the Redirect option, you must select the third-party endpoint as the Redirect URL in the respective plug-in QoS tab of the portal.
Response Timeout	The timeout, in seconds, for which CV-CUE keeps the data in its cache for sending it to the endpoint. After the timeout period, the data is deleted from the cache. The default value is 10 seconds. Response timeout can have a maximum value of 60 seconds.
Retry Count	This is an integer value that specifies the number of times server will try reconnecting to the third-party server. The maximum retry count is 3.
Notification Preview	Preview the Requested URL and encoded form data.

4. Select **Request Body** as Form Data. Click **Add new row** to add Parameters as specified in the following table. Repeat this step to add multiple parameters.

Field	Description
Parameter Type	The type of parameter to pass to the third-party application. Select Guest Manager if you want to pass a parameter captured by the Guest Manager. To send custom key-value pairs, select the Custom option. You can include a mix for Custom and Guest Manager notification parameters.
Key	The key name to which the corresponding value will be associated. You can define key names that map with the appropriate fields or attributes defined in the third-party application.
Value	The parameter to pass to the third-party application. For a Guest Manager parameter, select a predefined value from the drop-down list that will be mapped to the corresponding key. If the parameter type is Custom, you can enter any string here.

5. For **POST** operations, you can also define the parameters through the Raw Body section where you can define the JSON parameters in parentheses. The possible values for the parameters are:

portal_name	visit_count	birth_day
email	ap_mac	private_data
friends_count	languages	first_name
plugin_name	last_visit	birth_month
gender	ap_ssid	membership_id
followers_count	location	last_name
client_mac	date_created	phone_number
picture_url	username	marketing_option
birth_year	login_location	age_range

6. Click **Done.**

After you define a third-party endpoint, it must be configured in the portal plug-in. CV-CUE then sends the notification parameters (guest profile information) configured in the endpoint to the third-party application.

While CV-CUE tries to connect with the third party and fails to receive a response, it submits the request again after trying for the specified response time. The server can retry to establish a connection, but the maximum number of retries is only 3. There is no retry for failure in connection establishment.

24.4.2 View Logs

You can use logs to analyze usage pattern of the Wi-Fi as well as the actions performed on your account.

You can download and view the following logs:

- Audit Logs
- Guest Wi-Fi Access Logs
- SMS Logs
- Payment Logs

To download Engage Logs:

1. Navigate to **Engage** > **Admin Settings** > **Logs.**
2. Select **Log Type.** You can select from:

- **Audit Logs:** Audit logs provide information about the Guest Manager user activities. Audit logs are available for the past 365 days. They contain the following information:

Table 28: Audit Logs

Field	Description
IP Address	IP address of the computer device from which the operation was performed.
Operation Type	Type of operation. The operation types logged are Create, Read, Update, Delete, and Other. Some operations, such as login and logout, are categorized as Other.
Operation Performed	Details about the performed operation.
Date/Time	Date and time of the operation.
Username	Username of the CV-CUE user who performed the operation.
Role	Role of the user who performed the operation.
Portal Name	Name of the portal for which the operation was performed.

- **Wi-Fi Access Logs:** You can download access logs for a particular portal. Wi-Fi Access Logs contain the following information:

Table 29: Wi-Fi Access Logs

Field	Description
Portal	Name of the portal accessed by the guest user.
Type	Type of access operation. This indicates whether it is a login, logout, portal access or gate access. Portal access entry is recorded when the user accesses the portal. A gate access entry is recorded when the access point opens the gate for the user to access the Internet.
Client Public IP	IP address of the client used by the guest user to connect to the access point.
Client Local IP	If NAT is enabled, Client Local IP is from the IP Pool defined in the NAT configuration. If NAT is disabled, it is the same as Client Public IP.
Client MAC	MAC address of the client used by the guest user to connect to the access point.
AP MAC	MAC address of the access point used by the guest user to access Wi-Fi.
AP IP	IP address of the access point accessed by the guest user.
AP SSID	SSID of the access point accessed by the guest user.
AP Port	Port number used to communicate with the access point.
User Agent	User agent details of the browser used by the guest user to access Wi-Fi.
User URL	URL accessed by the guest user.
Username	The user account used to access the Wi-Fi, followed by the plug-in name.
Message	Provides gateway access and log-off URLs. Message also include session timeout, blackout time, download limit, upload limit, and the redirect URL configured on SSID.
Date/Time	Date and time of access by the guest user.

- **SMS Logs:** SMS logs contain detailed information about which code was sent to which number and how many times, the last login status, and other information such as the client and AP MAC address. SMS logs are generated for the selected account. SMS logs contain the following information:

Table 30: SMS Logs

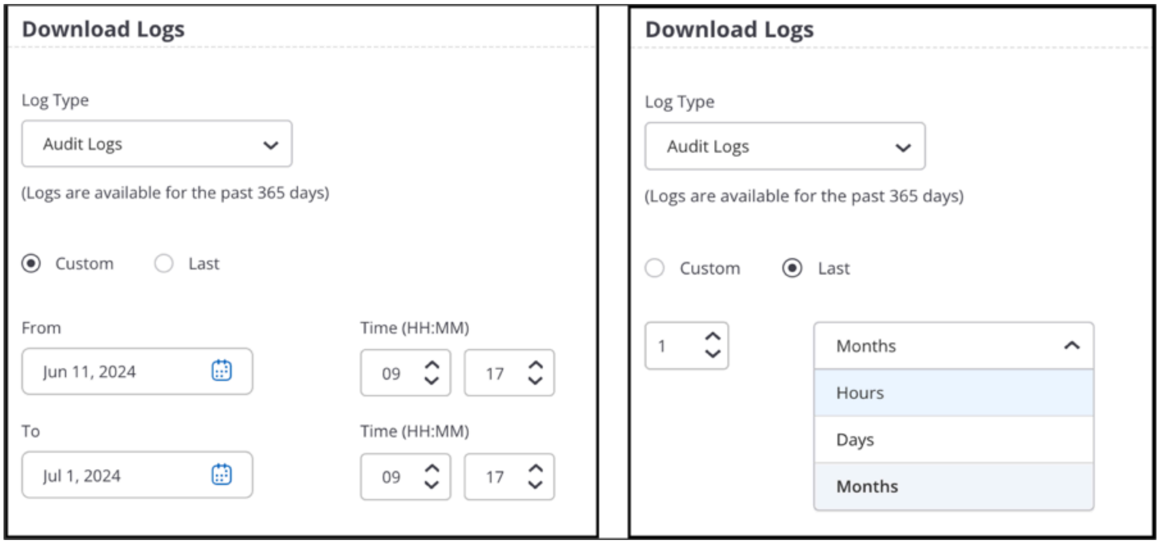
Field	Description
SMS Account Name	Name of the configured SMS account.
Service Provider	The service provider used to send the SMS. This can be Twilio, MSG91, or a custom service provider.
Sender ID	The Twilio number or short code configured or the MSG91 sender ID configured on the plug- in.
Mobile No	The mobile number provided by the guest for receiving the SMS with Internet access code.
SMS Content	Message content of the sent SMS containing the authentication code.
Date Created	Date of SMS code generation.
Sender Component	Sender Component could be SMS Test Health or SMS Authentication Plugin. SMS Test Health corresponds to the option to test out if the SMS App is working or not. SMS Authentication Plugin gets triggered through the Authentication workflow upon client connection.
Other	Other details such as SSID, Client MAC address, AP MAC address.

- **Payment Logs:** Payment Logs contain detailed information about payment transactions. The following information is captured in payment log:

Table 31: Payment Logs

Field	Description
MGM Transaction ID	Transaction ID generated by MGM for every transaction.
Payment Gateway Transaction ID	Transaction ID generated by the payment gateway.
Timestamp - Transaction Initiated	Timestamp when the transaction with the gateway was initiated.
Timestamp - Transaction Completed	Timestamp when the payment gateway responds with a code.
Status Internal	MGM recorded internal status of the transaction. • Initiated • Completed - Passed • Completed Failed • Timed out
Status - Payment Gateway	Payment gateway generated status.
Transaction Amount	Amount value of Transaction
Payment Tier Chosen by User	The tier that the user chose while doing the transaction.

3. Select **Custom** to enter a custom date and time or select **Last** to generate logs for the last specified days, hours, or months.



4. Click **Download.**

Audit Logs will be downloaded to your local download folder.

Chapter 25

Troubleshooting Wi-Fi

The **TROUBLESHOOT** view in CV-CUE provides tools that help the network administrators troubleshoot issues in the Wi-Fi network.

This chapter contains the following topics:

25.1 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 CV-CUE:

1. Go to **MONITOR** > **WiFi** > **Clients** or **MONITOR** > **WIPS** > **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**.
3. On the Capture tab, enter the following details and click **Start Packet Capture**.

Option	Description
Mode	Select the Mode of packet capture: • **Access Radio Inline:** Captures associated BSSID and client through the access radio. • **Access Radio Promiscuous**: Captures all packets through the access radio. • **Multi Function Radio:** OTA capture through the multi-function radio.
Duration of Packet Trace	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.
Streaming Option	It specifies the type of packet capture to be used: • **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. • **Wireshark on local machine:** The packet trace can be opened during an ongoing capturing process.
Filename Prefix	It is mandatory field to specify the prefix for a filename. For example, Packet_wireless_143438.pcap, where: • Packet: is the prefix of the file name. • _wireless_143438: is the name of the file. • .pcap: is the file extension which is compatible with Wireshark.
Wireless Settings	Select this option to edit advanced wireless settings.
Traffic Selection	It is the type of traffic that you prefer while troubleshooting. • **All packets on the channel**: To capture all packets from all clients visible to the troubleshooting AP sensor. • **Only packets for the selected Client <MAC address>**: To view only packets from the selected AP.
Packet Types	Select the type of packets that you want to capture.

Option	Description
Frequency Band and Channel Selection	Select the Frequency Band 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. A dialog displaying the ongoing progress for the capture packet trace is displayed. Click **Stop** to forcefully stop the packet capture.

A dialog displaying the ongoing progress for the capture packet trace is displayed. Click **Stop** to forcefully stop the packet capture.

4. After the successful completion of the packet trace, click **Download** to view the file in Wireshark.

25.2 View Packet Trace History for a Client

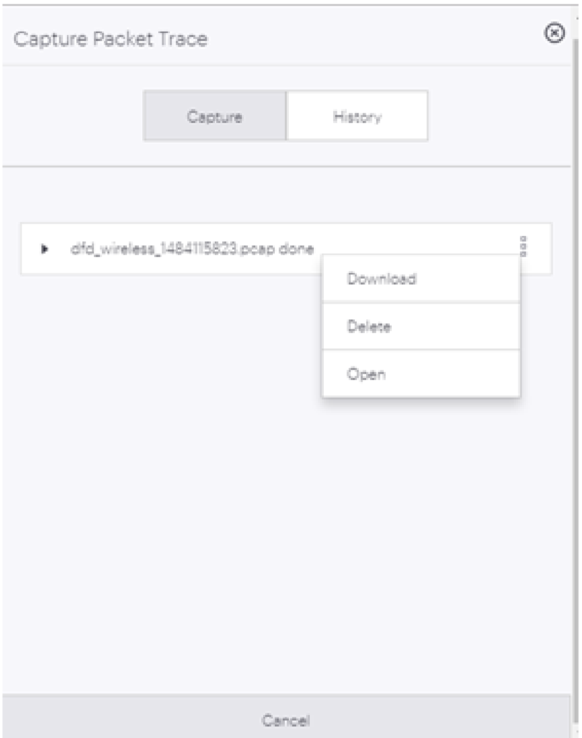
You can view the **Packet Trace History** for a selected client. The packet traces captured only during the last 30 minutes are displayed in the history.

To view the packet trace history, perform the following steps:

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:

Field	Description
Filename	Filename specifies the name of the captured packet trace.
MAC Address	MAC Address of the device for which packet trace is captured.
Capturing Device MAC Address	MAC Address of the device that has captured the packet trace.
Start	Start time of packet capture.
End	End time of packet capture.
Troubleshooting Mode	Mode of troubleshooting.
Status	Status specifies if the trace is completed or in progress.

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.

25.3 Capture Packet Trace for an Access Point

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** > **WiFi** > **Access Points** or **MONITOR** > **WIPS** > **Access Points**.
2. Right-click on the name of the AP for which you want to capture the packet trace and select **Capture Packet Trace.**
3. On the **Capture** tab, enter the following details and click **Start Packet Capture.**

Option	Description
Mode	Select the Mode of packet capture: • **Access Radio Inline:** Captures associated BSSID and client through the access radio. • **Access Radio Promiscuous**: Captures all packets through the access radio. • **Multi Function Radio:** OTA capture through the multi-function radio.
Timeout	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.
Streaming Option	It specifies the type of packet capture to be used: • **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. • **Wireshark on local machine**: The packet trace can be opened during an ongoing capturing process.
Filename Prefix	It is mandatory field to specify the prefix for a filename. For example, Packet_wireless_143438.pcap, where: • Packet: is the prefix of the file name. • _wireless_143438: is the name of the file. • .pcap: is the file extension which is compatible with Wireshark.
Wireless Settings	Select this option to edit advanced wireless settings.
Traffic Selection	It is the type of traffic that you prefer while troubleshooting. • **Packets of all BSSIDs on this access point:** Captures all the packets for all BSSIDs broadcasted by the selected AP. • **Packets of a single BSSID:** Captures the packets for a single BSSID broadcasetd by the selected AP. Select your BSSID from the given drop-down list. • **All packets on the configured channels in Frequency Band and Channel Selection section:** Captures all the packets for all the channels defined in the Frequency Band and Channel Selection section.

Option	Description
Protocol and Channel Selection	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.
Wired Settings	Select this option to capture packets from wired devices.
Interface	Select from the available ethernet ports from the list. The default value is eth0.
VLAN ID	Enter the VLAN Id.
ICMP, UDP, DHCP, MDNS, LLMNR, DNS, RADIUS, ARP, TCP	Select required protocols from the list.

A dialog displaying the ongoing progress for the capture packet trace is displayed. Click **Stop** to forcefully stop the packet capture.

4. After the successful completion of the packet trace, click **Download** to view the file in Wireshark.

25.4 View Packet Trace History for an Access Point

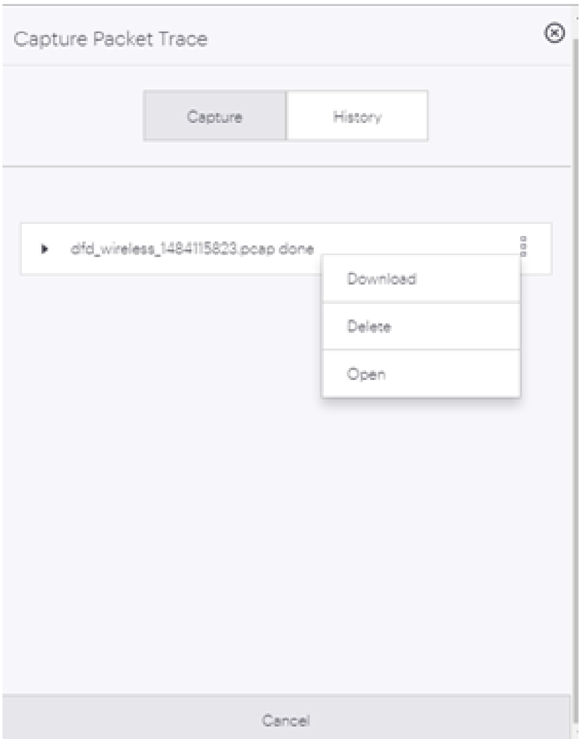
You can view the **Packet Trace History** for a selected AP. The packet traces captured only during the last 30 minutes are displayed in the history.

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:

Field	Description
Filename	Filename specifies the name of the captured packet trace.
MAC Address	MAC Address of the device for which packet trace is captured.
Capturing Device MAC Address	MAC Address of the device that has captured the packet trace.
Start	Start time of packet capture.
End	End time of packet capture.
Troubleshooting Mode	Mode of troubleshooting.
Status	Status specifies if the trace is completed or in progress.

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.

25.5 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

25.5.1 Start Live Debugging

You can start the live debugging for one client at a time. However, you can parallelly debug maximum 10 clients on CV-CUE.

To start live client debugging, perform the following tasks:

1. Navigate to **MONITOR** > **WiFi** > **Clients** or **MONITOR** > **WIPS** > **Clients**.
2. Right-click on the client that you want to debug and select **Start Client Live Debugging**.

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 locatiion 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.

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     : WebAppsDevC120
BSSID    : 00:11:74:F2:17:B0
AP NAME :  Mojo F2:17:BF
Chan     : 11
Time     : 2017.04.03 11:40:21 (Asia/Kolkata)
Tdiff(msec)          Timestamp
Event         0      2017.04.03 11:40:21          Deauthentication received from client because sending STA is leaving
              2      2017.04.03 11:40:21          Node LeftSSID    : WebAppsDevC120BSSID   : 00:11:74:F2:17:B0AP NAME
             12      2017.04.03 11:40:23          Client successfully (re)associated
             13      2017.04.03 11:40:23          First phase of WPA/WPA2 4-Way Handshake Completed
             66      2017.04.03 11:40:23          Second phase of WPA/WPA2 4-Way Handshake Completed
             67      2017.04.03 11:40:23          Third phase of WPA/WPA2 4-Way Handshake Completed
             95      2017.04.03 11:40:23          Node Authorized
             96      2017.04.03 11:40:23          Fourth phase of WPA/WPA2 4-Way Handshake Completed
            203      2017.04.03 11:40:23          Client sent DHCP DISCOVER
            271      2017.04.03 11:40:23          DHCP OFFER sent to Client from [172.16.100.254]
            272      2017.04.03 11:40:23          Client has received IP [172.16.100.1]
            295      2017.04.03 11:40:23          Client sent DHCP REQUEST
            370      2017.04.03 11:40:23          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.

25.5.2 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.**
2. Right-click on any such log, and select **Stop Live Debugging**.

Note: Alternatively, you can stop the debugging, by navigating to **MONITOR** > **WiFi** > **Clients** or **MONITOR** > **WIPS** > **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

25.5.3 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**.

> **Note:** To view the Live Client Debugging, you can also navigate to **MONITOR** > **WiFi** > **Clients** or **MONITOR** > **WIPS** > **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.

25.5.4 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.**
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**.

25.5.5 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.**
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**.
3. 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.

25.5.6 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.

25.6 Audit Logs

Audit logs are logs of various user actions such as logging into CV-CUE or logging out of CV-CUE, changes in location hierarchy, etc. Logs help in tracking user actions, which can be used for user accountability.

Note: Only a Superuser can download audit logs or configure the audit logs retention settings.

25.6.1 Audit Log Types

Log Type	Description
User Access	Logs user action related to user access such as password changes, RADIUS authentication changes, and others
All	Includes all log types
Devices	Logs user action related to the AP such as AP name changes, AP reboot, AP firmware upgrade, and others
Alerts	Logs user action related to alerts such as deleting an alert
Global Settings	Logs user action related to global settings such as changes to Google integration, Syslog server, and SNMP settings, and so on
Location Based Settings	Logs user action related to location based settings such as SSID settings, which includes firewall, role-based access control, network, and others
Location Hierarchy	Logs user action related to the location hierarchy such as adding or deleting a folder or group, floor map related changes, and others
Reports	Logs user action related to the location hierarchy such as adding or deleting a folder or group, floor map related changes, and others
Start/Stop Functions	Logs user action related to system services such as database, web server, and so on
System	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
Third Party and Others	Includes changes related to third party servers and custom files

25.6.2 Download Audit Logs

To 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.

25.6.3 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.

Chapter 26

Floor Plans

You can add floor plans to a location in CV-CUE.

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 CV-CUE, 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. This chapter contains the following topics:

- Add A Floor Plan
- Perform Operations on an Access Point from Floor Plan

26.1 Add A Floor Plan

You can add floor plans to a location in CV-CUE.

To add a floor plan to a location:

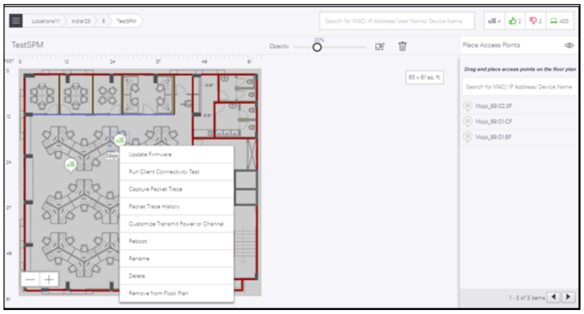
1. In the CV-CUE location hierarchy, go to the location where you want to add the floor plan.
2. Go to **Floor Plans** and click **Add Floor Plan**.
3. Enter the name you want to give to the floor plan.
4. Click **Upload Image** or **Upload SPM**.
5. Set the dimensions of the floor plan.
6. Click **Save** to save the floor plan.

26.2 Perform Operations on an Access Point 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 CV-CUE 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.



Chapter 27

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. This chapter contains the following topics:

- Default View
- AP Coverage View
- AP Link Speed View
- AP Channel Coverage View
- Resolution and Frequency Filters

27.1 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**.

27.2 Access Point 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**.

27.3 Access Point 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.

27.4 Access Point 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**.

27.5 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 the following 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.
- **6 GHz:** Data for only 6 GHz AP radios will be shown.
- **All bands:** Data for 2.4, 5, and 6 GHz AP radios will be shown.

Chapter 28

Locate Access Points and Clients

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 not 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 CV-CUE:

- FLOOR PLANS
- MONITOR > WiFi > Clients
- MONITOR > WiFi > Access Points
- MONITOR > WIPS > Managed WiFi Devices
- MONITOR > WIPS > Access Points
- MONITOR > WIPS > Clients
- Alert Drilldown

This chapter contains the following topics:

- Locationing Criteria
- Locate an Access Point or a Client in a Floor Plan
- Drill Down from a Device

28.1 Locationing Criteria

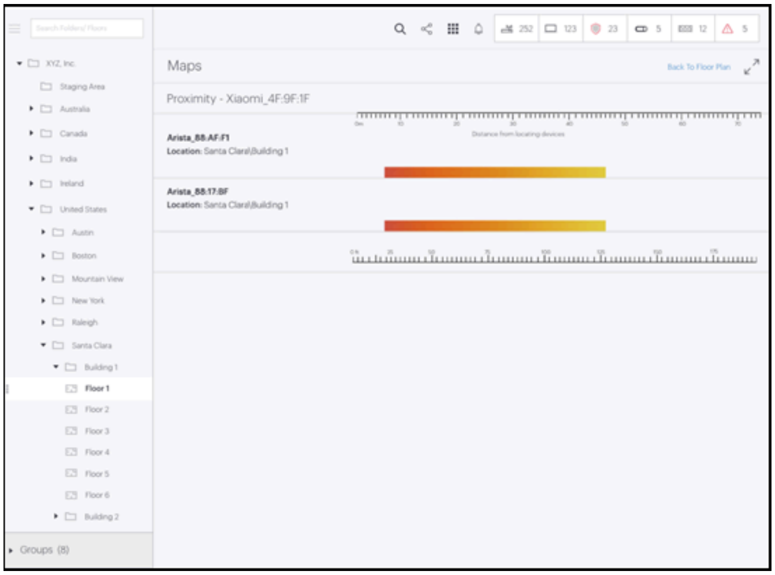
The server runs the locationing algorithm and, based on it, APs report another AP or client's RSSI. Whether APs can detect another AP or client depends on three criteria:

- 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 not 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 not 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 not 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 Wi-Fi 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.

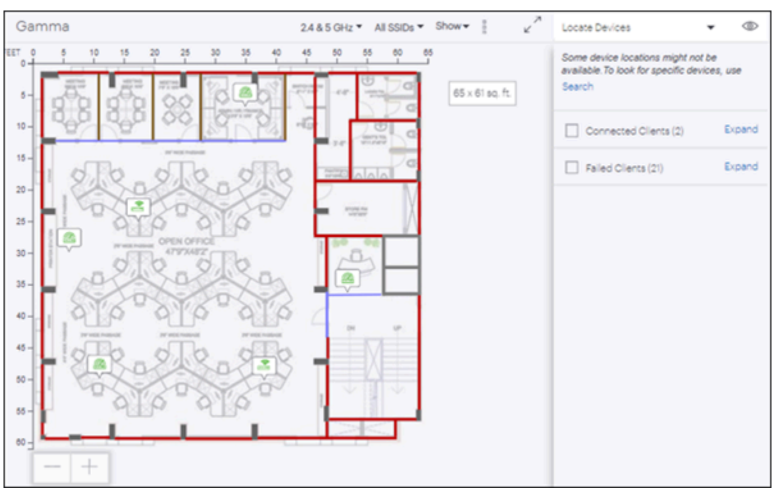
If CV-CUE can not locate a device because there is no placed AP or because fewer than three APs are placed on the floor, then it displays the Proximity view for the device. The Proximity page shows an approximate distance of the device with respect to other APs.



28.2 Locate an Access Point or a Client in a Floor Plan

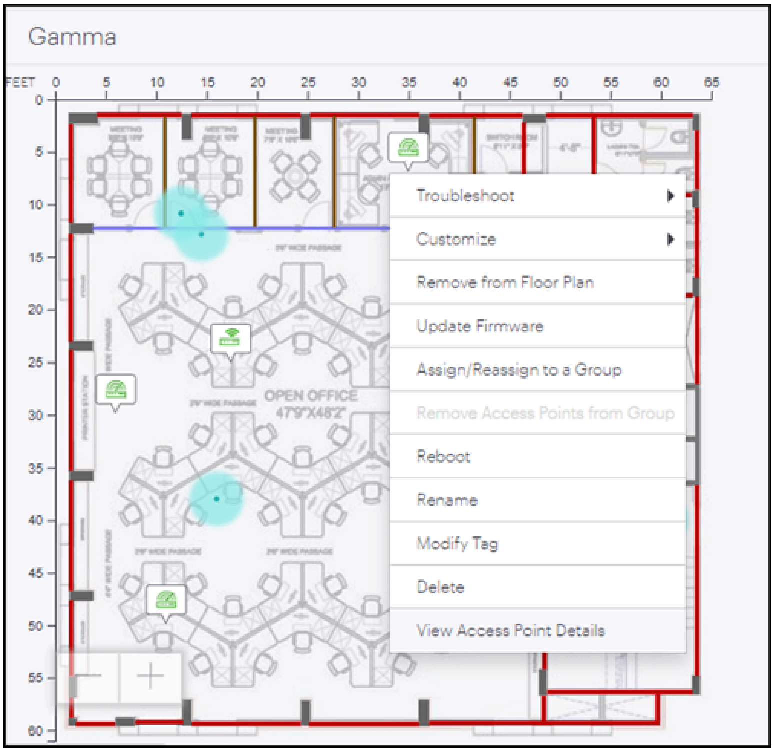
You can locate managed clients and devices using the Connected Clients and Failed Clients checkboxes. Use the Search option from the right panel to locate unmanaged and unplaced devices and clients, especially WIPS clients and devices. You can also use Search to see the Proximity views of clients that 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.



28.3 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.



28.3.1 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 not 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**.

28.3.2 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

Chapter 29

Reports in CV-CUE

CV-CUE currently supports the following types of reports.

Table 32: Reports in CV-CUE

WIPS	Wi-Fi	Alerts	Complaince
Reports about the Wi-Fi security posture	Reports about the Wi-Fi Clients, APs, Radios, WLANs,Applications, and Tunnels in the network.	Reports capturing Wi-Fi, WIPS, and System Alerts.	Reports to meet federal or industry-based regulatory compliance for Wi-Fi security.
Inventory Reports: • WIPS Clients - Instantaneous • WIPS Access Points - Instantaneous • Managed Wi-Fi Device Inventory • WIPS Managed Wi-Fi Devices - Instantaneous • WIPS Networks - Instantaneous **Policies Enforcement Reports:** • Security Status • Wireless Intrusion Prevention Summary • Access Point Classification • Airspace Risk Assessment • Client Classification • Wireless Vulnerability Assessment • WIPS Alerts	**Inventory Reports:** • WiFi Clients - Instantaneous • WiFi Access Point Details - Instantaneous • WiFi Radios - Instantaneous • WiFi Access Points - Instantaneous • WiFi Tunnels-Instantaneous **Connectivity Reports:** • Client Connectivity - Historical • Client Application Experience Report - Historical • WiFi Clients - Historical • Client Visibility • Client Association	**Alert Reports:** • Alerts WIPS • Alerts WiFi • Alerts System	**Compliance Reports:** • DoD Directive 8100.2 Compliance • GLBA Wireless Compliance • PCI DSS Wireless Compliance • HIPAA Wireless Compliance • SOX Wireless Compliance • PCI DSS Wireless Compliance Internal Audit Report • MITS Wireless Compliance

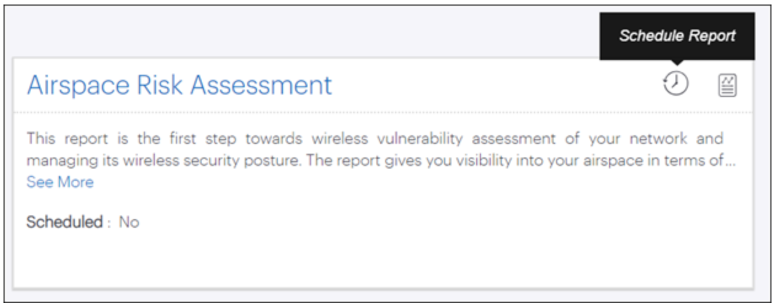
The reports can be accessed via the **Reports** tab on the left menu. You can view the definition and sections in each report, generate a report on-demand, or schedule one-time or recurring generation of a report.

This chapter contains the following topics:

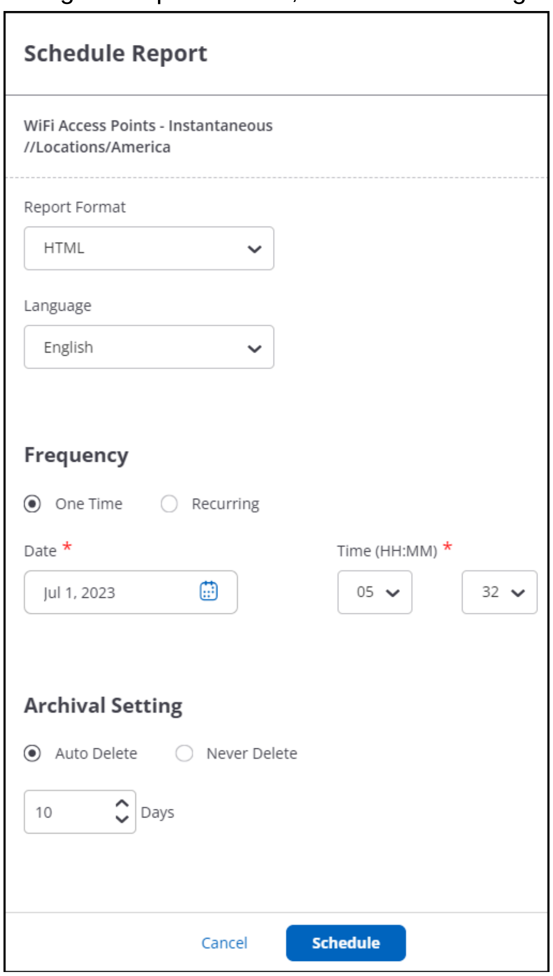
- Scheduling Reports
- On-Demand Generation of Reports
- Saving a Report

29.1 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.



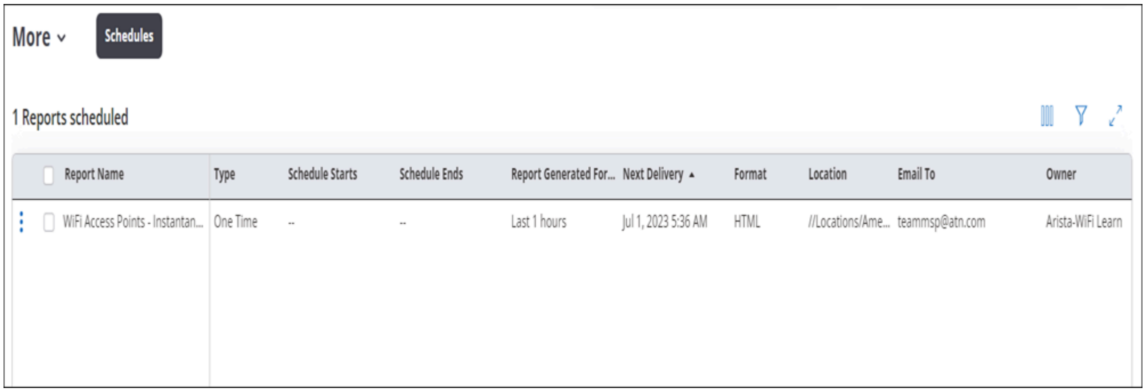
Clicking the **Schedule Report** icon opens a panel on the right-hand side of the screen, with a set of user-configurable parameters, as shown in the figure below.



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.

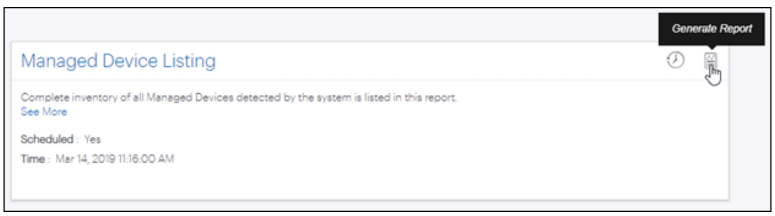
If the archival setting is set to Never Delete, then the URL sent in the email will always be valid until the report is manually deleted from the **REPORTS** > **More** > **Saved** page.

Once the report is successfully scheduled, it can be seen under **REPORTS** > **More** > **Schedules.**

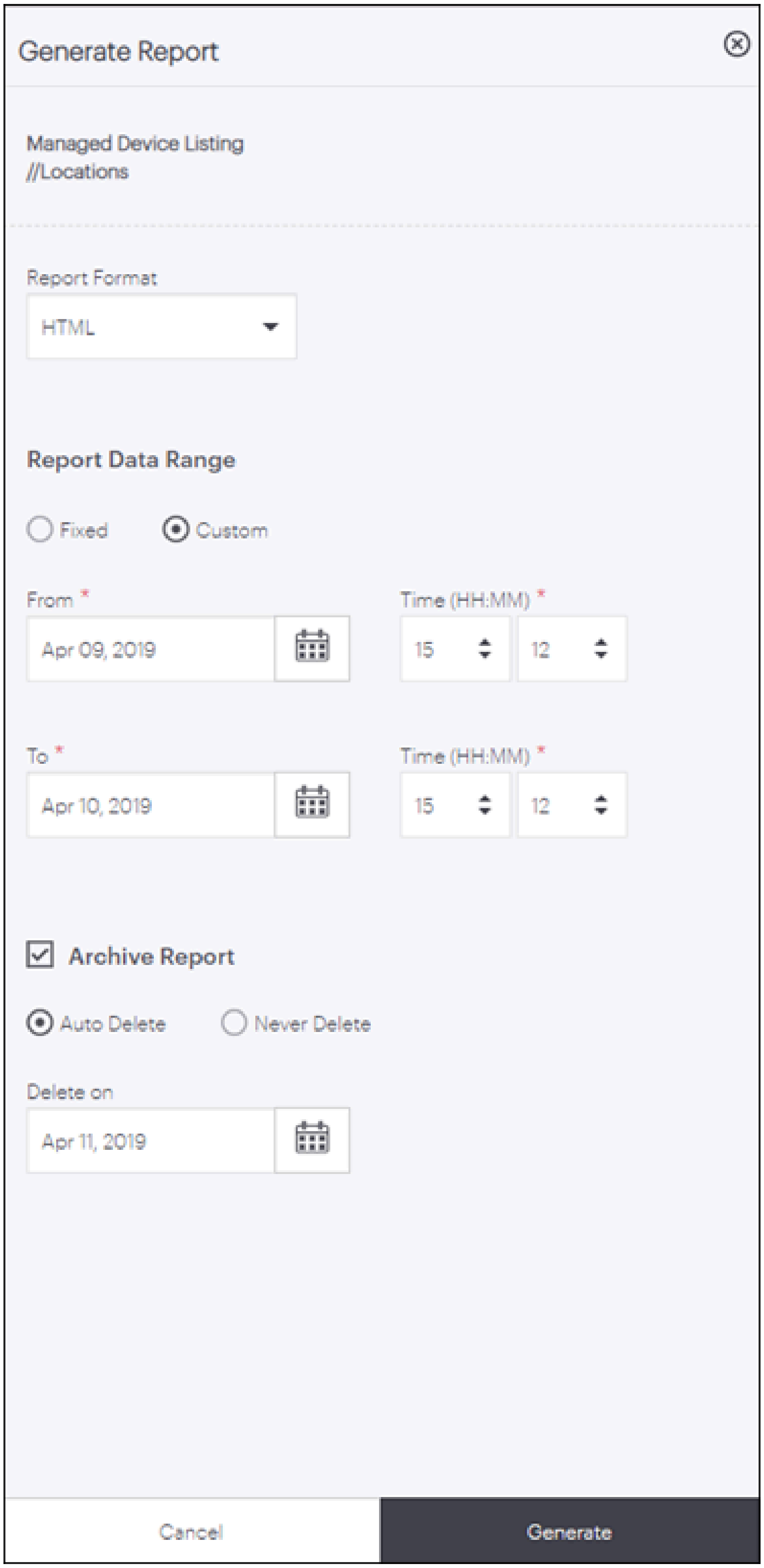


29.2 On-Demand Generation of Reports

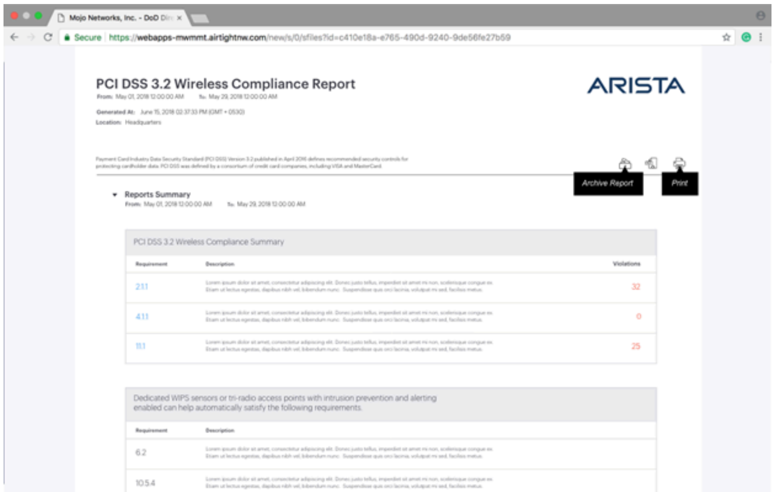
The following image shows the **Generate Report** icon:



Clicking 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



29.3 Saving a Report

Reports can be saved so that they can be viewed at a later time. When the report storage quota of a user is consumed, no more reports can be saved unless older reports are deleted. You can define the date when a saved report should be deleted or you can also disable the auto-deletion for a report.

Saved reports can be viewed under **REPORTS** > **More** > **Saved** tab in CV-CUE. Visibility of a saved report is not location-specific; it is based on a user's role. A saved report is always visible to a user who has previously generated the report. Role-based access is as follows:

- **Superusers -** can view all saved reports.
- **Administrators** - can view reports saved by them and for them.
- **Operators -** can view reports saved by them and for them.
- **Viewers -** cannot save or view a saved report.

Chapter 30

Third-Party Servers

Integration of third-party servers with CV-CUE is a system-level operation; it applies to the entire network.

This chapter contains the following topics:

30.1 Google Integration

You can integrate Google for Work with your network using CV-CUE.

To configure Google integration:

1. Go to **System** > **Third-Party Servers** > **Google Integration.**
2. Click **Upload JSON Key File**.
3. Select the JSON key file you have downloaded from Google and click **Open**.
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.

30.2 ArcSight Integration

Integration with ArcSight's Enterprise Security Management (ESM) enables CV-CUE 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). CV-CUE 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 CV-CUE to an ArcSight server.

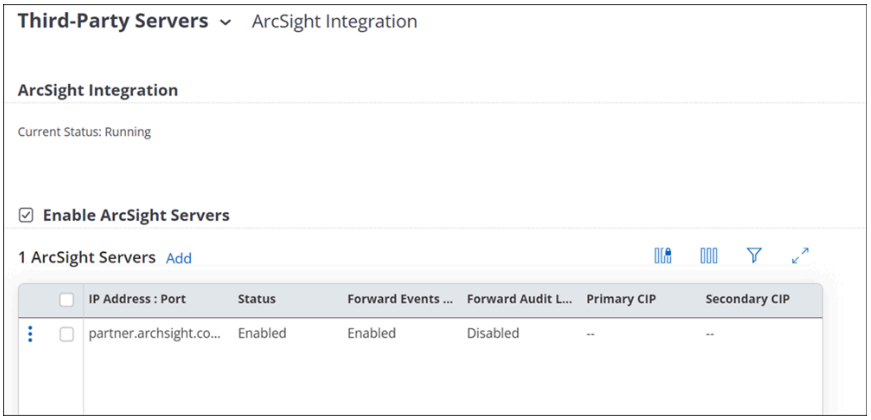
To add an ArcSight server, perform the following steps:

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 CV-CUE 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 CV-CUE 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.



You can also enable and disable individual ArcSight servers using the three-dot menu in the table.

30.3 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 CV-CUE to notify users through email, for example notification of alerts.

Note: Only on-premises CV-CUE 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 Servers** > **SMTP.**
2. Configure the following parameters:

Option	Description
SMTP Server IP Address/Hostname	IP Address or the host name of the SMTP server used by the system for sending e-mails. Default : 127.0.0.1
Port	Port number of the SMTP server. Default : 25
"From" Email Address	The source address from which e-mails are sent. Default : server@localhost.localdomain

3. Select **Enforce use of StartTLS (TLSv1)** to enforce the use of STARTTLS to send e-mails in an encrypted format.

   Info: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.
4. 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**.

   Info: If the certificate is imported successfully, the certificate file name and certificate details can be seen on the page.

   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.

5. To authenticate with the SMTP sever, select **Authentication Required**, and enter the **Username** and **Password**.
6. Click **Save**.

30.4 SNMP

You can configure CV-CUE to send information via SNMP traps to one or more SNMP servers. Depending on whether your network uses a cloud-based Arista Wi-Fi server or an on-premises one, the following information can be sent to SNMP servers:

- For a cloud-based Wi-Fi deployment, CV-CUE can send alerts to your SNMP servers.
- For an on-premises Wi-Fi server, CV-CUE can send alerts and system health metrics to your SNMP servers.

30.4.1 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.

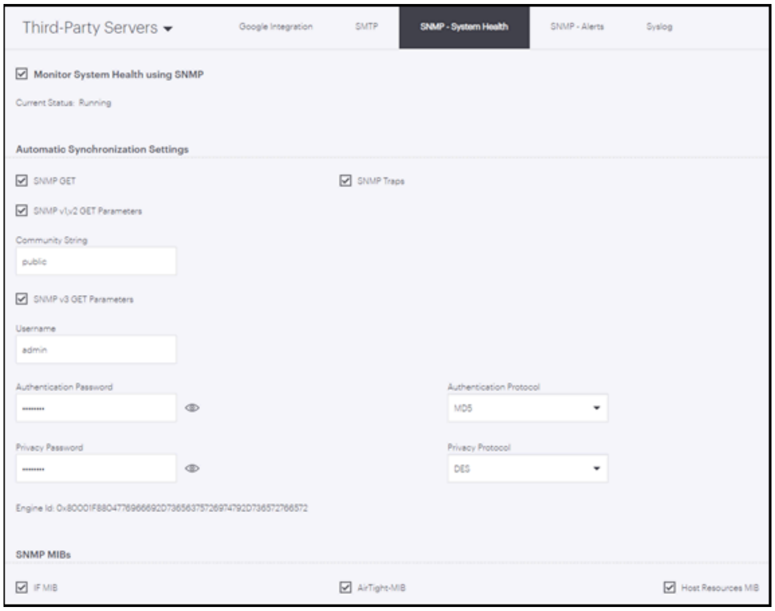
The settings are described in the table below.

Setting	Description
Enabled	Select to enable communication between CV-CUE and this SNMP server.
SNMP Trap Destination Server IP/Hostname	Enter the IP address or hostname of the SNMP server. **Note:** For a cloud-based Arista Wi-Fi deployment, if the SNMP server uses a private IP address, you need to select a Cloud Integration Point.
Port Number	The port number for the SNMP server-CV-CUE communication.
Primary Cloud Integration Point (CIP)	**Note**: This field does not appear for an on-premises Arista Wi-Fi server because it is needed only to integrate a cloud-based Wi-Fi 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.
Secondary Cloud Integration Point (CIP)	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.
SNMP Version	Select SNMP V2 or V3 for the Arista server communication with the controller.
Community String	For SNMP v2, define a custom community string to authenticate with the SNMP server. The default value is "public". Ensure that you change this community string.
Username	For SNMP V3, an auto-generated username for CV-CUE to log in to the SNMP server.
Authentication Password	The password to authenticate with the SNMP v3 server.
Authentication Protocol	The authentication protocol used for SNMP v3. The options are MD5 (default) and SHA.
Privacy Password	The private key used to encrypt SNMP v3-based traps.
Privacy Protocol	The method used to encrypt SNMP v3-based traps. The options are DES (default) and AES.

Note: Make sure that the "Send Alerts using SNMP" checkbox is enabled. Even if all the individual SNMP servers are "Enabled", CV-CUE will not send alerts unless the "Send Alerts using SNMP" checkbox is selected.

30.4.2 SNMP - Server Health

For an on-premises Arista Wi-Fi server, CV-CUE can send system health information to SNMP servers. To configure SNMP for system health, go to **SYSTEM** > **Third-Party Servers** > **SNMP-System Health** and configure the settings shown in the figure below.

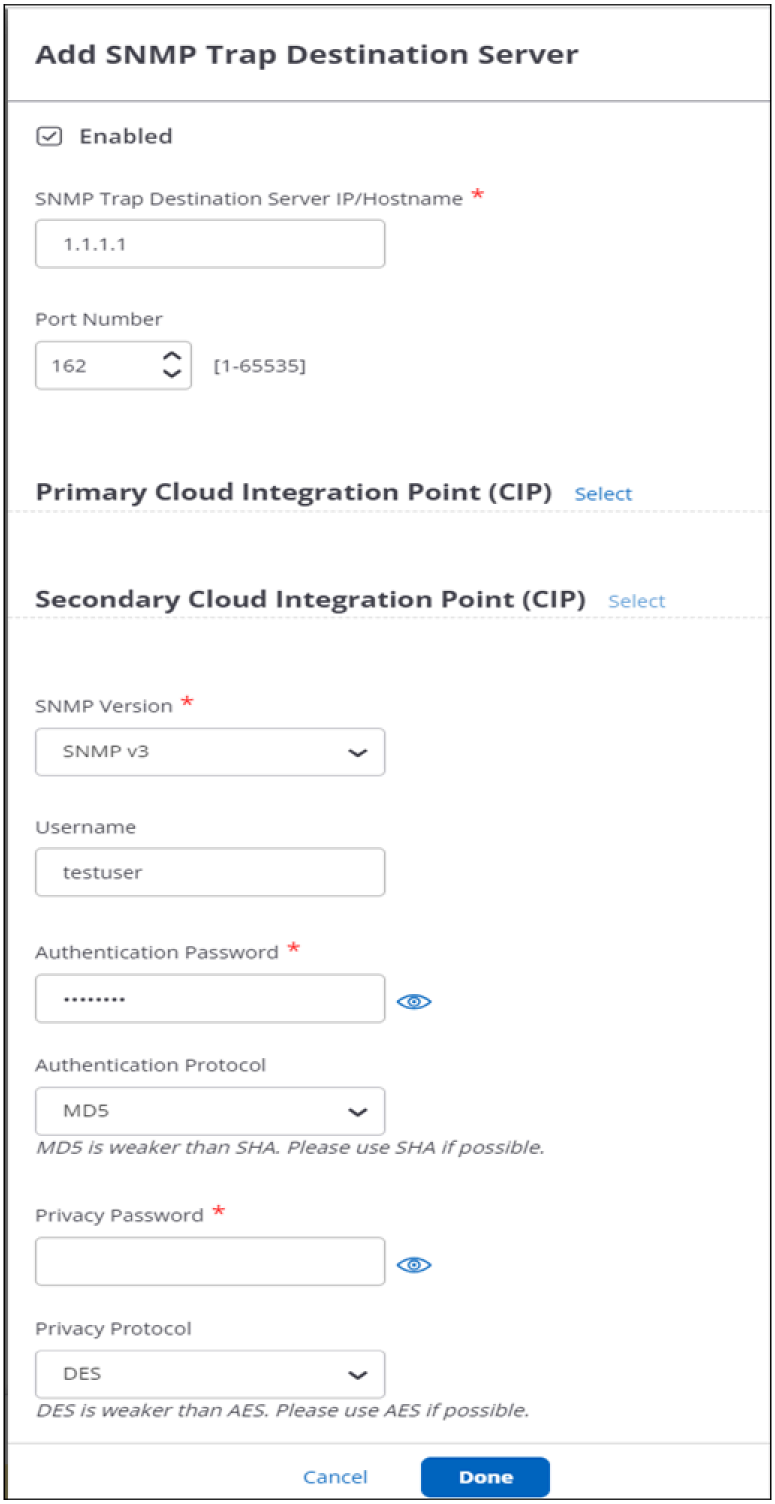


An SNMP Management Information Base (MIB) is a collection of definitions that define the properties of a managed object in a managed device. For example, the Arista Wi-Fi server is a managed device, its disk memory is a managed object, and the Host Resource MIB contains information about the disk memory of the Wi-Fi server.

The table below shows the SNMP Management Information Bases (MIBs) used for different system health metrics.

MIB	Description
IF MIB	Select to send information about network interfaces such as eth0 and eth1.
AirTight MIB	Select to send information about the Wi-Fi management specific processes running on the server.
Host Resource MIB	Select to send host resource information such as memory and CPU.
MIB-II	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.

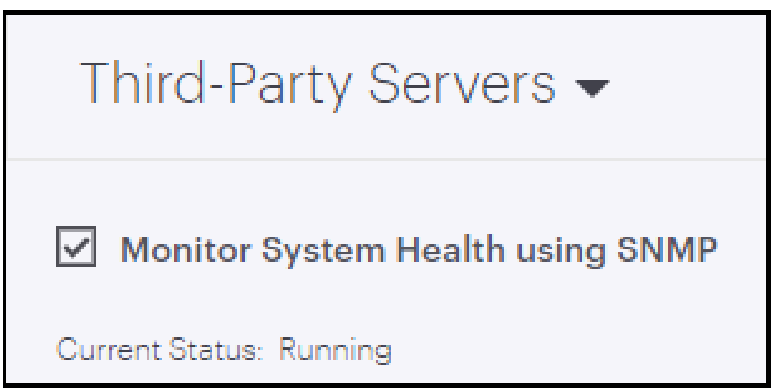
To add SNMP servers, click Add on the Destination SNMP Servers table. As shown in the figure below, the SNMP server settings panel opens up.



The settings are described in the table below.

Setting	Description
Enabled	Select to enable communication between CV-CUE and this SNMP server.
SNMP Trap Destination Server IP/Hostname	Enter the IP address or hostname of the SNMP server.
Port Number	The port number for the SNMP server-CV-CUE communication.
SNMP Version	Select one of the two options: a) SNMP V1,V2 or b) SNMP V3 for the the SNMP server-CV-CUE communication.
Username	For SNMP V3, an auto-generated username for CV-CUE to log in to the SNMP server.
Authentication Password	The password to authenticate with the SNMP v3 server.
Authentication Protocol	The authentication protocol used for SNMP v3. The options are MD5 (default) and SHA
Privacy Password	The private key used to encrypt SNMP v3-based traps.
Privacy Protocol	The method used to encrypt SNMP v3-based traps. The options are DES (default) and AES.

Note: Make sure that the "Monitor System heath using SNMP" checkbox is enabled. Even if all the individual SNMP servers are "Enabled", CV-CUE will not send system health information unless the "Monitor System heath using SNMP" checkbox is selected.



30.5 Syslog

You can configure a Syslog server from CV-CUE 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** > **Third-Party Servers** > **Syslog.**
2. The **Syslog Integration Status** indicates the status of the Syslog server. **Info:** 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 CV-CUE with Syslog server.
4. Click **Add**

5. Under**Add Syslog Servers** window, enter the following details:

Option	Description
Syslog Server IP/Hostname	Specifies the IP address or the hostname of the Syslog server.
Port Number	Specify the port number of the Syslog server to which the system sends alerts. Default : 514
Primary Cloud Integration Point (CIP)	**Note**: This field does not appear for an on-premises Arista Wi-Fi server because it is needed only to integrate a cloud-based Wi-Fi 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.
Secondary Cloud Integration Point (CIP)	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.
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.

30.6 Webhooks

Webhooks let you send alert notifications in real time to third-party applications. By configuring a webhook, you can share content and notifications with external applications such as Microsoft Teams, ServiceNow, Slack, GSpace, etc.

Configuring a webhook is a two-step process. You need to create a webhook endpoint in your external application and configure that endpoint in CV-CUE. For information on creating webhook endpoints, refer to Webhooks in CV-CUE.

To configure a webhook in CV-CUE:

1. Go to **SYSTEM > Third-Party Servers > Webhook.**
2. Select **Enable Webhook.**
3. Click **Add Endpoint.**

   Note:

   You can configure a maximum of 4 webhooks.
4. Provide the following details under the Basic tab:
   - **Name:** A unique name for the webhook.
   - **Endpoint URL:** The URL of the Webhook Endpoint.

     Note: HTTP URLs and IPv6 addresses are not supported. Ensure that you use a HTTPS URL.
   - Select the Method Type from the following:
     - POST - This is the default method for sending alerts.
     - PUT
     - GET

     - **Request Headers:** To add a request header, click Add New Row. A Request Header contains a set of inputs in the key-value pairs format. For example, Key is Content-Type and Value is application/JSON. You can add a maximum of 10 rows.
5. Provide the following details under the More Settings tab:
   - Description of the webhook.
   - Select **SSL Certificate Verification.** SSL Certificate Verification is enabled by default and Arista recommends that you keep it enabled.
   - **Response Timeout:** After the specified time if no response is received from the webhook endpoint, the current request expires, and a new request is raised for the same alert.
   - **Retry Count:** Number of times a request is retried for the alert.
   - **Fixed Query Parameters:** Query Parameters, such as token or key, to send as a part of the Webhook request. You can add up to 10 Query Parameters.
   - **Request Data Type:** Using this field, you can set the response parameters of the Webhook and set the data fields that you want to receive in Webhook messages.

     Note: GET Method supports the Form Data option only. With POST and PUT methods, you can select Form Data or Raw Body request data type.
   - Form Data: Using Form Data, you can set response parameters as key-value pairs.
   - **Raw Body:** You can customize the text message along with the fields that you want to send in webhook messages. Raw Data can be in the plain text format, JSON, or XML with the field in double curly braces[{{field_name}}].
   - **Primary Cloud Integration Point (CIP):** Select the Access Point (AP) you want to designate as the primary CIP.

     Note: Only CIP-enabled APs appear in the list. Ensure to enable CIP mode on the APs you want to use as CIPs.
   - **Secondary Cloud Integration Point (CIP):** 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. For on-prem deployments, CIP configuration is needed if you are using a firewall. CIP configuration is optional for clud deployments.
   - **Important:** You must open port number 3852 in your network from the CIP to Arista cloud.

After you have configured your webbook, you can check the **Notification Preview** from the Basic tab to verify the alert message format that would be sent to your webhook URL.

6. Click **Done.**

Note:

To send alerts using Webhooks, ensure that you select **Alert Notification Type** as **Notify** while configuring alerts.

Chapter 31

Advanced System Settings

Advanced system settings are system-level operations typically performed from the SYSTEM tab in CV-CUE. The settings apply to the entire network.

This chapter contains the following topics:

31.1 License Settings for On-Premises Users

You can apply licenses from CV-CUE 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. Got 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.

31.2 Language Settings

You can define the system language that is used by CV-CUE as a mode of communication. CV-CUE 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. Got to **SYSETM** > **Advanced Settings** > **Language.**
2. Select the system language and the SSID encoding language.
3. Save the changes.

31.3 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 not configure anything on this page. Configure the HA service using the CLI.

To see the HA status from CV-CUE, go to **System** > **Advanced Settings** > **High Availability Status.**

31.4 System Status

You can see the status of the Wi-Fi 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 Wi-Fi or WIPS or both services are enabled on the server.
- Software Version — Indicates the software version of CV-CUE
- Software Build — Indicates the software build version of CV-CUE
- Operating System
- Appliance Model
- IPv4 — Indicates the IPv4 address, if available
- IPv6 — Indicates the IPv4 address, if available

31.5 Cluster Configurations

A server cluster or a cluster is a group of Wireless Manager (WM) servers. A cluster comprises a parent WM server and one or more child WM servers. A cluster is created to manage multiple servers using a single server. This managing server is called the parent server and the servers that are managed from the parent server are called the child servers. A server can be part of only one cluster at any given time. A child server cannot be a parent of any other server in the cluster. Creating a cluster helps in managing multiple servers together. For example, you can create a policy and implement it across different servers using a cluster.

You can create clusters using the server command line console. For more information on creating clusters and managing servers in a cluster, refer to the following chapters in your respective server installation guide.

- **Setup and Manage Server Cluster** - For details on setting up server clusters
- **Server Config Shell Commands**- For details on server cluster commands.

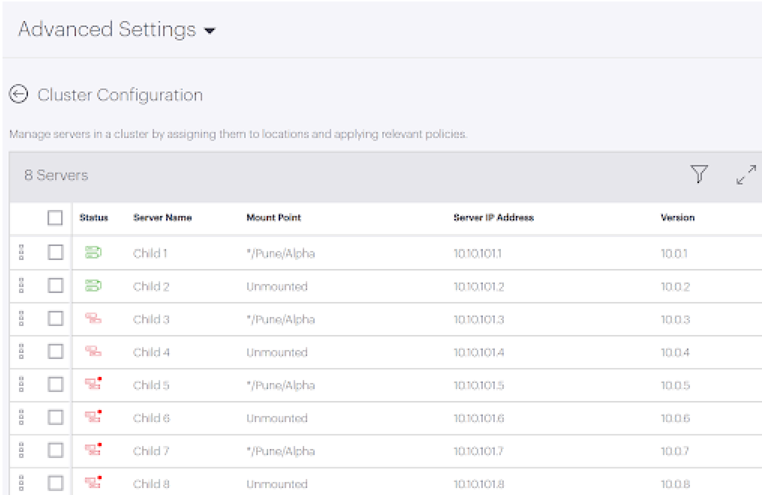
After you have assigned a parent server to a cluster and have added child servers to the server cluster, login into CV-CUE to view cluster data and manage cluster configuration.

Note: You must be a superuser to view cluster data and manage cluster configurations.

View Cluster Configurations

To view the cluster data:

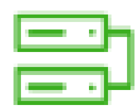
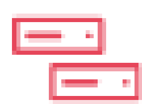
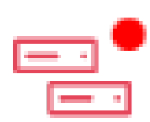
1. Go to **SYSTEM** > **Advanced Settings.**
2. Click the **Cluster Configuration** tile. All the existing servers in a cluster are displayed.



The table displays the following data:

Table 33: Cluster Configuration Details

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Status</td><td>The status of the server. The icons mean the following:

Table 34:
<table>
<tr><th>Icon</th><th>Description</th></tr>
<tr><td></td><td>Connected Server</td></tr>
<tr><td></td><td>Disconnected server</td></tr>
<tr><td></td><td>Expired license or mismatched version</td></tr>
</table>
</td></tr>
<tr><td>Server Name</td><td>Name of the server</td></tr>
<tr><td>Mount Point</td><td>Mount location of the server</td></tr>
<tr><td>Server IP Address</td><td>IP Address of the server</td></tr>
<tr><td>Version</td><td>Software Version number of the server</td></tr>
</table>

You can perform the following actions on a cluster server:

- Mount or Unmount the server
- Change mount location

- Copy Policies
- Fix version mismatch
- Fix License

Note: You can perform the actions only a connected server.

Mount or Unmount the Child Server

To view the server cluster data or to copy the parent server's policy, you need to mount the individual child servers on the parent server location tree. Before you mount the child server, ensure that you have applied a valid license to it and it has the same build version as the parent server.

To mount the child server:

1. Select the child server. Click **Mount** from the three-dot menu next to it.
2. Select the mount location and click **Save.**

The child server is mounted on the selected location.

Note: When you mount a child server, the parent server policies are not inherited by the child server automatically. The child server continues to use its existing policies. You need to explicitly apply the parent server's policy.

Similarly, you can umnount the child server from the parent server by clicking **Unmount** from the three-dot menu next to it.

Change the Mount Point of the Child Server

You can change the mount point of a child server and mount it to another location. Before you change the mount point of a server, ensure that a valid license is applied to it.

To change the mount location of the child server:

1. Select the child server. Click **Change Mount** from the three-dot menu next to it. The Change Mount Point pane appears.
2. Select the new mount point and click **Save.**

Copy Policies

Policies are configuration settings that you define for a server. If you want to keep the same configurations or settings across servers in a cluster setup, you need to create only one policy and copy the policy to all other servers. This helps in maintaining consistency in your settings, provides ease of replication, and reduces human errors. You can copy policy settings from a child server to another child server, a parent server to a child server, or a child server to a parent server. You can copy the following policies:

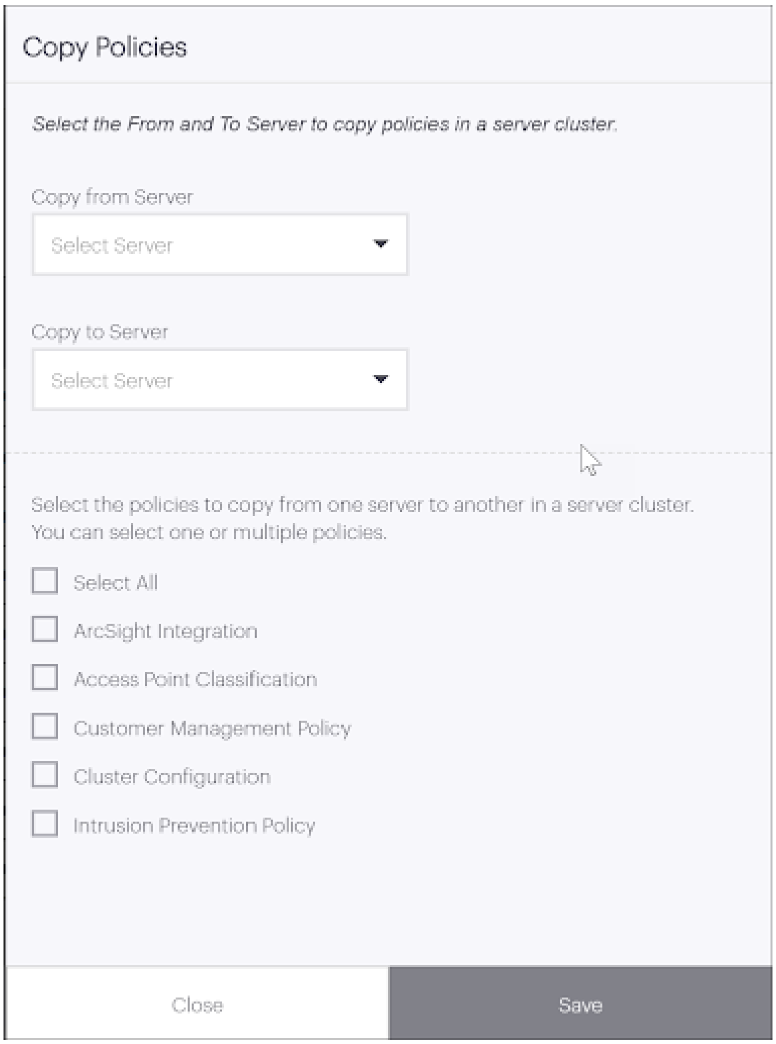
- Account Suspension
- Password Policy
- Language Setting
- Audit Logs
- Auto Deletion
- SMTP Configuration
- Radius Configuration
- Server Upgrade
- Certificate
- LDAP Configuration
- AP Server Key (Device Communication Key)
- ArcSight Integration
- Banned APs

- Banned Clients
- License
- Reports Look and Feel
- SysLog Integration
- SNMP

You can copy a single policy or copy multiple policies at once.

To copy policies in a cluster server:

1. Navigate to **SYSTEM** > **Advanced Settings.**
2. Click the **Cluster Configuration** tile. Alternatively, you can also navigate to the particular policy setting that you want to copy.
3. Click **Copy Policies.**
4. The Copy Policy pane is displayed. Select your To and From Servers.



5. Select the policies to copy.
6. Click **Save.** The **Confirm Copy Policy** dialog box appears.
7. Click **Confirm.**

Once the policy settings are copied, you will get the **Copy Policy Results** pane displaying the success or failure of the copied policies.

Fix Mismatched Version of the Child Server

The parent server and the child servers in a cluster must have the same software versions. If there is a mismatch between the versions of the parent server and the child server, you need to upgrade your child server to match the version of the parent server.

To fix the child server version:

1. Click **Fix Version Mismatch** from the three-dot menu next to it. The fix version mismatch pane opens.
2. Upgrade your child server. For more information on upgrading your server, refer to Upgrade Server.

Fix Invalid License of the Child Server

The child servers in a cluster must have a valid license. In case of a missing license or an expired license, you need to fix the license of the child server.

Note: This feature is available for on-premise setup only.

To fix the child server license:

1. Click **Fix License** from the three-dot menu next to it. The fix license pane opens.
2. Select the appropriate license file from your local storage and click **Apply License.**

31.6 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

31.7 Upgrade Server

You can check for available upgrades and upgrade your server to the latest version of CloudVision Cognitive Unified Edge (CV-CUE). Only a **Superuser** can initiate a server upgrade.

Note: This feature is available for on-premises deployments only.

Prerequisites for Upgrade

- TCP Port 8080 of the server is accessible from your computer.
- Popups are not blocked.

Upgrading your Server

Before you start, ensure that you have downloaded the upgrade bundle to your computer. Also note that you cannot abort or cancel the server upgrade process once the server upgrade is in progress. The upgrade process continues even if you close the browser window.

To upgrade your server:

1. Go to **SYSTEM** > **Advanced Settings** > **Upgrade Server.** The *Upgrade Server* screen displays the current build details.
2. Click **Check for Upgrade** to check if upgrades are available. You can download the upgrade bundle from Arista's support website.

3. (Optional) Select the **Check Server upgrade availability at each login** checkbox to check for available upgrades on every login.
4. Click **Select File** and select the upgrade bundle from your local storage.
5. Click **Check Compatibility** and verify that the upgrade bundle is compatible with the server.
6. Click **Upload and Upgrade.** The Confirm Upgrade screen displays the current build and upgrade build details.
7. Click **Confirm** to initiate the server upgrade. Once the upload is complete, the server upgrade starts automatically.
8. Refresh your browser and log in to CV-CUE after the server is upgraded.

While the server upgrade is in progress, you cannot access the CV-CUE UI. After the server upgrade is successful, the server reboots automatically. Wait for a few minutes for the server to reboot. After this, you can access the CV-CUE UI again.

Parent-Child or Multi Server Setup

If you have a Parent-Child or a Multiple Server setup and you are upgrading a child server, only the child server is inaccessible while it is upgrading. You will be redirected to the dashboard of the parent server and you can access the parent server.

If you are upgrading the parent server, wait for a few minutes for the server to reboot and log in again to access the server. While the parent server is upgrading, you can access the child server(s).

31.8 Base URLs for APIs

Since the Wireless Manager (WM) UI is deprecated, you canot access the WM directly. However, you can view the WM host URL in CV-CUE and use the URL to test APIs offered by CV-CUE or create your own applications. Similarly, if you use the Guest Manager sevices, you can also view the URL for guest analytics (Guest Manager) from CV-CUE.

To view the base URLs, navigate to **SYSTEM** > **Advanced Settings** > **Base URLs for APIs**.

The URLs for both guest analytics, and configuration and management are static links. For more information on availale APIs, see the API Help Portal. The URL for specific end point is available in the API Help Portal. The base URL is available in CV-CUE. For example, if the API endpoint is client, then the URL is *<wm_base_url>/wifi/api/clients*.

31.9 Import Devices

You can import an authorized AP List, and an authorized or unauthorized client list in CV-CUE. The Import Device feature is an efficient alternative to manual movement and classification of these devices.

You must have administrator privileges to import a device list. Import devices is a location specific feature and cannot be inherited from the parent location folder.

You can import Authorized AP List, Rogue AP List, Authorized Client List, Guest Client List, and Rogue Client List.

Follow these steps to import a device list:

1. Go to **System** > **Advanced Settings**.
2. Click the **Import Device** tile.
3. Download the CSV Template.
4. In the downloaded CSV file, delete the sample data and enter your device list by providing a comma-separated list of MAC Address, IP Address, and Device Name. Save the CSV file.
5. In the UI, select the **Device Type.**
6. Click **Select File** and select your saved file.

7. Click **Import.**

31.10 Password Policy

For on-premises deployments, you can configure the minimum requirements for a password in the **Password Policy** tab. The password settings apply to all user roles **-** Superuser, Administrator, Operator, and Viewer. If you change the password settings, older passwords are not affected. 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** > **Advanced Settings** > **Password Policy.**
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.

31.11 System Backup and Restore

You can back up the entire system or only the configuration files, and restore them when needed.

Note: This feature is available for on-premises deployments only.

System Backup

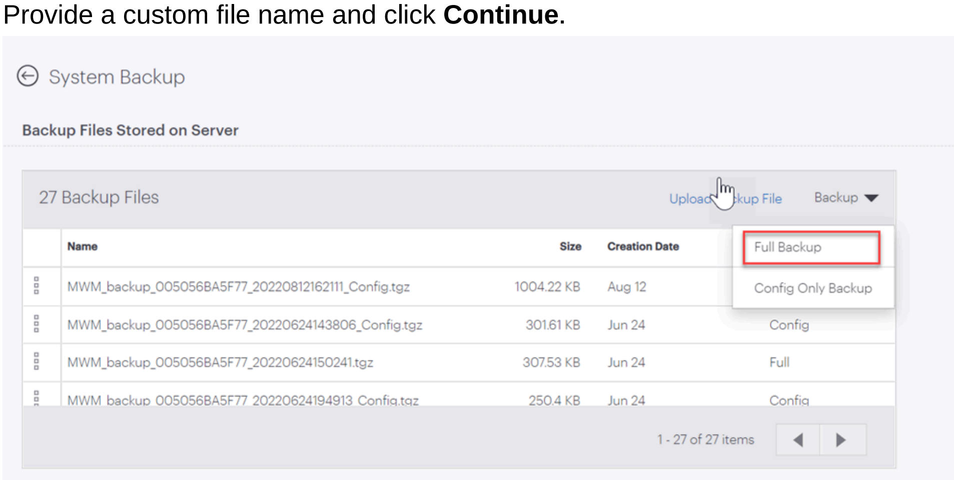
CV-CUE provides two types of backup — full backup and configuration-only backup. The full backup takes a complete backup of the configuration and data. In a configuration-only backup, data related to events, performance, analytics, etc are not backed up.

When you perform a system backup, a TGZ file and an MD5 file are generated. Backup is taken in the form of a TGZ file and the MD5 file is used to verify the data integrity.

Perform a Backup

To perform a full or config-only backup:

1. Go to **SYSTEM** > **Advanced Settings.**
2. Click the **System Backup** tile.
3. Click **Full Backup** or **Config Only Backup** from the Backup drop-down menu.
4. Provide a custom file name and click **Continue**.



After successful backup, the backup file is stored in the server and you can use it to restore your server database. You can also download the backup files to your local storage. To download a backup file, click the more-menu next to the backup file and download the backup file and MD5 file.

Note: You will be logged out of the server while the backup is in progress.

Renaming a Backup File

To rename the backup file:

1. Click the **System Backup** tile.
2. Click **Rename** from the more menu next to the backup file entry in the Backup Files table.
3. Provide the new file name and click **Ok.**

System Restore

If you have taken a backup of the Arista server database, you can restore the Arista server to a last known working state, in the case of a server failure. You can restore the database or configuration files from a list of backup files available on the server or you can upload a backup file and use it to restore the server.

Before you perform the restore, ensure that the TGZ and MD5 files are present in the same folder.

Restore Database from Available Backups

To restore the database from available backups:

1. Go to **SYSTEM** > **Advanced Settings.**
2. Click the **System Backup** tile.
3. Click the more menu next to the backup file entry in the Backup Files table.
4. Click **Restore Backup.**
5. In the pop-up, select Restore Licenses if you want to restore the licenses of the backup file as well.
6. Click **OK.**

Restore Database by Uploading a Restore Bundle

You can upload a restore bundle from an external location to restore the database on the server. The uploaded file is validated before it is used to restore the database.

To upload a restore bundle:

1. Go to **SYSTEM** > **Advanced Settings.**
2. Click the **System Backup** tile.
3. Click **Upload Backup** Files.
4. Select your .TGZ and .MD5 files and click **Save.**

Once the upload files are validated, the server will start the restore process.

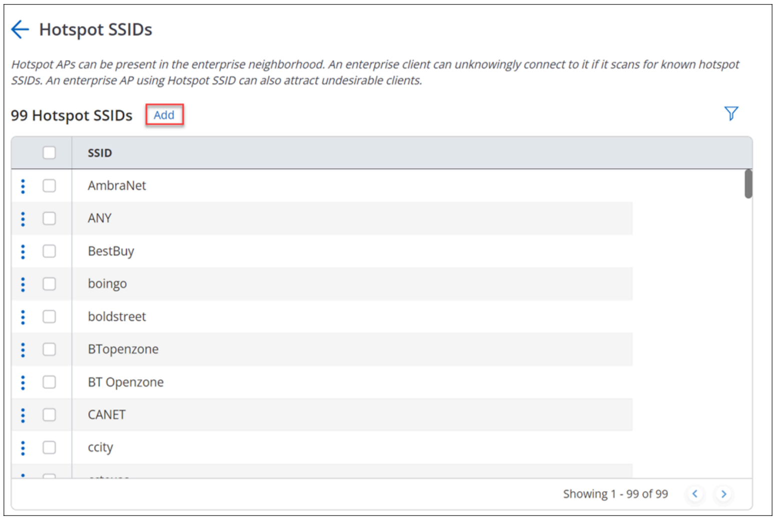
Note: You will be logged out of the server while the server restore is in progress.

31.12 Hotspot SSIDs

APs with Hotspot SSIDs can be present in the neighborhood. When an enterprise client probes for common Hotspot SSIDs, it is at risk of connecting to the neighborhood AP, without the user knowing about it. You can classify such SSIDs with a higher chance of undesirable connections as Hotspot SSIDs.

To add Hotspot SSIDs,

1. Go to **System** > **Advanced Settings.**
2. Click **Hotspot SSIDs.**



3. Click **Add.**
4. Enter your SSID name and click **Ok.**

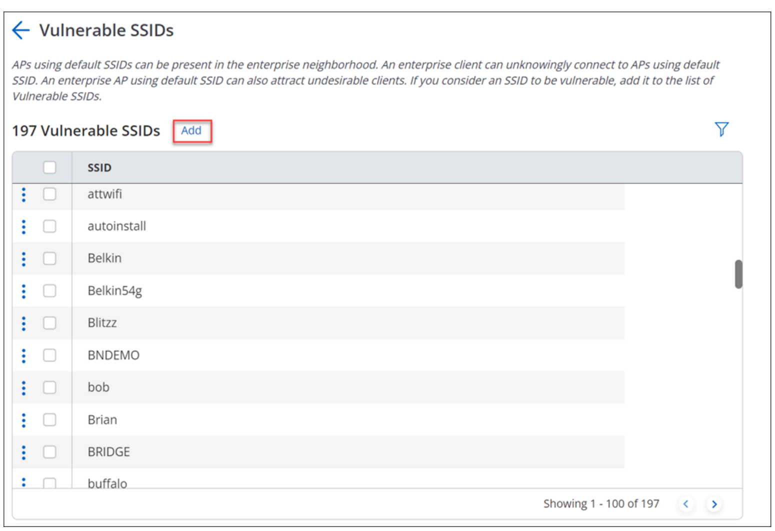
You can edit, delete, and search Hotspot SSIDs from the created list. You can also copy the list of Vulnerable SSIDs across servers present in the same cluster, by using the **Copy Policy** feature.

31.13 Vulnerable SSIDs

Access Points (APs) have default SSIDs. Many users do not change these SSIDs before deploying the APs. Therefore, it is very likely that APs using default SSIDs are present in the enterprise neighborhood. If an enterprise client probes for default SSIDs, it is at risk of connecting to the neighborhood AP, without the user knowing about it. Such SSIDs with a higher risk of undesirable connections are classified as Vulnerable SSIDs.

To add Vulnerable SSIDs,

1. Go to **System** > **Advanced Settings.**
2. Click **Vulnerable SSIDs.**



3. Click **Add.**
4. Enter your SSID name and click **Ok.**

You can edit, delete, and search Vulnerable SSIDs from the created list. You can also copy the list of Vulnerable SSIDs across servers present in the same cluster, by using the **Copy Policy** feature.

Chapter 32

Client Connectivity Test Using a Tri-radio Access Point

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. In CV-CUE, 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 Wi-Fi 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.

This chapter contains the following topics:

32.1 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 Wi-Fi 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.

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.

32.2 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.

Target AP	Tri-radio Client AP
Target APs are selected at random to avoid testing the same AP repeatedly in a recurring schedule.	At least one tri-radio AP should be able to see the target AP with good RSSI, e.g., -70dBm or greater.
The SSID and frequency band of the target AP must match those in the selected test profile.	The third radio of the tri-radio AP must not be busy in other activities such as intrusion prevention, troubleshooting, or another test.
The target AP must not be busy with another test.	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.

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.

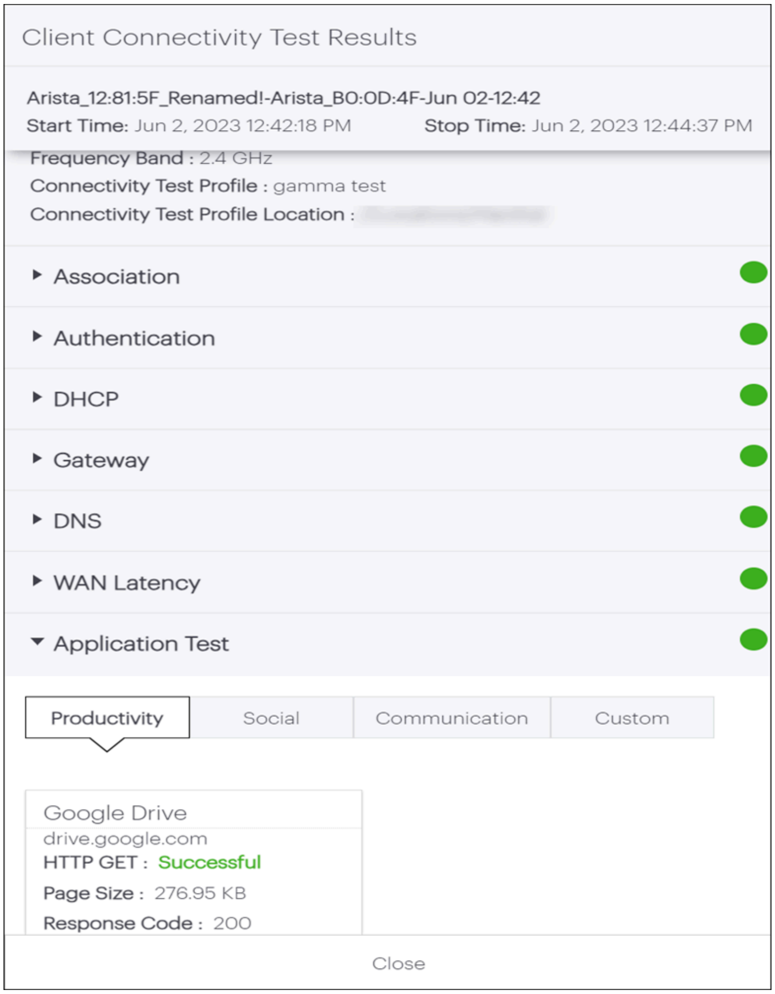
32.3 Results

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.

Field	Description

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)
	Note: 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

Field	Description

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

VoIP Test	• VoIP call status:
	  • Successful (Green)
	  • Failed (Red)

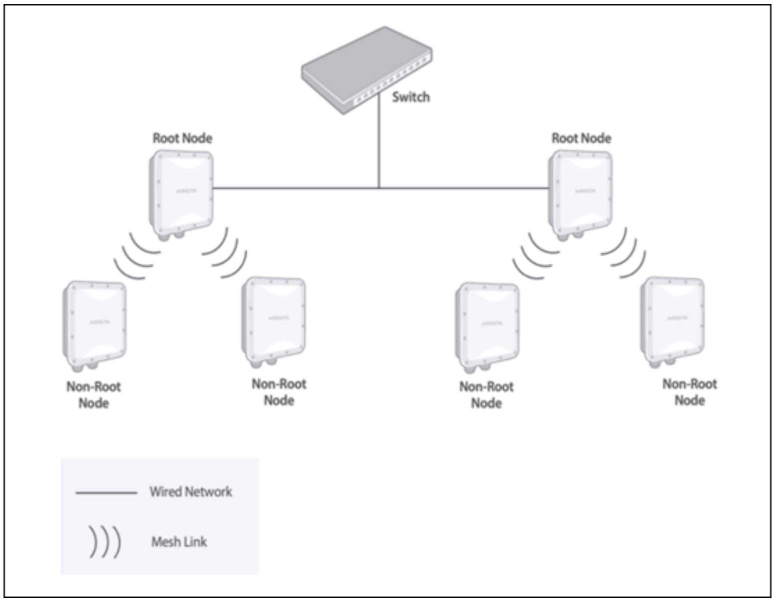
Field	Description

Throughput Test	• Internet/Wi-Fi throughput test status:
	  • Successful (Green)
	  • Failed (Red)
	• Internet Throughput Test
	• Upload and Download speeds
	• Wi-Fi Throughput Test
	  • TCP Upload and Download speeds
	  • UDP Upload and Download speeds

Chapter 33

Mesh Network

A mesh network is typically used when it is 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.

CV-CUE (CV-CUE) 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.

This chapter contains the following topics:

- Key Characteristics of Arista Mesh
- Features Affected By Mesh Mode
- Set Up Mesh Network
- Deployment and Post-Deployment

33.1 Key Characteristics of Arista Mesh

- CV-CUE 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 WMfor 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.

33.1.1 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** in the group where the mesh profile is defined and set **Background Scanning** to Off under **General** tab.
- 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** > **Device** > **Access Points.** Under **Channel Settings** in **WiFi Radios** tab, 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 is 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.

33.2 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.

33.3 Set Up Mesh Network

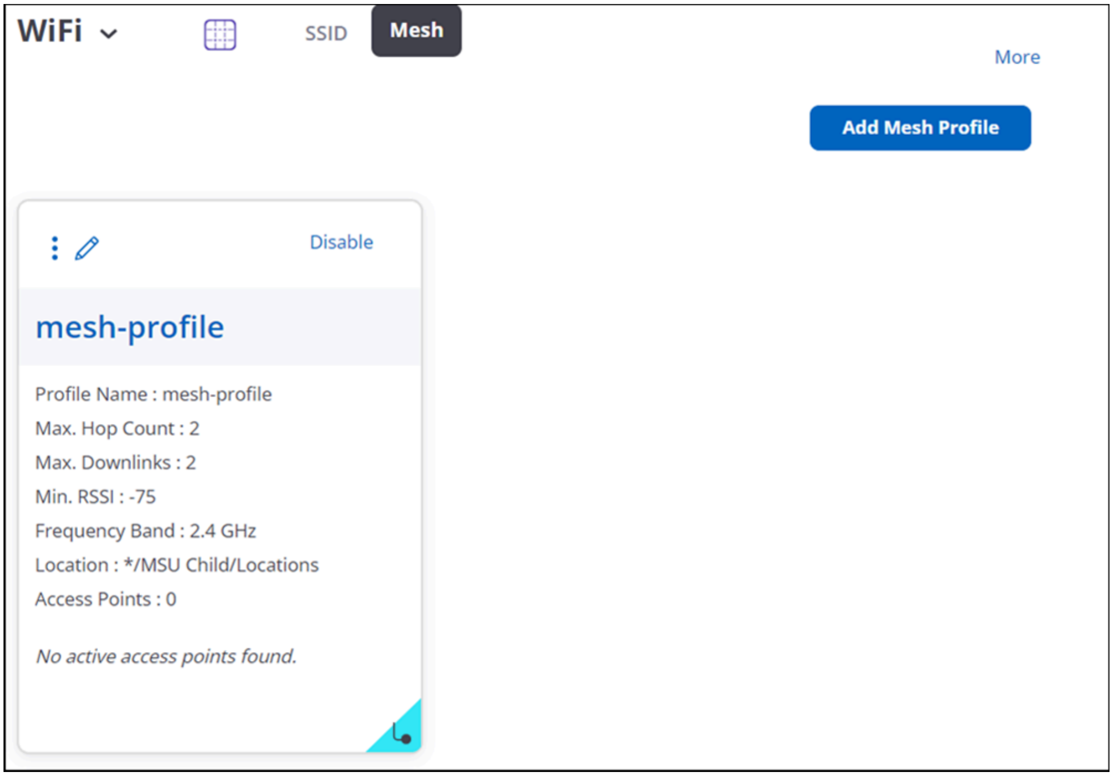
To set up a mesh network, you need to enable the mesh profile on all participating APs and define the root nodes before deploying the APs. You can then deploy them at their respective locations and connect the root nodes to the wired network.

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. **Info:**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 CV-CUE (CV-CUE) UI, go to **System** > **Navigator** > **Groups** and click on the “+” icon to create a group for the mesh network. **Note:**CV-CUE 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:

Field	Description
Mesh SSID Name	The external name for the mesh link that APs use when setting up mesh links.
Mesh Profile Name	Internal to the system. It is used to identify a mesh profile.
Max Hop Counts	The maximum number of wireless hops between a non-root AP and its root node. **Note**: The maximum allowed value is 8.
Max Downlink	The maximum number of APs downlink of an AP, i.e., the maximum number of “child” APs an AP can have. **Note**: The maximum allowed value is 5.
Min RSSI	The minimum RSSI required for APs to form mesh links with each other.

7. Save the mesh profile.
8. Go back to **CONFIGURE** > **WiFi** > **Mesh. 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.

33.4 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 Wi-Fi clients to use) to the mesh group so that they get pushed to all the APs in the mesh.

Chapter 34

User Accounts

For on-premises deployments, you can manage users from CV-CUE. 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 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.

This chapter contains the following topics:

34.1 User Roles and their Privileges

CV-CUE supports four types of users — Superuser, Administrator, Operator and Viewer. You must have the Superuser privileges to manage users in CV-CUE.

The following table details the role-wise privileges in CV-CUE.

Privileges	Superuser	Administrator	Operator	Viewer
User Account Management				
Set or modify identification and authentication option (Local, RADIUS, LDAP, and Certificate)	Yes	No	No	No
Add and delete users	Yes	No	No	No
View and modify properties of any users (in Users tab)	Yes	No	No	No
Define password strength, account locking policy, maximum concurrent sessions for all user.	Yes	No	No	No
View and modify preferences in Manage Account (email, password, language preferences, and time zone)	Yes	Yes	Yes	Yes
User actions audit				
Download user actions audit log	Yes	No	No	No
Modify user actions audit lifetime	Yes	No	No	No
System and operation settings				
Modify system settings and operating policies	Yes	Yes	No	No

Privileges	Superuser	Administrator	Operator	Viewer
Events, devices, and locations				
View generated events	Yes	Yes	Yes	Yes
Modify and delete generated events	Yes	Yes	Yes	No
View devices	Yes	Yes	Yes	Yes
Add, delete, and modify devices (APs, Clients, Sensors)	Yes	Yes	Yes	No
View locations	Yes	Yes	Yes	Yes
Add, delete, and modify locations	Yes	Yes	Yes	No
Calibrate location tracking	Yes	Yes	Yes	No
Reports				
Add, delete, modify — Shared Report	Yes	Yes (only self created)	Yes (only self created)	No
Generate — Shared Report	Yes	Yes	Yes	Yes
Schedule — Shared Report	Yes	Yes	Yes	No
Add, delete, modify, generate, schedule — My Report	Yes (only self created)	Yes (only self created)	Yes (only self created)	No

34.2 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.

Field	Description
User Type	Specifies the type of user. You can define a local, LDAP, or RADIUS user.
Login ID	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.
First Name	Specifies the first name of the user. Not applicable for LDAP users.
Last Name	Specifies the last name of the user. Not applicable for LDAP users.
Email	Specifies the e-mail id of the user. Not applicable for LDAP users.
Language Preference	Specifies the language in which the user wants to view the UI text. The default value is English.
Time Zone	Specifies the time zone in which the user operates.
Authorization	
Role	Specifies the role assigned to the user. Choose from Viewer, Operator, Administrator and Super User. For more information on what individual roles
Allowed Locations	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.
Wi-Fi Access Management	Enables users to access the Wi-Fi management settings and functions on CV-CUE. Depending on the role, users have restricted access to the Wi-Fi management operations.
WIPS Management	Enables users to access the WIPS management settings and functions on CV-CUE. Depending on the role, users have restricted access to the WIPS management operations.
Password (Not applicable for LDAP and RADIUS users)	
Set Password	Specifies the password for the user.
Confirm Password	Repeat the password for confirmation.
Force user to change password	Specifies that the user must change the password after the first login.

Field	Description
Password Expiry — Never Expires	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.
Password Expiry — Expires	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 do not change the password when intimated, they will be locked out of the application and the Superuser needs to reset their password.
Password Expiry — Expires After	Specifies the duration in days from the time of change of the password after which the password expires.
Password Expiry — Warn Before	Specifies the time in days before the password expiry to prompt the user to change the password.
Session Timeout	
Session Timeout	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 do not 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.
Additional User Fields (Not applicable for LDAP and RADIUS users)	
Additional User Fields	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.

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 have not 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.

34.3 LDAP Server-based Authentication

For on-premises deployments, you can configure your LDAP server and map it to CV-CUE to authenticate CV-CUE users. After you have configured the LDAP server, users or groups defined in the LDAP server can log in to CV-CUE. Based on the authentication and user role defined in CV-CUE, users get restricted access to Wi-Fi, WIPS, or both configuration pages.

You can configure the following attributes in LDAP:

- Connection Details: Connects CV-CUE 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

Field	Description
Primary Server IP Address/Hostname	The IP address or hostname of the primary LDAP server.
(Primary Server) Port	The port number of the primary LDAP server. The default port is 389.
Backup Server IP Address/Hostname	The IP address or hostname of the backup LDAP server.
(Backup Server) Port	The port number of the backup LDAP server.
Enforce Use of SSL/TLS	Enable this option to ensure only the SSL/TLS connection to the LDAP server is allowed. If you do not select this option, even Open connection to the LDAP server is allowed, besides SSL/TLS.
Verify LDAP Server's Certificate	Enable this option to ensure that the CV-CUE user cannot connect to the LDAP server unless the certificate check passes. When this option is not selected, the CV-CUE user can connect to the LDAP server without verifying the LDAP server certificate.

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.

Field	Description
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 (Distinguish 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: (|(memberOf=CN= Admins,DC=ITShop,DC=Com)OR (memberOf=CN= Reviewer,DC=ITShop,DC=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: (&(memberOf=CN=Admins, DC=ITShop,DC=Com) AND (memberOf=CN= Reviewer,DC=ITShop,DC=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

Field	Description
Admin User DN	Specifies the DN of the administrator user that is used for authentication in the LDAP server.
Password	Specifies the password for the administrator user.
Append Base DN	Indicates that when selected the base DN specified in the LDAP Configuration Details section is appended to the Admin User DN.

Privileges for LDAP Users

Feild	Description
User Role Attribute	Specifies the user role attribute string that the system uses to identify a user's role, as defined in the LDAP schema.
User Role	Specifies the default role for the new LDAP users. You can select one of the following four options — Superuser, Administrator, Operator, and Viewer.
User Location Attribute	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.
Locations	The location to which a new LDAP user has access rights. You can select another location by clicking Change.

34.4 RADIUS-based Authentication

For on-premises deployments, you can use a RADIUS server to facilitate user authentication to access CV-CUE. 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 CV-CUE using the command line. Click **UI** if you want the users to access CV-CUE 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 CV-CUE. 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 do not 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 do not select the check box, the realm or domain is used as a postfix notation.
7. Save the changes.

34.5 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.

34.6 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 CV-CUE — 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 35

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.

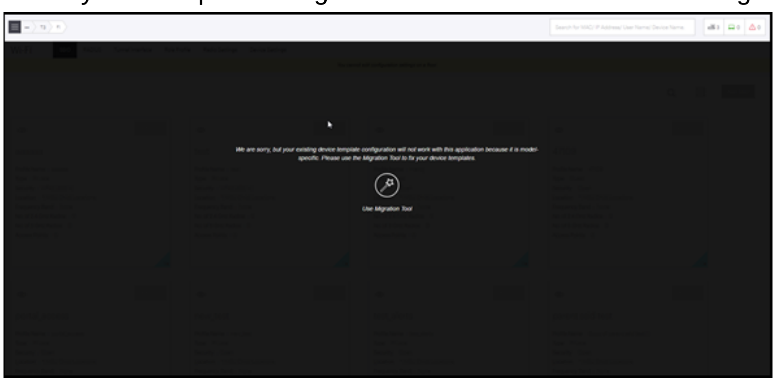
With phase-2 of the Migration tool, you will be able to migrate all device templates with model-specific configurations to universal configurations. You will see a link to launch the migration tool on folders that have device templates that need migration . The migration link helps to migrate the device 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.

This chapter contains the following topics:

35.1 How to Launch the Migration Tool

There are two ways you can launch the tool:

- When you attempt to configure a folder in CV-CUE that is using an outdated template.

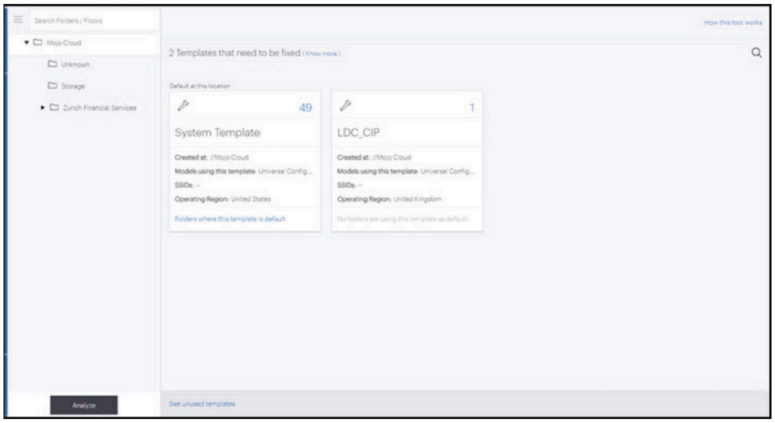


- Via the tool tip of the "bird" icon for folders that have outdated templates.

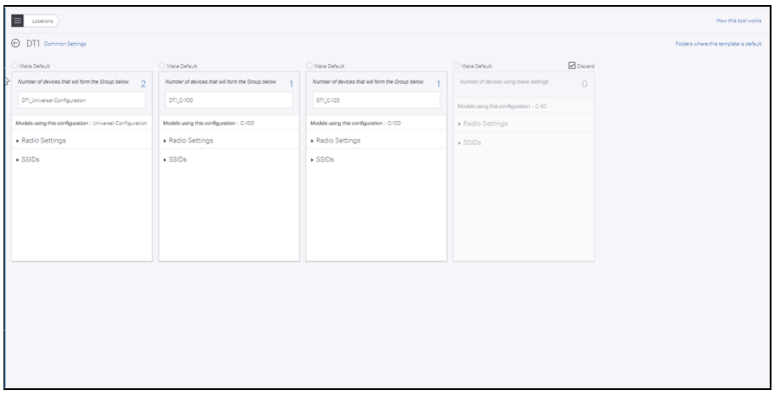
35.2 Steps to use Migration Tool

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 CV-CUE.
- 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.

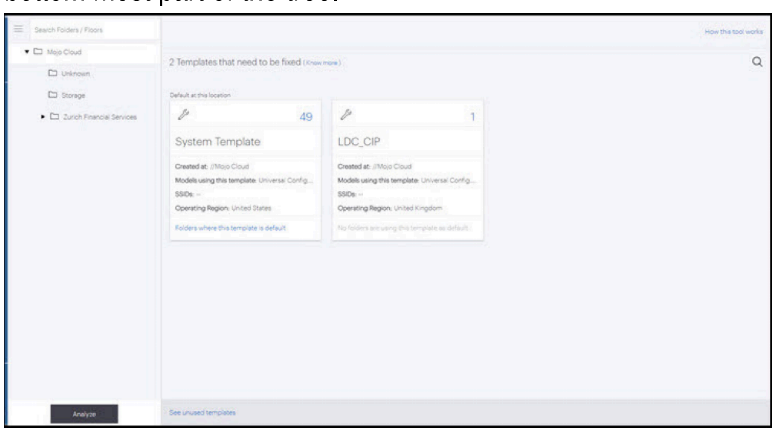
Click "Preview" to see the effect of your choices - i.e. to see which devices form groups and which ones continue to use the configuration you have chosen as Default.Click 'Fix This Template' to confirm.

35.3 How to Analyze Location Tree

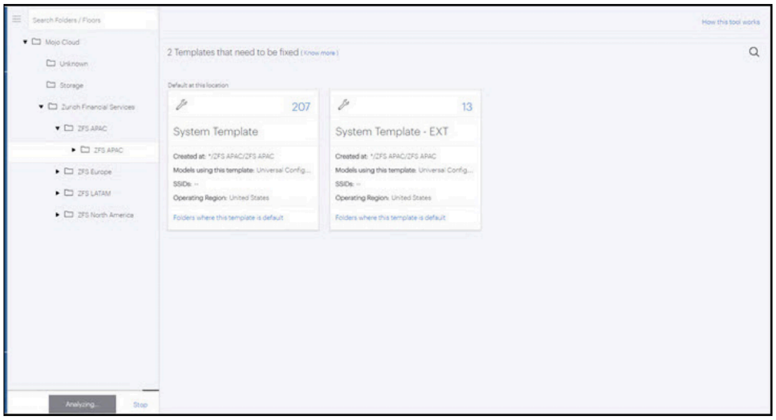
The migration of device templates can be done effectively by analyzing the entire location tree.

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.

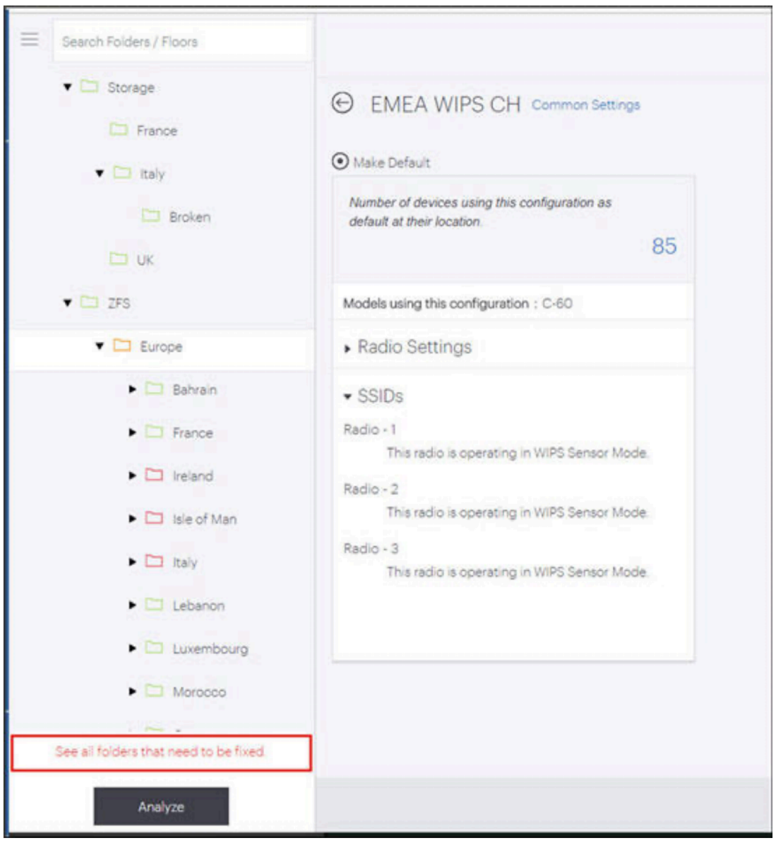
1. Click the Auto Migrate option. The location tree will be displayed. You can see the Analyze button at the bottom most part of the tree.



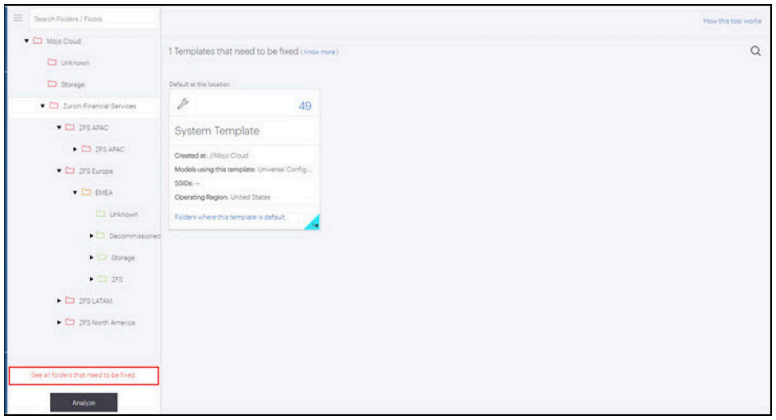
Once you click on Analyze, it starts analyzing the folders. During the analysis, you will not be able to perform any other operations on the Migration Tool.



2. Once the Analysis is completed, you can see red, orange, or green folders depending on their status.
   - Red - If the folder is colored Red, it means that none of the device templates under that folder has been fixed.
   - Orange - If the folder is colored orange, it means that some templates have been fixed, while others still need to be fixed.
   - 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.



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.


Search Folders / Floors
Mojo Cloud
Unknown
Storage
Zurich Financial Services
ZFS APAC
ZFS APAC
ZFS Europe
EMEA
Unknown
Decommissioned
Storage
ZFS
ZFS LATAM
ZFS North America
See all folders that need to be fixed
Analyze
How this tool works
1 Templates that need to be fixed (Know more)
Default at this location
49
System Template
Created at: //Mojo Cloud
Models using this template: Universal Config...
SSIDs: --
Operating Region: United States
Folders where this template is default

Chapter 36

Appendix A: AP Server Communication Workflow

With the 18.0 release, the Access Point (AP) and CV-CUE Server (previously called Wireless Manager Server or WM Server) connectivity for on-premises and cloud deployments have been updated with additional security and improved security posture of AP-Server communication.

For cloud deployments, APs connect to the CV-CUE Server via a redirector proxy server hosted in Arista Cloud. Establishing connections via a proxy server ensures additional security, eliminates direct access to the CV-CUE Server, and uplifts the security posture of AP-Server communication.

In the new communication workflow, the CV-CUE Server will generate a random communication key for new customers, and only authenticated and authorized APs can connect to it. In such cases, Administrators must enable the onboarding window from the CV-CUE UI for APs to connect to the CV-CUE Server. The details are described later in this article.

Important! Before 18.0 release, Access Points deployed in the customer's network communicated to Arista Redirector via port 443/TCP or port 3851/UDP. The Arista Redirector provided the Access Point with the URL of the CV-CUE Server, and the AP directly communicated with the Wireless Manager hosted in the cloud through port 3851/UDP.

From 18.0 release onwards, all APs must communicate with the CV-CUE Server through the Arista Redirector Proxy (which shares the same URL/domain name as the Arista Redirector) for better monitoring, scalability, and security. As part of this change, the range of IP addresses hosting the Arista Redirector has also been extended. Traffic from the Access Point must now be allowed to all the IP addresses or FQDN of the Arista Redirector on ports 443/TCP and 3851/UDP. Trusted Platform Module (TPM) APs will connect with the CV-CUE Server in Arista Cloud exclusively using 443/TCP instead of 3851/UDP.

Note the following scenarios and make the necessary changes to the firewall rules:

- If you have allowed communication from the AP to the individual IP addresses of Arista Redirector and Arista Wireless Manager over port 443/TCP, you must modify the firewall rule also to allow communication from the Access Point to the new IP addresses listed later in this article (in addition to the existing IP addresses) on port 443/TCP.
- If you have allowed communication from the AP to the FQDN of the Arista Redirector (redirector.online.spectraguard.net) over port 443/TCP, no action is required (as long as your firewall can automatically allow all the IP addresses that can resolve to the FQDN)
- If you have allowed communication from the AP to all the individual IP addresses of Arista Redirector and Arista Wireless Manager only on port 3851/UDP, you must modify the firewall rule also to allow communication from the Access Point to the new IP addresses listed later in this article (in addition to the existing IP addresses) on ports 443/TCP and 3851/UDP.
- If you have allowed communication from AP to the FQDN of Arista Cloud Redirector (redirector.online.spectraguard.net) only on port 3851/UDP, you must modify the firewall rule also to allow communication from Access Point to the FQDN of Arista Cloud Redirector (redirector.online.spectraguard.net) on port 443/TCP.
- Clarification: Only the Inside-to-Outside traffic from Access Points to Arista Redirector (IP address / FQDN) on ports 443/TCP and 3851/UDP needs to be allowed.
- Other services related to Arista Wi-Fi, such as CIP (cloud Integration Point) and image repository, will continue to operate on their current prescribed ports.
- These changes will improve the security posture of Arista APs and Cloud Communication, and move towards using TLS-based encryption as the primary method for authentication and communication with the Cloud.

The following list provides the IP addresses/URLs of the Redirector that you must enable for the AP-Server communication workflow to work:

URL: redirector.online.spectraguard.net

New IP Addresses:

- 35.209.220.35
- 35.208.54.203
- 35.208.115.139
- 35.206.94.152
- 35.208.235.177
- 35.209.160.80
- 35.208.144.161
- 35.208.5.204
- 35.207.108.103
- 35.207.79.102
- 35.214.29.19
- 35.214.13.105
- 35.213.241.166
- 35.213.201.253
- 35.207.206.240
- 35.207.229.20
- 35.213.96.138
- 35.213.55.222

Existing IP Addresses:

- 52.199.251.150
- 13.113.247.134
- 35.154.33.182
- 15.206.10.168
- 3.106.40.11
- 52.64.207.242
- 52.58.63.144
- 52.29.194.192
- 52.56.61.130
- 3.11.192.175
- 52.200.63.237
- 34.194.204.153
- 52.203.51.183
- 3.228.242.60
- 52.8.155.239
- 13.52.28.201

This chapter contains the following topics:

- Server Discovery by TPM Vs. Non-TPM AP
- Ensure Seamless ZTP for APs
- AP Server Communication Scenarios
- Change the Default AP-Server Communication Key
- Enable the AP-Server Communication Key Timers for the Onboarding Window

36.1 Server Discovery by TPM Vs. Non-TPM AP

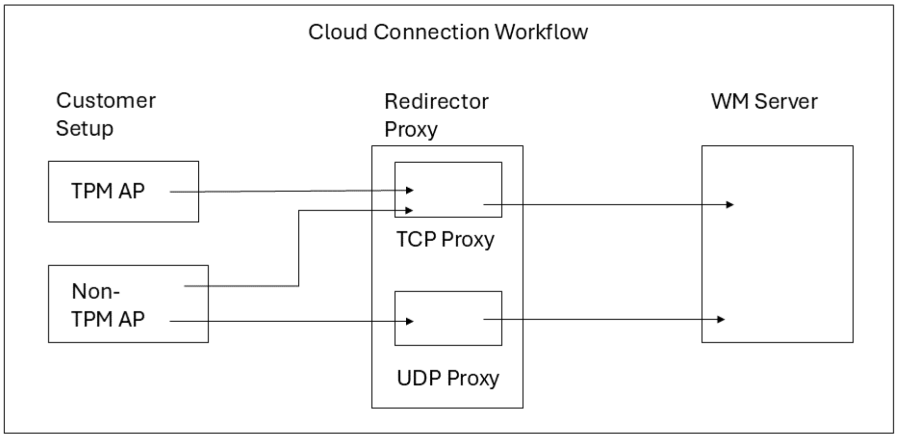
Arista has TPM (Trusted Platform Module) and non-TPM APs.

- **TPM APs:** C-200, C-230, C-230E, C-330, C-360, C-460, C-460E, W-318, O-235, O-235E
- N**on-TPM APs:** C-250, C-260, Wave 2 APs (1xx series of APs)

Depending on TPM or non-TPM APs, the process of server discovery differs.

Cloud Deployments

In cloud deployments, the TPM and non-TPM APs have different criteria to maintain the AP-Server communication.



TPM AP-Server Communication Workflow:

All TPM APs are mandated to connect to the CV-CUE Server via a TCP Proxy.

AP certificate (pre-loaded) is mandatory for authenticating and onboarding TPM APs.

TPM APs must be on Version 11.0 or higher.

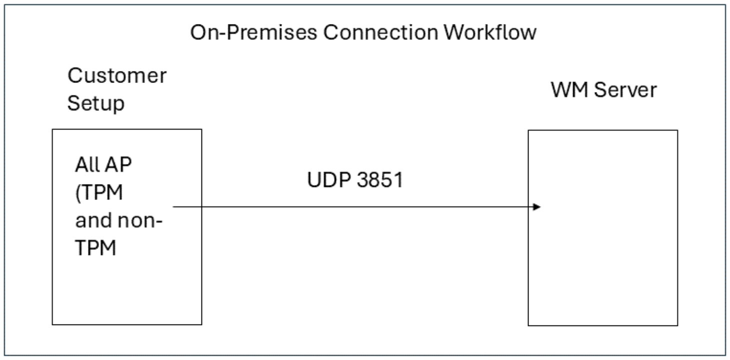
Non-TPM AP-Server Communication Workflow:

Non-TPM APs connect to the CV-CUE Server via a proxy server. They connect to the proxy using UDP 3851; if UDP is unreachable, they connect using TCP 443.

Administrators must enable the Non-TPM AP onboarding window from CloudVision CUE (CV-CUE) when the APs connect to the CV-CUE Server for the first time.

On-Premises Deployments

For on-premises deployments, the criteria for the communication workflow between TPM and non-TPM APs are the same.



APs connect to the CV-CUE Server over UDP on port 3851.

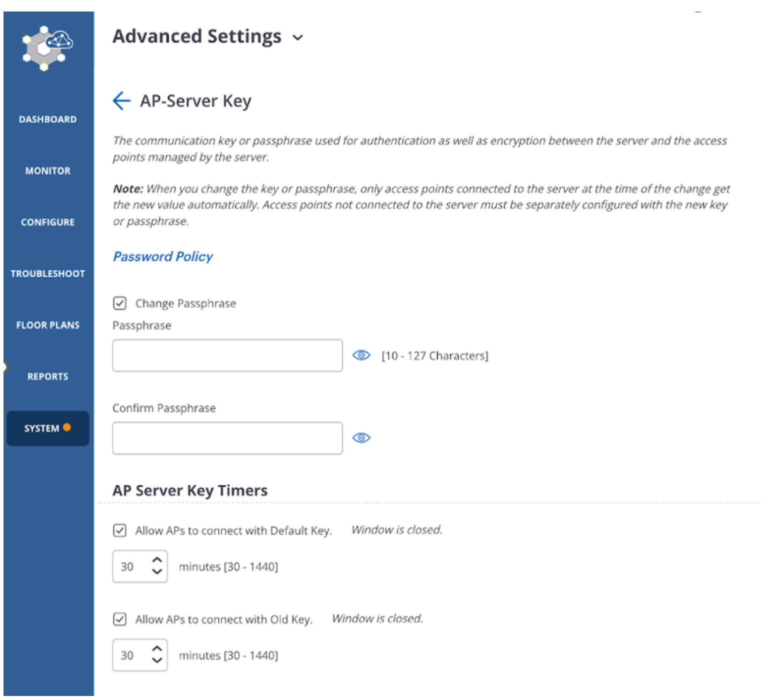
Administrators must enable the onboarding window from the CV-CUE UI when the APs connect to the CV-CUE Server for the first time.

36.2 Ensure Seamless ZTP for APs

To ensure that all existing and new APs connect seamlessly and maintain Zero Touch Provisioning (ZTP), the CV-CUE Server maintains three communication keys.

Three AP-Server communication keys:

- **Communication Key:** This is the current communication key for the AP and CV-CUE Server communication. The Administrator configures it from CV-CUE.
- **Default Communication Key:** The default communication key is flashed on every AP during manufacturing.
- **Old Communication Key:** The previous communication key that was used before the Administrator changed it to the current communication key.



Note that there is no option to restore the Default communication key.

36.3 AP Server Communication Scenarios

Consider these scenarios for AP-Server communication workflow when upgrading to the latest release.

Cloud Deployments

As a prerequisite for the Cloud-based deployment scenarios, ensure that you have made all the firewall changes mentioned in the Introduction section.

Scenario 1: Customers Upgrade the Version But Don't Change the Communication Key

Customers have AP version 11.0 or higher, and Arista upgraded the CV-CUE Server to version 18.0. Customers do not change the AP-Server communication key after the upgrade. This upgrade is like any other upgrade, with no network disruptions.

However, we highly recommend that customers change the communication key after the upgrade.

Scenario 2: Customers Upgrade the Version and Change the Communication Key

Customers have AP version 11.0 or higher, and Arista upgraded the CV-CUE Server to version 18.0. After the upgrade, customers change the communication key.

All connected APs (TPM and non-TPM) can connect seamlessly after upgrading the CV-CUE Server to Version 18.0 and changing the communication key. The CV-CUE Server pushes the new communication key automatically to the connected APs. There will not be any disruption in the AP-Server communication. For APs that were not connected or inactive when the communication key was being pushed from the CV-CUE Server:

- TPM APs will be able to connect automatically with the old communication key and get the new communication key from the CV-CUE Server for future connections.
- For non-TPM APs, Administrators must enable the onboarding window from CV-CUE. Afterward, the non-TPM APs can connect to the CV-CUE Server seamlessly within the time specified in the onboarding window. Enabling the onboarding window from CV-CUE is a one-time activity for the non-TMP APs. After they are connected to the CV-CUE Server, the Server automatically pushes the new key to such APs.

Scenario 3: Customers Upgrade the Version and Change the Communication Key. Then they Purchase New Arista APs.

Customers have AP version 11.0 or higher, and Arista upgraded the CV-CUE Server to version 18.0. After the upgrade, customers change the communication key. Then, they purchase some more new Arista APs.

This scenario is the same as Scenario 2 for existing APs. For the newly purchased APs, TPM APs will connect seamlessly with the CV-CUE Server.

For non-TPM APs, Administrators must enable the onboarding window from CV-CUE. Afterward, the non-TPM APs can connect to the CV-CUE Server seamlessly within the time specified in the onboarding window. Enabling the onboarding window from CV-CUE is a one-time activity for the non-TMP APs. After they are connected to the CV-CUE Server, the Server automatically pushes the new key to such APs.

Scenario 4: New Customers Purchase Arista APs.

New customers associate with Arista and purchase APs.

TPM APs will connect seamlessly with the server. For non-TPM APs, Administrators must enable the onboarding window from CV-CUE. Afterward, the non-TPM APs can connect to the CV-CUE Server seamlessly within the time specified in the onboarding window. Enabling the onboarding window from CV-CUE is a one-time activity for the non-TMP APs. After they are connected to the CV-CUE Server, the server automatically pushes the new key to such APs.

On-Premises Deployments

Scenario 1: Customers Upgrade the Version But Don't Change the Communication Key

Customers upgrade the CV-CUE Server to version 18.0 and do not change the AP-Server communication key after the upgrade. This upgrade is like any other upgrade, with no network disruptions.

However, we highly recommend that customers change the communication key after the upgrade.

Scenario 2: Customers Upgrade the Version and Change the Communication Key

Customers have AP version 11.0 or higher, and they upgraded the CV-CUE Server to version 18.0. After the upgrade, they change the communication key.

The CV-CUE Server pushes the new communication key automatically to the connected APs. There will not be any disruption in the AP-Server communication. For APs that were not connected or inactive when the communication key was being pushed from the CV-CUE Server, Administrators must enable the onboarding window from CV-CUE. Afterward, the APs can connect to the CV-CUE Server seamlessly within the time specified in the onboarding window. Enabling the onboarding window from CV-CUE is a one-time activity for the existing APs. After they are connected to the CV-CUE Server, the Server automatically pushes the new key to such APs.

Scenario 3: Customers Upgrade the Version and Change the Communication Key. Then they Purchase New Arista APs.

Customers have AP version 11.0 or higher, and they upgraded the server to version 18.0. After the upgrade, they change the communication key. Then, they purchase some more new Arista APs.

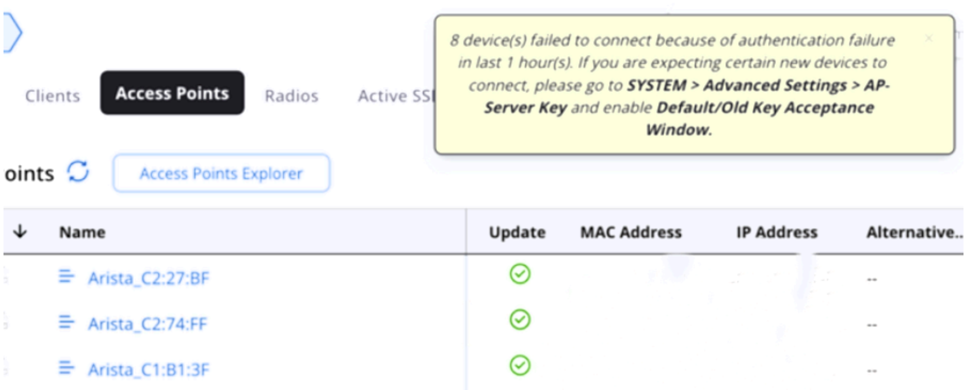
This scenario is the same as Scenario 2 for existing APs. For newly purchased APs, Administrators must again enable the onboarding window from CV-CUE so the APs can connect to the CV-CUE Server.

Scenario 4: New Customers Purchase Arista APs.

When new customers associate with Arista and purchase APs, Administrators must enable the onboarding window from CV-CUE. Afterward, the APs can connect to the CV-CUE Server seamlessly within the time specified in the onboarding window. Enabling the onboarding window from CV-CUE is a one-time activity for the APs. After they are connected to the CV-CUE Server, the Server automatically pushes the new key to such APs.

How Will Users Know if APs Fail to Connect Due to Incorrect Key

When APs fail to connect to the server due to an invalid key, a notification message appears on the AP listing page. You also get an alert in CV-CUE.



36.4 Change the Default AP-Server Communication 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** > **Advanced Settings.** > **AP-Server Communication Key**
2. Select **Change Communication Key** and change your default communication key.
3. Save the settings.

36.5 Enable the AP-Server Communication Key Timers for the Onboarding Window

AP-Server communication key timers give you control over which APs (having an old or default communication key) can connect to the CV-CUE Server and for how long the timer is available. The timer controls the duration of the onboarding window within which APs need to connect to the Server.

To enable the timers:

1. Select **SYSTEM > Advanced Settings > AP-Server Key.**
2. Enable the following checkboxes in AP-Server Key Timers and provide your time in minutes.
    - **Default Communication Key:** The default key is flashed on every AP during manufacturing.
    - **Old Communication Key:** The previous communication key that was used before the Administrator changed it to the current communication key.
3. Save the settings.

The APs can connect to the CV-CUE Server within the specified time using the default or old communication key.