

Aruba Central Troubleshooting Guide



a Hewlett Packard
Enterprise company

Copyright Information

© Copyright 2022 Hewlett Packard Enterprise Development LP.

Open Source Code

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

Hewlett Packard Enterprise Company
6280 America Center Drive
San Jose, CA 95002
USA

| | |
|---|----------|
| Contents | 3 |
| About this Guide | 4 |
| Terminology Change | 4 |
| Contacting Support | 4 |
| Troubleshooting Workflows | 6 |
| Client Connectivity | 6 |
| Troubleshooting Made Easy Using the AI Search Bar | 6 |
| Datapath of a WLAN Client | 7 |
| Client Health Issues | 8 |
| Offline Clients | 10 |
| Issues in the Application Layer | 15 |
| Roaming Issues in a Wireless Client | 18 |
| Client Connection to the Network | 20 |
| Client Live Troubleshooting | 23 |
| Packet Capture | 23 |
| Notifying Network and Client Anomalies to the Administrator | 25 |
| Client Devices do not Discover Printers across the Subnet | 29 |
| Poor Voice Call Quality Issues | 30 |
| Client Insights: Traffic Pattern Visibility | 33 |
| Viewing Visibility Dashboard | 33 |
| Graph View in the Visibility Dashboard | 34 |
| Device Issues | 35 |
| APs are not seen in the Aruba Central Network | 35 |
| Devices are Offline in the Aruba Central Network | 36 |
| Cabling Issues in Switch | 36 |
| Reboot an IoT Sensor | 37 |
| Device Troubleshooting with Remote Console | 38 |
| Viewing Recorded Console Sessions | 39 |
| AI Insights | 39 |
| AI Insights Anomalies | 39 |
| Network Check | 41 |
| Network Performance | 42 |

Aruba Central, is a cloud-based network management platform that manages your wireless, WAN, and wired networks with Aruba Instant APs, Gateways, and Switches.

This guide provides the necessary background information and available resources to troubleshoot features and services offered in Aruba Central.

This document does not cover every possible trouble event that might occur on Aruba Central but, instead focuses on those events that are frequently seen by Aruba's Technical Assistance Center (TAC) or frequently asked questions from newsgroups.

Terminology Change

As part of advancing HPE's commitment to racial justice, we are taking a much-needed step in overhauling HPE engineering terminology to reflect our belief system of diversity and inclusion. Some legacy products and publications may continue to include terminology that seemingly evokes bias against specific groups of people. Such content is not representative of our HPE culture and moving forward, Aruba will replace racially insensitive terms and instead use the following new language:

| Usage | Old Language | New Language |
|------------------------------------|----------------------|---------------------|
| Campus Access Points + Controllers | Master-Slave | Conductor-Member |
| Instant Access Points | Master-Slave | Conductor-Member |
| Switch Stack | Master-Slave | Conductor-Member |
| Wireless LAN Controller | Mobility Master | Mobility Conductor |
| Firewall Configuration | Blacklist, Whitelist | Denylist, Allowlist |
| Types of Hackers | Black Hat, White Hat | Unethical, Ethical |

Contacting Support

Table 1: *Contact Information*

| | |
|---|---|
| Main Site | arubanetworks.com |
| Support Site | asp.arubanetworks.com |
| Airheads Social Forums and Knowledge Base | community.arubanetworks.com |
| North American Telephone | 1-800-943-4526 (Toll Free) 1-408-754-1200 |

| | |
|---------------------------------|---|
| International Telephone | arubanetworks.com/support-services/contact-support/ |
| Software Licensing Site | lms.arubanetworks.com |
| End-of-life Information | arubanetworks.com/support-services/end-of-life/ |
| Security Incident Response Team | Site: arubanetworks.com/support-services/security-bulletins/ Email: aruba-sirt@hpe.com |

This section provides details on the typical issues you might face with the devices managed by Aruba Central network and the steps to help troubleshoot these issues.

For more information on the troubleshooting workflows, see the following topics:

- [Client Connectivity](#)
- [Device Issues](#)
- [AI Insights](#)
- [Network Check](#)

Client Connectivity

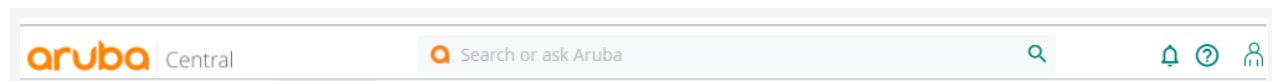
The following section provides details on the typical issues you might face while connecting to the clients in the Aruba Central network and the steps to help troubleshoot these issues.

Troubleshooting Made Easy Using the AI Search Bar

When there are many clients and devices in a network, it is difficult for a user to navigate and identify a particular client or a device to diagnose an issue. The search bar in the **Aruba Central** app enables users to search for clients, devices, and infrastructure connected to the network. The search also retrieves relevant documentation to help users efficiently operate their networks. The search engine uses Natural Language Processing (NLP) to analyze queries and return relevant search results.

The following figure illustrates the search bar option in Aruba Central.

Figure 1 Search Bar



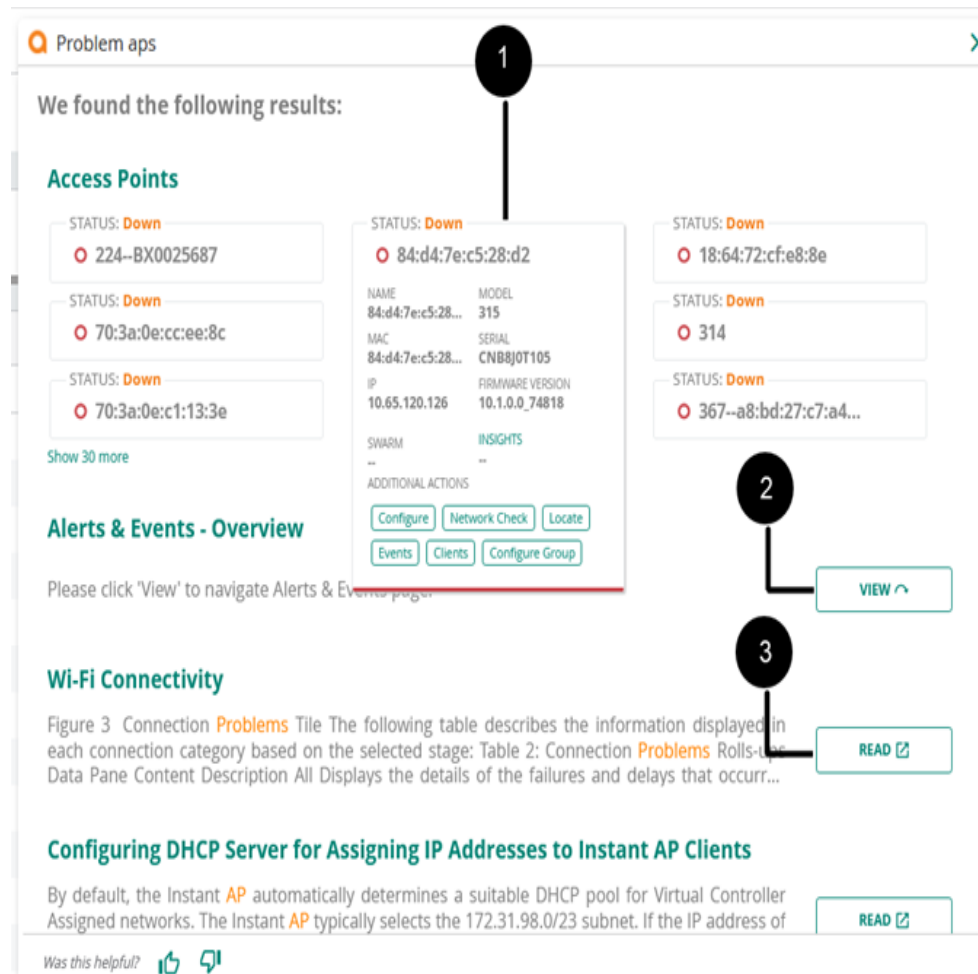
To start a search in the Aruba Central UI, click the search bar or press / (forward slash) on your computer keyboard.

When you click the search bar, you can see the search suggestions in the **Recent** and **Suggested Search** list.

- **Recent**—Shows the searches performed recently in the search bar. These suggestions help you quickly look at the previous searches.
- **Suggested Search**—Shows search suggestions corresponding to the workflow that you follow in the **Aruba Central** app. The suggested search help you perform onboarding, monitoring, configuring, and troubleshooting tasks.

The following figure illustrates the sample search result in Aruba Central.

Figure 2 Sample Search Result



From the search results, you can navigate to:

- **Search Cards**—displays monitoring summary and links to configuration, monitoring, and troubleshooting pages in the **Aruba Central** app.
- **View**—relevant links to the corresponding pages in the **Aruba Central** app.
- **Read**—relevant links to the help pages in the Aruba Central Help Center.

For more information on the list of recommended search terms for different categories, see [Using the Search Bar](#).

Datapath of a WLAN Client

Aruba Central automatically populates the datapath of a WLAN client.

To view the datapath of a WLAN client, complete the following steps:

1. In the **Aruba Central** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**.
The **Clients** page is displayed in **List** view.

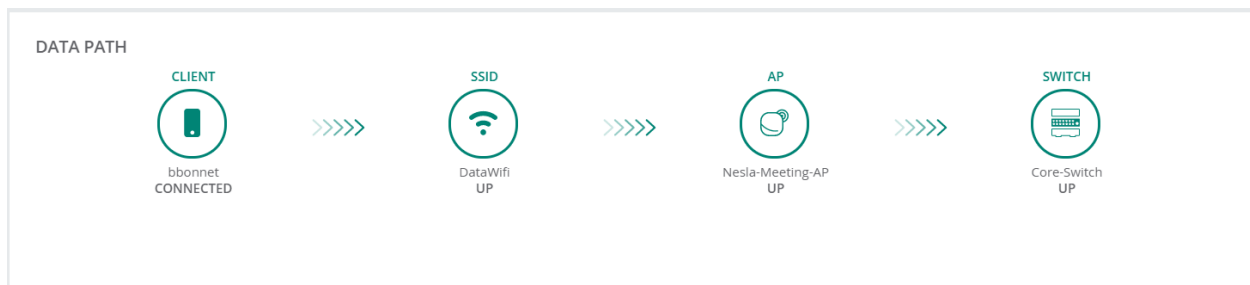


By default, the **Clients** page displays a unified list of all clients.

3. To filter clients based on the device to which the clients are connected, select the device type from the **Clients** drop-down list:
 - **All**—Displays a list of all the clients connected to the network.
 - **AP**—Displays a list of clients connected to the Instant AP.
 - **Switch**—Displays a list of clients connected to the switch.
 - **Gateway**—Displays a list of clients connected to the gateway.
4. To filter the clients based on the state of connectivity, click the connectivity type from the **Client Summary** bar:
 - **Connecting**—Displays a list of client connections that are in progress.
 - **Connected**—Displays a list of clients that are successfully connected to the network.
 - **Failed**—Displays a list of all failed client connections.
 - **Offline**—Displays a list of all offline clients.
 - **Blocked**—Displays a list of all blocked clients.
5. In the **Clients Summary** bar, click **Wireless** to filter the clients connected to the wireless network.
6. In the **Clients** table, click a client listed under **Client Name**.
The **Summary** tab is displayed.
7. In the **Client Details** page, the **Data Path** pane displays the datapath of the client in the network.
The **Datapath** can be one of the following:
 - **Client > SSID > AP**
 - **Client > SSID > AP > Switch**
 - **Client > SSID > AP > Switch > Gateway**
 - **Client > SSID > AP > Gateway**

The list of clients is populated for a time range of 3 hours. To view the list of clients for a different time range, click the **Time Range Filter** and select the required time period. Total data usage for the selected time period is displayed above the client summary bar.

Figure 3 *Client—Datapath*



Client Health Issues

Client health is the efficiency at which an AP transmits downstream traffic to a particular client. This value is determined as the ratio of ideal airtime required for transmitting a packet from an AP to a client to the actual time taken for the packet transmission in percentage. Ideal air time assumes highest data rate without any retransmission.

A client health metric of 100% means the actual airtime the AP spends transmitting data is equal to the ideal amount of time required to send data to the client. A client health metric of 50% means the AP is taking twice as long as is ideal, or is sending one extra transmission to that client for every packet. A metric of 25% means the AP is taking four times longer than the ideal transmission time, or sending 3 extra transmissions to that client for every packet.

Viewing the Client Health

To view the client health, complete the following steps:

1. In the **Aruba Central** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.

The dashboard context for the selected filter is displayed.

2. Under **Manage**, click **Clients**.

The **Clients** page is displayed in **List** view.




By default, the **Clients** page displays a unified list of all clients.

3. To filter clients based on the device to which the clients are connected, select the device type from the **Clients** drop-down list:

- **All**—Displays a list of all the clients connected to the network.
- **AP**—Displays a list of clients connected to the Instant AP.
- **Switch**—Displays a list of clients connected to the switch.
- **Gateway**—Displays a list of clients connected to the gateway.



The wired client will show up in the **All Clients** page only if the client is connected to an Aruba 2540 Series, Aruba 2920 Series, Aruba 2930F Series, Aruba 2930M Series, Aruba 3810 Series, or Aruba 5400R Series switch.

4. To filter clients based on the network to which the clients are connected, click the network type from the **Clients Summary** bar:
 - **All**—Displays a list of all the clients connected to the network.
 - **Wireless**—Displays a list of clients connected to the wireless network.
 - **Wired**—Displays a list of clients connected to the wired network.
 - **Remote**—Displays a list of clients connected through VPN. The remote clients are denoted by the  icon.
5. To filter the clients based on the state of connectivity, click the connectivity type from the **Clients Summary** bar:
 - **Connecting**—Displays a list of client connections that are in progress.
 - **Connected**—Displays a list of clients that are successfully connected to the network.
 - **Failed**—Displays a list of all failed client connections.
 - **Offline**—Displays a list of all offline clients.
 - **Blocked**—Displays a list of all blocked clients.
6. In the **Clients** table, click the **Health** column to view the health of the client. The value of the client health can be one of the following:

- **Poor**—0-30
- **Fair**—31-70
- **Good**—71-100

The list of clients is populated for a time range of 3 hours. To view the list of clients for a different time range, click the **Time Range Filter** and select the required time period. Total data usage for the selected time period is displayed above the client summary bar.

Offline Clients

Offline clients are the clients that were seen in a selected time duration, but are currently disconnected from the Aruba Central network. Aruba Central provides details of offline clients connected to the wireless and wired network. The **Clients** page provides a summary view of all the clients connected to the network.

To view the offline clients, complete the following steps:

1. In the **Aruba Central** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.

The dashboard context for the selected filter is displayed.

2. Under **Manage**, click **Clients**.

The **Clients** page is displayed in **List** view.




By default, the **Clients** page displays a unified list of all clients.

3. To filter clients based on the device to which the clients are connected, select the device type from the **Clients** drop-down list:

- **All**—Displays a list of all the clients connected to the network.
- **AP**—Displays a list of clients connected to the Instant AP.
- **Switch**—Displays a list of clients connected to the switch.
- **Gateway**—Displays a list of clients connected to the gateway.



The wired client will show up in the **All Clients** page only if the client is connected to an Aruba 2540 Series, Aruba 2920 Series, Aruba 2930F Series, Aruba 2930M Series, Aruba 3810 Series, or Aruba 5400R Series switch.

4. To filter clients based on the network to which the clients are connected, click the network type from the **Clients Summary** bar:
 - **All**—Displays a list of all the clients connected to the network.
 - **Wireless**—Displays a list of clients connected to the wireless network.
 - **Wired**—Displays a list of clients connected to the wired network.
 - **Remote**—Displays a list of clients connected through VPN. The remote clients are denoted by the  icon.

5. In the **Clients Summary** bar, click **Offline** to view the offline clients.

The list of clients is populated for a time range of 3 hours. To view the list of clients for a different time range, click the **Time Range Filter** and select the required time period. Total data usage for the selected time period is displayed above the client summary bar.

The **Clients** table lists the details of each client. By default, **All** clients is selected and the table displays the following columns: **Client Name, Status, IP Address, VLAN, Connected To, SSID/Port, AP Role,**

Gateway Role, and **Health**. The default columns displayed is different and contextual based on AP, switch, and gateway.

Click the ellipsis icon to perform additional operations:

- **Download CSV**—Downloads the client details in the .csv file format.
- **Select All**—Selects all columns.
- **Reset Columns**—Resets the table view to the default columns.

If a filter icon appears next to the column header, click and enter the filter criteria or select a filter criteria. For example, to search a client, click the predefined filter criteria: **Connecting**, **Connected**, **Offline**, **Failed**, or **Blocked** from the **Client Summary** bar and in the **Client Name** column enter the name of the client. Aruba Central provides a near-instant refresh of the client status if the client is connecting or connected to an access point.

Table 2: *All Client Details*

| Column Names | Applicability | Description |
|--------------------|--|--|
| Client Name | <ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Gateway | Username, hostname, or MAC address of the client. Click the client name to view the Summary page. |
| Status | <ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Gateway | <p>Client connection status. Use the filter option to view the following:</p> <ul style="list-style-type: none"> ■ Connecting—Applicable only for wireless clients. ■ Connected—Applicable for all client types. ■ Offline—Applicable for all client types. ■ Failed—Applicable only for wireless clients. ■ Blocked—Applicable only for wireless clients. <p>Hover the cursor over the status column to view a pop-up summary based on the connection status. The status summary is populated based on the status type. Each status type and the summary is described below:</p> <ul style="list-style-type: none"> ■ Connecting: <ul style="list-style-type: none"> ○ Client name—Name of the client. ○ Last Seen Time—Date and time the client was last connected. ■ Connected: <ul style="list-style-type: none"> ○ Client name—Name of the client. ○ Authentication—Type of authentication. Displays the authentication label only for authenticated clients. ○ IP address—Client IP address. ○ Connected Since—Date and time at which the client was connected. ○ Failure Stage—Stage of the connection where the client failed to connect. It is not applicable for the wired clients, so displayed as NA. ○ Health Score—Device health. ○ Connected Device Port—The device port that the wired client is connected to. ■ Failed: <ul style="list-style-type: none"> ○ Client name—Name of the client. ○ Last Seen Time—Date and time the client was last connected. ○ Failure Stage—Stage of the connection where the client failed to connect. |

Table 2: *All Client Details*

| Column Names | Applicability | Description |
|---------------------|--|--|
| | | <ul style="list-style-type: none"> ◦ Failure Reason—Reason for the connection failure. ■ Offline: <ul style="list-style-type: none"> ◦ Client name—Name of the client. ◦ Authentication—Type of authentication. Displays the authentication label only for authenticated clients. ◦ IP address—Client IP address ◦ Connected Since—Date and time at which the client was connected. ◦ Last Seen Time—Date and time the client was last connected. ◦ Failure Stage—Stage of the connection where the client failed to connect. ◦ Connected Device Port—The device port that the wired client is connected to. ■ Blocked: <ul style="list-style-type: none"> ◦ Client name—Name of the client. ◦ Last Seen Time—Date and time the client was last connected. |
| IP Address | <ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Gateway | IP address of the client. |
| VLAN | <ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Gateway | VLAN of the device to which the client is connected. |
| Connected To | All | AP name, Switch name, or Gateway name. This is the first layer 2 hop for the client. If the device does not have a name, the MAC address is displayed. |
| AP Role | <ul style="list-style-type: none"> ■ All ■ AP | Role assigned by the AP. |
| Gateway Role | <ul style="list-style-type: none"> ■ All ■ Gateway | Role assigned by the Aruba Gateway. |
| Health | <ul style="list-style-type: none"> ■ All ■ AP | Client health. The value can be one of the following: <ul style="list-style-type: none"> ■ Poor—0-30 ■ Fair—31-70 ■ Good—71-100 |
| SSID/Port | <ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Gateway | Displays the SSID for wireless clients and the port number for wired clients. The column title displays SSID and Port interchangeably based on the device filters. For APs, the column title displays SSID . For switch and gateway, the column title displays Port . |
| Insights | <ul style="list-style-type: none"> ■ All | The total number of AI insights generated for the client. |

Table 2: *All Client Details*

| Column Names | Applicability | Description |
|-----------------------|--|--|
| | <ul style="list-style-type: none"> ■ AP | |
| Switch Role | <ul style="list-style-type: none"> ■ All ■ Switch | Role assigned by the Aruba switch. |
| Failure Stage | <ul style="list-style-type: none"> ■ All ■ AP | <p>Failure status of the client that failed to connect. The failure reasons could be:</p> <ul style="list-style-type: none"> ■ Association failure ■ MAC authentication failure ■ 802.1X authentication failure ■ Key exchange failure ■ DHCP failure ■ Captive Portal failure |
| Group Name | <ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Gateway | Displays the name of the group that the device is connected to. The Connected To column displays the device name that the client is connected to. |
| Site Name | <ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Gateway | Displays the name of the site that the device is connected to. The Connected To column displays the device name that the client is connected to. |
| MAC Address | <ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Gateway | MAC address of the client. |
| Hostname | <ul style="list-style-type: none"> ■ All ■ AP ■ Gateway | Host name of the client. |
| User Name | <ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Gateway | Username of the client. |
| Key Management | <ul style="list-style-type: none"> ■ All ■ AP | Security mode used by the client. |
| Authentication | <ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Gateway | Authentication type used by the client to connect with the device. |

Table 2: *All Client Details*

| Column Names | Applicability | Description |
|------------------------------------|---|---|
| Global Unicast IPv6 Address | <ul style="list-style-type: none">■ All■ AP■ Gateway | When the IPv6 address is present for a client, you can view its Global Unicast IPv6 address. Click the ellipsis and select the column to view the value if the column is not displayed. |
| Link Local IPv6 Address | <ul style="list-style-type: none">■ All■ AP■ Gateway | When the IPv6 address is present for a client, you can view its Link Local IPv6 address. Click the ellipsis and select the column to view the value if the column is not displayed. |
| Capabilities | <ul style="list-style-type: none">■ All■ AP | Client 802.11 capabilities. |
| Usage | <ul style="list-style-type: none">■ All■ AP■ Switch■ Gateway | Total data usage for the selected time period. |
| Last Seen Time | <ul style="list-style-type: none">■ All■ AP■ Switch■ Gateway | Date and time when the client was last seen. |
| Connected Since | <ul style="list-style-type: none">■ All■ AP■ Switch■ Gateway | Date and time since when the client was connected. |
| AP Name | <ul style="list-style-type: none">■ All■ AP | Name of the AP. |
| AP Mac Address | <ul style="list-style-type: none">■ All■ AP | MAC address of the AP. |
| Channel/Band | <ul style="list-style-type: none">■ All■ AP | Last connected channel and band. |
| Switch Name | <ul style="list-style-type: none">■ All■ Switch | Name of the switch. |
| Port | <ul style="list-style-type: none">■ All■ Switch■ Gateway | Port number of the switch. |
| Gateway Name | <ul style="list-style-type: none">■ All■ Gateway | Name of the Aruba Gateway. |
| Tunneled | <ul style="list-style-type: none">■ All■ AP | Tunnel mode applicable for the Aruba Gateway managed WLAN, UBT, or PBT client. |

Table 2: *All Client Details*

| Column Names | Applicability | Description |
|------------------------|---|---|
| | <ul style="list-style-type: none">■ Switch■ Gateway | |
| Segmentation | <ul style="list-style-type: none">■ All■ AP■ Switch■ Gateway | Type of segmentation. The type of segmentation can be: <ul style="list-style-type: none">■ None■ UBT■ PBT■ Underlay■ Overlay <p>NOTE: To view the details about dynamic segmentation, a gateway must be licensed in Aruba Central and connected to the switch.</p> |
| Client Category | <ul style="list-style-type: none">■ All■ AP■ Gateway | Displays the category of the profiled device. For example, Access Points, Computer, Smart Device, VoIP phone, and so on. |
| Client Family | <ul style="list-style-type: none">■ All■ AP■ Gateway | Displays the type of operating system or vendor. For example, if the client category is Computer, the client family can be Windows, Linux, or Apple Mac. |
| Client OS | <ul style="list-style-type: none">■ All■ AP■ Gateway | Displays the operating system that the device runs on. For example, if the client category is Computer and the client family is Windows, the client OS can be Windows or Windows 8/10. |

Issues in the Application Layer

In an Aruba Central-managed network, Network Check aims to identify, diagnose, and debug issues on your network. The **Network Check** tab under **Analyze > Tools** page captures the troubleshooting utilities that are used to test a network entity and collect results based on your selection. You must have admin privileges or read-write privileges to perform network checks.

The following tests are available to diagnose issues pertaining to WLAN network connections:

- **HTTP Test**—The HTTP test is a performance test to identify the time taken to load a web page. It sends packets to the HTTP URL and tries to establish a connection and exchange data. If the HTTP website returns a response, the issue could be isolated to the client device.
- **HTTPS Test**—The HTTPS test is a performance test to identify the time taken to load a web page. It sends packets to the HTTPS URL and tries to establish a connection and exchange data. If the HTTPS website returns a response, the issue could be isolated to the client device.
- **TCP Test**—The TCP test verifies network connectivity to remote hosts with the remote host-port combination approach. It sends packets to the host, for example, FTP server, and tries to establish a connection and exchange data. If the FTP server returns a response, the issue could be isolated to the client device.

HTTP Test

To perform an HTTP test, complete the following steps:

1. In the **Aruba Central** app, search for a specific wireless client in the **Search Bar**.
2. Click on the wireless client listed in the search result under **Clients**, to navigate to the corresponding **Client Details** page.
3. Under **Analyze**, click **Tools**.
The Network Check tab is displayed.
4. From the **Device Type** drop-down list, select **Access Point**.
5. From the **Test** drop-down list, select **HTTP Test**.
6. The value in the **Sources** drop-down list is auto-populated based on the wireless client selected.
7. In the **URL** field, enter the HTTP URL for which you want to perform the HTTP test. For example, `http://hostname` or `http://ipaddress`.
8. Optionally, expand **Show Additional Test Settings** to enter the timeout value in seconds, in the **Timeout** field. The value should be between 1 to 10 seconds. The default timeout value is 5 seconds.



Show Additional Test Settings is disabled when no **Test** type is selected.

9. Click **Run**. The output is displayed in the **Device Output** section.

Figure 4 HTTP Test—Device Output

```

=== Troubleshooting session started ===

=====
Output Time: 2020-04-20 14:18:59 UTC
HTTP Test from CNH8KD00G1 to http://google.com has Passed
Timeout: 9
Download Rate: 6438.257 KB/sec
Download Bytes: 14.0 KB

=== Troubleshooting session completed ===

```



The HTTP test is supported only from ArubaOS 8.3.0.0 or later versions. The test support only IPv4 address or domain name in the URL field.

HTTPS Test

To perform an HTTPS test, complete the following steps:

1. In the **Aruba Central** app, search for a specific wireless client in the **Search Bar**.
2. Click on the wireless client listed in the search result under **Clients**, to navigate to the corresponding **Client Details** page.
3. Under **Analyze**, click **Tools**.
The Network Check tab is displayed.
4. From the **Device Type** drop-down list, select **Access Point**.
5. From the **Test** drop-down list, select **HTTPS Test**.
6. The value in the **Sources** drop-down list is auto-populated based on the wireless client selected.
7. In the **URL** field, enter the HTTPS URL for which you want to perform the HTTPS test. For example, `https://hostname` or `https://ipaddress`.
8. Optionally, expand **Show Additional Test Settings** to enter the timeout value in seconds, in the **Timeout** field. The value should be between 1 to 10 seconds. The default timeout value is 5 seconds.



Show Additional Test Settings is disabled when no **Test** type is selected.

9. Click **Run**. The output is displayed in the **Device Output** section.

Figure 5 *HTTPS Test—Device Output*

```
=== Troubleshooting session started ===  
  
=====  
Output Time: 2020-04-20 14:16:20 UTC  
HTTPS Test from CNFLK511F1 to https://google.com has Passed  
Timeout: 9  
Download Rate: 6176.113 KB/sec  
Download Bytes: 13.99 KB  
  
=== Troubleshooting session completed ===
```

CLEAR



The HTTPS test is supported only from ArubaOS 8.4.0.0 or later versions. The test support only IPv4 address or domain name in the URL field.

TCP Test

To perform a TCP test, complete the following steps:

1. In the **Aruba Central** app, search for a specific wireless client in the **Search Bar**.
2. Click on the wireless client listed in the search result under **Clients**, to navigate to the corresponding **Client Details** page.
3. Under **Analyze**, click **Tools**.
The Network Check tab is displayed.
4. From the **Device Type** drop-down list, select **Access Point**.
5. From the **Test** drop-down list, select **TCP Test**.
6. The value in the **Sources** drop-down list is auto populated based on the wireless client selected.
7. In the **Host** field, enter the IPv4 address. Hostname is not supported.
8. In the **Port** field, enter the port number. The port number should be in the range 1 to 65535.
9. Optionally, expand **Show Additional Test Settings** to enter the timeout value in seconds, in the **Timeout** field. The value should be between 1 to 10 seconds. The default timeout value is 5 seconds.



Show Additional Test Settings is disabled when no **Test** type is selected.

10. Click **Run**. The output is displayed in the **Device Output** section.

Figure 6 TCP Test—Device Output

```
=== Troubleshooting session started ===  
  
=====
```

CLEAR

```
Output Time: 2020-04-20 14:05:56 UTC  
TCP Test from CNFLK511BQ to 4.4.4.4 has Failed  
Port Number : 1  
Timeout: 9  
Failure Reason: connect timedout  
  
=== Troubleshooting session completed ===
```



The TCP test is supported only from ArubaOS 8.3.0.0 or later versions.

Viewing the Device Output

After you execute troubleshooting commands on the devices, Aruba Central displays the output in the **Device Output** section of the **Tools** page.

The output pane displays a list of devices on which the troubleshooting commands were executed, the test type, initial timestamp, source, and target. It also shows the status of the tests as, in progress, complete, and the buffer time. If there are multiple devices, select the device for which you want to view the output.



Output history of device with buffer space issues shall be automatically cleared.

You can perform the following tasks from the **Device Output** section:

- Click **Clear** to clear the output. You can clear the output for a single device or for all devices. The **Clear** option is disabled for read-only users.
- Click the **Search** icon to search for text in the output.
- Click the **Email** icon and click **Send** to send the output as an email. You can also add email recipients in the **CC** field.
- Click **Export** to export the command output as a zip file.
- Click the maximize icon to maximize the device output pane.

For more information on the output displayed for the CLI commands, see the following documents:

- *Aruba Instant CLI Reference Guide* for Instant AP CLI command output
- *HPE ArubaOS-Switch Management and Configuration Guide* for AOS-S switch CLI command output
- *ArubaOS CLI Reference Guide* for SD-WAN Gateway CLI command output

Roaming Issues in a Wireless Client

Roaming is the process of a wireless client moving from one source AP to another AP within the same Extended Service Set (ESS) without losing connection. When a wireless client roams between two APs, the association to the new AP terminates the previous AP association and the destination AP creates an event.

In Aruba Central, the **Roaming Experience** pane provides the details of the roaming events and latency parameters of a client.

Viewing the Roaming Experience Pane

To view the **Roaming Experience** pane, complete the following steps:


1. In the **Aruba Central** app, search for a specific wireless client in the **Search Bar**.
2. Click any one of the wireless clients listed in the search result under **Clients**, to navigate to the corresponding **Client Details** page.
3. In the **Client Details** page, the **Roaming Experience** pane displays the details of the roaming events and latency parameters of a client.

The **Roaming Experience** pane displays two views, the grid view and the trend view.

Grid View

The grid view is the default view and provides the following information:

Table 3: *Grid View*

| Parameter | Description |
|-----------------------|---|
| Date/Time | Displays the date and time of occurrence of the client roaming/association events. |
| SSID | The SSID to which the client is connected. |
| Latency (ms) | Roaming latency in milliseconds between source and destination AP. NOTE: Roaming latencies above 50 ms are considered as high latency roaming events. |
| To BSSID | The BSSID of the destination AP. |
| Source AP | AP to which the client was connected. |
| Destination AP | AP to which the client is connected. |
| Roaming Type | The type of roaming. Click the  icon to filter the data based on the following roaming types: <ul style="list-style-type: none"> ■ 11r ■ okc ■ 802.11 |
| Band | Radio band on which the client is connected. |
| RSSI (dBm) | Received Signal Strength Indicator (RSSI) on the client. It is the estimated measure of power level received by client from the AP. |

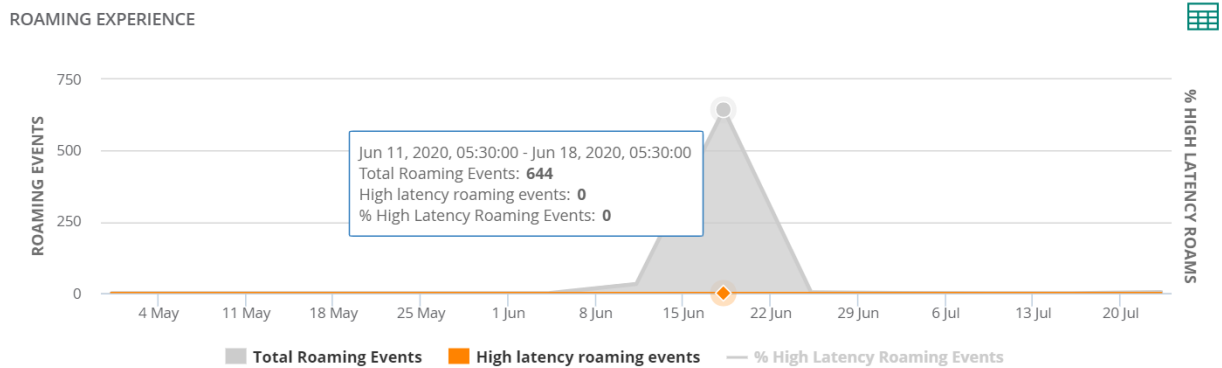


- By default, the **Roaming Experience** table displays data for the last 3 hours. To view the table for a different time range, use the **Time Range Filter**.
- A search filter is provided only for the **Data/Time** and **Roaming Type** columns.

Trend View

The trend view displays a chart that shows the percentage of high latency roaming events, total roaming events, and the number of high latency roaming events at a particular instance based on the value selected in the **Time Range Filter**.

Figure 7 *Roaming Experience—Trend View*



Client Connection to the Network

When a client tries to connect to the AP or the network, and is unable to do so, you can navigate to the **Clients** page and check the reasons for failure.

The **Clients** page provides a list view of all the clients connected to the network. You can filter clients based on the network the clients are connected to. This page displays key client information and also allows you to view a specific client detail page.

To view the list of **Failed** clients, complete the following steps:

1. In the **Aruba Central** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.

The dashboard context for the selected filter is displayed.

2. Under **Manage**, click **Clients**.

The **Clients** page is displayed in **List** view.




By default, the **Clients** page displays a unified list of all clients.

3. To filter clients based on the device to which the clients are connected, select the device type from the **Clients** drop-down list:
 - **All**—Displays a list of all the clients connected to the network.
 - **AP**—Displays a list of clients connected to the Instant AP.
 - **Switch**—Displays a list of clients connected to the switch.
 - **Gateway**—Displays a list of clients connected to the gateway.



The wired clients will show up in the **All Clients** page only if the client is connected to an Aruba 2540 Series, Aruba 2920 Series, Aruba 2930F Series, Aruba 2930M Series, Aruba 3810 Series, or Aruba 5400R Series switch.

4. To filter clients based on the network to which the clients are connected, click the network type from the **Client Summary** bar:
 - **All**—Displays a list of all the clients connected to the network.
 - **Wireless**—Displays a list of clients connected to the wireless network.
 - **Wired**—Displays a list of clients connected to the wired network.
 - **Remote**—Displays a list of clients connected through VPN. The remote clients are denoted by the  icon.

5. In the **Client Summary** bar, click **Failed** to view a list of all failed client connections.
6. In the **Clients** table, the **Failure Stage** column provides the following information:

Table 4: Client Details

| Failure Stage | <ul style="list-style-type: none"> ■ All ■ AP | Failure status of the client that failed to connect. The failure reasons could be: <ul style="list-style-type: none"> ■ Association error ■ MAC authentication error ■ 802.1X authentication error ■ Key exchange error ■ DHCP error ■ Captive Portal error |
|---------------|---|---|
|---------------|---|---|

Hover over the specific failure stage to display detailed information regarding the type of error. For example, if the failure stage column displays failure stage as **DHCP**, and you hover your mouse over **DHCP**, it displays the following:

- **Failure Reason**
- **Last Seen time**

The list of clients is populated for a time range of 3 hours. To view the list of clients for a different time range, click the **Time Range Filter** and select the required time period. Total data usage for the selected time period is displayed above the client summary bar.

Figure 8 Client Details

The screenshot shows the 'CLIENTS' section in the Aruba Central interface. At the top, there's a filter bar with 'ALL' selected and a refresh icon. To the right, data usage is shown as '138.83 KB (@ 33.56 KB | @ 105.27 KB)'. Below this is a status bar with filters: All (7), Connecting (0), Connected (0), Failed (1), Offline (6), Blocked (0), Wireless (7), Wired (0), and Remote (0). The main table has columns: Client Name, Status, IP Address, VLAN, Connected To, SSID/Port, AP Role, Gateway Role, Health, and Failure Stage. The 'Failed' status is highlighted. A tooltip is shown over the 'DHCP' failure stage, displaying the failure reason: 'Discover Timeout, Authentication: MAC Authentication' and the last seen time: 'Jan 13, 2022, 19:13'.

| Client Name | Status | IP Address | VLAN | Connected To | SSID/Port | AP Role | Gateway Role | Health | Failure Stage |
|---------------|---------|---------------|------|--------------|-----------------|-------------|--------------|--------|---------------|
| 192.168.9.73 | Offline | 192.168.9.73 | 234 | ap name | S305 | NA | NA | | DHCP |
| 192.168.4.18 | Offline | 192.168.4.18 | 405 | ap name | S404 | S404 | NA | | |
| | Offline | | | ap name | S405_Routed | S405_Routed | NA | | |
| | Offline | | | ap name | default_guest_# | NA | NA | | |
| 192.168.1.105 | Offline | 192.168.1.105 | 1 | ap name | S55 | NA | NA | | |

You must also check if multiple failures have occurred and if the client is denylisted. When a client is denylisted, it is not allowed to associate with an AP in the network. If a client is connected to the network when it is denylisted, a deauthentication message is sent to force client disconnection. You can denylist a client manually or dynamically.

Denylisting Clients Manually

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

To add a client to the denylist manually, complete the following steps:

1. In the **Aruba Central** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.

2. Under **Manage**, click **Devices > Access Points**.
A list of access points is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the access points are displayed.
4. Click **Show Advanced**, and click the **Security** tab.
The Security details page is displayed.
5. Click the **Denylisting** accordion.
6. Under **Manual Denylisting**, click **+** and enter the MAC address of the client to be denylisted.
7. Click **OK**.
8. Click **Save Settings**.

To delete a client from the manual denylist, select the MAC Address of the client under the **Manual Denylisting**, and then click the delete icon.



You can configure a maximum number of authentication failures by the clients, after which a client must be denylisted. For the denylisting to take effect, you must enable the denylisting option when you create or edit the WLAN SSID profile. Go to **WLANS > Security > Advanced Settings** and enable the **Denylisting** option.

Denylisting Clients Dynamically

Clients can be denylisted dynamically when they exceed the authentication failure threshold or when a denylisting rule is triggered as part of the authentication process.

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

In session firewall based denylisting, an ACL rule automates denylisting. When the ACL rule is triggered, it sends out denylist information and the client is denylisted.

To configure the denylisting duration, complete the following steps:

1. In the **Aruba Central** app, set the filter to a group containing at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
A list of access points is displayed in the **List** view.
3. Click the **Config** icon.
The tabs to configure the access points are displayed.
4. Click **Show Advanced**, and click the **Security** tab.
The Security details page is displayed.
5. Click the **Denylisting** accordion.
6. Under **Dynamic Denylisting**, enter the following information:
 - a. For **Auth Failure Denylist Time**, enter the duration after which the clients that exceed the authentication failure threshold must be denylisted.
 - b. For **Policy Enforcement Failure Rule Denylisted Time**, enter the duration after which the clients can be denylisted due to an ACL rule trigger.
7. Click **Save Settings**.



You can configure a maximum number of authentication failures by the clients, after which a client must be denylisted. To enable session-firewall-based denylisting, select the **Denylist** check box in the **Access Rule** page during the WLAN SSID profile creation.

After the failure reasons are detected, select the client and navigate to the **Clients Detail** page. Click **Tools** under **Analyze** in the left navigation pane, and perform network check and advance troubleshooting check under **Network Check** and **Commands** respectively.

Client Live Troubleshooting

Aruba Central allows you to troubleshoot issues related to a client or a site in real time for detailed analysis. Live troubleshooting is supported only if the Instant APs are running 8.4.0.0 firmware version or a later version.

To troubleshoot a client at the site level, complete the following steps:

1. In the **Aruba Central** app, set the filter to one of the options under **Sites**.
2. Under **Analyze**, click **Live Events**. The **Live Events** page is displayed.
3. Enter the MAC address of the client and click **Start Troubleshooting**.

To troubleshoot a wireless client, complete the following steps:

1. In the **Aruba Central** app, search for the specific wireless client in the **Search Bar** for which you want to perform live troubleshooting.
2. Click on the wireless client listed in the search result under **Clients**, to navigate to the corresponding **Client Details** page.
3. Under **Analyze**, click **Live Events**. The **Live Events** page is displayed.

The troubleshooting session runs for 15 minutes and the status is displayed every minute. If you want to stop live troubleshooting, click **Stop Troubleshooting** to go back to the historical view.

After the live troubleshooting session ends, the details of the events are displayed in the live events table.

Live Events Details

The following details are captured and displayed in the **Live Events** table:

- **Occurred On**—Displays the timestamp of the event. Use the filter option to filter the events by date and time.
- **Device Name**—Displays the name of the device the client is connected to. Set the filter to select a specific device under **Sites**.
- **AP Name**—Displays the name of the AP the client is connected to. Use the filter option to select a specific AP.
- **Category**—Displays the category of the event. Use the filter option to filter the events by category.
- **Description**—Displays a description of the event. Use the filter option to filter the events based on description.

Packet Capture

Aruba Central allows you to interact and launch a targeted packet capture on a client connected to a specific access point or a switch. After you start packet capture from the UI, Aruba Central notifies the access point and the switch. The default packet capture duration is 15 minutes. After you start packet capture, use the toggle button to stop packet capture, or go back to the **Client Overview** page.



For packet capture, for a wired client connected to an Aruba 5400R Switch Series (V3 mode), ensure that “no-allow v2 modules” is set for the switch. Packet capture for stack switches works only if the client is connected to the commander of the stack.

Starting Packet Capture

You can start packet capture from the wireless or wired clients page. Packet capture can be done at a site level (wireless client only) or for a selected client.

To start packet capture at a site level, perform the following steps:

1. In the **Aruba Central** app, set the filter to one of the options under **Sites** that contains at least one device. The dashboard context for the selected site is displayed.
2. Under **Analyze**, click **Live Events**. The **Live Events** page is displayed.
3. Enter the MAC address of the client.



At a site level, Aruba Central does not support packet capture for a wired client connected to a switch.

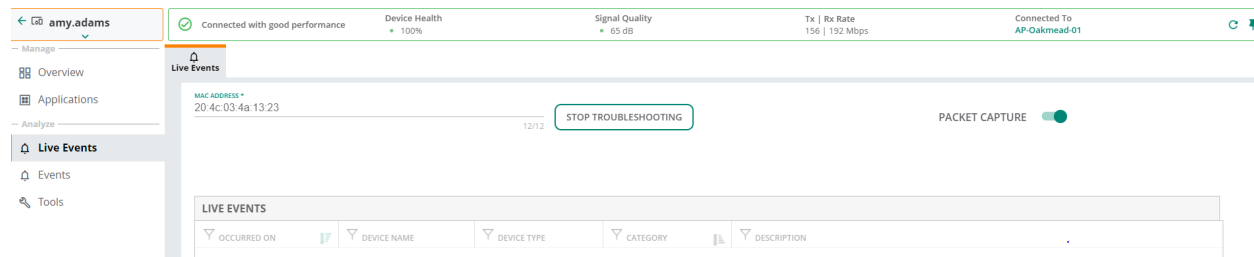
4. Enable the **Packet Capture** toggle button to start live packet capture for the selected client.
5. Click **Start Troubleshooting**.

To start packet capture for a wireless or wired client, perform the following steps:

1. In the **Aruba Central** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**. The Clients overview page is displayed in **List** view.
3. By default, the **Clients** table displays a unified list of clients.
4. Click the name of the wireless or wired client to open the corresponding **Client Details** page. If there are many clients connected to the network, click **Wireless** or **Wired** to filter the clients connected to the wireless or wired client respectively.
5. Enter the client name in the **Client Name** column, and click the client name.
6. Under **Analyze**, click **Live Events**. The **Live Events** page is displayed. The client live troubleshooting starts automatically for the selected client.
7. Click **Stop Troubleshooting** to stop live troubleshooting.
8. Enable the **Packet Capture** toggle button to start live packet capture for the selected client.
9. Click **Start Troubleshooting** to live troubleshoot the selected client. Live packet capture starts for the selected client.

The live troubleshooting session runs for a duration of 15 minutes. After the live troubleshooting session ends, a **Download PCAP** text appears above the live events table. Click **Download PCAP** to download the generated PCAP file on your local system.

Figure 9 *Live Events*



Notifying Network and Client Anomalies to the Administrator

The **Wi-Fi Connectivity** page in Aruba Central enables you to check connection details of all the clients connected to an AP in the network. The data can be used to notify administrators of the possible anomalies in the network.

To view the **Wi-Fi Connectivity** page, complete the following steps:

1. In the **Aruba Central** app, set the filter to one of the options under **Groups** or **Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
2. Under **Manage > Overview**, click **Wi-Fi Connectivity**.
The **Wi-Fi Connectivity** page is displayed.

By default, the graphs on the **Wi-Fi Connectivity** page is plotted for a time range of 3 hours. To view the graphs for a different time range, click the **Time Range Filter** icon. You can choose to view graphs for a time period of 3 hours, 1 day, 1 week, and 1 month.

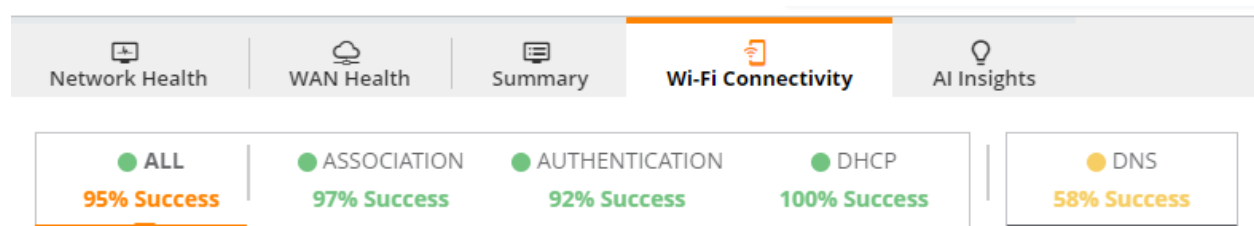
This section includes the following topics:

- [Connectivity Summary Bar](#)
- [Connection Experience](#)
- [AI Insights](#)
- [Connection Problems](#)
- [Connection Events](#)

Connectivity Summary Bar

The connectivity summary bar displays the details of all clients in percentage. It displays the percentage success rate of each stage for the users to know the network performance.

Figure 10 *Connectivity Summary Bar*



The following table describes the information displayed in each section:

Table 5: Connectivity Summary Bar

| Field | Description |
|-----------------------|--|
| All | Displays the aggregated success percentage of Association , Authentication , and DHCP for all clients connected to the network. |
| Association | Displays the percentage of successful attempts made by a client to connect to the network. |
| Authentication | Displays the percentage of successful attempts of client authentication. |
| DHCP | Displays the percentage of successful attempts of DHCP requests and responses when onboarding a client. |
| DNS | Displays the percentage of successful attempts in the detected DNS resolutions, when a client is connected to the network. |

Connection Experience

The **Connection Experience** tile displays the overall success percentage, total number of attempts, number of successful attempts, total delays, and the total failures for each of the stages based on the selected time range filter. To view the connection experience for each individual stage, select the stage type from the **Connectivity Summary** bar.

Figure 11 Connection Experience Tile



AI Insights

The **AI Insights** tile provides a list of AI Insights generated for a selected time range. To view the details, click on a selected **AI Insight**. The page gets redirected to the AI Insights under the **AI Insights** page. Click each of the listed AI Insight for a detailed analysis based on the impact on the network.



AI-Insights is not implemented for **Association** and **DNS**. AI Insights is not implemented at a Group level also. The page displays **No AI Insights observed**.

Connection Problems

The **Connection Problems** tile displays the details of **Failures** and **Delays** graphically for each of the categories from the drop-down list. Each graph displays the top five MAC addresses or SSID based on the selected category. Each category in the **Connection Problems** drop-down lists changes based on the selected stage in the **Connectivity Summary** bar. Selecting the required category from the drop-down displays the failures and delays in a pie chart with percentage, and a bar graph with the number of failures and delays. Hover the cursor over each graph to view the number of failures or delays for each stage.

Figure 12 Connection Problems Tile



The following table describes the information displayed in each connection category based on the selected stage:

Table 6: Connection Problems Rolls-Ups

| Data Pane Content | Description |
|-------------------|--|
| All | <p>Displays the details of the failures and delays that occurred during a client connection. The chart displays the failure details of Association, Authentication, and DHCP for each client. The Connection Problems drop-down list includes the following categories:</p> <ul style="list-style-type: none">■ By Stage■ By Clients■ By Access Points■ By Band■ By SSID |

| Data Pane Content | Description |
|-----------------------|---|
| Association | Charts the details of the failures and delays that occurred during a client association. The Connection Problems drop-down list includes the following categories: <ul style="list-style-type: none"> ■ By Clients ■ By Access Points ■ By Band ■ By SSID ■ By Reason |
| Authentication | Charts the details of the failures and delays that occurred during a client authentication. The Connection Problems drop-down list includes the following categories: <ul style="list-style-type: none"> ■ By Type ■ By Clients ■ By Access Points ■ By Band ■ By SSID ■ By Server |
| DHCP | Charts the details of the failures and delays that occurred during the attempts of DHCP requests and responses by a client. The Connection Problems drop-down list includes the following categories: <ul style="list-style-type: none"> ■ By Clients ■ By Access Points ■ By Reason |
| DNS | Charts the details of the failures and delays that occurred during the attempts in detected DNS resolutions when a client is connected to the network. The Connection Problems drop-down list includes the following categories: <ul style="list-style-type: none"> ■ By Access Points ■ By Reason ■ By Server |

Connection Events

The **Connection Events** table details out the list of delays and failures for each client based on the client MAC addresses. Click the **List** icon to view the connection events table. Click the **Connection Events** drop-down list to filter the events **By Clients** or **By Access Points**. The **Connection Events** table displays the following information:

Table 7: *Connection Events*

| Data Pane Content | Description |
|--------------------|--|
| MAC Address | Displays the MAC address of the client. |
| Name | Displays the name of the access point. |
| Delays | Displays the delays that occurred during the event. |
| Failures | Displays the failure details that occurred during the event. |

Client Devices do not Discover Printers across the Subnet

For client devices to discover printers across the subnet, you have to turn on the AirGroup service available in Aruba Central.

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

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

In addition to the mDNS protocol, Instant APs also support Universal Plug and Play (UPnP) and Digital Living Network Alliance (DLNA) enabled devices. DLNA is a network standard derived from UPnP, which enables devices to discover the services available in a network.

DLNA also provides the ability to share data between the Windows or Android-based multimedia devices. All the features and policies applicable to mDNS are extended to DLNA to ensure full interoperability between compliant devices.

To enable AirGroup services, complete the following steps:

1. In the **Aruba Central** app, set the filter to a group that contains at least one AP.
The dashboard context for the group is displayed.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the **Config** icon.
The tabs to configure access points is displayed.
4. Click **Show Advanced**, and then click the **Services** tab.
The Services details page is displayed.
5. Click the **AirGroup** accordion.
6. Select the **AirGroup** check box.

-
- The **mDNS (Bonjour)** and **SSDP (DLNA/UPNP)** check-boxes are selected by default. Select at least **mDNS (Bonjour)** or **SSDP (DLNA/UPNP)** to proceed further.
 - Optionally, select the **Guest Bonjour Multicast** check box to allow guest users to use the Bonjour services that are enabled in a guest VLAN. When **Guest Bonjour Multicast** is enabled, the Bonjour devices are visible only in the guest VLAN and AirGroup does not discover or enforce policies in guest VLAN.
-



7. Expand **AirGroup Settings**, and then select the **AirPrint** check box to enable wireless printing between AirPrint capable devices and AirPrint compatible printers.
 - Optionally, when enabling an AirGroup service, define disallowed roles. The disallowed roles are not allowed to use the specific AirGroup service. To disallow roles:
 1. Click **Edit** against **Disallowed Roles**.
 2. Move the roles from the **Available** pool to the **Selected** pool.
 3. Click **Ok**.

- Optionally, when enabling an AirGroup service, define disallowed VLANs. The disallowed VLANs are not allowed to use the specific AirGroup service. To disallow VLANs:
 1. Click **Edit** against **Disallowed VLANs**.
 2. Type the VLANs in **Enter comma-separated list of VLAN IDs**. Separate multiple VLANs with a comma.
 3. Click **Ok**.
 - Optionally, configure and enable a new AirGroup service. If defined, disallowed roles or VLANs are not allowed to use the new AirGroup service. To configure and enable a new AirGroup service:
 1. Click **Add New Service**.
 2. Type the service name in **Service Name**. Use alphanumeric characters.
 3. Type a service ID in **Service ID**. Use + to add additional service IDs.
Sample service ID: **urn:schemas-upnp-org:service:RenderingControl:1** or **_sleep-proxy._udp**.
 4. Click **Ok**.
 5. Select the check box against the new AirGroup service.
8. Optionally, under **ClearPass Settings** sub-accordion, configure the following parameters listed:

Table 8: *ClearPass Settings*

| Mode | Description |
|-----------------------------------|--|
| ClearPass Policy Manager Server 1 | Specify the ClearPass Policy Manager server to use. Select one from the drop-down or define a new ClearPass Policy Manager server. |
| Enforce ClearPass Registration | Specify is ClearPass registration should be enforced. |

9. Click **Save Settings**.

Poor Voice Call Quality Issues

The growing use of Wi-Fi and the proliferation of mobile tablet and smartphone clients cause control and visibility challenges for communication and collaboration applications. To overcome these challenges, Aruba offers the Unified Communication and Collaboration (UCC) application service to manage your enterprise communication ecosystem.

The UCC application on Aruba devices provides a seamless user experience for voice calls, video calls, and application sharing when using communication and collaboration tools. The UCC application actively monitors voice, video, and application sharing sessions, provides traffic visibility, and allows you to prioritize the required sessions. The UCC application also leverages the functions of the service engine on the cloud platform and provides rich visual metrics for analytical purposes.

To access the UCC application, obtain a valid subscription. To obtain a subscription for the UCC application, contact the Aruba Central Sales team.

To analyze the VOIP call quality of a specific client, complete the following steps:

1. In the **Aruba Central** app, search for a specific wireless client in the **Search Bar**.
2. Click on the wireless client listed in the search result under **Clients**, to navigate to the corresponding **Client Details** page.

3. Under **Manage**, click **Applications > UCC**.

The **UCC** page is displayed in the **List** view.

Alternatively, you can also perform the following steps to navigate to the **UCC** tab to check the VOIP call quality of a specific client:

1. In the **Aruba Central** app, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**.
The Clients page is displayed in the **List** view.
3. In the **Clients Summary** bar, click **Wireless** to filter the clients connected to the wireless network.
4. In the **Clients** table, click a client listed under **Client Name**.
The Summary tab is displayed.
5. Under **Manage**, click **Applications > UCC**.
The UCC page is displayed in the **List** view.

UCC Dashboard

The banner in the header pane shows the following details:

- **Calls**—Displays the total number of calls that have ended.
- **Good**—Displays the total number of good calls that have ended.
- **Fair**—Displays the total number of fair calls that have ended.
- **Poor**—Displays the total number of poor calls that have ended.
- **Unknown**—Displays the total number of calls whose status is unknown.



-
- For the ALG like Skype SDN, the end-to-end Mean Opinion Score (MOS) is used. A good call has a MOS of more than 3.5, a fair call has a MOS in the range of 2.0 to 3.5, a poor call has a MOS of less than 2.0, and an unknown call does not have a MOS.
 - Wi-Fi Calling calls are not tracked. Wi-Fi Calling calls are not assigned an UCC RTPA score and are categorized as unknown.
-

By comparing the call quality and client health score, you can find out if the wireless network was the reason for poor quality of VOIP calls. A poor value of the client health indicates that the issue is at the wireless network side. In that case, go to **Overview > AI Insights** page in the wireless **Client Details** page and check if the client is dwelling on 2.4 GHz band. If the client is dwelling on 2.4 GHz band, configure the VOIP Wireless LAN to 5 GHz band.

If there are no client insights in the **AI Insights** page, you must check for the following AI Insights in the site context:

- **Access Points were impacted by high 5 GHz usage**
- **Access Points impacted by high 2.4 GHz usage**
- **Access Points had an excessive number of channel changes**

Summary View

The **Summary** view in the **Applications > UCC** page provides the following charts:

- **Calls**—Displays the chart of all, good, fair, poor, or unknown calls. Chart can be viewed by Health, SSID, Protocol, Operating System, Session Type, or Quality. In any chart, hover your mouse over any segment of the chart to view additional information.
- **Access Points**—Displays the chart of access points. Chart can be viewed by Poor Quality % or Most Calls. Use **Show More** to view more details of the calls.
- **Clients**—Displays the chart of clients. Chart can be viewed by Poor Quality % or Most Calls. Use **Show More** to view more details of the calls.

The **Show More** option in the **Clients** chart displays the following details of the calls:

Table 9: *Clients with Calls*

| Parameter | Description |
|------------------------------|---|
| Client Name | Displays the name of the client. |
| Calls Total | Displays the total number of calls from the client. |
| Calls Good | Displays the total number of good calls from the client. |
| Calls Fair | Displays the total number of fair calls from the client. |
| Calls Poor | Displays the total number of poor calls from the client. |
| Calls Poor Percentage | Displays the percentage of poor calls from the client. |
| Calls Unknown | Displays the total number of unknown calls from the client. |

Hover your mouse over any row in the list to view additional information.

List View

The **List** view in the **Applications > UCC** page provides a variety of lists that allow you to assess the quality of calls in the network. The banner in the header pane shows the following details:

- **Calls**—Displays the total number of calls that have ended.
- **Good**—Displays the total number of good calls that have ended.
- **Fair**—Displays the total number of fair calls that have ended.
- **Poor**—Displays the total number of poor calls that have ended.
- **Unknown**—Displays the total number of calls whose status is unknown in the last 5 minutes.

The **Calls** list displays the following details of the calls:

Table 10: *Call Details*

| Parameter | Description |
|-------------------|--|
| From | Displays the device originating the call. |
| To | Displays the device receiving the call. |
| Start Time | Displays the date and time when the call originated. |
| Duration | Displays the duration of the call. |

Table 10: Call Details

| Parameter | Description |
|----------------|---|
| State | Displays the state of the call. Possible values are: <ul style="list-style-type: none">■ Active■ Success■ Terminated |
| Quality | Displays the quality of the call. Possible values are: <ul style="list-style-type: none">■ Good■ Fair■ Poor■ Unknown |
| AP Name | Displays the name of the AP. |
| Client | Displays the name of the client. |



The Call Detail Record (CDR) for FaceTime and Skype for Business calls may be incorrect. The CDR for a Facetime call may be empty or it may display the quality of the call as **unknown**. Duplicate CDRs may be created for a Skype for Business call.

Client Insights: Traffic Pattern Visibility

The **Application** page displays the **Visibility** tab.

The **Visibility** dashboard provides a summary of client traffic and their data usage to and from applications, and websites. You can use this data to analyze the client traffic flow using the graphs displayed in the **Visibility** dashboard. This data helps users to troubleshoot any traffic issues for any specific client. The tab consists of a list view and a graph view. The **Visibility** dashboard displays metrics and graphs related to client traffic flow in the following sections:

- **Applications**
- **Websites**

Viewing Visibility Dashboard

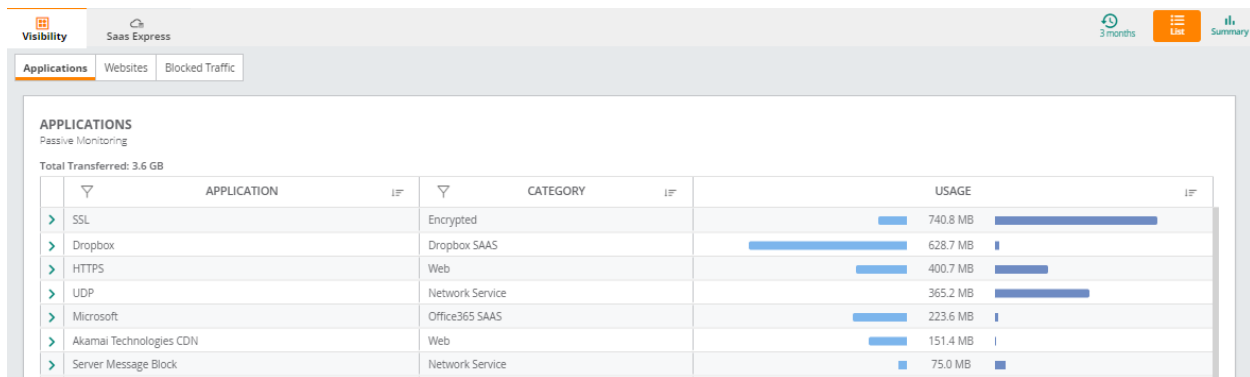
To view the **Visibility** dashboard, complete the following steps:

1. In the **Aruba Central** app, set the filter to one of the options under **Groups** or **Sites**.
For all devices, set the filter to **Global**. The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Applications**.
The visibility dashboard is displayed.

The **Visibility** dashboard displays metrics and graphs related to client traffic flow in the following sections:

- **Applications**
- **Websites**
- **Blocked Traffic**

Figure 13 *Visibility dashboard at the global level*



Graph View in the Visibility Dashboard

Click the **Summary** icon in the **Visibility** dashboard to view both the applications and websites graphical information:

■ Applications

- **Applications**—The stacked bar graph and the pie chart in this tab displays details of the client traffic flowing to or from the top five classified applications listed on the **Applications** table. The legend below the graphs displays the list of applications to which the traffic flow is detected. Select or deselect the application check box to show or hide the traffic flow data from the pie chart and stacked bar. By hovering the mouse on pie chart and stacked bar, you can view the size of data flowing to and from the application same as displayed in legend.
- **Categories**—The stacked bar graph in this tab displays details of the client traffic flowing to or from the top five classified application categories listed on the **Applications** table. The legend below the graphs displays the list of applications categories to which the traffic flow is detected. Select or deselect the application category check box to show or hide the traffic flow data from the pie chart and stacked bar. By hovering the mouse on pie chart and stacked bar, you can view the size of data flowing to and from the application same as displayed in legend.

■ Websites

- **Reputations**—The stacked bar graph and the pie chart in this tab displays details of client traffic flow for the top three reputations listed on the **Websites** table. The legend displays the list of websites based on its reputation, to which the traffic flow is detected. Select or deselect the reputation check box to show or hide the data from the pie chart and stacked bar. By hovering the mouse on pie chart and stacked bar, you can view the size of data flowing to and from each of the websites that are categorized based on reputation.
- **Web Categories**—The stacked bar graph and the pie chart in this tab displays details of client traffic flow for the top five web categories listed on the **Websites** table. Select or deselect the web category check box to show or hide the data from the pie chart and stacked bar. You can view the size of data flowing to and from each of the web categories by hovering the mouse on both the stacked bar graph and pie chart. The legend below the graphs displays the list of websites based on its reputation, to which the traffic flow is detected.

Figure 14 *Visibility dashboard in summary view*



- The Applications (Apps) and Web Categories charts are also displayed in the **Applications** pages for the Group, Site, APs, and Gateways levels.
- Application Visibility data is updated every 0th minute of every hour. The data population on the **Applications > Visibility** dashboard may be delayed by an hour when compared to the Application Visibility data displayed in the **Applications** pages for the Group, Site, APs, and Gateways levels.
- To view client traffic details, ensure that the DPI access rules are enabled on the Instant AP device.



Device Issues

The following section provides details on the typical issues you might face with devices provisioned and managed in the Aruba Central network and the steps to help troubleshoot these issues.

APs are not seen in the Aruba Central Network

Aruba Central validates device connectivity by the network Web socket connection that the device maintains with Aruba Central. If there is no communication of state information from the device for more than 5 minutes, Aruba Central marks the device as offline and the device is not configurable. You must also add device subscription licenses to enable the AP to appear in the Aruba Central network.

If the AP moves to a new network and the new connected Virtual Controller is not licensed, the AP is not shown in the network. For an AP to show up in Aruba Central, you must make sure that the MAC address and the serial number of the AP is added in the device inventory and also the AP is licensed in the inventory. Even after adding the device inventory, if the AP is not showing up in Aruba Central you must verify if the following ports and URLs are allowed by the firewall at the customer's site:

- TCP Port 443
- TCP Port 80
- UDP Port 123
- activate.arubanetworks.com

- device.arubanetworks.com
- rcs-m.central.arubanetworks.com (console)
- pool.ntp.org (time server)

If all the ports and URLs are allowed by the firewall and you are still unable to see the AP in Aruba Central, raise a ticket with the Aruba Technical Support.

Devices are Offline in the Aruba Central Network

If there is a network outage or the device loses Web socket connection to Aruba Central at the customer site, the device goes offline and is unable to communicate with Aruba Central. Apart from network issues, there are a few physical issues that could also cause the device to go offline.

- The LEDs on the AP are turned OFF.
- System LED lights are blinking in green or red—Depending on the warning and error messages the color of the LED lights change from green to red.
- Bad Ethernet port—If the Ethernet port on the AP has gone bad or the cable itself has some issue.
- Cable falling off—The AP is so heated up and has caused some physical damage. The AP shuts down automatically and reboots again because of the thermal issue.
- PoE issue—An AP is powered up either through an adapter or through the Ethernet port. There are two scenarios where an AP might not come up:
 - The Ethernet port does not provide sufficient power to the AP.
 - The Uplink port or PoE port is disabled or not configured correctly.

The **Switch Details** page will display PoE alerts and the status of the port that is connected to the AP.

In order to solve these physical issues of a device, you must issue a direct Return Merchandise Authorization (RMA).

Under Standard Warranty or Limited Lifetime Warranty (LLW) hardware RMAs are handled through best effort. Out of warranty and/or expired contract hardware requires Service Renewal prior to an RMA. TAC only handles defective RMAs under proper entitlement.

Cabling Issues in Switch

The **Cable Test** enables testing of the electrical connections in the switch cable. It checks whether the cabling is conformed to the cabling plans and is of expected quality. It is useful for production and maintenance.



Cable Test is supported only from ArubaOS Switch version 16.05.000 or later. **Cable Test** is not supported in Aruba CX switches.

Cable Test

To perform a **Cable Test** on a switch, complete the following steps:

1. In the **Aruba Central** app, select one of the following options:
 - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.

- To select a switch in the filter:
 - a. Set the filter to **Global**.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click a switch listed under **Device Name** for which you want to perform the cable test.
The dashboard context for the switch is displayed.
- 2. Under **Analyze > Tools**, click **Device Check**.
- 3. From the **Device Type** drop-down list, select **Switch**.
- 4. From the **Sources** drop-down list, select a source.
- 5. From the **Test** drop-down list, select **Cable Test**.
- 6. From the **Port** drop-down list, enter a port number.
- 7. Click **Run**. The output is displayed in the **Cable Test Results** section.



- By default, the **Device Type** is set to **Switch** if a switch is configured in the data path, else a warning is displayed.
- The action will cause a loss of link on all tested ports and will take several seconds per port to complete.
- Enter port numbers and/or port ranges separated by commas. For stacking switch, enter member id/port number.

Figure 15 *Cable Test-Device Output*

CABLE TEST RESULTS

=== Troubleshooting session started ===

COMMAND=clear cable-diagnostics

Status=SUCCESS

COMMAND=test cable-diagnostics 10

Status=SUCCESS

Executing the 'show cable-diagnostics' command to view the results

Reboot an IoT Sensor

Users can reboot an IoT sensor to troubleshoot and conduct event log analysis, renegotiate LLDP power supplied, apply new role configuration, or for enhanced serviceability.

The **PoE Bounce** test reboots an IoT sensor port interface and forces a client to re-initiate a DHCP request.



PoE Bounce is supported only from ArubaOS Switch version 16.04.000 or later.

PoE Bounce

To perform a **PoE Bounce** test on a switch, complete the following steps:

1. In the **Aruba Central** app, select one of the following options:

- To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
- To select a switch in the filter:
 - a. Set the filter to **Global**.
 - b. Under **Manage**, click **Devices > Switches**.
A list of switches is displayed in the **List** view.
 - c. Click a switch listed under **Device Name** for which you want to perform the PoE bounce test.
The dashboard context for the switch is displayed.
- 2. Under **Analyze > Tools**, click **Device Check**.
- 3. From the **Sources** drop-down list, select a source.
- 4. From the **Test** drop-down list, select **PoE Bounce**.
- 5. From the **Port** drop-down list, enter a port number.
- 6. Click **Run**. The output is displayed in the **Device Output** section.



-
- By default, the **Device Type** is set to **Switch** if a switch is configured in the data path, else a warning is displayed.
 - Multiple device selection is not allowed at this level.
 - Devices which are already running commands shall not execute newly added commands.
-

Figure 16 *PoE Bounce Test-Device Output*

```

=== Troubleshooting session started ===

16 Apr, 2020, 09:15:06
Test Type: PoE Bounce
Source: [Switch] Core-Switch
[ports] 20

COMMAND=no interface 20 power-over-ethernet
Status=SUCCESS

COMMAND=interface 20 power-over-ethernet
Status=SUCCESS

=== Troubleshooting session completed ===
  
```

Device Troubleshooting with Remote Console

Aruba Central allows you to open a remote console for a CLI session through SSH for a gateway, switch, and access point to troubleshoot device issues. Users with admin roles can access the device directly from the console to debug any device issues.

You can view the already recorded sessions or can create a new session to start troubleshooting your device.



When you create a new session Aruba Central records and saves it for future analysis.




Viewing Recorded Console Sessions

Aruba Central records an ongoing troubleshooting session and saves it for future analysis. You can view and download the session recordings and replay it anytime to diagnose any device issues in the network.

To view the recorded sessions, complete the following steps:

1. In the **Aruba Central** app, select one of the following options:
 - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
 - To select a device in the filter:
 - a. Set the filter to **Global**.
 - b. Under **Manage**, click **Devices**, and then click **Access Points, Switches, or Gateways**.
A list of devices is displayed in the **List** view.
 - c. Click a device listed under **Device Name**.
The dashboard context for the device is displayed.
2. Under **Analyze > Tools**, click the **Console** tab.
The **Remote Console Session** page is displayed and by default, the **New Session** tab is selected.
3. Click the **Saved Sessions** tab.
4. From the **Device Type** drop-down list, select the device type.
5. Select the device and click **View Recorded Session**.
The **Remote Console** terminal appears and starts playing the most recent recorded session.

You can perform the following tasks from the **Remote Console** section:

- Click  to open the **Device** pane to see the list of devices that have active sessions.
- Click the device drop-down list at the right corner to select the session that you want to play. You can also delete a session by clicking the delete  icon available next to each session name.
- Click the maximize icon to maximize the remote console pane.
- Click the download  icon to download a recorded session and replay for offline analysis.

AI Insights

The following section describes the anomalies observed in the Aruba Central network that might affect the quality of the overall network performance and the steps to help troubleshoot these issues.

AI Insights Anomalies

The **AI Insights** dashboard displays a report of network events that could possibly affect the quality of the overall network performance. These are anomalies observed at the access point, connectivity, and client level for the selected time range. Each insight provides specific details on the occurrences of these events for easy debugging.

In this release the insights are classified under three categories:

- **Connectivity**—Issues related to the wireless connectivity in the network.
- **Wireless Quality**—Issues related to the RF Info or RF Health in the network.
- **Availability**—Issues related to the health of your network infrastructure and the devices in the network such as, APs, switches, and gateways.

To launch the **AI Insights** dashboard, complete the following steps:


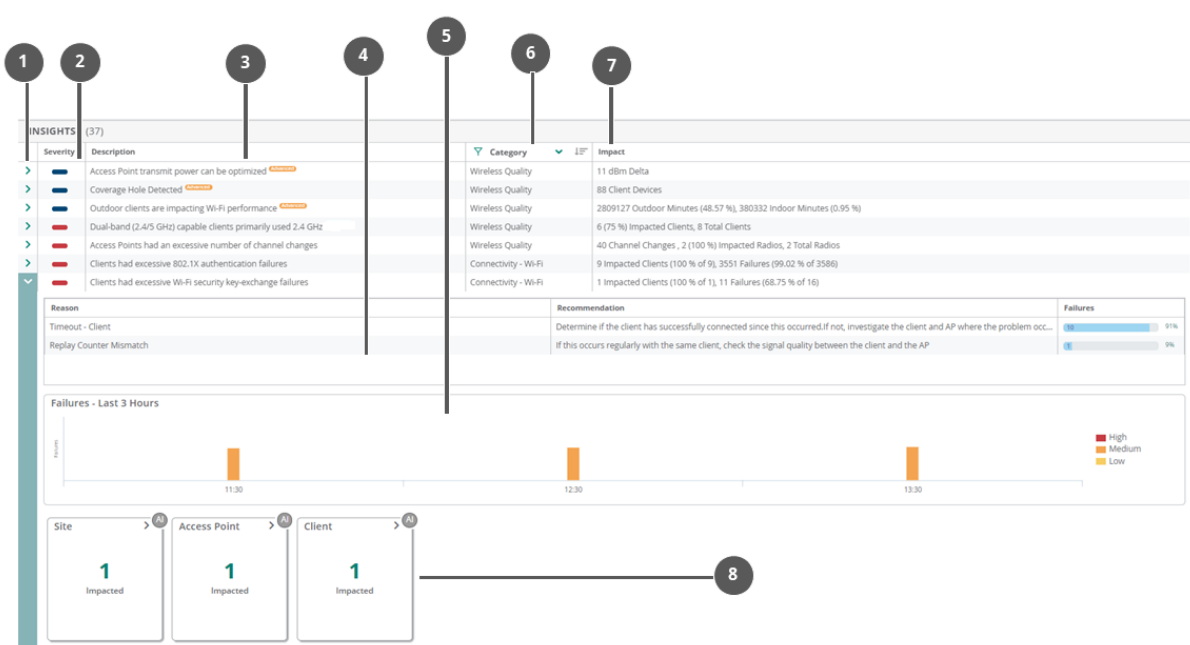
1. In the **Aruba Central** app, set the filter to **Global**. The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Overview > AI Insights**.
The Insights table is displayed. AI Insights listed in the dashboard are sorted from high priority to low priority.
3. Click  against each insight to view the further details.

Figure 17 *Insight Details*



| Callout Number | Description |
|----------------|---|
| 1 | Click this arrow to expand any specific insight to view further details. |
| 2 | Displays the insight severity, using the following colors: <ul style="list-style-type: none"> ■ Red—High priority ■ Orange—Medium priority ■ Yellow—Low priority |
| 3 | Short description of the insight. |
| 4 | Insight Summary displays the reason why the insight was generated along with recommendation. It also shows the number and percentage of failures that occurred against each failure reason. The reasons are classified into: <ul style="list-style-type: none"> ■ Static—These reasons rely on Aruba's domain expertise. |

| Callout Number | Description |
|----------------|---|
| | <ul style="list-style-type: none"> Dynamic—These reasons are generated based on error codes that is received from infrastructure devices. |
| 5 | Time Series graph is a graphical representation of the failure percentage or failure events that occurred for the selected time range. The entries in each time series bar can be customized to highlight a specific entry by clicking on it. Only one specific entry can be highlighted at a time. |
| 6 | Category of the insight. |
| 7 | Short description of the impact. |
| 8 | Cards display additional information specific to each insight. Cards might vary for each insight based on the context the insight is accessed from. |

All AI Insights generated are listed in the **Global > AI Insights** dashboard. Alternatively, AI Insights for a specific site, device, or client can be viewed by selecting the respective context.



AI Insights are displayed for a selected time period based on the time selected in the **Time Range Filter**. You can select one of the following: **3 Hours**, **1 Week**, **1 Day**, or **1 Month**.

Figure 18 *AI Insights Dashboard*

| INSIGHTS (37) | Severity | Description | Category | Impact |
|---------------|----------|--|-----------------------------|--|
| > | High | Access Point transmit power can be optimized | Wireless Quality | 11 dBm Delta |
| > | High | Coverage Hole Detected | Wireless Quality | 88 Client Devices |
| > | High | Outdoor clients are impacting Wi-Fi performance | Wireless Quality | 2809127 Outdoor Minutes (48.57 %), 380332 Indoor Minutes (0.95 %) |
| > | High | Dual-band (2.4/5 GHz) capable clients primarily used 2.4 GHz | Wireless Quality | 6 (75 %) Impacted Clients, 8 Total Clients |
| > | High | Access Points had an excessive number of channel changes | Wireless Quality | 40 Channel Changes, 2 (100 %) Impacted Radios, 2 Total Radios |
| > | High | Clients had excessive 802.1X authentication failures | Connectivity - Wi-Fi | 9 Impacted Clients (100 % of 9), 3551 Failures (99.02 % of 3586) |
| > | High | Clients had excessive Wi-Fi security key-exchange failures | Connectivity - Wi-Fi | 1 Impacted Clients (100 % of 1), 11 Failures (66.75 % of 16) |
| > | High | Clients had problems authenticating with the Captive Portal | Connectivity - Wi-Fi | 1 Impacted Clients (100 % of 1), 6 Failures (100 % of 6) |
| > | High | Access Points had a high number of reboots | Availability - Access Point | 5 (62.5 %) Impacted Access Points, 8 Total Access Points, 5 Reboots. |
| > | High | DNS server(s) rejected a high number of queries | Connectivity - Wi-Fi | 606 (88.08 %) Failed Requests, 688 Total Requests |
| > | High | DNS request/responses were significantly delayed | Connectivity - Wi-Fi | 14956 Average Delay (ms) |
| > | High | PVOS Switches had unusually high CPU utilization | Availability - Switch | 4 (40 %) Impacted Switches, 10 Total Switches |
| > | High | PVOS Switches had unusually high memory usage | Availability - Switch | 4 (40 %) Impacted Switches, 10 Total Switches |
| > | High | Gateways had unusually high CPU utilization | Availability - Gateway | 13 Gateways |
| > | High | Gateways had high memory usage | Availability - Gateway | 1 Gateways |
| > | High | Gateway tunnels failed to get established | Availability - Gateway | 5 Tunnels Down |
| > | High | Clients had a significant number of Low SNR minutes | Wireless Quality | 10 (40 %) Impacted Clients, 25 Total Clients |
| > | High | Clients had DHCP server connection problems | Connectivity - Wi-Fi | 3 Impacted Clients (33.33 % of 9), 1851 Failures (95.27 % of 1943) |
| > | High | Clients had a high number of Wi-Fi Association failures | Connectivity - Wi-Fi | 3 Impacted Clients (37.5 % of 8), 9 Failures (9.57 % of 94) |
| > | High | Clients had an unusual number of MAC authentication failures | Connectivity - Wi-Fi | 4 Impacted Clients (36.36 % of 11), 21 Failures (29.17 % of 72) |
| > | High | Access Points had unusually high CPU utilization | Availability - Access Point | 3 (30 %) Impacted Access Points, 10 Total Access Points |
| > | High | Access Points were impacted by high 2.4 GHz usage | Wireless Quality | 8 (40 %) Impacted Access Point Radios, 20 Total Access Point Radios |
| > | High | Access Points were impacted by high 5 GHz usage | Wireless Quality | 8 (40 %) Impacted Access Point Radios, 20 Total Access Point Radios |
| > | High | Access Point radios changed their transmit power frequently | Wireless Quality | 357 Power Changes, 2 (50 %) Impacted Radios, 4 Total Radios |
| > | High | DNS queries failed to reach or return from the server | Connectivity - Wi-Fi | 1146 (6.78 %) Lost Requests, 16900 Total Requests |
| > | High | PVOS Switches had an unusual number of port errors | Availability - Switch | 1 (20 %) Impacted Switches, 5 Total Switches |
| > | High | Access Points with unusually high memory usage were found | Availability - Access Point | 10 (10.1 %) Impacted Access Points, 99 Total Access Points |
| > | High | Information (telemetry) was not received from APs/Radios | Availability - Access Point | 21 (1.87 %) Impacted Access Point Radios, 1124 Total Access Point Radios |

For more information, see [AI Insights Dashboard](#).

Network Check

The following section provides details on the typical network issues you might face with the devices managed by Aruba Central network and the steps to help troubleshoot these issues.

Network Performance

To identify the network speed, you must perform a network check on the APs in the network. A network check aims to identify, diagnose, and debug issues detected in an Aruba Central-managed network. The **Network Check** tab on the **Tools** page captures the troubleshooting utilities that are used to test a network entity and collect results based on your selection.

The following tests are available for APs to troubleshoot issues pertaining to WLAN network connections:

- [Ping Test](#)
- [NSLookup](#)
- [Traceroute](#)
- [TCP Test](#)
- [HTTP Test](#)
- [HTTPS Test](#)
- [Speed Test \(iPerf\)](#)

Ping Test

Sends ICMP echo packets to the hostname or IP addresses of the selected devices to check for latency issues.

To perform a ping test on APs, complete the following steps:

1. In the **Aruba Central** app, select one of the following options:
 - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
 - To select a device in the filter:
 - a. Set the filter to **Global**.
 - b. Under **Manage**, click **Devices > Access Points**.
A list of access points is displayed in the **List** view.
 - c. Click an access point listed under **Device Name** for which you want to perform the ping test.
The dashboard context for the access point is displayed.
2. Under **Analyze > Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Access Point**.
4. From the **Test** drop-down list, select **Ping Test**.
5. From the **Sources** drop-down list, select source(s). You can select multiple APs.
6. From the **Destination Type** drop-down list, select one of the following:
 - **Hostname/IP Address**—Enter the hostname or IP address.
 - **Client**—Select a client.
7. To use additional parameters, click **Show Additional Test Settings** and enter values in the following fields:



Show Additional Test Setting is not displayed when a **Test** type is not selected.

- a. In the **Packet Size** field, enter the packet size in order to capture and store the data packet to analyze network issues at a later stage. The range is from 10 to 65507 bytes.
 - b. In the **Count** field, enter the count. The value should be between 1 to 2147483647.
 - c. Select **Port** from the **Source Interface** drop-down list and select the port number.
8. Click **Run**. The output is displayed in the **Device Output** section.

Figure 19 Ping Test—Device Output

```

=== Troubleshooting session started ===

=====
Output Time: 2020-04-16 10:04:04 UTC
TCP Test from CT0469457 to 8.8.8.8 has Failed
Port Number : 1
Timeout: 9
Failure Reason: connect timeout

=== Troubleshooting session completed ===
=== Troubleshooting session started ===

17 Apr, 2020, 11:21:44
Test Type: PING
Source: [Access Point] 94:b4:0f:ca:51:f8
Target: [CLIENT] b8:27:eb:a7:71:4a

```

As mentioned in the steps, you can ping a client, gateway, or a WAN IP address to identify the wireless speed. When you ping the client, it sends the packets at a specified speed. If the network is slow, the time taken for the transfer will be high and some packets may get lost in the process. This behavior indicates that there is an issue between the AP and the client. Hence, when you notice that the network is slow, execute a ping test in **Tools** and check if the ping test is optimal. Similarly, you can choose your destination to be a gateway or a WAN/IP address. The tests show the same network speed from an AP to a gateway or from an AP to an outside WAN.

NSLookup

NSLookup is a program to query Internet domain name servers. To perform a NSLookup test on APs, complete the following steps:

1. In the **Aruba Central** app, select one of the following options:
 - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
 - To select a device in the filter:
 - a. Set the filter to **Global**.
 - b. Under **Manage**, click **Devices > Access Points**.
A list of access points is displayed in the **List** view.
 - c. Click an access point listed under **Device Name** for which you want to perform the traceroute test.
The dashboard context for the access point is displayed.
2. Under **Analyze > Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Access Point**.
4. From the **Test** drop-down list, select **NSLOOKUP**.
5. From the **Sources** drop-down list, select source(s). You can select multiple APs.
6. Enter the hostname or IP address.
7. To use additional parameters, click **Show Additional Test Settings** and in the **DNS Server** field

enter the hostname or IP address.



Show Additional Test Settings is not displayed when a **Test** type is not selected.

8. Click **Run**. The output is displayed in the **Device Output** section.

Traceroute

Tracks the packets routed from a network host.

To perform a traceroute test on APs, complete the following steps:

1. In the **Aruba Central** app, select one of the following options:
 - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
 - To select a device in the filter:
 - a. Set the filter to **Global**.
 - b. Under **Manage**, click **Devices > Access Points**.
A list of access points is displayed in the **List** view.
 - c. Click an access point listed under **Device Name** for which you want to perform the traceroute test.
The dashboard context for the access point is displayed.
2. Under **Analyze > Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Access Point**.
4. From the **Test** drop-down list, select **Traceroute**.
5. From the **Sources** drop-down list, select source(s). You can select multiple APs.
6. Enter the hostname or IP address.
7. Click **Run**. The output is displayed in the **Device Output** section.

Figure 20 Traceroute Test—Device Output

```
=====
Output Time: 2020-04-23 05:18:45 UTC

COMMAND=traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 38 byte packets
 1 * * *
 2 10.8.131.254 1.381 ms 1.052 ms 1.046 ms
 3 10.8.4.10 1.099 ms 1.033 ms 1.050 ms
 4 10.8.0.1 1.348 ms 1.308 ms 1.319 ms
 5 104.36.250.1 1.491 ms 1.419 ms 1.393 ms
 6 104.36.251.248 18.008 ms 21.580 ms 27.538 ms
 7 104.36.249.246 1.678 ms 1.543 ms 1.532 ms
 8 206.223.116.21 2.100 ms 2.045 ms 2.056 ms
 9 108.170.242.225 2.663 ms 108.170.243.1 4.004 ms 108.170.242.241 3.855 ms
10 72.14.239.97 2.645 ms 209.85.252.251 3.249 ms 74.125.252.151 3.240 ms
11 8.8.8.8 2.496 ms 2.440 ms 2.559 ms
=== Troubleshooting session completed ===
```

TCP Test

Sends packets to the host such as an FTP server, and tries to establish a connection and exchanges data. If the FTP server returns a response, the issue could be isolated to the client device.

To perform a TCP test on APs, complete the following steps:

1. In the **Aruba Central** app, select one of the following options:
 - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.

The dashboard context for the selected filter is displayed.

- To select a device in the filter:
 - a. Set the filter to **Global**.
 - b. Under **Manage**, click **Devices > Access Points**.
A list of access points is displayed in the **List** view.
 - c. Click an access point listed under **Device Name** for which you want to perform the TCP test.

The dashboard context for the access point is displayed.

2. Under **Analyze > Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Access Point**.
4. From the **Test** drop-down list, select **TCP Test**.
5. From the **Sources** drop-down list, select source(s). You can select multiple APs.
6. Enter a valid IPv4 address in the **Host** field. Hostname is not supported.
7. Enter the port number in the **Port** field. The port number should be between 1 to 65535.
8. To use additional parameters, click **Show Additional Test Settings** and in the **Timeout** field, to enter the timeout value in seconds.

The value should be between 1 to 10 seconds. The default timeout value is 5 seconds.



Show Additional Test Settings is not displayed when a **Test** type is not selected.

9. Click **Run**. The output is displayed in the **Device Output** section.

Figure 21 TCP Test—Device Output

```
=== Troubleshooting session started ===

=====
Output Time: 2020-04-20 14:05:56 UTC
TCP Test from CNFLK511BQ to 4.4.4.4 has Failed
Port Number : 1
Timeout: 9
Failure Reason: connect timedout
=====

=== Troubleshooting session completed ===
```

CLEAR



The TCP test is supported only from ArubaOS 8.3.0.0 or later versions.

HTTP Test

Sends packets to the HTTP URL and tries to establish a connection and exchange data. If the HTTP website returns a response, the issue could be isolated to the client device.

To perform an HTTP test on APs, complete the following steps:

1. In the **Aruba Central** app, select one of the following options:
 - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

The dashboard context for the selected filter is displayed.

- To select a device in the filter:
 - a. Set the filter to **Global**.
 - b. Under **Manage**, click **Devices > Access Points**.
A list of access points is displayed in the **List** view.
 - c. Click an access point listed under **Device Name** for which you want to perform the HTTP test.
The dashboard context for the access point is displayed.
- 2. Under **Analyze > Tools**, click **Network Check**.
- 3. From the **Device Type** drop-down list, select **Access Point**.
- 4. From the **Test** drop-down list, select **HTTP Test**.
- 5. From the **Sources** drop-down list, select source(s). You can select multiple APs.
- 6. Enter the HTTP URL for which you want to perform the HTTP test, in the **URL** field, For example, `http://hostname` or `http://ipaddress`.
- 7. To use additional parameters, click **Show Additional Test Settings** and in the **Timeout** field, enter the timeout value in seconds.
The value should be between 1 to 10 seconds. The default timeout value is 1 second.



Show Additional Test Settings is not displayed when a **Test** type is not selected.

8. Click **Run**. The test output is displayed in the **Device Output** section.

Figure 22 HTTP Test—Device Output

```

=== Troubleshooting session started ===

=====
Output Time: 2020-04-20 14:18:59 UTC
HTTP Test from CNH8KD00G1 to http://google.com has Passed
Timeout: 9
Download Rate: 6438.257 KB/sec
Download Bytes: 14.0 KB

=== Troubleshooting session completed ===
  
```



The HTTP test is supported only from ArubaOS 8.3.0.0 or later versions. The test support only IPv4 address or domain name in the URL field.

HTTPS Test

Sends packets to the HTTPS URL and tries to establish a connection and exchange data. If the HTTPS website returns a response, the issue could be isolated to the client device. HTTPS is a performance test to identify the time taken to load a web page.

To perform an HTTPS URL test on APs, complete the following steps:

1. In the **Aruba Central** app, select one of the following options:
 - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.

The dashboard context for the selected filter is displayed.

- To select a device in the filter:
 - a. Set the filter to **Global**.
 - b. Under **Manage**, click **Devices > Access Points**.
A list of access points is displayed in the **List** view.
 - c. Click an access point listed under **Device Name** for which you want to perform the HTTPS test.

The dashboard context for the access point is displayed.

2. Under **Analyze > Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Access Point**.
4. From the **Test** drop-down list, select **HTTPS Test**.
5. From the **Sources** drop-down list, select source(s). You can select multiple APs.
6. Enter the HTTPS URL for which you want to perform the HTTPS test, in the **URL** field, For example, `https://URL` or `https://IPv4`.
7. To use additional parameters, click **Show Additional Test Settings** and in the **Timeout** field, enter the timeout value in seconds.
The value should be between 1 to 10 seconds. The default timeout value is 1 second.



Show Additional Test Settings is not displayed when a **Test** type is not selected.

8. Click **Run**. The test output is displayed in the **Device Output** section.

Figure 23 *HTTPS Test—Device Output*

```
=== Troubleshooting session started ===

=====
Output Time: 2020-04-20 14:16:20 UTC
HTTPS Test from CNFLK511F1 to https://google.com has Passed
Timeout: 9
Download Rate: 6176.113 KB/sec
Download Bytes: 13.99 KB

=== Troubleshooting session completed ===
```

CLEAR



If there is an application server running at the customer site and the application server has HTTPS and HTTP service enabled you can run these tests from the AP to the server. Once you run the test, the test status, download rate, and the download bytes indicate the network speed.

Speed Test (iPerf)

Performs a speed test to measure network speed and bandwidth. The speed test diagnostic tool is available only for Instant APs. To perform a speed test, you must provide the iPerf server address, protocol type, and speed test options such as bandwidth.

To execute a speed test on APs, complete the following steps:

1. In the **Aruba Central** app, select one of the following options:
 - To select a group, label, site, or all devices in the filter, set the filter to one of the options under **Groups, Labels, or Sites**. For all devices, set the filter to **Global**.
The dashboard context for the selected filter is displayed.
 - To select a device in the filter:
 - a. Set the filter to **Global**.
 - b. Under **Manage**, click **Devices > Access Points**.
A list of access points is displayed in the **List** view.
 - c. Click an access point listed under **Device Name** for which you want to perform the speed test.
The dashboard context for the access point is displayed.
2. Under **Analyze > Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Access Point**.
4. From the **Test** drop-down list, select **Speed Test (iPerf)**.
5. From the **Sources** drop-down list, select source(s). You can select multiple APs.
6. In the **Host** field, enter a valid hostname.
7. From the **Protocol** drop-down list, select the protocol. The available options are **TCP** or **UDP**.
8. To use additional parameters, click **Show Additional Test Settings** and in the **Options** field, enter the option. For example, bandwidth.



Show Additional Test Settings is not when a **Test** type is not selected.

9. Click **Run**. The test output is displayed in the **Device Output** section.

Figure 24 *Speed Test—Device Output*

```
=== Troubleshooting session started ===
17 Apr, 2020, 11:27:57
Test Type: SPEED_TEST
Source: [Access Point] 94:b4:0f:c9:b8:70
[protocol] udp
[Host] 8.8.8.8

=====
Output Time: 2020-04-17 11:27:58 UTC

COMMAND=speed-test 8.8.8.8 udp 10
% Parse error.

=== Troubleshooting session completed ===
```



While troubleshooting APs, a maximum of 20 APs are listed in the drop-down list. If there are more than 20 APs, use the **Search** option to search for an AP on which you would like to perform diagnostic checks

In addition to the **Network Check** tests, you can also leverage the **Commands** tab to troubleshoot your network performance using the available CLI commands. The **Commands** tab on the **Tools** page lists commands specific to a particular device to test the device entity and collect results based on your selection.

Figure 25 Advanced Device Troubleshooting

The screenshot shows the 'COMMANDS' tab in the Aruba Central interface. At the top, there are three tabs: 'NETWORK CHECK', 'DEVICE CHECK', and 'COMMANDS'. Below the tabs, there's a section for selecting a device type and available devices. The 'DEVICE TYPE' is set to 'Access Point' and 'AVAILABLE DEVICES' is set to '6c:f3:7f:c5:13:b8'. Below this, there's a section for selecting commands from one or more categories. The 'CATEGORIES' list includes 'Logs', 'All Category', 'Wireless', 'Security', 'Central', and 'Custom'. The 'COMMANDS' list includes 'AP Log Conversion', 'AP Log Driver', 'AP Log Wireless', 'AP Log User', 'AP Log VPN Tunnel', and 'AP Log Tunnel Status Management'. There are buttons for 'Add >', '< Remove', and '< Remove All'. The 'SELECTED COMMANDS' section shows 'AP Log All' and 'AP Log AP-Debug'. Below this, there's a section for repeating commands with a 'Repeat' checkbox and 'INTERVAL' and 'TOTAL DURATION' dropdowns. At the bottom, there's a 'RUN' button and a 'RESET' button. A light blue banner at the bottom states: 'Devices which are already running commands shall not execute newly added commands. Output history of device with buffer space issues shall be automatically cleared.'

When a troubleshooting operation is initiated, Aruba Central establishes a session with the devices selected for the troubleshooting operation and displays the output in the **Device Output**.

Figure 26 Command Test—Device Output

The screenshot shows the 'Device Output' section with a 'CLEAR' button in the top right corner. The output text is as follows:

```
=== Troubleshooting session started ===

=====
Output Time: 2020-04-23 05:49:23 UTC

COMMAND=show log debug
Apr 23 05:47:45 awc[2348]: wsc: receive message from cli, len 652
Apr 23 05:47:45 awc[2348]: wsc: receive message type POST_REQUEST(11), payload_type=1
Apr 23 05:47:45 awc[2348]: wsc: receive a post request from CLI, topic state.sync, data len 630.
Apr 23 05:47:45 awc[2348]: wsc: LWS_CALLBACK_SET_MODE_POLL_FD case POLLOUT
Apr 23 05:47:45 awc[2348]: wsc: callback_central(1685) LWS_CALLBACK_SET_MODE_POLL_FD POLLOUT, DispatchInput input_write_id = 4889176
Apr 23 05:47:45 awc[2348]: wsc: insert queue a message to websocket server, use_payloadfile=0, msg_len=649.
Apr 23 05:47:45 awc[2348]: wsc: wsc_service_wd_fd(1789), poll write, device fd 8
Apr 23 05:47:45 awc[2348]: wsc: callback_central(1609) LWS_CALLBACK_CLEAR_MODE_POLL_FD, POLLOUT, dispatcher input_write_id=4889176
Apr 23 05:47:45 awc[2348]: wsc: libwebsocket write send len 649
Apr 23 05:47:45 awc[2348]: wsc: libwebsocket write return n= 649
```

Viewing the Device Output

After you execute troubleshooting commands on the devices, Aruba Central displays the output in the **Device Output** section of the **Tools** page.

The output section displays information, such as list of devices on which the troubleshooting commands were executed, initial timestamp, **Test Type**, **Source**, and **Target**. It also shows the status of the tests as, in progress, complete, and buffer time. If there are multiple devices, select the device for which you want to view the output.

You can perform the following tasks from the **Device Output** section:

- Click **Clear** to clear the output. You can clear the output for a single device or for all devices. The **Clear** option is disabled for read-only users.
- Click the **Search** icon to search for text in the output.
- Click the **Email** icon and click **Send** to send the output as an email. You can also add email recipients in the **CC** field.
- Click **Export** to export the command output as a zip file.
- Click the maximize icon to maximize the device output pane.