Proximity Tracing using Aruba Central and Aruba AirWave

a Hewlett Packard
Enterprise company

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

The following table lists the revisions of this document.

Table 1: *Revision History*

Revision	Change Description
03	Updated the **Data Sent by AirWave to Central** section.
02	Updated the **Prerequisites**, **Configuring the Aruba Central Details in AirWave**, **Licensing for AirWave Customers**, and **Data Sent by AirWave to Central** sections.
01	Initial Publication

Chapter 1
Introduction

Aruba has introduced a new feature in the Aruba Central platform to perform queries for contact and location tracing. Aruba customers can use these features to complement a host of other tools/techniques to address their overall preparedness for return to work initiatives during the ongoing COVD-19 pandemic. The list of contacts and locations provided by this feature will ultimately be used by human contact tracers to interview persons of interest and to prioritize areas for disinfection and deep cleaning.

Aruba AirWave

AirWave is a network management platform that provides a single console where you can monitor, analyze, and configure wired and wireless networks. Irrespective of whether the network is simple, large, complex, or a multi-vendor installation, AirWave makes it easy to monitor the network using features like AppRF, Clarity, and VisualRF.

Aruba Central supports Contact and Location Tracing (CLT) analytics for Campus Wi-Fi customers using AirWave. This feature requires users to sign up for Aruba Central, and then use the AirWave Command-Line Interface to configure the CLT feature to send information to the Central cloud.

This document provides guidelines for setting up an account in Aruba Central, proximity tracing feature in Central, the necessary configuration on AirWave, data sent from AirWave, and firewall requirements. It is a companion document to the Wi-Fi-Based Contact / Location Tracing in Aruba Central. Refer to the Proximity Tracing using Aruba Central tech note for more details on usage of the feature, export options, third-party integrations with BI tools, Exit out features, Privacy Considerations, and Frequently Asked Questions.

Prerequisites

- Aruba AirWave version 8.2.10 or higher

Aruba AirWave 8.2.11.2 supports CLT feature natively. Contact Aruba TAC to apply a patch, if you require support for CLT feature in Aruba AirWave 8.2.10, 8.2.10.1, 8.2.11, and 8.2.11.1 versions.

- Bidirectional access on tcp port (443) for the following URLs:
  - cltanalytics.s3-us-west-2.amazonaws..com
  - nookgw.netinsight.arubanetworks..com

Important Note

The following important points should be taken into consideration before configuring the Contact/Location tracing feature:

- The data from all AirWave customers first comes to S3 buckets in an AWS data center in the US West. The data is rendered in a .csv file and is stored in Aruba's Data Lake platform (S3 buckets on AWS). It is not

associated with Central clusters.

- The data is then converted to the parquet format and sent to the customer-specific home Central clusters distributed across the globe. The data is only temporarily received in S3, and is converted to a format that is amenable to further processing, prior to shipping to the respective Central clusters.
- The data from AirWave is sent daily at midnight (AirWave server time) to the Data Lake server and is processed within 4 hours in the respective Central cluster. The data will be available in Central for 21 days and the first set of data will be deleted only after 21 days. Central will have the data for 21 days for Proximity Tracing.
- AirWave customers will use the Central cluster regionally closer to them (NA customers will use US-2).
- All the processing and storing of data for querying purposes is done in the local Central clusters.
- If your country or organization has restrictions in sending data to the US, it is recommended to contact the respective accounts team for details.
- You need to sign up for this feature in Aruba Central, as the CLT configuration steps in AirWave, requires that you enter the customer ID, e-mail address, and the secret key used in Central.
- Central-on-premises (COP) is not a supported platform.

Steps to Configure Contact and Location Tracing

Listed below are the steps to set up contact and location tracing:

Creating an Evaluation Account in Aruba Central

Setting up AirWave connection in Aruba Central

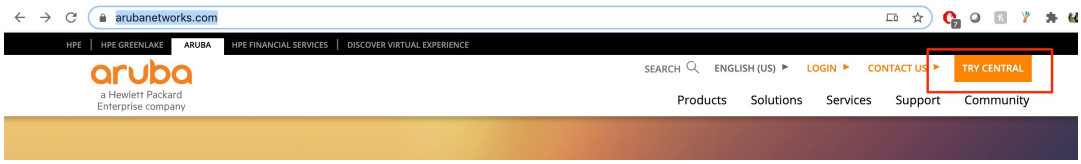
Configuring the Aruba Central Details in AirWave

Chapter 2
Creating an Evaluation Account in Aruba Central

The following section describes how to create an evaluation account in Aruba Central :

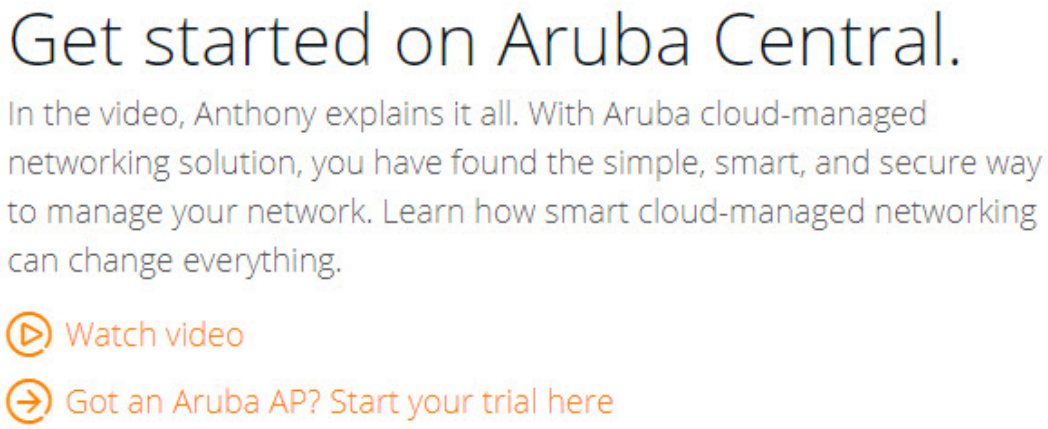
1. Open the Aruba Networks website, https://www.arubanetworks.com/ and click on **Try Central.**

   Figure 1 *Try Central*



2. The page then navigates to **Try Aruba Central**. Scroll down to **Get started on Aruba Central** and **click Got an Aruba AP ? Start your trial here**.

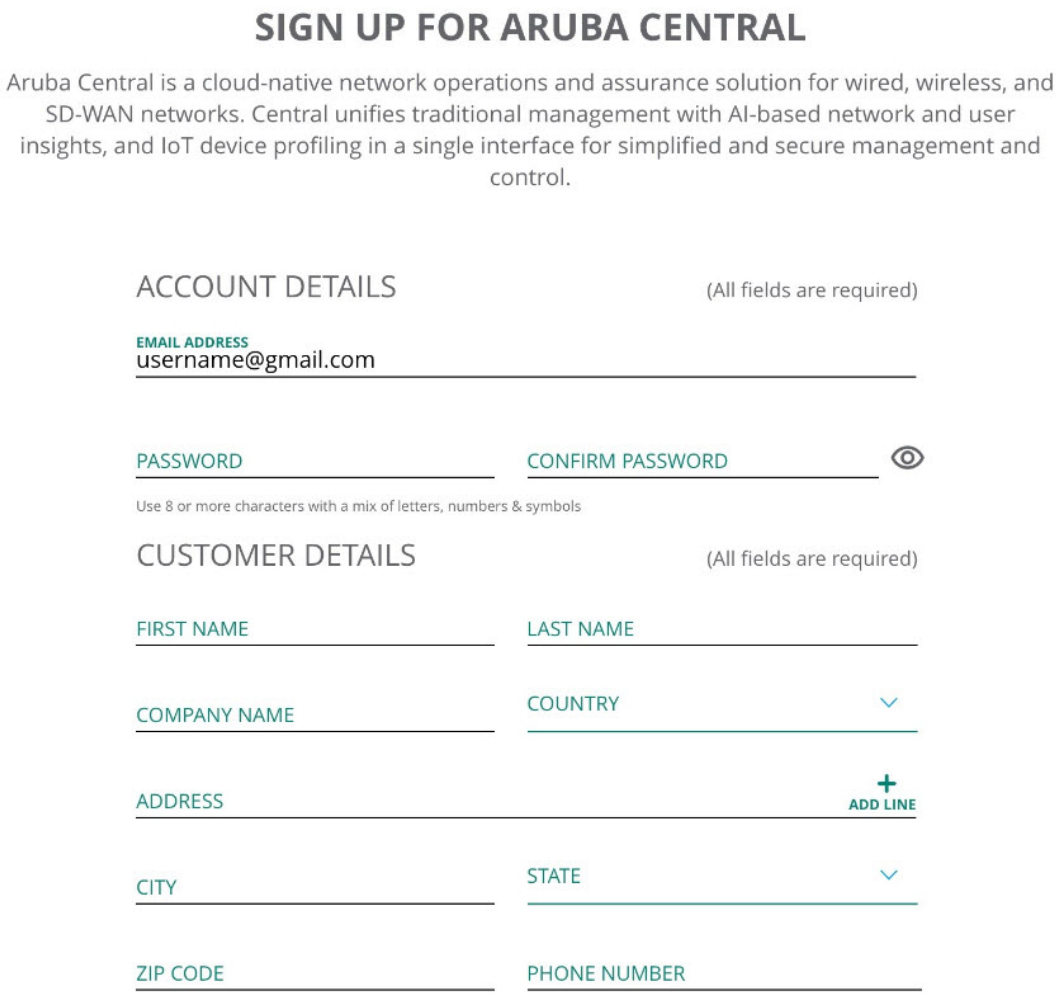
   Figure 2 *Get Started on Aruba Central*



   - You will be redirected to the **Sign Up for Aruba Central** page.

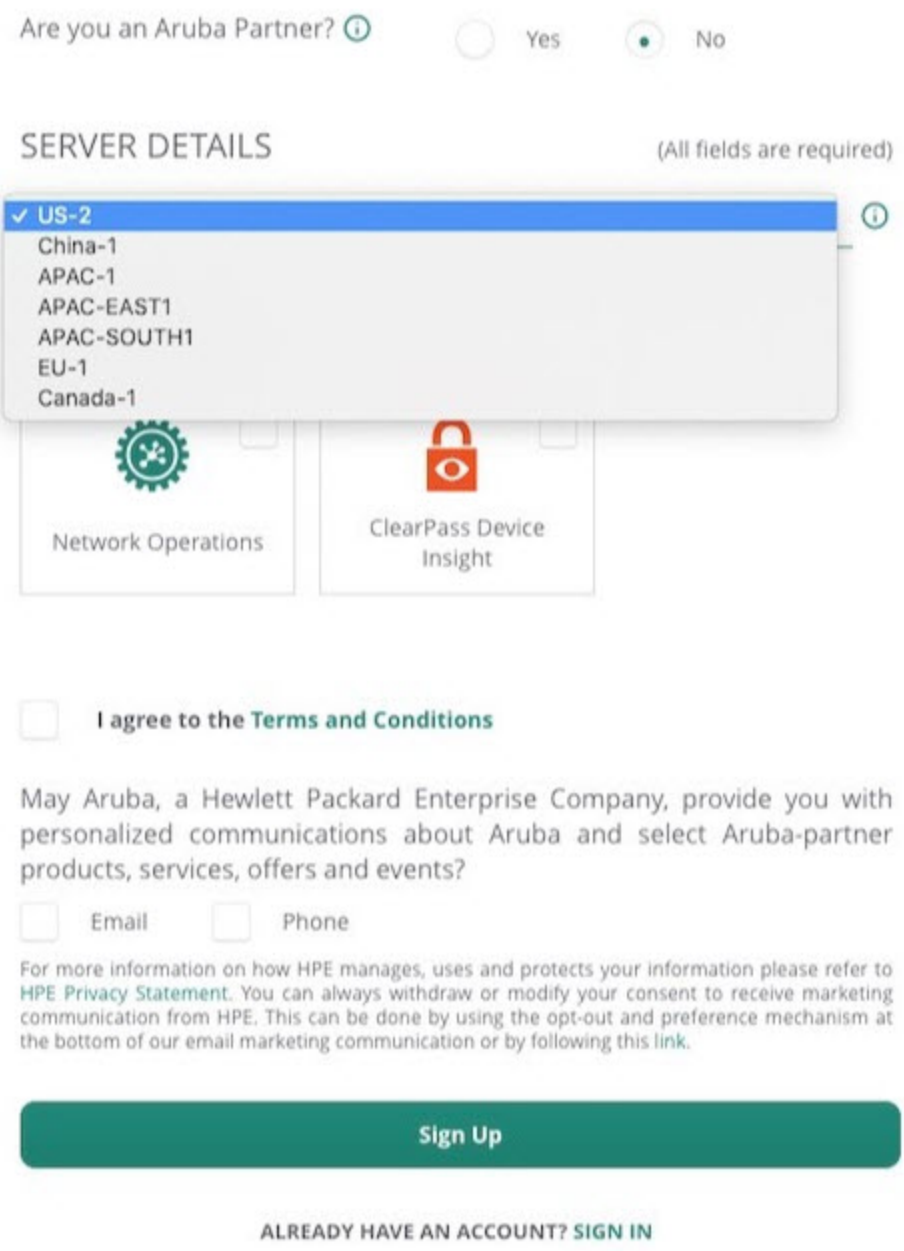
3. Enter a user name and password and fill in the details under **Customer Details** section. If you are already a Central user, it is recommended to use the same account.
4. If you are a Central user for branch office networks (IAP), but an AirWave user for Data center (Controller based and IAP), create a new account for AirWave as both the data sources are different.

Figure 3 *Customer Details Section*



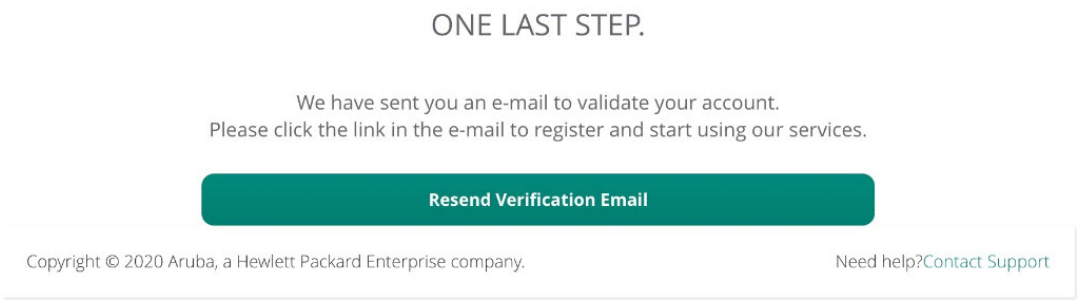
5. Select a Central server based on your region.
6. Select **Network Operations** for **Interested Apps**.
7. Click **I agree to the Terms and Conditions**.

Figure 4 *Server Details*



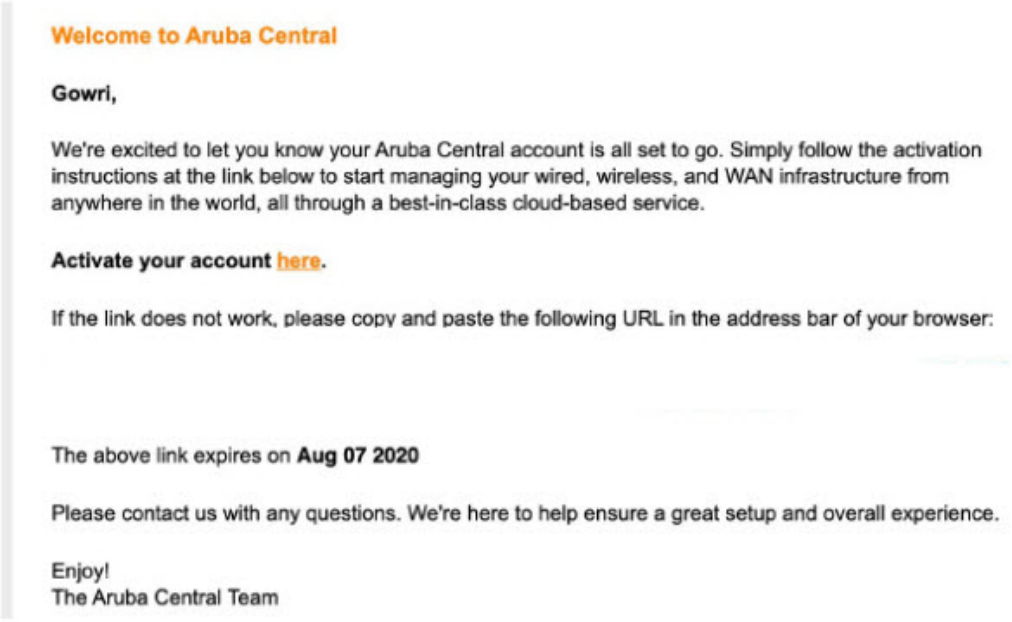
8. Click **Sign Up**.

Figure 5 *Verification Mail*



9. An email is sent to the registered email address . Click **Activate your account here** or click the URL provided to activate the account.

Figure 6 *Account Activation*



Once the account is verified you will be redirected to the Aruba Central page.

10. Select US-2 as server for NA customers and other respective Central servers based on your region.

    The data will be first sent to the Data Lake server in the US and then the processed and packaged data will be sent to the respective regional servers that were chosen while creating the account.

Figure 7 *US-2 Server*

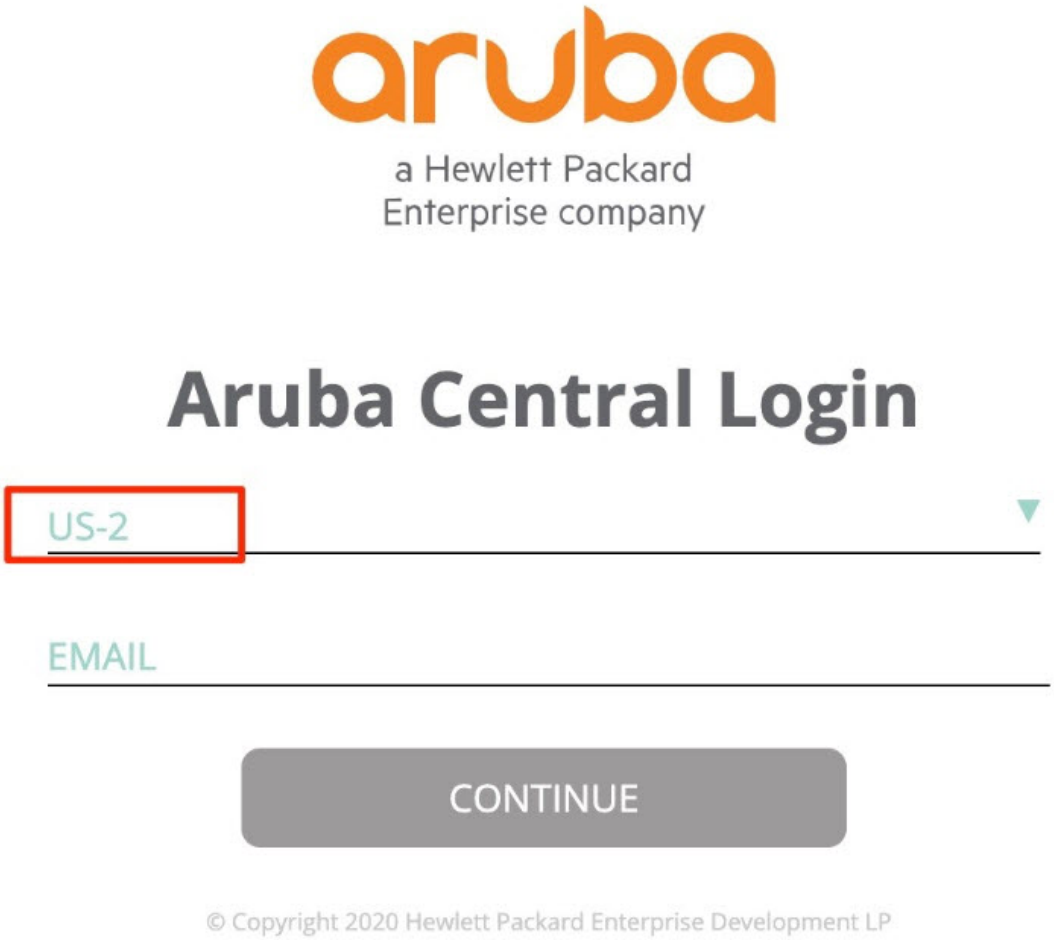
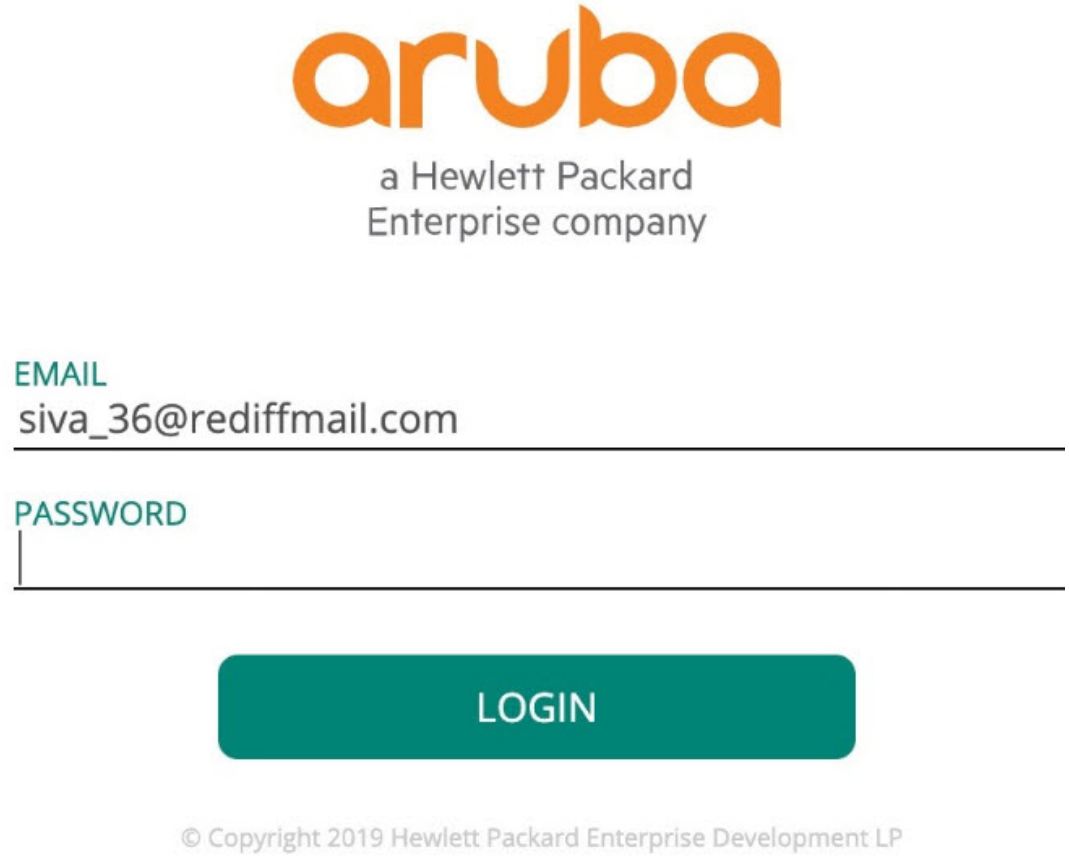


Figure 8 *Aruba Central Login*



11. Log in with the registered credentials, you will be redirected to Aruba Central. Select **Evaluate Now.**

Figure 9 *Evaluate Now to Continue Trial*

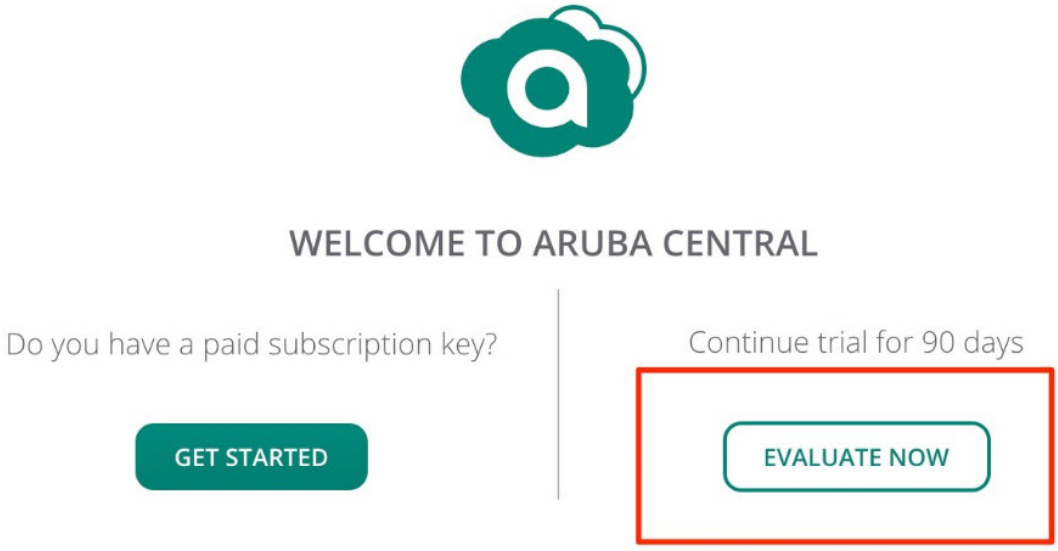


Figure 10 *Welcome Page*

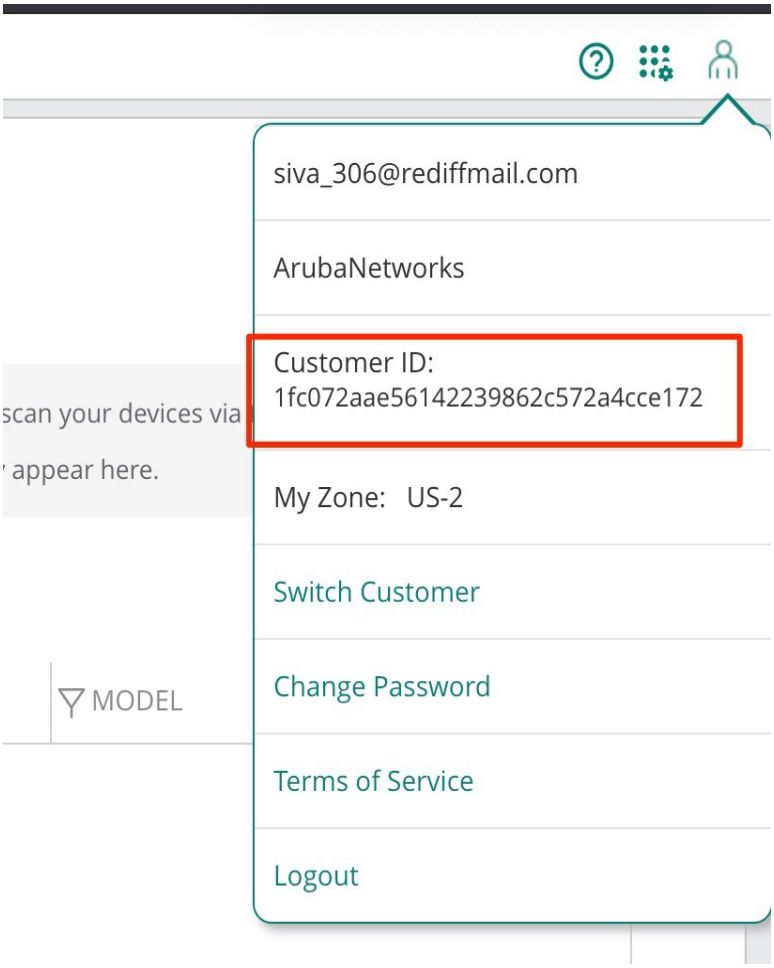
- A 90-day evaluation key will be created . Refer to the Licensing section for more details. The account will be created with a Customer ID.

NOTE

Make note of the customer ID as it is required for AirWave configuration.

- Customer ID is also available under the profile section on the top right corner of the Aruba Central home page.

Figure 11 *Customer ID*

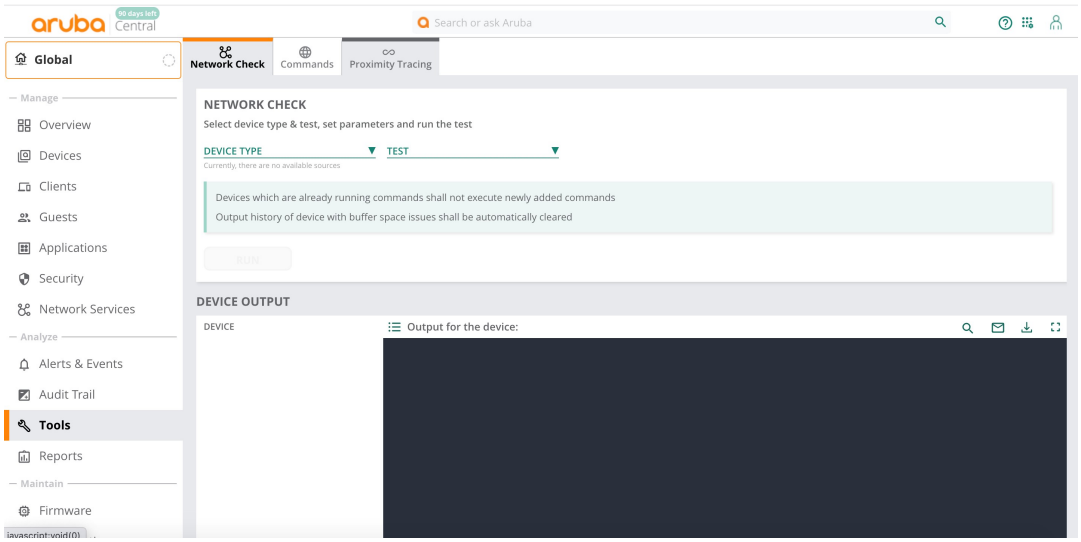


The following section describes how to set up an AirWave connection in Aruba Central:

1. Log in to Aruba Central.
2. In the **Network Operations** app, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
3. Under **Analyze**, click **Tools > Proximity Tracing**.

Figure 12 *Analyze > Tools > Proximity Tracing*

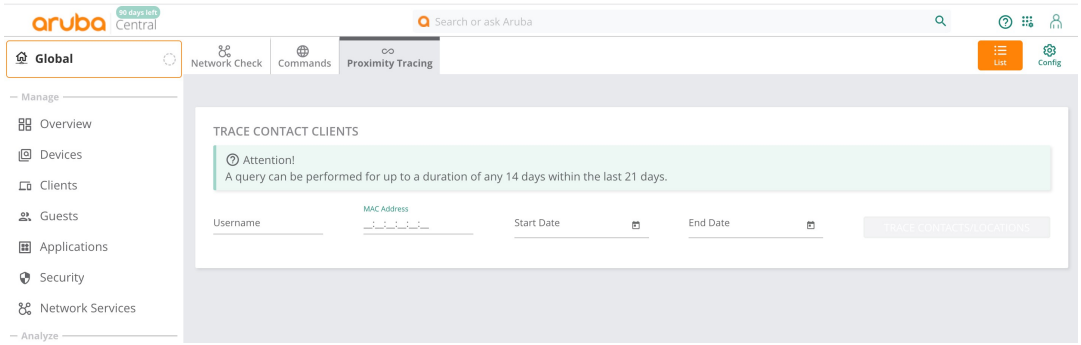


NOTE

For AirWave customers where Central is not the Network Management System (NMS) tool, all other tabs except **Proximity Tracing** do not populate data as device data is not available.

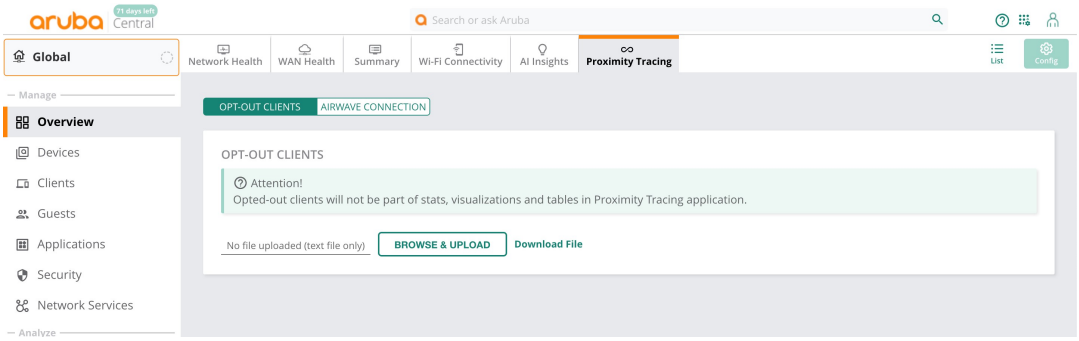
4. Click the config icon.

Figure 13 *Proximity Tracing Tab*



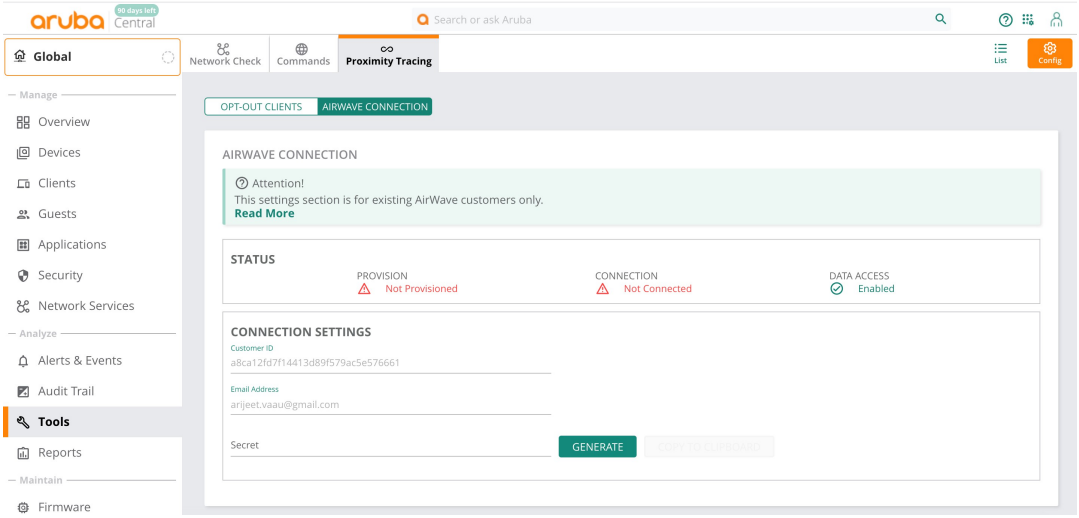
- The **Proximity Tracing** tab displays the following tabs:
  - **Opt-Out Clients**
  - **Airwave Connection**

Figure 14 *Opt-Out Clients and AirWave Connection Tabs*



5. Click the **Airwave Connection** tab. Initially, the **Status** of **Provision** and **Connection** will be displayed in red. The **Data Access** is enabled by default and cannot be modified while provisioning.

Figure 15 *AirWave Connection Tab*

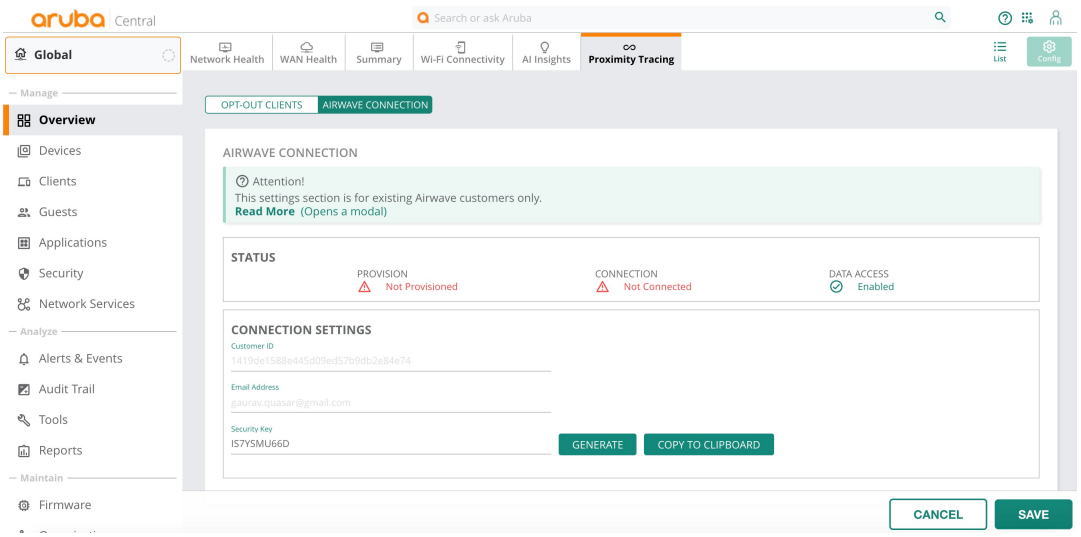


6. The **Customer ID** and **Email address** are auto populated and are not editable. The details will be taken from the logged in user/admin.
7. The **Secret Key** can either be entered or generated.

- The option to **Cancel** or **Save** is available when all the required field details are entered. It is recommended to save the combination securely as it will be used during the AirWave CLI Configuration.
- **Copy to Clipboard** allows you to copy and save the secret key.

Secret key is not viewable after the information is saved.

Figure 16 *Cancel and Save Options*



- The page is refreshed after clicking **Save** . The status of **Provision, Connection,** and **Data Access** changes to **Provisioned**, **Not Connected** and **Enabled** respectively.
  - The status of the **Connection** will be displayed as **Not Connected** until AirWave is configured to send data to Central.
  - Use the **Data Access** toggle switch enable/disable data collection. If **Data Access** in disabled, then Central will stop getting the latest data from AirWave for proximity tracing.

Figure 17 *AirWave Connection Status*

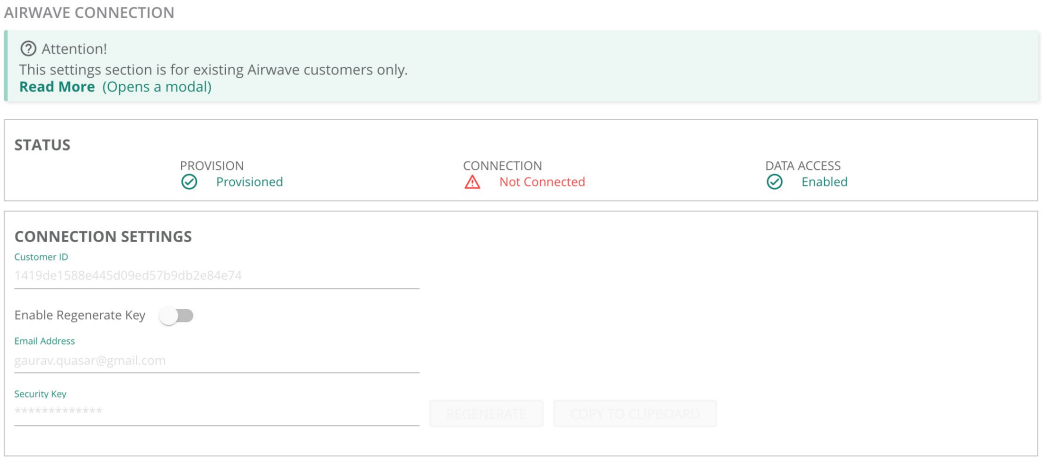


Figure 18 *Disabling Data Access*

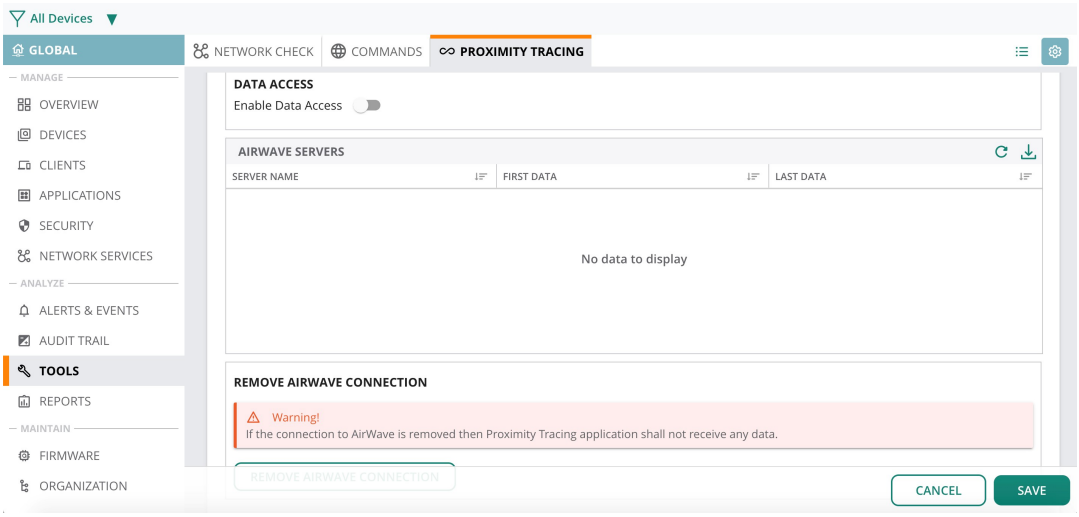
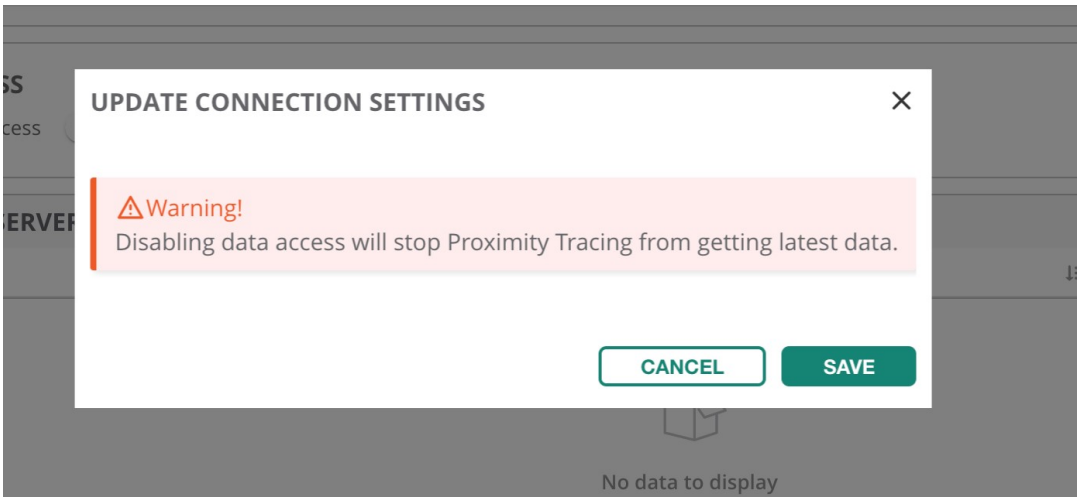


Figure 19 *Prompt when Data Access is Disabled*



- Use the **Enable Regenerate Key** toggle switch to enable the option to change the Secret key and Email address after the initial provisioning . However, this will require an update on all AirWave servers which were already configured to send data. Unless the email address used during original provisioning belongs to an ex-employee, it is recommend to use the same email address during key regeneration.

Figure 20 *Enable Regenerate Key*

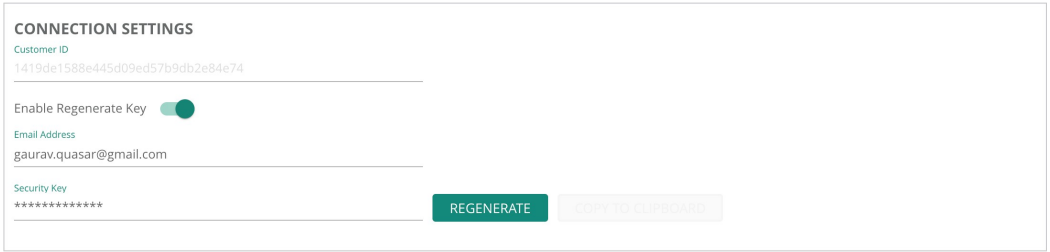


Figure 21 *Note for AirWave Users*

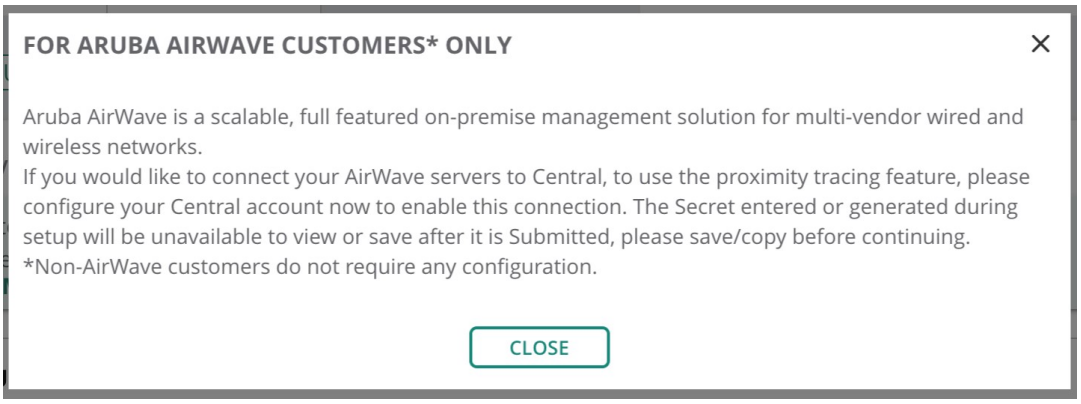


Figure 22 *Update Connection Settings*

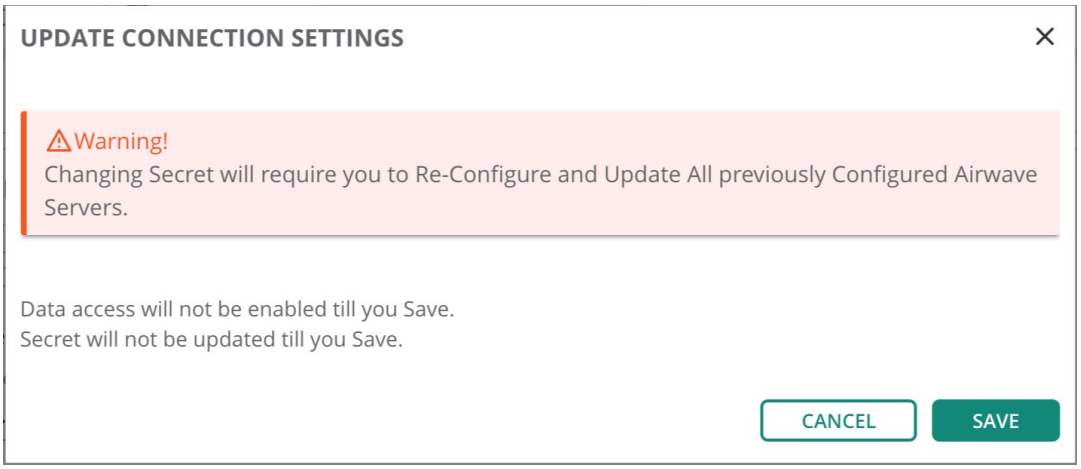
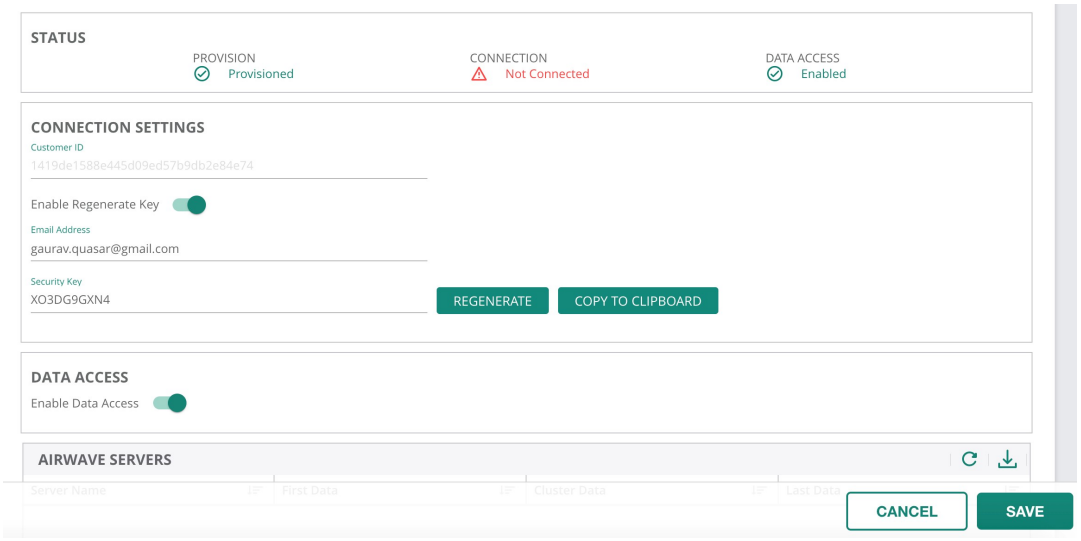


Figure 23 *Status of the Connection Settings*

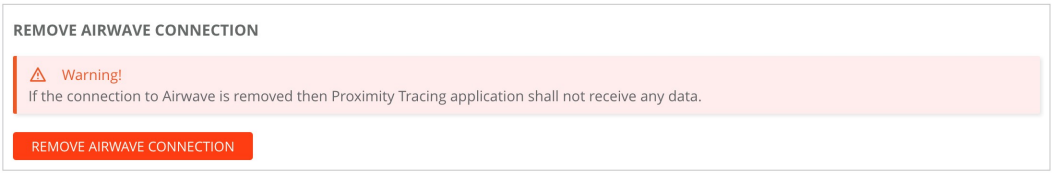


- To de-provision an AirWave server, click **Remove Airwave Connection.** After de-provisioning, the original provisioning information will be available for a maximum of 24 hours before it gets auto de-provisioned. During this time , the AirWave servers will be able to fetch the information that the Customer ID is de-

provisioned and will clean up their own state.

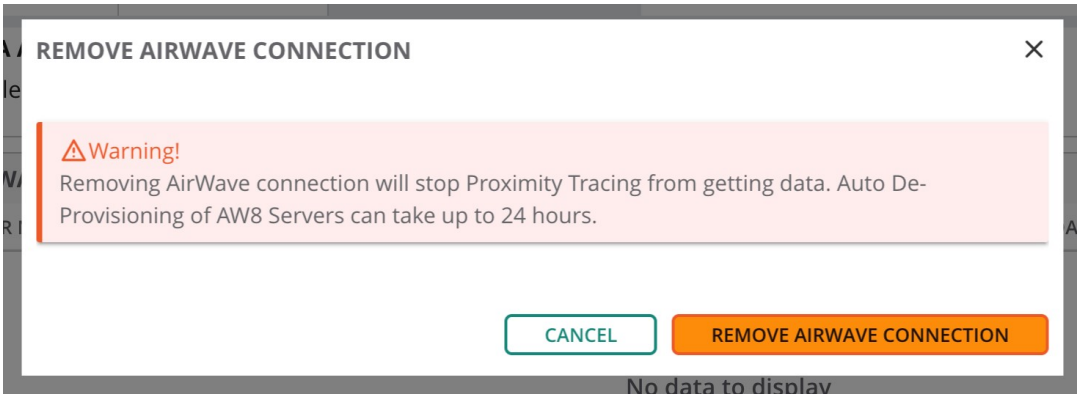
- If the AirWave server was accidentally de-provisioned , it is recommended to wait for at least 24 hours before provisioning the server again and this should be followed by AirWave CLI configuration.

Figure 24 *Remove AirWave Connection*



- The **Remove AirWave Connection** prompt is displayed.

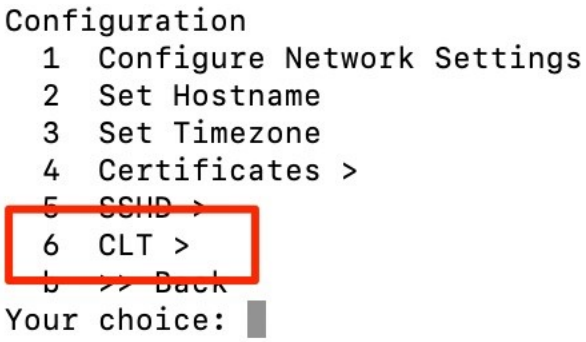
Figure 25 *Remove AirWave Connection Prompt*



The following section describes the steps to configure Aruba Central details in AirWave:

1. Log in to Aruba AirWave CLI using ampadmin credentials.
2. In the CLI menu, enter 3 to access **Configuration** and enter 6 for **CLT** configuration.

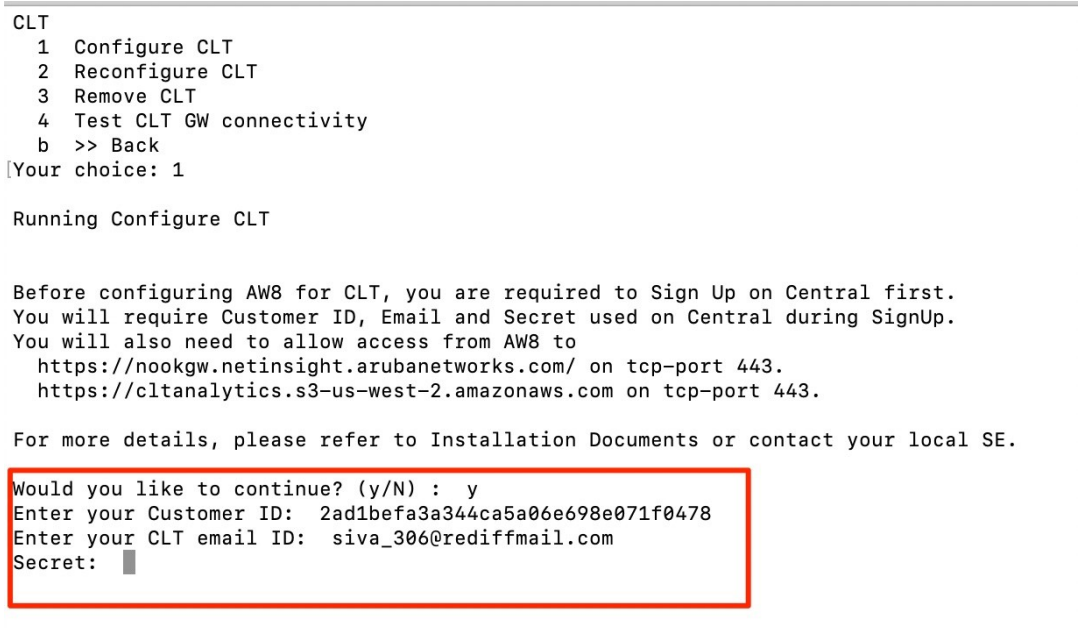
Figure 26 *CLI Configuration*



3. Enter 1 to configure CLT.
4. Enter the customer ID, email address, and the secret key.

AirWave is configured to send data to Central.

Figure 27 *CLT Configuration*



The following table describes the other options available for CLT configuration.

Table 2: *CLT Options*

Options	Function
2	Reconfigures the Central communication with customer ID, email address, or secret key. For example, refer Appendix A.
3	Removes the CLT configuration and the Central settings from AirWave. For example, refer Appendix B.
4	Assists in determining the reachability status of the AirWave server to Central.

Following is the snippet of the connectivity test from AirWave to Central:

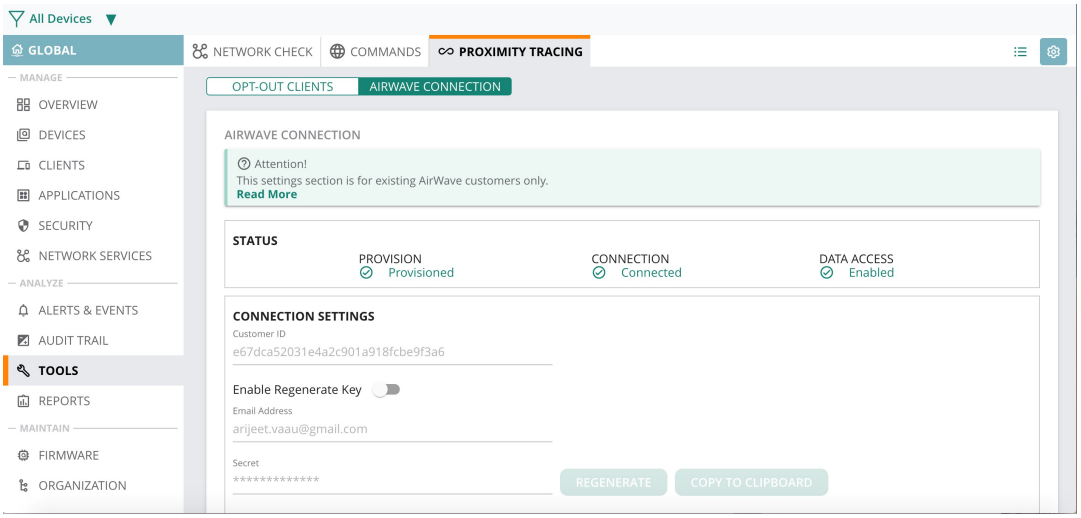
```
Running Test CLT GW connectivity
This will just establish a TCP connection with https://nookgw.netinsight.arubanetworks.com.
Response helps you to identify any firewall issue in reaching it which will in-turn affect
functioning of CLT.
Do you want to proceed with test (y/N) :  y
curl -v https://nookgw.netinsight.arubanetworks.com
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
Dload  Upload   Total   Spent    Left  Speed
* About to connect() to nookgw.netinsight.arubanetworks.com port 443 (#0)
*   Trying 54.201.191.140...
* Connected to nookgw.netinsight.arubanetworks.com (54.201.191.140) port 443 (#0)
* Initializing NSS with certpath: sql:/etc/pki/nssdb
*   CAfile: /etc/pki/tls/certs/ca-bundle.crt
CApath: none
* SSL connection using TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
* Server certificate:
*       subject: CN=nookgw.netinsight.arubanetworks.com
*       start date: Jun 16 00:00:00 2020 GMT
*       expire date: Jul 16 12:00:00 2021 GMT
*       common name: nookgw.netinsight.arubanetworks.com
*       issuer: CN=Amazon,OU=Server CA 1B,O=Amazon,C=US
> GET / HTTP/1.1
> User-Agent: curl/7.29.0
> Host: nookgw.netinsight.arubanetworks.com
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Mon, 29 Jun 2020 15:46:53 GMT
< Content-Length: 0
< Connection: keep-alive
< Vary: Accept-Encoding
<
* Connection #0 to host nookgw.netinsight.arubanetworks.com left intact
Hit return to continue ...
```

The connectivity test from AirWave CLI performs a curl command only to nookgw.netinsight.arubanetworks.com. The connectivity check to cltanalytics.s3-us-west-2.amazonaws.com is not a part of the connectivity test menu in the current AirWave version.

It is planned for future AirWave versions. It is important to ensure that AirWave can reach both the URLs mentioned in prerequisites section. To check the connectivity to both the URLs, Aruba TAC can assist by logging in to the CLI shell and run the curl commands.

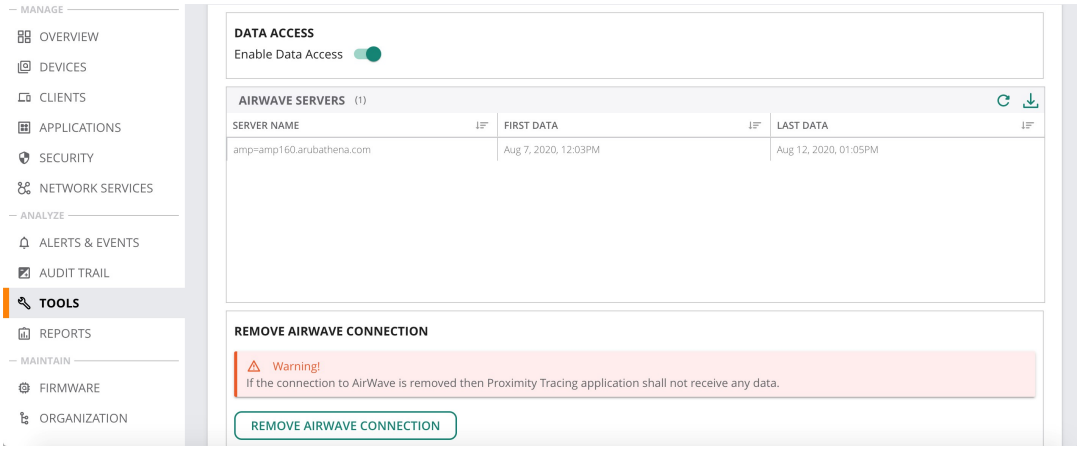
When the AirWave connection to Central is established, the status of the **Connection** changes to **Connected** in the **Proximity Tracing** tab. The status might change only after 24 hours since Airwave communicates with Central only at midnight (AirWave server time).

Figure 28 *Connection Status in Proximity Tracing Tab*



The list of available AirWave servers is displayed in the **AirWave Servers** table.

Figure 29 *List of AirWave Servers*

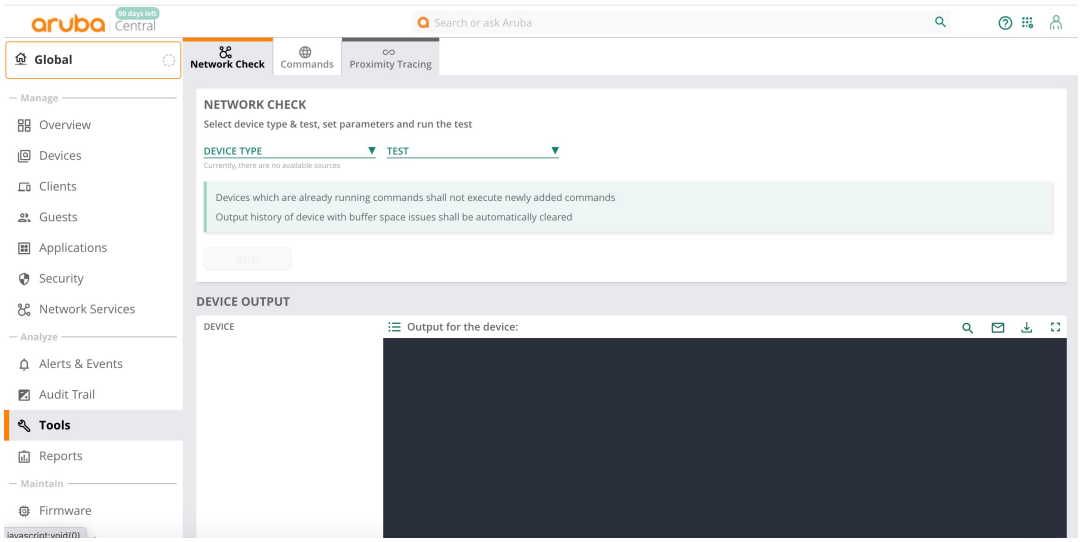


The following section describes how to use the proximity feature. Refer to the Proximity Tracing using Aruba Central tech note for more details.

1. Log in to Aruba Central.
2. In the **Network Operations** app, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
3. Under **Analyze**, click **Tools > Proximity Tracing**.

Figure 30 *Analyze > Tools > Proximity Tracing*



NOTE

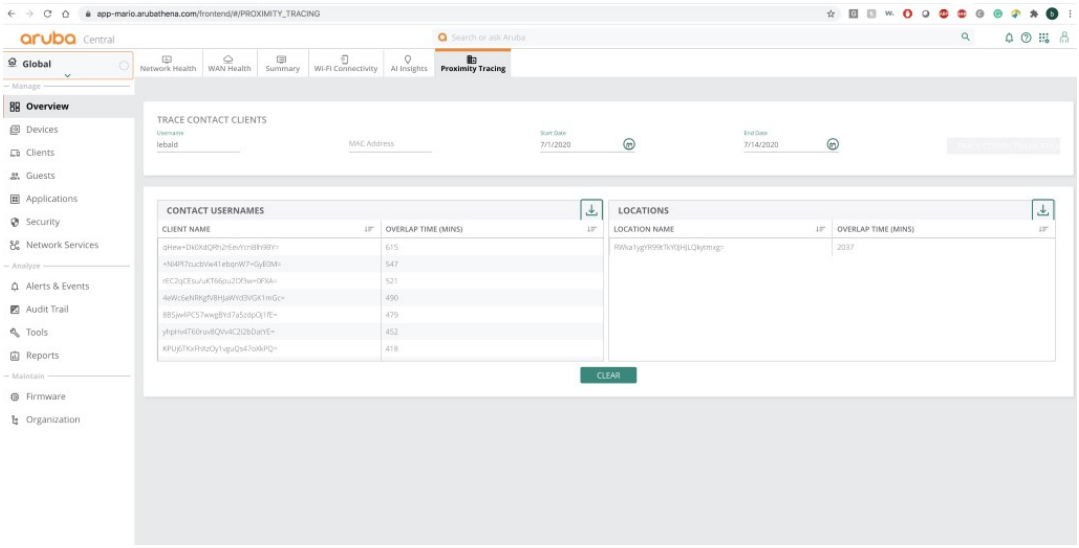
Other tabs are present, however the tabs will not populate data as the devices are not present on Aruba Central but on Aruba AirWave.

The data from AirWave is sent daily at midnight (AirWave server time) and is processed within 4 hours in Central and the data is available in Central for 21 days.

4. Enter the **Username, MAC Address, Start Date,** and **End Date.** Click **Trace Contact Location.**

   The **Contact Usernames** table on the page refreshes to display the names of the contact users and the shared minutes, sorted in descending order of shared minutes.

Figure 31 *Proximity Tracing Details*



5. Click the download icon to download the proximity tracing details.

Chapter 6
Data Sent by AirWave to Central

The following information is sent as individual csv.tar.gz files:

- AP table for AP details including AP name, Mac Address, model etc.
- ap_discovery_event table which includes the AP RN neighbor information
- ap_folder table for AP to site/folder relation in AirWave
- ap_radio table for AP radio information for the enabled radios on the AP.
- BSSID table for BSSIDs of the APs.
- Client table for client information of iusername, MAC address etc
- client_first_last which includes data of the client session information and connection details.
- client_historical for historical client session information
- VisualRF tables for campus, building and floor information for location tracing and information. VisualRF data is currently sent but it is not displayed in this release. However, future releases will use the following VisualRF information:
  - visualrf.building
  - visualrf.campus
  - visualrf.floor
  - visualrf.floor_managed_device.
  - visualrf.managed_device

The raw data that drives the tracing applications in Aruba Central is taken from the access points that are managed in AirWave platforms. This data contains information related to client association history, AP neighbor and VisualRF data. The previous day AirWave data will be available at noon next day in tenant timezone for query. This data will be refreshed on a daily basis. Data will be available for query with a delay of 4 hours. For example, hour_0 (going from hour_0_min_00 through hour _0_min_59) will be available at the beginning of hour_5.

If the tables do not have data, the proxmity tracing feature in Central will display only emplty feilds as it received empty data from AirWave. Hence, it is important to ensure that AirWave has related data for contact and location tracing.

The contact tracing details will be displayed in Central only if client and AP tables in AirWave have data including AP neighbor information. If the data for AP neighbors is not sent by AirWave, then the information will not be present in Central. Poll local controllers for improved Rogue location has to be enabled in the RAPIDS Setup page for AirWave to display the AP neighbor information. This setting helps to get the AP's RF neighbor information.

If the AP name is the MAC address of the AP or if any other name other than what is being configured on AirWave is used as AP name, it is possible that AirWave did not learn the AP name. This also applies to other fields like location. Hence, it is recommended to contact Aruba TAC to check why data is not populated.

If the ap_discovery_event table is missing, IDS profile on controller might not have the **Ap Neighbor Message** enabled. Hence, ensure to enable ap state in the AMON profiles of the controller.

The AirWave Connections tab in Aruba Central displays the list of tables not populated in AirWave server. Download the AirWave connections table before calling technical support to submit a case.

Data Output for AirWave in Central

CT CSV File Columns - AirWave

The following information is displayed:

- Input_User
- Input_Device_MAC
- Contact_User
- Contact_Device_MAC
- Contact_Device_Type
- Campus_Name
- Building_Name
- Floor_Name
- Access_Point_Name
- Contact_Duration
- Date_Hour
- Time_EPOCH

Backend DB field

- username1_imputed
- stamac1
- username2_imputed
- stamac2
- device_type2
- site_imputed
- building_name_imputed
- floor_name_imputed
- apname_imputed
- contact_minutes
- date_hour
- ts_bin

Third-Party Devices on AirWave

Though AirWave supports third-party devices, Aruba doesn't claim to test the third-party devices with proximity tracing in Aruba Central. However, Aruba Central displays the data sent by third-party devices on AirWave. The data can be queried and exported for further use.

Chapter 7
Licensing for AirWave Customers

As an AirWave customer, you can continue to use your on-prem AirWave deployments for NMS features and use Central exclusively for proximity tracing. Since none of your Aruba devices are managed by the Central NMS app, you can sign up for Central using a 90-day trial license. You can continue to use Aruba Central even after the license expiry. Logging in to your Central account will not be affected by the expiry of the 90-day evaluation license.

You do not need to contact anybody at Aruba TAC or PLM or Sales team to extend access to the proximity tracing feature as it is set to function beyond the initial 90-day evaluation license period. It will continue to work indefinitely as there is a free access to this feature during the COVID-19 pandemic crisis.

If you use AirWave and Central for different networks, it is required to create an additional Central account to us the proximity tracing feature for AirWave data. Central account can be used for proximity tracing for devices managed by Central. For example, if you use Central for IAP management and AirWave for controller monitoring, you can use your existing Central account for proximity tracing feature for IAP data. Create a new evaluation Central account to send data from AirWave and avail the proximity tracing feature for controller-based APs (network).

If AirWave is used for monitoring IAPs and/or Campus APs and Central is not used for IAP monitoring, then a single evaluation Central account will suffice to send data from AirWave.

Central CIDs with existing IAP infrastructure does not support AirWave proximity tracing feature.

Initially if Proximity Tracing is configured for AirWave and when IAPs are added later to the same account, AirWave connection under Proximity Tracing feature will not be available. Ensure to create an additional account to monitor IAPs.

Chapter 8
Frequently Asked Questions

1. Is this feature available for all Central and AirWave customers?

   Yes, but note the restrictions of the data sent in the Prerequisites section of this document.
2. Which ArubaOS versions are required for this feature?

   Both ArubaOS 6.x and ArubaOS 8.x versions are supported. The solution supports Aruba Wi-Fi access points/controllers that are managed by the respective AirWave and Central platforms.
3. Does this feature support both Instant and Campus Access Points?

   Yes, both are supported.
4. What is the amount of data transmitted for this solution?

   It is in the order of 5-10 Kbps per AP. It is difficult to fix the overall size of data transferred from AirWave to Central, as it depends on number of APs and clients connected to each AP.
5. If AirWave is the only solution currently deployed, is there any benefit in moving to Central?

   Yes. Central data will be processed more frequently and for a more near real-time.
6. Is Central a multi-tenant environment? Who has access to the data? Will the data be used for any other purpose other than this solution?

   Yes, Central is a multi-tenant environment hosted in Aruba Cloud. Aruba Engineers working on this solution will have access to data and the data will not be used for anything other than this solution.
7. Can I choose to opt out of this feature?

   Yes, you can choose to opt-out of all Wi-Fi related tracing features in both Central and AirWave. However, all Wi-Fi users are opted-in by default.

This solution does not store any health-related information. Also, it does not keep a track of the past queries.

The email address and the secret key used for CLT feature can be changed any time and it has to be applied on all AirWave servers. The reconfiguration option changes either the email address or the secret key. If the customer ID changes, then remove the CLT configuration (Refer Appendix B) and then configure CLT again.

In the AMP CLI Menu, navigate to Option 6 (CLT) > option 2 (Reconfigure CLT)

```
CLT
1  Configure CLT
2  Reconfigure CLT
3  Remove CLT
4  Test CLT GW connectivity
b  >> Back
Your choice: 2
Running Reconfigure CLT
Reconfigure is only for the configured Customer ID. For any other Customer ID, please remove
and configure again.
Do you want to proceed with reconfigure (y/N) :  y
Enter your customer ID:  a83db6a008a74fd6b471def39a006876
Enter your CLT email ID:  arijeet.ghosh@hpe.com
secret:
CLT reconfigured successfully.
Hit return to continue ...
```

The following error message is displayed if an incorrect customer ID is entered:

```
Do you want to proceed with reconfigure (y/N) :  y
Enter your customer ID:  1c55f76eea6546daab3c3e667bd40859
Entered customer ID does not match the configured customer ID.
Hit return to continue ...
```

The **Remove CLT** option is based on the already registered customer ID. In the AMP CLI menu, select Option 6 (CLT) and then option 3 to remove an existing CLT:

```
CLT
1  Configure CLT
2  Reconfigure CLT
3  Remove CLT
4  Test CLT GW connectivity
b  >> Back
Your choice: 3
Running Remove CLT
Do you want to proceed with remove (y/N) :  y
Enter your customer ID:  a83db6a008a74fd6b471def39a006876
CLT configurations removed successfully.
Hit return to continue ...
```

The following error message is displayed if an incorrect customer ID is entered:

```
Running Remove CLT
Do you want to proceed with remove (y/N) :  y
Enter your customer ID:  1c55f76eea6546daab3c3e667bd40859
Entered customer ID does not match the configured customer ID.
Hit return to continue ...
```