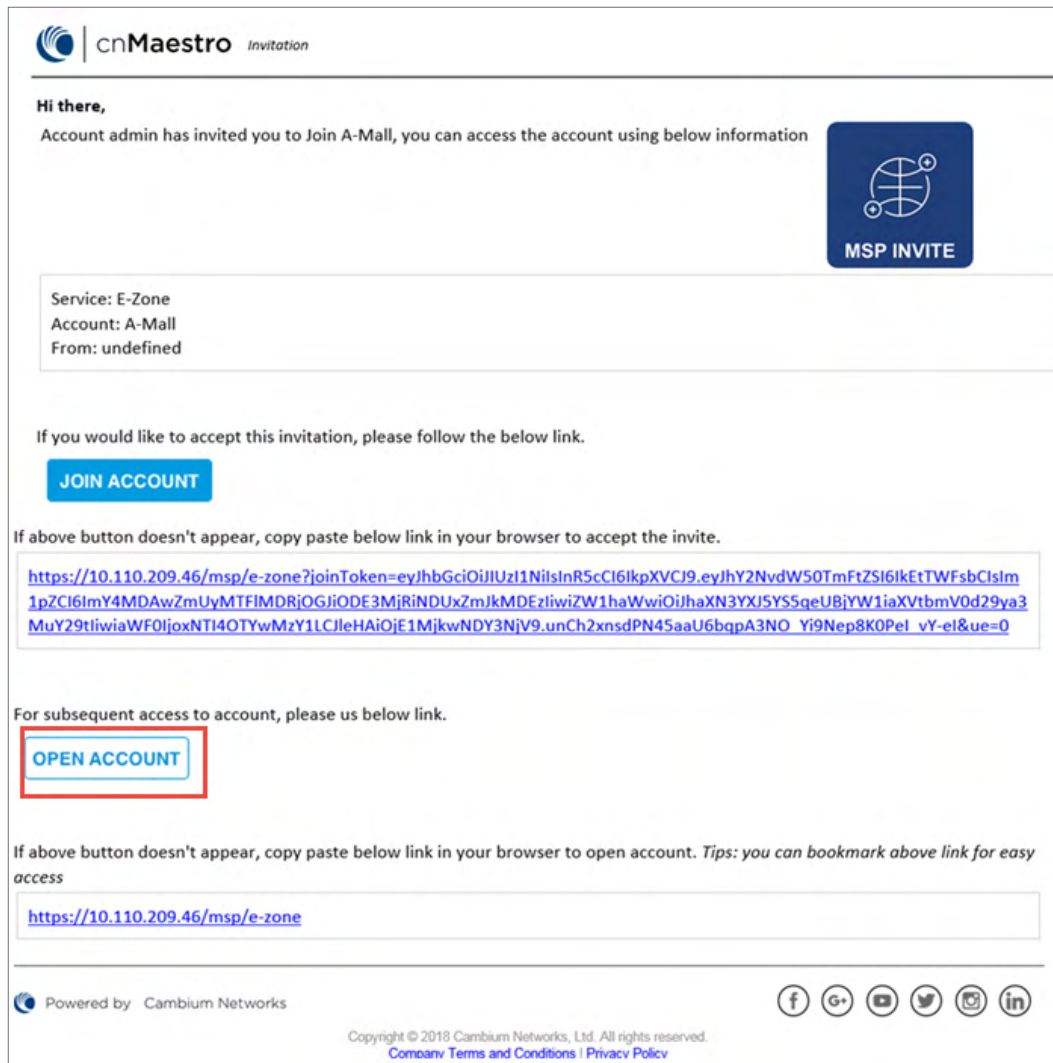


Figure 478 Checking Account Administrator User Email



Create Account in Account Service

Clicking the link prompts the user to create a new Account or use an existing Account.



Note

If a user already has an Account in the Account Service, they can use their existing email login to accept the invite for the new Account. In the global cnMaestro UI, switching between accounts is accomplished using the choice box in the UI header (upper right).

Login to the Accounts UI

Once the Account Administrator (User) is created, use the URL listed in the **Login Path** column to login.

Figure 479 A Sample Login URL

Managed Services > Managed Accounts x

Accounts Account Services

Account Services optionally map Managed Accounts to external Tenant Administrators. The Account Service supports a unique Tenant database and Login URL. System administrators maintain full control of the accounts and can assign role-based access to Managed Account users.

New Account Service

Name	Color	Login Path	Users	Accounts	
aye	#25478D	https://cloud.cambiumnetworks.com:443/msp/aye	1	1	
cbrs-msp	#213F79	https://cloud.cambiumnetworks.com:443/msp/cbrs-msp	1	2	
CNM_SIT_TEST	#25478D	https://cloud.cambiumnetworks.com:443/msp/cnm_sit_test	0	1	
gfjyhgjh	#213F79	https://cloud.cambiumnetworks.com:443/msp/gfjyhgjh	0	0	
ghhgacloud	#25478D	https://cloud.cambiumnetworks.com:443/msp/ghhgacloud	1	1	
hgbygh	#213F79	https://cloud.cambiumnetworks.com:443/msp/hgby	0	0	
	#ff4949	https://cloud.cambiumnetworks.com:443/msp/	1	1	
	#213F79	https://cloud.cambiumnetworks.com:443/msp/	0	1	
	#64ed1f	https://cloud.cambiumnetworks.com:443/msp/	1	1	
	#213F79	https://cloud.cambiumnetworks.com:443/msp/	1	0	

Showing 1 - 10 Total: 25 10 < Previous 1 2 3 Next >

Managed Account Administration

Overview

Once Managed Accounts are enabled, there are three ways to administrator the Accounts.

- [System View](#)
- [Account View](#)
- [Account Administrator \(User\) View](#)

Important Points to Remember

Please note the following points for Account Services administration:



Note

- When a device is moved from one Account to other, it goes offline for one minute before appearing online. Only active alarms are moved to the new account and other data is retained in the old account.
- The Managed Accounts feature can be disabled only if all devices in Accounts are deleted or moved to Base Infrastructure account.
- Administrators of Accounts do not have access to the settings page of the server to change the account type.
- When Global Super Administrators trigger Configure/Software/Reports Jobs, the Account users cannot view them.
- When Account Users trigger Configure/Software/Reports Jobs, they are reflected under the Global Super Administrator view along with respective Job IDs enrolled in the respective Accounts.
- The devices that have not started Software/Configure Jobs cannot be moved across Accounts.
- The Global Super Administrator and the Account Administrator cannot trigger a Software or

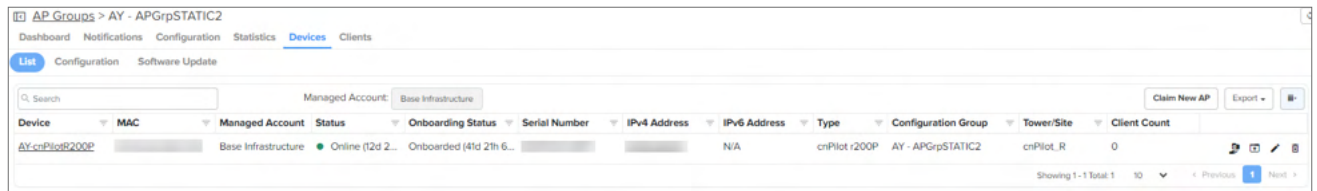
Configure Job simultaneously on the same device.

- The Lock AP configuration can be enabled only by the Global Super Administrator. But whenever a device configuration is changed outside of cnMaestro by either a Global Super Administrator or an Accounts Administrator, the Auto Synchronization Job starts automatically with the configuration job ID as in Accounts and reflects in both the Global Super Administrator and Accounts Administrator accounts.

System View

At the System level, one can view APs, AP Groups, or Sites across all Managed Accounts in a single, unified table. This allows one to review the status of all accounts in context to each another. The following figure displays the AP table, and specifies which APs are mapped to Accounts.

Figure 480 System View



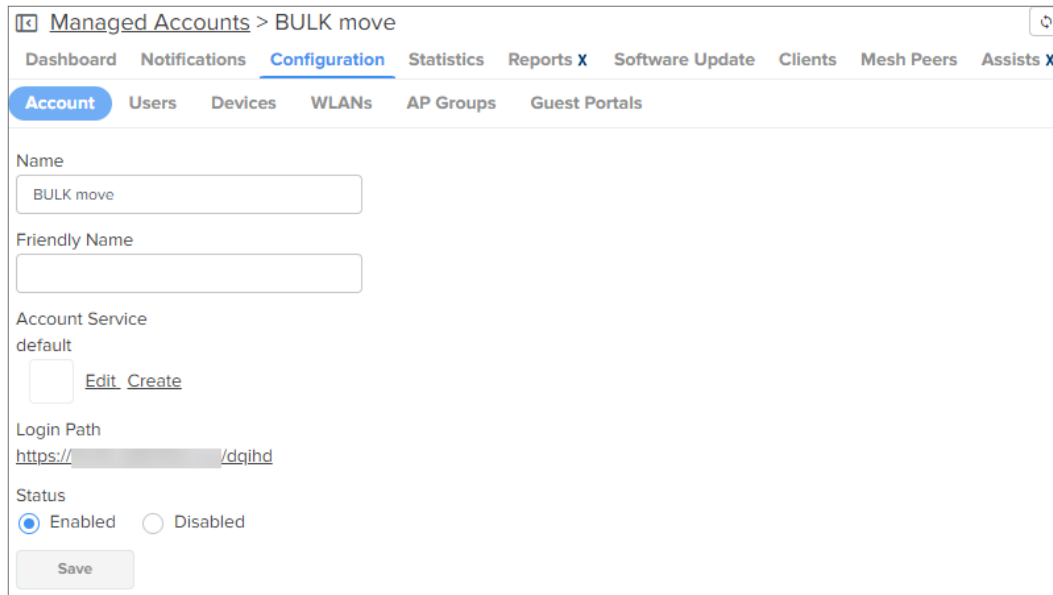
The screenshot shows the 'AP Groups > AY - APGrpSTATIC2' page. It has tabs for Dashboard, Notifications, Configuration, Statistics, Devices, and Clients. The 'List' tab is active. A search bar and a 'Managed Account' dropdown (set to 'Base Infrastructure') are at the top. A table lists APs with columns: Device, MAC, Managed Account, Status, Onboarding Status, Serial Number, IPv4 Address, IPv6 Address, Type, Configuration Group, Tower/Site, and Client Count. One device is listed: 'AY-cnPilot200P' with status 'Online (12d 2h 6m)' and 'Onboarded (41d 21h 6m)'. The bottom right shows 'Showing 1 - 1 Total 1' and pagination controls.

Device	MAC	Managed Account	Status	Onboarding Status	Serial Number	IPv4 Address	IPv6 Address	Type	Configuration Group	Tower/Site	Client Count
AY-cnPilot200P		Base Infrastructure	Online (12d 2h 6m)	Onboarded (41d 21h 6m)			N/A	cnPilot r200P	AY - APGrpSTATIC2	cnPilot_R	0

Account View

The **Managed Accounts > Accounts** page allows you to select individual Accounts, which launches the Account View. This provides full status and configuration for all components of the Account, including Dashboard, Notifications, Configuration, Software Update, Reports, Clients, etc.

Figure 481 Account View

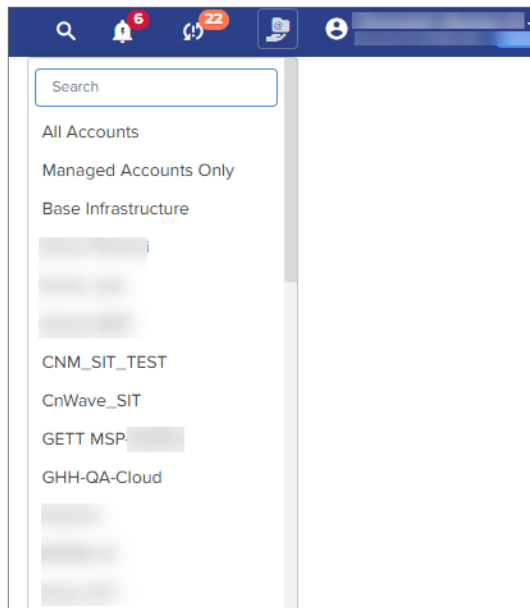


The screenshot shows the 'Managed Accounts > BULK move' configuration page. It has tabs for Dashboard, Notifications, Configuration, Statistics, Reports X, Software Update, Clients, Mesh Peers, and Assists X. The 'Configuration' tab is active, and the 'Account' sub-tab is selected. The form includes: a 'Name' field with 'BULK move'; a 'Friendly Name' field; 'Account Service' set to 'default' with 'Edit' and 'Create' links; a 'Login Path' field with 'https://.../dqihd'; 'Status' set to 'Enabled' with a 'Disabled' option; and a 'Save' button.

Account Administrator (User) View

The Account Administrator View presents the branded Account UI, without having to explicitly log into it. It is accessed through the Account drop-down in the UI header. Selecting a specific Account (rather than **All**) updates the UI to the Account Administrator's view. From here, the Global Administrator can update the configuration and monitor issues.

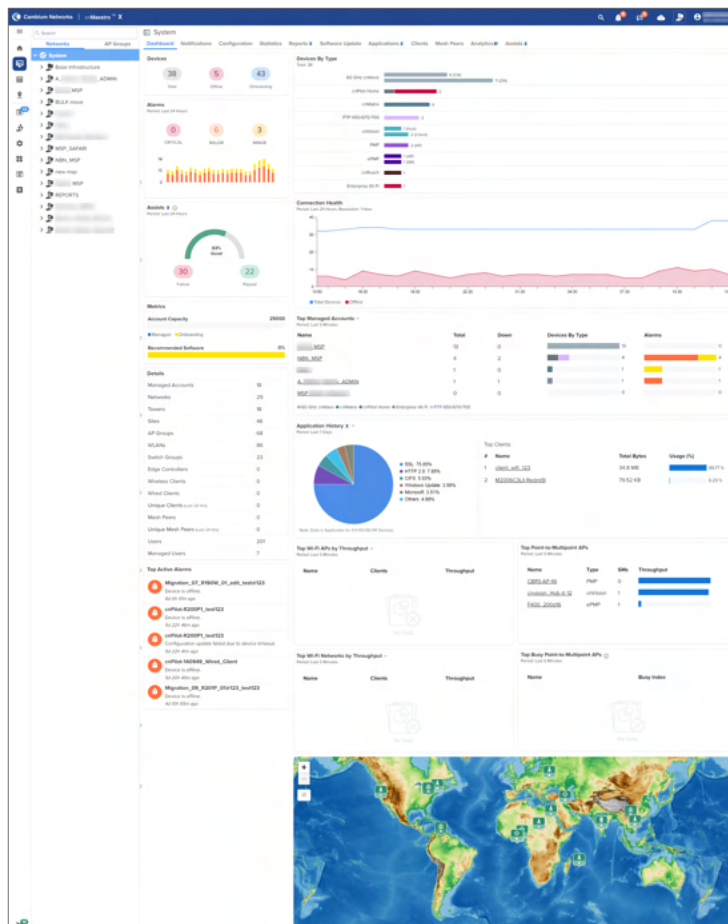
Figure 482 Managed Account Administrator (User) View



System Dashboard

The System Dashboard integrates Accounts into the global health component. It ranks the top Accounts based upon device count.

Figure 483 System Dashboard



Account Administration

AP Groups, WLANs, and Switch Groups have three types of accessibility scope as shown below:

Table 107 *Types of Scope*

State	Description
Base Infrastructure	The object is only available for the global account.
Managed Account	The object belongs to a Managed Account.
Shared	The object is shared among all Managed Accounts. It can be mapped to devices in the Account, but it cannot be modified. To change the configuration, it needs to be copied into the Account and then updated.



Note

Once the scope has been configured on an object, it cannot be changed.

Device Management

Devices are added at the global System level or within Managed Accounts. Devices added at the System level can be moved into Accounts at a later time.

System Onboarding

Onboarding at the global System level supports both MSN and Cambium ID. In the example below, a Management Account can be selected for all devices onboarded in the MSN batch.

Figure 484 *System Onboarding*

Claim Devices with Serial Number

Enter the Serial Numbers (MSNs) of the devices you want to add to your account (comma-separated or one per line). Once a device is claimed, it is placed in the Onboarding Queue when it comes online.

Note: All devices with 12 digit strong Serial Numbers can be claimed here. Other devices can be claimed using [Cambium ID](#).

Managed Account

Base Infrastructure

Search

Base Infrastructure

1-MSP-25NoV

ma_test_nbi_api_d579d

Claim Devices Clear

Device Onboarding

Onboarding devices through the Managed Account UI automatically places the devices in the Account.



Note

cnMaestro supports onboarding through either MSN or Cambium ID. Within Accounts, only MSN onboarding is supported.

Moving a Device Between Accounts

You can move a device from one Managed Account to another by using the **Change** option in the device configuration page.

Figure 485 *Moving a Device Between Accounts*


In Enterprise view, the device can be moved between Accounts using the **Managed Account** () icon in the **AP Groups** > <AP-group-name> > **Devices** > **List** tab.

Figure 486 *Moving a device between Accounts in Enterprise View*

Account Deletion



Note

All devices must be removed from the Account before deleting the account.

To delete a Managed Account, navigate to the **Account Services** page and click the delete icon.

Figure 487 *Account Deletion*

Disabling the Managed Accounts feature

The Managed Accounts feature can be disabled within the system only after all the devices are deleted or moved to the Global context. By disabling Account Services, the Account field will be disabled across all the tables, such as Clients, Notifications, Inventory.

Managing subscribers (end-customer)

To enable a subscriber to manage the router using the Android or iOS application, you must add a subscriber profile in cnMaestro and send an invitation to the subscriber.

This process involves the following actions:

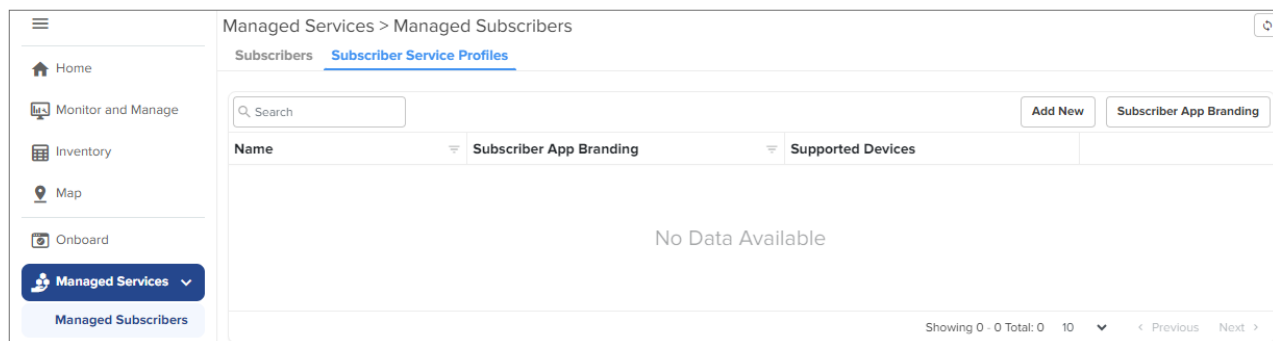
1. [Adding a Subscriber Service Profile](#)
2. [Adding a subscriber](#)
 - a. [Modifying the owner details for the Subscriber App](#)
3. [Claiming the Home Mesh Router](#)

Adding a Subscriber Service Profile

To add a subscriber service profile, complete the following steps:

1. Navigate to the **Manage Services > Managed Subscribers > Subscriber Service Profiles** tab.

The **Subscriber Service Profiles** page appears.



2. Click **Add New**.

The **Add Subscriber Service Profile** window appears.

Add Subscriber Service Profile

Name*

Scope

Base Infrastructure

Description

Download (Mbps)*

Upload (Mbps)*


Type	Device Configuration
<input checked="" type="checkbox"/> RV22 Home Mesh	

Subscriber App Branding*

Cancel Save

3. Select the Home Mesh Router configuration to which you want to associate with the subscriber service profile and configure the parameters as described in [Table 108](#).

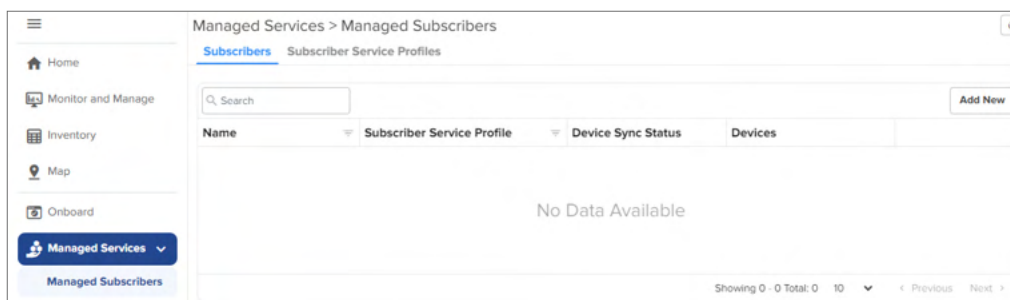
Table 108 *Subscriber Service Profile parameters*

Parameter	Description
Name	Name of the subscriber service profile.
Description	Brief description for the subscriber service profile.
Download (Mbps)	Download speed (in Mbps) configured for the profile.
Upload (Mbps)	Upload speed (in Mbps) configured for the profile.
Type	Displays the device type as RV22 Home Mesh . This field cannot be modified.
Device Configuration	Specifies the Wi-Fi AP group (created for the Home Mesh Router device type) that must be associated with the service profile. Select the group from the drop-down list.
Subscriber App Branding	Specifies the cnMaestro Subscriber application branding that must be used in this profile. All routers sent to subscribers in this service profile contain the selected branding logo and information. Select the required branding from the drop-down list. If no branding is present, create one by clicking the add () icon. See cnMaestro Subscriber application branding for more information.

4. Click **Save**.

Adding a subscriber

- Click the **Subscribers** tab on the **Managed Subscribers** page.




- Click **Add New**.

The **Add Subscriber** window appears.

- In the **Add Subscriber** window, configure the details of the subscriber in the **Basic Information** section, as described in [Table 109](#).

Table 109 *Subscriber > Basic tab parameters*

Parameter	Description
Full Name	Name of the subscriber.
Email ID	<p>Email address of the subscriber.</p> <p>This email address receives the invitation to join the Home Mesh Router (RV22) site. Through this email address the user will be able to access and manage the router as a primary user and invite other users (secondary users), through the mobile application, to manage the routers.</p> <div>  <div> <p>Note</p> <p>You can edit this email address at anytime. However, editing this email address will remove all existing users, both primary and secondary. For information about how to modify the email ID, refer to Modifying the owner details for the Subscriber App.</p> </div> </div>

Parameter	Description
Phone Number	Phone number of the subscriber.
Customer ID	Unique ID for the subscriber.
Address	Address of the subscriber where the routers will be installed.

8. Click **Next**.

The **Service Configuration** tab is displayed.

The screenshot shows the 'Add Subscriber' form with the 'Service Configuration' tab selected. The form includes a 'Subscriber Service Profile*' dropdown menu, 'Download (Mbps)*' and 'Upload (Mbps)*' input fields, an 'AP Group' input field, and a '+ Home Wi-Fi Devices Setting Override' button. At the bottom right are 'Previous' and 'Save' buttons.

9. Select the subscriber service profile to be associated with this subscriber from the **Service Profile** drop-down list.
10. Click **Save**.

A new tab, **Devices** appears, where you can link (or claim) the Home Mesh Router to the subscriber. See [Claiming the Home Mesh Router](#).

The cnMaestro Subscriber application invitation email is sent to the subscriber with the link to join the account.

11. Click **Devices**.

The screenshot shows the 'Add Subscriber' form with the 'Devices' tab selected. The form includes a 'Deployment Type' section with radio buttons for 'Fiber', 'Fixed Wireless', and 'Home Site' (which is selected). Below this is a 'Home Site*' search field with a magnifying glass icon and a '+' button. There is an 'Add Devices to Subscriber' section with an 'Add New' button. A table with columns 'Name', 'Serial Number', 'MAC Address', 'Mesh Type', and 'Status' is shown, followed by a 'No Data Available' message. At the bottom right are 'Previous' and 'Save' buttons.

12. Select one of the following options in the **Deployment Type** field to filter the available deployment types:

- **Fiber**—Select the Optical Network Unit (ONU) device that you want to associate with the subscriber's router by searching in the **ONU** search box.
- **Fixed Wireless**—Select the Subscriber Module (SM) device that you want to associate with the subscriber's router by searching in the **SM** search box.
- **Home Site**—Select the home site you want to associate with the subscriber's router by searching in the **Home Site** search box. To add a home site, see [Adding a Home Site](#).

13. Before linking the Home Mesh Router to the subscriber, click **Save**.

Modifying the owner details for the Subscriber App

You can modify the owner details for the Subscriber App by modifying the email ID.



Warning

Modifying the email address will remove all existing users, both primary and secondary.

To modify the email address, complete the following steps:

1. Navigate to the **Manage Services > Managed Subscribers > Subscribers** tab.
2. In the list of subscribers, click the subscriber name for which you want to modify the email ID.

The corresponding subscriber details are displayed.

3. Under the **Email** parameter, click **Change Owner**.

The Change Owner window is displayed.

4. Enter the new email ID for the subscriber.
5. Click **Update**.

Claiming the Home Mesh Router

After adding a subscriber profile and a subscriber, you must now associate the Home Mesh Router to the subscriber by claiming the router in cnMaestro.

To claim the router, complete the following steps:

1. Navigate to the **Manage Services > Managed Subscribers > Subscribers** tab.
2. In the list of subscribers, select the subscriber name for which you want to associate the Home Mesh Router.
3. Click the **Devices** tab.
4. In the **Add Devices to Subscriber** section, click **Add New**.

The screenshot shows the 'Add Subscriber' window with the 'Devices' tab selected. The left sidebar has 'Basic Information', 'Service Configuration', and 'Devices' (highlighted with a red exclamation mark icon). The main content area shows 'Deployment Type' with radio buttons for 'Fiber', 'Fixed Wireless', and 'Home Site' (selected). Below is a 'Home Site*' search field. The 'Add Devices to Subscriber' section features an 'Add New' button and a table with columns: Name, Serial Number, MAC Address, Mesh Type, and Status. The table is currently empty, displaying 'No Data Available'. At the bottom are 'Previous' and 'Save' buttons.

The **Link Subscriber** window appears.

5. In the **Link Subscriber** window, link the Home Mesh Router to the subscriber by using any of the following methods:
 - To claim a new router that is not onboarded to cnMaestro, select the **Claim new and assign** option and enter the serial number of the device to be claimed.

You can claim multiple routers by adding multiple serial numbers separated by commas.

The screenshot shows the 'Add New Device(s)' window. It has two radio buttons: 'Claim new device and assign' (selected) and 'Search from inventory and assign'. Below is a text area with instructions: 'Enter the Serial Numbers (MSNs) of the RV22 Home Mesh devices you want to add to your account (comma-separated or one per line). Once a device is claimed, it is placed in the Onboarding Queue when it comes online.' The 'Device Type' is set to 'RV22 Home Mesh'. A large text box for serial numbers is provided with a note: 'Place a cursor in the box and use a barcode scanner to quickly claim devices.' A 'Cancel' button is at the bottom right.

- To claim a router that is already onboarded to cnMaestro, select the **Search for inventory and assign** option.

Enter the details of the router you want to claim.


Add New Device(s)

☐ Claim new device and assign
☒ Search from inventory and assign

Cancel


6. Click **Assign**.

The assigned router appears in the **Add Devices to Subscriber** section.

Add Devices to Subscriber					Add New
Name	Serial Number	MAC Address	Mesh Type	Status	
RV22			Base	● Onboarded	



Note

Click the unlink () icon to unlink the router from the subscriber.

Network Services

This section includes the following topics:

- [API Client](#)
- [RESTful API](#)
- [Guest Access](#)
- [EasyPass](#)
- [RADIUS Proxy](#)
- [CBRS](#)
- [Organization](#)
- [LTE](#)
- [Managing Edge Controller](#)
- [cnArcher Summary](#)
- [Spectrum Analyzer](#)

API Client

Overview

The cnMaestro RESTful API allows customers to manage their deployment programmatically using their own client applications. The API is supported over HTTPS, and messages are exchanged in JSON format. Modern programming languages have rich support for RESTful interfaces.



Note

cnMaestro currently provides monitoring data over the API (such as inventory, statistics, events, and alarms).

API Clients

API Clients are external applications that access the RESTful API over HTTPS using OAuth 2.0 Authentication. They require a Client ID and Client Secret for access, both of which are detailed later in this chapter. For more information, refer to [RESTful API Specification](#).

Application Name	Application Description	Client Id	Actions
Test API	test	5b09b4LHPKEYEe	
Cloud API	To, Test APIs	NfCGgRQ0gLMbLK	

To add **API Client**:

1. Navigate to **Network Services > API Clients**.

Application Name	Application Description	Client Id	Actions
Test API Now	Test NBI/API		
Test API	Test NBI/API		

2. Click **Add API Client**.

API Clients > Add API Client

Basic Information

Name*

Description*

Expiration Time
 OAuth 2.0 Access Token expiration seconds

Token Renewal Time
 OAuth 2.0 Access Token renewal seconds

3. Enter **Name**.
4. Enter **Description**.
5. Enter **Expiration Time**.
6. Enter **Token Renewal Time**.
7. Click **Save**.

Once the API Clients is added you can able to view or download credentials shown in the **OAuth 2.0 Access Credentials**.

API Clients > Edit API Client x

Basic Information

Name*

Description*

Expiration Time
 OAuth 2.0 Access Token expiration seconds

Token Renewal Time
 OAuth 2.0 Access Token renewal seconds

OAuth 2.0 Access Credentials

These credentials are required to create an Access Token and invoke the API.

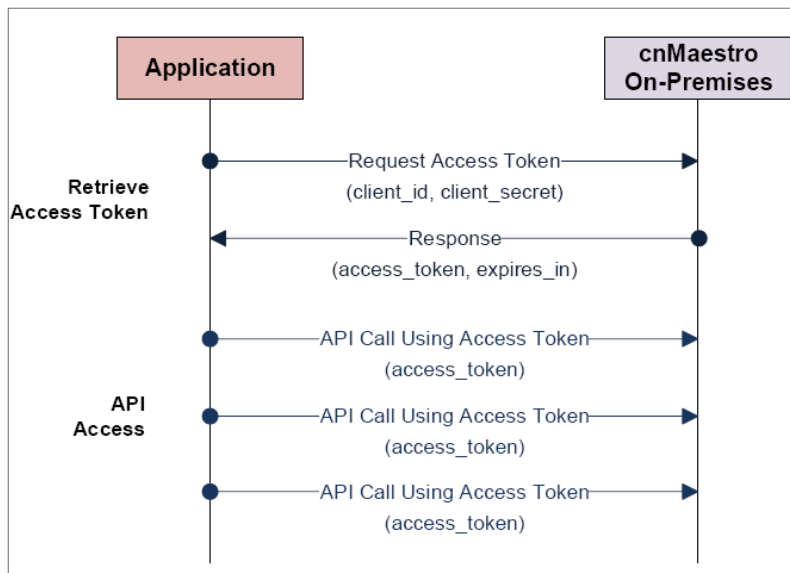
Client Id

Client Secret

RESTful API Specification

Authentication

API Authentication uses OAuth2. The client retrieves an Access Token to start the session. It then sends API requests until the Access Token times out, at which point the token can be regenerated.



Establish a Session

A session is created by sending the Client ID and Client Secret to the cnMaestro server. These are generated in the cnMaestro UI and stored within the application. The Client ID defines the cnMaestro account and application, and the Client Secret is a private string mapped to the specific application. The Client Secret should be stored securely.

If the session is established successfully, an Access Token is returned along with an expiration string. The Access Token is used to authenticate the session. The expiration is the interval, in seconds, in which the Access Token remains valid. If the Access Token expires, a new session needs to be created.

API Access

The application sends the Access Token, in every API call. The token is sent in an Authentication header. Details are provided later in this document.

Session Expiration

If a token expires, an expiration error message is returned to the client. The client can then generate a new token using the Client ID and Client Secret. The token expires immediately if the Client API account is deleted. The default expiration time for a token is 3600 seconds (1 hour). The session expiration is configurable in the UI.

Rate Limiter

The Rate Limiter API request helps in improving the availability of API based services by avoiding resource starvation.

This API calculates the rate limit per customer based on various factors such as system configuration, number of devices onboarded, Network, Towers, Sites, etc.

The API limits the number of NBI API calls to a single cnMaestro account per minute. Once the limit is reached, the API receives a standard HTTP Response Status code such as 429 or 503.

HTTP Response Status Code	Response Headers	Explanation	Action to be taken
429	RateLimit-Limit: 10	Number of API calls allowed for the cnMaestro account per minute	If the RateLimit-Remaining value is 0, then the client application waits for the number of seconds to Reset-RateLimit before sending the next subsequent API requests
	RateLimit-Remaining: 0	Number of remaining API calls for the current minute is zero	
	RateLimit-Reset: 35	Number of seconds remaining to reset the rate limit	
503	Retry-After	Number of seconds during which users wait before retrying	If the value of Retry-After is greater than 0, then the client application waits for the number of seconds to Retry-After before sending the next subsequent API requests

The following table below displays the approximate limit calculated by the system on a 4 vCPU, 8 GB RAM Cloud instance.

Devices	GET	POST/Others
101	10	3
501	24	3
1001	47	5
2001	92	10
4001	163	17

Example of a Python client:

```
import sys
import requests
import json
import base64
import time

HOST = # host here
CLIENT_ID = # client id here
CLIENT_SECRET = # client secret here
TOKEN_URL = # token url here

# Retrieve access parameters (url, access_token, and expires_in).
def get_access_parameters(token_url, client_id, client_secret):
    """
    Authenticates to API.
    Parameters:
        `token_url` - Endpoint to authenticate to\n
        `client_id` - Auth client id\n
        `client_secret` - Auth client secret\n
    Returns:
        `(access_token, expiry)`
    """
    data = "%s:%s" % (client_id, client_secret)
    encoded_credentials = base64.b64encode(data.encode('ascii')).decode('ascii')
    headers = {
        "Authorization": "Basic %s" % encoded_credentials,
        "Content-Type": "application/x-www-form-urlencoded"
    }
    body = "grant_type=client_credentials"
    r = requests.post(token_url, body, headers=headers, verify=False)
    print ("Status Code: %s" % r.status_code)
    return r.json()['access_token'], r.json()['expires_in']

def call_api(method, host, path, access_token):
    """
```

Makes HTTP call to an API with given method.

Parameters:

```
`method` -  
method for the new Request object: GET, OPTIONS, HEAD, POST, PUT, PATCH, or DELETE  
TE  
  
`host` - host for the url  
  
`path` - path for the url  
  
`access_token` - a valid access token for header
```

Returns:

```
`(response_status_code, headers, body)`  
"""  
  
api_url = "https://%s%s" % (host, path)  
  
headers = {  
    "Authorization": "Bearer %s" % access_token,  
}  
  
response = requests.request(method=method, url=api_  
url, headers=headers, verify=False)  
  
headers = response.headers  
  
body = response.json()  
  
response_status_code = int(response.status_code)  
  
return response_status_code, headers, body
```

```
def main():
```

```
    try:  
        # Getting the access token using client id and client secret  
        access_token, expires_in = get_access_parameters(TOKEN_URL, CLIENT_  
ID, CLIENT_SECRET)  
  
        # For the purpose of the example, let's send 100 requests back to back  
        for i in range(100):  
            # Calling the endpoint with GET method  
            status_code, header, body = call_api  
( 'GET', HOST, '/api/v2/devices/statistics', access_token)  
            # identifying any client or server side error codes  
            client_errors = (status_code - status_code%100) == 400  
            server_errors = (status_code - status_code%100) == 500
```

```

        # handling error status code
        if client_errors or server_
errors: # check for all 400 and 500 responses
            print("Failure: [%s]-[%s]" %(status_code, (json.dumps
(body, indent=2))))

            # For 429, wait until `RateLimit-Reset` seconds
            if (status_code == 429):
                sleep_time = 10 # default wait time
                # try block prevents any dict value exception
                try:
                    # Reading the header
                    sleep_time = int(header["RateLimit-Reset"])
                except: pass
                # if sleep_
time is not greater than 0, defaulting to 10 seconds
                sleep_time = sleep_time if sleep_time > 0 else 10
                print("Sleeping for %d seconds" % sleep_time)
                # sleeping the main thread
                time.sleep(sleep_time)

            if (status_code == 503):
                sleep_time = 10 # default wait time
                # try block prevents any dict value exception
                try:
                    # Reading the header
                    sleep_time = int(header["Retry-After"])
                except: pass
                # if sleep_
time is not greater than 0, defaulting to 10 seconds
                sleep_time = sleep_time if sleep_time > 0 else 10
                print("Sleeping for %d seconds" % sleep_time)
                # sleeping the main thread
                time.sleep(sleep_time)

            else:
                # process response
                print("Success: [%s]" %(json.dumps(body, indent=2)))

    except Exception as E:

```



```

        print("Failure: [%s]"%E)

        sys.exit()

if __name__ == "__main__":
    main()

```

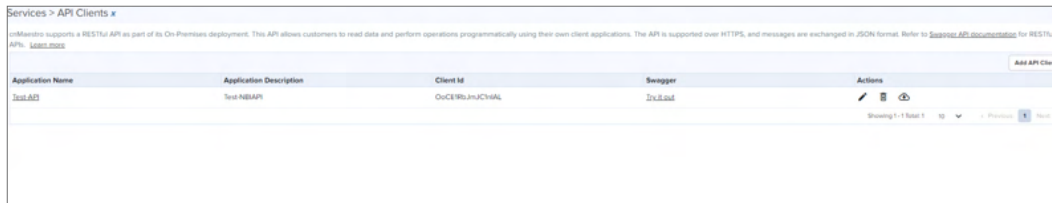
Swagger API

Introduction

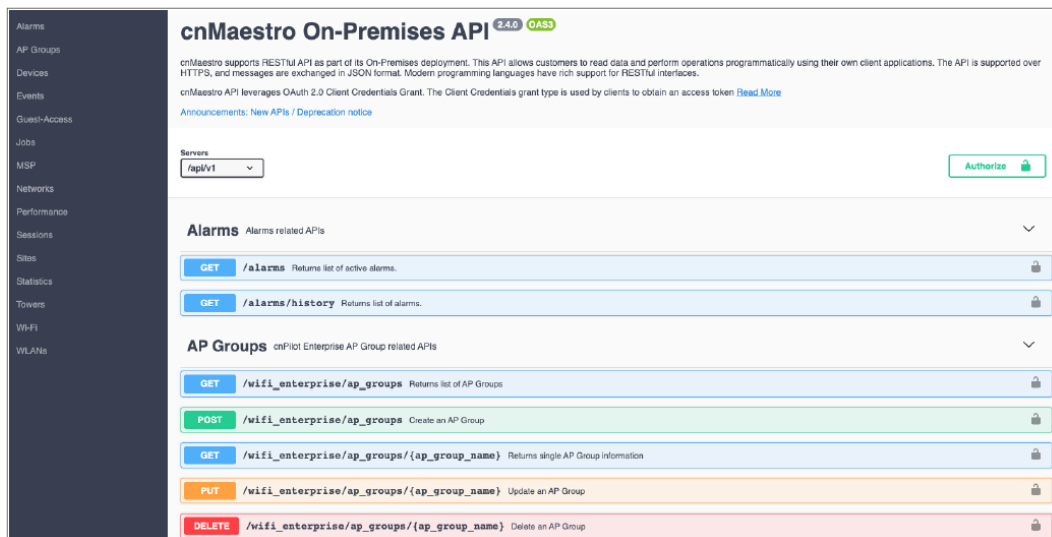
The RESTful API documentation is supported through Swagger, which allows visualization and interaction with the API resources.

To access Swagger, perform the following steps:

1. Navigate to **Services > API Client** grid.
2. Click **Swagger API documentation**.



Sample Swagger UI



Generating Client ID and Client Secret

cnMaestro User Interface

To create the Client Id and Client Secret in the cnMaestro UI, perform the following steps:

1. Navigate to **Services > API Client**.
Each client application should be added as an API Client.

Services > API Clients

cnMaestro supports a RESTful API as part of its On-Premises deployment. This API allows customers to read data and perform operations programmatically using their own client applications. The API is supported over HTTPS, and messages are exchanged in JSON format. Refer to [Swagger API documentation](#) for RESTful API. [Learn More](#)

Application Name	Application Description	Client ID	Swagger	Actions
Test API	Test API	OnCE8b0mJC4H4L	Swagger	

Showing 1 of 1 total 1 | Previous Next

2. Click **Add APIClient** to add a client.

Add API Client window pops up.

API Clients > Add API Client

Basic Information

Name*

Description*

Expiration Time
 OAuth 2.0 Access Token expiration seconds

☐ Concurrent Access Allow multiple Access Tokens to exist simultaneously

3. Enter **Name** and **Description**.

4. Click **Save**.

Download the Client ID and Client Secret

You can download and store the Client ID and Client Secret by clicking **Download Credentials**. The Client Id is required to create an API session.

API Clients > Edit API Client

Basic Information

Name*

Description*

Expiration Time
 OAuth 2.0 Access Token expiration seconds

☐ Concurrent Access Allow multiple Access Tokens to exist simultaneously

OAuth 2.0 Access Credentials

These credentials are required to create an Access Token and invoke the API.

Client Id

Client Secret

API Session

Introduction

The cnMaestro API leverages the Client Credentials section of the [OAuth 2.0 Authorization Framework \(RFC 6749\)](#). An API session can be created using any modern programming language. The examples below highlight how messages are encoded and responses returned.

Retrieve Access Token

Access Token Request (RFC 6749, section 4.4.2)

To generate a session, the client should retrieve an Access Token from cnMaestro. This is done by base64 encoding the **Client_ID** and **Client_Secret** downloaded from the cnMaestro UI and sending them to the cnMaestro server. The **Authorization** header is created by base64 encoding these fields as defined below.



Note

The fields are separated by a colon (:).

Authorization: Basic BASE64(<client_id>:<client_password>)

In the body of the **POST** the parameter **grant_type** must be set to **client_credentials**.

```
POST /api/v2/access/token HTTP/1.1
Host: server.example.com
Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW
Content-Type: application/x-www-form-urlencoded

grant_type=client_credentials
```

Alternatively, the credentials can be passed within the body of the **POST** without using the **Authorization** header.

```
POST /api/v2/access/token HTTP/1.1
Host: server.example.com
Content-Type: application/x-www-form-urlencoded

grant_type=client_credentials&client_id=s6BhdRkqt3&client_secret=7Fjfp0ZBr1KtDRbnfVdmIw
```

Access Token Response (RFC 6749, section 4.4.3)

The response returned from cnMaestro includes the **Access_Token** that should be used in subsequent requests. The **expires_in** field defines how many seconds the token is valid.

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache
{
  "access_token": "2YotnFZFEjrlzCsicMWpAA",
  "token_type": "bearer",
  "expires_in": 3600
}
```

Sample 200 response body.

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache
{
  "access_token": "290eeaba71d3f4885405eac2fd18a4f3c300448d",
  "expires_in": 3600,
  "token_type": "bearer",
  "redirect_uri": "https://10.110.241.252"
}
```



Note

The returned **redirect_uri** should be used to generate the session.

Error Response (RFC 6749, section 5.2)

If there is an error, an HTTP 400 (Bad Request) error code is returned along with one of the following error messages as shown below:

Table 110 *Error Response*

Message	Details
invalid_request	Required parameter is missing from the request.
invalid_client	Client authentication failed.
unauthorized_client	The client is not authorized to use the grant type sent.
unsupported_grant_type	The grant type is not supported.

An example error response is below:

```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache
{
  "error": "invalid_request"
}
```

Access Resources

When the **Access_Token** is retrieved, API requests are sent to cnMaestro server using the format below. The **Access_Token** is sent within the HTTP **Authorization** header.

```
GET /api/v2/devices
Accept: application/json
Authorization: Bearer ACCESS_TOKEN
```

API Details

HTTP Protocol

HTTP Response codes

[Table 111](#) lists the response codes that are supported in cnMaestro and may be returned through the HTTP protocol.

Table 111 *HTTP Response codes returned*

Code	Description	Use in cnMaestro
200	OK	Standard response for successful HTTP requests.
400	Bad Request	Status field in request validation related errors.
401	Unauthorized	User tried to access a resource without authentication.
403	Forbidden	An authenticated user tries to access a non-permitted resource.

Code	Description	Use in cnMaestro
404	Not Found	Server could not locate the requested resource.
405	Method Not Allowed	A method (GET, PUT, POST) is not supported for the resource.
413	Payload Too Large	The request is larger than the server is willing to handle
422	Unprocessable Entity	The server understands the request but cannot process it.
429	Too Many Requests	The client has sent too many requests in a given interval.
431	Request Header Fields Too Large	The header fields are too large to be processed.
500	Internal Server Error	A server-side error happened during processing the request.
501	Not Implemented	The request method is not recognized.
502	Bad Gateway	Internal server error that may require a reboot.
503	Service Unavailable	Internal server error that may require a reboot.

HTTP Response codes

[Table 112](#) lists the HTTP request codes supported in cnMaestro.

Table 112 *Request Headers*

Header	Details
Accept	Set to application/json
Authorization	Used in every API request to send the Access Token. Example: Authorization: Bearer <Access-Token>
Content-Type	Set to application/json

REST Protocol

Resource URLs

The format for cnMaestro path and parameters are the following:

Access a collection of resources:

```
/api/{version}/{resource}?{parameter}={value}&{parameter}={value}
```

Access a single resource:

```
/api/{version}/{resource}/{resource_id}?{parameter}={value}&{parameter}={value}
```

Access a sub-resource on a collection (this is also possible on single resources):

```
/api/{version}/{resource}/{sub-resource}?{parameter}={value}&{parameter}={value}
```

For example – read the statistics for MAC, Type, and IP on all devices:

```
/api/v2/devices/statistics?fields=mac,type,ip_wan
```

Version

The version is equal to v2 in this release.

Resource

Resources are the basic objects in the system. Examples include:

Table 113 *Resource*

Context	Details
alarms	Current active alarms.
alarms/history	Historical alarms, including active alarms.
devices	Devices, including ePMP, PMP, and WiFi.
events	Historical events.
mshp	MSP managed services.
networks	Configured networks.
sites	Configured WiFi sites.
towers	Configured Fixed Wireless towers.

Sub-Resources

Sub-Resources apply to top-level resources. They provide a different view of the resource data, or a filtered collection based upon the resource. Examples include:

Table 114 *Sub-Resources*

Context	Details
alarms	Alarms mapped to the top-level resource.
alarms/history	Historical alarms mapped to the top-level resource.
clients	Wireless LAN clients mapped to the top-level resource.
devices	Devices mapped to the top-level resource.
events	Events mapped to the top-level resource.
mesh/peers	Wireless LAN mesh peers mapped to the top-level resource.
operations	Operations available to the top-level resource
performance	Performance data for the top-level resource.
statistics	Statistics for the top-level resource.

Responses

Successful Response

In a successful HTTP 200 response, data is returned using the following structure. The payload is presented in JSON format.

The request URL is:

```
/api/v2/devices?fields=mac,type&limit=5
```

Response:

```
{
  "paging": {
    "offset": 0,
    "limit": 5,
    "total": 540
  },
  "data": [
    {
      "mac": "C1:00:0C:00:00:21",
      "type": "wifi-home"
    }
  ]
}
```

```

    },
    {
      "mac": "C1:00:0C:00:00:18",
      "type": "wifi-home"
    },
    {
      "mac": "C1:00:0C:00:00:12",
      "type": "wifi-home"
    },
    {
      "mac": "C1:00:0C:00:00:15",
      "type": "wifi-home"
    },
    {
      "mac": "C1:00:0C:00:00:06",
      "type": "wifi-home"
    }
  ]
}

```

Error Response

Error Responses return a message and an error cause.

```

{
  "error": {
    "message": "Missing required property: stop_time \n Missing required property: start_time",
    "cause": "InvalidInputError"
  }
}

```

Parameters

Most APIs can filter the data and limit the number of entries returned. The parameter options are listed below. The specific fields and the appropriate values vary for each API.

Field selection

Field selection is supported through the optional **Fields** parameter, which can specify the data to return from the server. If this parameter is missing, all available fields will be returned.

Table 115 *Fields*

Parameter	Details
fields	Define exactly what fields should be returned in a request. The names are provided as a comma-separated list.

Fields can limit which JSON parameters are returned as shown below:

Example: To retrieve name, type and location information for all devices.

Request:

```
/api/v2/devices?fields=mac,type
```

Response:

```
{
```

```

    "paging": {
      "total": 3,
      "limit": 100,
      "offset": 0
    },
    "data": [
      {
        "mac": "00:44:E6:34:89:48",
        "type": "wifi-enterprise"
      },
      {
        "mac": "00:44:16:E5:33:E4",
        "type": "wifi-enterprise"
      },
      {
        "mac": "00:44:26:46:32:22",
        "type": "wifi-enterprise"
      }
    ]
  }
}

```

Filtering

A subset of fields support filtering. These are defined as query parameters for a particular resource, and they are listed along with the API specification.

[Table 116](#) describes the standard filtering parameters as shown below:

Table 116 *Filtering*

Field	Details
network	(Devices) Configured Network name.
severity	(Alarms, Events) Alarm or Event severity (critical, major, minor, notice).
site	(Devices) Configured Site name.
state	(Alarms) Alarm state (active, cleared).
status	(Devices) Device status (online, offline, onboarding).
tower	(Devices) Configured Tower name.
type	(Devices) Device type (60ghz-cnwave, cnreach, cnmatrix, epmp, pmp, wifi-enterprise, wifi-home, wifi, ptp) (wifi includes wifi-home and wifi-enterprise).

Filters can be used simultaneously for **Resources** and **Sub-Resources**.

Example: Retrieve all WiFi devices that are online.

Request:

```
/api/v2/devices?type=wifi&status=online
```

Response:

```

{
  "paging": {
    "total": 1,
    "limit": 100,
    "offset": 0
  },
  "data": [

```



```

{
  "ip": "233.187.212.38",
  "location": {
    "type": "Point",
    "coordinates": [
      77.55310127974755,
      12.952351523837196
    ]
  },
  "mac": "C1:00:0C:00:00:24",
  "msn": "SN-C1:00:0C:00:00:24",
  "name": "Hattie",
  "network": "Bangalore",
  "product": "cnPilot R201",
  "registration_date": "2017-05-23T21:28:37+05:30",
  "status": "online",
  "site": "Bangalore_Industrial",
  "type": "wifi-home",
  "hardware_version": "V1.1",
  "software_version": "2.4.4",
  "status_time": 1495560086
}
]
}

```

Time Filtering

Events, Alarms, and Performance data can be filtered by date and time using ISO 8601 format.

Example: January 12, 2015 UTC would be encoded as **2015-01-12**.

Example: January 12, 2015 1:00 PM UTC would be encoded as **2015-01-12T13:00:00Z**.

If the parameters that are described in the [Table 117](#) are not specified, then the start or stop times will be open-ended.

Table 117 *Time Filtering*

Parameter	Details
start_time	Inclusive start time of interval.
stop_time	Inclusive stop time of interval.

Sorting

Sorting is supported on a subset of fields within certain requests. Sort is used to specify sorting columns. The sort order is ascending unless the path name is prefixed with a '-', in which case it would be descending.

Table 118 *Sort*

Parameter	Details
sort	Used to get the records in the order of the given attribute.

Example: To retrieve devices in sorted (ascending) order by name.

Request:

```
/api/v2/devices?sort=name
```

Example: To retrieve devices in sorted (descending) order by mac.

Request:

/api/v2/devices?sort=-mac

Pagination

The limit and offset query parameters are used to paginate responses.

Table 119 *Pagination*

Parameter	Details
limit	Maximum number of records to be returned from the server.
offset	Starting index to retrieve the data.

Example: To retrieve the first 10 ePMP devices

Request:

/api/v2/devices?offset=3&limit=1

Response:

```
{
  "paging": {
    "total": 6,
    "limit": 1,
    "offset": 3
  },
  "data": [
    {
      "status": "online",
      "product": "cnPilot E400",
      "network": "Mumbai",
      "software_version": "3.3-b14",
      "registration_date": "2017-04-28T08:57:33+00:00",
      "site": "Central",
      "hardware_version": "Force 200",
      "status_time": "3498",
      "msn": "Z834275ABCDH",
      "mac": "00:04:36:46:34:AA",
      "location": {
        "type": "Point",
        "coordinates": [
          0,
          0
        ]
      },
      "type": "wifi-enterprise",
      "name": "E400-4634AA"
    }
  ]
}
```

Internal Response limits

When clients try to access a resource type without pagination, the server will return the first 100 entries that match the filter criteria. The response will always carry metadata to convey total count and current offset and limit.

Maximum number of results at any point is 100 even when the provided is more than 100.

Example: To retrieve all devices.

Request:

/api/v2/devices

Response:

```
{
  data: {devices: [ {name: 'ePMP_5566', type:'ePMP', location:'blr'} , {...}... ] },
  paging:{
    "limit":25,
    "offset":50,
    "total":100
  }
}
```

The response returns the following values in the paging section:

Table 120 *Internal Response limits*

Parameter	Details
limit	Current setting for the limit.
offset	Starting index for the records returned in the response (begins at 0).
total	Total number of records that can be retrieved.

Access API

Token (basic request)

POST

/api/v2/access/token

The access API generates token using the **Client ID** and **Client Password** created in the cnMaestro UI. The token can be leveraged by API calls through the expiration time. Only one token is supported for each Client ID at any given time.

Request

[Table 121](#) describes about the header and its values as shown below:

Table 121 *Headers*

Header	Value
Accept (optional)	application/json.
Authorization	Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW.
Content-Type	application/x-www-form-urlencoded.

The **client_id** and **client_secret** are encoded and sent in the Authorization header. The encoding is:

```
BASE64(client_id:client_secret)
```

Body

The body needs to have the **grant_type**.

```
grant_type=client_credentials
```

Response

The response returns credentials for API access.

Body

Name	Details
access_token	Access token to return with each API request.
expires_in	Time in seconds that the API session will remain active.
token_type	This will always be bearer.
<pre>{ "access_token": "2YotnFZFEjrlzCsicMWpAA", "token_type": "bearer", "expires_in": 3600 }</pre>	

Example

Request
<pre>curl https://10.110.134.12/api/v2/access/token \ -X POST -k \ -u 8YKCxq72qpjnYmXQ:pcX5BmdJ2f4QLM5RfgsS4jOtxAdTRF \ -d grant_type=client_credentials</pre>
Response
<pre>{"access_token": "d587538f445d30eb2d48e1b7f7a6c9657d32068e", "token_type": "bearer", "expires_in": 86400}</pre>

Token (alternate request)

POST
/api/v2/access/token

An alternative form is supported in which the **client_ID** and **client_secret** are sent in the body, rather than the Authorization header.

Request

Headers

Header	Value
Accept (optional)	application/json
Content-Type	application/x-www-form-urlencoded

Body

grant_type=client_credentials&client_id=s6BhdRkqt3&client_secret=7Fjfp0ZBr1KtDRbnfVdmIw

Response

The response to both forms is the same.

Body

Name	Details
access_token	Access token to return with each API request.
expires_in	Time in seconds that the API session will remain active.
token_type	This will always be bearer.

Name	Details
	<pre>{ "access_token": "2YotnFZFEjrlzCsicMWpAA", "token_type": "bearer", "expires_in": 3600 }</pre>

Example

Request
<pre>curl https://10.110.134.12/api/v2/access/token \ -X POST -k \ -d grant_type=client_credentials \ -d client_id=8YKCxq72qpjnYmXQ \ -d client_secret=pcX5BmdJ2f4QLM5RfgsS4jOtxAdTRF</pre>
Response
<pre>{"access_token": "ee4e077cf457196eb4d27cf6f02686dc07763059", "token_type": "bearer", "expires_in": 86400}</pre>

Validate Token

GET
/api/v2/access/validate_token

Verify if an Access Token is valid and return the time remaining before it expires.

Request

HTTP Headers

Header	Value
Accept (optional)	application/json
Authorization	Bearer <ACCESS_TOKEN>

Response

Body

Name	Details
expires_in	Time in seconds that the API session will remain active.
	<pre>{ 'expires_in': 86399 }</pre>

Example

Request
<pre>curl https://10.110.134.12/api/v2/access/validate_token \ -X GET -k \ -H "Authorization: Bearer ee4e077cf457196eb4d27cf6f02686dc07763059"</pre>
Response
<pre>{"expires_in": 85643}</pre>

Selected APIs

Overview

cnMaestro APIs are defined within the Swagger specification, accessed here <https://docs.cloud.cambiumnetworks.com/api/5.1.1/index.html>. This section only presents additional details for the Device, Statistics and Performance APIs, which have unique responses based upon Device Type, and are difficult to present within Swagger.

cnMaestro v2 API

Beginning with cnMaestro 3.0.0, the API version changes from **v1** to **v2**. The **v1** version will be supported through 3.1.0, but Cambium recommends updating existing API code to use **v2**. For most commands, swapping v1 in the URL with v2 should be sufficient. However, the following APIs may need to be rewritten while moving to the **v2** version.

- AP Groups
- Devices
- Statistics
- Performance
- Mesh Peers
- Operations

There are unique API responses such as:

- [Devices API Response \(v2 Format\)](#)
- [Statistics API Response \(v2 Format\)](#)
- [Performance API Response \(v2 Format\)](#)

Devices API Response (v2 Format)

Name	Details	ePM P	PM P	Wi- Fi	cnRea ch	cnVisi on	PT P	PT P 8xx	cnMatr ix	60 GHz cnWav e	cnWav e 5G Fixed	NS E
profile_ attached	Profile attached to the device			✓								✓
ap_group	AP Group			✓								✓
cbrs_state	CBRS state		✓									
cbrs_status	CBRS status		✓									
config.sync_ reason	Configuration synchronizati on reason	✓	✓	✓	✓	✓	✓	✓	✓			✓
config.sync_ status	Configuration synchronizati on status	✓	✓	✓	✓	✓	✓	✓	✓			✓
config.variabl	Device is	✓	✓	✓	✓	✓	✓	✓	✓			✓

Name	Details	ePM P	PM P	Wi- Fi	cnRea ch	cnVisi on	PT P	PT P 8xx	cnMatr ix	60 GHz cnWav e	cnWav e 5G Fixed	NS E
es	mapped to configuration variables											
config.version	Current configuration version	✓	✓	✓	✓	✓	✓	✓	✓			✓
country	Country	✓	✓	✓		✓						
country_code	Regulatory band						✓					
description	Description	✓	✓	✓	✓	✓	✓		✓	✓		✓
hardware_version	Hardware version	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
inactive_software_version	Inactive software version	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
ip	IP address	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
ipv6	IPv6	✓		✓		✓				✓	✓	
last sync	Last Synchronized							✓				
last_reboot_reason	Reason for the last reboot (see 24.1)	✓	✓	✓	✓	✓	✓		✓		✓	✓
link_symmetry	Link symmetry						✓					
location	Location	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
mac	MAC address	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
managed_account	Managed account name	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
maximum_range	Maximum range (KM)	✓	✓			✓	✓					
mode	Mode type							✓			✓	✓
msn	Manufacturer serial number	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
name	Device name	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
network	Network	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
onboarding.error_code	Error code of the device if it fails to onboard	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Name	Details	ePMP	PMP	Wi-Fi	cnReach	cnVision	PTP	PTP 8xx	cnMatrix	60 GHz cnWave	cnWave 5G Fixed	NSE
onboarding.state	Onboarding state of the device	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
online	Offline or online	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
product	Product name	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
registration_date	Registration date	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
role							✓					
site	Site			✓					✓	✓		✓
site_id	Site unique identifier			✓					✓	✓		
software_version	Active Software version	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
status	Status (online, offline, onboarding).	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
status_time	Uptime/downtime time interval (sec)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
temperature	Temperature							✓				
tower	Tower	✓	✓		✓	✓	✓	✓	✓		✓	
type	Device type (epmp, pmp, wifi-home, wifi-enterprise, cnreach, ptp, cnmatrix, 60ghz-cnwave, nse)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Devices onboarding error codes

Error Codes	Details
ERR_UNSUPPORTED_DEVICE	Claiming {{type}} devices is not currently supported.
ERR_NON_ENTERPRISE_WIFI_TYPE	Only cnPilot Enterprise (ePMP Hotspot), Enterprise Wi-Fi (E-Series and XE/XV-Series) and cnMatrix devices are allowed into Enterprise account.
ERR_NON_WIFI_TYPE	Cannot claim non Wi-Fi device under a Site.
ERR_UNSUPPORTED_	Unsupported device type in current account view - {{view}}.

Error Codes	Details
TYPE	
ERR_UNKNOWN_DEVICE	Unknown Device.
ALREADY_CLAIMED	Device already claimed.
LTE_CLAIMED	cnRanger devices are not supported in production accounts.
ERR_INVALID_MSN	Invalid Serial Number.
ERR_OWNER_DIFFERENT	Device is claimed into another account.
ERR_INTERNAL	System encountered an internal error; please try again later. If the problem persists, contact support.
ERR_INVALID_MAC	Invalid MAC.
ERR_DUPLICATE_KEY	The device is already claimed.
UNPROCESSABLE	Device state does not allow to cloud sync.
CBRS_ERROR_DEVICES	MAC is already claimed. It cannot be claimed on CBRS.
SUBSCRIPTION_FAIL	Device could not acquire slot.
SUBSCRIPTION_FAIL_FEATURE_MISMATCH	Device is mapped to another onprem instance.
SUBSCRIPTION_FAIL_TOO_MANY ASSOCS	Device is mapped to another onprem instance.

Statistics API Response (v2 Format)

Statistics API Response v2 format are shown for the following devices:

- [60 GHz cnWave](#)
- [cnMatrix](#)
- [cnReach](#)
- [Fixed Wireless](#)
- [PTP](#)
- [PTP 820/850](#)
- [Wi-Fi](#)
- [cnWave 5G Fixed](#)

60 GHz cnWave

General

Name	Details	Mode
cpu	CPU utilization	All
last_sync	Last synchronization (UTC Unix time milliseconds)	All
mac	MAC address	All
IP	IP address	All
managed_account	Managed account name	All
memory	Available memory	All
mode	Device mode	All

Name	Details	Mode
name	Device name	All
network	Network	All
site	Site name	All
site_id	Site ID	All
status	Status [online, offline, claimed, waiting, onboarding]	All
status_time	Uptime/downtime interval (seconds)	All
sync_mode	Radio Sync mode [RF, GPS, None]	All
type	Device type	All

Networks

Name	Details	Mode
ipv6	IPv6 address	All

Radios (Array format)

Name	Details	Mode
radios[].channel	Channel	All
radios[].id	Radio Id	All
radios[].mac	Radio MAC	All
radios[].rx_bps	Receive bits per second	All
radios[].sync_mode	Radio Sync mode [RF, GPS, None]	All
radios[].tx_bps	Transmit bits per second	All

Ethernet Ports (Array format)

Name	Details	Mode
ethports[].port	Port name	All
ethports[].rx_pkts	Received packets	All
ethports[].rx_errors	Received packets errors	All
ethports[].rx_pkts_drop	Dropped received packets	All
ethports[].speed	Port speed and duplex	All
ethports[].tx_pkts	Transmitted packets	All
ethports[].tx_errors	Transmitted packets errors	All
ethports[].tx_pkts_drop	Dropped transmitted packets	All

cnMatrix

General

Name	Details
cpu	CPU utilization
config_version	Configuration version
last_sync	Last synchronization (UTC Unix time milliseconds)

Name	Details
mac	MAC address
managed_account	Managed account name
memory	Available memory
mode	Device mode
name	Device name
network	Network
site	Site name
site_id	Site unique identifier
status	Status [online, offline, claimed, waiting, onboarding]
status_time	Uptime/downtime interval (seconds)
tower	Tower name
type	Device type

Networks

Name	Details
ip	IP address

cnReach

General

Name	Details	Mode
config_version	Configuration version	All
connected_sms	Connected SM count	All
last_sync	Last synchronization (UTC Unix time milliseconds)	All
mac	MAC address	All
managed_account	Managed account name	All
mode	Device mode	All
name	Device name	All
network	Network	All
status	Status [online, offline, claimed, waiting, onboarding]	All
status_time	Uptime/downtime interval (seconds)	All
tower	Tower name	All
type	Device type	All

Networks

Name	Details	Mode
ip	IP address	All

Radios (Array format)

Name	Details	Mode
radios[].device_id	Device ID	Radios
radios[].id	Radio Id	Radios
radios[].linked_with	Linked with	Radios
radios[].mac	Radio MAC	Radios
radios[].margin	Margin	Radios
radios[].mode	Radio mode [ap, ep, rep]	Radios
radios[].neighbors	Radio neighbors	Radios
radios[].network_address	Network address	Radios
radios[].noise	Average noise (dB)	Radios
radios[].power	Transmit power	Radios
radios[].rssi	RSSI value (dB)	Radios
radios[].rx_bytes	Receive bytes	Radios
radios[].software_version	Current software version.	Radios
radios[].temperature	Radio temperature	Radios
radios[].type	Radio type [ptp, ptmp]	Radios
radios[].tx_bytes	Transmit bytes	Radios

Fixed Wireless (cnVision, ePMP and PMP)

General

Name	Details	cnVision	ePMP	PMP
ap_mac	AP MAC	SM	SM	SM
config_version	Configuration version	AP/SM	AP/SM	AP/SM
connected_sms	Connected SM count	AP	AP	AP
cpu	CPU utilization			AP/SM
distance	SM distance (KM)	SM	SM	SM
gain	Antenna gain (dBi)	AP/SM	AP/SM	AP/SM
gps_sync_state	GPS synchronization state	AP/SM	AP/SM	
last_sync	Last synchronization (UTC Unix time milliseconds)	AP/SM	AP/SM	AP/SM
mac	MAC address	AP/SM	AP/SM	AP/SM
managed_account	Managed account name	AP/SM	AP/SM	AP/SM
mode	Device mode	AP/SM	AP/SM	AP/SM
name	Device name	AP/SM	AP/SM	AP/SM
network	Network	AP/SM	AP/SM	AP/SM
reboots	Reboot count	AP/SM	AP/SM	
status	Status [online, offline, claimed, waiting, onboarding]	AP/SM	AP/SM	AP/SM
status_time	Uptime/downtime interval (seconds)	AP/SM	AP/SM	AP/SM
temperature	Temperature			AP/SM

Name	Details	cnVision	ePMP	PMP
tower	Tower name	AP	AP	AP
type	Type	AP/SM	AP/SM	AP/SM
vlan	VLAN			AP/SM

Networks

Name	Details	cnVision	ePMP	PMP
default_gateway	Default gateway	AP/SM	AP/SM	AP/SM
ip	IP address	AP/SM	AP/SM	AP/SM
ipv6	IPv6 address	AP/SM	AP/SM	
ip_dns	DNS	AP/SM	AP/SM	AP/SM
ip_dns_secondary	Secondary DNS			AP/SM
ip_wan	WAN IP	AP/SM	AP/SM	
lan_mode_status	LAN mode status [no-data, half, full]	AP/SM	AP/SM	
lan_mtu	MTU size	SM	SM	
lan_speed_status	LAN speed status	AP/SM	AP/SM	
lan_status	LAN status [down, up]	AP/SM	AP/SM	AP/SM
netmask	Network mask	AP/SM	AP/SM	AP/SM

Radios

Name	Details	cnVision	ePMP	PMP
radio.auth_mode	Authentication mode	SM	SM	
radio.auth_type	Authentication type ePMP [open, wpa1, eap-ttls] PMP [disabled, enabled]	AP/SM	AP/SM	AP/SM
radio.channel_width	Channel width ePMP [5 MHz, 10 MHz, 20 MHz, 40 MHz] PMP [...]	AP/SM	AP/SM	AP/SM
radio.color_code	Color code			AP/SM
radio.dfs_status	DFS status ePMP: [not-applicable, channel-availability-check, in-service, radar-signal-detected, alternate-channel-monitoring, not-in-service] PMP: [Status String]	AP/SM	AP/SM	AP/SM
radio.dl_err_drop_pkts	Downlink error drop packets	SM	SM	
radio.dl_err_drop_pkts_percentage	Downlink error drop packets percentage	SM	SM	
radio.frequency	RF frequency	AP/SM	AP/SM	AP/SM
radio.frame_period	Frame period			AP
radio.dl_frame_utilization	Downlink frame utilization			AP
radio.dl_lqi	Downlink Link Quality Indicator			SM

Name	Details	cnVision	ePMP	PMP
radio.dl_mcs	Downlink MCS	SM	SM	
radio.dl_modulation	Downlink Modulation			SM
radio.dl_pkts	Downlink packet count	AP/SM	AP/SM	AP/SM
radio.dl_pkts_loss	Downlink packet loss			AP/SM
radio.dl_retransmits	Downlink Retransmission	AP/SM	AP/SM	
radio.dl_retransmits_pct	Downlink Retransmission percentage	AP/SM	AP/SM	
radio.dl_rssi	Downlink RSSI	SM	SM	SM
radio.dl_rssi_imbalance	Downlink RSSI imbalance			AP
radio.dl_snr	Downlink SNR (dB)	SM	SM	
radio.dl_snr_h	Downlink SNR (dB) horizontal			SM
radio.dl_snr_v	Downlink SNR (dB) vertical			SM
radio.dl_throughput	Downlink throughput	AP/SM	AP/SM	AP/SM
radio.mac	Wireless MAC	AP/SM	AP/SM	
radio.mode	Radio mode [eftp-master, eftp-slave, tdd, tdd-ptp, ap/sm]	AP/SM	AP/SM	
radio.sessions_dropped	Session drops	AP	AP	AP/SM
radio.software_key_throughput	Software key – max throughput			SM
radio.ssid	SSID	AP/SM	AP/SM	
radio.sync_source	Synchronization source			AP
radio.sync_state	Synchronization state			AP
radio.tdd_ratio	TDD ratio ePMP [75/25, 50/50, 30/70, flexible] PMP [...]	AP	AP	AP
radio.tx_capacity	SM transmit capacity	SM	SM	
radio.tx_power	Radio transmit power	AP/SM	AP/SM	AP/SM
radio.tx_quality	SM transmit quality	SM	SM	
radio.ul_err_drop_pkts	Uplink error drop packets	SM	SM	
radio.ul_err_drop_pkts_percentage	Uplink error drop packets percentage	SM	SM	
radio.ul_frame_utilization	Uplink frame utilization			AP
radio.ul_mcs	Uplink MCS	AP/SM	AP/SM	
radio.ul_modulation	Uplink Modulation example [2X MIMO-B]			SM
radio.ul_lqi	Uplink Link Quality Indicator			SM
radio.ul_pkts	Uplink packet count	AP/SM	AP/SM	AP/SM
radio.ul_pkts_loss	Uplink packet loss			AP/SM
radio.ul_retransmits	Uplink Retransmission	SM	SM	
radio.ul_retransmits_pct	Uplink Retransmission percentage	AP/SM	AP/SM	
radio.ul_rssi	Uplink RSSI	SM	SM	SM
radio.ul_snr	Uplink SNR (dB)	SM	SM	

Name	Details	cnVision	ePMP	PMP
radio.ul_snr_h	Uplink SNR (dB) horizontal			SM
radio.ul_snr_v	Uplink SNR (dB) vertical			SM
radio.ul_throughput	Uplink throughput	AP/SM	AP/SM	AP/SM
radio.wlan_status	WLAN status [down, up]	AP/SM	AP/SM	

PTP 650/670/700

General

Name	Details	Mode
config_version	Configuration version	All
connected_sms	Connected SM count	Master
gain	Antenna gain (dBi)	All
last_sync	Last synchronization (UTC Unix time milliseconds)	All
mac	MAC address	All
managed_account	Managed account name	All
mode	Device mode	All
name	Device name	All
network	Network	All
status	Status [online, offline, claimed, waiting, onboarding]	All
status_time	Uptime/downtime interval (seconds)	All
temperature	Temperature	All
tower	Tower name	All
type	Device type	All
vlan	VLAN	All

Networks

Name	Details	Mode
default_gateway	Default gateway	All
ip	IP address	All
ip_dns	DNS	All
ip_dns_secondary	Secondary DNS	All
lan_status	LAN status [down, up]	All
netmask	Network mask	All

Ethernet Ports (Array format)

Name	Details	Mode
ethports[].port	Port name	All
ethports[].rx_frames	Ports receive frames oversize	All
ethports[].rx_util	Ports receive bandwidth utilization	All
ethports[].speed	Ports speed and duplex	All
ethports[].tx_util	Ports transmit bandwidth utilization	All

Radios

Name	Details	Mode
radio.byte_error_ratio	Byte Error Ratio	All
radio.channel_width	Channel width ePMP: [5 MHz, 10 MHz, 20 MHz, 40 MHz] PMP: [...]	All
radio.color_code	Color code	All
radio.rx_frequency	Receive frequency	All
radio.tx_frequency	Transmit frequency	All
radio.tx_power	Radio transmit power	All

PTP 820/850

General

Name	Details	Mode
ip	IP address	All
last_sync	Last synchronized	All
mac	MAC address	All
managed_account	Managed account name	All
mode	Device mode	All
name	Device name	All
network	Network	All
status	Status [online, offline, claimed, waiting, onboarding]	All
status_time	Uptime/downtime interval (seconds)	All
temperature	Temperature	All
tower	Uptime/downtime interval (seconds)	All
type	Device type	All

Radio

Name	Details	Mode
radios[].defective_blocks	Radio defective blocks	All
radios[].id	Radio Id	All
radios[].radio_location	Radio location	All
radios[].rx_bps	Receive bits/second	All
radios[].rx_level	Receive level	All
radios[].rx_frequency	Receive frequency	All
radios[].tx_bps	Transmit bits/second	All
radios[].tx_level	Transmit level	All
radios[].tx_frequency	Transmit frequency	All
radios[].tx_mute_status	Transmit mute status	All
radios[].modem_mse	Modem Mean Square Error (MSE) in dB	All
radios[].modem_xpi	Modem Cross-Polar Isolation (XPI) in dB	All

Interfaces

Name	Details	Mode
interfaces[].admin_state	Admin state	All
interfaces[].auto_negotiation	Auto Negotiation	All
interfaces[].interface_location	Interface location	All
interfaces[].mac	MAC address	All
interfaces[].media_type	Media type	All
interfaces[].operational_status	Operational Status	All
interfaces[].port_duplex	Interface duplex type	All
interfaces[].speed	Interface speed	All

Wi-Fi



Note

Mode is Enterprise, Home, or All.

General

Name	Details	Mode
config_version	Configuration version	All
cpu	CPU utilization	All
mac	MAC address	All
managed_account	Managed account name	All
memory	Available memory	All
mode	Device mode	All
name	Device name	All
network	Network	All
parent_mac	Parent MAC	All
site	Site name	All
site_id	Site unique identifier	All
status	Status [online, offline, claimed, waiting, onboarding]	All
status_time	Uptime/downtime interval (seconds)	All
type	Device type	All

Networks

Name	Details	Mode
ip	IP address	All
ipv6	IPv6 address	All
ip_dns	DNS	All
ip_dns_secondary	Secondary DNS	All
ip_wan	WAN IP	All
lan_mode_status	LAN mode status [no-data, half, full]	Enterprise
lan_speed_status	LAN speed status	All

Name	Details	Mode
lan_status	LAN status [down, up]	Home
netmask	Network mask	All

Radios (Array format)

Name	Details	Mode
radios[].airtime	Airtime	All
radios[].band	Radio band	All
radios[].bssid	Radio mac	Enterprise
radios[].channel	Channel	All
radios[].id	Radio Id	All
radios[].multicast_rate	Multicast rate	Enterprise
radios[].noise_floor	Noise floor	Enterprise
radios[].num_clients	Number of clients	All
radios[].num_wlans	Number of WLANs	Enterprise
radios[].power	Transmit power	All
radios[].quality	RF Quality description	Enterprise
radios[].radio_state	Radio state	Enterprise
radios[].rx_bps	Receive bits/second	All
radios[].rx_bytes	Receive bytes	All
radios[].tx_bps	Transmit bits/second	All
radios[].tx_bytes	Transmit bytes	All
radios[].unicast_rates	Unicast rates	Enterprise
radios[].utilization	Radio utilization	Enterprise

cnWave 5G Fixed

General

Name	Details	Mode
cpu	CPU utilization	All
last_sync	Last synchronization (UTC Unix time milliseconds)	All
mac	MAC address	All
managed_account	Managed account name	All
ip	IP Address	All
mode	Device mode	All
name	Device name	All
network	Network	All
tower	Tower name	All
status	Status [online, offline, claimed, waiting, onboarding]	All
status_time	Uptime/downtime interval (seconds)	All
config_version	Current config version	All
type	Device type	All

Name	Details	Mode
connected_cpe	Number of CPEs connected to the BTS	BTS
registered_cpe	Number of CPEs registered with the BTS	BTS
cpe_registration_state	CPEs Registration State	CPE
cpe_registration_count	CPEs Registration Count	CPE
cpe_imsi	CPE Device Identity	CPE

Boot

Name	Details	Mode
startup_count	Startup Count for the device	BTS
startup_reason	Startup Reason for the device	BTS

Shutdown (Array format)

Name	Details	Mode
shutdown[].date	Shutdown Date	BTS
shutdown[].detail	Shutdown Detail	BTS
shutdown[].index	Shutdown Index	BTS
shutdown[].reason	Shutdown Reason	BTS

Interface Config

Name	Details	Mode
sfp1_speed	SFP1 Speed	BTS
sfp2_speed	SFP2 Speed	BTS

Interfaces (Array format)

Name	Details	Mode
interfaces[].port_name	Port name	BTS
interfaces[].in_octets	Received octets	BTS
interfaces[].out_octets	Transmitted octets	BTS
interfaces[].in_ucast_pkts	Received unicast packets	BTS
interfaces[].out_ucast_pkts	Transmitted unicast packets	BTS
interfaces[].in_mcast_pkts	Received multicast packets	BTS
interfaces[].out_mcast_pkts	Transmitted multicast packets	BTS
interfaces[].in_bcast_pkts	Received broadcast packets	BTS
interfaces[].out_bcast_pkts	Transmitted broadcast packets	BTS
interfaces[].in_discards	Received discarded packets	BTS
interfaces[].out_discards	Transmitted discarded packets	BTS
interfaces[].in_errors	Received errored packets	BTS
interfaces[].out_errors	Transmitted errored packets	BTS

Radio

Name	Details	Mode
dl_throughput	Received Throughput	BTS
ul_throughput	Transmitted Throughput	BTS
frequency	Frequency	BTS
max_eirp	Maximum EIRP	BTS
polarization	Polarization	All
link_symmetry	Link Symmetry	BTS
bandwidth	Bandwidth	BTS
ul_target_rxPower	Transmitted Target Power	BTS
ul_tx_power_init	Transmitted Initial Power	BTS
ul_tx_power_cont	Transmitted Control Power	BTS
ul_frame_util	Transmitted Frame Utilization	BTS
dl_frame_util	Received Frame Utilization	BTS
dl_mcs	Downlink MCS	CPE
ul_mcs	Uplink MCS	CPE
alignment_active	Alignment Active Status	CPE
cpe_range	Range of CPE	CPE
current_eirp	Current Effective radiated power	CPE
ul_backoff	Uplink Backoff	CPE
dl_backoff	Downlink Backoff	CPE
ul_sounding_state	Uplink Sounding State	CPE
dl_sounding_state	Downlink Sounding State	CPE
ul_channel_distortion	Uplink Channel Distortion	CPE
dl_channel_distortion	Downlink Channel Distortion	CPE
ul_evm	Uplink EVM	CPE
dl_evm	Downlink EVM	CPE
ul_rx_power	Uplink Received Power	CPE
dl_rx_power	Downlink Received Power	CPE
ul_spatial_freq	Uplink Spatial Frequency	CPE
dl_spatial_freq	Downlink Spatial Frequency	CPE

Wireless and Ethernet interfaces

Name	Details	Mode
in_octets	Received octets	CPE
out_octets	Transmitted octets	CPE
in_ucast_pkts	Received unicast packets	CPE
out_ucast_pkts	Transmitted unicast packets	CPE
in_mcast_pkts	Received multicast packets	CPE
out_mcast_pkts	Transmitted multicast packets	CPE

Name	Details	Mode
in_bcast_pkts	Received broadcast packets	CPE
out_bcast_pkts	Transmitted broadcast packets	CPE
in_discards	Received discarded packets	CPE
out_discards	Transmitted discarded packets	CPE
in_errors	Received errored packets	CPE
out_errors	Transmitted errored packets	CPE

Performance API Response (v2 Format)

Performance API Response v2 Format are shown for following devices:

- [60 GHz cnWave](#)
- [cnMatrix](#)
- [cnReach](#)
- [Fixed Wireless](#)
- [PTP 650/670/700](#)
- [PTP 820/850](#)
- [Wi-Fi](#)
- [cnWave 5G Fixed](#)

60 GHz cnWave

General

Name	Details	Mode
mac	MAC address	All
managed_account	Managed account name	All
mode	Device mode	All
name	Device name	All
network	Network	All
online_duration	Duration of device connection with server (seconds)	All
site	Site	All
timestamp	Timestamp	All
type	Device type	All
uptime	Device online time (seconds)	All

Radios (Array format)

Name	Details	Mode
radios[].id	Radio ID	All
radios[].rx_bps	Receive bits per second	All
radios[].tx_bps	Transmit bits per second	All

Ethernet Ports (Array format)

Name	Details	Mode
ethports[].max_rx	Ports maximum receive bytes	All
ethports[].max_tx	Ports maximum transmit bytes	All
ethports[].min_rx	Ports minimum receive bytes	All
ethports[].min_tx	Ports minimum transmit bytes	All
ethports[].port	Port name	All
ethports[].rx	Ports receive bytes	All
ethports[].tx	Ports transmit bytes	All
ethports[].rx_bps	Ports receive bits per second	All
ethports[].tx_bps	Ports receive bits per second	All
ethports[].min_rx_bps	Ports minimum receive bits per second	All
ethports[].min_tx_bps	Ports minimum transmit bits per second	All
ethports[].max_rx_bps	Ports maximum receive bits per second	All
ethports[].max_tx_bps	Ports maximum transmit bits per second	All

cnMatrix

General

Name	Details
mac	MAC address
managed_account	Managed account name
mode	Device mode
name	Device name
network	Network
site	Site
timestamp	Timestamp
tower	Tower
type	Device type

Switch

Name	Details
switch.rx.broadcast_pkts	Receive broadcast packets
switch.dl_kbits	Downlink usage (in kbits on hour or minute basis)
switch.dl_throughput	Downlink throughput (Kbps)
switch.ul_kbits	Uplink (in Kbits on hour or minute basis)
switch.rx.multicast_pkts	Receive multicast packets
switch.ul_throughput	Uplink throughput (Kbps)
switch.rx.pkts_err	Receive Packet error
switch.rx.unicast_pkts	Receive unicast packets
switch.tx.broadcast_pkts	Transmit broadcast packets

Name	Details
switch.tx.multicast_pkts	Transmit multicast packets
switch.tx.pkts_err	Transmit packet error
switch.tx.unicast_pkts	Transmit unicast packets

cnReach

General

Name	Details	Mode
mac	MAC address	All
managed_account	Managed account name	All
mode	Device mode	All
name	Device name	All
network	Network	All
online_duration	Duration of device connection with server (seconds)	All
sm_count	Connected SM count	All
timestamp	Timestamp	All
tower	Tower	All
type	Device type	All
uptime	Device online time (seconds)	All

Radios (Array format)

Name	Details	Mode
radios[].id	Radio ID	Radios
radios[].neighbors	Radio neighbors	Radios
radios[].noise	Average noise	Radios
radios[].power	Transmit power	Radios
radios[].rssi	RSSI value	Radios
radios[].rx_bytes	Receive bytes	Radios
radios[].throughput	Total throughput	Radios
radios[].tx_bytes	Transmit bytes	Radios

Fixed Wireless (cnVision, ePMP and PMP)

General

Name	Details	cnVision	ePMP	PMP
mac	MAC address	AP/SM	AP/SM	AP/SM
managed_account	Managed account name	AP/SM	AP/SM	AP/SM
mode	Device mode	AP/SM	AP/SM	AP/SM
name	Device name	AP/SM	AP/SM	AP/SM
network	Network	AP/SM	AP/SM	AP/SM

Name	Details	cnVision	ePMP	PMP
online_duration	Duration of device connection with server (seconds)	AP/SM	AP/SM	AP/SM
sm_count	Connected SM count	AP	AP	AP
sm_drops	Session drops	AP/SM	AP/SM	AP
timestamp	Timestamp	AP/SM	AP/SM	AP/SM
tower	Tower	AP/SM	AP/SM	AP/SM
type	Device type	AP/SM	AP/SM	AP/SM
uptime	Device online time (seconds)	AP/SM	AP/SM	AP/SM

Radios

Name	Details	cnVision	ePMP	PMP
radio.dl_frame_utilization	Downlink frame utilization			AP
radio.dl_kbits	Downlink usage (in Kbits on hour or minute basis)	AP/SM	AP/SM	
radio.dl_mcs	Downlink MCS	SM	SM	
radio.dl_modulation	Downlink modulation			SM
radio.dl_pkts	Downlink packet count	AP/SM	AP/SM	
radio.dl_pkts_loss	Downlink packet loss			AP/SM
radio.dl_retransmits_pct	Downlink retransmission percentage	AP/SM	AP/SM	
radio.dl_rssi	Downlink RSSI	SM	SM	SM
radio.dl_rssi_imbalance	Downlink RSSI imbalance			SM
radio.dl_snr	Downlink SNR	SM	SM	
radio.dl_snr_h	Downlink SNR (dB) horizontal			SM
radio.dl_snr_v	Downlink SNR (dB) vertical			SM
radio.dl_throughput	Downlink Throughput (Kbps)	AP/SM	AP/SM	AP/SM
radio.ul_frame_utilization	Uplink frame utilization			AP
radio.ul.kbits	Uplink usage (in Kbits on hour or minute basis)	AP/SM	AP/SM	
radio.ul_mcs	Uplink MCS	SM	SM	
radio.ul_modulation	Uplink modulation			SM

Name	Details	cnVision	ePMP	PMP
radio.ul_pkts	Uplink packet count	AP/SM	AP/SM	
radio.ul_pkts_loss	Uplink packet loss			AP/SM
radio.ul_retransmits_pct	Uplink Retransmission percentage	AP/SM	AP/SM	
radio.ul_rssi	Uplink RSSI	SM	SM	SM
radio.ul_snr	Uplink SNR	SM	SM	
radio.ul_snr_h	Uplink SNR (dB) horizontal			SM
radio.ul_snr_v	Uplink SNR (dB) vertical			SM
radio.ul_throughput	Uplink Throughput (Kbps)	AP/SM	AP/SM	AP/SM

PTP 650/670/700

General

Name	Details	Mode
mac	MAC address	All
managed_account	Managed account name	All
mode	Device mode	All
name	Device name	All
network	Network	All
sm_count	Connected SM count	Master
timestamp	Timestamp	All
tower	Tower	All
type	Device type	All

Ethernet Ports (Array format)

Name	Details	Mode
ethports[].max_rx	Ports maximum receive bytes	All
ethports[].max_tx	Ports maximum transmit bytes	All
ethports[].min_rx	Ports minimum receive bytes	All
ethports[].min_tx	Ports minimum transmit bytes	All
ethports[].pkt_error	Ports packet error	All
ethports[].port	Port name	All
ethports[].rx	Ports receive bytes	All
ethports[].tx	Ports transmit bytes	All
ethports[].rx_bps	Ports receive bits per second	All
ethports[].tx_bps	Ports receive bits per second	All
ethports[].min_rx_bps	Ports minimum receive bits per second	All
ethports[].min_tx_bps	Ports minimum transmit bits per second	All

Name	Details	Mode
ethports[].max_rx_bps	Ports maximum receive bits per second	All
ethports[].max_tx_bps	Ports maximum transmit bits per second	All

Ethernet

Name	Details	Mode
ethernet.link_loss	Link loss	All
ethernet.pcb_temperature	PCB temperature	All
ethernet.rx_channel_util	Receive channel utilization	All
ethernet.rx_capacity	Receive capacity	All
ethernet.ssr	Signal strength ratio	All
ethernet.rx_power	Receive power	All
ethernet.sfp_interface.tx	SFP transmit bytes	All
ethernet.rx_throughput	Receive throughput	All
ethernet.tx_channel_util	Transmit channel utilization	All
ethernet.tx_capacity	Transmit capacity	All
ethernet.tx_power	Transmit power	All
ethernet.tx_throughput	Transmit throughput	All
ethernet.vector_error	Vector error	All

PTP 820/850

General

Name	Details	Mode
mac	MAC address	All
managed_account	Managed account name	All
mode	Device Mode	All
name	Device name	All
network	Network	All
online_duration	Duration online	All
timestamp	Timestamp	All
tower	Tower	All
type	Device type	All
uptime	Device online time (seconds)	All

Radio

Name	Details	Mode
radios[].id	Radio ID	All
radios[].max_rsl	Radio Maximum Receiver Signal Level	All
radios[].max_tsl	Radio Maximum Transmission Signal Level	All
radios[].min_rsl	Radio Minimum Receiver Signal Level	All

Name	Details	Mode
radios[].min_tsl	Radio Minimum Transmission Signal Level	All
radios[].peak_throughput	Radio Peak Throughput	All
radios[].radio_location	Radio Location	All
radios[].throughput	Radio Throughput	All
radios[].modem_max_mse	Modem maximum MSE in dB	All
radios[].modem_min_mse	Modem minimum MSE in dB	All
radios[].modem_max_xpi	Modem maximum XPI in dB	All
radios[].modem_min_xpi	Modem minimum XPI in dB	All
radios[].modem_max_mrmc_profile	Modem maximum MMRC	All
radios[].modem_min_mrmc_profile	Modem minimum MMRC	All

Radio Groups

Name	Details	Mode
radios_groups[].id	Radio Group ID	All
radios_groups[].peak_throughput	Radio Group peak throughput	All
radios_groups[].radio_location	Radio Group location	All
radios_groups[].throughput	Radio Group throughput	All

Wi-Fi

General

Name	Details	Mode
mac	MAC address	All
managed_account	Managed account name	All
mode	Device mode	All
name	Device name	All
network	Network	All
online_duration	Duration of device connection with server (seconds)	All
site	Site	All
timestamp	Timestamp	All
type	Device type	All
uptime	Device online time (seconds)	All

Radios (Array format)

Name	Details	Mode
radios[].clients	Number of clients	All
radios[].id	Radio ID	All
radios[].rx_bps	Receive bits/second	All
radios[].throughput	Total throughput	All
radios[].tx_bps	Transmit bits/second	All
radios[].band	Radio band (2.4 GHz/5 GHz)	All

General

Name	Details	Mode
mac	MAC address	All
managed_account	Managed account name	All
mode	Device mode	All
name	Device name	All
network	Network	All
online_duration	Duration of device connection with server (seconds)	All
timestamp	Timestamp	All
type	Device type	All
uptime	Device online time (seconds)	All
cpe_registered	Registered CPEs count	BTS
cpe_connected	Connected CPEs count	BTS
cpe_registrationCnt	Number of times the CPE registered with the BTS	CPE

Radio

Name	Details	Mode
ul_throughput	Uplink Throughput	BTS
dl_throughput	Downlink Throughput	BTS
cpe_ul_throughput	Uplink Throughput	CPE
cpe_dl_throughput	Downlink Throughput	CPE
cpe_ul_evm	Uplink EVM	CPE
cpe_dl_evm	Downlink EVM	CPE
cpe_ul_mcs	Uplink MCS	CPE
cpe_dl_mcs	Downlink MCS	CPE
cpe_ul_rxPower	Uplink Rx Power	CPE
cpe_dl_rxPower	Downlink Rx Power	CPE

Client API Response (v2 Format)

Client details API Response v2 format are shown below:

Name	Details	Wi-Fi
ap_mac	AP MAC	
client_type	Client type(Client Guest Client)	
download_quota	Download quota (Note: only applicable for Guest Client)	
download_quota_balance	Download quota balance (Note: only applicable for Guest Client)	
ip	IP address of client	
mac	Client MAC	

Name	Details	Wi-Fi
managed_account	Managed account name	
manufacturer	Manufacturer name	
name	Client name	
radio.band	Band(2.4 GHz/5 GHz)	
radio.rssi	RSSI	
radio.rx_bytes	Received bytes	
radio.snr	SNR	
radio.ssid	SSID	

External Guest Access Login API

Integrates an external captive portal with the Cambium Networks AP while posting directly to cnMaestro. This API provides the support for the external captive portal to make login requests.

POST /api/v2/ext-portals/login

Request:

curl -X

```
/api/v2/ext-portals/login" -H "accept: */*" -H "Authorization: Bearer
e88916f5b663c1ea966af835c8a0a19c20d17686" -H "Content-Type: application/json"-d
```

Body

```
"{"ga_ap_mac":"11-22-33-44-55-66","ga_cmac":"11-22-33-44-55-65","ga_
Qv":"eUROBR86HBgAGDEEVgQAGw4UWRUCACYVMgFPMV5ZWVFfUVdGX1ZFJXxZR1dLBhMUMww","ga_
user":"test-user","ga_pass":"test-pass"}"
```

Response:

```
{
  "data": {
    "mType": 3,
    "msgId": 28,
    "status": <integer values>,
    "prefixQs": <true/false>,
    "expiry": <integer values>,
    "action": <integer values>,
    "cmac": <client mac>,
    "msg": <Radius Returned Message>,
    "extURL": <external url string>
  }
}
```

The status value description is provided in the table below.

Status	Description
0	Login is successful.
1	Invalid login request, the client is not currently associated to the AP which is being requested for login here.
2	RADIUS reject due to invalid username/password.
3	RADIUS timeout, AP didn't received the RADIUS response.
4	Missing RADIUS server config on the WLAN config of the AP.

Status	Description
5	If LDAP configured on the AP for authentication then LDAP server responded back with reject.
6	LDAP timeout happened on the AP for the request.
7	Missing LDAP configuration on the WLAN configuration of the AP.
8	Logout is successful.
9	Logout failed due to missing session on the AP. Most likely client session is already deleted from this AP.

The response parameter name and details is shown below.

Name	Details
action	0: On success action redirects the user to AP onboard logout page. 1: On success redirects user to an external URL. 2: On success redirects user to its original URL.
cmac	MAC address of the client.
expiry	Displays the session time for the given guest session.
msg	Message is based on RADIUS attribute reply message (18) in the RADIUS Access Accept or Reject message.
prefixQs	True: Add query strings to landing URL on success. False: Remove query strings from landing URL on success. <code>prefixQs</code> and <code>action</code> values are driven based on WLAN configuration.

60 GHz cnWave RESTful API

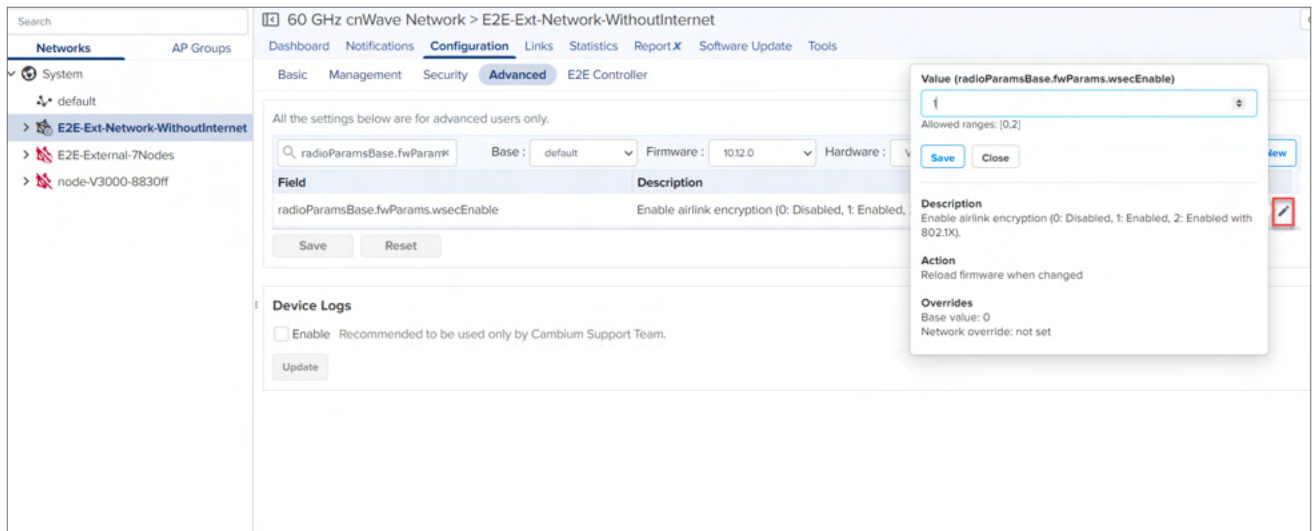
cnMaestro supports configuration overrides for 60 GHz cnWave E2E Network, E2E Controller, and Node(s) using the RESTful API.

E2E Network

To determine the configuration parameters available in an E2E Network, navigate to **E2E Network > Configuration > Advanced**. Search for the desired **Field**, and review its **Description**, allowed **Values**, and **Override status**. Use the RESTful API to override single or multiple fields.

GET /api/v2/cnwave60/networks/{network_id}/configuration

PUT /api/v2/cnwave60/networks/{network_id}/configuration



Field names are separated by dots. Each substring between the dots will be converted to objects and the last substring will be the key and value.

Example

In case of field name `radioParamsBase.fwParams.wsecEnable`, payload will be:

```
{
  "radioParamsBase": {
    "fwParams": {
      "wsecEnable": 1
    }
  }
}
```



Warning

Partial update is not allowed. Always send full configuration that needs to be pushed to E2E Network.

Optimization

To determine the optimization parameters available in an E2E Network, navigate to **E2E Network > Configuration > Advanced**.

GET `/api/v2/cnwave60/networks/{network_id}/optimization/{optimization_type}`

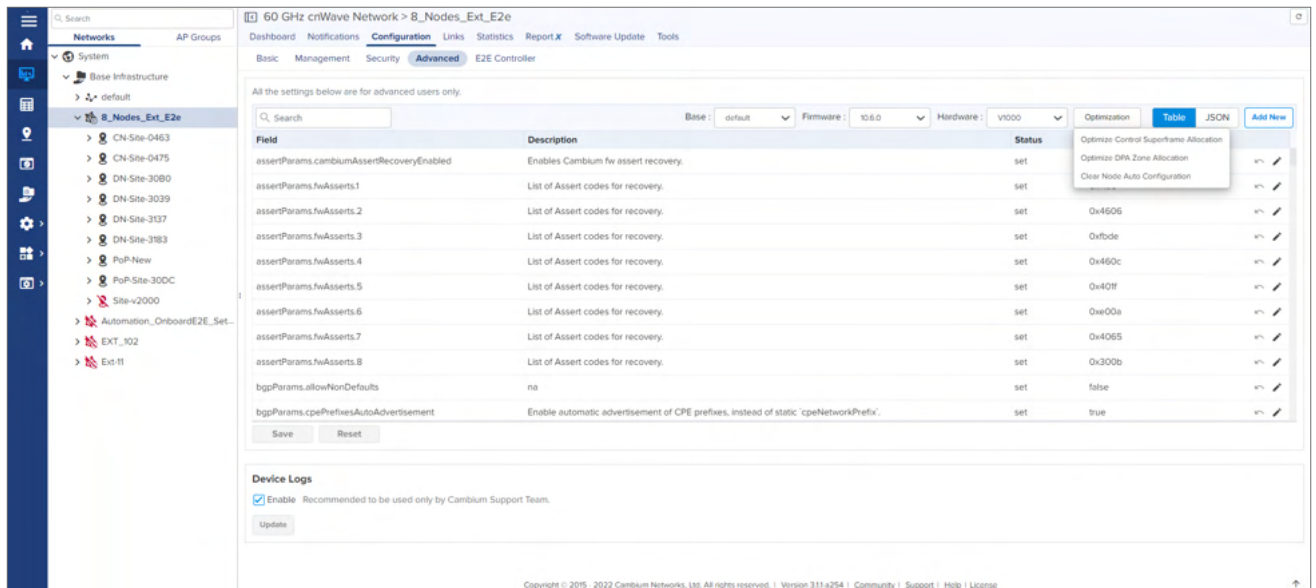
PUT `/api/v2/cnwave60/networks/{network_id}/optimization/{optimization_type}`

Available values :

`controlSuperframeAllocation,`

`dpaZoneAllocation`

`clearNodeAutoConfig`



Example

```
{
  "clearUserConfig": true,
  "nodes": [
    "string"
  ],
  "configPaths": "string"
}
```

Device (Node) Configuration

To update Device configuration, navigate to **Node > Configuration > Advanced**. Search for the **Field**, and review its **Description**, allowed **Values**, and **Overrides status**. Use the RESTful API to override those fields.

GET /api/v2/cnwave60/networks/{mac}/configuration

PUT /api/v2/cnwave60/networks/{mac}/configuration

Field names are separated by dots. Each substring between the dots will be converted to objects and the last substring will be the key and value.

Example

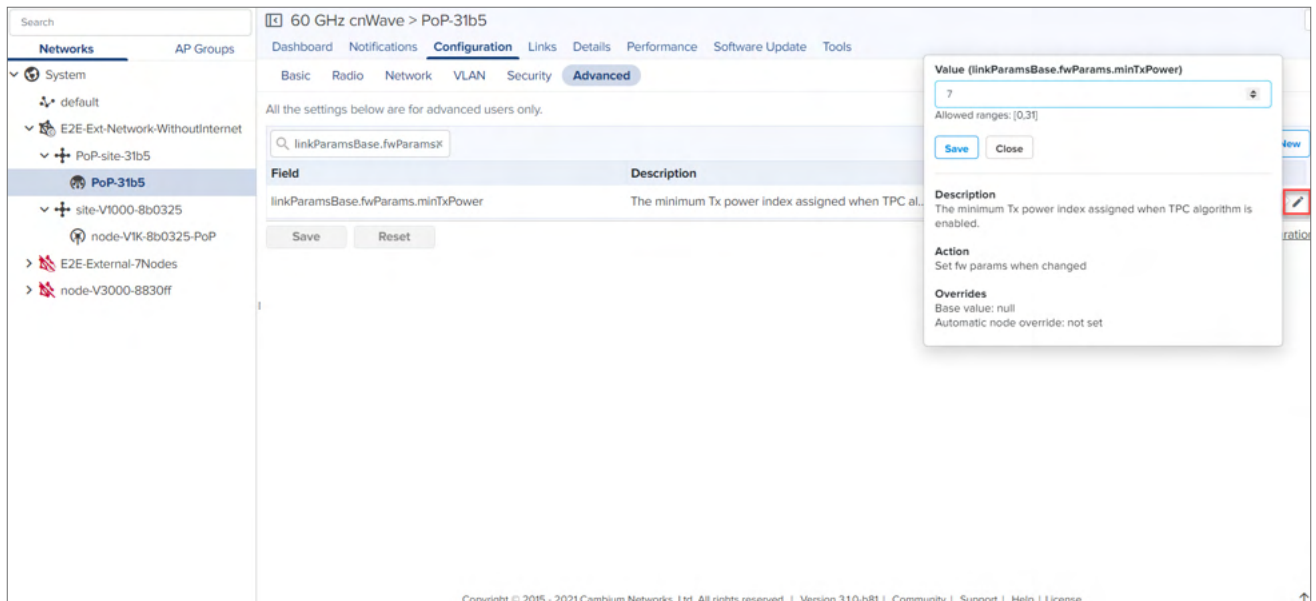
In case of field name `linkParamsBase.fwParams.minTxPower`, object to send in the API payload will be:

```
{
  "linkParamsBase": {
    "fwParams": {
      "minTxPower": 6
      "maxTxPower": 8
    }
  }
}
```

The below two APIs are introduced in Release 3.1.0 to update multiple device configurations overrides.

GET /api/v2/cnwave60/networks/{network_id}/devices/overrides

PUT /api/v2/cnwave60/networks/{network_id}/devices/overrides



Warning

Partial update is not allowed. Always send full configuration that needs to be pushed to 60 GHz cnWave Devices.

The example payload for PUT request is seen from cnMaestro UI.

Example

```
{
  "device1_name": {
    "radioParamsBase": {
      "fwParams": {
        "txPower": 6
      }
    }
  },
  "device2_name": {
    "popParams": {
      "POP_IFACE": "nic2"
    }
  }
}
```



Note

You can download the full config of the node by clicking on the **Show Full Configuration** as well and then get the JSON key and pass in RESTful API.

E2E Controller

To update E2E Controller configuration, navigate to **E2E Network > Configuration > E2E Controller**. Search for the desired **Field**, and review its **Description**, allowed **Values**, and **Override status**. Use the RESTful API to override those fields.

GET /api/v2/cnwave60/networks/{network_id}/controller/configuration

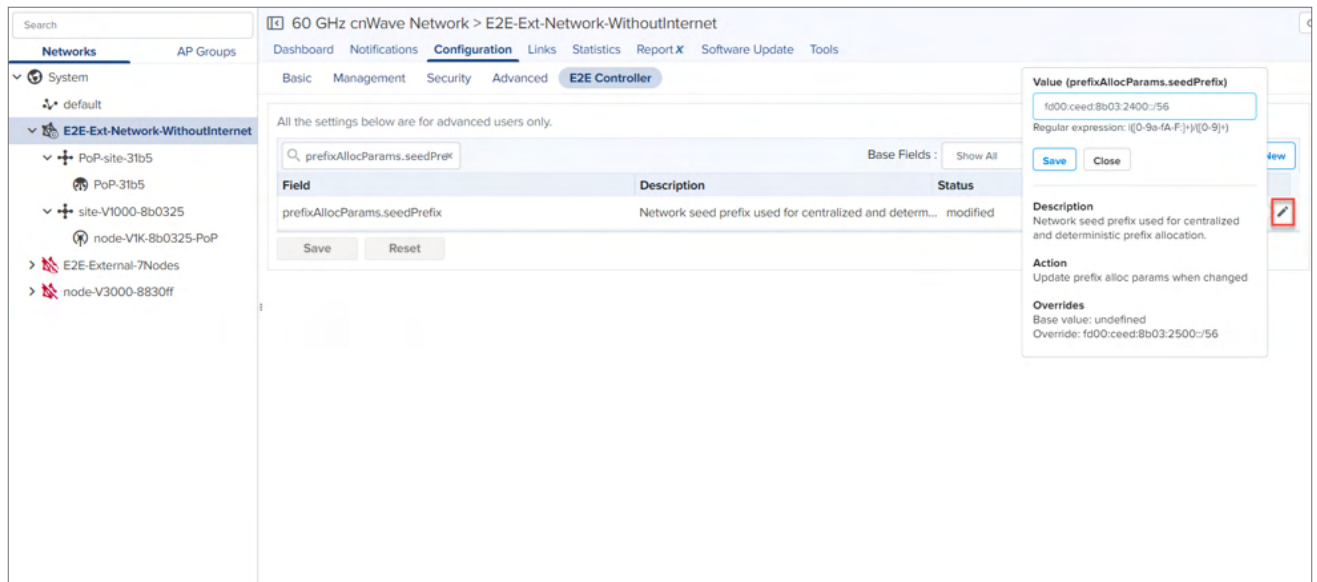
PUT /api/v2/cnwave60/networks/{network_id}/controller/configuration

Field names are separated by dots. Each substring between the dots will be converted to objects and the last substring will be the key and value.

Example

In case of field name `prefixAllocParams.seedPrefix`, payload will be:

```
{
  "prefixAllocParams": {
    "seedPrefix": "fd00:ceed:1992:1400::/56"
  }
}
```



Warning

Partial update is not allowed. Always send full configuration that needs to be pushed to the E2E Controller.

Guest Access

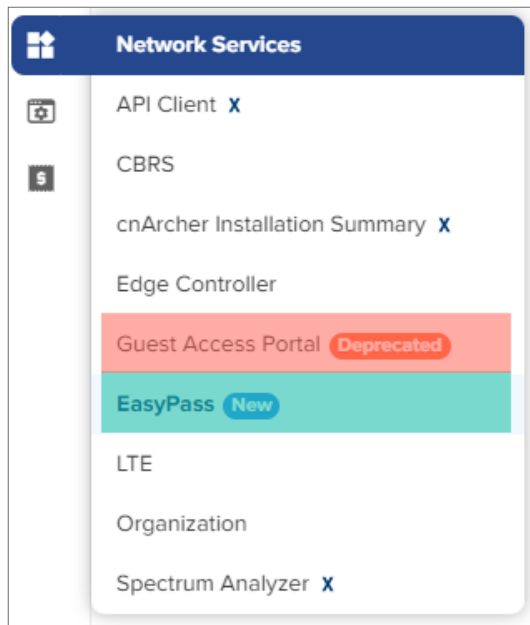
This section describes how to configure Guest Access using cnMaestro. This feature allows the clients to connect to the internet through Free Tier, Vouchers, or Paid Access types.



Note

From cnMaestro 5.1.0 release onwards, the **Guest Access Portal** configuration wizard is deprecated, and a new wizard called **EasyPass** is introduced, as shown in [Figure 488](#).

Figure 488 *Network Services*



Note

For information on EasyPass, see [EasyPass](#).

The Guest Access feature creates a separate network for guests by providing Internet access to guest wireless devices such as mobiles, tabs, and laptops.



Note

The Guest Access feature is supported only on Enterprise Wi-Fi devices.

Configuration

- Create the Guest Access Portal in cnMaestro
- Map the device to cnMaestro

Creating the Guest Access Portal in cnMaestro

1. [Basic Details](#)
2. [Access Portal](#)
3. [Design Page](#)
4. [Sessions](#)
5. [Guests](#)

Procedure for Creating Guest Access

1. Navigate to **Network Services > Guest Access Portal**.

Services > Guest Access Portal

You must update your AP software to version 3.5-r1 or higher in order to use Guest Access Portal in Managed Accounts.

Managed Account: All Accounts Delete Add Portal

<input type="checkbox"/>	Guest Portal Name	Description	Managed Account	Event Logging	Free Access	Paid Access	Voucher Access	
<input type="checkbox"/>	GAP_Test_NOV25		Base Infrastructure	Yes	Yes	No	Yes	
<input type="checkbox"/>	nbi_base_portal		Base Infrastructure	No	Yes	No	Yes	
<input type="checkbox"/>	nbi_ma_portal		ma_test_nbi_api_d579d	No	Yes	No	Yes	
<input type="checkbox"/>	1-GAP_Test		Base Infrastructure	Yes	No	No	No	
<input type="checkbox"/>	2-GAP_Test_1		Base Infrastructure	Yes	No	No	No	
<input type="checkbox"/>	3-GAP_Test		Base Infrastructure	Yes	No	No	No	
<input type="checkbox"/>	4-GAP_Test	45rtfg	Base Infrastructure	Yes	No	No	No	
<input type="checkbox"/>	5-GAP_Test		Base Infrastructure	Yes	No	No	No	
<input type="checkbox"/>	GAP_Test_6		Base Infrastructure	Yes	No	No	No	
<input type="checkbox"/>	GAP_Test_msp_1		1-MSP-25NoV	Yes	No	No	No	

Showing 1 - 10 Total: 10 10 < Previous 1 Next >

2. Click **Add Portal**. A maximum of four portals can be created per account.
3. Enter a name and brief description for the portal.

Add Guest Portal

Managed Account
Base Infrastructure

Name*

Description

☐ Client Login Event Logging

Save

Cancel

4. Click **Save**.

Basic Details

The **Basic** details page contains the **Managed Account** Type, **Name**, and **Description**.

Guest Access Portal > Raja-GA-Test

Basic Access Design Sessions Guests X

Managed Account

Base Infrastructure

Name*

Raja-GA-Test

Description

☒ Client Login Event Logging

Save



Note

A name once created for the Portal cannot be changed.

Access Portal

The Access Portal tab has four different access types:

- [Free](#)
- **Enterprise** ^X [access through one of the following options:](#)
 - Microsoft Azure
 - Sponsored Guest
 - Self Registration
 - Google
- **Paid** ^X
- [Vouchers](#)

The parameters under each access method can be configured only after the corresponding access method is enabled.



Note

Microsoft Azure and Google-based access are not supported on devices running release version 4.x.

Free Access Type Configuration

[Guest Access Portal](#) > Raja-GA-Test

Basic

Access

Design

Sessions

Guests X

Free

Enterprise X

Paid X

Vouchers

☒ Enable Free Access

☒ Enable Logout functionality for the guest client

☒ Bypass Captive Portal Detection

Client Session

Renewal Frequency

Hour(s) ▼

Valid range is 1-43800 hour(s)

Session Duration

Hour(s) ▼

Valid range is 1-43800 hour(s)

Client Rate Limit

Client Quota Limit

Social Login

SMS Authentication

Add Whitelist

Save

Free Access type contains configurable parameters such as:

- Session validity
- Renewable frequency
- Client rate limits
- Social login

You can select authentication using Google, Facebook, Twitter and Office 365, or all. You will need to enter the App ID of your social login App. If you enable Facebook login you will also need to enter your Facebook App secret.

Table 122 *Free Access Type Parameters*

Parameter	Description
Add Whitelist	Options for configuring the IP address or the domain name.
Client Rate Limit	Options for configuring downlink and uplink parameters in kbps to limit the data transfer rate to or from the client. If a client rate limit parameter is blank, no limits are applied.

Table 122 Free Access Type Parameters

Parameter	Description
Client Quota Limit	<p>The data quota limit feature has been added for RADIUS-based as well as controller-based guest portals. For controller-based, it is either directional or total data quota limit. Once the client logs in as a guest, the data quota limit is enforced and the values are sent to the AP to which the client is connected. The access point keeps track of the data limits and sends client statistics to the controller every 30 minutes. In case of multiple devices allowed for a given policy, the data quota limits enforcement has some limitations and works with the latency of 30 minutes during which the cumulative data quota limits of the devices can be exceeded beyond the configured data quota limits.</p> <p>The similar behavior is supported through RADIUS attributes for RADIUS-based onboard guest access clients.</p> <p>RADIUS_VENDOR_ID_CAMBIUM 9 (17713)</p> <p>RADIUS_VENDOR_ATTR_CAMBIUM_WIFI_QUOTA_UP (151)</p> <p>RADIUS_VENDOR_ATTR_CAMBIUM_WIFI_QUOTA_DOWN (152)</p> <p>RADIUS_VENDOR_ATTR_CAMBIUM_WIFI_QUOTA_UP_GIGWORDS (153)</p> <p>RADIUS_VENDOR_ATTR_CAMBIUM_WIFI_QUOTA_DOWN_GIGWORDS (154)</p> <p>RADIUS_VENDOR_ATTR_CAMBIUM_WIFI_QUOTA_TOTAL (155)</p> <p>RADIUS_VENDOR_ATTR_CAMBIUM_WIFI_QUOTA_TOTAL_GIGWORDS (156)</p> <p>The <code>gigwords</code> attributes are used for supporting data quota limits above 4 GB when required.</p>
Renewable Frequency	Once the session duration for the client expires, the client needs to wait for the period specified by renewal frequency before logging in again.
Session Duration	The duration for which the client is provided access.
SMS Authentication	SMS OTP supports Twilio, SMS Country, and SMS Gupshup SMS gateway providers. Any one of the gateway providers can be used to support the SMS OTP to be delivered to the cell phone of the end user. Once OTP is received the client can enter the OTP to get Internet access.
Social Login	<p>Consists of the following options:</p> <ul style="list-style-type: none"> • Domain URL: The redirected URL used by the client when trying to access the Internet. • Google: Consists of ID and Secret options to configure, which admin can create from https://console.cloud.google.com/. • Facebook: Consists of ID and Secret options to configure, which admin can create from https://developers.facebook.com/apps/. • Twitter: Consists of consumer key, consumer secret key, and callback URL. • Office 365: Consists of ID and Replyback URL.

**Note**

- Renewal frequency should be greater than session expiration.
- Client will get Social login options only when enabled in Access Control page in Portal.
- If Social login is enabled, it is mandatory in free access method for client to login through Google/Facebook/Twitter/Office 365.

Enterprise Wi-Fi Access **X** using Microsoft Azure Login, Sponsored Guest, Self Registration, or Google



Note

- Microsoft Azure and Google-based access are supported only on Enterprise Wi-Fi 6 APs running firmware version 6.5.1 and later.
- Microsoft Azure is supported on cnMaestro 4.1.0 and later versions.
- Google-based access is supported on cnMaestro 5.0.0 and later versions.

Microsoft Azure

Enterprise Microsoft Azure access page enables Microsoft Azure users to log in to access the Enterprise Wi-Fi. To set up users to authenticate from Microsoft Azure, navigate to **Network Services > Guest Access Portal > Access > Enterprise X > Microsoft Azure**, complete the following parameters and click **Save**:

Guest Access Portal > Raja-GA-Test

Basic **Access** Design Sessions Guests **X**

Free **Enterprise X** Paid **X** Vouchers

Microsoft Azure

☒ Enable Microsoft Azure Login

Microsoft Azure

Authorize

Admin Email

Azure Primary Domain

Allowed Domains*

Allowed Groups

students × teachers ×

Type and press Enter

Device Limit

5

Client Session

Session Duration*

10 Min(s) Valid range is 1-2628000 min(s)

Client Rate Limit

Downlink

Uplink

Kbps

Kbps

Client Quota Limit

Quota Type

None

Device Limit

5

Save

Sponsored Guest

In this type of access, guests must provide their own email address and their sponsor's email address to request Internet access.

To allow sponsored guests to access the Wi-Fi, navigate to **Network Services > Guest Access Portal > Access > Enterprise X > Sponsored Guest** complete the following parameters, and click **Save**:

Guest Access Portal > Raja-GA-Test

BasicAccessDesignSessionsGuests X

FreeEnterprise XPaid XVouchers

Microsoft Azure

Sponsored Guest

Self Registration

Google

☒ Enable Sponsored Guest

Sponsor Guest Settings

Guests must provide their own email and their sponsor's email to request Internet access.

Sponsor Email Domains*

cambiumnetworks.com

Client Session

Session Duration*

100

Min(s) ▼ Valid range is 1-2628000 min(s)

Client Rate Limit

Downlink

20000

Kbps

Uplink

20000

Kbps

Client Quota Limit

Quota Type

None

▼

Save

Self Registration

Self registration enables guests to register themselves when connecting to the Wi-Fi network for the first time. The Wi-Fi administrator can configure the self registration process to require a sponsor approval or not. The sponsor approval can also be configured to be manual or automatic confirmation.

To configure self registration, navigate to **Network Services > Guest Access Portal > Access > Enterprise X > Self Registration** and configure the following parameters.

The screenshot shows the 'Self Registration' configuration page in the Guest Access Portal. The left sidebar includes navigation options like Basic, Access, Design, Sessions, and Guests. The main content area is titled 'Self Registration' and contains several sections: 'Enable Self Registration' (checked), 'Sponsor Guest Settings' (with 'Manual Confirmation' selected), 'Sponsor Email List' (a text input field), 'Receive password via text' (unchecked), 'Client Session' (with a session duration input), 'Client Rate Limit' (with downlink and uplink inputs), 'Client Quota Limit' (with a quota type dropdown), and 'Device Limit' (with a device limit input). A 'Save' button is at the bottom.

Table 123 *Self Registration Parameters*

Parameter	Description
Enable Self Registration	Select the check box to enable self registration feature and configure the following parameters.
Sponsor Guest Settings <p>The guests must enter a sponsor email address when registering to connect to the wireless network. The administrator can choose to configure whether the sponsor must manually approve each request or the approval is automatic.</p>	
Require Sponsor	<p>Select the check box if you want the self registration to be approved by a sponsor.</p> <p>The guests must enter the sponsor email address when registering for access to the SSID.</p>
Sponsor Type	<p>Specifies whether the sponsor approval for guest internet access must be automatic or manual. The following options are available:</p> <ul style="list-style-type: none"> • Manual Confirmation—The sponsor receives an email for approving the guest's access request. After approval, the guest receives an email confirmation along with the password to connect to the wireless network. • Automatic Confirmation—If the guest provides a configured sponsor's email address, the password to access the network is automatically emailed to the guest and the sponsor is also notified via email.
Sponsor Email List	Configure the list of sponsor email addresses for approving access requests.

Table 123 *Self Registration Parameters*

Parameter	Description
Receive password via text By default, the guests receive the password to their email address. However, if you want the guests to receive the password to their mobile devices as well, configure the following parameters.	
Enable	Select the check box to send the password to the guest's mobile device.
SMS Gateway Provider	Select the SMS gateway to be used to send the OTP to the guest's mobile device. The following gateways are supported (each of the gateways have their own respective parameters that must be configured): <ul style="list-style-type: none"> • Fast SMS • Generic SMS API • SMS Country • SMS Gupshup • SMSAPI • Twilio • Victory Link SMS Each of the above gateways must be configured with their respective parameters.
Client-related parameters	
Client Session— Session Duration	Specifies the maximum duration (in minutes) that the guest can browse the internet in a single session. Supported range: 1-2628000 minutes
Client Rate Limit	Specifies the download and upload speed limit (in Kbps) for the guests. Configure the speed limit in the Downlink and Uplink fields.
Client Quota Limit	
Quota Type	Specifies the type of quota for configuring the data usage limit. The following options are supported: <ul style="list-style-type: none"> • None—No limit is configured for data usage. Guests can access unlimited data in the configured session duration. • Directional—Configure limits separately for downlink and uplink directions. The Downlink and Uplink fields are enabled. • Total—Configure the limit for both directions totally. The Total field is enabled.
Downlink	Specifies the downlink data usage limit (in either MB or GB, selected from the drop-down list). This field is available only when you select Directional in the Quota Type field.
Uplink	Specifies the uplink data usage limit (in either MB or GB, selected from

Table 123 Self Registration Parameters

Parameter	Description
	the drop-down list). This field is available only when you select Directional in the Quota Type field.
Total	Specifies total data usage limit for both the directions (in either MB or GB, selected from the drop-down list). This field is available only when you select Total in the Quota Type field.
Device Limit	Specifies the number of devices that the guest can connect to the wireless network. Default: 5.

Google-based access

Google-based access enables users with a Google account to connect to the wireless network by synchronizing the active directory. When enabled, if a guest who is part of the supported group tries to connect to the Wi-Fi network, the AP provides access to the guest.



Note

To configure Google-based access, you must have a Google Workspace account.

To configure Google-based access, navigate to **Network Services > Guest Access Portal > Access > Enterprise X > Google** and configure the following parameters.

The screenshot shows the 'Guest Access Portal' configuration page. The 'Access' tab is selected, and the 'Enterprise X' sub-tab is active. The 'Google' section is expanded, showing the following configuration options:

- Enable Google Login:** A checked checkbox.
- Google Login:**
 - Enable Directory Synchronization:** An unchecked checkbox.
 - Allowed Domains*:** A text input field with the placeholder 'Type and press Enter'.
- Device Limit:** A text input field with the value '5'.
- Client Session:**
 - Session Duration*:** A text input field with a 'Min(s)' dropdown menu and a note 'Valid range is 1-2628000 min(s)'.
- Client Rate Limit:**
 - Downlink:** A text input field with a 'Kbps' unit label.
 - Uplink:** A text input field with a 'Kbps' unit label.
- Client Quota Limit:**
 - Quota Type:** A dropdown menu with 'None' selected.

A 'Save' button is located at the bottom of the configuration section.

Table 124 Google Parameters

Parameter	Description
Enable Google Login	Select the check box to enable Google-based Wi-Fi access and configure the following parameters.
Device Limit	Specifies the number of devices that the guest can connect to the wireless network.

Table 124 *Google Parameters*

Parameter	Description
	Default: 5.
Google Login	
Enable Directory Synchronization	Select the check box to enable synchronization of Google Apps Domain Directory. This functions requires authorization. Click Follow these steps for information on configuring your Google Apps Domain Directory.
Allowed Domains	List of domains to be allowed for Google-based access. Enter the domain name in the text box.
Client-related parameters	
Client Session—Session Duration	Specifies the maximum duration (in minutes) that the guest can access internet in a single session. Supported range: 1-2628000 minutes
Client Rate Limit	Specifies the download and upload speed limit (in Kbps) for the guests. Configure the speed limit in the Downlink and Uplink fields.
Client Quota Limit	
Quota Type	Specifies the type of quota for configuring the data usage limit. The following options are supported: <ul style="list-style-type: none"> • None—No limit is configured for data usage. Guests can access unlimited data in the configured session duration. • Directional—Configure limits separately for downlink and uplink directions. The Downlink and Uplink fields are enabled. • Total—Configure the limit for both directions totally. The Total field is enabled.
Downlink	Specifies the downlink data usage limit (in either MB or GB, selected from the drop-down list). This field is available only when you select Directional in the Quota Type field.
Uplink	Specifies the uplink data usage limit (in either MB or GB, selected from the drop-down list). This field is available only when you select Directional in the Quota Type field.
Total	Specifies total data usage limit for both the directions (in either MB or GB, selected from the drop-down list). This field is available only when you select Total in the Quota Type field.

Designing the Guest Access Login Page and Email Templates

To design the guest login page for users to see when requesting access, navigate to **Network Services > Guest Access Portal > Design > Login Page**, complete the following parameters, and click **Save**:

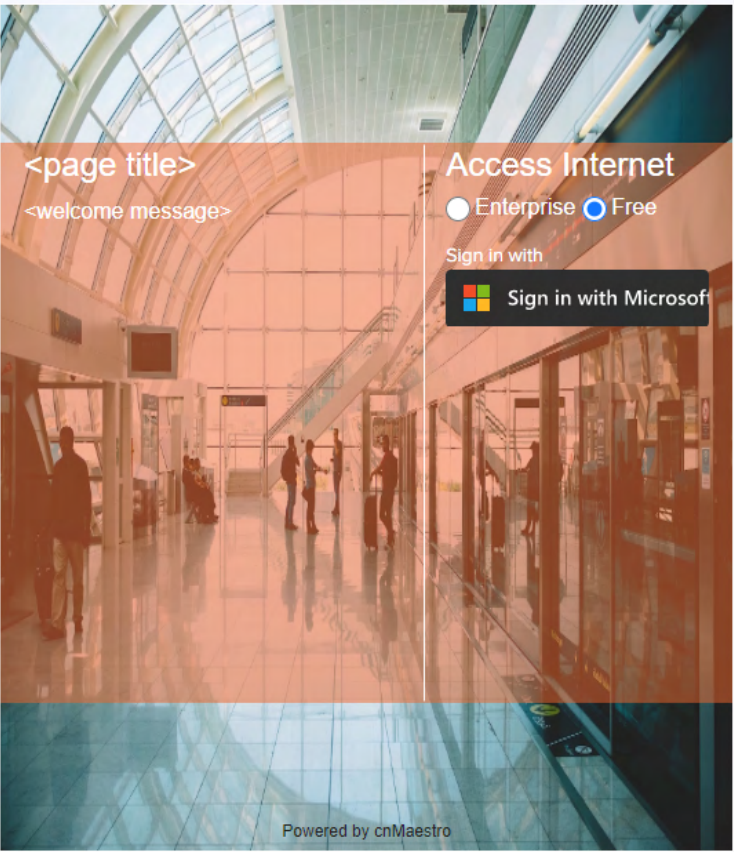
Guest Access Portal > AZURE_TEST_MARCH_1

Basic Access **Design** Sessions

Login Page Email Template

Preview

Airport Beach Coffee Hotel WIFI4EU



<page title>
<welcome message>

Access Internet

● Enterprise ● Free

Sign in with

Sign in with Microsoft

Powered by cnMaestro

Logo

Logo ⓘ

Browse

Logo Background

Background

Background

Background Image ⓘ

Browse

☐ Hide Background Image

☐ Repeat Background

Background Placement

Left Top ▾

Content Area

Text Design

Content

Advanced

Custom Fields

WIFI4EU Beta

Save

To design the email template that should be used to send approval request to the sponsor (in Sponsored Guest and Self Registration access types), navigate to **Network Services > Guest Access Portal > Design > Email Template > Sponsor**, complete the following parameters, and click **Save**:


Guest Access Portal > AZURE_TEST_MARCH_1

Basic Access **Design** Sessions

Login Page **Email Template**

Preview

Sponsor Guest



Internet Access Request


Hello,

[Guest_Name] is requesting access to internet. To approve, click the button below.

Network Name: [GUEST_SSID]
Duration: [hh:mm]

[Approve Internet Access](#)

If you think this request is suspicious, do not approve and report it to your IT admin.



Powered by Cambium Networks

Logo

Logo

[Select File](#)

Recommended size 300x X 50px. Maximum size of 3MB.JPEG, JPG,PNG or GIF

Content

Company Name*

Guest user email body *

[Save](#)

To design the email template that should be used to send approved access details to the guest, navigate to **Network Services > Guest Access Portal > Design > Email Template > Guest**, complete the following parameters, and click **Save**:

Guest Access Portal > AZURE_TEST_MARCH_1


Basic Access **Design** Sessions

Login Page **Email Template**

Preview

Sponsor

Guest



Approved Internet Access


Hello [Guest_Name],

We offer you free internet access. Enjoy free fast internet.

[Sponsor_Email_ID] approved your internet access.

Network Name: [GUEST_SSID]

Duration: [hh:mm]



Powered by Cambium Networks

Logo

Select File

Recommended size 300x X 50px. Maximum size of 3MB.JPEG, JPG,PNG or GIF

Content

Company Name*

Cambium Networks

Guest user email body *

We offer you free internet access. Enjoy free fast internet.

Save

Paid Access^x

Paypal has been added as a payment gateway service where end users can purchase Internet connectivity using a credit card or their existing PayPal accounts. For purchasing Internet plans, clients are directed to PayPal portal where they purchase the plan and then they are automatically redirected to guest access portal where the purchased voucher is displayed. The user should ensure to save this Voucher information if s/he plans to use it on multiple devices.

Guest Access Portal > HarshitGP

Basic **Access** Splash Sessions

Free **Paidx** Vouchers

☒ Enable Paid Access

Paypal Payment Gateway

IPpay Gateway ^{Beta}

QuickPay Gateway ^{Beta}

Orange Money ^{Beta}

mPesa Gateway ^{Beta}

Plan Details

Name	Price	Duration	Uplink	Downlink	Client Quota	Device Limit
No Data Available						

Save

Note: Splash page needs to be saved to reflect any changes in access portal settings.

Table 125 *Paid Access Type Parameters*

Parameter	Description
General	Plan Name: The name of the plan.
	Session Duration: The duration for which the client is allowed to access the network.
	Client Rate Limit: The uplink and the downlink values in kbps to limit the data transfer rate to or from the client. If a client rate limit parameter is blank, no limits are applied.
	Device Limit: The device limit allow that number of devices to be connected or select the unlimited to connect any number of devices.

Add New Field

Plan Name

Plan Cost

USD

Session Duration

Min(s)

Downlink Rate Limit

Kbps

Uplink Rate Limit

Kbps

Quota Type
None

Device Limit
☐ Unlimited
☒ 1

Save

Voucher Access Type Configuration

Important Points to Remember

- Vouchers can only be generated after enabling Vouchers and creating at least one Voucher plan.
- A maximum of 50,000 Vouchers per portal can be created on cnMaestro.



Note

User is allowed to add only 1000 vouchers at a time. In order to create 50,000 vouchers user needs to add 50 times.

- A maximum of 1,000 Vouchers per portal can be created on cnMaestro Cloud (<https://cloud.cambiumnetworks.com/>).
- Total number of generated Vouchers = Vouchers Unclaimed + Vouchers Claimed + Vouchers Expired.
- The admin can export all/valid/current page Voucher codes as PDF/CSV document.

Voucher contains options to add new plans and Vouchers. Based on user requirements, the plans can be created with different validity and rate limits.

1. Create a plan

- Navigate to **Network Services > Access Control Portal** page and select **Access Control** tab.
- Enable **Vouchers**.
- Click **Add New Plan** button. The window with general and design parameters for the plan is displayed.

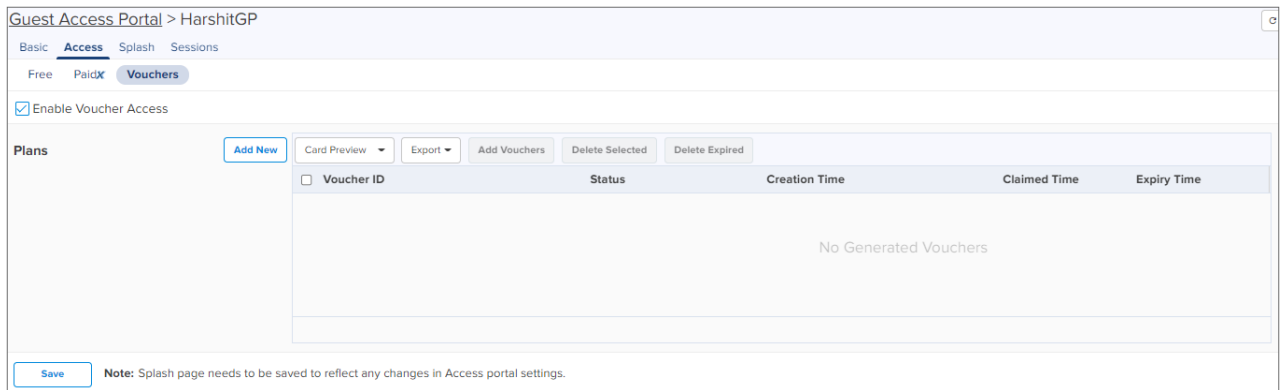


Table 126 *Voucher Access Type Parameters*

Parameter	Description
Design	<ul style="list-style-type: none"> • Color: There are options to modify colors for the title, message, code, and background. • Background Image: You can browse and select a background image for this page. • Title: The title of the voucher plan. • Message: Detailed information about the plan. • Access Code Message: 8 digit access code will be provided to use the voucher. <p>With all the above parameters, administrators can create their own design for the card with text, color, and message to be displayed on card.</p>
General	<ul style="list-style-type: none"> • Name: The name of the plan. • Session Duration: The duration for which the client is allowed network access. • Voucher Expiry: The expiry time for the generated Vouchers. Once this time lapses, the Vouchers cannot be used. • Client Rate Limit: The uplink and the downlink values in kbps to limit the data transfer rate to or from the client. If a client rate limit parameter is blank, no limits are applied. • Voucher Device Limit: Limit the devices to use the voucher.

Add New plan

☒ Plan Details

Name

Session Duration Valid range is 1-3600000 mins

Voucher Expiry Valid range is 1-3600000 mins

Download Rate Limit Kbps

Upload Rate Limit Kbps

Quota Type

Voucher Device Limit

☐ Bind Voucher to Device

☒ Vouchers Design

Background image

Title

Message

Access Code Message

Internet Access Voucher
Enjoy complimentary Internet services for 1 hr
Here is your access code
XXXXXXXX

2. Once a plan is configured, Vouchers can be generated for it. Each Voucher is a unique, randomized alphanumeric code.

Figure 489 Select a plan

☒ Enable Voucher Access

Plans

Test-Vchr

Figure 490 Add Vouchers

Add more cards

Quantity

3. Once the plan is created and the Vouchers are generated, the following page is displayed.

Guest Access Portal > GAP-Test-NOV25

Basic **Access** Splash Sessions

Free Paid **Vouchers**

☒ Enable Voucher Access

Plans

<input type="checkbox"/>	Voucher ID	Status	Creation Time	Claimed Time	Expiry Time	<input type="button" value="Delete"/>
<input type="checkbox"/>		unclaimed	Wed Nov 25 2020 14:16:55 UTC +0530	-	Fri Mar 05 2021 14:16:55 UTC +0530	<input type="button" value="Delete"/>
<input type="checkbox"/>		unclaimed	Wed Nov 25 2020 14:16:55 UTC +0530	-	Fri Mar 05 2021 14:16:55 UTC +0530	<input type="button" value="Delete"/>
<input type="checkbox"/>		unclaimed	Wed Nov 25 2020 14:16:55 UTC +0530	-	Fri Mar 05 2021 14:16:55 UTC +0530	<input type="button" value="Delete"/>
<input type="checkbox"/>		unclaimed	Wed Nov 25 2020 14:16:55 UTC +0530	-	Fri Mar 05 2021 14:16:55 UTC +0530	<input type="button" value="Delete"/>
<input type="checkbox"/>		unclaimed	Wed Nov 25 2020 14:16:55 UTC +0530	-	Fri Mar 05 2021 14:16:55 UTC +0530	<input type="button" value="Delete"/>

Showing 1-5 Total 5

Note: Splash page needs to be saved to reflect any changes in Access portal settings.

Figure 491 Sample Voucher Code



Note

The modified values in the Access Portal page is reflected on the design page only when the design page is saved after making the changes.

Design Page

The Design page refers to the page to which a wireless client is redirected when it connects to the guest portal. Administrators can create their own Design page by modifying the default logo, background, and text to be displayed in the Design page with different colors and fonts.

- If **Free** is selected in **Access Portal**, the client only sees free access related parameters.
- If **Voucher** is selected in **Access Portal**, the client only sees Voucher related parameters with a text box to enter the **Voucher code**.
- If both **Free** and **Voucher** are selected, then the client sees both Free and Voucher related parameters.

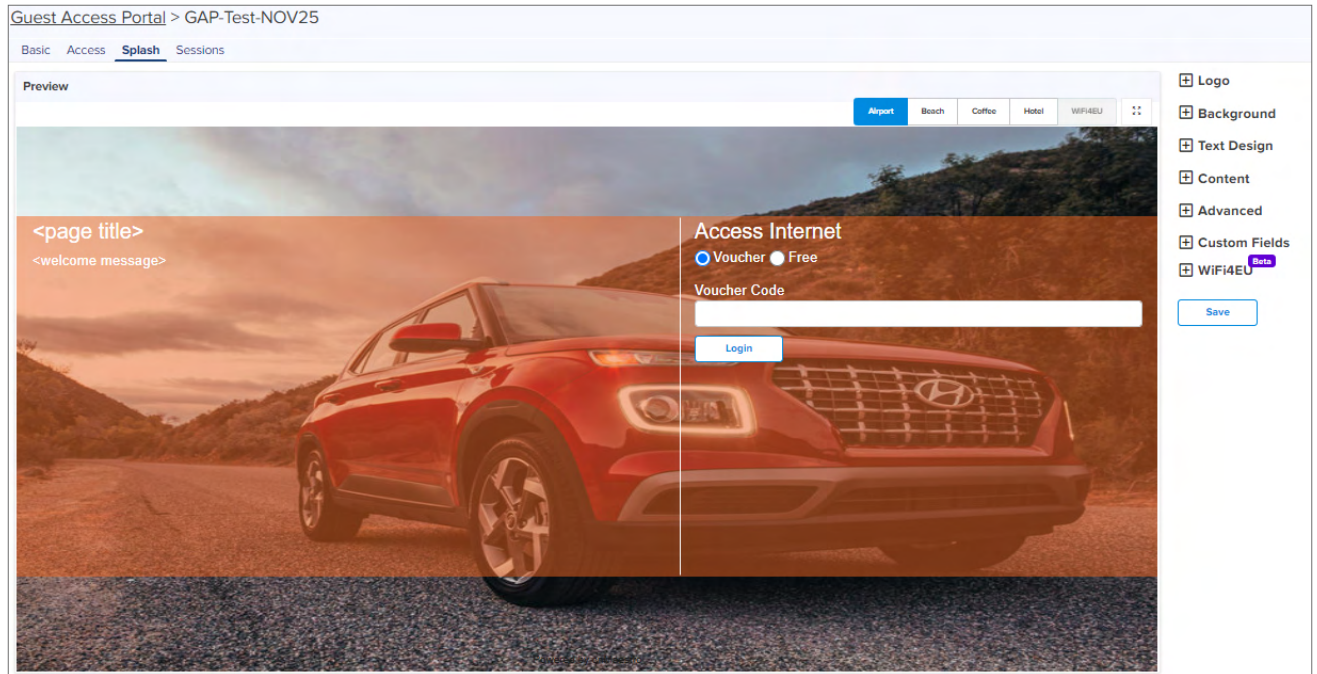


Table 127 Design Page Parameters

Parameter	Description
Accept Terms Message	Text to appear as the accept terms message.
Advanced	Expand Advanced option. Browse and select the advanced fields.
Background	Browse and select the image that needs to be displayed as the background. <ul style="list-style-type: none"> • Recommended image resolution—1024 pixels × 800 pixels

Table 127 *Design Page Parameters*

Parameter	Description
	<ul style="list-style-type: none"> Maximum supported image file size—5 MB Supported file formats—JPEG, JPG, PNG, and GIF
Background Placement	Choose the option from the drop-down for placing the background image in the Design page.
Custom Fields	Expand Custom Field option. The user can customize the fields in the Design page by choosing the Custom Field option in the Guest Access Portal page and clicking Add New button.
Enter Voucher Code Message	Enter the text to appear in Voucher Code Message .
Free Label	Enter the text that should appear on the Free Label .
Login Button	Enter the text that should appear on the window to submit.
Login Failure Message	Message to appear when any error occurs during login.
Login Success Message	Message to appear after successful login.
Login Title	Title of the login section.
Logo	Browse and select the logo that needs to be displayed on the Design page. <ul style="list-style-type: none"> Recommended image resolution—300 pixels × 50 pixels Maximum supported image file size—3 MB Supported file formats—JPEG, JPG, PNG, and GIF
Message	Text to appear as the welcome text. You can choose the font style and size for the welcome text.
On Success Redirect to URL	Enter the URL to be redirected to a page, such as Google, Twitter, and Facebook.
Opacity	The transparency of background image.
Page Title	Text to appear as the title of the page. You can choose the font style and size for the title.
Please wait Message	Text to appear in the waiting screen.
Repeat Background	Enable the check box if you want the background image to be repeated.
Select Plans Label	Enter the text to appear in the label to select plan.
Server Error Message	Text to appear if there is an error while contacting server.
Terms and Conditions Title	Text to appear as the title for the terms and the conditions.
Terms and Conditions	Text to appear as the terms and conditions.
Terms Agree	Text to appear in the terms agree button.

Table 127 Design Page Parameters

Parameter	Description
Button	
Terms Cancel Button	Text to appear in the terms cancel button.
Text Design	Choose the appropriate colors for the background, logo in the background, content area, and for the text.
Voucher Code	Enter the text to appear in Voucher Code, Voucher Label, Enter Voucher Code Message, and Voucher Code Error Message.
Voucher Code Error Message	Enter the text to appear in Voucher Code Error Message.
Voucher Label	Enter the text to appear in Voucher Label.
Failure	Enter the text to appear in Google Authentication Failure Message, Twitter Authentication Failure Message, and Facebook Authentication Failure Message.
WiFi4EU	WiFi4EU provides free, high-quality Internet access only across the European Union.

WiFi4EU

WiFi4EU provides free, high-quality Internet access across the European Union. Administrators can enable the WiFi4EU checkbox to provide access to the free internet.

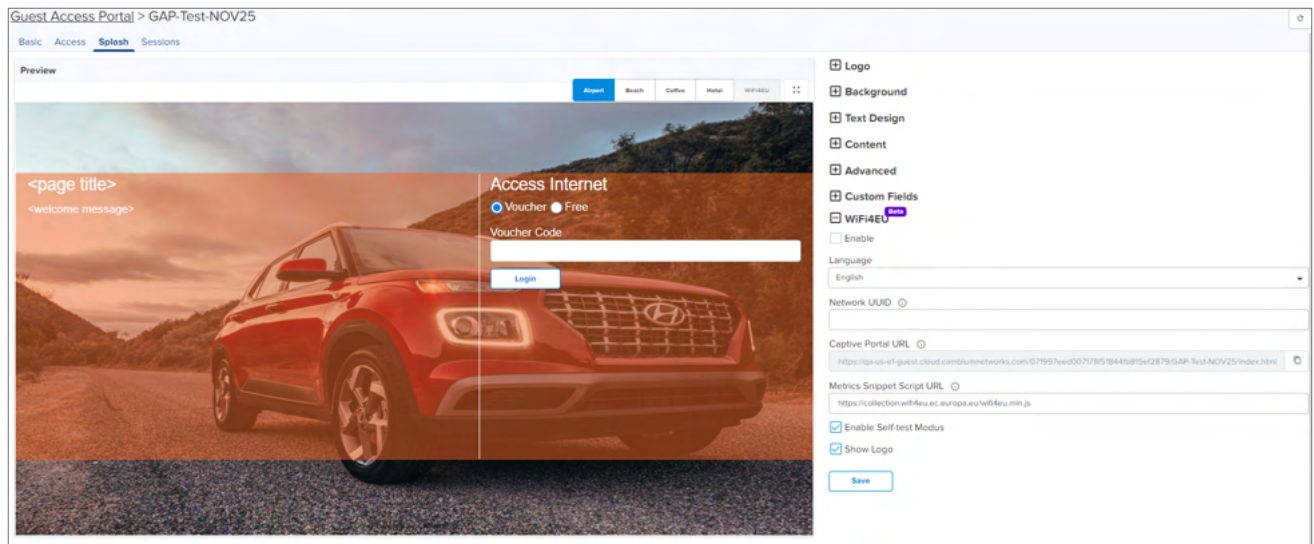


Table 128 WiFi4EU Parameters

Parameter	Description
General	<ul style="list-style-type: none"> • Network UUID: Universally Unique Identifier (UUID) that the EC attribute is generated when the network installation is created in the Installation. • Language: Allows to select the preferred language. • Enable Self Test Mode: Allows the browsers background script verification. • Show Logo: Displays the WiFi4EU logo provided by the European union.

Sessions

Sessions tab contains Client MAC address, Access Point MAC address, Access Type as Free (Google or Facebook) or Voucher, WLAN-SSID of client connected AP, Remaining time and Disconnect option.

Administrator can check how many clients are connected, Access Type (Free/Voucher) of the client, and can disconnect the clients.

Guest Access Portal > Raja-GA-Test

Basic Access Design Sessions Guests X

Sessions and Login Events Paid Transactions Users X

Client Session

Disconnect Selected

Client MAC Access Type SSID Access Point Remaining Time Voucher Code Disconnect

No Data Available

Showing 0 - 0 Total: 0 10 < Previous Next >

Client Login Events

Export

Client MAC	Portal	Access Type	SSID	Access Point	Voucher Code	Login Time	Email	Mobile Number
	-GA-Test	Payment-Gateway	5.0.0-GA-Open			16 Nov 2023, 12:32 PM		
	-GA-Test	Google	5.0.0-GA-Open			16 Nov 2023, 12:15 PM		
	-GA-Test	Self-Registration	5.0.0-GA-Open			16 Nov 2023, 12:13 PM		
	-GA-Test	Voucher	5.0.0-GA-Open			16 Nov 2023, 12:07 PM		
	-GA-Test	Ent-Self-Register	5.0.0-GA-Open			16 Nov 2023, 11:21 AM		
	-GA-Test	GoogleDomainDirectory	5.0.0-GA-Open			16 Nov 2023, 10:51 AM		
	-GA-Test	GoogleDomainDirectory	5.0.0-GA-Open			15 Nov 2023, 07:34 PM		
	-GA-Test	GoogleDomainDirectory	5.0.0-GA-Open			15 Nov 2023, 04:29 PM		
	-GA-Test	Ent-Self-Register	5.0.0-GA-Open			13 Nov 2023, 06:32 PM		
	-GA-Test	Ent-Self-Register	5.0.0-GA-Open			13 Nov 2023, 06:30 PM		

Showing 1 - 10 Total: 17 10 < Previous 1 2 Next >

Client Login Events table creates events of client login sessions. It maintains the login events for 7 days. This table has Client MAC address, Portal Name, SSID, Access point MAC, Voucher code (if client connected with Voucher), Access type (Google/Facebook/Voucher).

Admin can export the client login events as PDF / CSV.

Table 129 Sessions Parameters

Parameter	Description
Access Point	MAC address of the Access Point.
Access Type	Access type as Free or Voucher.
Client MAC	MAC address of the client.
Disconnect	Displays if the client is disconnected from the network.
Remaining Time	The time left for the client to access the Internet. It depends upon the session duration configured in the Access Portal.
Voucher	Displays the valid applied voucher.
WLAN	SSID of the network.



Note

For **Free** access method, the client MAC address is displayed even after the free session duration expires. Delete the MAC address of the client after the Renewable Frequency completes.

Users table displays details of users accessing the network using Enterprise Google-based access.

Guest Access Portal > Raja-GA-Test

Basic Access Design Sessions **Guests X**

Sessions and Login Events Paid Transactions **Users X**

☐ Email Group Registered Devices

No Data Available

Showing 0 - 0 Total: 0 10 < Previous Next >

Table 130 *Users Table Parameters*

Parameter	Description
Email	Email address of the registered user.
Group	Name of the group to which the user belongs.
Registered Devices	MAC address of the registered devices.

Guests X

The Guests page allows you to view details of self registered guests connecting to the wireless network. However, to view this page, you must first enable and configure self registration under **Network Services > Guest Access Portal > Access Type > Enterprise X > Self Registration**.

You can also add new guest details on this page. These users can directly access the wireless network after entering the required details in the access portal.

To add a new user, complete the following steps:

1. Click **Add New** on the **Guests** page.

The **Add New User** window is displayed.

Add New User X

Name*

Email*

Notes

Add Cancel

2. Configure the name and email address of the guest in the **Name** and **Email** fields.
Add a description, if required, in the **Notes** field.
3. Click **Add**.

The details of the Enterprise self registered guests that are connected to the Wi-Fi network are displayed in

the table

The screenshot shows a web interface for a Guest Access Portal. At the top, there's a breadcrumb trail: 'Guest Access Portal > Raja-GA-Test'. Below this, there are tabs for 'Basic', 'Access', 'Design', 'Sessions', and 'Guests X'. The 'Guests X' tab is selected. On the left, there's a sidebar with various icons. The main area contains a table with the following columns: Name, Email, Mobile Number, Status, Device Count, Notes, Activation, and Expiration. There are 'Add New' and 'Delete' buttons at the top right of the table. The table is currently empty, and a message 'No Data Available' is displayed in the center. At the bottom right, there's a pagination control showing 'Showing 0 - 0 Total 0 100' and 'Previous Next' links.

Table 131 *Guests Table Details*

Parameter	Description
Name	Name of the guest that was entered at registration.
Email	Email address of the guest.
Status	Displays the whether the guest is connected or offline.
Device Count	Displays the number of devices that the guest has connected to the network.
Notes	Displays the comments or description provided when adding the guest.
Activation	Displays the date and time when the guest first connected to the network.
Expiration	Displays the date and time when the guest disconnected from the network. For currently connected guests, this field displays the date and time of session expiration.

Mapping the device to Guest Access Portal in cnMaestro

The administrator needs to configure the name of the Guest Access Portal in the device which redirects the device to cnMaestro for client connectivity.



Note

The client gets the fully configured **Design** page for login only if the Access Point is onboarded to the server.

Configuration at device level

To configure the Guest Access at device level, perform the following:

1. Login to the device.
2. Navigate to **Configuration > WLAN > Guest Access**.

WLANs > Radio_Off

Configuration APs

WLAN

AAA Servers

Guest Access

Access Control

Passpoint

ePSK

Basic Settings

☐ Enable

Portal Mode
☒ Internal Access Point ☐ External Hotspot ☐ cnMaestro

Access Policy
☒ Clickthrough Splash page where users accept terms and conditions to get on the network
☐ RADIUS Splash page with username and password, authenticated with a RADIUS server
☐ LDAP Redirect users to a login page for authentication by a LDAP server
☐ Local Guest Account Redirect users to a login page for authentication by local guest user account

AP Server Protocol
☒ HTTP Use unsecured HTTP protocol for AP guest access server
☐ HTTPS Use secured HTTPS protocol for AP guest access server

Redirect Hostname
 Redirect Hostname for the splash page (up to 255 characters)

Title
 Title text in splash page (up to 255 characters)

Contents
 Main contents of the splash page (up to 255 characters)

Terms
 Terms and conditions displayed in the splash page (up to 255 characters)

Logo
 Logo to be displayed on the splash page
 Eg: http://domain.com/logo.png

Background Image
 Background image to be displayed on the splash page
 Eg: http://domain.com/backgroundimage.jpg

Success Action
☒ Internal Logout Page
☐ Redirect User to External URL
☐ Redirect User to Original URL

Success Message

☒ Advanced Settings

☒ Whitelist

☒ Captive Portal bypass User Agent

Save

3. Enable the **Guest Access** check box.
4. Choose the **Portal Mode** radio as **cnMaestro**.
5. In the **Guest Portal Name** text box, select the name of the portal that was created in cnMaestro and enter the respective parameters.

Configuration at cnMaestro side

The administrator can push the configuration from cnMaestro through policy or advanced configuration.

Policies

WLAN Management

GUESTCLOUD

Info

WLAN

RADIUS Servers

Guest Access

Usage Limits

Scheduled Access

Access

Passpoint

Enable: ☒

Portal Mode: ☐ Internal Access Point ☐ External Hotspot ☒ cnMaestro

Guest Portal Name: QA

Session Timeout: 28800 Session time in seconds (60 to 86400)

Inactivity Timeout: 1800 Inactivity time in seconds (60 to 28800)

Add White List

IP Address or Domain Name: Add

IP Address or Domain Name:

Advanced Configurations (optional)

Template settings entered below will be merged into or appended to the profile created. This allows making configuration setting not supported or prevented by previous screens.

Settings entered below are not validated or error checked, and may overwrite settings made in previous screen. You are solely responsible for ensuring that the resulting profile is valid and safe to use.

```
!
wireless wlan 1
  guest-access
  guest-access portal-mode cnMaestro GAP1
!
```

Access Types

The following table describes the parameters described in configuring SMS authentication parameters:

Parameter	Description	SMS Gateway Provider				
		Fast SMS	SMS Country	SMS Gupshup	Twilio	Victory Link SMS
Enable	It indicates to enable the SMS Authentication feature.	✓	✓	✓	✓	✓
Username	Indicates the username of the vendor.	✓	✓	✓	X	✓
Sender ID	It is the name or number which flashes on the recipients mobile phone when they receive SMS. This is Optional not mandatory.	✓	✓	✓	X	✓
API Key	It's a token which is provided by vendors.	✓	X	X	X	X
Account Type	It shows type of accounts such as International, OTP, Promotional and Transaction.	✓	X	X	X	X
OTP Template	The template with which SMS has to be sent.	✓	✓	✓	✓	✓
Password	It indicates the password.	X	✓	✓	X	✓
Country Code	It enables to select country code based on deployments.	X	✓	✓	X	X
Auth Token	It acts as a password.	X	X	X	✓	X
Account SID	It acts as a username.	X	X	X	✓	X
From	It enables to select the country code.	X	X	X	✓	X
Language	It indicates the Language.	X	X	X	X	✓

SMS Authentication

☒ Enable

SMS Gateway Provider

Twilio

Auth Token

Account SID

From

US (+1)

OTP Template

Your OTP is %code%

The OTP template should include %code% as displayed in the sample text. Template may need to be approved, it's advised to contact respective SMS Gateway Provider. %code% will be replaced by the OTP code in the SMS.

Add Whitelist

Save

To configure SMS Authentication on cnMaestro, perform the following:

1. Enable SMS Authentication feature.
2. In SMS Gateway provider, select your required gateway from the drop-down.
3. Enter the **User Name**.
4. Enter the **Sender ID**. This field is optional. This allows user to send SMS through the ID which he chooses.
5. Enter **API Key**.
6. Select your **Account Type** from the drop-down.

7. Enter the **OTP Template**. The OTP template should include “%code%. %code% replaces the OTP code in the SMS.

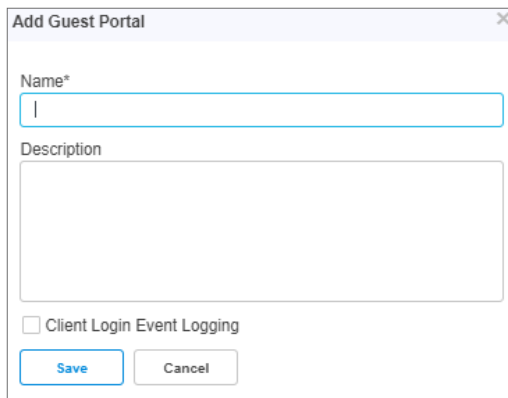
Guest Access using Social Login

Configuration

To achieve cnMaestro Guest Access using Social Logins like Google, Twitter, Facebook, and Office 365, perform the following steps:

To create Guest Access profile on cnMaestro, do the following:

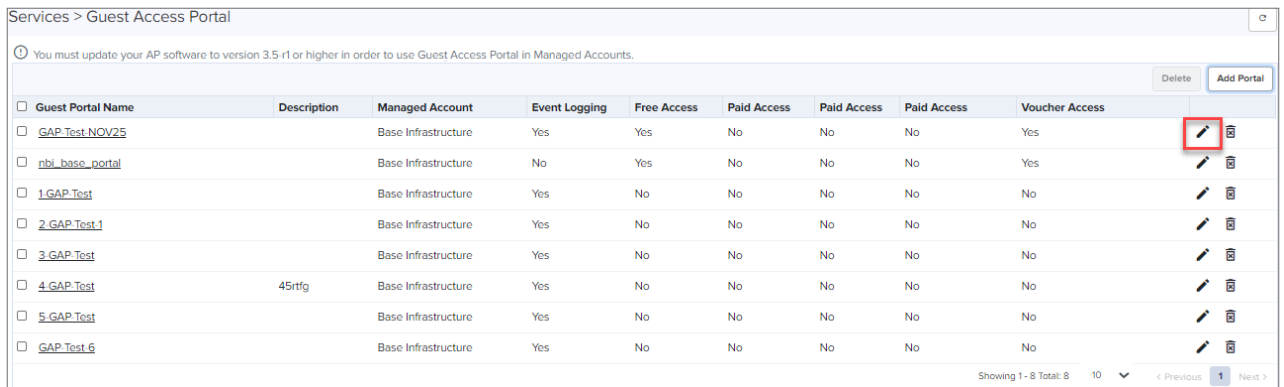
1. Login to cnMaestro and navigate to **Network Services > Guest Access Portal > Add Portal**.
2. Enter Portal Name, Description, enable logging for client login events.
3. Click **Save**.











The 'Add Guest Portal' dialog box contains the following fields and controls:

- Name***: A text input field with a single character 'I' entered.
- Description**: A larger text area, currently empty.
- ☐ **Client Login Event Logging**: An unchecked checkbox.
- Buttons**: 'Save' and 'Cancel' buttons at the bottom.

4. Click **Edit Guest Portal Details**.



The table displays a list of Guest Access Portals. The first row is highlighted, and the edit icon (pencil) is circled in red.

<input type="checkbox"/>	Guest Portal Name	Description	Managed Account	Event Logging	Free Access	Paid Access	Paid Access	Paid Access	Voucher Access	
<input type="checkbox"/>	GAP_Test_NOV25		Base Infrastructure	Yes	Yes	No	No	No	Yes	
<input type="checkbox"/>	nbi_base_portal		Base Infrastructure	No	Yes	No	No	No	Yes	
<input type="checkbox"/>	1_GAP_Test		Base Infrastructure	Yes	No	No	No	No	No	
<input type="checkbox"/>	2_GAP_Test_1		Base Infrastructure	Yes	No	No	No	No	No	
<input type="checkbox"/>	3_GAP_Test		Base Infrastructure	Yes	No	No	No	No	No	
<input type="checkbox"/>	4_GAP_Test	45rtfg	Base Infrastructure	Yes	No	No	No	No	No	
<input type="checkbox"/>	5_GAP_Test		Base Infrastructure	Yes	No	No	No	No	No	
<input type="checkbox"/>	GAP_Test_6		Base Infrastructure	Yes	No	No	No	No	No	

Showing 1 - 8 Total: 8 10 < Previous 1 Next >

5. Navigate to **Access** tab and expand **Social Login**.

Guest Access Portal > HarshitGP

Basic **Access** Splash Sessions

Free PaidX Vouchers

☒ Enable Free Access

☐ Enable Logout functionality for the guest client

☐ Bypass Captive Portal Detection

Client Session

Renewal Frequency
10 Min(s) Valid range is 1-2628000 min(s)

Session Duration
10 Min(s) Valid range is 1-2628000 min(s)

Client Rate Limit

Client Quota Limit

Social Login

SMS Authentication

Add Whitelist

Save

6. Select Google, Twitter, Facebook, Office 365 based on your requirement.

Guest Access Portal > HarshitGP

Basic **Access** Splash Sessions

Free PaidX Vouchers

☒ Enable Free Access

☐ Enable Logout functionality for the guest client

☐ Bypass Captive Portal Detection

Client Session

Renewal Frequency
10 Min(s) Valid range is 1-2628000 min(s)

Session Duration
10 Min(s) Valid range is 1-2628000 min(s)

Client Rate Limit

Client Quota Limit

Social Login

Guest Portal Hostname / IP
gp-us-e1-guest.cloud.cambiumnetworks.com ⓘ Configure this URL in the Social login application settings.

Note: Captive portal bypass will be enabled if social login with Facebook or Google is enabled. This is required as the Captive-portal Network Assistant (Guest portal signon popup on mobile devices) is not compatible with the social login API provided by these services.

☒ Google

Id
[Text Field]

☒ Twitter

Consumer API Key
[Text Field]

Consumer API Secret Key
[Text Field]

Callback URL
https://gp-us-e1-guest.cloud.cambiumnetworks.com/cn-ctrl/guest/5f1cc5274ef7432a9a76f3edbf1d6a0a/HarshitGP/twiterCallback

☒ Facebook

Id
[Text Field]

Secret
[Text Field] Show

Reply URL
https://gp-us-e1-guest.cloud.cambiumnetworks.com/cn-ctrl/guest/5f1cc5274ef7432a9a76f3edbf1d6a0a/HarshitGP/facebook ⓘ

☒ Office 365

Reply URL
https://gp-us-e1-guest.cloud.cambiumnetworks.com/assets/Views/office.html ⓘ Configure this URL as Reply URL under Office365 application settings

Id
[Text Field]

SMS Authentication

Add Whitelist

Save

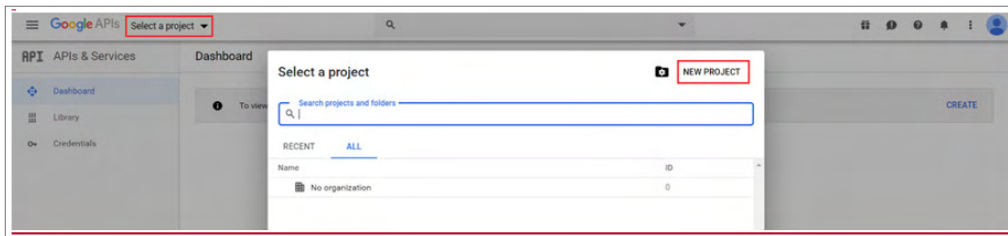
API Key Generation

Perform the following steps to create APIs for cnMaestro to integrate with Google, Twitter, Facebook, and Office 365:

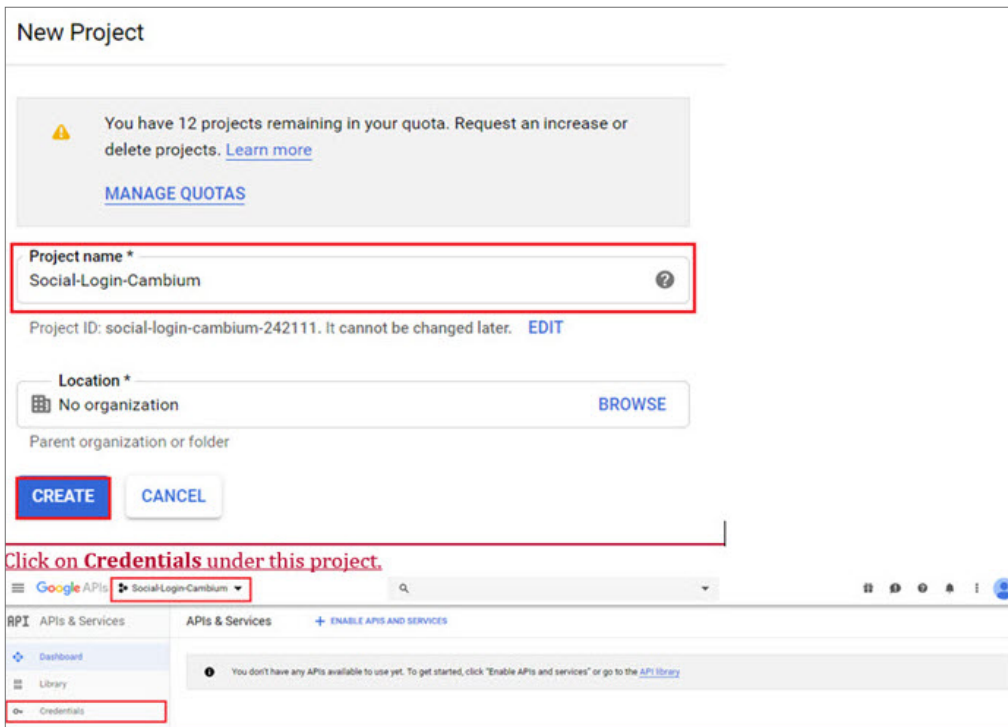
- [Google](#)
- [Twitter](#)
- [Facebook](#)
- [Office 365](#)

Google

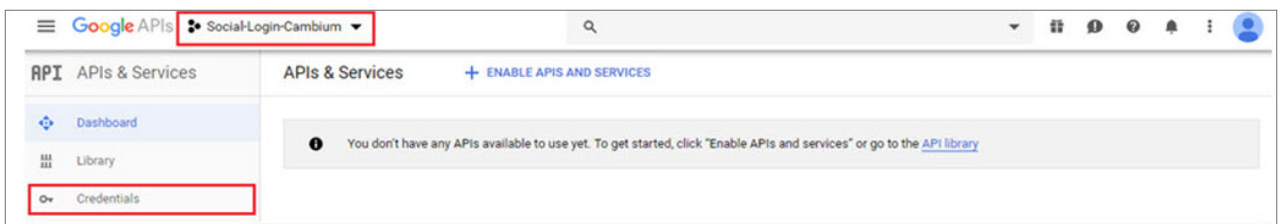
1. Login to Google Account and navigate to <https://console.cloud.google.com/>.
2. Click **Select a Project** and create a **New Project**.



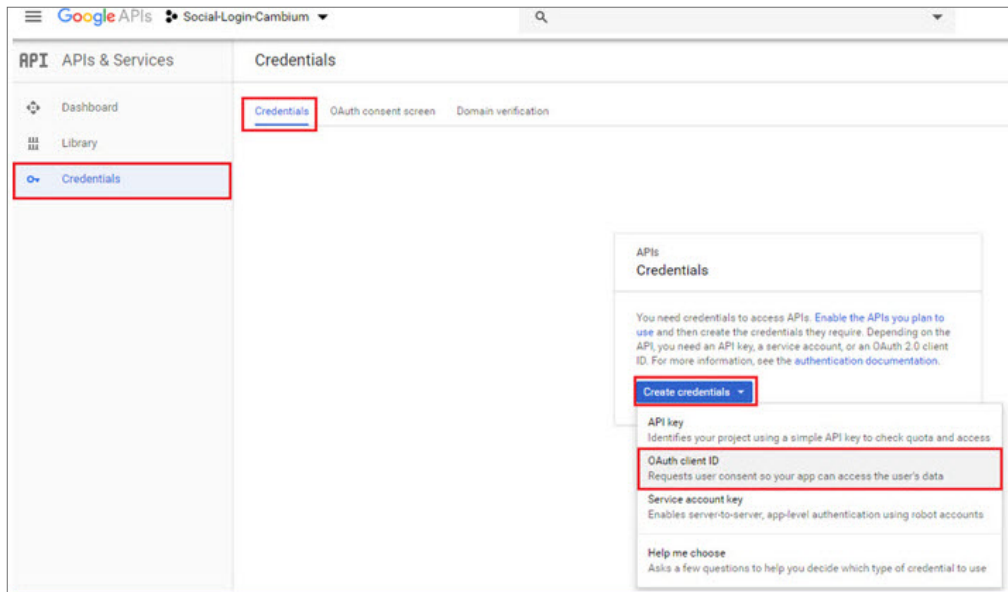
3. Give a name to the Project and click **CREATE**..



4. Click **Credentials** under this project.



5. Under **Credentials** tab, create OAuth Client ID.



6. Click **Configure Consent Screen**



7. Assign a name to the application, map to an email address, add cambiumbnetworks.com to the authorized domain and click **Save**.

Google APIs Social-Login-Cambium

APIs & Services

Credentials

OAuth consent screen

Before your users authenticate, this consent screen will allow them to choose whether they want to grant access to their private data, as well as give them a link to your terms of service and privacy policy. This page configures the consent screen for all applications in this project.

Verification status
Not published

Application name ⓘ
The name of the app asking for consent
Social-Login

Application logo ⓘ
An image on the consent screen that will help users recognize your app
Local file for upload **Browse**

Support email ⓘ
Shown on the consent screen for user support
example@gmail.com

Scopes for Google APIs
Scopes allow your application to access your user's private data. [Learn more](#)
If you add a sensitive scope, such as scopes that give you full access to Gmail or Drive, Google will verify your consent screen before it's published.

email
profile
openid

Add scope

Authorized domains ⓘ
To protect you and your users, Google only allows applications that authenticate using OAuth to use Authorized Domains. Your application's links must be hosted on Authorized Domains. [Learn more](#)
cambiumnetworks.com
example.com
Type in the domain and press Enter to add it

Application Homepage link
Shown on the consent screen. Must be hosted on an Authorized Domain.
https:// or http://

Application Privacy Policy link
Shown on the consent screen. Must be hosted on an Authorized Domain.
https:// or http://

Save Submit for verification Cancel

8. Once clicked **Save** for above page it redirects to creation of OAuth Client ID.
9. Select **Application type** as **Web Application**, give a Name, add Guest Portal Hostname URL/IP which you will get from cnMaestro UI and click **Create**.

Google APIs Social-Login-Cambium

Create OAuth client ID

For applications that use the OAuth 2.0 protocol to call Google APIs, you can use an OAuth 2.0 client ID to generate an access token. The token contains a unique identifier. See [Setting up OAuth 2.0](#) for more information.

Application type
Web application
Android [Learn more](#)
Chrome App [Learn more](#)
iOS [Learn more](#)
Other

Name ⓘ
cnMaestro

Restrictions
Enter JavaScript origins, redirect URIs, or both. [Learn more](#)
Origins and redirect domains must be added to the list of Authorized Domains in the [OAuth consent settings](#).

Authorized JavaScript origins
For use with requests from a browser. This is the origin (URI) of the client application. It can't contain a wildcard (https://*.example.com) or a path (https://example.com/subdir). If you're using a nonstandard port, you must include it in the origin URI.
https://ap-s1-guest.cloud.cambiumnetworks.com
https://www.example.com
Type in the domain and press Enter to add it

Authorized redirect URIs
For use with requests from a web server. This is the path in your application that users are redirected to after they have authenticated with Google. The path will be appended with the authorization code for access. Must have a protocol. Cannot contain URL fragments or relative paths. Cannot be a public IP address.
https://www.example.com
Type in the domain and press Enter to add it

Create Cancel

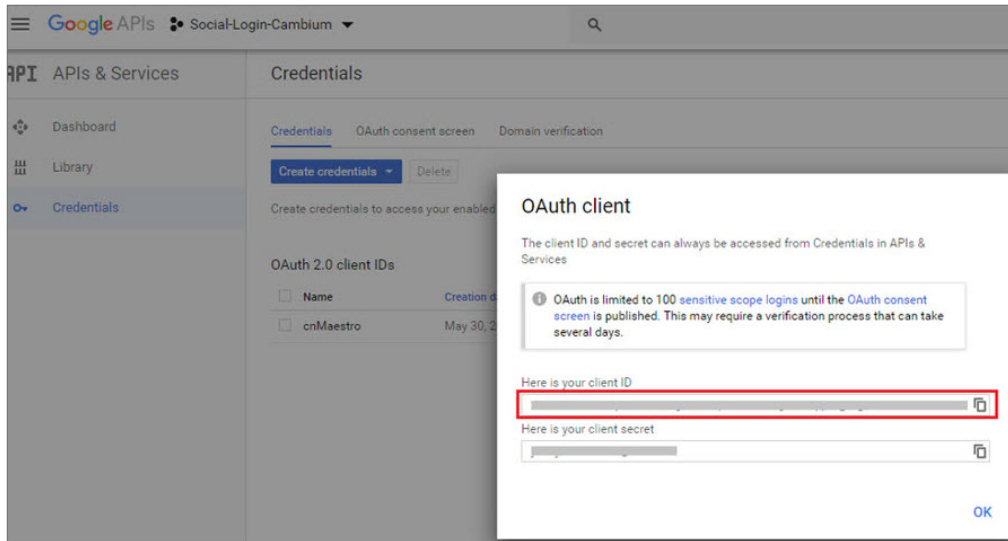
cnMaestro GUI

Guest Portal Hostname / IP: **ap-s1-guest.cloud.cambiumnetworks.com**

Note: Captive portal bypass will be enabled if social login with Facebook or Google these services.

☐ Google
☐ Twitter
☐ Facebook
☐ Office 365

10. Clicking Create on above page it redirects to the screen showing Client ID and Client Secret.



11. Copy the Client ID and paste it to the cnMaestro enabling Google under Social Logins and click **Save**.

Social Login
Guest Portal Hostname / IP
qk-us-el-guest.cloud.cambiumnetworks.com ⓘ Configure this URL in the Social login application settings.

Note: Captive portal bypass will be enabled if social login with Facebook or Google is enabled. This is required as the Captive-portal Network Assistant (Guest portal signon popup on mobile devices) is not compatible with the social login API provided by these services.

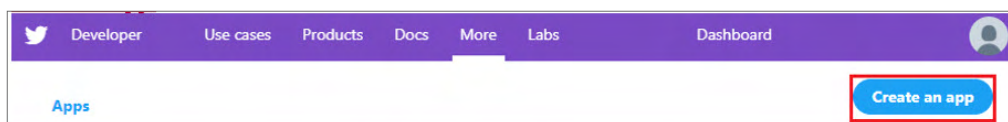
☒ Google
Id

☐ Twitter
☐ Facebook
☐ Office 365

SMS Authentication
Add Whitelist

Twitter

1. Login to Twitter Account and access <https://developer.twitter.com/en/apps> and click **Create an app**.



App details

The following app details will be visible to app users and are required to generate the API keys needed to authenticate Twitter developer products.

App icon Upload
Maximum size of 700x, JPG, GIF, PNG

App name (required)
TestTwitter
Maximum characters: 32

Application description (required)
Share a description of your app. This description will be visible to users so this is a good place to tell them what your app does.
Test_Twitter
Between 10 and 200 characters

Website URL (required)
https://www.cambiumnetworks.com

Allow this application to be used to sign in with Twitter [Learn more](#)
☒ **Enable Sign in with Twitter**

Callback URLs (required)
OAuth 1.0a applications should specify their oauth_callback URL on the request token step, which must match the URLs provided here. To restrict your application from using callbacks, leave these blank.
https://ap-s1-guest.cloud.cambiumnetworks.com/cn-ctrl/guest/
[+ Add another](#)

Terms of Service URL
https://ap-s1-s1-5pkodub8un.cloud.cambiumnetworks.com

Privacy policy URL
https://ap-s1-s1-5pkodub8un.cloud.cambiumnetworks.com

Organization name
Cambium

Organization website URL
http://www.cambiumnetworks.com

Tell us how this app will be used (required)
This field is only visible to Twitter employees. Help us understand how your app will be used. What will it enable you and your customers to do?
Provide WiFi access to guest client by using twitter as authentication media.
This is purely for WiFi testing purpose.

cnMaestro GUI

☒ Twitter
Consumer API Key:
Consumer API Secret Key:
Callback URL: https://ap-s1-guest.cloud.cambiumnetworks.com/cn-ctrl/guest/756a2

Cancel **Save**

- Click **Keys** and **Tokens** and copy **Consumer API Key** and **Consumer API Secret Key**..

Keys and tokens
Keys, secret keys and access tokens management.

Consumer API keys
[Redacted] (API key)
[Redacted] (API secret key)
[Regenerate](#)

- Paste them to cnMaestro GUI for Twitter social login.

Social Login

Guest Portal Hostname / IP
 Configure this URL in the Social login application settings.

Note: Captive portal bypass will be enabled if social login with Facebook or Google is enabled. This is required as the Captive-portal Network Assistant (Guest portal signon popup on mobile devices) is not compatible with the social login API provided by these services.

☐ Google
☒ Twitter

Consumer API Key

Consumer API Secret Key

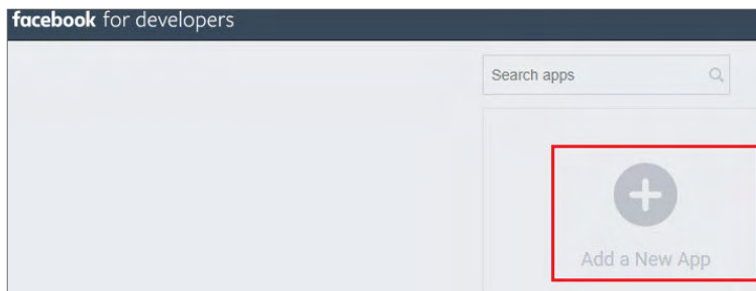
Callback URL

☐ Facebook
☐ Office 365

SMS Authentication
☐ Add Whitelist

Facebook

1. Login to Facebook Account and access <https://developers.facebook.com/apps/> and click **Add a New app**.



2. Enter App **Display Name**, **Contact Email**, and click on **Create App ID**.

Create a New App ID

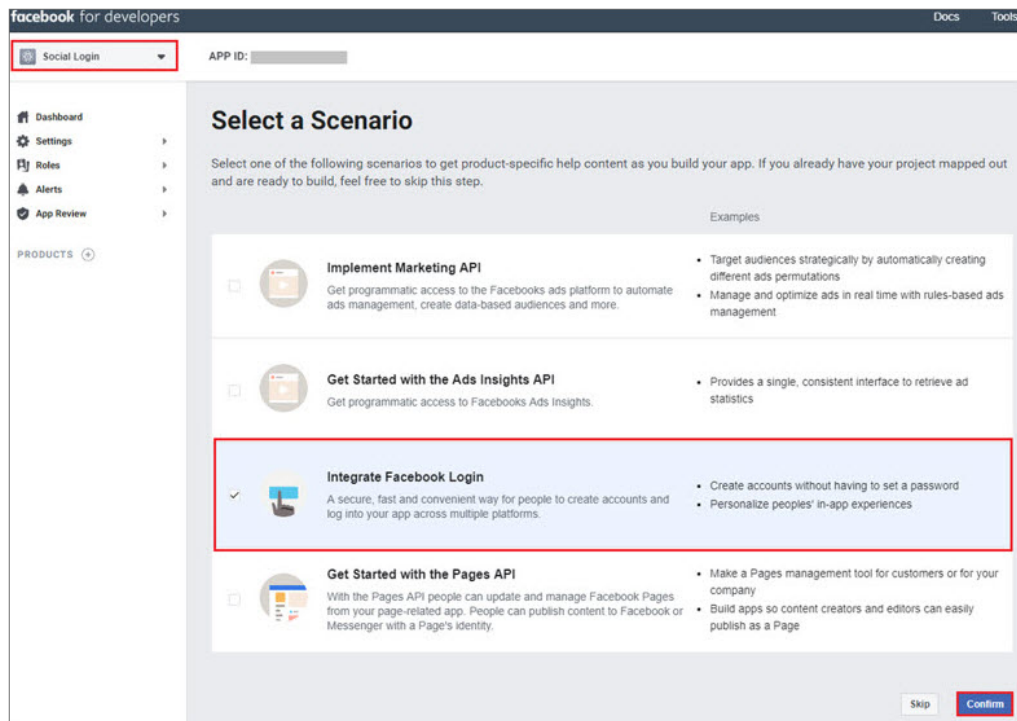
Get started integrating Facebook into your app or website.

Display Name

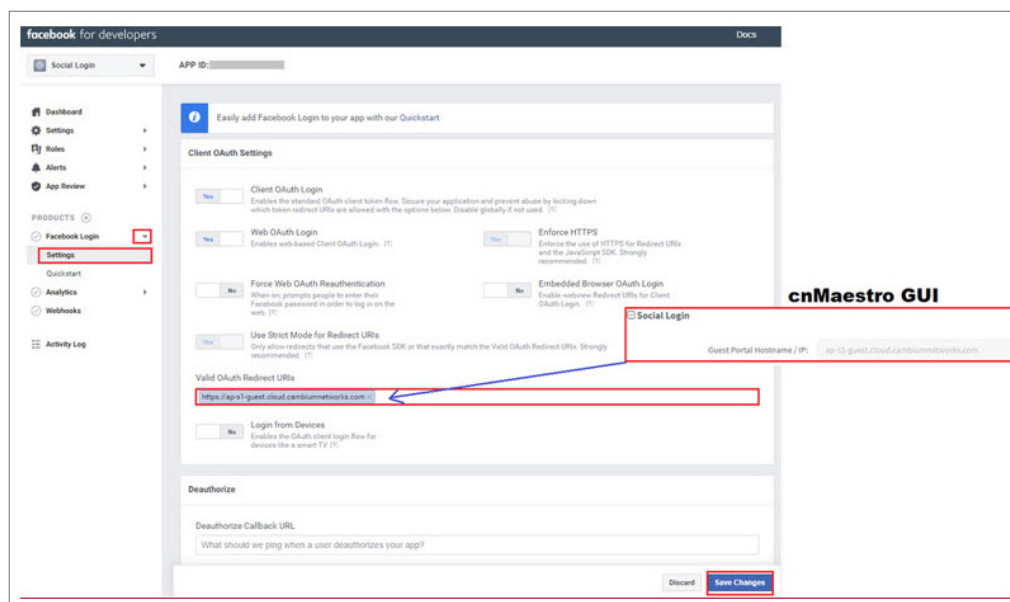
Contact Email

By proceeding, you agree to the Facebook Platform Policies

3. Select a Scenario as Integrate Facebook Login and click **Confirm**.



4. Navigate to **Settings** tab under Facebook Login and add Guest Portal Hostname from cnMaestro to Valid OAuth Redirect URLs section and click **Save Changes**.



5. Navigate to **Settings > Basic** and copy **App ID** and **App Secret**.

Social Login APP ID: [redacted]

Dashboard
Settings
Basic
Advanced
Roles
Alerts
App Review

PRODUCTS
Facebook Login
Analytics
Webhooks
Activity Log

App ID [redacted] App Secret [redacted] Show

Display Name: Social Login Namespace: [redacted]

App Domains: [redacted] Contact Email: [redacted]@gmail.com

Privacy Policy URL: Privacy policy for Login dialog and App Details Terms of Service URL: Terms of Service for Login dialog and App Details

App Icon (1024 x 1024)
1024 x 1024

Category: Choose a Category
Find out more information about app categories here

Business Use
This app uses Facebook tools or data to:
☐ Support my own business
☐ Provide services to other businesses

Social Login
Guest Portal Hostname / IP: [redacted] Configure this URL in the Social login application settings.

Note: Captive portal bypass will be enabled if social login with Facebook or Google is enabled. This is required as the Captive-portal Network Assistant (Guest portal signon popup on mobile devices) is not compatible with the social login API provided by these services.

☐ Google
☐ Twitter
☒ Facebook

Id: [redacted]
 Secret: [redacted] Show

Reply URL: [redacted] Configure this URL in the Social login application settings.

☐ Office 365

SMS Authentication
 Add Whitelist

Save

Office 365

1. Login to Office 365 Account and access <https://apps.dev.microsoft.com/> and click **Add an app**.

Microsoft Application Registration Portal Tools Docs Feedback

We will no longer support registering and managing converged and Azure AD applications here starting May 2019. We recommend that you manage your existing applications and register new applications by using the App registrations (now Generally Available) experience in the Azure portal. [Click this banner to launch the new and improved experience.](#)

My applications [Learn More](#)

We recommend registering and managing converged applications by using the new and improved App registrations experience in the Azure Portal. [Go to the Azure portal](#)

Add an app

New Application Registration

We will no longer support registering and managing converged applications here starting May 2019. We recommend registering this application by using the new and improved App registrations (now Generally Available) experience in the Azure portal. [Go to the Azure portal](#)

Name

Social Login

By proceeding, you agree to the Microsoft Platform Policies: [Terms of use](#)

Create application Cancel

2. Upon Adding your App name and clicking Create application, it redirects to App page.
3. Copy Application ID and paste it to cnMaestro Guest Access page under Office 365.
4. Click **Generate New Password**.
5. Copy Reply URL from cnMaestro and paste it under Redirect URLs.
6. Add my.centrify.com to the Whitelist on the cnMaestro.

Name: Social Login

Application Id: XXXYyzzz-12345-4565-aabbcc ① → Copy and paste it to cnMaestro →

Application Secrets

Generate New Password Generate New Key Pair Upload Public Key

Type	Password/Public Key	Created
Password	yoq*****	Feb 15, 2019 11:44:35 AM

Platforms

Add Platform

Web

Allow Implicit Flow

Redirect URLs Add URL

https://ap-s1-guest.cloud.cambiumnetworks.com/assets/views/office.html ③

Logout URL

e.g. https://myapp.com/end-session

Add Whitelist

IP Address / Domain Name	Delete
aaq0175.my.centrify.com ④	✕

Add aaq0175.my.centrify.com to the whitelist

Social Login

Guest Portal Hostname / IP

qa-us-e1-guest.cloud.cambiumnetworks.com

Note: Captive portal bypass will be enabled if social login with Facebook or Google is enabled. This is required as the Captive-portal Network Assistant (Guest portal signon popup on mobile devices) is not compatible with the social login API provided by these services.

Google

Twitter

Facebook

Office 365

Reply URL

https://qa-us-e1-guest.cloud.cambiumnetworks.com/assets/views/office.html

Id

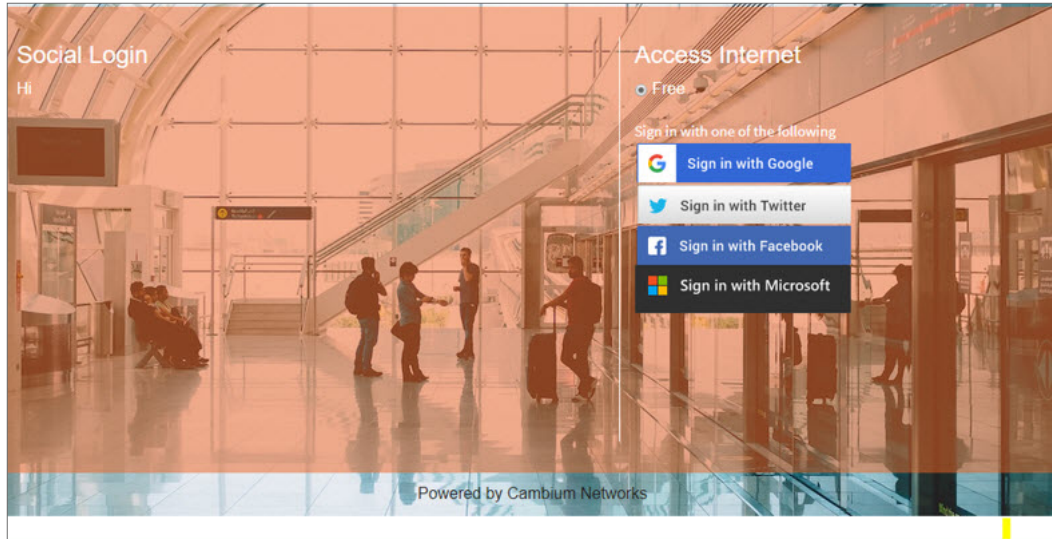
SMS Authentication

Add Whitelist

Save

Sample Template

Sample of client login page is displayed below:



Guest Access Portal Logout

To logout from cnMaestro Guest Access Portal perform as follows:

1. Navigate to **Services > Guest Access Portal** page and select the respective **Guest Portal Name**.
2. Select **Access** tab.
3. Select **Enable Logout functionality for the guest client** check box.
4. Click **Save**.

Guest Access Portal > HarshitGP

Basic **Access** Splash Sessions

Free PaidX Vouchers

☒ Enable Free Access

☒ Enable Logout functionality for the guest client

☐ Bypass Captive Portal Detection

Client Session

Renewal Frequency

10 Min(s) Valid range is 1-2628000 min(s)

Session Duration

10 Min(s) Valid range is 1-2628000 min(s)

Client Rate Limit

Client Quota Limit

Social Login

SMS Authentication

Add Whitelist

Save

The users can access and use the Guest Access Portal at any time within the specified **Renewal Frequency** and **Session Duration** provided.

SMS Authentication

The gateway provider sends a text SMS containing the OTP to the end user's phone number. Once OTP is received the client can enter the OTP and get Internet access.

Twilio, SMS Country, and SMS Gupshup are the SMS gateway providers that support the SMS OTP. Also there is a generic SMS gateway option, which provides flexibility to configure any preferred SMS gateway by cnMaestro users. Configuring SMS Gateway through this generic SMS gateway does require a little more involvement to review the integration specifications of the given SMS gateway. Please follow the guidelines as mentioned on the [Generic SMS Gateway configuration](#) section.

Generic SMS Gateway configuration

SMS Service providers expose a SMS API which typically works over HTTP GET or HTTP POST requests. Most of the SMS Gateways use username and password in the API requests to validate a given SMS send a request and some use special authorization token in the HTTP Headers.

Apart from that many API have specific tokens that need to be passed into the request along with the authentication part. To start off one has to first go through the SMS API document of the given SMS provider and understand all components do that need to be provided in the HTTP request and then build the corresponding cnMaestro configuration.

In general, all SMS API documents show example curl commands which can be used to create an SMS request with the server. Curl examples demonstrate the required components in the request and help to find the right configuration for the cnMaestro Guest Portal Generic SMS API.

The cnMaestro Generic SMS API configuration is split into multiple components which makes it easy to configure the static and the dynamic parts of the SMS API request. It also provides a way to handle the SMS API response and validate the API success or failure case. To handle the reply type, refer the **Advanced** options.

SMS Gateway provider name

Provide the SMS Gateway name which is used for reference purposes. This is not part of API request so please provide a meaningful name to identify this SMS Gateway service provider.

HTTP Request type

Based on the SMS gateway provider and the API document information, identify the SMS API. The SMS API uses HTTP GET or HTTP POST requests for communication with the SMS gateway server.

Example HTTP GET API request

`https://smsapiserver.com/service/sms/send?user=xxx&password=yyyyy&message="Your OTP is ABCD"&mobileNumber=123456789&dnd=yes&sid=SenderId&v=1.1&messagType=N`

Curl command to do HTTP GET request

```
Curl -v https://smsapiserver.com/service/sms/send?user=xxx&password=yyyyy&message=' Your OTP is ABCD' &mobileNumber=123456789&dnd=yes&sid=SenderId&v=1.1&messagType=N
```

Example HTTP POST request

HTTP POST URL

<https://smsapiserver.com/service/sms/send>

HTTP POST Form Content

`user=xxx&password=yyyyy&message="Your OTP for Internet Access is QW123"&mobileNumber=123456789&dnd=yes&sid=SenderId&v=1.1&messagType=N`

Curl command to do HTTP POST request


```
curl -v "https://smsapiserver.com/service/sms/send" -H "Content-Type: application/x-www-form-urlencoded" -X POST \
--data-urlencode 'user=xxx' \
--data-urlencode 'passwd=yyyyy' \
--data-urlencode 'mobilenumber=1234567789' \
--data-urlencode 'message=Your OTP for Internet access is QW123' \
--data-urlencode 'sid=Sid' \
--data-urlencode 'v=1.1' \
--data-urlencode 'mtype=N' \
--data-urlencode 'dnd=yes' \
--data-urlencode 'DR=Y'
```

If the SMS Gateway is using an authorization token, then below example curl request shows how the **Authorization** field is added into a HTTP header.

```
curl -v -H "Authorization: Bearer nZYIoU7QoUxuD03ct1CC2YvInqI7DmUAH6RYz01K1" \
"https://smsapiserver.com/service/sms/send?from=Test&\
to=123456789&\
message='Your OTP for Internet access is QW123'&\
format=json"
```

All the SMS API have components as follows:

- Static components which are part of the request.
- Two dynamic components which are part of the mobile number, to which the SMS needs to be sent and the message which contains the OTP.

Static components

API URL

Based on the above curl request example the URL configures as <https://smsapiserver.com/service/sms/send> where the request needs to be sent.

API URL information

From the example curl request please find the static components of the URL. Based on our above example this configures as user=xxx&password=yyyyy&dnd=yes&sid=SenderID&v=1.1&messagType=N.

Remove the message and mobile number query strings from that URL and configure the rest. This is what a static component is for a given SMS API so identify what all options are required for the SMS API request and add it in the format: key1=value1&key2=value2....

HTTP request header key

Based on the above example, If the SMS Gateway Provider API uses some HTTP header field like authorization token, etc. The corresponding HTTP header field name will be configured as **Authorization**.

HTTP request header key value

Based on the above example, the SMS gateway API configuration settings expose some authorization token or auth token, and the provided HTTP header key value will be configured as Bearer nZYIoU7QoUxuD03ct1CC2YvInqI7DmUAH6RYz01K1 in this configuration.

Dynamic components

Message parameter name

From the example curl request or the SMS gateway provider the parameter name used for the message key component where the OTP is added. It could be something like `message!text!msg` or whatever custom parameter name is used for sending the message component.

For example curl request, we have used “message” and this is what configures based on the example curl request.

Mobile number parameter name

From the example curl request or the SMS gateway provider the parameter name used for the mobile number key component where the OTP has to be sent. It could be something like `Tolmobile!mobile number` or whatever custom parameter name is used for sending the mobile number component.

In our example curl request, we have used `mobile number` and this is what configures based on the example curl request.

Advanced options

If you care for adding functionality for parsing the SMS API response on the `cnMaestro` and find if the request was successful or if the server returned an error. Then one can use this advanced configuration to let `cnMaestro` parse the SMS API reply.

The usual HTTP response code is anyway handled by default and this advanced config parses the reply content is configured. This should be configured by advanced users only and in case if there is any failure seen in SMS functionality then disable this and report the issue to Cambium Networks support.

Reply type

The SMS gateway API sends back a response to let the client know about the request results, this result could be in text format or in json/xml format. So based on the SMS API document select the reply type here as **TEXT**.

Success

Configure the text to match the success case as follows:

- Typically, servers may respond with a text message in reply like `success` or `sent`, then configure the exact message which should be matched in the response.
- If a server response is like `success`, `sent message to xxxxx`, then configure just `success` which matches in the reply.

Error

Configure the text which matches the failure case as follows:

- Typically, servers may respond with a text message in reply like **Error** or **Failure**, then configure the exact message which should be matched in the response.
- If a server response is like **ERROR**, `failed to send SMS to xxxxx`, `out of credit`, then configure just **ERROR** which matches in the reply to mark it as an error.

Reply Type JSON

JSON reply success key name

Please look for the SMS gateway provider API document in detail and find the JSON examples for the reply and identify the key which contains the successful response status value.

cnMaestro guest portal generic SMS supports nested JSON too and one has to configure the complete path for the given result key which contains the SMS message sent status. Example JSON replies are given below to be configured for this configuration:

Example 1

```
{
  "messages": {
    "to": "123456789",
    "status": {
      "id": 0,
      "groupId": 0,
      "groupName": "ACCEPTED",
      "result": [
        {
          "status": "MESSAGE_ACCEPTED"
        }
      ],
      "description": "Message accepted"
    },
    "smsCount": 1,
    "messageId": "2250be2d4219-3af1-78856-aabe-1362af1edfd2"
  }
}
```

Success key name to be configured based on the above example `messages.status.result[0].status`.

Example 2

```
{
  "count": 1,
  "list": [
    {
      "id": "1460978572913968440",
      "points": 0.16,
      "number": "48500500500",
      "date_sent": 1460978579,
      "submitted_number": "48500500500",
      "status": "QUEUE"
    }
  ]
}
```

Success key name to be configured based on the above example `list [0]. Status`.

Example 3

```
{
  "status": "Sent"
}
```

Success key name to be configured based on the above example is `status`.

JSON reply success key value

The success status can be single or multiple values based on the SMS Gateway provider and SMS gateway can respond back with a status as a message successfully sent or successfully queued, which is also a success case that the queued message sends out shortly.

Based on our examples the status or the result field can be mapped to multiple values like as follows:

- Sent
- Queued
- Success
- Message Accepted

So in this configuration one can add multiple such values that should be matched for the success case for the value as received for the JSON reply success key name field.

JSON reply failure key name

Look for the SMS Gateway Provider API document in detail and find the JSON examples for the reply and identify the key which contains the Error/Failure response status value.

cnMaestro guest portal generic SMS supports nested JSON too and one has to configure the complete path for the given result key which contains the SMS message sent failure field. Example JSON replies are given below to be configured for this configuration:

Example

```
{
  "invalid_numbers": [
    {
      "number": "456456456",
      "submitted_number": "456456456",
      "message": "Invalid phone number"
    }
  ],
  "error": 13,
  "message": "No correct phone numbers"
}
```

JSON reply failure key name to be configured based on the above example is error.

JSON reply key value

The error/failure status can be single or multiple values based on the SMS Gateway provider and SMS gateway can respond back with a status as a message sent error or multiple error codes for the corresponding error.

Based on our examples the error can be mapped to multiple values like 13|12|-1 etc. So in this configuration, one can add multiple such values which should be matched for the failure case for the value as received for the JSON reply failure key name field. reply type **XML**.

Reply type XML

XML reply success element

Look for the SMS gateway provider API document in detail and find the XML examples for the reply and identify the elements which contain the successful response status value.

cnMaestro guest portal generic SMS supports nested XML too and one has to configure the complete path for the given result element which contains the SMS message sent status. Example XML replies are given below to be configured for this configuration:

Example 1

```
<items>
<item id="0001" type="result">
<status>Success</status>
</item>
```

```
</items>
```

Success Element Name to be configured based on the above example is items/item/status.

Example 2

```
<?xml version="1.0" encoding="utf-8"?>
<int xmlns="http://tempuri.org/">-11</int>
```

Success Element Name to be configured based on the above example.

XML reply success element value

The success status can be single or multiple values based on the SMS Gateway provider and SMS gateway can respond back with a status as a message successfully sent or successfully queued, which is also a success case that the queued message sends out shortly.

Based on our examples the status or the result field can be mapped to multiple values like as follows:

- Sent
- Queued
- Success
- Message Accepted

So in this configuration one can add multiple such values that should be matched for the success case for the value as received for the XML Reply Success Element field.

SMS message sent failure field. Example XML replies are given below to be configured for this configuration:

Example 1

```
<items>
<item id="0001" type="result">
<error>-12</status>
</item>
</items>
```

XML Reply Failure Key Name to be configured based on the above example is items/item/error.

Example 2

```
<items>
<item id="0001" type="result">
<status>Error</status>
</item>
</items>
```

XML Reply Failure Key Name to be configured based on the above example is items/item/status.

Example 3

```
<?xml version="1.0" encoding="utf-8"?>
<int xmlns="http://tempuri.org/">-11</int>
```

XML Reply Failure Key Name to be configured based on the above example is int.

XML reply failure element value

The error/failure status can be single or multiple values based on the SMS Gateway provider and SMS gateway can respond back with a status as a message sent error or multiple error codes for the corresponding error.

Based on our examples the error can be mapped to multiple values like 13121-1 etc so in this configuration, one can add multiple such values which should be matched for the failure case for the value as received for the XML reply failure element field.

Sample configuration in the cnMaestro

Figure 492 : *Guest Access Portal*

The screenshot shows the 'Guest Access Portal' configuration page for 'SAS1_GAP'. The 'Access' tab is selected, showing options for 'Free', 'Paid', and 'Vouchers'. Under 'Free', 'Enable Free Access' and 'Enable Logout functionality for the guest client' are checked, while 'Bypass Captive Portal Detection' is unchecked. The 'Client Session' section includes 'Renewal Frequency' and 'Session Duration' both set to 1000 minutes. Below are expandable sections for 'Client Rate Limit', 'Client Quota Limit', 'Social Login', and 'SMS Authentication' (which is enabled). The 'SMS Gateway Provider' is set to 'Twilio', with fields for 'Auth Token', 'Account SID', and 'From' (set to 'US (+1)'). An 'OTP Template' is shown as 'Your OTP is %code%'. A note explains that %code% is a placeholder for the OTP code. At the bottom, there is an 'Add Whitelist' button and a 'Save' button.

EasyPass

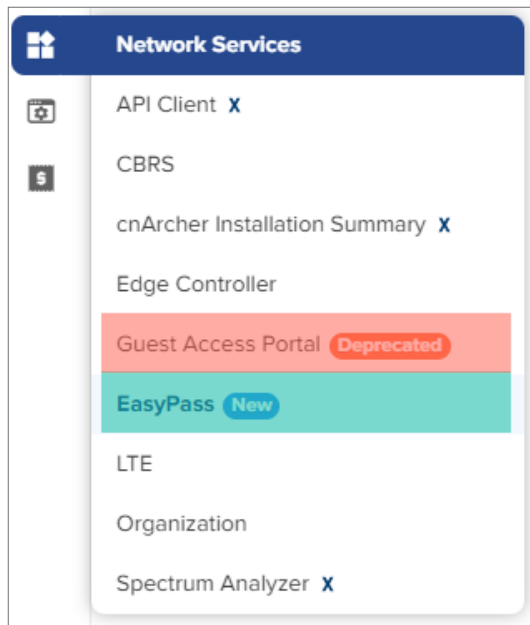
cnMaestro supports a guest access solution which provides an intuitive interface for various guest access methods used in the customer deployments. It allows the clients to connect to the internet through free tiers, vouchers, or paid access types. It also creates a separate network for guests by providing internet access to wireless devices such as mobile phones, tablets, and laptops.



Note

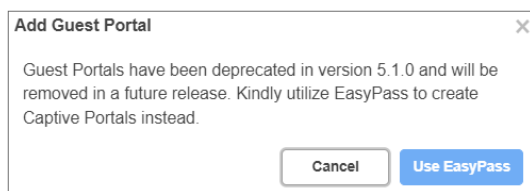
From cnMaestro 5.1.0 release onwards, the **Guest Access Portal** configuration wizard is deprecated and a new wizard, **EasyPass**, is introduced (as shown in [Figure 493](#)).

Figure 493 *Network Services > EasyPass*



When you create a new portal in the **Guest Access Portal** page, a window appears notifying that guest portals are discontinued and **EasyPass** must be used (as shown in [Figure 494](#)).

Figure 494 *The Add Guest Portal window*



The EasyPass access services provide secure and controlled access to users and visitors on your Wi-Fi network.

[Table 132](#) lists the supported devices and their compatibility with EasyPass.

Table 132 *List of supported devices - EasyPass*

Device	EasyPass support
Wi-Fi 5	Yes Note: Azure and GSuite are not supported.
Wi-Fi 6	Yes
Wi-Fi 7	Yes
Xirrus APs	No

EasyPass portal types are grouped into the following categories:

- [Guest/Public Access](#)
- [Employee/Student Access](#)
- [Combined](#)

Each category serves a different purpose and provides distinct features to accommodate various user requirements and access levels.

Guest/Public Access

This category includes the following portal types:

- **One Click**— All guests have access after agreeing to terms of use without needing to create an account. The **Social Login** options are integrated with One Click.
- **Self Registration X**— Guests must register themselves when connecting to the Wi-Fi network for the first time. The administrator can configure the self-registration process to determine whether sponsor approval is required. The sponsor approval can also be configured as manual or automatic confirmation. Additionally, the **SMS Gateway Provider** option is available as a self-registration method.
- **Sponsored Guest X**— Guests must provide their email address and their sponsor's email address to request internet access.
- **Voucher**— Users can access the network using a pre-assigned voucher. A voucher allows network administrators to create unique guest keys in bulk for retailers, hotels, conventions, and enterprises providing temporary visitor Wi-Fi access. These keys can be exported into a CSV file and integrated with other systems as point-of-sale (POS), property management, ticketing, or registration systems. Voucher also allows administrators to set a device limit for guests. If a guest tries to connect with more devices than allowed, the system alerts the guest with a warning message. Guests can manage their devices by deleting some of the device accounts without IT assistance.
- **Paid X**— IP Pay and Quickpay payment methods allow users to purchase internet services using a credit card. For purchasing internet plans, users are directed to a portal where they purchase the plan and then they are automatically redirected to the guest access portal where the purchased voucher is displayed. The users must save the voucher information if they use it on multiple devices.
- **WiFi4EU**— Provides free internet access only across the European Union (EU) to citizens and visitors through free-of-charge Wi-Fi hotspots in public spaces such as parks, squares, administrations, libraries, and health centers.



Note

X indicates that the feature is available only in cnMaestro **X**.

Employee/Student Access

This category includes the following portal types:

- **Microsoft Azure X**—A single sign-on process allows seamless access to Microsoft Azure X by integrating Wi-Fi and authentication.
- **Google Login X**—A single sign-on process allows seamless access to Google Login X by integrating Wi-Fi and authentication.



Note

Azure and Google Workspace are available on 6.x and later versions supporting firmware AP.

Combined

This category includes the following portal types:

- **One Click + Voucher**—Combines the benefits of both One Click access and voucher-based promotions, providing users with an easy and cost-effective way to access services.
- **One Click + Paid X**—Combines the benefits of One Click access with paid access to services.
- **Voucher + Paid X**—Combines the benefits of voucher-based promotions and paid access to services.

**Note**

- Using **Essentials**, you can create a maximum of four EasyPass portals.
- Using **cnMaestro-X**, you can create a maximum of 500 EasyPass portals.

Implementation of EasyPass portals for various types of users

[Table 133](#) lists the various types of users for whom the EasyPass portals can be implemented or best suited:

Table 133 *Implementation of EasyPass portals for various types of users*

EasyPass portal type	BYOD Employee or Student	Co-working Space User	Business Visitor	MDU Resident	Residence Hall Student	Hotel Guest	Retail Customer	Convention/Fair Attendee	Sports Event Fan	Public Wi-Fi user
Self Registration X		✓				✓	✓	✓	✓	✓
Sponsored Guest X			✓							
Voucher			✓			✓	✓	✓		
One Click							✓	✓	✓	✓
Paid X		✓				✓		✓		✓
WiFi4EU										✓
Microsoft Azure X	✓				✓					
Google Login X	✓				✓	✓				

EasyPass configuration

You can configure EasyPass using the cnMaestro UI. The EasyPass configuration process involves the following tasks:

- [Creating a portal](#)
 - [Creating One Click portal](#)
 - [Creating Self Registration X portal](#)
 - [Creating Sponsored Guest X portal](#)
 - [Creating Voucher portal](#)
 - [Creating Paid X portal](#)
 - [Creating WiFi4EU portal](#)

- [Creating Microsoft Azure X portal](#)
- [Creating Google Login X portal](#)
- [Creating One Click + Voucher portal](#)
- [Creating One Click + Paid X portal](#)
- [Creating Voucher + Paid X portal](#)
- [Configuring common parameters](#)
 - [The Basic screen parameters](#)
 - [The Limits screen parameters](#)
 - [The Design screen parameters](#)
 - [The Voucher screen parameters](#)
 - [The Plans screen parameters](#)
- [Accessing the common tabs](#)
 - [Sessions](#)
 - [Guests](#)
 - [Adding a new guest user](#)
 - [Vouchers](#)
 - [Paid Transactions X](#)
 - [Users X](#)

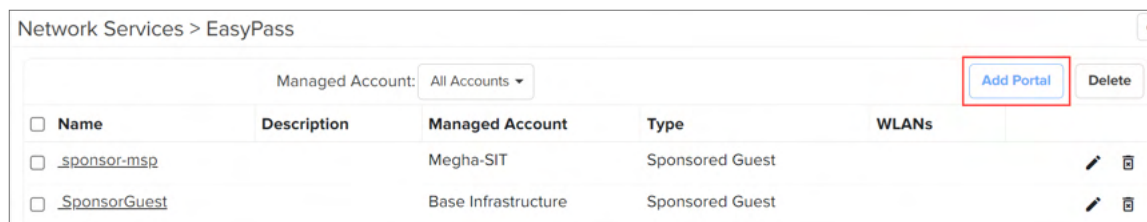
Creating a portal

Complete the following steps to create a portal:

1. From the home page of cnMaestro UI, navigate to **Network Services > EasyPass**.

The **Network Services > EasyPass** screen appears.

Figure 495 *The EasyPass screen*



2. Click the **Add Portal** button.

The **Select Portal Type** window appears.



Note

The options in the **Select Portal Type** window are different for **cnMaestro Essentials** and **cnMaestro X**.

[Figure 496](#) displays the options available for cnMaestro Essentials.

Figure 496 The Select Portal Type window—cnMaestro Essentials

Figure 497 displays the options available for cnMaestro X.

Figure 497 The Select Portal Type window—cnMaestro X



Note

The **WiFi4EU** option is applicable only to users in the EU region. Users from Asia-Pacific (APAC), Americas, and other non-EU regions do not have access to this option.

3. In the **Name** field, enter a name for the portal. For example, **test1**.

A name once created for the portal cannot be changed.

The **Name** field supports:

- A minimum of five and maximum of 64 characters.
 - Only alphanumeric, underscore (_), and dashes (-).
4. Select the required option from the **Managed Account** drop-down list. For example, **Base Infrastructure**.

**Note**

- When creating the EasyPass service, select the required managed account to which the service must be mapped.

5. Select the required option from the **Select Portal Type** window.
6. Click the **Save and Continue** button.

The portal is created and the **Basic** screen appears.

For information on parameters of the **Basic** screen, see [The Basic screen parameters](#).

7. Click the next tab.

Depending on the option you select, you will either see a **Limits** screen or portal-specific screen.

- For a **Self Registration X** portal type, follow the additional steps described in [Creating Self Registration X portal](#).
- For the **Sponsored Guest X** portal type, follow the additional steps described in [Creating Sponsored Guest X portal](#).
- For the **Voucher** portal type, follow the additional steps described in [Creating Voucher portal](#).
- For the **WiFi4EU** portal type, follow the additional steps described in [Creating WiFi4EU portal](#).
- For the **Microsoft Azure X** portal type, follow the additional steps described in [Creating Microsoft Azure X portal](#).
- For the **Google Login X** portal type, follow the additional steps described in [Creating Google Login X portal](#).

8. Configure the parameters of the **Limits** screen.

For information on parameters of the **Limits** screen, see [The Limits screen parameters](#).

9. Click the **Design** tab.

The **Design** screen appears.

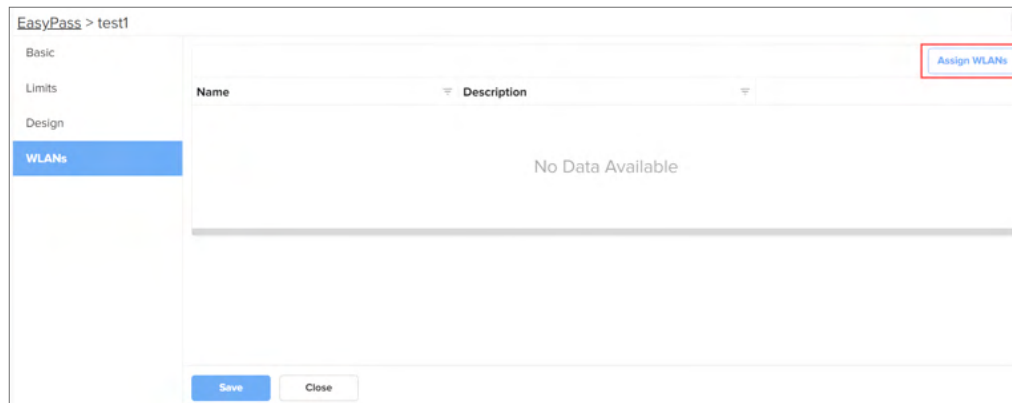
10. Configure the parameters of the **Design** screen.

For information on parameters of the **Design** screen, see [The Design screen parameters](#).

11. Click the **WLANS** tab.

The **WLANS** screen appears.

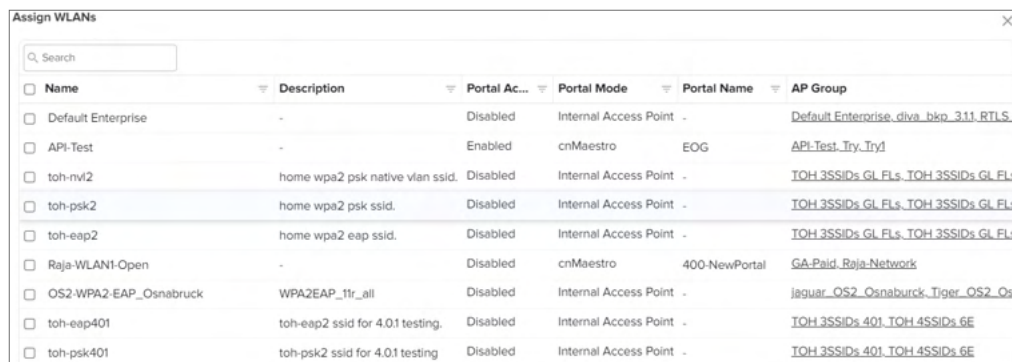
Figure 498 *The WLANs screen*



12. Click the **Assign WLANs** button.

The **Assign WLANs** window appears.

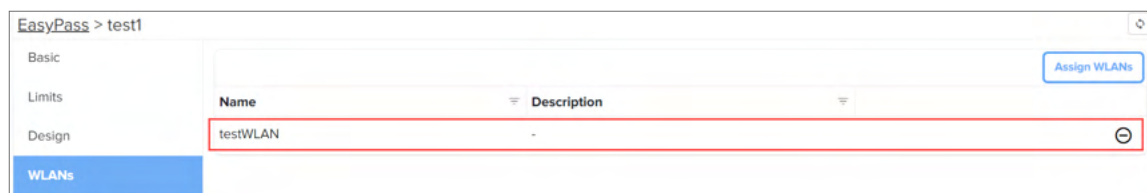
Figure 499 *The Assign WLANs window*



13. Select the required WLAN(s) and click **Assign**. For example, **testWLAN**.

The selected WLAN is added to the WLANs page.

Figure 500 *Assigned WLAN*



- Use the unlink (⊖) icon to unlink a WLAN.
- Use the **Save** button to apply the changes.
- Use the **Close** button to exit from the portal.

These buttons are available across all portal types.



Note

- The **Voucher**, **One Click + Voucher**, and **Voucher + Paid X** portal types have some common parameters that you must configure on their respective **Voucher** screens. For information on parameters of the **Voucher** screen, see [The Voucher screen parameters](#).

- The **Paid X**, **One Click + Paid X**, and **Voucher + Paid X** portal types have some common parameters that you must configure on their respective **Plans** screens. For information on parameters of the **Plans** screen, see [The Plans screen parameters](#).

14. Click **Save**.

Configuring common parameters

The following are the common parameters required for creating various portal types in EasyPass:

- [The Basic screen parameters](#)
- [The Limits screen parameters](#)
- [The Design screen parameters](#)
- [The Voucher screen parameters](#)
- [The Plans screen parameters](#)

The Basic screen parameters

[Figure 501](#) displays the **Basic** screen parameters.

Figure 501 *The Basic screen*

The screenshot shows the 'EasyPass > test1' interface. On the left is a sidebar with a menu containing 'Basic' (selected), 'Limits', 'Design', and 'WLANs'. The main area is titled 'Basic' and contains the following fields and controls:

- Name***: A text input field containing 'test1'.
- Managed Account**: A dropdown menu showing 'Base Infrastructure'.
- Description**: A large text area for entering a description.
- Client Login Event Logging**: A checkbox that is currently unchecked.
- Hide Advanced**: A link to toggle advanced settings.
- Landing Page**: A text input field with a placeholder text: 'Where should users go after the splash page? Keep it blank to send user to URL they were trying to fetch.'
- Pre-Login Allowed Domains**: A text input field with a placeholder text: 'Enter IP Address/Domain Name. Press Enter to add multiple values.'

At the bottom of the form are two buttons: 'Save' and 'Close'.

[Table 134](#) describes the **Basic** screen parameters that appear across all portal types on their respective **Basic** screens.

Table 134 *The Basic screen parameters*

Parameter	Description
Description	A brief description of the portal.
Client Login Event Logging	Indicates whether the Client Login Event Logging parameter is enabled or disabled. By default, this parameter is disabled.
Show Advanced This section consists of settings related to the landing page and pre-login allowed domains.	
Landing Page	Determines where the users are directed to after they have viewed or interacted with a splash page or login screen. Enter the complete URL with the protocol. For example, https://www.google.com Note: If the landing page field is kept blank, the users are automatically redirected to

Table 134 *The Basic screen parameters*

Parameter	Description
	the URL they were trying to access.
Pre-Login Allowed Domains	<p>Allows the administrators to specify domains that are allowed for access before the user logs in.</p> <p>Enter the IP address or domain name.</p> <p>Note: You can add multiple IP addresses or domain names.</p>

**Note**

After configuring the **Basic Screen** parameters, proceed to step 7 described in the [Creating a portal](#) process.

The Limits screen parameters

[Figure 502](#) displays the **Limits** screen parameters.

Figure 502 *The Limits screen*

EasyPass > test1

Basic

Limits

Design

WLANs

Session Expiry*

15 Minutes

How long will guests be able to access the Wi-Fi? Once a guest's session expires, they will need to register again.

Lockout Time*

None

Once the session expires, the client is locked out from network access for this duration.

Client Rate Limit*

Unlimited

Client Quota Limit*

Unlimited

[Table 135](#) describes the **Limits** screen parameters that appear across all portal types on their respective **Limits** screens.

Table 135 *The Limits screen parameters*

Parameter	Description
Session Expiry	<p>The specified duration after which a user's session automatically expires, disconnecting the user from the Wi-Fi network.</p> <p>The following options are supported:</p> <ul style="list-style-type: none"> • 15 Minutes • 1 Hour • 1 Day • 1 Month • End of Day (Midnight) • End of week (Saturday) • Custom <p>By default, 15 Minutes is selected.</p> <p>Select the required option from the drop-down list.</p>
Lockout Time	The lockout time restricts the ability to create a new session for the specified duration when a session expires.

Table 135 *The Limits screen parameters*

Parameter	Description
	<p>The following options are supported:</p> <ul style="list-style-type: none"> • None • 15 Minutes • 1 Hour • 1 Day • 1 Month • End of Day (Midnight) • End of week (Saturday) • Custom <p>By default, None is selected.</p> <p>Select the required option from the drop-down list.</p> <p>Note: The Lockout Time parameter is not available for Self Registration X, Sponsored Guest X, Voucher, Paid X, Microsoft Azure X, and Google Login X portal types.</p>
Client Rate Limit	<p>Indicates the client rate limit.</p> <p>The following options are supported:</p> <ul style="list-style-type: none"> • Limited—When the Limited option is selected, the Downlink and Uplink parameters appear. • Unlimited <p>By default, Unlimited is selected.</p>
Downlink	<p>This parameter is applicable only when Client Rate Limit is set to Limited.</p> <p>Downlink of client rate limit in Kbps.</p> <p>Maximum value: 1000000</p>
Uplink	<p>This parameter is applicable only when Client Rate Limit is set to Limited.</p> <p>Uplink of client rate limit in Kbps.</p> <p>Maximum value: 1000000</p>
Client Quota Limit	<p>Indicates the client quota limit.</p> <p>The following options are supported:</p> <ul style="list-style-type: none"> • Limited—When the Limited option is selected, the Total parameter appears. • Unlimited <p>By default, Unlimited is selected.</p>
Total	<p>The total client quota in MB or GB.</p> <p>You can either select MB or GB option from the drop-down list. By default, MB option is selected.</p> <p>Note: This parameter supports:</p> <ul style="list-style-type: none"> • A minimum of 1 MB and a maximum of 8000000 MB.

Table 135 *The Limits screen parameters*

Parameter	Description
	<ul style="list-style-type: none"> A minimum of 1 GB and a maximum of 8000 GB.
<p>Note: An additional parameter, Device Limit, must be configured for the following portal types in the Limits screen:</p> <ul style="list-style-type: none"> Self Registration X Microsoft Azure X Google Login X <p>The Device Limit parameter must also be configured for the following portal types:</p> <ul style="list-style-type: none"> Voucher— Use the Vouchers tab to configure the Device Limit parameter. Paid X— Use the the Add New Plan window of the Plans screen to configure the Device Limit parameter. 	
Device Limit	<p>Specifies the number of devices that the guest can connect to the wireless network.</p> <p>Default value: 1</p> <p>Maximum value supported: 10</p>



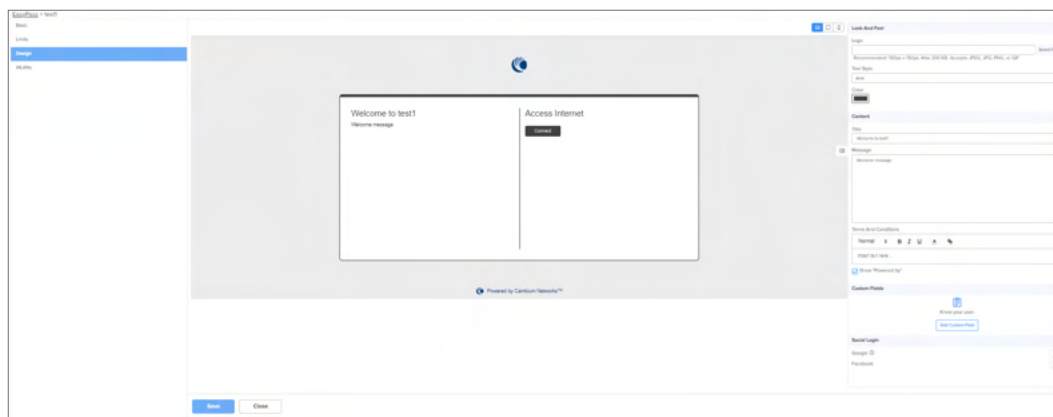
Note

After configuring the **Limits screen** parameters, proceed to step 9 described in the [Creating a portal](#) process.

The Design screen parameters

[Figure 503](#) displays the **Design** screen parameters.

Figure 503 *The Design screen*



[Table 136](#) describes the common **Design** screen parameters that appear across all portal types on their respective **Design** screens.

Table 136 *The Design screen parameters*

Parameter	Description
Logo	Logo for the design page.
Text Style	<p>Text style for the design page.</p> <p>The following options are supported:</p> <ul style="list-style-type: none"> Arial

Table 136 *The Design screen parameters*


Parameter	Description
	<ul style="list-style-type: none"> • Times New Roman • Verdana • Tahoma
Color	Color for the design page.
Title	Title for the design page.
Message	Welcome message for the design page.
Terms and Conditions	Terms and Conditions for the design page.
Show Powered By	<p>Indicates that a service is provided by an organization.</p> <p>You can disable this parameter.</p> <p>By default, this parameter is enabled.</p>
Custom fields	<p>Select the required field(s) to include in the design page by clicking the Add Custom Field button.</p> <p>The following options are supported:</p> <ul style="list-style-type: none"> • Date • Email • Name • Number • Phone • Text
Connect	<p>An option to provide access for users to the internet.</p> <p>Click the Connect button to access the internet.</p> <p>This is the default option available on the design page.</p>
Social Login	<p>You can enable the required social login option(s).</p> <p>The following options are supported:</p> <ul style="list-style-type: none"> • Google • Facebook <p>When social login option(s) are enabled, the design page contains Sign in with Facebook and Sign in with Google options.</p>  <p>Note: When Sign in with Facebook and Sign in with</p>

Table 136 *The Design screen parameters*


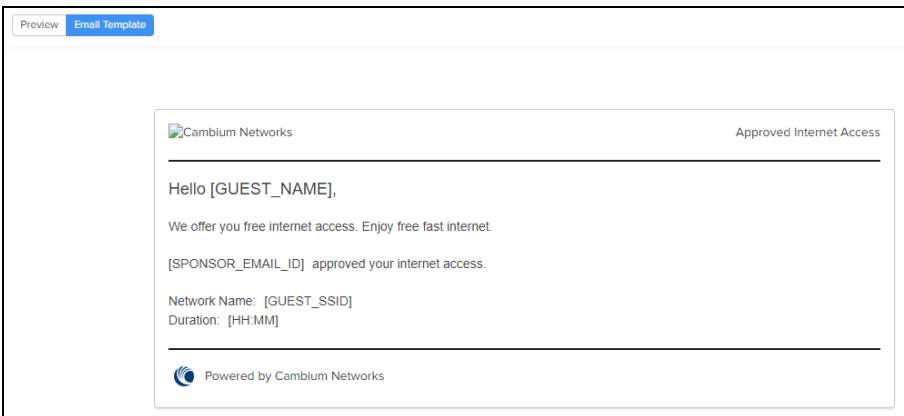
Parameter	Description
	Google options are enabled, they replace the default Connect option.
Device-specific view options of the design page 	The view options on the design page are tailored for various devices. The following options are supported: <ul style="list-style-type: none"> • Desktop View • Tablet/iPad View • Mobile View By default, Desktop View is selected. Note: The device-specific view options are available across all portal types on their respective Design screens.
Note: For the Self RegistrationX portal type, you must also configure additional parameters using the Preview tab and the Email Template tab.	
Preview tab The Preview tab is selected, by default. The following fields appear on the design page.	
Email	Enter the email ID. This field is mandatory.
Password	Enter the password. This field is mandatory.
Email Template tab When you click the Email Template tab, the following email template appears: <div data-bbox="224 1092 1123 1505" data-label="Image">  </div>	
Note: For the Sponsored Guest X portal type, configuration of additional parameters is required to identify users, create personalized accounts, verify email ownership, and send targeted notifications to guests. Additionally, these fields are necessary to notify users of important updates, promotions, or account-related changes. Configure the following additional parameters:	
Guest Name	Enter the guest name.
Guest Email	Enter the guest email ID.
Sponsor Email	Enter the sponsor email ID.
Note: For the Voucher portal type, configure the following additional parameter:	
Voucher Code	Indicates a voucher code.

Table 136 *The Design screen parameters*

Parameter	Description
	Enter a voucher code. This is a mandatory field.
Note: For the Paid X portal type, configure either of the following options:	
Select a Plan	Select the required plan from the drop-down list.
Payment Code	The payment code of the plan. Enter the payment code.
Note: For the Microsoft Azure X portal type, the following option is available:	
Sign in with Microsoft	Use this option to sign in with Microsoft.
Note: For the Google Login X portal type, the following option is available:	
Sign in with Google	Use this option to sign in with Google.
Note: For the One click + Voucher portal type, configure either of the following options:	
Free	You can select this option to provide free access to the internet.
Voucher	You must enter a voucher code when you select this option.
Note: For the One click + Paid X portal type, configure either of the following options:	
Free	You can select this option to provide free access to the internet.
Paid	When you select this option, you can either use Select a Plan or Payment Code option.
Note: For the Voucher + Paid X portal type, configure either of the following options:	
Voucher	When you select this option, you must enter a voucher code.
Paid	When you select this option, you can either use Select a Plan or Payment Code option.

**Note**

After configuring the **Design screen** parameters, proceed to step 11 described in the [Creating a portal](#) process.

The Voucher screen parameters

[Table 137](#) displays the **Voucher** screen parameters that appear across **Voucher**, **One Click + Voucher**, and **Voucher + Paid X** portal types on their respective **Voucher** screens.

Table 137 *The Voucher screen parameters*

Parameter	Description
Voucher Plan Name	Name of the voucher plan. Note: This parameter supports: <ul style="list-style-type: none"> A minimum of one and maximum of 64 characters. Only alphanumeric, underscore (_), and dashes (-). This parameter is mandatory.

Table 137 *The Voucher screen parameters*

Parameter	Description
Quantity	Quantity (in integers) of the voucher. Minimum value: 1 Maximum value: 2000
Voucher Message	Message for the voucher. This parameter supports a minimum of one and maximum of 128 characters.
Session Expiry	For information on this parameter, see Table 135 .
Voucher Expiry	The expiry time of the voucher. The following options are supported: <ul style="list-style-type: none"> • 15 Minutes • 1 Hour • 1 Day • 1 Month • End of Day (Midnight) • End of week (Saturday) • Custom By default, 1 Day is selected. This parameter is mandatory.
Client Rate Limit	For information on these parameters, see Table 135 .
Downlink	
Uplink	
Client Quota Limit	
Total	
Device Limit	
Bind Voucher to Device	Allows you to associate a voucher with a specific device. By default, this parameter is disabled.
Unlimited	Enable or disable the parameter. By default, this parameter is disabled. If you enable the check box, you can connect unlimited number of devices.

The Plans screen parameters

[Figure 504](#) displays the **Plans** screen parameters that appear across **Paid X**, **One Click + Paid X**, and **Voucher + Paid X** portal types on their respective **Plans** screens.

Figure 504 *The Plans screen*

EasyPass > test5

Basic

Plans

Design

WLANs

Payment Gateway*

Add Plan

Name	Price	Duration	Uplink	Downlink	Client Quota	Device Limit
------	-------	----------	--------	----------	--------------	--------------

No Data Available



Note

Before selecting a payment gateway, you must add a plan.

To add and manage a plan, complete the following steps:

1. Click the **Add Plan** button (as shown in [Figure 504](#)).

The **Add New Plan** window appears.

Figure 505 *The Add New Plan window*

Add New Plan

Plan Name*

Plan Cost*

Session Expiry*

15 Minutes

How long will guests be able to access the Wi-Fi? Once a guest's session expires, they will need to register again.

Client Rate Limit*

Unlimited

Client Quota Limit*

Unlimited

Device Limit

☒ Unlimited

Cancel Add

[Table 138](#) describes the common **Plans** screen parameters that appear across **Paid X**, **One Click + Paid X**, and **Voucher + Paid X** portal types on their respective **Plans** screens.

Table 138 *The Add New Plan window parameters*

Parameter	Description
Plan Name	Name for the plan. This parameter supports a minimum of one and maximum of 32 characters. Note: Alphanumeric and special characters are supported. This parameter is mandatory.
Plan Cost	Cost for the plan. This parameter is mandatory.
Currency	Currency for the plan. By default, USD is selected.
Session Expiry	For information on these parameters, see Table 135 .
Client Rate Limit	
Downlink	
Uplink	
Client Quota Limit	
Total	
Device Limit	
Unlimited	Enable or disable the parameter. If you disable the check box, you must specify the device limit. If you enable the check box, you can connect unlimited number of devices.

- Click the **Add** button (as shown in [Figure 505](#)).

The plan is added.

Figure 506 *Plan added*

EasyPass > test5

Basic

Plans

Design


WLANs

Payment Gateway*

Add Plan

Name	Price	Duration	Uplink	Downlink	Client Quota	Device Limit
test	USD 1000	15 Minutes	Unlimited	Unlimited	Unlimited	Unlimited

**Note**

Use the edit () icon to modify a plan.

- Select the required payment gateway option from the **Payment Gateway** drop-down list (as shown in [Figure 507](#)).

Figure 507 *Payment gateway options*

EasyPass > test5

Basic

Plans

Design

Payment Gateway*

IP Pay

Quickpay

The following options are supported:

- IP Pay
- Quickpay



Note

Set the mandatory fields for the selected payment gateway option(s).

[Figure 508](#) displays the parameters available for the **IP Pay** payment gateway.

Figure 508 *The IP Pay option*

Payment Gateway*
IP Pay

Callback URL
https://qa-us-e1-guest.cloud.cambiumnetworks.com/cn-cfr/guest/55cc5996c70e6c04d70 Configure this URL as Callback URL under IPPay application settings.

Paypage URL*

Paypage API*

Merchant ID*

Customer ID*

Terminal ID*
ram.sudharsanam@cambiumnetworks.com

Password*
Show

When you select the **IP Pay** option, you must configure the parameters described in [Table 139](#).

Table 139 *Parameters specific to the IP Pay option*

Parameter	Description
Callback URL	A URL that is called back by the payment gateway after a transaction is processed. Configure the Callback URL in the IPPay application settings.
Paypage URL	A URL that users are redirected to when they are asked to pay for a transaction. This URL typically points to a payment page where the user can enter the payment information. Enter the paypage URL. This parameter is mandatory.
Paypage API	A paypage API to create and manage payments, and retrieve payment information. Enter the Paypage API. This parameter is mandatory.
Merchant ID	A merchant ID to identify the merchant. Enter the merchant ID. This parameter is mandatory.
Customer ID	A customer ID to identify the customer. Enter the customer ID. This parameter is mandatory.
Note: Terminal ID and Password fields are populated, by default.	
Terminal ID	A terminal ID to identify the terminal and authenticate transactions processed through it.

Table 139 *Parameters specific to the IP Pay option*

Parameter	Description
Password	A password to authenticate the user.
Note: The parameters of the IP Pay option are also applicable to One Click + Paid X and Voucher + Paid X portal types.	

[Figure 509](#) displays the parameters available for the **Quickpay** payment gateway.

Figure 509 *The Quickpay option*

Payment Gateway*
Quickpay

Callback URL
https://qa-us-e1-guest.cloud.cambiumnetworks.com/cn-cbr/guest/b5cc5996cf0e6cc04d70 Configure this URL as Callback URL under QuickPay application settings.

Merchant ID*
ram.sudharsanam@cambiumnetworks.com

Merchant Key*
Show

Payment Window Agreement ID.*

Payment Window API Key*

When you select the **Quickpay** option, you must configure the parameters described in [Table 140](#).

Table 140 *Parameters specific to the Quickpay option*

Parameter	Description
Callback URL	A URL that is called back by the payment gateway after a transaction is processed. Configure the Callback URL in the QuickPay application settings.
Note: Merchant ID and Merchant key fields are populated, by default.	
Merchant ID	A merchant ID to identify the merchant.
Merchant key	A merchant key to authenticate the merchant's identity.
Payment Window Agreement ID	Payment window agreement ID. Enter the payment window agreement ID. This parameter is mandatory.
Payment Window API Key	Payment window API key. Enter the payment window API key. This parameter is mandatory.
Note: The parameters of the Quickpay option are also applicable to One Click + Paid X and Voucher + Paid X portal types.	

Accessing the common tabs

The following common tabs are available for various portal types in EasyPass:

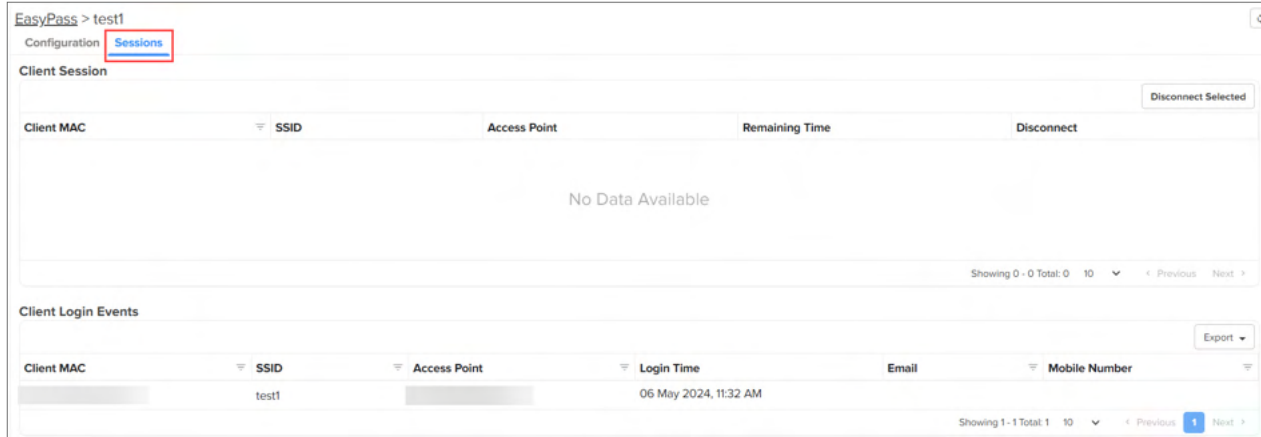
- [Sessions](#)
- [Guests](#)
 - [Adding a new guest user](#)
- [Vouchers](#)
 - [EasyPass](#)

- [Paid Transactions X](#)
- [Users X](#)

Sessions

You can access the **Sessions** page using the **Sessions** tab from, as shown in [Figure 510](#), from any of the portals.

Figure 510 *The Sessions page*



The **Sessions** tab includes two sections:

- Client Session—Administrators can view the details of all client sessions.
- Client Login Events—Administrators can view the details of all the sessions of client login events.



Note

- The **Client Login Events** section displays the client login events only if the **Client Login Event Logging** check box is selected on the **Basic** screen. This checkbox is available across all portal types.
- The **Client Login Events** section displays the login events for 7 days.

Administrators can export the client login events using the following options:

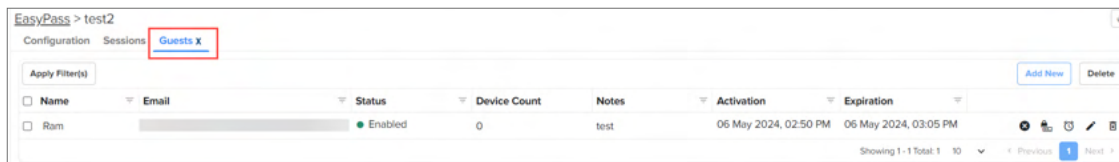
- Export page as CSV
- Export page as PDF
- Export all as CSV

Guests

The **Guests** page allows you to view details of self-registered guests connecting to the wireless network.

You can access the **Guests** page using the **Guests** tab (as shown in [Figure 511](#)).

Figure 511 *The Guests page*



Note

The **Guests** tab appears only for the **Self Registration X** portal type.

Adding a new guest user

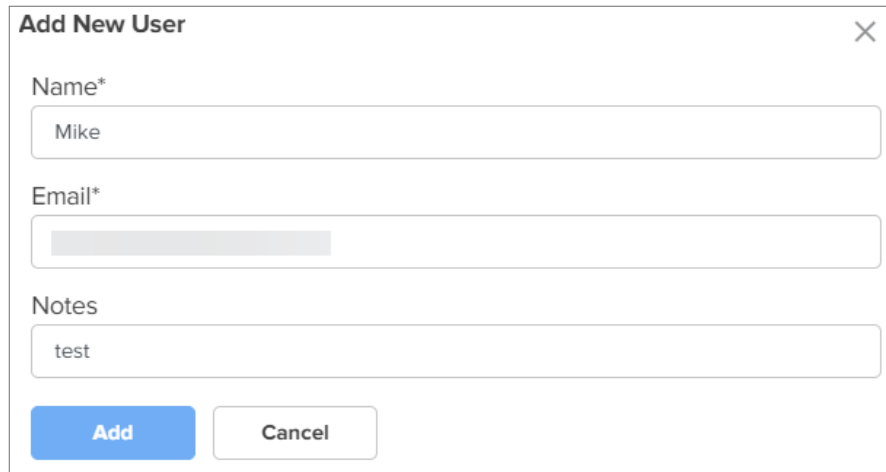
You can also add a new guest user from the **Guests** page.

Complete the following steps to add a new user:

1. On the **Guests** page, click **Add New**.

The **Add New User** window appears.

Figure 512 The Add New User window

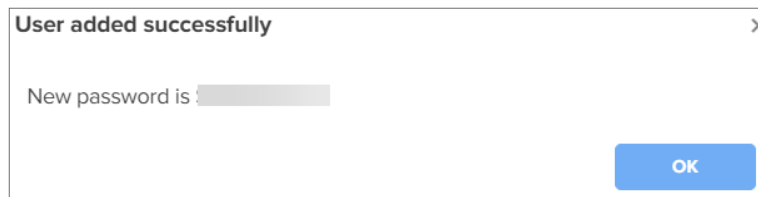


The 'Add New User' window is a modal dialog with a close button (X) in the top right corner. It contains three input fields: 'Name*' with the value 'Mike', 'Email*' which is empty, and 'Notes' with the value 'test'. At the bottom, there are two buttons: 'Add' (blue) and 'Cancel' (white with a grey border).

2. In the **Name** field, enter the name of a user. This field is mandatory.
3. In the **Email** field, enter an email ID of the user. This field is mandatory.
4. In the **Notes** field, enter the description for creating a new user. This field is optional.
5. Click the **Add** button.

The **User added successfully** window appears with a message showing a new password (as shown in [Figure 513](#)).

Figure 513 The User added successfully window

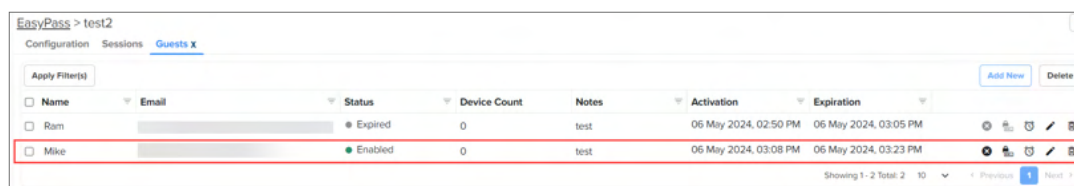


The 'User added successfully' window is a modal dialog with a close button (X) in the top right corner. It displays the message 'New password is : ' followed by a masked password field. At the bottom right, there is a blue 'OK' button.

6. Click **OK**.

A new guest user is added (as shown in [Figure 514](#)).

Figure 514 The new guest user details



The screenshot shows the 'EasyPass > test2' interface with the 'Guests' tab selected. A table lists guest users. The row for 'Mike' is highlighted with a red border. The table has columns for Name, Email, Status, Device Count, Notes, Activation, and Expiration. There are also 'Add New' and 'Delete' buttons at the top right of the table area.

Name	Email	Status	Device Count	Notes	Activation	Expiration
Ram		Expired	0	test	06 May 2024, 02:50 PM	06 May 2024, 03:05 PM
Mike		Enabled	0	test	06 May 2024, 03:08 PM	06 May 2024, 03:23 PM

You can view the details of the self registered guest connected to the Wi-Fi network (as shown in [Figure 514](#)).



Note

- Use the disable access (🔒) icon to disable access.
- Use the reset password (🔑) icon to reset a password.
- Use the extend session (🕒) icon to extend a session.
- Use the edit (✎) icon to edit the user details.
- Use the delete (🗑️) icon to delete a user.

Vouchers

You can access the **Vouchers** page using the **Vouchers** tab (as shown in [Figure 515](#)).

You can view a list of created vouchers, edit an existing voucher plan, and add a new voucher plan using the **Vouchers** tab. You also have options to add vouchers and delete all expired voucher(s).

Figure 515 *The Vouchers tab*

Voucher ID	Status	Creation Time	Claimed Time	Expiry Time
WTR4HTXT	Unclaimed	20 May 2024, 11:31 AM	-	21 May 2024, 11:31 AM
F2D4XTRT	Unclaimed	20 May 2024, 12:51 PM	-	21 May 2024, 12:51 PM



Note

The **Vouchers** tab appears only for the **Voucher**, **One Click + Voucher**, and **Voucher + Paid X** portal types.

Paid Transactions X

You can access the **Paid Transactions X** page using the **Paid Transactions X** tab (as shown in [Figure 516](#)).

Figure 516 *The Paid Transactions X tab*

Client MAC	Plan	Access Point	Voucher Code	Start Time	End Time	Transaction ID
No Data Available						



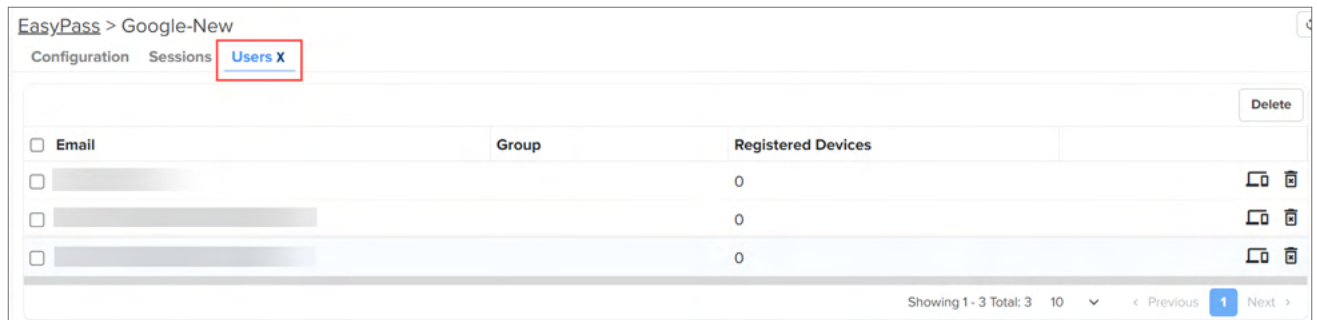
Note

The **Paid Transactions X** tab appears only for the **Paid X**, **One Click + Paid**, and **Voucher + Paid X** portal types.

Users X

You can access the **Users X** page using the **Users X** tab (as shown in [Figure 517](#)).

Figure 517 *The Users X tab*



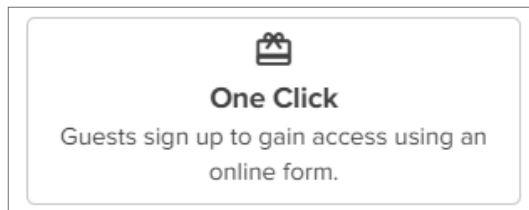
Note

The **Users X** tab appears only for the **Microsoft Azure X** and **Google Login X** portal types.

Creating One Click portal

You can create a One Click portal to provide guests with quick Wi-Fi access, adherence to policies, customized brand experiences, and secure Wi-Fi management with timing controls.

Figure 518 *The One Click option*



Note

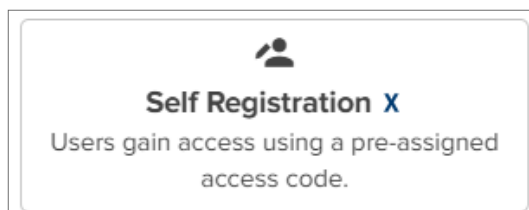
To create a One Click portal, complete the initial steps described in [Creating a portal](#) and continue with the next steps to configure the parameters of the **Basic** screen, **Limits** screen, **Design** screen, and **WLANs** screen.

Creating Self Registration X portal

You can create a self-registration portal to provide guests with easy account management, minimize IT involvement, offer SMS integration, email password delivery, sponsor workflow approvals, and enhance security and access control.

This section includes only the additional parameters that you must configure for the Self Registration X portal.

Figure 519 *The Self Registration X option*



Note

To create a Self Registration X portal, complete the initial steps described in [Creating a portal](#) and continue with the next steps to configure the parameters of the **Basic** screen, **Self Registration** screen, **Limits** screen, **Design** screen, and **WLANs** screen.

Follow these additional steps to create a Self Registration X portal:

1. From the **Basic** screen, click the **Self Registration** tab.

The **Self Registration** screen appears.

Figure 520 *The Self Registration screen*

2. Configure the parameters described in [Table 141](#).

Table 141 *The Self Registration screen parameters*

Parameter	Description
Approval required	<p>Enable or disable this option. By default, this option is disabled.</p> <p>When this parameter is enabled, you must provide the approver email ID(s) in the Approver Emails field.</p> <p>When this parameter is enabled, you have an option to select the required mode.</p>
Approver Emails	<p>This parameter is applicable when the Approval required check box is selected.</p> <p>Indicates the approver email ID(s) that must be provided.</p> <p>This parameter is mandatory.</p>
Mode	<p>This parameter is applicable when the Approval required check box is selected.</p> <p>The following options are supported:</p> <ul style="list-style-type: none"> • Manual—The sponsor receives an email with a link to approve the access request from the guest. Once the sponsor approves, the guest receives an email confirmation with password to access the network. • Auto—If the guest provides a configured sponsor's email, the password to access the network is automatically emailed to the guest and the sponsor is also notified through email.
Receive password via text	
By default, the guests receive the password through email address and text message.	
Enable	<p>Select the Enable check box. This parameter is disabled by default.</p> <p>When you select the Enable check box, the SMS Gateway Provider option is enabled.</p>
SMS Gateway Provider	Select the required SMS gateway option to be used to send the OTP to the guest's mobile device.

Table 141 *The Self Registration screen parameters*

Parameter	Description
	<p>By default, the Twilio option is selected.</p> <p>The following gateway options are supported:</p> <ul style="list-style-type: none"> • Fast SMS • Generic SMS API • SMS Country • SMS Gupshup • SMSAPI • Twilio • Victory Link SMS <p>Each of these gateway options can be configured with their respective parameters. For more information on the gateway options, see SMS Gateway Providers section.</p>

SMS Gateway Providers

This section describes the different types of SMS gateway providers.

[Figure 521](#) displays the parameters available for the **Twilio** option.

Figure 521 *Twilio option*


When you select the **Twilio** option, you must configure the parameters described in [Table 142](#).

Table 142 *Parameters of Twilio*

Parameter	Description
Note: The Username and Password fields are populated, by default.	
Auth Token	Auth token. Enter the auth token.
Account SID	Account SID. Enter the account SID.
From	Select the required country code from the drop-down list and enter the mobile number.
OTP Template	OTP template.

Table 142 *Parameters of Twilio*

Parameter	Description
	Enter the password in the OTP Template field. This parameter is mandatory.

[Figure 522](#) displays the parameters available for the **Generic SMS API** option.

Figure 522 *Generic SMS API option*

Receive password via text

☒ Enable

SMS Gateway Provider
Generic SMS API Beta

SMS Gateway Provider Name

HTTP Request Type
HTTP GET Request

HTTP Request Header Key

HTTP Request Header Key Value

API URL

API URL Information

Message Parameter Name

Mobile Number Parameter Name

Hide Advanced

API Reply Type
Text

Success

Failure

Country Code

OTP Template*

ⓘ The OTP template should include %password% as displayed in the sample text. Template may need to be approved, it's advised to contact respective SMS Gateway Provider. %password% will be replaced by the OTP code in the SMS.

When you select the **Generic SMS API** option, you must configure the parameters described in [Table 143](#).

Table 143 *Parameters of Generic SMS API*

Parameter	Description
SMS Gateway Provider Name	SMS gateway provider name. Enter a name for the SMS gateway provider. Enter the user name.

Table 143 *Parameters of Generic SMS API*

Parameter	Description
HTTP Request Type	<p>HTTP request type.</p> <p>The following options are supported:</p> <ul style="list-style-type: none"> • HTTP GET Request • HTTP POST Request
HTTP Request Header Key	HTTP request header key
HTTP Request Header Key Value	HTTP request header key value
API URL	<p>API URL</p> <p>Enter the API URL.</p>
API URL Information	<p>API URL information.</p> <p>Enter the API URL information.</p>
Message Parameter Name	<p>Message parameter name.</p> <p>Enter the message parameter name.</p>
Mobile Number Parameter Name	<p>Mobile number parameter name.</p> <p>Enter the mobile number parameter name.</p>
Show Advanced	
This section consists of advanced settings related to API reply type.	
API Reply Type	<p>API reply type.</p> <p>Select the required option from the drop-down list.</p> <p>The following options are supported:</p> <ul style="list-style-type: none"> • Text • JSON • XML
Text	
Success	<p>Success message.</p> <p>Enter the success message.</p>
Failure	<p>Failure message.</p> <p>Enter the failure message.</p>
JSON	
JSON Reply Success Key Name	<p>JSON reply success key name.</p> <p>Enter the JSON reply success key name.</p>
JSON Reply Success Key Value	<p>JSON reply success key value.</p> <p>Enter the JSON reply success key value.</p>
JSON Reply Failure Key Name	<p>JSON reply failure key name.</p> <p>Enter the JSON reply failure key name.</p>

Table 143 *Parameters of Generic SMS API*

Parameter	Description
JSON reply Failure Key Value	JSON reply failure key value. Enter the JSON reply failure key value.
XML	
XML Reply Success Element	XML reply success element. Enter the XML reply success element.
XML Reply Success Element Value	XML reply success element value. Enter the reply success element value.
XML Reply Failure Element	XML reply failure element. Enter the XML reply failure element.
XMI Reply Failure Element Value	XML reply failure element value. Enter the XML reply failure element value.
Country Code	Country code. Select the required country code from the drop-down list. For example, United States (+1)
OTP Template	OTP template. Enter the password in the OTP Template field. This parameter is mandatory.

[Figure 523](#) displays the parameters available for the **Fast SMS** option.

Figure 523 *Fast SMS option*

When you select the **Fast SMS** option, you must configure the parameters described in [Table 144](#).

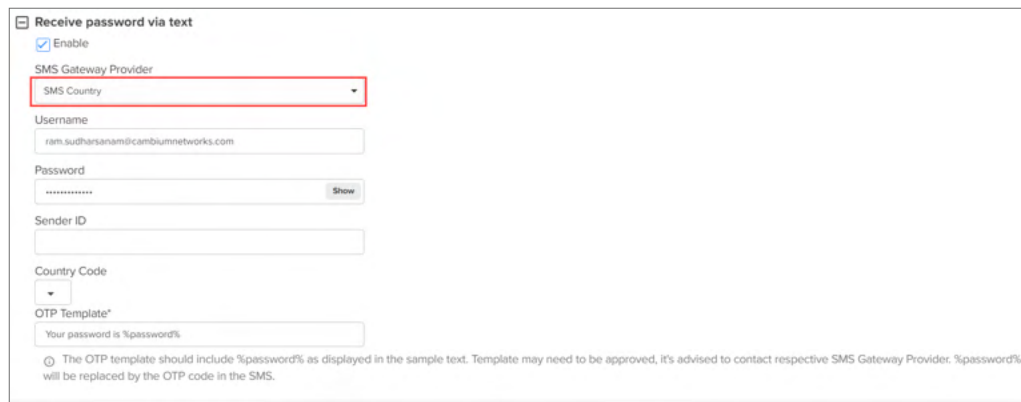
Table 144 *Parameters of Fast SMS*

Parameter	Description
Username	User name. Enter the user name. This field is optional.
Note: The Sender ID and API key fields are populated, by default.	
Account Type	Account type. Select the required option from the drop-down list.

Table 144 *Parameters of Fast SMS*

Parameter	Description
	<p>The following options are supported:</p> <ul style="list-style-type: none"> • Transaction • Promotional • International • OTP • Other
OTP Template	<p>OTP template.</p> <p>Enter the password in the OTP Template field.</p> <p>This parameter is mandatory.</p>

[Figure 524](#) displays the parameters available for the **SMS Country** option.

Figure 524 *SMS Country option*


☐ Receive password via text

☒ Enable

SMS Gateway Provider

SMS Country

Username
ram.sudharsanam@cambiumnetworks.com

Password
Show

Sender ID

Country Code

OTP Template*
Your password is %password%

The OTP template should include %password% as displayed in the sample text. Template may need to be approved, it's advised to contact respective SMS Gateway Provider. %password% will be replaced by the OTP code in the SMS.

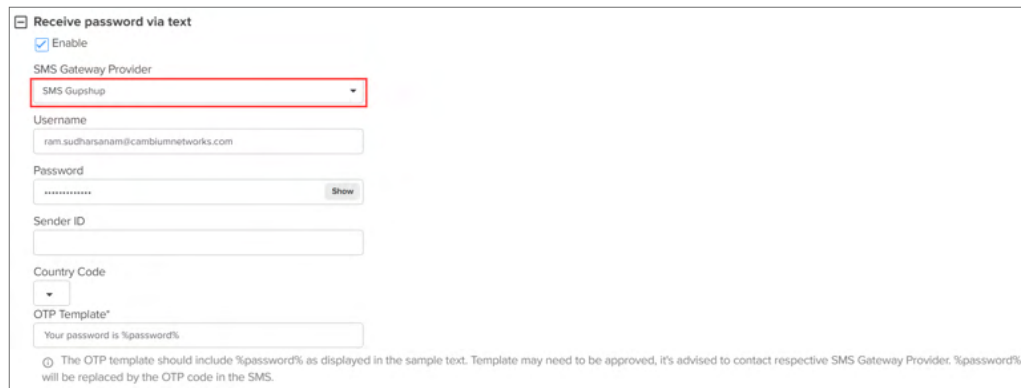
When you select the **SMS Country** option, you must configure the parameters described in [Table 145](#).

Table 145 *Parameters of SMS Country*

Parameter	Description
Note: The Username and Password fields are populated, by default.	
Sender ID	<p>Sender ID.</p> <p>Enter the sender ID.</p>
Country Code	<p>Country code.</p> <p>Select the required country code from the drop-down list. For example, United States (+1)</p>
OTP Template	<p>OTP template.</p> <p>Enter the password in the OTP Template field.</p> <p>This parameter is mandatory.</p>

[Figure 525](#) displays the parameters available for the **SMS Gupshup** option.

Figure 525 SMS Gupshup option



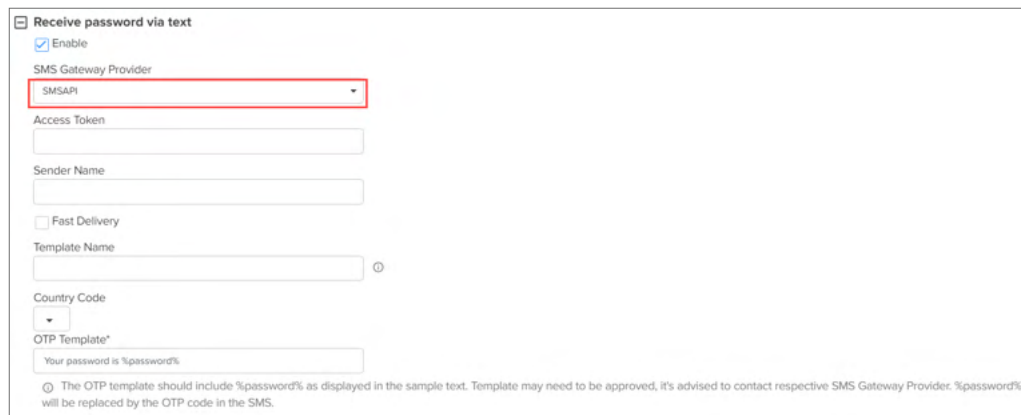
When you select the **SMS Gupshup** option, you must configure the parameters described in [Table 146](#).

Table 146 Parameters of SMS Gupshup

Parameter	Description
Note: The Username and Password fields are populated, by default.	
Sender ID	Sender ID. Enter the sender ID.
Country Code	Country code. Select the required country code from the drop-down list. For example, United States (+1)
OTP Template	OTP template. Enter the password in the OTP Template field. This parameter is mandatory.

[Figure 526](#) displays the parameters available for the **SMS API** option.

Figure 526 SMS API option



When you select the **SMS API** option, you must configure the parameters described in [Table 147](#).

Table 147 Parameters of SMS API

Parameter	Description
Note: The Username and Password fields are populated, by default.	

Table 147 *Parameters of SMS API*

Parameter	Description
Access Token	Access token. Enter the access token.
Sender Name	Sender name. Enter the sender name.
Fast Delivery	Enable the check box. By default, the check box is disabled.
Template Name	Template name. Enter the template name.
Country Code	Country code. Select the required country code from the drop-down list. For example, United States (+1)
OTP Template	OTP template. Enter the password in the OTP Template field. This parameter is mandatory.

[Figure 527](#) displays the parameters available for the **Victory Link SMS** option.

Figure 527 *Victory Link SMS option*


☐ Receive password via text

☒ Enable

SMS Gateway Provider
Victory Link SMS

Username
ram.sudhansam@cambiumnetworks.com

Password
***** Show

Language

Sender ID

OTP Template*
Your password is %password%

ⓘ The OTP template should include %password% as displayed in the sample text. Template may need to be approved, it's advised to contact respective SMS Gateway Provider. %password% will be replaced by the OTP code in the SMS.

When you select the **Victory Link SMS** option, you must configure the parameters described in [Table 148](#).

Table 148 *Parameters of Victory Link SMS*

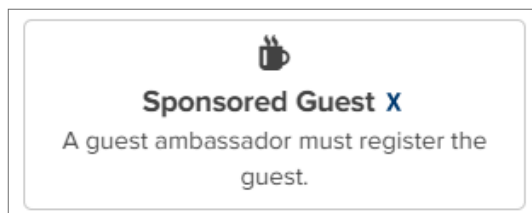
Parameter	Description
Note: The Username and Password fields are populated, by default.	
Language	Language. Enter the language.
Sender ID	Sender ID. Enter the sender ID.
OTP Template	OTP template. Enter the password in the OTP Template field. This parameter is mandatory.

Creating Sponsored Guest X portal

You can create a sponsored guest portal to enable non-IT staff to create, delete, or extend the validity of guest accounts.

This section includes only the additional parameters that you must configure for the Sponsored Guest X portal.

Figure 528 *The Sponsored Guest X option*



Note

To create a Sponsored Guest X portal, complete the initial steps described in [Creating a portal](#) and continue with the next steps to configure the parameters of the **Basic** screen, **Sponsored Domains** screen, **Limits** screen, **Design** screen, and **WLANs** screen.

Follow these additional steps to create a Sponsored Guest X portal:

1. From the **Basic** screen, click the **Sponsored Domains** tab.

The **Sponsored Domains** screen appears.

Figure 529 *The Sponsored Domains screen*

The screenshot shows the "Sponsored Domains" configuration screen. On the left is a sidebar with navigation tabs: Basic, Sponsored Domains (selected), Limits, Design, and WLANs. The main area has a header "EasyPass > test3". Below the header, it says "Guests must provide their own email and their sponsor's email to request Internet access." followed by "Sponsor Email Domains*" and a text input field containing "e.g. cambiumnetworks.com".

2. Configure the parameters described in [Table 149](#).

Table 149 *The Sponsored Domains screen parameters*

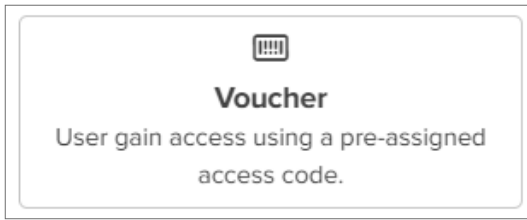
Parameter	Description
Sponsor Email Domains	Sponsor's domain(s). This parameter is mandatory.

Creating Voucher portal

You can create a voucher portal to create unique guest keys in bulk for retailers, hotels, conventions, and enterprises providing temporary visitor or guest Wi-Fi access.

This section includes only the additional parameters that you must configure for the Voucher portal.

Figure 530 *The Voucher option*



Note

To create a Voucher portal, complete the initial steps described in [Creating a portal](#) and continue with the next steps to configure the parameters of the **Basic** screen, **Voucher** screen, **Design** screen, and **WLANS** screen.

Follow these additional steps to create a Voucher portal:

1. From the **Basic** screen, click the **Voucher** tab.

The **Voucher** screen appears.

Figure 531 *The Voucher screen*

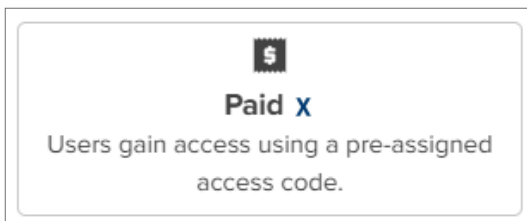
A screenshot of the EasyPass web interface showing the "Voucher" configuration screen. The left sidebar has tabs for "Basic", "Voucher", "Design", and "WLANS", with "Voucher" currently selected. The main area contains several configuration fields: "Voucher Plan Name*" (text input), "Quantity*" (input with minus and plus buttons, showing 0), "Voucher Message" (text input with placeholder "Enjoy Internet Services. Here is your access code."), "Session Expiry*" (dropdown menu showing "15 Minutes"), "Voucher Expiry*" (dropdown menu showing "1 Day"), "Client Rate Limit*" (dropdown menu showing "Unlimited"), "Client Quota Limit*" (dropdown menu showing "Unlimited"), "Device Limit" (checkbox for "Unlimited" and a text input showing "1"), and a checkbox for "Bind Voucher to Device". At the bottom are "Save" and "Close" buttons.

2. Configure the parameters described in [Table 137](#).

Creating Paid X portal

You can create a Paid X portal with IP Pay or Quickpay gateway for smooth internet connectivity purchase, and improving user experience.

Figure 532 *The Paid X option*



Note

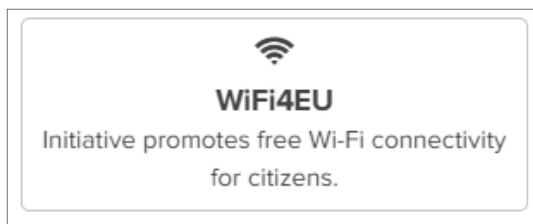
To create a Paid X portal, complete the initial steps described in [Creating a portal](#) and continue with the next steps to configure the parameters of the **Basic** screen, **Plans** screen, **Design** screen, and **WLANS** screen.

Creating WiFi4EU portal

You can create a WiFi4EU portal to provide free Wi-Fi access across the European Union (EU) to citizens and visitors in public spaces such as parks, squares, administrations, libraries, and health centers.

This section includes only the additional parameters that you must configure for the WiFi4EU portal.

Figure 533 *The WiFi4EU option*



Note

To create a WiFi4EU portal, complete the initial steps described in [Creating a portal](#) and continue with the next steps to configure the parameters of the **Basic** screen, **WiFi4EU** screen, **Limits** screen, **Design** screen, and **WLANs** screen.

Follow these additional steps to create a WiFi4EU portal:

1. From the **Basic** screen, click the **WiFi4EU** tab.

The **WiFi4EU** screen appears.

Figure 534 *General parameters*

A screenshot of a web-based configuration interface. At the top, it says "EasyPass > test6". On the left is a vertical sidebar with five tabs: "Basic", "WiFi4EU" (which is highlighted in blue), "Limits", "Design", and "WLANs". The main content area is for the "WiFi4EU" tab. It contains several fields: a "Language" dropdown menu set to "English"; a "Network UUID" text input field; a "Captive Portal URL" text input field containing "https://ga-us-e1-guest.cloud.cambiumnetworks.com/42b2a7c"; a "Metrics Snippet Script URL" text input field containing "https://collection.wifi4euec.europa.eu/wifi4eu.min.js"; and two checkboxes, "Enable Self-test Modus" and "Show Logo", both of which are currently unchecked. At the bottom of the form are "Save" and "Close" buttons. There is also a small text block explaining the UUID and the captive portal URL requirements.

2. Configure the parameters described in [Table 150](#).

Table 150 *General parameters - WiFi4EU*

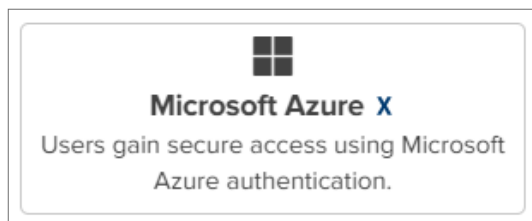
Parameter	Description
Language	Select the preferred language from the drop-down list.
Network UUID	Universally Unique Identifier (UUID) that the EC attributed to the WiFi4EU network installation.
Enable Self-test Modus	Allows the browsers background script verification.
Show Logo	Displays the WiFi4EU logo provided by the European union.

Creating Microsoft Azure X portal

Creating a **Microsoft Azure X** portal allows you to combine Wi-Fi access with authentication using Microsoft Office 365 credentials, making it easier for users to connect to the Wi-Fi network and access domain resources.

This section includes only the additional parameters that you must configure for the Microsoft Azure X portal.

Figure 535 *The Microsoft Azure X option*



Note

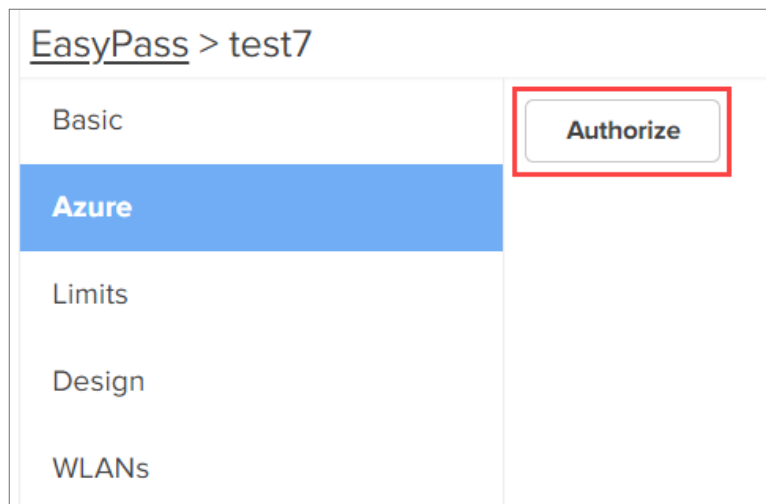
To create a Microsoft Azure X portal, complete the initial steps described in [Creating a portal](#) and continue with the next steps to configure the parameters of the **Basic** screen, **Azure** screen, **Limits** screen, **Design** screen, and **WLANs** screen.

Follow these additional steps to create a Microsoft Azure X portal:

1. From the **Basic** screen, click the **Azure** tab.

The **Azure** screen appears.

Figure 536 *The Azure screen*



Note

Only Microsoft Azure administrator role users can perform the **Authorize** step.

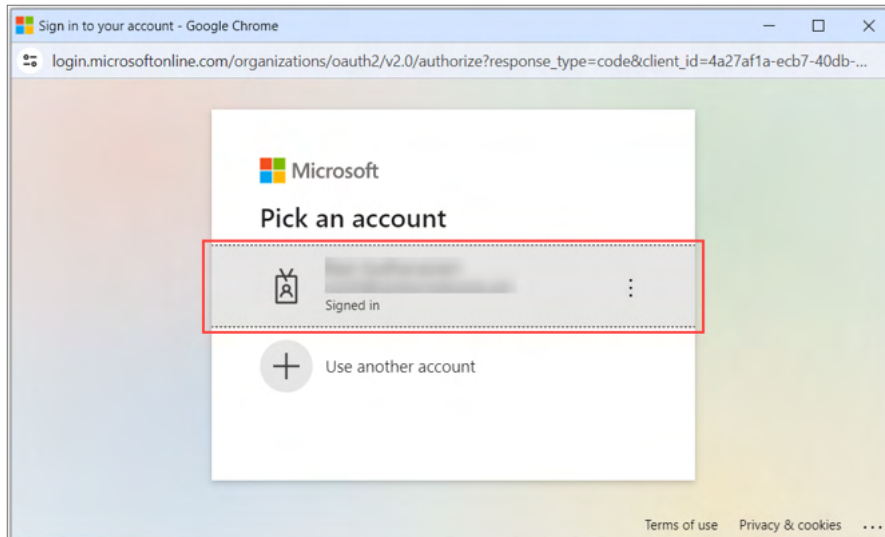
The **Authorize** step allows the EasyPass Azure application to:

- Make API calls to Microsoft Azure customer
- Sign in users
- Periodically sync the customer Azure directory
- Ensure only active user sessions are maintained or enforce relogin if user group information changes

2. Click the **Authorize** button.

The following screen appears, as shown [Figure 537](#).

Figure 537 Sign in to your account page



NOTE:

For information on how to integrate Active Directory with Azure, see [Azure AD Integration](#).

Creating Google Login X portal

Creating a **Google Login X** portal enables users with a Google account to connect to the wireless network by synchronizing the active directory. When enabled, if a guest who is part of the supported group tries to connect to the Wi-Fi network, the AP provides access to the guest.

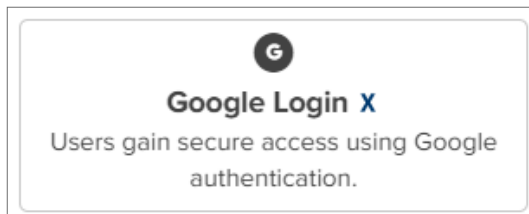


NOTE:

You must have a Google Workspace account before creating a Google Login X portal.

This section includes only the additional parameters that you must configure for the Google Login X portal.

Figure 538 The Google Login X option



Note

To create a Google Login X portal, complete the initial steps described in [Creating a portal](#) and continue with the next steps to configure the parameters of the **Basic** screen, **Google** screen, **Limits** screen, **Design** screen, and **WLANS** screen.

Follow these additional steps to create a Google Login X portal:


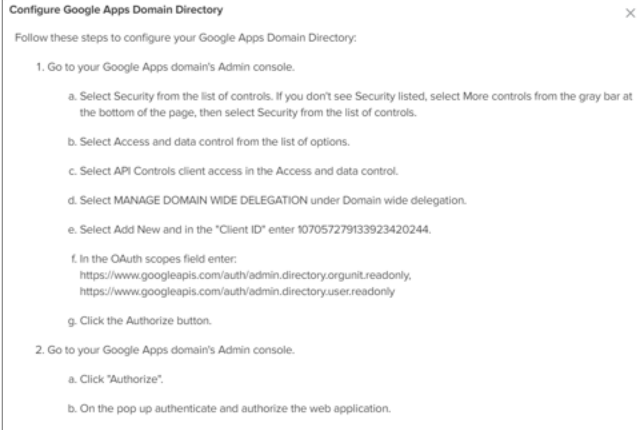
1. From the **Basic** screen, click the **Google** tab.

The **Google** screen appears.

Figure 539 *The Google screen*

2. Configure the parameters described in [Table 151](#).

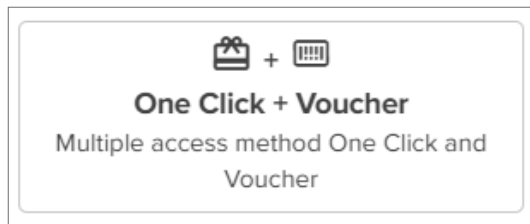
Table 151 *The Google screen parameters*

Parameter	Description
Enable Directory Synchronization	<p>Select the check box to enable the directory synchronization.</p> <p>When you select the Enable Directory Synchronization check box, the following screen appears:</p>  <p>When you click the Follow these steps link, the following window appears describing how to configure the Google Apps domain category.</p> <p>Follow the steps to configure your Google Apps domain directory.</p>  <p>Note: For information on how to integrate Active Directory with Google Workspace, see Google Workspace AD Integration.</p> <p>When you clear the Enable Directory Synchronization checkbox, you must configure the Allowed Domains parameter.</p>
Allowed Domains	<p>Enter the required domain(s).</p> <p>This is a mandatory parameter.</p>

Creating One Click + Voucher portal

Creating a One Click + Voucher portal combines the benefits of both One Click access and voucher-based promotions, providing users with an easy and cost-effective way to access services.

Figure 540 *The One Click + Voucher option*



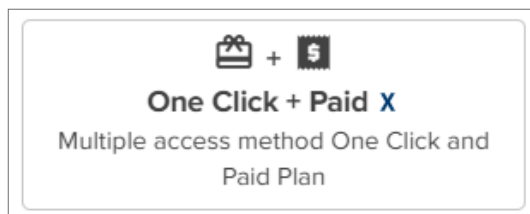
Note

To create a One Click + Voucher portal, complete the initial steps described in [Creating a portal](#) and continue with the next steps to configure the parameters of the **Basic** screen, **One Click** screen, **Design** screen, and **WLANS** screen.

Creating One Click + Paid X portal

Creating a One Click + Paid X portal combines the benefits of One Click access with paid access to services.

Figure 541 *The One Click + Paid X option*



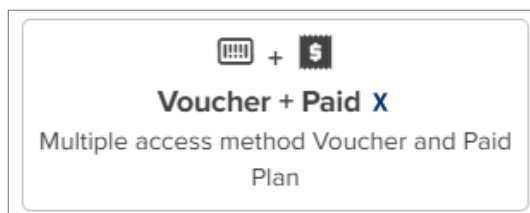
Note

To create a One Click + Paid X portal, complete the initial steps described in [Creating a portal](#) and continue with the next steps to configure the parameters of the **Basic** screen, **Plans** screen, **One Click** screen, **Design** screen, and **WLANS** screen.

Creating Voucher + Paid X portal

Creating a Voucher + Paid X portal combines the benefits of voucher-based promotions and paid access to services.

Figure 542 *The Voucher + Paid X option*



Note

To create a Voucher + Paid X portal, complete the initial steps described in [Creating a portal](#) and continue with the next steps to configure the parameters of the **Basic** screen, **Voucher** screen, **Plans** screen, **Design** screen, and **WLANS** screen.

MarketApps^X

This section includes the following topics:

- [Overview](#)
- [Adding a new MarketApp](#)
- [Managed Wi-Fi App](#)
 - [Basic tab](#)
 - [Settings tab](#)
 - [Design tab](#)
- [Self-Service Personal Wi-Fi App](#)
 - [Basic tab](#)
 - [Personal Wi-Fi configuration](#)
- [How to configure units by property managers](#)

Overview

MarketApps is an advanced service within cnMaestro that is designed to enhance network management through tailored applications. It offers specialized tools that empower Managed Service Providers (MSPs) to deliver greater value to their customers and end users by addressing their specific needs and challenges.

MarketApps introduces two new apps for the Multi-Dwelling Unit (MDU) market within MarketApps—**Managed Wi-Fi** and **Self-Service Personal Wi-Fi**. These applications simplify management of Wi-Fi services for property managers, residents, and service providers, by featuring an intuitive and streamlined workflow.

Target audience

- **Property managers**—MarketApps empowers property managers to centrally administer Wi-Fi access across their properties. They can set up community-wide Wi-Fi networks and manage personal Wi-Fi networks for local residents.
- **Residents**—Residents can set up and manage their own Wi-Fi networks within the community, ensuring personalized and secure internet access.
- **Solution providers**—MarketApps helps the solution providers to offer tailored Wi-Fi solutions, enhancing network performance and user satisfaction in multi-dwelling units and apartment complexes.

Benefits

- **Centralized management**—Property managers can oversee and control Wi-Fi access across multiple units or buildings from cnMaestro.
- **Customization**—Residents can set up personal Wi-Fi networks with customized SSIDs and passwords, enhancing their user experience.

To access MarketApps, navigate to **Network Services > MarketApps** in cnMaestro.

Figure 543 *MarketApps*

Name	Description	Managed Account	Type
Larry_suites	Residential cottages	Base Infrastructure	Self Service Personal Wi-Fi
Lakeshore Condominiums	Luxury apartment complex	Base Infrastructure	Managed Wi-Fi

Showing 21 - 30 Total: 34 < Previous 1 2 3 4 Next >

Adding a new MarketApp

To add a new MarketApp, complete the following steps:

1. Navigate to **Network Services > MarketApps** in cnMaestro.
2. Click the **Add New** button on the top right corner.
3. A new window **Select App Type** appears.

Select App Type

Name* Managed Account

Managed Wi-Fi
Apps for property managers and residents (Personal Wi-Fi optional).

Self Service Personal Wi-Fi
Simple App for residents only.

Cancel Save and Continue

4. Enter a name for the new Market App in the **Name** field.
5. Choose the type of managed account for the app from the **Managed Account** drop-down box.
6. Select the required app.
7. Click **Save and Continue**.

The respective app screens appears as discussed in the sections below.

Managed Wi-Fi App

The Managed Wi-Fi App in MarketApps enables property managers to centrally administer and manage Wi-Fi networks within their properties. This feature provisions both community-wide Wi-Fi networks and personal Wi-Fi networks for residents, allowing control and customization.

Figure 544 *Managed Wi-Fi App type*

Select App Type

Name*
Test_Cambium

Managed Account
Base Infrastructure

Managed Wi-Fi
Apps for property managers and residents (Personal Wi-Fi optional).

Self Service Personal Wi-Fi
Simple App for residents only.

Cancel Save and Continue

Basic tab

The Basic tab in MarketApps allows you to provide a description for your Wi-Fi network. The network name and managed account details are automatically populated and cannot be modified. Enter a brief description to clarify the network's purpose.

Figure 545 *Basic tab parameters*

MarketApps > Test_Cambium x

Basic ✓

Settings !

Design !

Name
Test_Cambium

Managed Account
Base Infrastructure

Description

Save Close

To configure the Basic tab, complete the following steps:

1. **Name**—Displays the chosen name for the Wi-Fi network.
2. **Managed Account**—This field is pre-populated based on previous selections.
3. **Description**—Enter a brief description that clearly explains the intended purpose or specific details of this Wi-Fi configuration.
4. Click **Save**.

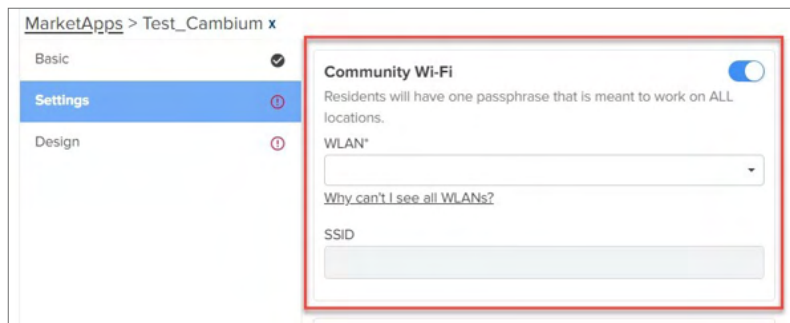
Settings tab

The Settings tab in MarketApps enables you to configure advanced settings for your Wi-Fi network. You can set up Community Wi-Fi, Personal Wi-Fi, or other options based on your specific requirements.

Community Wi-Fi

Community Wi-Fi in MarketApps allows property managers to set up and manage a single SSID for all residents within a property. This configuration is designed to provide centralized control over Wi-Fi access while ensuring uniform connectivity for all users.

Figure 546 Community Wi-Fi settings



To configure Community Wi-Fi under the Settings tab in Managed Wi-Fi, complete the following steps:

1. Select the **WLAN** for the community-wide Wi-Fi network.



Note

Valid WLANs must satisfy the following conditions:

- WLAN's Personal SSID must be disabled.
- Local ePSK table must not have any existing entries.
- WLAN Security settings must be configured as **WPA2 Pre-Shared Keys**, **WPA3 Pre-Shared Keys**, or **WPA2/ WPA3 Pre-Shared Keys**.
- WLAN should not be mapped to any existing MarketApps or EasyPass.

2. Select the SSID for the community Wi-Fi from the **SSID** drop-down list.
3. Click **Save**.

Personal Wi-Fi

The Personal Wi-Fi option in MarketApps allows residents to set up and manage their own personalized Wi-Fi networks within the community. This feature provides flexibility and customization for individual units, enhancing the user experience by allowing residents to manage their SSIDs and passwords.

Figure 547 *Personal Wi-Fi settings*

MarketApps > Test_Cambium x

Basic

Settings

Design

Community Wi-Fi

Residents will have one passphrase that is meant to work on ALL locations.

Personal Wi-Fi

Residents can create an additional personalized SSID for their unit, utilizing the common passphrase.

WLAN*

[Why can't I see all WLANs?](#)

Allow resident to change Wi-Fi Settings

Allow property manager to suspend and terminate internet service

Invite Property Managers

Type and press Enter

Property managers will have the ability to activate and oversee internet services for residents within their property.

Save Close

To configure Personal Wi-Fi under the Settings tab in Managed Wi-Fi, complete the following steps:

1. Select the WLAN for the personal Wi-Fi network from the **WLAN** drop-down list.



Note

Valid WLANs must satisfy the following conditions:

- WLAN's Personal SSID must be enabled.
- WLAN Security settings must be configured as **WPA2 Pre-Shared Keys**, **WPA3 Pre-Shared Keys**, or **WPA2/ WPA3 Pre-Shared Keys**.
- WLAN should not be mapped to any existing MarketApps or EasyPass.

2. **Allow Resident to Change Wi-Fi Settings**—Solution providers can enable or disable the option for residents to configure their own personalized settings.
3. **Allow Property Manager to Suspend and Terminate Internet Service**—Solution providers can enable or disable the option for property managers to suspend or terminate internet service.
4. Enter the property manager's email address in the **Invite Property Managers** text box to send an invitation. Property managers can activate and oversee internet services for residents within their property.
5. Click **Save**.



Note

Solution providers can select Community Wi-Fi, Personal Wi-Fi, or both options, depending on their requirements.

Design tab

The Design tab in MarketApps allows you to customize the branding and appearance of the property manager and resident portals, ensuring a cohesive and professional user experience.

Figure 548 Design tab parameters

MarketApps > Test_Cambium x

Basic ☒ Settings ☐ Design ☒

Login Page Title*
Welcome to Test_Cambium

Property Name*
Cambium
Name will be displayed for email communications

Logo
Select File
We recommend uploading a transparent PNG cropped to the edges of your logo. Image maximum size should be 200x200 pixels.

Color Theme
#25478d
Choose a custom accent color for the portal page.

Privacy URL
Privacy Policy that accounts has to acknowledge on their first access to the service.

Terms and Conditions URL
Terms and Conditions that accounts has to acknowledge on their first access to the service.

☐ Show "Powered by"

Save Close

Sample screen

Welcome to Test_Cambium
Email ID
Send me one time link
You'll receive an email containing a one-time sign-in link. Clicking this link will take you directly to the Wi-Fi Resident App, where you can see and manage your personal Wi-Fi settings.
Tip: Bookmark this page in your browser for easy access later.
Resident Portal

Table 152 Design tab parameters

Parameter	Description
Login Page Title	Customize a welcome message displayed on the login page
Property Name	Specify the property name used for internal identification and email communications.
Logo	Upload a logo file (PNG recommended) cropped to the edges and sized up to 200x200 pixels.
Color Theme	Customize the portal's color scheme with a chosen accent color.
Privacy URL	Provide the URL to your Privacy Policy that users must acknowledge on first access.
Terms and Conditions URL	Provide the URL to your Terms and Conditions that users must acknowledge.
Show "Powered by"	Enable this option to display the Powered by message.
Sample screen	<p>The sample screen section includes three views:</p> <ol style="list-style-type: none"> Property Manager—Displays the Property Manager interface where users can enter their email and request a one-time link for access. Resident Portal—Shows the Resident Portal interface where users can input their email to receive a one-time link for accessing their personal Wi-Fi settings. Email—Provides a view of the email format that users receive, which contains a link to access the Wi-Fi Manager App.

Self-Service Personal Wi-Fi App

The Self-Service Personal Wi-Fi App in MarketApps allows residents to independently manage and customize their Wi-Fi networks within residential properties. This feature provides residents with the capability to create and personalize SSIDs for their units, enhancing their control over network settings.

Figure 549 *Self-Service Personal Wi-Fi App*

Select App Type

Name*
Cambium_Test

Managed Account
Base Infrastructure

Managed Wi-Fi
Apps for property managers and residents (Personal Wi-Fi optional).

Self Service Personal Wi-Fi
Simple App for residents only.

Cancel Save and Continue

Basic tab

The configuration steps for the Basic tab are the same as those detailed earlier in the documentation. For information on setting the network name, managed account, and description, refer to the [Basic tab](#) configuration steps.

Personal Wi-Fi configuration

Residents can create personalized SSIDs for their units, allowing them to customize their network identification.

Figure 550 *Personal Wi-Fi settings*

MarketApps > Test_Camb x

Basic
Settings
Design

Personal Wi-Fi
Residents can create personalized SSID for their unit.

WLAN*

[Why can't I see all WLANs?](#)

Allow resident to change Wi-Fi Settings

Enable Open SSID
In areas with unreliable cellular connectivity, residents can connect to the internet via this Open SSID to scan the QR code and access the resident portal for changing their Wi-Fi SSID and password. Administrators can also set rate limits for this SSID from the WLAN settings page.

WLAN*

[Why can't I see all WLANs?](#)

Save Close

To configure Personal Wi-Fi, complete the following steps:

1. Select the WLAN for the personal Wi-Fi network from the **WLAN** drop-down list.

**Note**

Valid WLANs must satisfy the following conditions:

- WLAN's Personal SSID must be disabled.
- WLAN Security settings must be configured as **WPA2 Pre-Shared Keys, WPA3 Pre-Shared Keys, or WPA2/ WPA3 Pre-Shared Keys**.
- WLAN should not be mapped to any existing MarketApps or EasyPass.

2. **Allow Resident to Change Wi-Fi Settings**—Solution owners can enable or disable the option for residents to configure their own personalized configuration.
3. **Enable Open SSID** option allows residents to connect to the internet, scan the QR code, and access the resident portal to change their Wi-Fi SSID and password. Administrators can set rate limits for this SSID from the WLAN settings page.
4. Select the WLAN for the Open SSID network from the **WLAN** drop-down list.

**Note**

Valid WLANs must satisfy the following conditions:

- WLAN's Personal SSID must be disabled.
- WLAN Security settings must be configured as Open or OWE.
- WLAN should not be mapped to any existing MarketApps or EasyPass.

5. Click **Save**.

How to configure units by property managers

This sections contains the following topics:

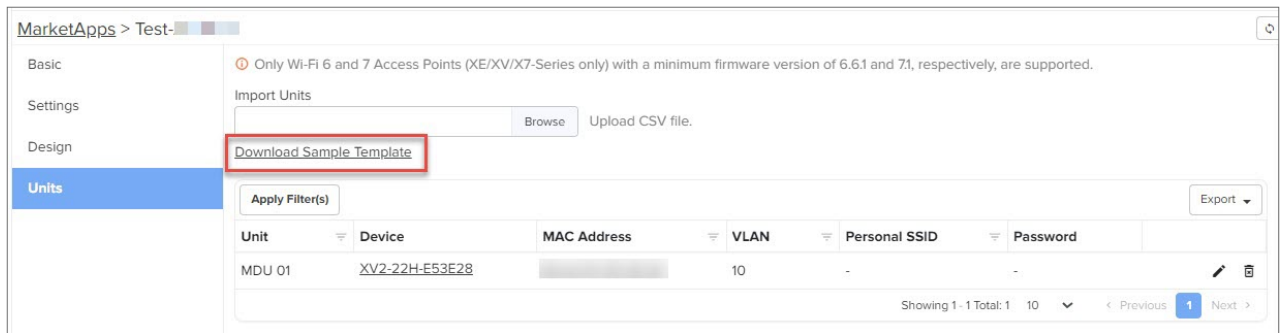
- [Units managed in the Managed Wi-Fi App](#)
 - [Assign Unit](#)
 - [Send Portal Link](#)
 - [Suspend](#)
 - [Extend](#)
 - [Terminate](#)
 - [View options in the Property Manager App](#)
- [Units managed in Self-Service Personal Wi-Fi App](#)

Units managed in the Managed Wi-Fi App

Managed Wi-Fi enables property managers to configure and oversee network settings for units using cnMaestro.

To set up and manage your Wi-Fi networks, complete the following steps:

1. Navigate to the **Unit** tab and click on the **Download Sample Template** option to get the sample file.

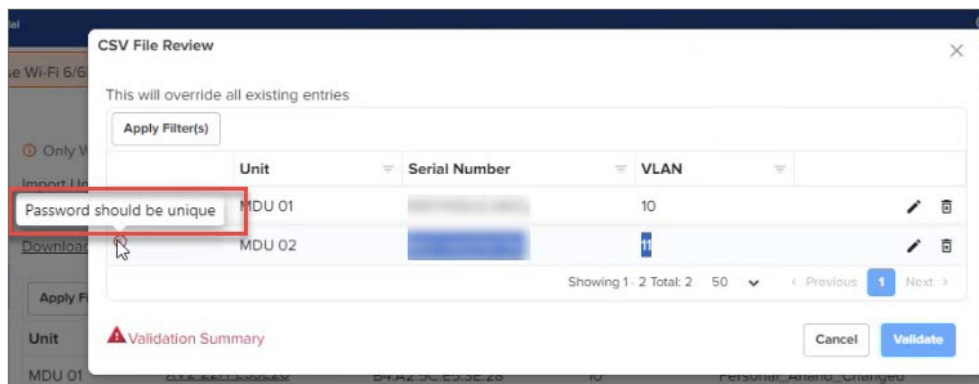


2. An example of the sample template and parameters is shown below:

Unit	Serial Number	MAC Address	VLAN	Personal SSID	Password
Unit name	Serial number of device	MAC Address of device	VLAN ID	SSID for the personal Wi-Fi	Password for Wi-Fi
MDU 01	B1000D000000	B1:00:0D:00:00:00	10	SSID 01	Pa\$\$Word123
MDU 02	B1000D000001	B1:00:0D:00:00:01	13	SSID 02	Pa\$\$Word123

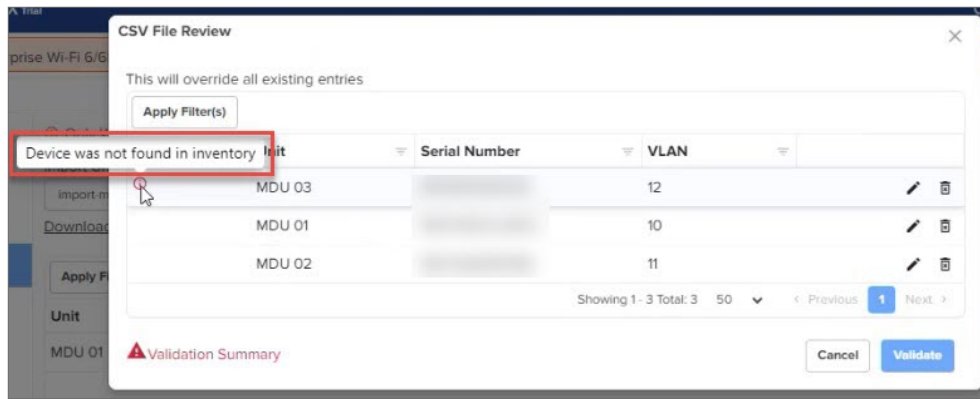
Parameter	Description
Unit	Enter the name or number of the unit (for example, MDU01 and MDU 02 are apartment numbers).
Serial Number	Enter the serial number of the device.
VLAN	Enter the VLAN ID assigned to the unit.
Personal SSID	Enter the SSID for the personal WiFi network.
Password	Enter the password for the Wi-Fi network.

3. After entering the details, save the Excel file with a new name to ensure you have a copy of the filled template and import it to cnMaestro. Note this step is crucial to avoid overwriting the original template.
4. During the import, you might encounter validation error messages. Here are some common error messages and their solutions:
 - a. **Password should be unique**—Ensure each unit has a unique password. Modify the password in the template so no two units share the same password.

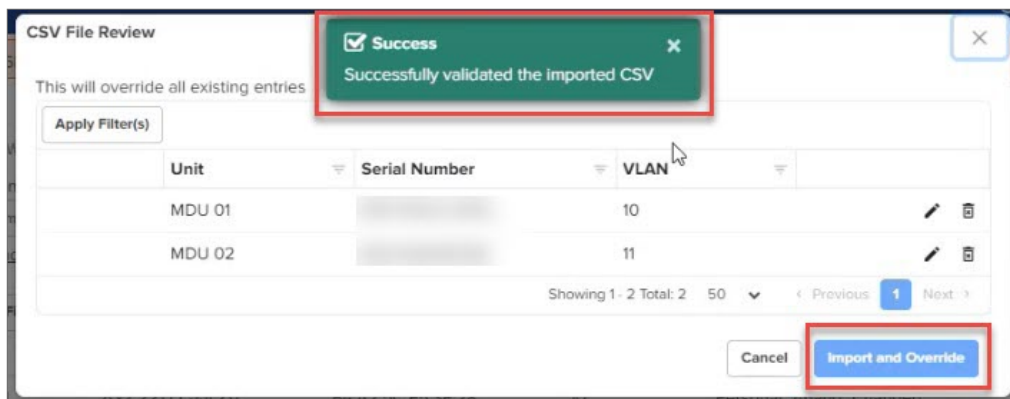


- b. **Device not found in inventory**—Ensure the serial number and MAC address entered correspond to devices that are already registered in the cnMaestro inventory. Make sure to import the details only after

onboarding the device.



- c. **Validates the unit**—Ensure the unit is less than 32 characters and contains only alphanumeric characters, underscores (_), hyphens (-), and spaces.
 - d. **Checks for duplicate units**—Ensure each unit is unique.
 - e. **Validates the password**—Ensure the password is between 8 and 64 characters long and does not include ", ' , / , ? , = , - , + , or spaces.
 - f. **Validates the SSID**—Ensure the SSID is less than 32 characters and contains only alphanumeric characters, underscores (_), hyphens (-), and spaces.
 - g. **Validates the VLAN**—Ensure the VLAN is an integer between 1 and 4094.
 - h. **Check if the device is already linked to another EasyApp**—Ensure devices are not linked to another application.
 - i. **Checks for duplicate devices**—Ensure each device is unique.
 - j. **Ensures that there is a device present**—Verify a device is specified as it is required.
 - k. **Validates that the AP group is linked to the personal WLAN**—Ensure the device has an AP group linked with the personal WLAN.
 - l. **Ensures the SSID is not duplicated**—Ensure each SSID is unique.
5. Once the file imports correctly, you can see the Successfully validated the imported CSV message as shown in the below figure.



6. Click **Import and Override** to finalize the import process.



Note

After importing, note the following points:

- Ensure the SSID name and password in the Excel sheet remain unchanged unless updated by the customer.
- Residents can modify their SSID and password through the resident portal later on.
- If **Allow residents to change Wi-Fi settings** (Figure 547) is enabled, tenants can change their SSID and password settings, and these changes do not get overwritten later.

7. Once the devices are successfully added, click **Save**.

MarketApps > Test-Anand x

Basic
Settings
Design
Units

Only Wi-Fi 6 and 7 Access Points (XE/XV/X7-Series only) with a minimum firmware version of 6.6.1 and 7.1, respectively, are supported.

Import Units
Browse Upload CSV file.

Download Sample Template

Apply Filter(s)

Unit	Device	MAC Address	VLAN	Personal SSID	Password
MDU 01	XV2-22H-E53E28		10	Personal-Changed	password@123_Changed
MDU 02	XV2-21X-E5384C		11	Personal-J	1234

Showing 1 - 2 Total: 2 50 < Previous 1 Next >

Save Close

8. The property manager receives an email titled **Welcome to the Wi-Fi Manager APP** and can **Sign In**.

Welcome to the Wi-Fi Manager App for [redacted]

Hello, you've been invited by the service provider to join Wi-Fi Manager App for Ananda's , you can access it using the button below.

Sign In

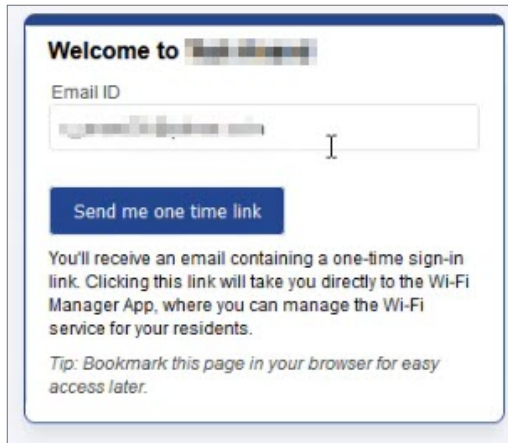
Thanks,
Cambium Networks

If you're having trouble with the button above, copy and paste the below link into your web browser.
https://qa-us-e1.test-easy-apps.cloud.cambiumnetworks.com/mdu-portal/manager/app/62d73e1f2d5a403598001cc1c2c7c762/login?em=v_anand31%40yahoo.co.in

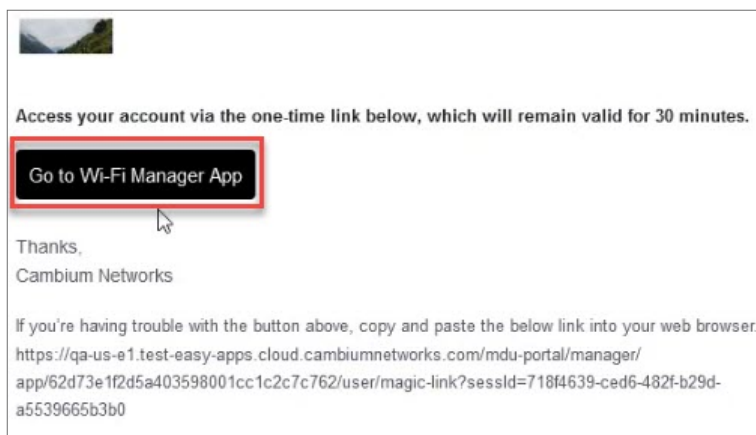
Tip: Bookmark the above link for Easy Access!

To quickly access your account in the future, consider bookmarking this login page in your web browser. This will save you time and effort when logging in next time!

9. The property manager enters the same email ID provided in the Managed Wi-Fi settings.



10. clicks **Send me a one-time link**.
11. The property manager receives an email containing a one-time link for logging into the property manager app.



12. Click **Go to Wi-Fi Manager App**.
13. The Property Manager app interface is shown below.

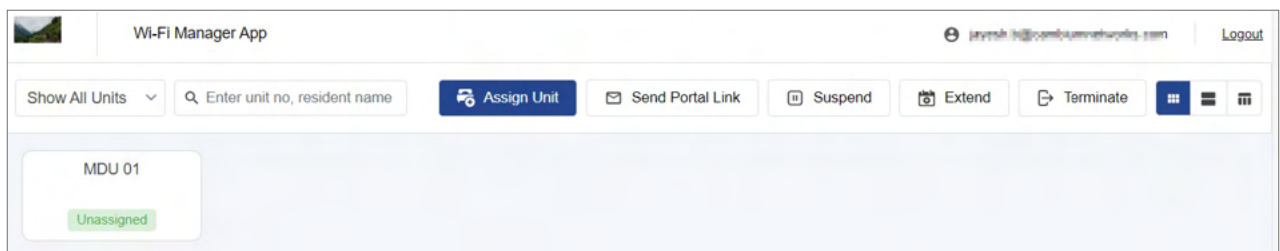


Table 153 *Wi-Fi Manager App Interface*

Options	Description
Show All Units	Provides a drop-down menu with the following options: <ul style="list-style-type: none"> • Show Assigned—Filters the list to display only the assigned units. • Show Unassigned—Filters the list to display only the unassigned units. • Show Suspended—Filters the list to display only the suspended units.
Search	Allows searching for units or residents by entering the unit number or resident name.

Options	Description
Assign Unit	Assigns a unit to a resident.
Send Portal Link	Sends a link to the resident for accessing the portal.
Suspend	Suspends a unit, making it temporarily inactive.
Extend	Extends the duration of a unit's assignment.
Terminate	Terminates a unit's assignment, making it available for reassignment.

Assign Unit

The Assign Unit option allows property managers to allocate specific units to residents. This feature simplifies tenant management and facilitates communication between managers and residents.

To assign a unit, follow these steps:

- Click on **Assign Unit** in the Property Manager app.
- A new window titled **Assign Unit** appears.

The screenshot shows a modal window titled "Assign Unit" with a close button (X) in the top right corner. The form inside includes the following fields and values:

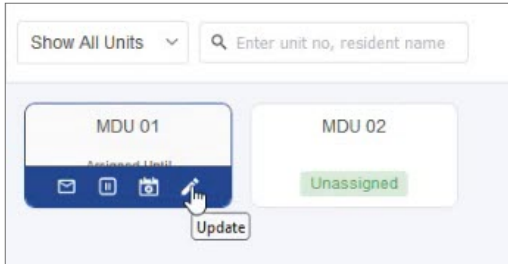
- Unit***: A dropdown menu showing "MDU 01".
- Full Name***: A text input field with a blurred placeholder.
- Email ID***: A text input field with a blurred placeholder.
- Description**: A text input field containing "A's Home".
- Start Date**: A date picker showing "07 / 25 / 2024".
- End Date**: A date picker showing "07 / 26 / 2024".
- Duration**: A label "2 Day(s)" below the date fields.

At the bottom of the window, there are two buttons: "Cancel" and "Assign Unit".

- Select the unit from the **Unit** drop-down menu.
 - Enter the resident's **Full Name**.
 - Enter the resident's **Email ID**.
 - Provide a **Description**.
 - Set the **Start Date** for the assignment.
 - Set the **End Date** for the assignment.
- Note:** Minimum duration is one day.
- Review the **Duration** displayed in days.
 - Click **Assign Unit** to finalize the assignment.
 - A message confirms **Assign Unit action completed successfully**.



- l. After updating, if the property manager wants to change any of these parameters, they can do so by clicking the cursor below the unit as shown.



- m. A new window titled **Update** appears.

- n. The property manager can update any details and then click **Update**.

Send Portal Link

This feature allows you to send the portal link associated with a specific unit to residents or other designated recipients.

To send a portal link, complete the following steps:

- Click on the **Send Portal Link** in the Property Manager app.
- A new window titled **Send Portal Link** appears.

Send Portal Link

Unit*

MDU 01

- c. Select the unit number or name from the **Unit** drop-down.
- d. A new window titled **Send Portal Link** appears.

Send Portal Link

Unit*
MDU 01

Full Name*

Email ID*

Start Date: 07 / 25 / 2024

End Date: 07 / 25 / 2024

Cancel Send Portal Link

- e. Click **Send Portal Link** to send the portal link.
- f. A message confirms **Send Portal Link action completed successfully**.

Send Portal Link action completed successfully!

- g. An email is sent to the resident to log in to the resident portal.

Suspend

The Suspend option allows you to temporarily suspend a unit in the Property Manager app.

To suspend a unit, complete the following steps:

- a. Click on **Suspend** in the Property Manager app.
- b. A new window titled **Suspend** appears.

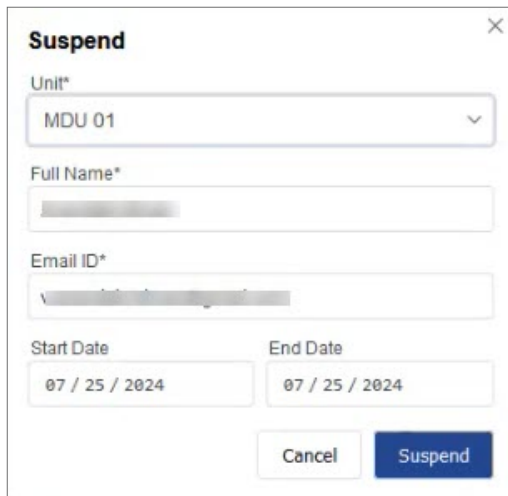
Suspend

Unit*

MDU 01

- c. Select the unit number or name from the **Unit** drop-down.

- d. A new window titled **Suspend** appears.



The **Suspend** window contains the following fields and controls:

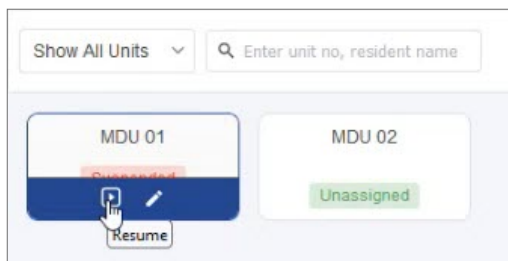
- Unit***: A dropdown menu with "MDU 01" selected.
- Full Name***: A text input field with a blurred placeholder.
- Email ID***: A text input field with a blurred placeholder.
- Start Date**: A date input field showing "07 / 25 / 2024".
- End Date**: A date input field showing "07 / 25 / 2024".
- Buttons**: "Cancel" and "Suspend" buttons at the bottom right.

- e. Click **Suspend** to confirm.

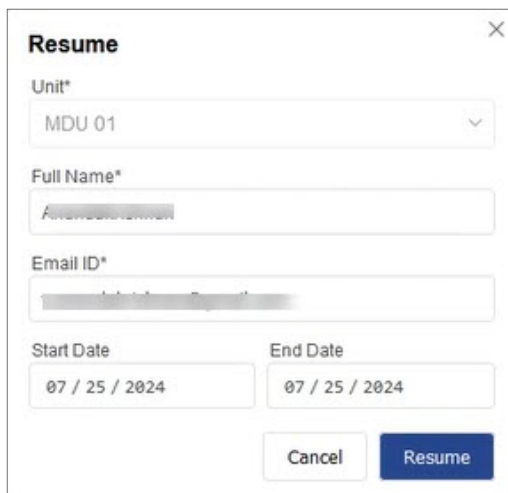
- f. A message confirms **Suspend action completed successfully**.



- g. After a unit is suspended, the property owner can resume the unit by clicking the cursor below the unit as shown below.



- h. A new window titled **Resume** appears.

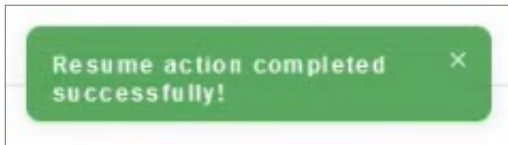


The **Resume** window contains the following fields and controls:

- Unit***: A dropdown menu with "MDU 01" selected.
- Full Name***: A text input field with a blurred placeholder.
- Email ID***: A text input field with a blurred placeholder.
- Start Date**: A date input field showing "07 / 25 / 2024".
- End Date**: A date input field showing "07 / 25 / 2024".
- Buttons**: "Cancel" and "Resume" buttons at the bottom right.

- i. Click **Resume** to confirm.

- j. A message confirms **Resume action completed successfully**.



Extend

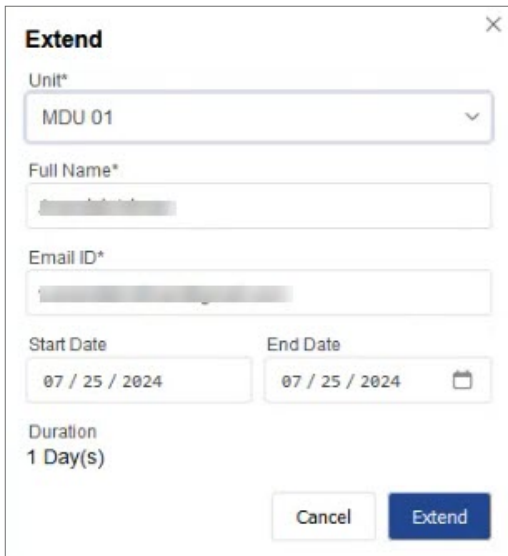
Extend allows you to prolong the duration of a unit's assignment period within the Property Manager app.

To extend a unit, complete the following steps:

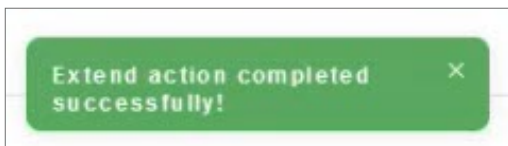
- a. Click on **Extend** in the Property Manager app.
- b. A new window titled **Extend** appears.



- c. Select the unit number or name from the **Unit** drop-down.
- d. A new window titled **Extend** appears.



- e. Set the **End Date** for the assignment.
- f. Review the **Duration** displayed in days.
- g. Click **Extend** to confirm.
- h. A message confirms **Extend action completed successfully**.



Terminate

Terminate allows you to end the assignment of a unit within the Property Manager app.

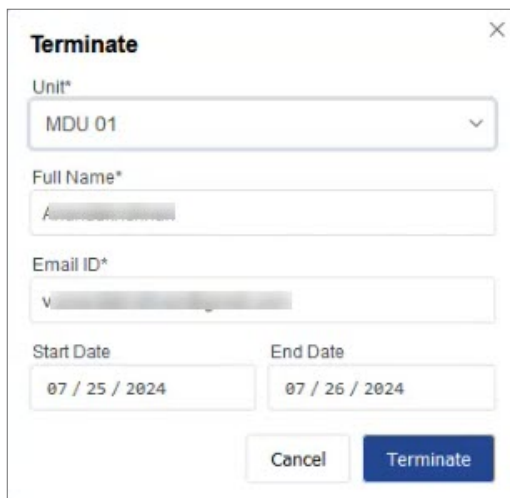
To terminate a unit, complete the following steps:

- a. Click on **Terminate** in the Property Manager app.
- b. A new window titled **Terminate** appears.



The screenshot shows a window titled "Terminate" with a close button (X) in the top right corner. Below the title is a label "Unit*" followed by a dropdown menu. The dropdown menu is open, showing a search bar with a magnifying glass icon and a list of items. The first item, "MDU 01", is highlighted, and a mouse cursor is pointing at it.

- c. Select the unit number or name from the **Unit** drop-down.
- d. A new window titled **Terminate** appears.



The screenshot shows a window titled "Terminate" with a close button (X) in the top right corner. Below the title is a label "Unit*" followed by a dropdown menu showing "MDU 01". Below this is a label "Full Name*" followed by a text input field. Below that is a label "Email ID*" followed by a text input field. Below these are two date fields: "Start Date" with the value "07 / 25 / 2024" and "End Date" with the value "07 / 26 / 2024". At the bottom are two buttons: "Cancel" and "Terminate".

- e. Click **Terminate** to confirm.
- f. A message confirms **Terminate action completed successfully**.

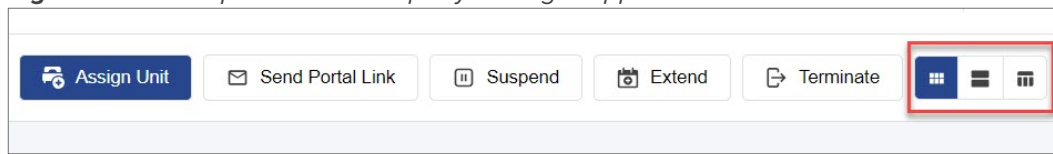


The screenshot shows a green message box with a close button (X) in the top right corner. The text inside the box reads "Terminate action completed successfully!".

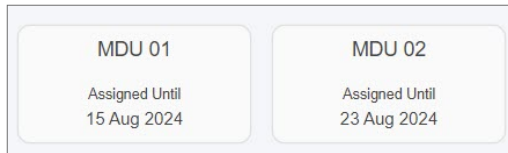
View options in the Property Manager App

In the Property Manager app, there are three different view options to manage units efficiently. These view options can be accessed using icons located at the top right corner of the Property Manager app interface as shown in [Figure 551](#).

Figure 551 View options in the Property Manager App

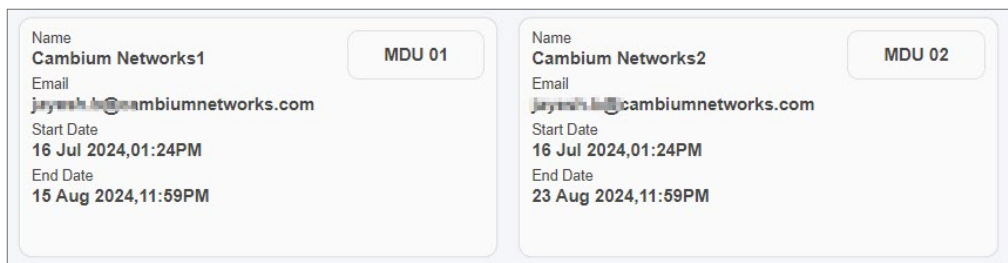


1. **Thumbnail View**—This view displays units as thumbnails or small images, providing a visual representation of each unit.



Beneath each thumbnail, you can access options such as Send Portal Link, Suspend, Extend, and Update by hovering your cursor over the unit.

2. **Title View**—Units are listed with their names or titles, showing unit name, email ID, start date, and end date for quick reference.



3. **Table View**—Table View presents units in a structured table format with columns for Unit, Status, Name, Email, Start Date, and End Date, allowing for detailed management and organization of unit information.

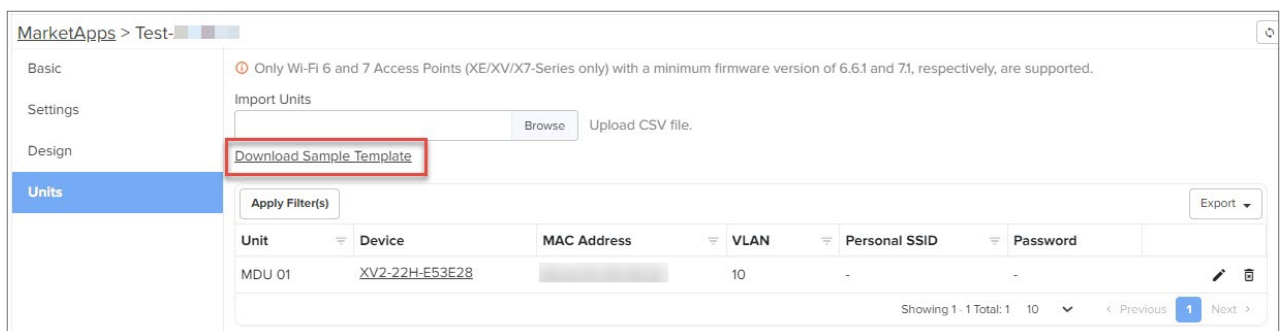
Unit	Status	Name	Email	Start Date	End Date	
MDU 01	● Assigned	Cambium Networks1	jayash.k@cambiumnetworks.com	16 Jul 2024,01:24PM	15 Aug 2024,11:59PM	✉ ⏸ 📅 ↗ ✎
MDU 02	● Assigned	Cambium Networks2	jayash.k@cambiumnetworks.com	16 Jul 2024,01:24PM	23 Aug 2024,11:59PM	✉ ⏸ 📅 ↗ ✎

Units managed in Self-Service Personal Wi-Fi App

Self-Service Personal Wi-Fi App allows users to configure their personal Wi-Fi networks using cnMaestro.

To set up and manage your personal Wi-Fi network settings, complete the following steps:

1. Navigate to the **Unit** tab and click on the **Download Sample Template** option to get the sample file.

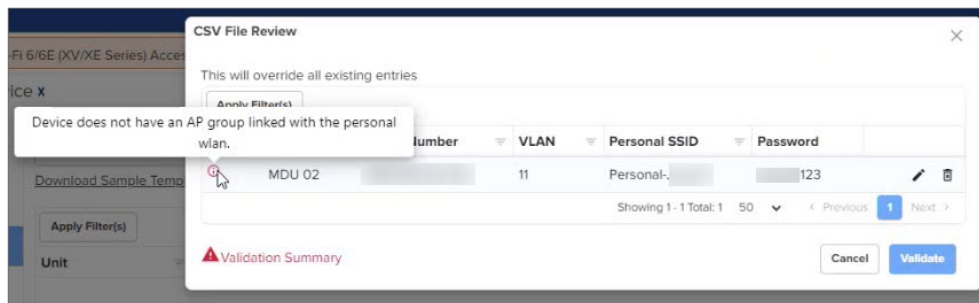


2. An example of the sample template and parameters is shown below:

Unit	Serial Number	MAC Address	VLAN	Personal SSID	Password
Unit name	Serial number of device	MAC Address of device	VLAN ID	SSID for the personal Wi-Fi	Password for Wi-Fi
MDU 01	B1000D000000	B1:00:0D:00:00:00	10	SSID 01	Pa\$\$Word123
MDU 02	B1000D000001	B1:00:0D:00:00:01	13	SSID 02	Pa\$\$Word123

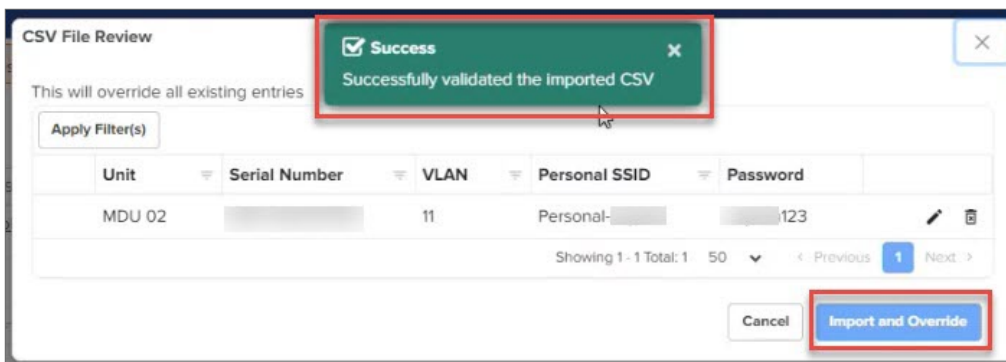
Parameter	Description
Unit	Enter the name or number of the unit (For example, MDU01 and MDU 02 are apartment numbers).
Serial Number	Enter the serial number of the device.
VLAN	Enter the VLAN ID assigned to the unit.
Personal SSID	Enter the SSID for the personal WiFi network.
Password	Enter the password for the Wi-Fi network.

3. After entering the details, save the Excel file with a new name to ensure you have a copy of the filled template and import it to cnMaestro. Note this step is crucial to avoid overwriting the original template.
4. During the import, you might encounter validation error messages. Here are some common error messages and their solutions:
 - a. **Device does not have an AP group linked with the personal wlan**—Ensure each device is only linked to one application at a time. Verify the device has an AP group associated with the personal WLAN before proceeding with the configuration.



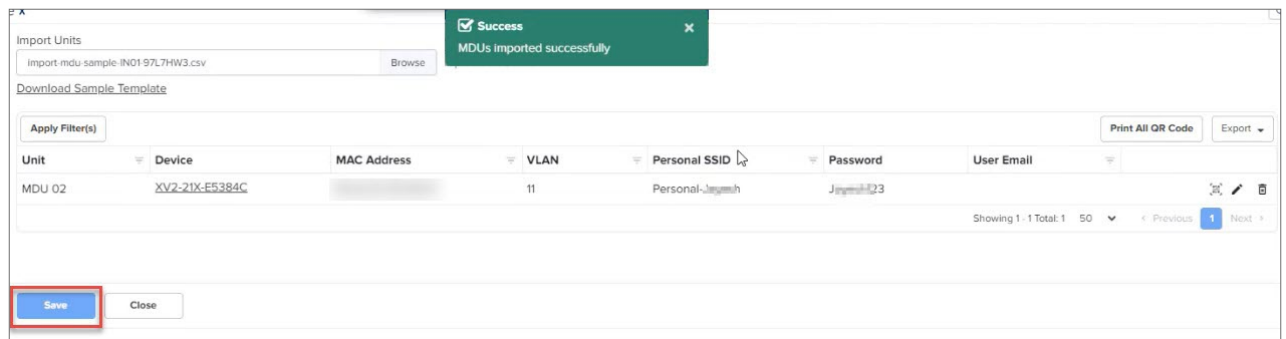
All the error messages are similar to those described in the [Units managed in Managed Wi-Fi](#) sections.

5. Once the file imports correctly, you can see the **Successfully validated the imported CSV** message as shown in the below figure.

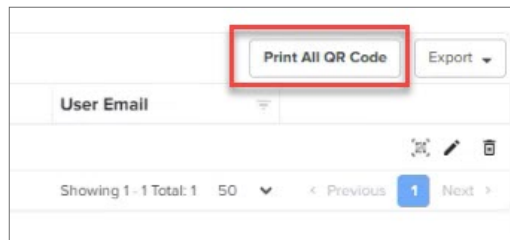


6. Click **Import and Override** to finalize the import process.

7. Once the devices are successfully added, click **Save**.




8. Click the **Print All QR Code** option on the right side to open a QR scan page.



9. Scan the QR code using your mobile device to get a link.



10. Enter your email ID and click **Send me a one time link**.




Welcome to Test--SelfService

Email ID

Send me one time link

You'll receive an email containing a one-time sign-in link. Clicking this link will take you directly to the Wi-Fi Resident App, where you can see and manage your personal Wi-Fi settings.

Tip: Bookmark this page in your browser for easy access later.




Check your inbox.

If the information you entered matches our records, you'll soon receive an email containing a one time sign-in link.

Don't see your email?

Check your spam folder or [resend](#) the link.

11. Open the email and click **Go to the Wi-Fi Manager App**.



Access your account via the one-time link below, which will remain valid for 30 minutes.

Go to Wi-Fi Manager App

Thanks,
Cambium Networks

If you're having trouble with the button above, copy and paste the below link into your web browser.
<https://qa-us-e1.test-easy-apps.cloud.cambiumnetworks.com/mdu-portal/manager/app/62d73e1f2d5a403598001cc1c2c7c762/user/magic-link?sessionId=718f4639-ced6-482f-b29d-a5539665b3b0>

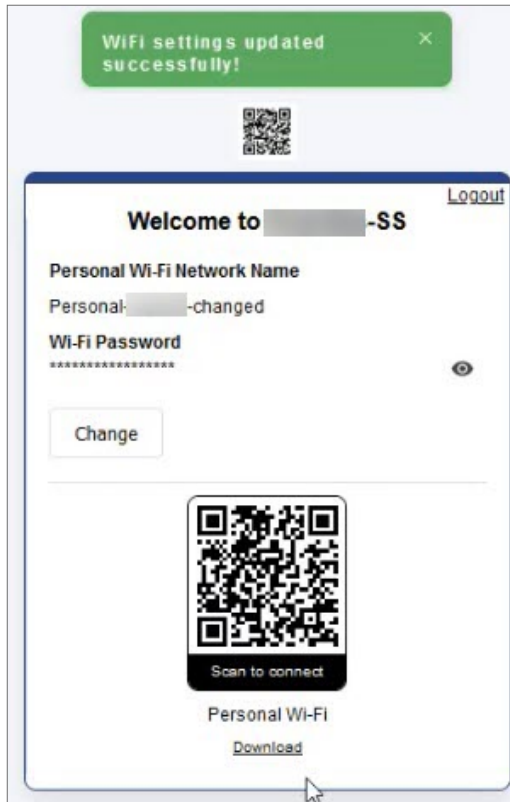
12. You see a page titled **Welcome to APP** and click on **Change**.



13. A new window titled **Change Wi-Fi Settings** appears. Change your Personal Wi-Fi Network Name and Wi-Fi password in the respective fields.



14. Click **Update**.
15. You receive a message says **Wi-Fi settings updated successfully**.



16. Scan the QR code to verify that your Personal Wi-Fi Network Name and Wi-Fi password have been updated.

RADIUS Proxy X



Note

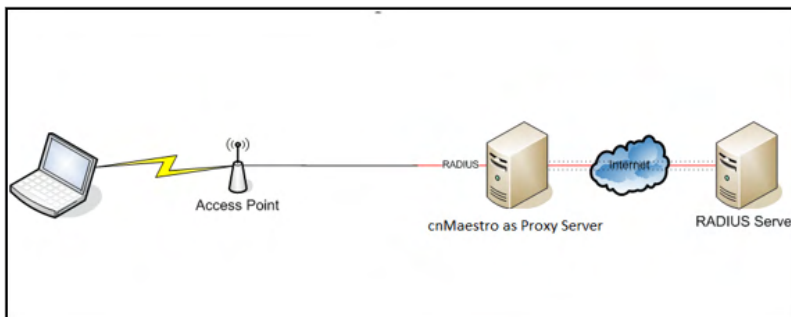
- **RADIUS Proxy** is not supported in cnMaestro Cloud.
- It is available only as a cnMaestro X feature.

Overview

cnMaestro can act as a proxy server to authenticate **RADIUS** requests for cnPilot Wi-Fi devices. In this scenario, cnMaestro acts as a Network Access Server (NAS) for the RADIUS server.

The Access Point sends RADIUS packets to cnMaestro, and cnMaestro sends them to the RADIUS server. cnMaestro can act as a proxy for either authentication or accounting messages, as show in [Figure 552](#).

Figure 552 RADIUS Proxy on cnMaestro On-Premises



Minimum version requirements are as follows:

- Minimum cnPilot AP release version required: 3.3.

RADIUS Proxy Configuration

To configure RADIUS Proxy on cnMaestro, perform the following:

1. Navigate to **Shared Settings > AP Groups and WLANs** page.
2. Select **Enterprise WLAN** to edit, and then select **AAA Servers**.
3. Under AAA servers, select **Proxy RADIUS through cnMaestro** check box.
4. Configure **Authentication Server** details.
5. Configure **Accounting Server** details.
6. Configure **NAS-Identifier**.



Note

Include **NAS-Identifier** attribute to use the RADIUS request packets and default the system name.

7. Push the configuration from cnMaestro to AP.

Figure 553 RADIUS Proxy Configuration

WLANs > Default Enterprise

Configuration APs

WLAN

AAA Servers

Guest Access

Access Control

Passpoint

ePSK

Warning: AAA Servers are configured separately for each WLAN.

☒ Proxy RADIUS through cnMaestro X

Proxy RADIUS packets through cnMaestro (on-premises) instead of directly to the RADIUS server from the AP

Authentication Server

1. Host Secret Port* Realm

2. Host Secret Port* Realm

3. Host Secret Port* Realm

Timeout 3 Timeout in seconds for each request attempt (1-30)

Attempts 1 Number of attempts before giving up (1-3)

Accounting Server

Advanced Settings

Save

Citizens Broadband Radio Service (CBRS)

This chapter details cnMaestro support for the Citizens Broadband Radio Service (CBRS) subscription which is required to manage CBRS-compliant devices in the 3.6 GHz band (3550 MHz to 3700 MHz).

This topic describes the following sections:

- [Enabling CBRS in Cloud](#)
- [Management Tool](#)
- [Domain Proxy View](#)
- [Actions for Existing CBRS On-Premises Users](#)

Enabling CBRS in Cloud

1. Login to a cnMaestro Cloud NMS account or Cloud Anchor account (if hosting on an On-Premises instance).
2. Navigate to **Network Services > CBRS** page.
3. Select the preferred SAS vendor from the **Spectrum Access System (SAS)** drop-down list.

Figure 554 *Network Services > CBRS > Account tab*

The screenshot shows the 'Network Services > CBRS' page. It contains a heading 'Enable Citizens Broadband Radio Service subscription for the CBRS-compliant devices in 3.6 GHz band (3550 MHz to 3700 MHz). [Learn more](#)'. Below this is a dropdown menu for 'Spectrum Access System (SAS)' with the text 'Please select a SAS vendor'. There are two checkboxes: 'I accept the [CAMBIUM NETWORKS, LTD. "CBRS" TERMS OF SERVICE](#)' and 'I accept the [CBRS Service payment terms](#)'. At the bottom is an 'Enable' button.

4. Read both the terms and conditions, and accept them by selecting the checkboxes.
5. Click **Enable**.
6. In the **Billing Information** window configure the following details:

The screenshot shows the 'CBRS Account' form. It starts with a message: 'We require a Business Contact and a Technical Contact for your account. [Learn more](#)'. There are three sections: 'Business Contact', 'Technical Contact', and 'SAS Portal Contact'. Each section has fields for First Name, Last Name, Email, Phone, Street Address, City, Zip Code/Postal Code, State, and Country. The 'SAS Portal Contact' section also has radio buttons for 'Business Contact', 'Technical Contact', and 'Other', and an 'Email (if not Business Contact or Technical Contact)' field. At the bottom are 'Save' and 'Cancel' buttons.

- **Business Contact**

- First Name
- Last Name
- Email

- Phone
- Street Address
- Zip Code
- Country
- State

- **Technical Contact**

Enable **Same as Business Contact** or enter a separate Technical Contact.

- First Name
- Last Name
- Email

- **SAS Portal Contact**

Cambium Networks creates the SAS portal account on behalf of the operator.

7. Click **Save**.

The CBRS account is enabled.

After you save the CBRS account, you must complete the following steps:


1. The **Account** page displays the following information and configurable parameters:

- Token
- Status
- Total Devices
- SAS
- Contact Details
- Payment Details

Services > CBRS


Account Management Tool Domain Proxy View

Please contact [Cambium Support](#) to disable CBRS operations or to change SAS Vendor. [Learn more](#)

Token 

Status

- ✓ Account Created
- ✓ Payment Method Verified
- ✓ SAS-ID Allocated
- ✓ Account Enabled
- Effective Mar 19 2020 15:02:02 (110d 2h 0m)

Total Devices  [Usage History](#)

1 APs, 1 SIMs

Spectrum Access System (SAS)

Federated Wireless (Developer-ICD)

Contact Details

To make changes to the contact details, overwrite the existing entry and click "Update". [Learn more](#)

Business Contact

First Name

Last Name

Email

Phone

9876543

Street Address

rttyulo

City

BANGALORE

Zip Code/Postal Code

987654

State

..hantband

Country

India

Technical Contact

First Name

Last Name

Kar

Email

SAS Portal Contact

Cambium will set up a SAS portal account on your behalf. Please indicate whether you want us to use your Business Contact or Technical Contact for this purpose. Note that Google requires a Gmail address for registration.

☒ Business Contact ☐ Technical Contact ☐ Other

Email (if not Business Contact or Technical Contact)

Options

Payment Details

To update your payment method, make a selection under "Add Payment Method" and enter the new payment method details, the click "Submit".

Credit Card

XXXXXXXXXXXX1234 12/15-12/20

Add Payment Method



☐ Add Credit Card Details ☐ Add ACH Payment Details

a. **Token:**

Token used for authenticated communication with SAS through Cambium Domain Proxy. It gets generated automatically once CBRS is enabled for the Cloud account.

b. **Status:**

Displays the account status.

Pending Status	Success Status
<p>Status</p> <ul style="list-style-type: none"> ✓ Account Created ✗ Payment Method Verification Pending ✗ SAS-ID Allocation Pending <p>● Effective Jul 07 2020 16:54:10 (<1m)</p> <p>Total Devices  Usage History</p> <p>0 APs, 0 SIMs</p>	<p>Status</p> <ul style="list-style-type: none"> ✓ Account Created ✓ Payment Method Verified ✓ SAS-ID Allocated ✓ Account Enabled ● Effective Mar 19 2020 15:02:02 (110d 2h 0m) <p>Total Devices  Usage History</p> <p>3 APs, 68 SIMs</p>

- Account Creation:** Displays as **Account Created** once the account is enabled. Refer to **Step f** for entering contact information and enabling account.
- Payment Method:** Displays as **Verified** once the Payment Details are approved. Refer to **Step g** [Payment Details](#).
- SAS ID:** Once the payment details are verified, the SAS ID is allocated automatically.



Note

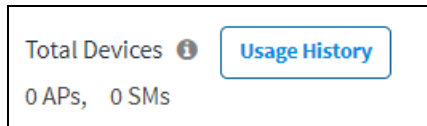
When the SAS ID allocation is pending or unavailable in the server,

even after the payment details are configured and verified,
It may take up to one day for the SAS ID to be allocated.

iv. **Effective:**

- **Grey:** indicates the **Pending Status**.
- **Green:** indicates **Success Status**.
- **Red:** indicates the account has been **Deactivated**.

- c. **Total Devices:** Displays the count of **Total Devices** registered with the SAS using the **Token ID**. **Usage History** provides the list of devices registered with **Month** and **Year**.



Note

Initially the device counts will be 0 APs and 0 SMs.

- d. **SAS:** Displays the SAS vendor preferred by the operator.



Note

Contact Cambium support to disable CBRS operation or to change SAS Vendor.

- e. **SAS:** An operator needs to select which SAS vendor they prefer.

f. **Contact Details:**

For new CBRS account migrations, this information would have already been entered in [Citizens Broadband Radio Service \(CBRS\)](#). Review and update if necessary, else refer to [Payment Details](#).

Cambium Networks selectively communicates with both the **Business Contact** and the **Technical Contact** with changes of interest: such as SAS administrator updates, CBRS initiative changes from the CBRS Alliance and WinnForum, and announcements of new Cambium Network CBRS features and options.

Business Contact

Cambium Networks communicates with the **Business Contact** for all commercial aspects of the CBRS Service such as invoicing, payment, change in terms, change in pricing, and other details. This page requires:

- **First Name**
- **Last Name**
- **Email**
- **Phone**
- **Street Address**
- **City**
- **Zip code/Postal Code**
- **State**
- **Country**

Technical Contact

Cambium Networks communicate with the **Technical Contact**: such as software updates, release notes, learning guides, technical issues, etc.

- **First Name**
- **Last Name**
- **Email**

SAS Portal Contact

Cambium Networks sets up the SAS portal account on behalf of the operator. Please select whether to use the **Business Contact**, **Technical Contact**, or **Other**.



Note

Google requires a Gmail address for registration.

- Click **Update**.



Note

Clicking **Update** on the **Account Page** overwrites the current entries.

g. Payment Details

Select one of the payment methods below:

- [Add Credit Card Details](#)
- [Add ACH Payment Method](#)

Payment Details

To update your payment method, make a selection under "Add Payment Method" and enter the new payment method details, the click "Submit".

Credit Card

*****1111 (expiration 1/2023)

Add Payment Method

☒ Add Credit Card Details
 ☐ Add ACH Payment Details

Add Credit Card Details

Enter the following and click **Submit**:

- 16 digit Credit **Card Number**.
- **Expiration Date** and **Year** on the card.
- **CVV** and **Cardholder Name**.

Payment Details

To update your payment method, make a selection under "Add Payment Method" and enter the new payment method details, the click "Submit".

Credit Card

*****1111 (expiration 1/2023)

Add Payment Method

☒ Add Credit Card Details
 ☐ Add ACH Payment Details

Please Fill in Your Credit Card Details

Card Type

Card Number

Expiration Date

- Select One

/

- Select One

CVV

Cardholder Name

Required Field

submit

Add ACH Payment Method

Enter the following details and click **Submit**:

- **ABA/Routing Number**.
- **Bank Account Number**.
 - Select one of the following for **Account Type**:
 - Checking
 - Saving
 - Business Checking

- **Bank Name and Account Holder Name.**

☐ Payment Details

To update your payment method, make a selection under "Add Payment Method" and enter the new payment method details, then click "Submit".

Credit Card

*****1111 (expiration 1/2023)

Add Payment Method

☐ Add Credit Card Details
 ☒ Add ACH Payment Details

Please Enter Your Payment Details

ABA/Routing Number

Bank Account Number

Account Type

Bank Name

Account Holder Name

☐ Required Field

Management Tool

The Management Tool allows one to register CBRS devices to the SAS provider before physically connecting CBRS-complaint devices to the network. The following Cambium CBRS-compliant devices operate in 3.6 GHz band frequency, ranging from 3550 to 3700 MHz:



Note

The CBRS Multi-Grant feature was first supported in cnMaestro 3.0.2 and PMP 20.2.

- PMP 450b 3 GHz
- PMP 450m AP 3 GHz
- PMP 450i AP and SM 3 GHz
- PMP 450 AP and SM 3.6 GHz
- PTP 450i BHM and BSHS 3 GHz
- PTP 450 BHM and BHS 3.6 GHz
- LTE 3 GHz cnRanger 201 SM
- LTE 3 GHz cnRanger 210 RRH

The CBRS procedure can be performed by an authorized CPI (Certified Professional Installer). CPIs are required to enter necessary credentials to update the CBRS parameters.

A CBRS sector view is shown below:

Network Services > CBRS

Account
 Management Tool
 Domain Proxy View

SAS Admin Tool helps CPI (Certified Professional Installer) to manage CBRS-compliant devices prior to installation. CPI info is never stored either in the client side or server side. After adding a new sector or AP, click on that newly added AP to allow you to start the tool.

MAC Address	Device Name	Device Type	Health	User ID	Tool Frequency (MHz)	Operating Frequency (MHz)	Grant Type	Sector ID	Spectrum Reuse ID	Include User ID
88		PMP 450 Connectorized	Offline		3570 - 3590	N/A	Multigrant		N/A	N/A
3d		PMP 450 Connectorized	Offline		3560 - 3580	N/A	Multigrant		N/A	N/A
100:80		PMP 450 Connectorized	Offline		3570 - 3590	N/A	Multigrant		N/A	N/A

Showing 1 - 3 Total: 3

Export

The **Export** button allows one to export multiple device reports in the **CSV** format.

Network Services > CBRS

Account **Management Tool** Domain Proxy View

SAS Admin Tool helps CPI (Certified Professional Installer) to manage CBRS-compliant devices prior to installation. CPI info is never stored either in the client side or server side. After adding a new sector or AP, click on that newly added AP to allow you to start the tool.

MAC Address

Add AP/BHM/RRH **Import Sector** **Relinquish Grant** **Export**

Device Name	Device Type	Health	User ID	Tool Frequency (MHz)	Operating Frequency (MHz)	Grant Type	Sector ID	Spectrum Reuse ID	Include User ID
<input type="checkbox"/> 3d	PMP 450 Connectorized	Offline		3570 - 3590	N/A	Multigrant		N/A	N/A
<input type="checkbox"/> 3bd	PMP 450 Connectorized	Offline		3560 - 3580	N/A	Multigrant		N/A	N/A
<input type="checkbox"/> 3ool3a2	PMP 450 Connectorized	Offline		3570 - 3590	N/A	Multigrant		N/A	N/A

Showing 1 - 3 Total: 3 **1**

Relinquish Grant

The Relinquish Grant button relinquishes all grants of selected sector and places devices in the Registered state. The device will start the Multi-Grant procedure if the Multi-Grant feature is enabled on the device.

Network Services > CBRS

Account **Management Tool** Domain Proxy View

SAS Admin Tool helps CPI (Certified Professional Installer) to manage CBRS-compliant devices prior to installation. CPI info is never stored either in the client side or server side. After adding a new sector or AP, click on that newly added AP to allow you to start the tool.

MAC Address

Add AP/BHM/RRH **Import Sector** **Relinquish Grant** **Export**

Device Name	Device Type	Health	User ID	Tool Frequency (MHz)	Operating Frequency (MHz)	Grant Type	Sector ID	Spectrum Reuse ID	Include User ID
<input checked="" type="checkbox"/> 3d	PMP 450 Connectorized	Offline	SITMGABLAZ9	3570 - 3590	N/A	Multigrant	34-89-23-09-12-27	N/A	N/A
<input type="checkbox"/> 3bd	PMP 450 Connectorized	Offline	SITMGABLAZ9	3560 - 3580	N/A	Multigrant	12-90-34-90-34-67	N/A	N/A
<input type="checkbox"/> 3ool3a2	PMP 450 Connectorized	Offline	SITMGABLAZ9	3570 - 3590	N/A	Multigrant	12-45-67-34-78-21	N/A	N/A

Showing 1 - 3 Total: 3 **1**



Note

- Relinquish Grant can be performed only for the Config_Synced devices running in Single Grant.
- PMP devices must be upgraded to release 20.2, which supports the Multi-Grant feature.

Relinquish grant creates a job in **Action** page, when relinquish of sector is initiated from **Management Tool** page.

Administration > Jobs

Configuration Update Software Update Reports **Actions**

Managed Account: **All Accounts**

ID	Type	Managed Account	Source	Occurrence	Created by	Created on	Completed on	Status
<input type="checkbox"/> 19	Relinquish	Base Infrastructure	System	Now		Nov 07, 2022 11:44	Nov 07, 2022 11:44	Completed
<input type="checkbox"/> 18	Reboot	Base Infrastructure	Ext-EZE-101	Schedule		Nov 04, 2022 15:43	Nov 04, 2022 15:54	Completed
<input type="checkbox"/> 17	Reboot	Base Infrastructure	Ext-EZE-101	Schedule		Nov 04, 2022 11:48	Nov 04, 2022 16:53	Completed
<input type="checkbox"/> 16	Reboot	Base Infrastructure	Ext-EZE-102	Schedule		Nov 03, 2022 19:10	Nov 04, 2022 10:15	Completed
<input type="checkbox"/> 15	Reboot	Base Infrastructure	Onboard-79	Schedule		Nov 03, 2022 18:27	Nov 04, 2022 09:32	Completed
<input type="checkbox"/> 14	Reboot	Base Infrastructure	rseries_site	Schedule		Nov 03, 2022 15:52	Nov 04, 2022 12:57	Completed
<input type="checkbox"/> 13	Reboot	Base Infrastructure	crmatix_site	Schedule		Nov 03, 2022 15:52	Nov 04, 2022 12:56	Completed
<input type="checkbox"/> 12	Reboot	All Accounts	System	Schedule		Nov 03, 2022 11:44	Nov 04, 2022 11:49	Completed
<input type="checkbox"/> 11	Reboot	All Accounts	System	Now		Nov 03, 2022 11:38	Nov 03, 2022 11:38	Completed
<input type="checkbox"/> 10	Reboot	Base Infrastructure	System	Schedule		Oct 29, 2022 17:28	Oct 29, 2022 17:33	Completed

Showing 1-10 Total: 18 **1**

Creating a Management Tool Sector

A sector can be created by two ways:

- Add AP/BHM/RRH: Add all parameters manually of an AP/BHM/RRH.
- Import Sector: Upload a file with details from all sector devices.

Add AP/BHM

- Navigate to **Services > CBRS > Management Tools** and click **Add AP/BHM/RRH**.
- Enter all parameters under the following categories when the user selects the **Mode** as **AP/BHM**:

- **Common parameters:** Device Name, Mode, Device Type, MAC Address, and MSN.
- **Location related parameters:** Latitude, Longitude, Height, and Height Type, Horizontal Accuracy, and Vertical Accuracy.
- **Antenna related Parameters:** External Antenna Gain, Beamwidth, Azimuth, and Down Tilt.
- **Co-Existence related parameters:** Sector ID, Spectrum Reuse ID, and Include User ID.



Note

Include User ID parameter is applicable only for PMP devices, when SAS is **Federated Wireless**.
Select **Yes** or **No** to Include the user ID.

- **Add CPI Certificate:** Certificate File, File Password, CPIR Name.

3. Click **Add** to add a sector.

Add RRH

1. Navigate to **Services > CBRS > Management Tools** and click **Add AP/BH/RRH**.
2. Enter all parameters under the following categories when the user selects the **Mode** as **RRH**:
 - **Common Parameters:** Device Name, Mode, Device Type, MAC Address, and MSN.
 - **Location Related Parameters:** Latitude, Longitude, Height and Height Type, Horizontal Accuracy, and Vertical Accuracy.
 - **Antenna Related Parameters:** External Antenna Gain, Beamwidth, Azimuth, and Down Tilt.
 - **ECGI Related Parameters:** PLMN ID, ECI (eNode ID + PCI), and ECGI.

- **Co-Existence Related Parameters:** Sector ID and Spectrum Reuse ID.
- **Add CPI Certificate:** Certificate File, File Password, CPIR Name.

3. Click **Add** to add a sector.



Note

Refer to [CBRS Device Parameters](#) for additional details.

Import Management Tool Sector

To import a sector:

1. Navigate to **Services > CBRS > Management Tool** and click **Import Sector** button.

1. Click **Download Template** if user does not have an Import Sector template. Users can download two different template formats:
 - a. PMP: Excel or ODS
 - b. LTE: Excel or ODS
2. Click **Import Excel** to select **Import Sector** template file. File must be Microsoft Excel format (.xlsx) or OpenDocument Spreadsheet (ods) format.
3. Enter CPI credentials:
 - a. Upload CPI Certificate File by clicking **Import Certificate**.
 - b. Enter CPI File Password.
 - c. Enter CPI Registered Name.
4. Enter the **Sector ID**.
5. Select **Spectrum Reuse ID** from the drop-down.
6. Select **Include User ID**.

Selecting **Yes** in the **Include User ID** parameter prefixes the **User ID** to the **Sector ID** and **Spectrum Reuse ID** in the registration message of the SAS.



Note

- **Include User ID** is applicable only for PMP devices, when SAS is selected as **Federated Wireless**.
- See the [CBRS Consolidated Procedures Guide](#) and the [Cambium PMP Release 20.3](#) training slides for more details on when to select **Yes** or **No**.

7. Click **Import**.

Import status is displayed as **Success**, **Info**, and **Invalid**.

8. Details of **Success**, **Info**, and **Invalid** section can be seen by clicking expand (▼) arrow.

Invalid: 1 Device(s) are not valid.	
MAC	Error
0a-00-3e-45-11-e4	Serial Number is invalid

9. If the device is already claimed, it can be onboarded by clicking the onboard link.

Info: 2 MAC(s) already claimed. Please onboard these devices, if not onboarded yet.

Management Tool Sector Statistics

To view Sector Statistics:

1. Navigate to **Services > CBRS > Management Tool**.
2. Click **View Sector Statistics**  under **Status**.

Network Services > CBRS

Account **Management Tool** Domain Proxy View

SAS Admin Tool helps CPI (Certified Professional Installer) to manage CBRS-compliant devices prior to installation.
CPI info is never stored either in the client side or server side.
After adding a new sector or AP, click on that newly added AP to allow you to start the tool.

MAC Address Search

<input type="checkbox"/> Device Name	Device Type	Health	User ID	Tool Frequency (MHz)	Operating Frequency...	Grant Type	Sector ID	Spectrum Reuse ID	Include User ID	
<input type="checkbox"/> 224-AP	PMP 450b High Gain	Online	SITMGABL...	3565 - 3595	3565 - 3595	Multigrant		N/A	N/A	
<input type="checkbox"/> dummy_sector	PMP 450 Connectorized	Offline	SITMGABL...	3550 - 3570	N/A	Multigrant		N/A	N/A	

Showing 1 - 2 Total: 2

3. **Sector Statistics** window pops up.

224-AP Sector Statistics	
Device Information	
Registered	2
Grant Information	
Granted	4
Authorized	4



Note

Refer to the [CBRS State Diagram](#) for additional details.

Search Management Tool Sector

To search for a sector:

1. Navigate to **Services > CBRS > Management Tool**.
2. Select **CBSD** or **MAC**.
 - For **CBSD**: Search by CBSD ID.
 - For **MAC**: Search by MAC Address.
3. Enter text in search box to display filtered records.

MAC Address Search

CBSD ☐ Device Type ☐ Health ☐

MAC Address ☐ PMP 450b High Gain ☐

Device Name ☐



Note

- If an AP device is entered into Search, it displays both AP devices and the related SM

selector()

☐ **General**

☒ Device Name

☒ Device Type

☒ Health

☐ CBSID ID

☐ Horizontal Accuracy

☐ ECGI (E-UTRAN Cell Global Identifier)

☒ MAC Address

☒ Mode

☒ Serial Number

☒ Sync Expiry Time

☐ Vertical Accuracy

☒ Grant Status

☒ Sync State

☐ **Location**

☒ Latitude

☒ Height

☒ Longitude

☐ Height Type

☐ **Antenna**

☐ Integrated Antenna Gain (dBi)

☐ Azimuth (degrees)

☐ Max EIRP (dBm)

☐ Granted EIRP (dBm)

☐ External Antenna Gain (dBi)

☐ Beamwidth (degree)

☐ Down Tilt (degrees)

☐ Requested EIRP (dBm)

☐ SAS Recommended EIRP (dBm)

- User can use following button to control the CBRS procedure:

Management Tool > Mibank-5G

Tool Frequency (MHz): 3550 - 3580
Operating Frequency (MHz): N/A

Add SM/BHS

Relinquish Grant

Delete

Deregister







Spectrum Inquiry

Re-init


Start

Export

Import

Device Name	MAC Address	Device Type	Mode	Health	Serial Number	Latitude	Longitude	Sync Expiry Time	Height	Grant Status	Sync State	Actions
<input checked="" type="checkbox"/> Mibank-5G		PMP 450i Connectorized	AP	Offline		25.7678	-80.1919	N/A	40	● Deregistered	Not Synced	 
<input type="checkbox"/> Mibank-3G		PMP 450i Connectorized	SM	Offline		45.215	-96.6339	N/A	30	● Deregistered	Not Synced	 
<input type="checkbox"/> Mibank-5G		PMP 450i Connectorized	SM	Offline		45.215	-96.6339	N/A	20	● Deregistered	Not Synced	 

Showing 1 - 3 Total: 3 10 < Previous 1 Next >

- **Start** and **Stop**: manage to start and stop CBRS procedure of a sector.
 - **Reinitialize**: restarts the CBRS procedure and reinitializes the devices.
 - **Deregister**: deregisters the device (single or multiple).
 - **Spectrum Inquiry**: checks the availability of frequencies.
 - **Delete**: deletes the device (single or multiple).
 - **Unblock**: clears the de-registered state on an LTE, allowing a registration or reregistration request.
 - **Export**: exports the sector data in .xlsx format.
 - **Import**: imports the SM in the sector.
 - **Relinquish Grant**: relinquishes grants generated in Wide-Grant mode.
- Once the sector is authorized (AUTHORIZED state),  button transfers grant details from the Management Tool to real devices.

Add SM or BHS

1. Navigate to **Services > CBRS > Management Tool** > select a sector.
2. Click **Add SM** or **BHS** to add SM in a sector.

3. Enter all parameters under following categories:

- **Common parameters:** Device Name, Device Type, MAC Address, and MSN.
- **Location related parameters:** Latitude, Longitude, Height and Height Type, Horizontal Accuracy, and Vertical Accuracy.
- **Antenna related parameters:** Integrated Antenna Gain, Beam width, Azimuth, and Down Tilt.
- **Add CPI Certificate:** Certificate File, File Password, and CPIR Name.

4. Click **Add** to add an SM.

Import SMs

1. Navigate to **Services > CBRS > Management Tool** and select a sector.
2. Click **Import** button to import SMs into a sector.
3. Enable the **ReImport Devices** to overwrite the previous imported data and deregister all existing devices.

4. Click **Download Template** if user does not have Import Sector template. Users can download two different template formats:
 - PMP: Excel or ODS
 - LTE: Excel or ODS
5. Click **Import Excel** to select Import Sector template file. File must be Microsoft Excel format (.xlsx) or Open Document Spreadsheet (ods) formats.
6. Enter the following CPI credentials:
 - Upload CPI Certificate File by clicking **Import Certificate** button.
 - Enter CPI File Password.
 - Enter CPI Registered Name.

7. Click **Import**.

Import status will be shown under **Success**, **Info**, and **Invalid** sections.

8. Details of **Success**, **Info** and **Invalid** can be seen by clicking ▼.

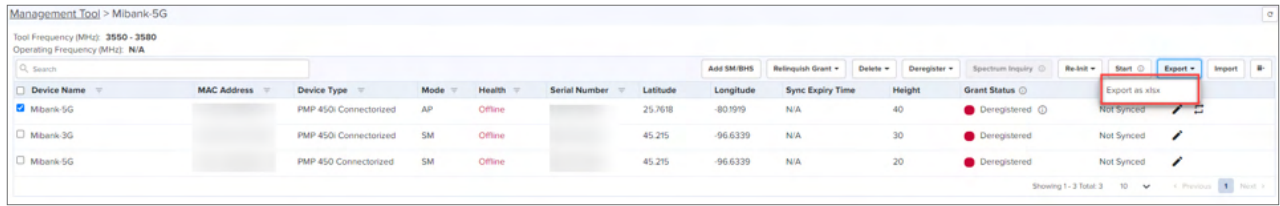
MAC	Error
0a-00-3e-45-11-e4	Serial Number is invalid

9. If the devices is already claimed, it can be onboarded by clicking the **onboard** link.

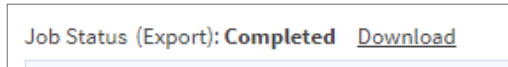
10. Once the user clicks **Import**, a job is scheduled.

Export Sector

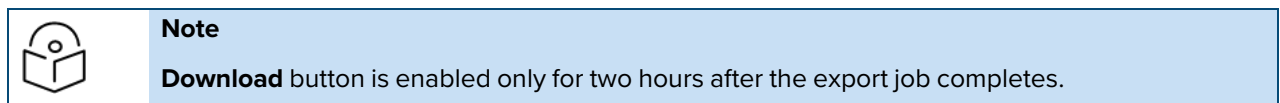
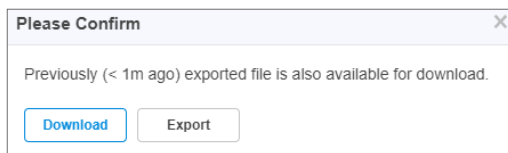
1. Navigate to **Services > CBRS > Management Tool** and then select a sector.
2. Click **Export** button to export the sector (export as xlsx).



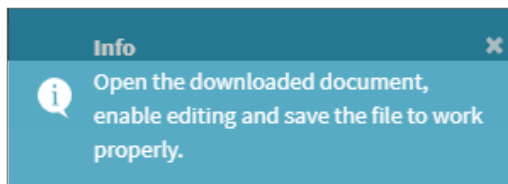
3. Once the user clicks **Export**, a job is scheduled.



4. Once the Job status is Completed, **Download** the Sector xlsx.



5. User can use the .xlsx file for importing back into the sector. To import, save the file as shown in the below figure.



Edit Device

1. Navigate to **Services > CBRS > Management Tool** and select a sector.
2. Click **Stop** button if the CBRS procedure is running.
3. Click **Edit** button to edit device parameters.
4. Enter CPI credentials:
 - Upload CPI Certificate File by clicking **Import Certificate** button.
 - Enter CPI File Password.
 - Enter CPI Registered Name.
5. After editing the device. The device should go to derigestered state.

6. Click **Save**.

Delete Device


1. Navigate to **Services > CBRS > Management Tool** and select a sector.
2. Click **Stop** button if the CBRS procedure is running (the CBRS procedure is running if the START procedure described below has been invoked, and if all devices in AUTHORIZED state).
3. Deleting SM:
 - Select SM to deregister if it is not in UNREGISTERED state (Refer to the [CBRS State Diagram](#)).
4. Once the SM selected click **Delete** and display popup **All** or **Selected**. click **Selected**:
 - **All**: Deletes all registered SM devices.
 - **Selected**: Deletes the selected devices.

Device Name	MAC Address	Device Type	Mode	Health	Serial Number	Latitude	Longitude	S	Alt	Height	Grant Status	Sync State	Actions
<input checked="" type="checkbox"/> Mibank-5G		PMP 450i Connectorized	AP	Offline		25.7618	-80.1919	N	Selected	0	Deregistered	Not Synced	
<input type="checkbox"/> Mibank-3G		PMP 450i Connectorized	SM	Offline		45.215	-96.6339	N/A		30	Deregistered	Not Synced	
<input type="checkbox"/> Mibank-5G		PMP 450i Connectorized	SM	Offline		45.215	-96.6339	N/A		20	Deregistered	Not Synced	

5. Click **Yes** to confirm.

Please Confirm

This action will delete 1 device(s) under current sector. Do you want to continue?

☒  The device will be deregistered from SAS, if it is registered and synced.

Yes No

- Once the user clicks **Yes**, a job will be scheduled.

Job Status (Delete): **Completed** [with device\(s\) failure](#)

- Deleting AP:

All SMs of the sector must be deregistered and deleted before deleting the AP. Refer to the [Deregistration](#) procedure to deregister all SM devices.

- Select the AP of the sector to delete.
- Click **Delete**.






Note

If the procedure is started for the device and it is registered, then, while deleting the device, you must select the **Deregister** checkbox, otherwise the deletion will fail.

Unblock Device


- Navigate to **Services > CBRS > Management Tool** and select a sector.
- If LTE device is **Config Synced**, and if device deregister flag is enabled, unblock removes the deregistration flag on the device.
- Once the device is selected, click **Unblock** and choose **All** or **Selected** from the drop-down.
 - All**: Unblocks all registered devices.
 - Selected**: Unblocks the selected devices.

Device Name	Device Type	Mode	Health ID	MSIN	Latitude	Longitude	Sync Expiry Time	Registered ID	Sync State	Actions
4001	Third Party	4001	Offline		90	90	N/A		Not Synced	
SM-1	3GPP co-located 201 SM	SM	Offline		44.5679	-110.98769	N/A	DEREGISTERED	Not Synced	
SM-2	Tyndall 201	SM	Offline		44.56799	-110.987694	N/A	DEREGISTERED	Not Synced	

- Click **Selected** display the **Please Confirm** window.

Please Confirm

This action will unblock CBRS registration in the device after it is deregistered. Do you want to continue?

 Note: This is applicable only for synced devices.

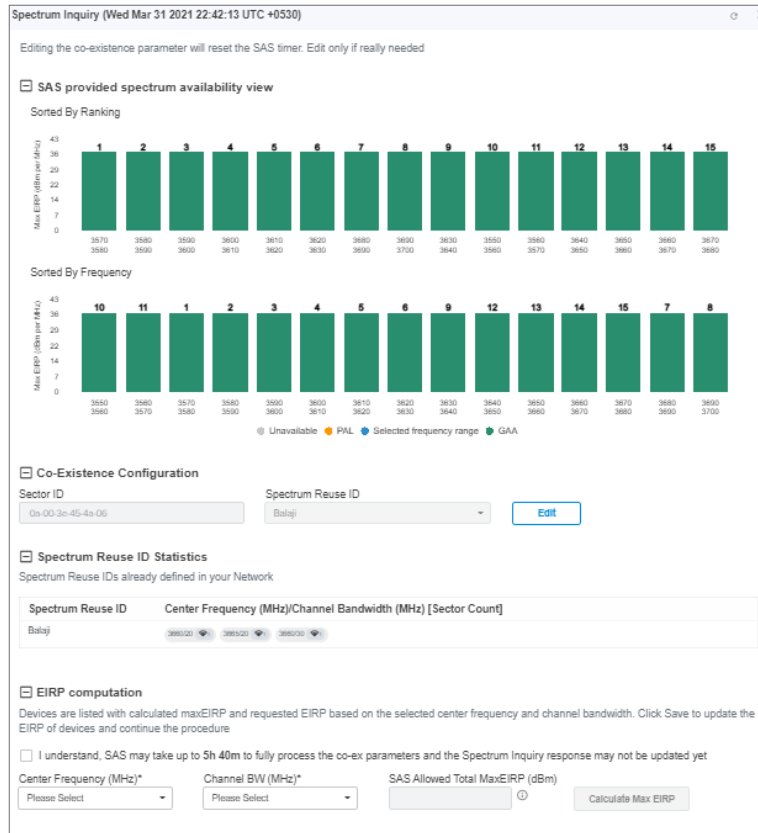
Yes No

- Click **Yes** to confirm the action.

Start CBRS Procedure

The Start button starts the CBRS procedure for a sector.

1. Navigate to **Services > CBRS > Management Tool** and select a sector.
2. Click **Start** to start CBRS procedure of a sector.
3. Once the user clicks start, the **Spectrum Inquiry** window pops up.



Note

- Multi-Grant is enabled by default.
- **Sorted By Ranking** is applicable for users selecting Google or Federated Wireless SAS.
- User can enable or disable the multigrant only if the device version is less than 21, if device version is 21 and above only multigrant is possible.

4. User can disable the Multi-Grant feature by disabling the checkbox **This feature will enable multi grant on the tool**. For more details refer [Multiple Grant](#).
5. Click **Edit** to edit **Co-Existence Configuration** and **EIRP Computation**.
 - **Spectrum Reuse ID Statistics** displays the devices running on different sector, channels, and bandwidth based on the **Spectrum Reuse ID**.
6. Once the Spectrum Inquiry is verified, click **Save**.

The Sector is created displays as shown below:

Management Tool > Mibank-5G											
Tool Frequency (MHz): 3550 - 3580											
Operating Frequency (MHz): N/A											
<div> <input type="text" value="Search"/> <input type="button" value="Add SM/BHS"/> <input type="button" value="Relinquish Grant"/> <input type="button" value="Delete"/> <input type="button" value="Deregister"/> <input type="button" value="Spectrum Inquiry"/> <input type="button" value="Re-init"/> <input type="button" value="Start"/> <input type="button" value="Export"/> <input type="button" value="Import"/> </div>											
<input type="checkbox"/> Device Name	MAC Address	Device Type	Mode	Health	Serial Number	Latitude	Longitude	Sync Expiry Time	Height	Grant Status	Sync State
<input type="checkbox"/> Mibank-5G		PMP 450i Connected	AP	Offline		25.7618	-80.1919	N/A	40	● Deregistered	Not Synced
<input type="checkbox"/> Mibank-5G		PMP 450i Connected	SM	Offline		45.215	-96.6339	N/A	30	● Deregistered	Not Synced
<input checked="" type="checkbox"/> Mibank-5G		PMP 450i Connected	SM	Offline		45.215	-96.6339	N/A	20	● Deregistered	Not Synced
Showing 1 - 3 Total: 3											



Note

- If the device is already synced with the Management Tool, the CBRS Start and Stop procedures are not applicable for all the synced devices.
- If user does not see the **Start** button, it means the CBRS procedure is already running.
- If all devices of the sector are in AUTHORIZED or HALT status and the user tries to start the CBRS procedure, the **Start** button will go to Stop state (as CBRS procedure is completed for all devices).

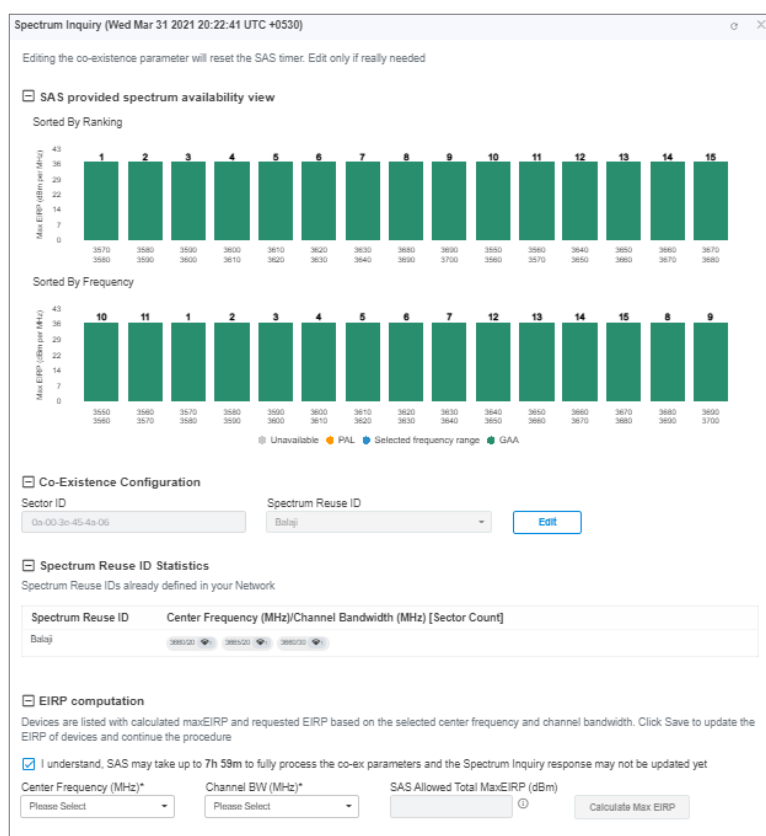
Multi-Grant

Multi-Grant feature divides selected channel bandwidth into multiple of 10 MHz channels. If the selected channel bandwidth is 5 MHz or low/high frequency contains 5 MHz raster, the slice would be in 5 MHz channel. Each slice will initiate a separate Grant procedure.

To enable Multiple Grant for a new sector:

1. Navigate to **Services > CBRS > Management Tool** and select a sector.
2. Click **Start** to start CBRS procedure of a sector.
3. Once the user clicks **Start**.

The Spectrum Inquiry window pops up as shown below.



Note

- Multi-Grant is enabled by default.
- Include User ID is applicable only for PMP devices, if user selects SAS is either Federated Wireless.

- Click **Edit** to edit Co-Existence Configuration and EIRP Computation.
 - Spectrum Reuse ID Statistics displays the devices running on different sector, channels, and bandwidth based on the Spectrum Reuse ID.
- Accept the checkbox process of the Co-Existence parameters.



Note

The Federated Wireless or Google SAS might need hours to fully process the Co-Existence parameters in the Registration, (before they are properly reflected in the Spectrum Inquiry Response). For more details see the CBRS Standalone Procedures Guide.

- Once the Spectrum Inquiry is verified, click **Save**.

A Sector created with Multiple Grants will be displayed as shown below:

Management Tool > devicesno

Tool Frequency (MHz): 3645 - 3675
Operating Frequency (MHz): N/A
Job Status (Procedure): Completed

Device Name	Device Type	Mode	Health	MSN	Latitude	Longitude	Sync Expiry Time	Height	Grant Status	Sync State	Actions
devicesno	PMP 450 Conn...	AP	Offline		44.4	-110.4	2d 2h 5m	1	1 2 3 4 5	Not Synced	
devicesdev	PMP 450 Conn...	SM	Offline		44.444	-110.444	2d 2h 32m	1	1 2 3 4 5	Not Synced	

Showing 1 - 2 Total 2 10 > < Previous 1 Next >

- To view the Grant Status click the info (i) icon.

Grant Status

1 Authorized	Last Heartbeat: Apr 07 2021 22:38:58 Frequency (MHz): 3645 - 3650 Channel BW (MHz): 5 Granted EIRP (dB/MHz): 11.2
2 Authorized	Last Heartbeat: Apr 07 2021 22:38:58 Frequency (MHz): 3650 - 3660 Channel BW (MHz): 10 Granted EIRP (dB/MHz): 11.2
3 Authorized	Last Heartbeat: Apr 07 2021 22:38:58 Frequency (MHz): 3660 - 3670 Channel BW (MHz): 10 Granted EIRP (dB/MHz): 11.2
4 Authorized	Last Heartbeat: Apr 07 2021 22:38:58 Frequency (MHz): 3670 - 3675 Channel BW (MHz): 5 Granted EIRP (dB/MHz): 11.2

Relinquish Grant

Relinquish Grant relinquishes all grants of selected sector. This will make devices enter the Registered state. The device will start Multi-Grant procedure if Multi-Grant feature is enabled on it.

To Relinquish Grant Perform as follows:

- Navigate to **Services > CBRS > Management Tool** and select a sector with Single Grant.
- Once the SM is selected, click **Relinquish Grant** to display **All** or **Selected**. Click **Selected**.
 - All**: relinquish all the registered devices.
 - Selected**: relinquish the selected device.

Management Tool > Mibank-5G

Tool Frequency (MHz): 3550 - 3580
Operating Frequency (MHz): N/A

Search

Device Name	MAC Address	Device Type	Mode	Health	Serial Number	Latitude	Longitude	Height	Grant Status	Sync State
<input type="checkbox"/> Mibank-5G		PMP 450i Connected	AP	Offline		25.7618	-80.191	40	Deregistered	Not Synced
<input type="checkbox"/> Mibank-3G		PMP 450 Connected	SM	Offline		45.215	-96.6339	30	Deregistered	Not Synced
<input checked="" type="checkbox"/> Mibank-5G		PMP 450 Connected	SM	Offline		45.215	-96.6339	20	Deregistered	Not Synced

Showing 1-3 Total 3

- Click **Yes** to confirm the action.

Please Confirm

This action will perform relinquish on 1 device(s) having single grant. After relinquishing the grant, the AP will request multiple grants.

Live update information may take up to several minutes to show the changes.

Do you want to proceed?



Note

Live update information may take upto several minutes to display the changes of reflected relinquish status.

- Once the user clicks **Yes**, **Wider Grant** gets converted to the **Multiple Grants** as shown below:

Management Tool > devicesno

Tool Frequency (MHz): 3645 - 3675
Operating Frequency (MHz): N/A
Job Status (Procedure): Completed

Search

Device Name	Device Type	Mode	Health	MSN	Latitude	Longitude	Sync Expiry Time	Height	Grant Status	Sync State	Actions
<input checked="" type="checkbox"/> devicesno	PMP 450 Conn...	AP	Offline		44.4	-110.4	2d 21h 5m	1	1 2 3 4 5	Not Synced	
<input type="checkbox"/> devicesdev	PMP 450 Conn...	SM	Offline		44.444	-110.444	2d 21h 32m	1	1 2 3 4 5	Not Synced	

Showing 1-2 Total 2

Stop CBRS Procedure

The **Stop** button stops the CBRS procedure for a sector.

- Navigate to **Services > CBRS > Management Tool** and select a sector.
- Click **Stop** button to stop CBRS procedure.



Note

- If the device is already synced with the Management Tool, the CBRS Start and Stop procedures are not applicable to the synced devices.
- If user does not see the **Stop** button, it means the CBRS procedure is already in stopped state, **Start** and **Stop** are toggles.
- If all devices of the sector are in AUTHORIZED state, the CBRS procedure will automatically stop.

Reinitialize CBRS Procedure

The **Re-init** button allows the user to start the CBRS procedure for a sector and reinitialize selected devices (Reinitialize = Start of sector + Reinitialization of user selected devices). At least one device must be selected in order to enable the **Re-init** button. Clicking **Re-init** reinitializes selected devices to UNREGISTERED (irrespective of previous CBRS state).

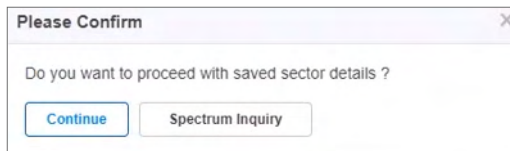
1. Navigate to **Services > CBRS > Management Tool** and select a sector.
2. Click **Stop** if the CBRS procedure is already running.
3. Select one or more devices to be reinitialized.



Note

You might notice some delay in enabling **Re-init** button after pressing **Stop**. It is due to a delay in properly stopping the CBRS procedure.

4. Click **Re-init** to start the reinitialization procedure
5. Confirmation window pops up:
 - Click **Continue** or
 - Select **Spectrum Inquiry** to edit the **EIRP values** as shown in [Start procedure.](#)



Note

- Synced devices cannot be reinitialized.
- Reinitialize modifies or corrects the parameters. For example, if a device is in HALT state due to a parameter error, the user can stop the CBRS procedure and reinitialize the device after modifying device parameters.


Deregistration

The deregistration procedure allows user to deregister the devices from the SAS server .

1. Navigate to **Network Services > CBRS > Management Tool** and select a sector.
2. Click **Stop** button if the CBRS procedure is already running.
3. Select one or many devices which need to be deregistered.
4. Click **Deregister** button to deregister selected devices.

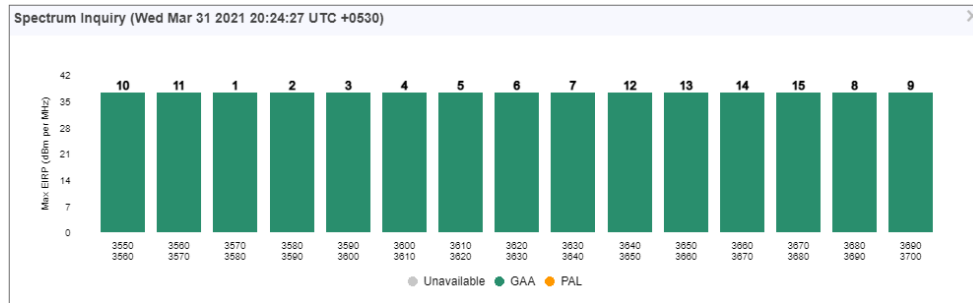
Once the user clicks **Deregister**, a job is scheduled.

Job Status (Deregistration): Completed

5. If the deregistration fails, the reasons will be indicated under .

Spectrum Inquiry

1. Navigate to **Services > CBRS > Management Tool** and select a Sector.
2. Click **Spectrum Inquiry** button.
3. **Spectrum Inquiry** status button is enabled once the device is registered (REGISTERED state) to the SAS.
 - If the selected SAS is not Google, EIRP is unsupported, and Spectrum Inquiry is displayed as shown below:



- If the user is selected SAS is **Google**, it supports **EIRP**. Spectrum Inquiry displays as below:



- **GAA**: General Authorized Access
- **PAL**: Priority Access License

Spectrum availability can be checked by hovering over frequencies.

Device Sync

The Sync procedure allows user to transfer grant information from Management Tool to respective device.

For a PMP sector, the Sync action can only be performed on an AP or BHM. The SM and BHS gets synced automatically when it comes online.

For an LTE sector, which supports a Cambium SM with a 3rd party BBU and RRH, the sync action will sync the Cambium SMs in this sector.

1. Navigate to **Services > CBRS > Management Tool** and select a sector.
2. Click **Sync** button to perform sync procedure.
3. Click **Yes** on the pop-up or click **NO** to cancel the sync procedure.

Once **Yes** is clicked, the Management Tool will check the accessibility of AP/BHM before proceeding with sync.



Note

- PMP SM cannot be manually synced. It is only synced automatically.
- Once the device is synced, for both PMP and LTE devices, primary management is transferred from the tool to the device itself. However, some actions and procedures are still supported on the tool. See the [CBRS Consolidated Procedures Guide](#) for more details.
- Sync procedure copies complete CBRS parameters to device and enables CBRS to transmit with configured parameters.

Live Status Update

Once the device is **Config synced**, CBRS details like CBSD ID, Grant ID, CBSD Grant State, and Last Heartbeat Time are read from the device every 5 minutes.

Management Tool > 27_183

Tool Frequency (MHz): 3650 - 3670
Operating Frequency (MHz): 3650 - 3670
Job Status (Procedure): Completed

Device Name	Device Type	Mode	Health	MSN	Latitude	Longitude	Sync Expiry Time	Height	Grant Status	Sync State	Actions
27_183	PMP 450i Conn...	AP	Online		45.114386	-96.642475	N/A	22	Authorized	Config Synced	
25_184	PMP 450 Integr...	SM	Online		45.114385	-96.642474	N/A	22	Authorized	Config Synced	

Showing 1 - 2 Total: 2 | < Previous 1 Next >

It displays the possible single Grant state such as:

- Authorized
- Deregistering
- Grant
- Grant Suspended
- Grant Terminate
- Registered
- Registering
- Relinquished Spectrum
- Relinquishing Spectrum
- Unregistered
- Unknown

Domain Proxy View



Note

Domain Proxy View is available only on cnMaestro Cloud and the Cloud Anchor account.

In Domain Proxy view, Sectors and Non-Sector page helps check CBRS-complaint devices connected through this server and On-Premises server using the token ID of this server. This page displays all the devices connected to CBRS.

Network Services > CBRS

Account Management Tool Domain Proxy View

Sector Non Sector

Lists all registered CBRS-compliant devices within 3.6 GHz band (3550 MHz to 3700 MHz) on SAS. Devices may be registered through cnMaestro or through AP and might not be managed by cnMaestro.

MAC Address Search

Device Name	Device Type	Mode	User ID	Center Frequency (MHz)	Channel BW (MHz)	CBSD ID	Active S/W Version
PMP_678954	PMP	AP		3580	20		

Showing 1 - 1 Total: 1 | < Previous 1 Next >

- **Sectors Page:** displays the devices according to the parenting AP list.
- **Non-Sector Page:** displays each individual AP and SM of **LTE** and **PMP**.

Searching a Domain Proxy Sector

To search a sector:

1. Navigate to **Services > CBRS > Domain Proxy View > Sector** page.
2. Select search option **CBSD or MAC**.

- For **CBSD**: Search by CBSD ID
- For **MAC**: Search by MAC ID.

Network Services > CBRS

Account Management Tool Domain Proxy View

Sector Non Sector

Lists all registered CBRS-compliant devices within 3.6 GHz band (3550 MHz to 3700 MHz) on SAS. Devices may be registered through cnMaestro or through AP and might not be managed by cnMaestro.

MAC Address Search

Device Name	Device Type	Mode	User ID	Center Frequency (MHz)	Channel BW (MHz)	CBSD ID	Active S/W Version
PMP-678954	PMP	AP		3580	20		

Showing 1 - 1 Total: 1 < Previous 1 Next >

3. Enter text in search box.



Note

- If AP device is entered , it displays the both AP devices and the related SM device in the search result.
- If SM devices is entered , it displays only the SM devices in the search result.

4. Filtered device can be cleared by clicking **Clear** button.

Domain Proxy Sector view

1. Click a Sector from Sector AP column to get the list of devices.
2. All the devices of the sector will be displayed.

Network Services > CBRS

Account Management Tool Domain Proxy View

Sector Non Sector

Lists all registered CBRS-compliant devices within 3.6 GHz band (3550 MHz to 3700 MHz) on SAS. Devices may be registered through cnMaestro or through AP and might not be managed by cnMaestro.

MAC Address Search

Device Name	Device Type	Mode	User ID	Center Frequency (MHz)	Channel BW (MHz)	CBSD ID	Active S/W Version
PMP-678954	PMP	AP		3580	20		

Showing 1 - 1 Total: 1 < Previous 1 Next >

3. CBSD state shows current status of device and whether it is registered or deregistered with SAS.
4. Click **Deregister** to deregister the device from CBRS.
5. The Sectors view displays the following columns by default:
Device Name, Device Type, Mode, User ID, Center Frequency (MHz), Channel BW (MHz), CBSD ID, and Active S/W Version.

Searching a Domain Proxy in Non Sector View

To search for a device in the non-sector view, complete the following steps:

1. Navigate to **Services > CBRS > Domain Proxy View > Non Sector** page.
2. Select one of the following search options from the drop-down list—**CBSD**, **MAC Address**, or **Heartbeat Status**.
 - For **CBSD**, search by the CBSD ID
 - For **MAC Address**: search by the MAC address of the device
 - For **Heartbeat Status**, search by the heartbeat status of registered devices:

- Heartbeating
- Not Heartbeating for Last 24 Hours
- Not Heartbeating for Last 7 Days
- Not Heartbeating for Last 30 Days
- Not Heartbeating for Last 60 Days
- Not Heartbeating for Last 90 Days

Network Services > CBRS

Account Management Tool Domain Proxy View

Sector Non Sector

Last Heartbeat timestamp will be updated every 12 hours.

MAC Address Search

Device Name	MAC Address	Device Type	Mode	Health	Serial Number	CBSD ID	Latitude	Longitude	Height	Registered	Heartbeat Status	Last Heartbeat	
-	-	-	SM	Offline	-	-	-	-	-	No	-	-	Deregister
PMP-894356	-	PMP	SM	Offline	-	-	-	-	-	No	-	-	Deregister
PMP-678954	-	PMP	AP	Offline	-	-	44	-110	13	No	-	-	Deregister

Showing 1-3 Total: 3 < Previous 1 Next >



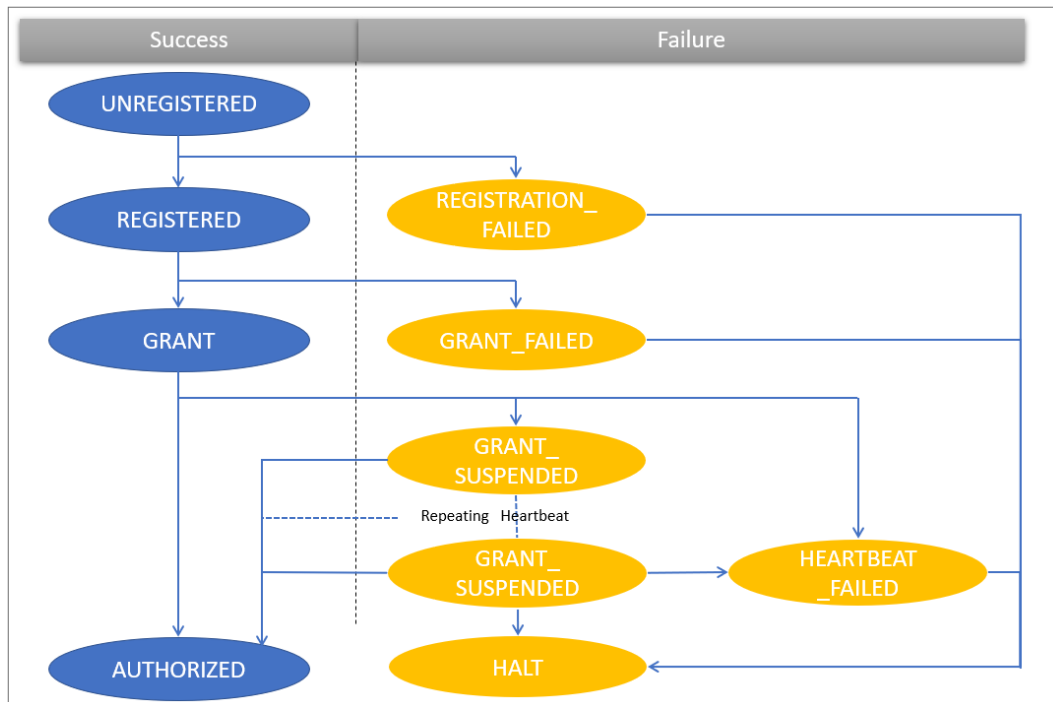
Note

Information in the **Heartbeat Status** and **Last Heartbeat** columns is displayed only for registered devices.

cnMaestro checks the heartbeat status of a CBRS device every 12 hours. The following statuses are updated in the **Heartbeat Status** column, based on whether the device is online or offline:

- **Heartbeating**: When the device is online and the heartbeat check is successful. Also, the last successful heartbeat time is updated in the **Last Heartbeat** column.
- **Not Heartbeating**: When the device is offline for 24 hours or more.

CBRS State Diagram



**Note**

GRANT_SUSPENDED is a temporary suspend state where HEARTBEAT message is sent for an extended period of time prior to obtaining the AUTHORIZED state.

CBRS Device Parameters

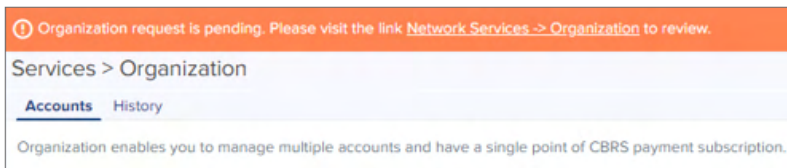
Category	Parameter	Details
Common	Channel BandWidth (MHz)	Channel Bandwidth of AP or BHM in MHz.
	Center Frequency (MHz)	Center frequency of AP or BHM in MHz.
	Device Name	Name given to device on SAS Admin (A maximum of 120 characters are supported. However, this name is not copied to the device when synchronized.)
	Device Type	Drop-down selection of supported devices types.
	MAC Address	MAC address of the device.
	MSN	Serial number of device.
	User ID	Unique identifier is assigned by the SAS. The User ID is part of the registration request message. The wrong User ID leads to REGISTRATION_FAILED.
Location	Height	Device antenna height in meters.
	Height Type	Should be AGL or AMSL as follows: <ul style="list-style-type: none">• AGL height is measured relative to the ground level.• AMSL height is measured relative to the mean sea level.
	Horizontal Accuracy	A positive number in meters to indicate the accuracy of the device antenna horizontal location.
	Latitude	Latitude of the device antenna location in degrees.
	Longitude	Longitude of the CBSD antenna location in degrees.
	Vertical Accuracy	A positive number in meters to indicate the accuracy of the device antenna vertical location.
Co-Existence Related Parameters	Sector ID	The default AP MAC address (allows editing the default MAC).
	Spectrum Reuse ID	The Spectrum Reuse ID defined in the network.
	Include User ID	Prefixes the User ID to the Sector ID and Spectrum reuse ID.
ECGI Related Parameters	PLMN ID	Public and Mobile Network Identifier.
	ECI	E-UTRAN Cell Identifier. It is a length of 28 bits and contains the eNodeB-ID.
	ECGI	Enter the both PLMN ID and ECI parameters and it displays in the ECGI field.
	Azimuth (degrees)	Boresight direction of the horizontal plane of the antenna in degrees with respect to True North.

Category	Parameter	Details
Antenna Parameters	Beamwidth (degree)	3-dB antenna beam width of the antenna in the horizontal-plane in degrees.
	Downtilt (degrees)	Antenna downtilt in degrees.
	External Antenna Gain (dBi)	Peak gain of external antenna connected to device in dBi.
	Integrated Antenna Gain (dBi)	Peak gain of integrated antenna in dBi.
Add Certificate	Certificate File	CPI (Certified Professional Installer) certificate.
	CPIR Name	CPI registered name.
	File Password	CPI private password.

Actions for Existing CBRS On-Premises Users

Current CBRS On-Premises customers maintain their CBRS billing and SAS configuration in an NMS Account. This must be updated to support Anchor accounts. To create an anchor account, refer to [Manage Instances](#).

If an action is required for existing Cloud NMS users, the UI will display the following notification:



After clicking the notice, navigate to **Services**.

- **Link an Anchor Account to this Account:** Select if managing CBRS devices in both Cloud and On-Premises. It creates an Organization that shares configuration between a Primary NMS account and a Secondary Anchor account (without deregistering existing CBRS devices).
- **Convert this Account to Anchor Account:** Select only if managing devices On-Premises and NMS do not have any devices. It converts the existing NMS Account to an Anchor Account.

Link an Anchor Account to this Account

Select this to manage CBRS devices in both Cloud and On-Premises. An Anchor account must be created to manage the CBRS On-Premises devices without deregistration.



Note

Cambium recommends selecting this option when the user is managing devices in both cnMaestro Cloud and On-Premises.

Before linking an Anchor account, please do the following:

- Ensure the cnMaestro Anchor account is linked to the cnMaestro On-Premises instance(s).
- Add the Anchor account as a Secondary account to Primary NMS account. Refer to Create Organization.

To convert the existing account:

1. Navigate to **Services > CBRS > Account** page.

There are some actions pending related to CBRS. Please visit the link [Network Services > CBRS](#) to review.

Network Services > CBRS

Account Management Tool Domain Proxy View

Action Required

This Cloud NMS Account is linked to one or more On-Premises NMSs. We recommend that you connect your On-Premises NMSs to an Anchor Account to optimally manage CBRS. [Learn more](#)

Please note: Linking On-Premises NMSs to an Anchor Account will be required in order to upgrade to cnMaestro 3.2 in the near future.

Link an Anchor Account to this Account

Choose this option if you want to manage CBRS devices in both the Cloud and On-Premises. It allows an Anchor Account to support the CBRS devices registered to this account

Prerequisites

1. Create a cnMaestro Anchor Account and link it to your cnMaestro On-Premises instance
2. Add the Anchor Account as a Secondary to this account. You can do this from the Organization page
3. In the Anchor Account, accept Shared SAS ID service and create CBRS account
4. Choose the Anchor Account from the below dropdown and submit the support request

Please note:

1. Full directions for creating Anchor Accounts and Organizations are available in the User Guide
2. This operation will take up to 24 hours to complete

Select Anchor Account

There are no anchor accounts linked to this account

☐ I authorize Cambium Networks to make changes to the selected account

[Request Support](#)

Convert this Account to Anchor Account

Choose this option if you will only manage devices using cnMaestro On-Premises. It converts the existing NMS Account to an Anchor Account

Prerequisites

1. Deregister all CBRS devices managed by this Cloud Account
2. Remove all devices managed by this Cloud Account

Please note:

1. All NMS configuration will be lost when this account is converted to an Anchor Account
2. This operation will take up to 24 hours to complete and it cannot be reversed
3. Once complete, you need to associate cnMaestro On-Premises to the new account. Instructions are available in the User Guide

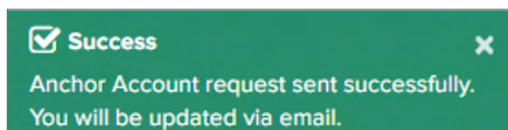
2. Select **Anchor Account** from the drop-down list.



Note

Users are allowed to select only one Anchor account from the drop-down list.

3. Enable **I authorize Cambium Networks to make changes to the selected account.**
4. Click **Request Support** and a **Success** window pops up.



Note

The Cambium Support team validates the request and creates an Organization from the NMS and Anchor accounts within 24 hours. Alternately, you can create the Organization yourself using the directions specified earlier in this document.

Convert this Account to Anchor Account

Select this to manage CBRS devices in On-Premises only. It converts an existing NMS account to an Anchor account.



Note

Cambium recommends selecting this option when the user only plans to manage devices using cnMaestro On-Premises. Cloud account devices must be deregistered and deleted from the NMS account and registered back to On-Premises before the conversion.

To convert the existing account:

1. Navigate to **Services > CBRS > Account** page.

< 1/2 > | Your account is under the data retention period until 07-Aug-2021. Please renew the subscriptions at the earliest to avoid loss of long term historical data and configuration data related to cnMaestro X features.

Network Services > CBRS

Account Management Tool Domain Proxy View

Action Required

This Cloud NMS Account is linked to one or more On-Premises NMSs. We recommend that you connect your On-Premises NMSs to an Anchor Account to optimally manage CBRS. [Learn more](#)

Please note: Linking On-Premises NMSs to an Anchor Account will be required in order to upgrade to cnMaestro 3.2 in the near future.

☐ Link an Anchor Account to this Account

Choose this option if you want to manage CBRS devices in both the Cloud and On-Premises. It allows an Anchor Account to support the CBRS devices registered to this account

Prerequisites

1. Create a cnMaestro Anchor Account and link it to your cnMaestro On-Premises instance
2. Add the Anchor Account as a Secondary to this account. You can do this from the Organization page
3. In the Anchor Account, accept Shared SAS ID service and create CBRS account
4. Choose the Anchor Account from the below dropdown and submit the support request

Please note:

1. Full directions for creating Anchor Accounts and Organizations are available in the User Guide
2. This operation will take up to 24 hours to complete

Select Anchor Account

There are no anchor accounts linked to this account

☐ I authorize Cambium Networks to make changes to the selected account

Request Support

☒ Convert this Account to Anchor Account

Choose this option if you will only manage devices using cnMaestro On-Premises. It converts the existing NMS Account to an Anchor Account

Prerequisites

1. Deregister all CBRS devices managed by this Cloud Account
2. Remove all devices managed by this Cloud Account

Please note:

1. All NMS configuration will be lost when this account is converted to an Anchor Account
2. This operation will take up to 24 hours to complete and it cannot be reversed
3. Once complete, you need to associate cnMaestro On-Premises to the new account. Instructions are available in the User Guide

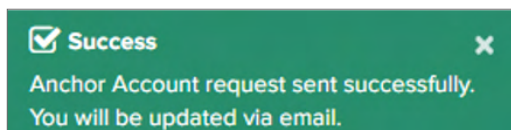
2. Select **Convert this Account to Anchor Account**.



Note

- Deregister and remove all devices from the NMS account before the conversion.
- All NMS configuration will be lost when the account is converted to Anchor, including:
 - Guest Access Portal
 - Templates
 - Performance Graph Data, etc.
- The process of converting an NMS account to an Anchor account cannot be reversed.

3. Provide your consent by selecting the **I authorize Cambium Networks to make changes to the selected account** checkbox.
4. Click **Request Support** and the following success message is displayed.



The Cambium Support team validates the request and creates an Organization from the NMS and Anchor accounts within 24 hours.

Organizations for CBRS

An Organization allows multiple accounts to share CBRS billing and SAS ID. The Primary Account owns this configuration, and the Secondary Account can optionally share it. Both accounts must authorize the sharing.



Note

- There is only one Primary Account in an Organization.
- CBRS configuration can be set in the Primary Account and optionally shared to Secondary Accounts.

This chapter provides the following information:

- [Create an Organization](#)
- [Remove Accounts](#)
- [Disable Secondary Account Services](#)
- [Edit Services](#)
- [Share CBRS Configuration with the On-Premises Instance](#)
- [Organization History](#)

Create an Organization

Primary Account

Perform the following steps on the Primary Account:

1. Navigate to **Network Services > Organization > Accounts**.

Services > Organization

Accounts History

Organization enables you to manage multiple accounts and have a single point of CBRS payment subscription.

Account Information

Account ID **000676a3d519bea9d5b22b5a57063914**

① To make this a secondary account, copy the account ID, login to the primary account, navigate to the Organization page and add this as a secondary account.

① To make this a primary account, click "Add Secondary Account"

[Add secondary account](#)

2. Click **Add Secondary Account**.

Add Secondary Account

Secondary Account ID

Copy the Account ID from the secondary account

Close

Navigate to the planned Secondary Account and copy the Account ID of the Secondary Account using the Copy to Clipboard.

3. Paste the copied **Account ID** in the **Secondary Account ID** text box.
4. Once the Secondary Account is validated, the **Cambium ID** is displayed as shown below.

Add Secondary Account

Secondary Account ID


7972ccc4d7dd0da4af1617c8c85a4d01

Copy the Account ID from the secondary account

Cambium ID

DOCUMNETATION2

Shared SAS ID




SAS ID

Use Primary Account's SAS ID

☐ Enable Shared SAS ID

Unified Payments



Use Primary Account's Payment

☐ Enable Unified Payments

ⓘ

Please Note: Enabling Shared SAS ID will also enable Unified Payments

Add

Close

5. The Primary Account can offer services such as:

- **Shared SAS ID:** This allows the Secondary Account to use the CBRS SAS ID configured in the Primary Account.
- **Unified Payments:** This allows the Secondary Account to use payment details configured in the Primary Account.



Note

Sharing the SAS ID automatically enables **Unified Payments**.

6. Enable the Services **Shared SAS ID** or **Unified Payments**.

Add Secondary Account

Secondary Account ID


7972ccc4d7dd0da4af1617c8c85a4d01

Copy the Account ID from the secondary account

Cambium ID

DOCUMNETATION2


Shared SAS ID



Use Primary Account's SAS ID

☒ Enable Shared SAS ID

Unified Payments



Use Primary Account's Payment

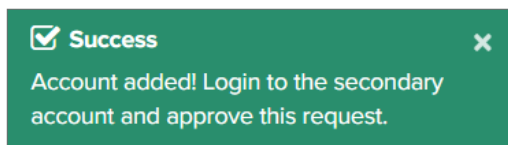
☒ Enable Unified Payments

ⓘ Please Note: Enabling Shared SAS ID will also enable Unified Payments

Add

Close

7. Click **Add**. It displays the **Success** message as shown below:



Note

The Secondary Account administrator must approve this request from the Primary Account to join the Organization.

8. 1. In the **Secondary Accounts** table, the **Approval Status** is displayed as **Waiting for approval**.

Services > Organization

Accounts History

Organization enables you to manage multiple accounts and have a single point of CBRS payment subscription.

Account Information - Primary Account

Account ID 000676a3d519bee9d5b22b5a57063914 ⓘ

Account Type Network Management System

Cambium ID	Account ID	Account Type	Approval Status	Enabled Services
DOCUMNETATION2	7972ccc4d7dd0da4af1617c8c85a4d01	NMS	Waiting for approval ⓘ	Shared SAS ID*, Unified Payments*

* - Service has not been accepted by the secondary Account

Secondary Account

Login to the Secondary Account to complete Organization creation. The Secondary Account must approve the request and authorize the shared services. The Secondary Account can also request additional services (which must be approved by the Primary Account).

Perform the following steps in the Secondary Account:

1. Navigate to **Network Services > Organization > Accounts**.
2. Click **Approve**.

Organization request is pending. Please visit the link [Network Services > Organization](#) to review.

Services > Organization

Accounts History


Organization enables you to manage multiple accounts and have a single point of CBRS payment subscription.

Account Information - Secondary Account
Account ID: 7972ccc4d7dd0da4af1617c8c85a4d01
Account Type: Network Management System


Primary Account
The following primary account wants to add you to its organization.
Cambium ID: QA_SANDBOX_SB2
Approval Status: **Waiting for approval**
Approve **Reject**

3. The **Approve Services** window pops up. Review the services requested and click **Approve**.

Approve Services

Shared SAS ID

Use Primary Account's SAS ID
☒ Accept Shared SAS ID

Primary account is requesting to enable this service

Unified Payments

Use Primary Account's Payment
☒ Accept Unified Payments

Primary account is requesting to enable this service

Please Note: Accepting Shared SAS ID will also accept Unified Payments

Approve **Close**

Additional service requests from the Secondary Account

Additional services can be added after the Secondary Account joins the Organization, such as including the Unified Payments Service.

Perform the following steps on the Secondary Account:

1. Navigate to **Network Services > Unified Payments** and click **Enable**.

**Note**

This generates a request to the Primary Account to provide support for Unified Payments.

Network Services > Organization

Accounts History

Organization enables you to manage multiple accounts and have a single point of CBRS payment subscription.

Account Information - Secondary Account

Account ID **7972ccc4d7dd0da4af1617c8c85a4d01**

Account Type **Network Management System**

Primary Account

The following Primary account wants to add you to its organization.


Cambium ID **QA_SANDBOX_SB2**

Approval Status **Approved**

[Remove From Organization](#)

Services

Shared SAS ID




Use Primary Account's SAS ID

⊗ Service has been disabled

[Enable](#)

Unified Payments



Use Primary Account's Payment

⊗ Service has been disabled

[Enable](#)

2. Once the services are enabled and approved in the Primary Account, the following displays in the Secondary Account.

Network Services > Organization

Accounts History

Organization enables you to manage multiple accounts and have a single point of CBRS payment subscription.

Account Information - Secondary Account

Account ID: 895bd0491a0cf955eeb474252a29d0bf

Account Type: Anchor

Primary Account

The following Primary account wants to add you to its organization.


Cambium ID: VINOD_ACCOUNT_NMS

Approval Status: **Approved**

[Remove From Organization](#)

Services

Shared SAS ID




SAS ID

Use Primary Account's SAS ID

☒ Service has been disabled

[Enable](#)

Unified Payments



Unified Payments

Use Primary Account's Payment

☒ Service has been enabled

[Disable](#)

3. The enabled services will be displayed in the Primary Account.

Network Services > Organization

Accounts History

Organization enables you to manage multiple accounts and have a single point of CBRS payment subscription.

Account Information - Primary Account

Account ID: c211eeb63cb0dd63776769ee4779853a

Account Type: Network Management System

Secondary Accounts

Cambium ID	Account ID	Account Type	Approval Status	Enabled Services	Pending Service Request	
3_0_2_EST_1_SRV_1_IOT_RGVN	250c38fb22c5526c73dcb6b615b5bf90	NMS	Approved	-	-	
VINOD_ACCOUNT_ANCHOR	51420be0a3f98170e4573bd849b3a7	Anchor	Approved	Shared SAS ID*, Unified Payments	-	
VINOD_ACCOUNT_ANCHOR3	895bd0491a0cf955eeb474252a29d0bf	Anchor	Approved	Shared SAS ID*, Unified Payments	-	
VINOD_ACCOUNT_ANCHOR2	b8740772e975f6d9350b6c415ddc1f	Anchor	Approved	Unified Payments	-	
241_FRESHACCOUNT	bd36a8c159d9f384e892a762820b105	NMS	Approved	-	Unified Payments	Review


[Add New](#)

* - Service has not been accepted by the Secondary account

Removing Accounts

Remove through Primary Account

Perform the following steps on the Primary Account to remove the Secondary Account:

1. Navigate to **Network Services > Organization > Accounts**.
2. In the **Secondary Accounts**, click Delete () icon.

Services > Organization

[Accounts](#) [History](#)

Organization enables you to manage multiple accounts and have a single point of CBRS payment subscription.

Account Information - Primary Account

Account ID: 000676a3d519bea9d5b22b5a57063914

Account Type: Network Management System

Secondary Accounts

Cambium ID	Account ID	Account Type	Approval Status	Enabled Services
DOCUMNETATION2	7972ccc4d7dd0da4af1617c8c85a4d01	NMS	Approved	Shared SAS ID **, Unified Payments **

[Add New](#)

** - Service has been accepted by the secondary Account but has errors

3. The **Remove From Organization** window pop up.

Remove From Organization

Please specify the reason so that the other account knows why this action was carried out.

Cambium ID: DOCUMNETATION2

Reason: test

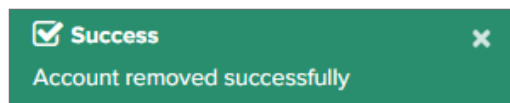
[Proceed](#)

4. Enter the **Reason**.

5. Click **Proceed**.

Without Active Services

- If services such as **Shared SAS ID** or **Unified Payments** are inactive in the Secondary Account, it can be deleted without any approval.
- The following message displays if successful.



With Active Services

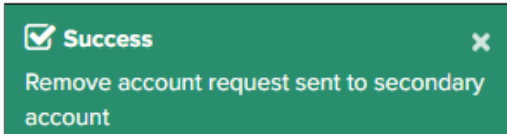
- If services such as **Shared SAS ID** or **Unified Payments** are active in the Secondary Account, the services need to be disabled from the Secondary Account, and the request must be approved by the Secondary Account administrator.



Note

- User needs to disable the active services such as [Shared SAS ID](#) and [Unified Payments](#) before removing the Secondary Account, or an Error message is shown.
- Shared SAS ID can be removed by contacting Cambium support to deactivate the current CBRS account to stop using Shared SAS ID.
- Active Services will be highlighted in **Green** color.

- The following message displays if successful.



- In the **Secondary Accounts** table, the UI displays the **Approval Status** as **Delete Pending**.

Services > Organization

Accounts History

Organization enables you to manage multiple accounts and have a single point of CBRS payment subscription.

Account Information - Primary Account

Account ID 000676a3d519bea9d5b22b5a57063914

Account Type Network Management System

Secondary Accounts

Cambium ID	Account ID	Account Type	Approval Status	Enabled Services
RAR_QA_SRV_3	6414d2df6a7ca908a6e0f303a8e80b1a	NMS	Delete pending	Unified Payments

[Add New](#)

The Secondary Account administrator must approve the remove request from the Primary Account. For more details, refer to [Approve Remove Request \(with active services\)](#).

Remove Organization from Secondary Account

Perform the following steps on the Secondary Account to remove an Organization:

1. Navigate to **Network Services > Organization > Accounts**.
 - a. Click **Remove From Organization** (without active services).
 - To remove the Secondary Account from an Organization with no active services.

Network Services > Organization

Accounts History

Organization enables you to manage multiple accounts and have a single point of CBRS payment subscription.

Account Information - Secondary Account

Account ID 7972ccc4d7dd0da4af1617c8c85a4d01

Account Type Network Management System

Primary Account

The following Primary account wants to add you to its organization.

Cambium ID QA_SANDBOX_SB2

Approval Status **Approved**

Remove From Organization

Services

Shared SAS ID

Use Primary Account's SAS ID

① SAS ID will be copied from primary on CBRS account creation.

[Disable](#)

Unified Payments

Use Primary Account's Payment

① Unified payments will be used on CBRS account creation.

[Disable](#)

- Click **Yes** in **Please confirm** window to remove this account.

Please confirm

Are you sure you want to remove this account?

Yes

No

b. **Approve Remove Request** (with active services).



Note

Disable active services before **Approve Remove Request**.

- If the Secondary Account is using services such as **Shared SAS ID** or **Unified Payments**, the following message displays.

Organization unlink request is pending. Please visit the link [Network Services -> Organization](#) to review.

Services > Organization

Accounts

History

Organization enables you to manage multiple accounts and have a single point of CBRS payment subscription.

Account Information - Secondary Account

Account ID

6414d2df6a7ca908a6e0f303a8e80b1a

Account Type

Network Management System

Primary Account

The following primary account wants to add you to its organization.

Cambium ID

QA_SANDBOX_SB2

Approval Status

Approved

Remove From Organization

Remove Request

Primary Account has requested to remove you from its organization.

Reason

test

Approve Remove Request

Reject

Services

Shared SAS ID

SAS ID

Use Primary Account's SAS ID

Primary has not granted this service

Request

Unified Payments

Unified Payments

Use Primary Account's Payment

Service has been enabled

Disable

- Click **Yes** in **Please confirm** window to approve the request.

Please confirm

Are you sure you want to approve the remove request? You will not able use primary account's services.

Yes

No

2. The following message displays if successful.

Success

Account removed successfully

×

Disable Secondary Account services

With no active services

The Secondary Account user can disable services without leaving the Organization.

1. Navigate to **Services > Organization > Accounts** and select **Services**.
2. Click **Disable**.

Services > Organization

Accounts History

Organization enables you to manage multiple accounts and have a single point of CBRS payment subscription.

Account Information - Secondary Account

Account ID: 7972ccc4d7dd0da4af1617c8c85a4d01

Account Type: Network Management System

Primary Account

The following primary account wants to add you to its organization.


Cambium ID: QA_SANDBOX_SB2

Approval Status: Approved

[Remove From Organization](#)

Services

Shared SAS ID




Use Primary Account's SAS ID

ⓘ SAS ID will be copied from primary on CBRS account creation.

[Disable](#)

Unified Payments



Use Primary Account's Payment

ⓘ Unified payments will be used on CBRS account creation.

[Disable](#)

3. Click **Yes** in the **Please confirm** window.

Please confirm

Are you sure you want to remove this service?

[Yes](#) [No](#)


4. After disabling, the following displays.

Network Services > Organization

Accounts History

Organization enables you to manage multiple accounts and have a single point of CBRS payment subscription.

Account Information - Secondary Account

Account ID **7972ccc4d7dd0da4af1617c8c85a4d01** 

Account Type **Network Management System**

Primary Account

The following Primary account wants to add you to its organization.


Cambium ID **QA_SANDBOX_SB2**

Approval Status **Approved**


[Remove From Organization](#)

Services

Shared SAS ID




Use Primary Account's SAS ID


 Service has been disabled

[Enable](#)

Unified Payments



Use Primary Account's Payment

 Service has been disabled

[Enable](#)

5. Click **Enable** to reactivate the services.

With active shared SAS ID services



Note

Active Services are highlighted in **Green** color.

The Secondary Account user can disable the **Shared SAS ID** services.

1. Navigate to **Services > Organization > Accounts** and select **Services**.

Network Services > Organization

Accounts History

Organization enables you to manage multiple accounts and have a single point of CBRS payment subscription.

Account Information - Secondary Account

Account ID 895bd0491a0cf955eeb474252a29d0bf

Account Type Anchor

Primary Account

The following Primary account wants to add you to its organization.


Cambium ID VINOD_ACCOUNT_NMS

Approval Status **Approved**

[Remove From Organization](#)

Services

Shared SAS ID




Use Primary Account's SAS ID

✓ Service has been enabled

[Disable](#)

Unified Payments



Use Primary Account's Payment

✓ Service has been enabled

[Disable](#)

2. Click **Disable** in the **Shared SAS ID**.
3. Click **Yes** in the **Please confirm** window.

Please confirm

Are you sure you want to remove this service?

[Yes](#) [No](#)

4. If CBRS account is active in Secondary Account, while disabling it displays the following error message.

Error

CBRS account is currently active in secondary. Cannot remove shared SAS ID. Please contact Cambium support to deactivate the current CBRS account to stop using Shared SAS ID.

If an **Error** message pops up, the user needs to raise a request to Cambium Support for the SAS vendor cancellation. Cambium Support will disable the CBRS services and deregister all devices associated to the Secondary Account.

Once disabled, the Secondary Account user can view the SAS vendor page and create a new CBRS account as shown below.

Network Services > CBRS

Enable Citizens Broadband Radio Service subscription for the CBRS-compliant devices in 3.6 GHz band (3550 MHz to 3700 MHz). [Learn more](#)

Spectrum Access System (SAS) ⓘ

Please select a SAS vendor

☐ I accept the [CAMBIUM NETWORKS LTD. "CBRS" TERMS OF SERVICE](#)

☐ I accept the [CBRS Service payment terms](#)

Enable

For further information on creating a new CBRS account, refer to [CBRS](#).



Note

Services in the Secondary Account cannot be disabled unless CBRS is inactive in Secondary Account. Contact Cambium Support to disable CBRS operation or change SAS Vendor.

With active Unified Payments

The Secondary Account user can disable Unified Payments.

1. Navigate to **Services > Organization > Accounts** and select **Services**.

Organization unlink request is pending. Please visit the link [Network Services -> Organization](#) to review.

Services > Organization

Accounts History

Organization enables you to manage multiple accounts and have a single point of CBRS payment subscription.

Account Information - Secondary Account

Account ID: 6414d2df6a7ca908a6e0f303a8e80b1a

Account Type: Network Management System

Primary Account

The following primary account wants to add you to its organization.

Cambium ID: QA_SANDBOX_SB2

Approval Status: **Approved**

Remove From Organization

Remove Request: **Primary Account has requested to remove you from its organization.**

Reason: test

Approve Remove Request Reject

Services

Shared SAS ID

SAS ID

Use Primary Account's SAS ID

Primary has not granted this service

Request

Unified Payments

Use Primary Account's Payment

Service has been enabled

Disable

2. Click **Disable** within **Unified Payments**.
3. Click **Yes** in **Please confirm** window.

Please confirm

Are you sure you want to remove this service?

Yes
No

- If **Unified Payments** is active in CBRS of the Secondary Account, it displays an **Error** message.

!
Error

Payment method has to be added before disabling this service. Please go to the CBRS page to add new payment method.

If this happens, the user needs to add new CBRS payment details into the Secondary Account.

Payment Details

☒ Using primary account payment details
Add New Payment Method

For further information on Payment details, refer to [CBRS](#).

The user can disable the **Unified Payments** once the new payment details are added successfully to the Secondary Account.

Edit Services

Enable services in the Primary Account

The Primary Account can edit or disable services shared with the Secondary Account as shown below:



Note

When the services are active in CBRS of the Secondary Account, the Primary Account cannot disable those services.

- Navigate to **Accounts > Secondary Accounts** tab.
- Click Edit () icon.

Services > Organization

Accounts
History



Organization enables you to manage multiple accounts and have a single point of CBRS payment subscription.

Account Information - Primary Account

Account ID
000676a3d519bea9d5b22b5a57063914

Account Type
Network Management System

Secondary Accounts

Cambium ID	Account ID	Account Type	Approval Status	Enabled Services	
DOCUMENTATION2	7972ccc4d7dd0da4af1617c8c85a4d01	NMS	Approved	Shared SAS ID **, Unified Payments **	<div>   </div>
Add New					

** - Service has been accepted by the secondary Account but has errors

- Edit Secondary Account** window pops up.

Edit Secondary Account


Secondary Account ID
7972ccc4d7dd0da4af1617c8c85a4d01

Copy the Account ID from the secondary account

Cambium ID
DOCUMNETATION2

Services


Shared SAS ID



Use Primary Account's SAS ID

☒ Enable Shared SAS ID

Unified Payments



Use Primary Account's Payment

☒ Enable Unified Payments

Please Note: Enabling Shared SAS ID will also enable Unified Payments

Update
Close

- Disable the **Services** and click **Update**.

Edit Secondary Account

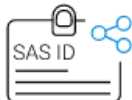
Secondary Account ID
7972ccc4d7dd0da4af1617c8c85a4d01

Copy the Account ID from the secondary account

Cambium ID
DOCUMNETATION2

Services


Shared SAS ID



Use Primary Account's SAS ID

☐ Enable Shared SAS ID

Unified Payments



Use Primary Account's Payment

☐ Enable Unified Payments

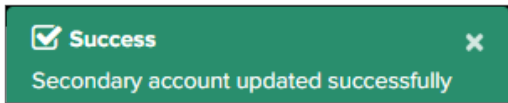
Please Note: Enabling Shared SAS ID will also enable Unified Payments

Update
Close

966 | Organizations for CBRS

Cambium cnMaestro Cloud | User Guide

5. The following message displays if successful.

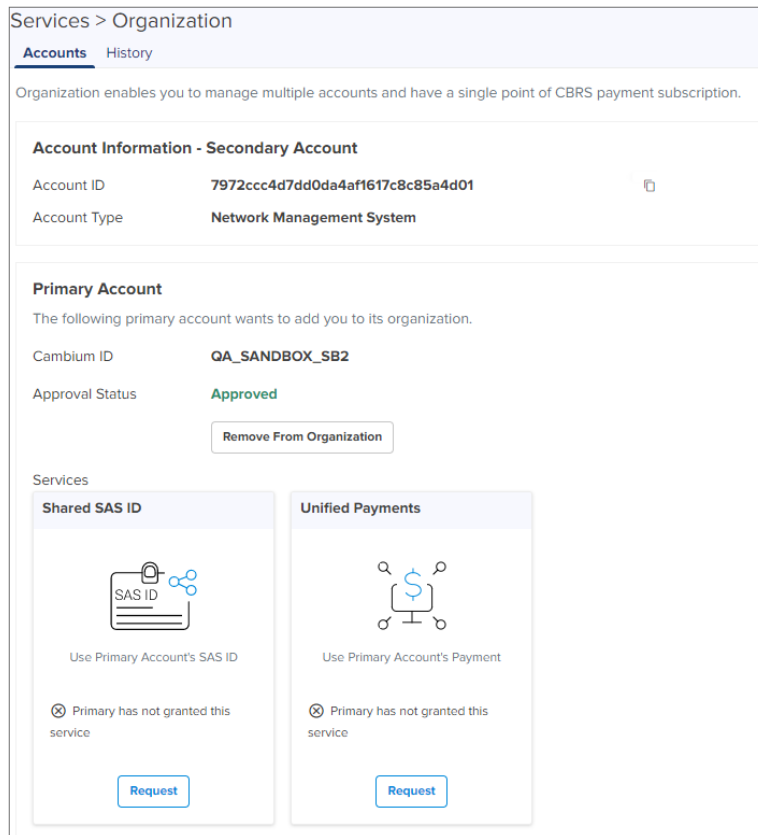


Request services from Secondary Account

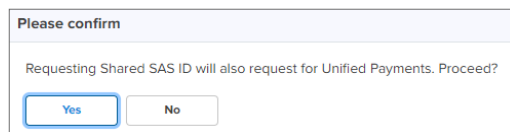
If the services are disabled, the Secondary Account needs to make a request to the Primary Account to activate them.

To request activation, perform the following on the Secondary Account:

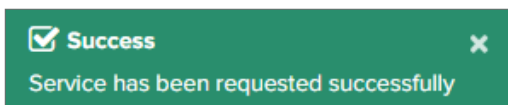
1. Navigate to **Network Services > Organization > Accounts**.
2. Click **Request**.



3. Click **Yes** in **Please confirm** window.



4. It displays the **Success** message as shown below:



5. Once requested, login to the **Primary Account** page and **Approve** the request.

The Primary Account administrator must approve this request from the Secondary Account in order to enable the services.

Review service request in Primary Account

Perform the following steps on the Primary Account.

1. Navigate to **Services > Secondary Accounts** tab.
2. Click **Review** in **Pending Service Request**.

There are some actions pending in the organization page. Please visit the link [Network Services -> Organization](#) to review.

Services > Organization

[Accounts](#) [History](#)

Organization enables you to manage multiple accounts and have a single point of CBRS payment subscription.

Account Information - Primary Account

Account ID 000676a3d5f9bea9d5b22b5a57063914

Account Type Network Management System

Secondary Accounts

Cambium ID	Account ID	Account Type	Approval Status	Enabled Services	Pending Service Request
DOCUMNETATION2	7972ccc4d7dd0da4af1617c8c85a4d01	NMS	Approved	-	Shared SAS ID, Unified Payments Review

[Add New](#)

3. The **Review** window pops up. Click **Approve**.

Review

Secondary Account ID

7972ccc4d7dd0da4af1617c8c85a4d01


Copy the Account ID from the secondary account

Cambium ID


DOCUMNETATION2

Services

Shared SAS ID




Use Primary Account's SAS ID


 Service has been requested.
Awaiting Primary Account's approval

[Approve](#) [Reject](#)


Unified Payments



Use Primary Account's Payment

 Service has been requested.
Awaiting Primary Account's approval

[Approve](#) [Reject](#)

 Please Note: Approving Shared SAS ID will also approve Unified Payments

[Close](#)

- Once approved, the requested services are enabled in the **Secondary Account**.


Review

Secondary Account ID
7972ccc4d7dd0da4af1617c8c85a4d01
Copy the Account ID from the secondary account

Cambium ID
DOCUMNETATION2

Services


Shared SAS ID



Use Primary Account's SAS ID

Service has been enabled

Unified Payments



Use Primary Account's Payment

Service has been enabled

Please Note: Approving Shared SAS ID will also approve Unified Payments

Close

Share CBRS Configuration with the On-Premises Instance



Note

Starting with version 3.0.3, cnMaestro supports synchronizing CBRS Configuration to On-Premises instance.

Once On-Premises is connected to the Anchor Account, the user can synchronize CBRS details (SAS ID, Token) to the cnMaestro On-Premises instance to register CBRS devices.

Manage Instances

Onboarding On-Premises Instances

Name	Type	Status	Last Connected	Onboarded	Uptime	CBRS Sync Status
cnMaestro	OVA	Online	May 28, 2021 14:38	May 12, 2021 21:20	0d 6h 48m	Sync Now

Showing 1 - 1 Total: 1

Services > CBRS

User must have an account in cnMaestro cloud anchor account prior to enabling CBRS services in On-Premises. As best practice, test the proxy configuration before saving.

Token

Sync From Cloud

Configure CBRS HTTP Proxy

☒ No HTTP Proxy

☐ cnMaestro as HTTP Proxy

☐ External HTTP Proxy (Recommended)

User can configure existing HTTP proxy as an external proxy or can configure new HTTP proxy with the help document. [Learn more](#)

Save Domain expiry test

- If the user shares (sync) CBRS details configured on Anchor account to connected On-Premises and if any devices are registered in On-Premises with different CBRS token or SAS ID it displays the deregister error as

shown below.

The screenshot shows the 'Manage Instances' interface with the 'On-Premises Instances' tab selected. A search bar is at the top left. A table lists instances with columns: Name, Type, Status, Last Connected, Onboarded, and Uptime. One instance, 'cnMaestro-184-64', is listed as 'OVA' and 'Online'. A 'Sync Now' button is next to it. A tooltip message says: 'There are some devices in registered state. Please deregister them before updating the token.' At the bottom right, it says 'Showing 1 - 1 Total: 1'.

Name	Type	Status	Last Connected	Onboarded	Uptime
cnMaestro-184-64	OVA	Online	Jun 11, 2021 16:58	Jun 11, 2021 16:58	0d 21h 31m

Organization History

In Organization History user can view changes to the Organization status over time. This includes details of Primary Account, Secondary Account, Action, Performed by, and Reason.

To view Organization History:

Navigate to **Network Services > Organization > History** tab.

Services > Organization

Accounts History

Primary Account	Secondary Account	Action	Performed by	Reason	Time
QA_SANDBOX_SB2	DOCUMNETATION2	Approved	DOCUMNETATION2		May 21 2021 07:20:15
QA_SANDBOX_SB2	DOCUMNETATION2	Added	QA_SANDBOX_SB2		May 21 2021 07:19:27
QA_SANDBOX_SB2	RAR_QA_SRV_3	Remove Approved	RAR_QA_SRV_3		May 21 2021 07:10:12
QA_SANDBOX_SB2	RAR_QA_SRV_3	Remove Requested	QA_SANDBOX_SB2	test	May 21 2021 06:48:31
QA_SANDBOX_SB2	RAR_QA_SRV_3	Approved	RAR_QA_SRV_3		May 21 2021 06:43:47
QA_SANDBOX_SB2	RAR_QA_SRV_3	Added	QA_SANDBOX_SB2		May 21 2021 06:43:38
QA_SANDBOX_SB2	DOCUMNETATION2	Removed	QA_SANDBOX_SB2	test	May 21 2021 06:39:22
QA_SANDBOX_SB2	DOCUMNETATION2	Approved	DOCUMNETATION2		May 20 2021 22:25:38
QA_SANDBOX_SB2	DOCUMNETATION2	Added	QA_SANDBOX_SB2		May 20 2021 21:45:44
QA_SANDBOX_SB2	DOCUMNETATION2	Removed	QA_SANDBOX_SB2	test	May 20 2021 21:44:44
QA_SANDBOX_SB2	DOCUMNETATION2	Added	QA_SANDBOX_SB2		May 20 2021 21:44:24
QA_SANDBOX_SB2	RAR_QA_SRV_3	Remove Approved	RAR_QA_SRV_3		May 20 2021 16:29:24
QA_SANDBOX_SB2	RAR_QA_SRV_3	Remove Requested	QA_SANDBOX_SB2	test	May 20 2021 16:27:03
QA_SANDBOX_SB2	RAR_QA_SRV_3	Approved	RAR_QA_SRV_3		May 19 2021 12:34:59
QA_SANDBOX_SB2	RAR_QA_SRV_3	Added	QA_SANDBOX_SB2		May 19 2021 12:34:40
QA_SANDBOX_SB2	RAR_QA_SRV_3	Remove Approved	RAR_QA_SRV_3		May 19 2021 12:33:26
QA_SANDBOX_SB2	RAR_QA_SRV_3	Remove Requested	QA_SANDBOX_SB2		May 19 2021 12:31:11

LTE

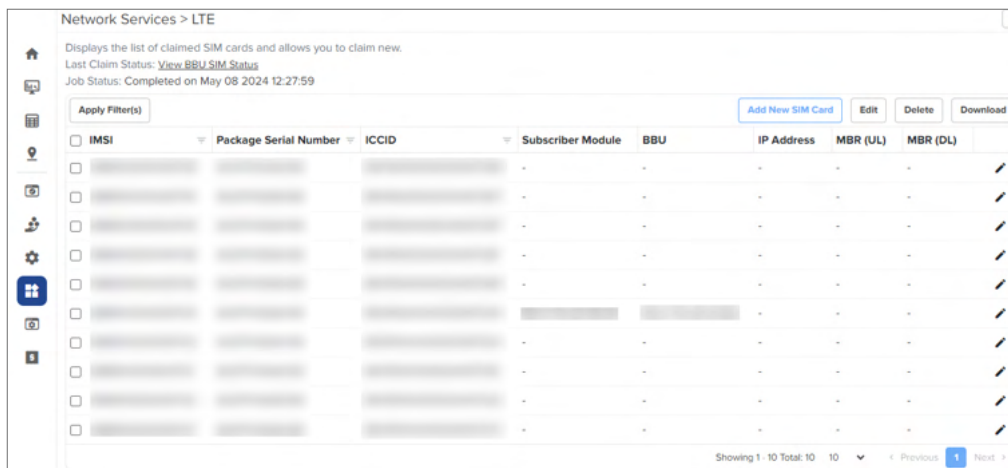
cnMaestro supports LTE as part of its cnMaestro deployment. LTE allows customers to onboard the SM with IMSI into cnMaestro.

System access in cnRanger is dependent on installation of SIM credentials on every BBU in the operator network. To ease the operations aspects of SIM card management, cnMaestro provides utilities for claiming, managing, and distributing Cambium Networks cnRanger SIM card credentials (3rd party SIM cards are not currently supported on cnRanger).

Adding SIM Cards

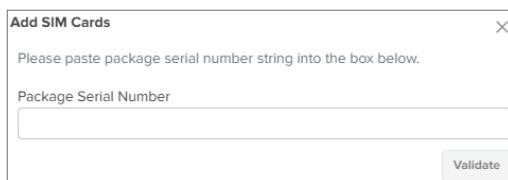
To add a SIM card, complete the following steps:

1. Navigate to **Network Services > LTE**.



The screenshot shows the 'Network Services > LTE' interface. It includes a sidebar with navigation icons, a main header with the title and a description: 'Displays the list of claimed SIM cards and allows you to claim new.' Below the header, there are status links: 'Last Claim Status: View BBU SIM Status' and 'Job Status: Completed on May 08 2024 12:27:59'. A table of SIM cards is displayed with columns: IMSI, Package Serial Number, ICCID, Subscriber Module, BBU, IP Address, MBR (UL), and MBR (DL). The table has 10 rows of data. At the bottom right, it says 'Showing 1 - 10 Total: 10' and has pagination controls for 'Previous', '1', and 'Next'.

2. Click **Add New SIM Card**. The following window appears.



The 'Add SIM Cards' dialog box has a title bar with a close button. The main text says 'Please paste package serial number string into the box below.' Below this is a text input field labeled 'Package Serial Number'. At the bottom right is a 'Validate' button.

3. Enter appropriate **Serial Number** of SIM package and click **Validate**.
4. After successful validation of the serial number, click **Add**.

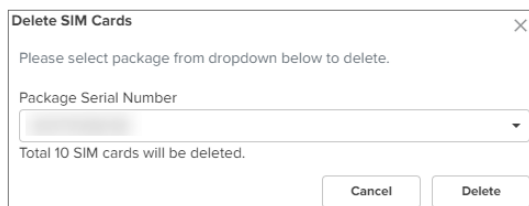


Note

User can download the .CSV file from the Cloud account once the Serial Number is validated from the cnMaestro Cloud database.

Delete SIM Cards

To delete a SIM card from the list, click **Delete**. The following window appears.



The 'Delete SIM Cards' dialog box has a title bar with a close button. The main text says 'Please select package from dropdown below to delete.' Below this is a dropdown menu labeled 'Package Serial Number'. Below the dropdown, it says 'Total 10 SIM cards will be deleted.' At the bottom are 'Cancel' and 'Delete' buttons.



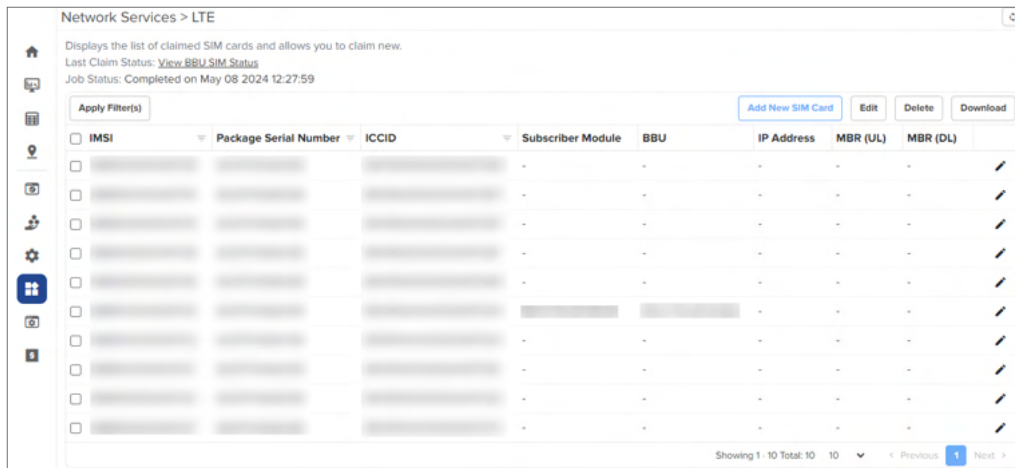
Note

IMSI numbers get deleted with the mapped Serial Number.

Update SIM Details


User can edit the SIM details as follows.

1. Navigate to **Network Services > LTE**.

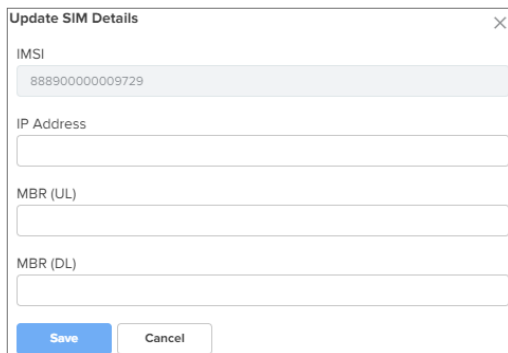


The screenshot shows the 'Network Services > LTE' interface. It includes a sidebar with navigation icons, a main header with a home icon and a description: 'Displays the list of claimed SIM cards and allows you to claim new.' Below this, it shows 'Last Claim Status: View BBU SIM Status' and 'Job Status: Completed on May 08 2024 12:27:59'. A table lists SIM cards with columns: IMSI, Package Serial Number, ICCID, Subscriber Module, BBU, IP Address, MBR (UL), and MBR (DL). Each row has an edit icon (pencil) on the right. At the bottom, it says 'Showing 1 - 10 Total: 10' and has 'Previous' and 'Next' buttons.

IMSI	Package Serial Number	ICCID	Subscriber Module	BBU	IP Address	MBR (UL)	MBR (DL)
			-	-	-	-	-
			-	-	-	-	-
			-	-	-	-	-
			-	-	-	-	-
			-	-	-	-	-
			-	-	-	-	-
			-	-	-	-	-
			-	-	-	-	-
			-	-	-	-	-

2. Click the edit () icon for the IMSI that you want to edit.

The **Update SIM Details** window pops-up.



The 'Update SIM Details' window is a modal form. It has a title bar with a close button (X). The form contains four input fields: 'IMSI' (pre-filled with '888900000009729'), 'IP Address', 'MBR (UL)', and 'MBR (DL)'. At the bottom, there are 'Save' and 'Cancel' buttons.

Update SIM Details

IMSI
888900000009729

IP Address

MBR (UL)

MBR (DL)

Save Cancel

3. Enter a valid **IP Address**.
4. Enter the **MBR (UL)** and **MBR (DL)**.
5. Click **Save**.

Viewing BBU SIM Status

Allows the users to view the status of the SIM connected to the BBU.

1. Navigate to **Network Services > LTE**.

Network Services > LTE

Displays the list of claimed SIM cards and allows you to claim new.
 Last Claim Status: [View BBU SIM Status](#)
 Job Status: Completed on May 08 2024 12:27:59

Apply Filter(s) [Add New SIM Card](#) [Edit](#) [Delete](#) [Download](#)

IMSI	Package Serial Number	ICCID	Subscriber Module	BBU	IP Address	MBR (UL)	MBR (DL)	
			-	-	-	-	-	
			-	-	-	-	-	
			-	-	-	-	-	
			-	-	-	-	-	
			-	-	-	-	-	
			-	-	-	-	-	
			-	-	-	-	-	
			-	-	-	-	-	
			-	-	-	-	-	
			-	-	-	-	-	

Showing 1 - 10 Total: 10 [Previous](#) [1](#) [Next](#)

2. Click **View BBU SIM Status**.

BBU SIM Status

Apply Filter(s)

Name	IP	MAC	State	Last Updated Time
S800-123	10.110.209.204		COMPLETE	May 08 2024 12:26:42

Showing 1 - 1 Total: 1 [Previous](#) [1](#) [Next](#)

Managing Edge Controller

This chapter provides the details about how Edge Controllers are configured to discover PTP 820/850 devices in a network using SNMP protocol. To view the onboarded Edge Controllers in cnMaestro, perform the following steps:

1. Navigate to **Network Services > Edge Controller**.

A list of onboarded Edge Controllers in a table format is displayed, as shown in [Figure 555](#).

Figure 555 Edge Controllers

Network Services > Edge Controller

Name	IP Address	Status	Managed Account	Version	Duration	Topology Sync
Centos-7	10.110.221.35	Online (19h 10m ago)	Base Infrastructure	1.0.0-b36	11d 9h 1m ago	Success (4m ago) Refresh Edit Delete
Centos-8	10.110.221.34	Online (7h 36m ago)	Base Infrastructure	1.0.0-b39	9h 57m ago	Success (< 1m ago) Refresh Edit Delete

Showing 1 - 2 Total: 2 [Previous](#) [1](#) [Next](#)

The following parameters are available to view in a table format: Name, IP Address, Status, Managed Account, Version, Duration, and Topology Sync Status. You can perform the following actions in the Edge Controller page.

- Topology Sync
- Edit
- Delete

Select the required Edge Controller name in the page, to perform the following actions:

- [Topology Sync](#)

- [Edit](#)
- [Delete](#)

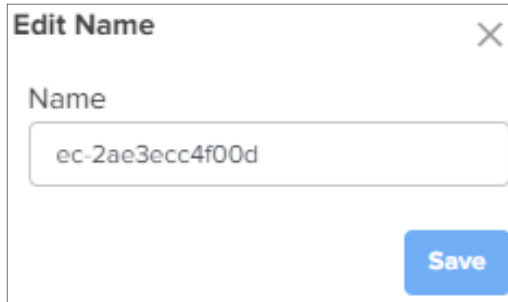
Topology Sync

Click on the **Topology Sync** (🔄) icon to run topology synchronization for the required Edge Controller.

Edit

1. Click the edit (✎) icon in the Edge Controller page.

The **Edit name** window appears, edit the name of the Edge Controller.



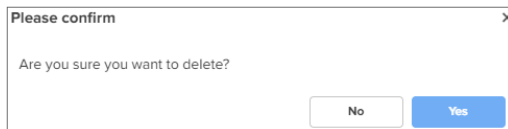
The 'Edit Name' dialog box has a title bar with 'Edit Name' and a close button (X). Inside, there is a label 'Name' above a text input field containing the text 'ec-2ae3ecc4f00d'. At the bottom right of the dialog is a blue button labeled 'Save'.

2. Click **Save**.

Delete

1. Click the delete (🗑) icon in the Edge Controller page.

The delete confirmation window appears.



The 'Please confirm' dialog box has a title bar with 'Please confirm' and a close button (X). Inside, it asks 'Are you sure you want to delete?'. At the bottom are two buttons: 'No' and 'Yes'.

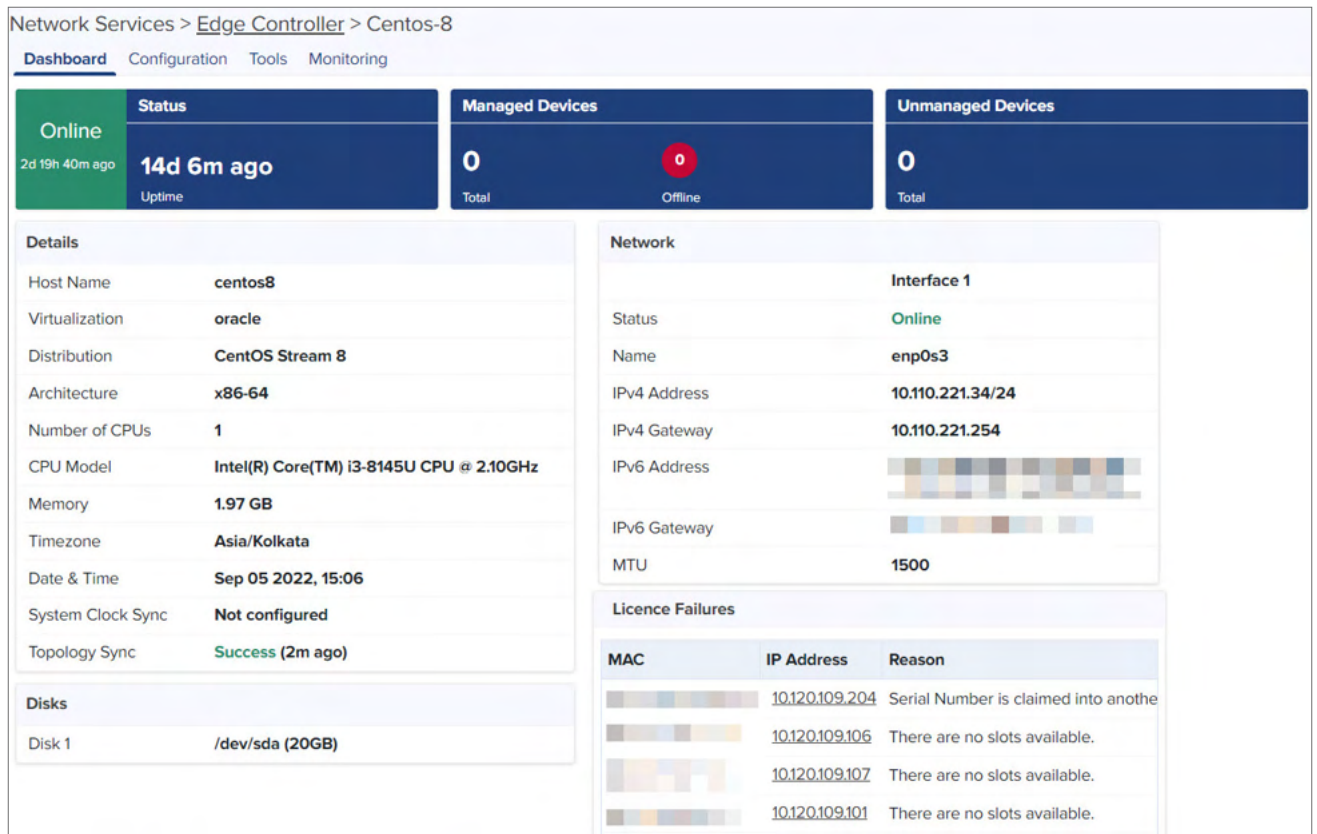
2. Click **Yes**.

In the Edge Controller page, you can navigate to the following tabs:

- [Dashboard](#)
- [Configuration](#)
- [Tools](#)
- [Monitoring](#)

To view the Edge Controller dashboard, click on the name of the Edge Controller. The Edge Controller dashboard page appears as shown in [Figure 556](#).

Figure 556 The Edge Controller dashboard



Dashboard

The dashboard page displays status of managed and unmanaged PTP 820/850 devices, details of Edge Controller, disk space availability, and network details of Edge Controller as shown in [Table 154](#).

Figure 557 Edge Controller and PTP 820/850 devices status

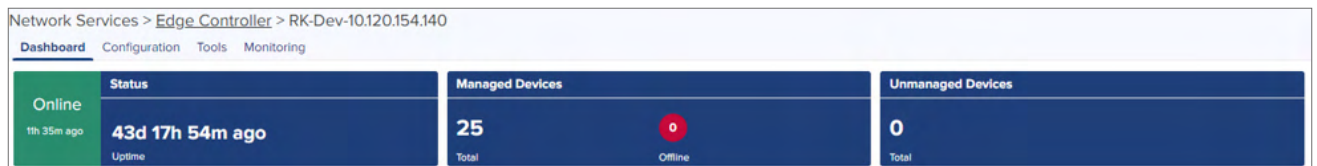


Table 154 Fields in the Edge Controller dashboard

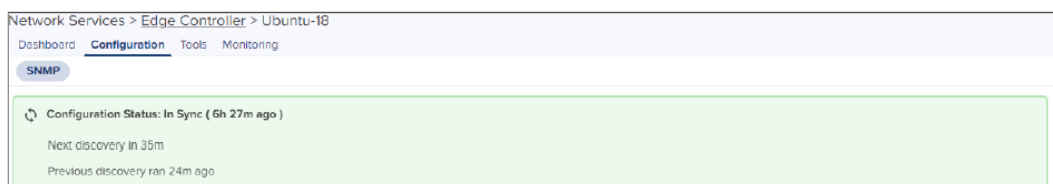
Field	Description
Host name	Name of the host.
Virtualization	Type of virtualization such as VMware or Oracle.
Distribution	Type of distribution such as Ubuntu and CentOS versions.
Architecture	CPU and Operating System installed.
Number of CPUs	Total number of CPUs utilized.
CPU Model	Type of CPU model.
Memory	Available memory.
Timezone	Current timezone.

Table 154 Fields in the Edge Controller dashboard

Field	Description
Date & Time	Current date and time.
System Clock Sync	Configuration of System Clock Synchronization.
Disk	Current Disk space usage.
Status	Status of Network Interface Online or Offline.
Name	Name of the Network Interface.
IPv4 Address	Configured IPv4 Address.
IPv4 Gateway	Configured IPv4 Gateway.
IPv6 Address	Configured IPv6 Address.
IPv6 Gateway	Configured IPv6 Gateway.
MTU	Maximum Transmission Unit of network interface of Edge Controller.
License Failures	Displays MAC, IP Address, and Reason. The reasons for license failure are as follows: When the discovery exceeds the slot availability. When the individual devices are already onboarded in other Cloud account.
Topology Sync	Status of Topology Sync.
Version	Software version of the device.

Configuration

In the **Configuration** page, you need to configure SNMP rules to discover and onboard PTP 820/850 devices. The **SNMP** tab in the **Configuration** page displays **Configuration Status**. The **Configuration Status** displays when the Edge Controller is **In Sync** or **Not Sync** with cnMaestro. The synchronization status is shown in days, hours and minutes. **Next discovery** and **Previous discovery** ran is displayed in minutes as shown in [Figure 558](#).

Figure 558 Configuration Status

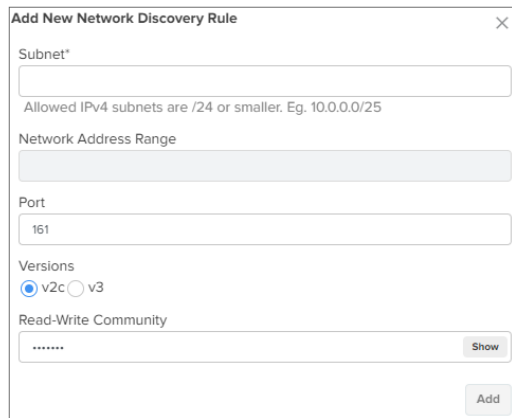
Rules

To add a new rule, perform the following steps:

1. Click **Add New**.



The **Add New Network Discovery Rule** window appears.



2. Type **Subnet** range in CIDR format (for example, 10.204.88.0/28) to discover PTP 820/850 devices.

The range of IP addresses in the **Network Address Range** field is displayed.

3. Type **Port** number.
4. Choose SNMP **Version**:

For SNMP version **v2c**, perform the following:

- a. Enter preferred community string when you create a SNMP discovery rule.
- b. Click **Add**.

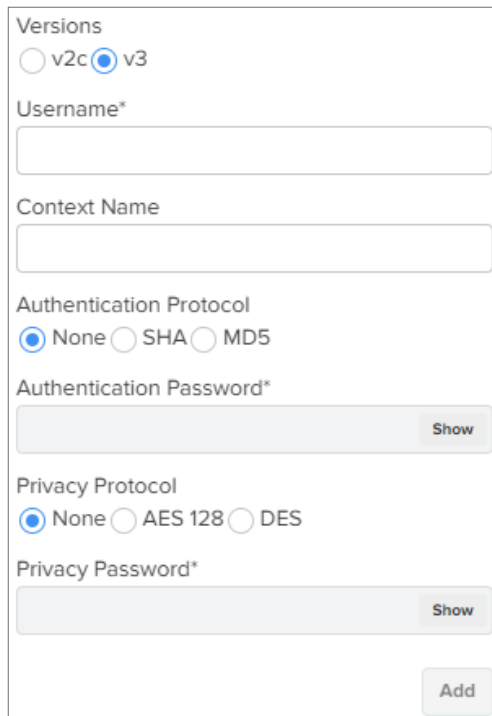


Note

Default community string is private.

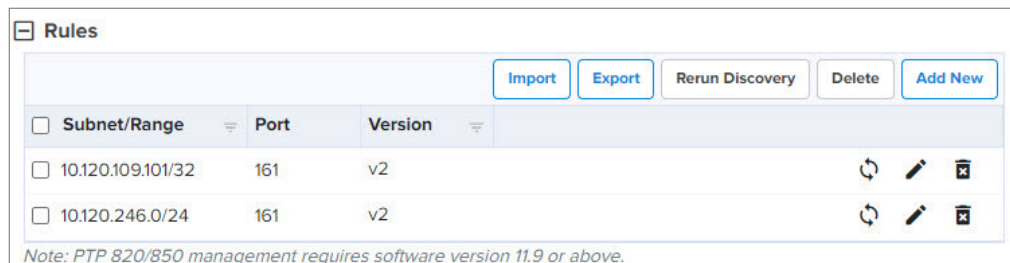
For SNMP Version **v3**, perform the following:

- a. Choosing SNMP v3 version allows you to enter the parameters as shown in the following figure.



- b. Enter the following fields:
 - **Username.**
 - **Context Name** field is optional.
- c. Choose any one of the **Authentication Protocol**.
 - None
 - SHA
 - MD5
- d. Choose any one of the **Privacy Protocol**.
 - None
 - AES128
 - DES
- e. Type **Privacy Password**.
- f. Click **Add**.

SNMP Rules added are listed in the Rules table as shown in the following figure.



<input type="checkbox"/> Subnet/Range	Port	Version	
<input type="checkbox"/> 10.120.109.101/32	161	v2	
<input type="checkbox"/> 10.120.246.0/24	161	v2	

Note: PTP 820/850 management requires software version 11.9 or above.

5. Click **Rerun Discovery** to start SNMP discovery for the rules added in the table or select specific **Subnet/Range** in the table and manually run **Rerun Discovery** () icon.

Import

To import SNMP rules, perform the following steps:

1. Click **Import**.
Import window appears.
2. Browse to **Select File** or **Download Sample Template** to change or configure the SNMP as per the requirements in **Downloaded Sample Template**.



Import

Upload a file (csv) as per the format specified in the template.

[Select File](#)

[Download Sample Template](#) [Import](#)

3. Click **Import**.

Export

To export SNMP rules, perform the following steps:

1. Select one or more SNMP rules required to export.
2. Click **Export**.

<input type="checkbox"/>	Subnet/Range	Port	Version
<input checked="" type="checkbox"/>	10.120.246.161/32	161	v2c

3. It exports the rules in the CSV file format as shown in the following figure.



Note

By default all SNMP rules are exported, if none of the rules are selected from the table.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	Subnet	Port	Version	Community	Username	Contextname	Authentication Protocol	Authentication P	Privacy Protocol	Privacy Password				
2	10.120.109.101/32	161		2 private										
3	10.120.246.0/24	161		2 private										

Delete

To delete SNMP rules in the table, perform the following steps:

1. Select one or more SNMP rules in the table.
2. Click **Delete**, to delete one or more entries in the table or click **Delete** (🗑️) icon to delete specific rule in the table.

Edit

To edit SNMP rule in the table, perform the following steps:

1. Click Edit (✎) icon to edit SNMP rule.

Edit Network Discovery Rule window appears. Edit the required field values.

Edit Network Discovery Rule

Subnet*
10.120.246.161/32
Allowed IPv4 subnets are /24 or smaller. Eg. 10.0.0.0/25

Network Address Range
10.120.246.161 - 10.120.246.161

Port
161

Versions
☒ v2c ☐ v3

Read-Write Community
..... Show

Save

2. Click **Save**.

Blacklist

To blacklist PTP 820/850 devices, perform the following steps:

1. Click **Add New**.

Add Blacklist IP Address window appears.

2. Type **IP Address**.
3. Click **Save**.

Blacklisted IP Addresses are displayed in the table.

4. Select one or more blacklisted IP addresses in the table.
5. Click **Delete**, to delete one or more entries in the table or click **Delete** (🗑️) icon to delete specific blacklist entry in the table.

Advanced Settings

In **Advanced Settings** section, configure the following parameters:



Note

- By default, **Auto Discovery** option is disabled.
- By default, **Auto Discovery Interval** option is 24 hours, when enabled and fields are auto-filled.

Enable **Auto Discovery** if you want to run SNMP discovery rules manually and perform the following steps:

1. Select **Auto Discovery Interval** option from the drop-down.
2. Enter **Timeout** in seconds between 5 to 60 seconds.
3. Enter **Retries** values between 0 and 3.

Advanced Settings

☒ Auto Discovery

Auto Discovery Interval (Hours)

1

Should be between 1 and 24 hours

Timeout (Seconds)

20

Should be between 5 and 60 seconds

Retries

1

Should be between 0 and 3

- Click **Save**.

Tools

The Tools page allows you to perform the following actions:

- [Diagnostics](#)
- [Operations](#)
- [Services](#)

Diagnostics

Diagnostics page allows you to gather technical support dump which can be downloaded and sent to Cambium Networks support team.

Technical Support Dump

The Technical Support Dump gathers important runtime and configuration information from the Edge Controller. It can be sent to Cambium Support to aid in resolving issues.

1. Navigate to **Edge Controller > Tools > Diagnostics**.
2. Click **Download** under Technical Support Dump.

Diagnostics

Network Services > **Edge Controller** > ec-2ae3ecc4f00d

Dashboard Configuration **Tools** Monitoring

Diagnostics Operations Services

Technical Support Dump

The technical support dump gathers important runtime and configuration information from your Edge Controller installation. It can be sent to Cambium Support to aid in resolving issues.

[Download](#)

Logging Severity

Change the logging severity level of Edge Controller to diagnose issues on the running system. The logging severity should be set to the default (Information) and it should only be changed under guidance of the technical support team.

Log Level

[Debug](#) [Save](#)

Service Logs

Select Service [Select Duration](#)

[Edge Agent](#) [Last 5 minutes](#)

[Show Logs](#)

Output

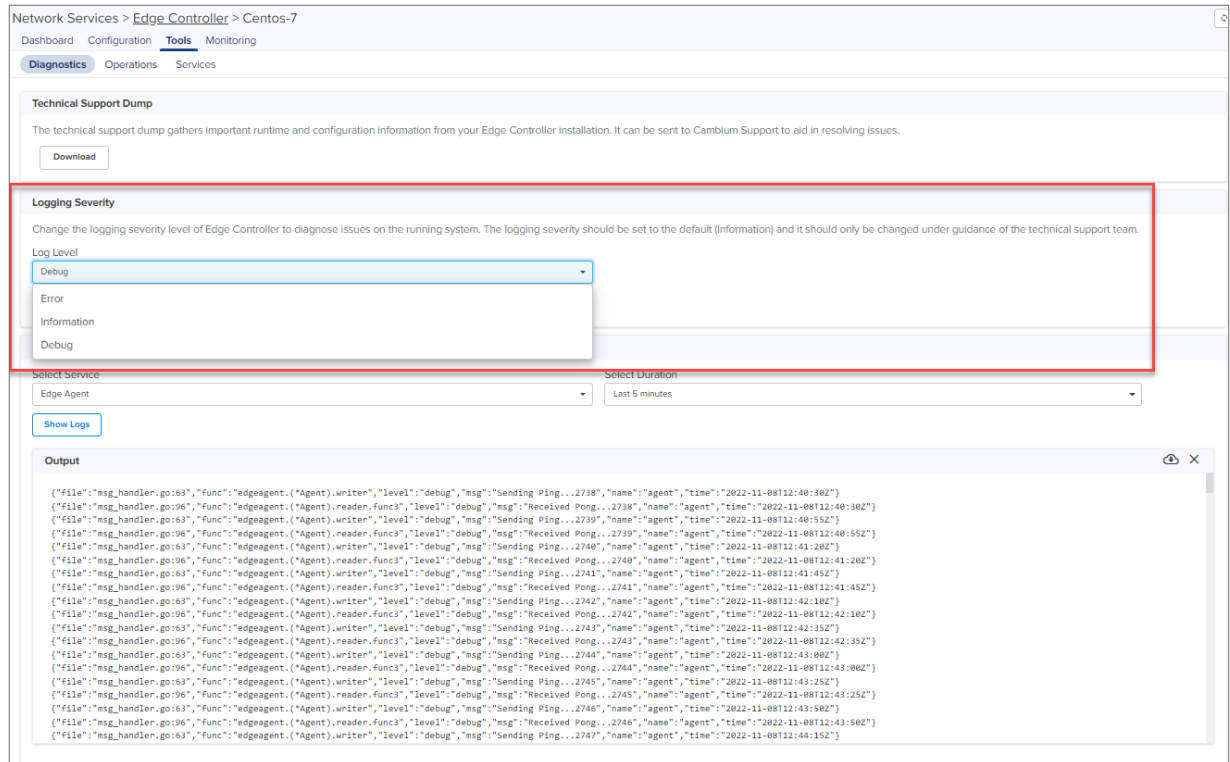
```
{
  "file": "msg_handler.go:63",
  "func": "edgeagent.(*Agent).writer",
  "level": "debug",
  "msg": "Sending Ping...4743",
  "name": "agent",
  "time": "2024-05-09T20:46:28Z"
}
{
  "file": "msg_handler.go:96",
  "func": "edgeagent.(*Agent).reader.func3",
  "level": "debug",
  "msg": "Received Pong...4743",
  "name": "agent",
  "time": "2024-05-09T20:46:28Z"
}
{
  "file": "msg_handler.go:63",
  "func": "edgeagent.(*Agent).writer",
  "level": "debug",
  "msg": "Sending Ping...4744",
  "name": "agent",
  "time": "2024-05-09T20:46:53Z"
}
{
  "file": "msg_handler.go:96",
  "func": "edgeagent.(*Agent).reader.func3",
  "level": "debug",
  "msg": "Received Pong...4744",
  "name": "agent",
  "time": "2024-05-09T20:46:53Z"
}
{
  "file": "msg_handler.go:63",
  "func": "edgeagent.(*Agent).writer",
  "level": "debug",
  "msg": "Sending Ping...4745",
  "name": "agent",
  "time": "2024-05-09T20:47:18Z"
}
{
  "file": "msg_handler.go:96",
  "func": "edgeagent.(*Agent).reader.func3",
  "level": "debug",
  "msg": "Received Pong...4745",
  "name": "agent",
  "time": "2024-05-09T20:47:18Z"
}
```

Logging Severity

The Logging Severity level of Edge Controller diagnose issues on the running system. The logging severity should be set to the default (Information) and it should only be changed under guidance of the technical support team.

1. Navigate to **Edge Controller > Tools > Diagnostics**.
2. In **Logging Severity** section, select one of the log level from **Log level** drop-down.
 - Error
 - Information

- Debug



3. Click **Save**.
4. Click **Reset** to revert to the previous **Log level** option.

Service Logs

The Service Logs allows you to diagnose any issues in the services running in the Edge Controller.

1. Select **Service** and **Duration** from the drop-down.

The following list of service and duration (5 minutes, 15 minutes, 30 minutes and last 1 hour) are available from the drop-down:

- Edge Agent
- Device SNMP
- Core Metadata
- Core Command
- RabbitMQ
- MariaDB
- SFTP

2. Click **Show Logs**.

The output for the selected criteria appears as shown:

Network Services > **Edge Controller** > Centos-7

Dashboard Configuration **Tools** Monitoring

Diagnostics Operations Services

Technical Support Dump

The technical support dump gathers important runtime and configuration information from your Edge Controller installation. It can be sent to Cambium Support to aid in resolving issues.

[Download](#)

Logging Severity

Change the logging severity level of Edge Controller to diagnose issues on the running system. The logging severity should be set to the default (Information) and it should only be changed under guidance of the technical support team.

Log Level
Debug

[Save](#) [Reset](#)

Service Logs

Select Service: Edge Agent

Select Duration: Last 5 minutes

```

{"file":"msg_handler.go:63","func":"edgeagent.(*Agent).reader.func1","level":"debug","msg":"Received Pong...2740","name":"agent","time":"2022-11-08T12:41:29Z"}
{"file":"msg_handler.go:63","func":"edgeagent.(*Agent).writer","level":"debug","msg":"Sending Ping...2741","name":"agent","time":"2022-11-08T12:41:45Z"}
{"file":"msg_handler.go:96","func":"edgeagent.(*Agent).reader.func1","level":"debug","msg":"Received Pong...2741","name":"agent","time":"2022-11-08T12:41:45Z"}
{"file":"msg_handler.go:63","func":"edgeagent.(*Agent).writer","level":"debug","msg":"Sending Ping...2742","name":"agent","time":"2022-11-08T12:42:10Z"}
{"file":"msg_handler.go:96","func":"edgeagent.(*Agent).reader.func1","level":"debug","msg":"Received Pong...2742","name":"agent","time":"2022-11-08T12:42:10Z"}
{"file":"msg_handler.go:63","func":"edgeagent.(*Agent).writer","level":"debug","msg":"Sending Ping...2743","name":"agent","time":"2022-11-08T12:42:35Z"}
{"file":"msg_handler.go:96","func":"edgeagent.(*Agent).reader.func1","level":"debug","msg":"Received Pong...2743","name":"agent","time":"2022-11-08T12:42:35Z"}
{"file":"msg_handler.go:63","func":"edgeagent.(*Agent).writer","level":"debug","msg":"Sending Ping...2744","name":"agent","time":"2022-11-08T12:43:00Z"}
{"file":"msg_handler.go:96","func":"edgeagent.(*Agent).reader.func1","level":"debug","msg":"Received Pong...2744","name":"agent","time":"2022-11-08T12:43:00Z"}
{"file":"msg_handler.go:63","func":"edgeagent.(*Agent).writer","level":"debug","msg":"Sending Ping...2745","name":"agent","time":"2022-11-08T12:43:25Z"}
{"file":"msg_handler.go:96","func":"edgeagent.(*Agent).reader.func1","level":"debug","msg":"Received Pong...2745","name":"agent","time":"2022-11-08T12:43:25Z"}
{"file":"msg_handler.go:63","func":"edgeagent.(*Agent).writer","level":"debug","msg":"Sending Ping...2746","name":"agent","time":"2022-11-08T12:43:50Z"}
{"file":"msg_handler.go:96","func":"edgeagent.(*Agent).reader.func1","level":"debug","msg":"Received Pong...2746","name":"agent","time":"2022-11-08T12:43:50Z"}
{"file":"msg_handler.go:63","func":"edgeagent.(*Agent).writer","level":"debug","msg":"Sending Ping...2747","name":"agent","time":"2022-11-08T12:44:15Z"}

```

3. Click download (📄) icon to download the generated output.
4. Click clear (✕) icon to clear the output.

Operations

In the **Operations** page, you can view the current software version of the Edge Controller. You can also view history of the last five software updates.

1. Navigate to **Tools > Operations**.
2. Click **Check for new software update**, checks for any new available software update.

Network Services > **Edge Controller** > Centos-8

Dashboard Configuration **Tools** Monitoring

Diagnostics **Operations** Services

Software Update

New Software version is available (1.0.0-b35). [Update](#)

History

Date and Time	Status	Version
Wed Aug 03 2022 20:12:54 UTC +0530	Success	1.0.0-b34
Tue Aug 02 2022 19:51:08 UTC +0530	Success	1.0.0-b33
Mon Aug 01 2022 09:47:13 UTC +0530	Success	1.0.0-b32
Fri Jul 15 2022 18:23:21 UTC +0530	Success	1.0.0-b30
Tue Jul 12 2022 19:25:36 UTC +0530	Success	1.0.0-b29

Services

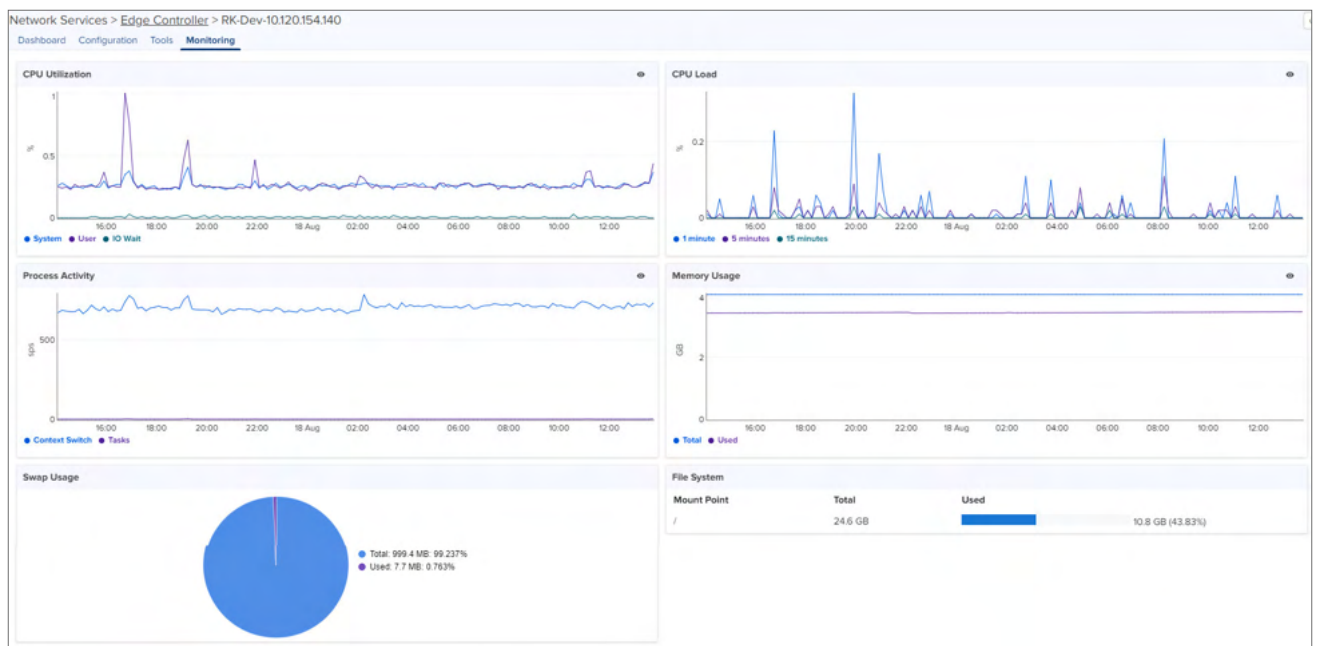
In **Services** page you can view the services running in the Edge Controller.

Figure 559 *Services*

Network Services > Edge Controller > RK-Dev-10.120.154.140					
Dashboard Configuration Tools Monitoring					
Diagnostics Operations Services					
Name	Version	Status	Uptime	CPU	Memory
ec-rabbitmq	3.10.5	Running	41d 19h 10m	0.27%	3.23% [127.6MiB]
ec-device-snmp	1.0.0-b37	Running	31d 20h 38m	0.02%	1.45% [57.29MiB]
ec-core-command	1.0.0-b7	Running	41d 19h 10m	0.00%	0.19% [7.566MiB]
ec-edgeagent	1.0.0-b35	Running	4d 19h 20m	0.04%	0.27% [10.7MiB]
ec-mariadb	10.6.8	Running	41d 19h 10m	0.01%	2.65% [104.5MiB]
ec-core-metadata	1.0.0-b8	Running	41d 19h 10m	0.00%	0.28% [11.2MiB]
ec-sftp	v1.3	Running	34d 21h 42m	0.00%	0.15% [5.883MiB]

Monitoring

In the **Monitor** page, you can view details of CPU utilization, CPU Load, Process Activity, Memory Usage, Swap Usage, and File System.



cnArcher Installation Summary

cnArcher is a mobile application used to install PMP Subscriber Modules (SMs), ePMP (SMs), and cnRanger SMs. The installation summary provides an overview of the data collected by cnArcher during the installation process.



Note

- cnArcher Installation Summary is a cnMaestro X feature.
- cnArcher Installation summary of PMP SM is available for users in cnMaestro Cloud and OnPremises from 3.1.0 release.
- cnArcher Installation summary of ePMP SM is available for users in cnMaestro Cloud and OnPremises from 3.1.1 release.
- ePMP PTP 550 (two radio devices) and ePMP Elevate are not supported for cnArcher Installation

Summary.

To view the installation summary:

1. Navigate to **Network Services > cnArcher Installation Summary**.
The **cnArcher Installation Summary** page appears.
2. You can **Search** cnArcher Summary details by using **MAC Address**, **Name at Installation**, **Date and Time**, **Added By**, and **Comments**.

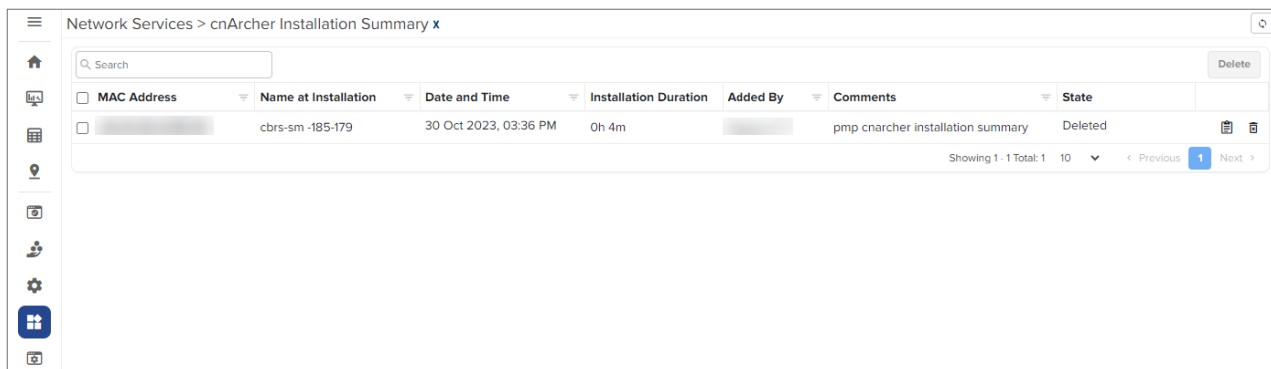


Table 155 *Fields in cnArcher Installation Summary*

Field	Description
MAC Address	MAC address of the device.
Name at Installation	Name given to the device when installed.
Date and Time	Date and time of installation.
Installation Duration	Duration of installation.
Added By	Name of the user adding the device.
Comments	Comments about the installation.
State	Current state of the device such as Managed or Deleted.

3. Click **View Details**  icon to view detailed Installation Summary.

Installation Summary : cbrs-sm -185-179 on 30 Oct 2023, 03:36 PM

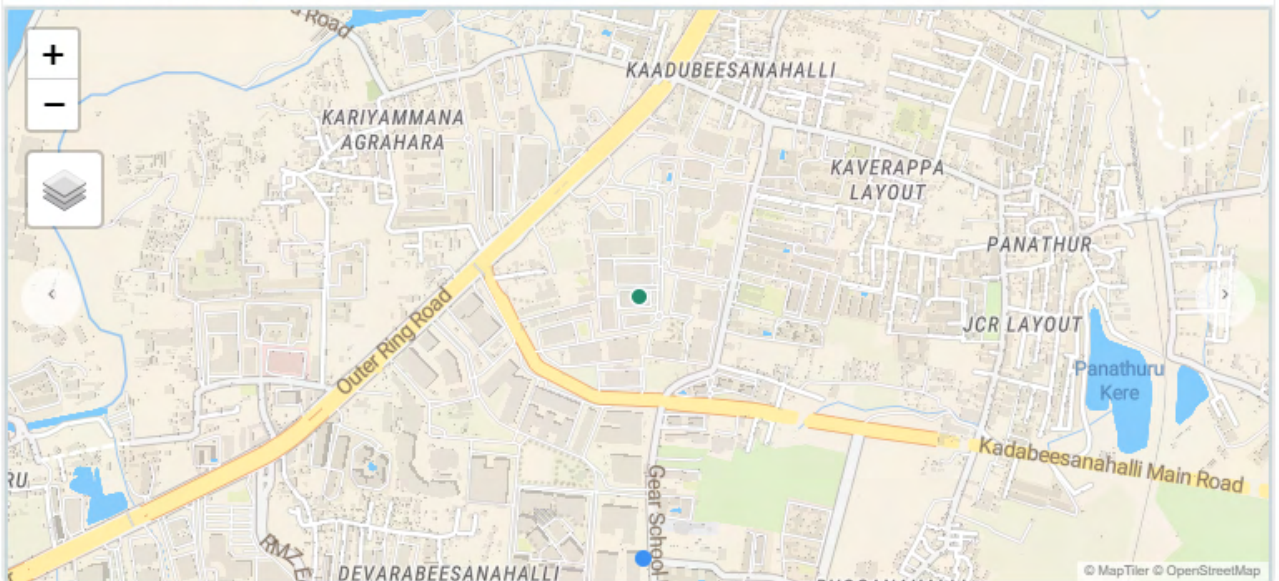
Summary

SM Name	cbrs-sm -185-179
MAC Address	
MSN	
Product	PMP 450 SM 3.6 GHz
Software Version	CANOPY 22.1 SM
RSSI	-35.4 dBm
SSR	1.4
External Antenna	No External Antenna
Start Timestamp	30 Oct 2023, 03:32 PM
End Timestamp	30 Oct 2023, 03:36 PM
Added By	
Comment	pmp cnarcher installation sum...

Configuration

IP Address/Setting	/Static
Subnet	
Gateway	
DNS	
Management VLAN	Not Configured
Data VLAN	Not Configured
Security	none
PSK	-
Status	Already Onboarded
Software Update	Not Configured
Template	Not Configured
Onboarding Details	SM was already cloud manag...

Photos & Location: Map



Link Test Result

Time	Mode	Throughput Uplink/Downlink	Modulation Uplink/Downlink
30 Oct 2023, 03:35 PM	Extrapolated	1.7 Mbps / 38.5 Mbps	8 X / -

AP Scan Result

AP MAC	AP Bandwidth	AP Frequency	Registered
	30 MHz	3580.0 MHz	Yes

Table 156 *Summary fields in cnArcher Installation*

Field	Description
SM Name	Name of the device.
MAC Address	MAC address of SM.
MSN	Serial number of device.
Product	Device model and type.
Software Version	Software version of device.
RSSI	Receiver Signal Strength Indicator (RSSI) of SM.
SSR	Signal Strength Ratio (SSR).
External Antenna	Peak gain of external antenna connected to the device.
Start Timestamp	Start time of the summary.
End Timestamp	End time of the summary.
Added By	Name of the user adding the device.
Comment	Comments about the installation process.

Configuration

Table 157 *Configuration fields in cnArcher Installation*

Field	Description
IP Address/Setting	IP settings such as for DHCP or Static IP allocation.
Subnet	Subnet mask of the device.
Gateway	IP address of the gateway.
DNS	Name of the DNS server.
Management VLAN	Configured Management VLAN.
Data VLAN	Configured Data VLAN.
Security	Security settings.
PSK	Type of PSK (Pre-Shared Key): WPA or WPA2.
Status	Current SM state such as Onboarded or Already Onboarded.
Software Update	Software version provided to upgrade.
Template	Name of the configuration template to apply.
Onboarding Details	Onboarding details related to SM.

Photos and Location

Photos and Location displays the photos taken during installation. You can view a maximum of four photos at a time.

Link Test Result

Link Test Result displays the link related test results with respect to throughput.

Table 158 *Link Test Results fields*

Field	Description
Time	Time at which the link test was performed.
Mode	Modes such as Extrapolated Link Test or Link Test with Bridging.
Throughput Uplink/Downlink	Uplink and Downlink Throughput.
Modulation Uplink/Downlink	Uplink and Downlink Modulation.

AP Scan Result

AP Scan Result displays a list of scanned APs.

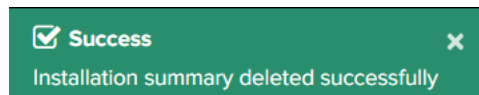
Table 159 *Fields in AP Scan Result*

Field	Description
AP MAC	MAC address of the AP.
AP Bandwidth	Bandwidth of the AP.
AP Frequency	Frequency of the AP.
Registered	Details of the registered SM.

1. Click the delete (🗑️) icon to delete single or multiple entries from the **cnArcher Installation Summary** page.
2. Click **Yes** to delete.

Please confirm
Are you sure you want to delete?

3. A confirmation message is displayed on a successful delete.



Note

cnArcher uploads Installation Summary with cnMaestro when Internet connection is available to users mobile device. This feature is support only in Android.

Spectrum Analyzer^X

The Spectrum Analyzer feature monitors and analyzes wireless spectrum for PMP AP and SM devices, allowing users to optimize network performance.



Note

- The Spectrum Analyzer is a cnMaestro X feature.
- Spectrum Analysis is supported on devices running PMP software version 22.1.0 and above.
- Spectrum Analyzer feature is available for users in cnMaestro Cloud and On-Premises.

To view Spectrum Analyzer page:

1. Navigate to **Network Services > Spectrum Analyzer**.
2. You can view the Spectrum Analyzer details by using **Name, Status, Type, Sector Count, Start Time, and End Time**.

Network Services > Spectrum Analyzer x

Apply Filter(s) [Add New](#) [Set Alarm Threshold](#) [Delete](#)

<input type="checkbox"/>	ID	Name	Status	Type	Sector Count	Start Time	End Time	
<input type="checkbox"/>	30	sa	● Scheduled	Daily	3	10 May 2024, 12:12 PM	-	
<input type="checkbox"/>	29	dw	● Completed	Now	1	06 May 2024, 12:50 P...	06 May 2024, 12:57 PM	
<input type="checkbox"/>	28	DP	● Completed	Now	3	06 May 2024, 12:22 P...	06 May 2024, 12:31 PM	
<input type="checkbox"/>	26	cfew	● Completed	Now	2	06 May 2024, 11:54 AM	06 May 2024, 12:08 P...	
<input type="checkbox"/>	25	safari	● Scheduled	Daily	1	10 May 2024, 03:17 PM	-	
<input type="checkbox"/>	24	check sa	● Completed	Now	7	12 Apr 2024, 10:24 AM	12 Apr 2024, 10:38 AM	
<input type="checkbox"/>	23	12sa	● Completed	Daily	9	09 Apr 2024, 03:14 PM	10 Apr 2024, 04:55 PM	
<input type="checkbox"/>	22	SA	● Completed	Now	8	27 Mar 2024, 12:12 PM	27 Mar 2024, 12:26 PM	
<input type="checkbox"/>	21	alarm	● Completed	Now	5	19 Mar 2024, 10:48 AM	19 Mar 2024, 11:02 AM	
<input type="checkbox"/>	20	1	● Completed	Now	2	05 Mar 2024, 11:20 AM	05 Mar 2024, 11:26 AM	

Showing 1 - 10 Total: 19 10 < Previous 1 2 Next >

Table 160 Fields in Spectrum Analyzer

Field	Description
Name	The user-defined name for the spectrum analysis job or scan.
Status	The current status of the spectrum analysis.
Type	The type of analysis performed (for example, Now, Weekly).
Sector Count	The number of sectors or wireless areas analyzed in the spectrum scan.
Start Time	The scheduled start time for the spectrum analysis job.
End Time	The scheduled end time for the spectrum analysis job.

3. Click **View Result** icon on top right corner to view the detailed Spectrum Analyzer summary.

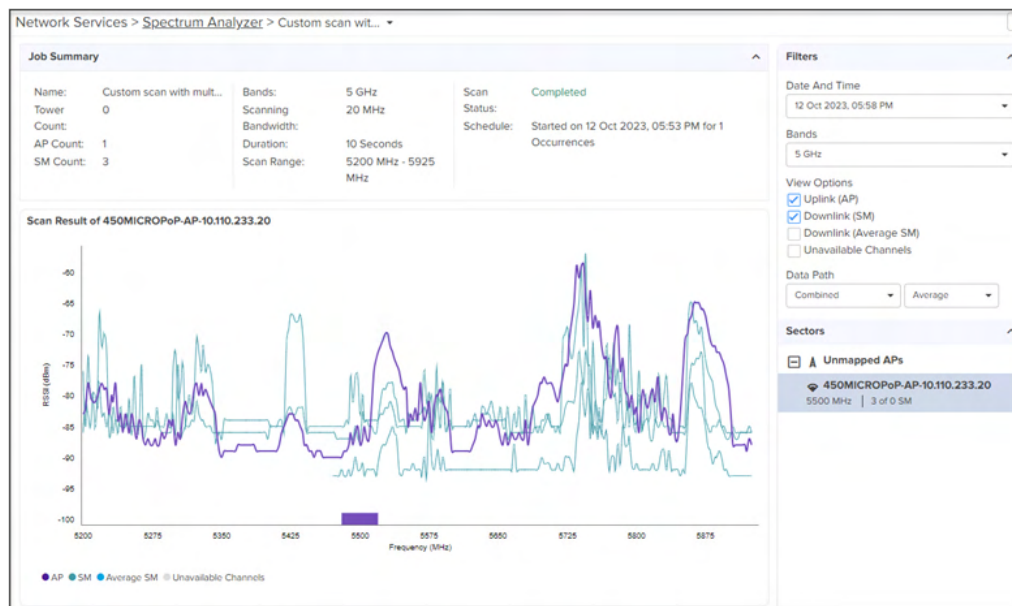


Table 161 *Job Summary parameters*

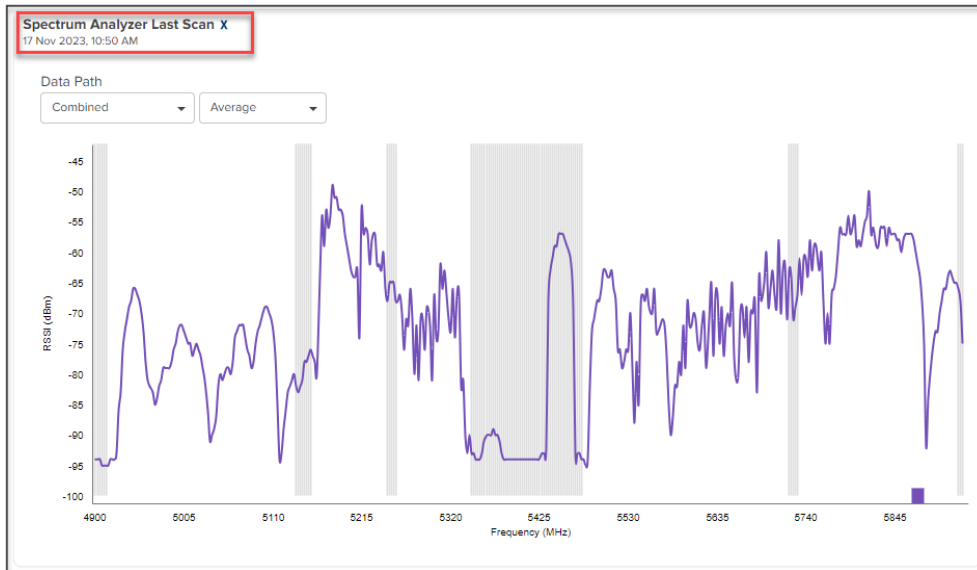
Field	Description
Name	The user-assigned name for the analysis job.
Tower Count	The number of towers included in the analysis.
AP Count	The number of APs in the analysis.
SM Count	The number of SMs in the analysis.
Bands	The frequency bands under analysis.
Scanning Bandwidth	The width of the frequency band being scanned.
Duration	The duration of the analysis job.
Scan Range	The spectrum range analyzed.
Scan Status	The current status of the analysis job.
Schedule	The scheduling details for the analysis job.

Table 162 *Filters parameters*

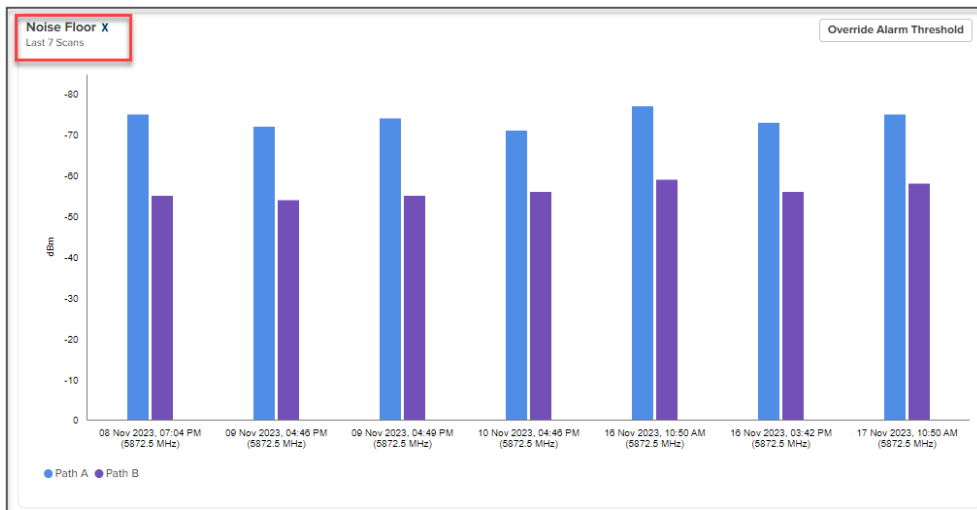
Field	Description
Date and Time	The specific date and time when the spectrum analysis is conducted.
Bands	The frequency bands included in the analysis.
View Options	<p>The viewing options for analyzing the spectrum.</p> <ul style="list-style-type: none"> • Uplink (AP) • Downlink (SM) • Downlink (Average SM) • Unavailable Channels
Data Path	<p>The data path used for the analysis.</p> <ul style="list-style-type: none"> • Combined: Combines data from Path A and Path B for analysis. • Average: Calculates the average and maximum values for the analysis data.


4. **Scan Result** displays the scanning result graph.
5. To view the last scan results at the device level:

- a. Navigate to PMP device **Dashboard > Spectrum Analyzer Last Scan**.



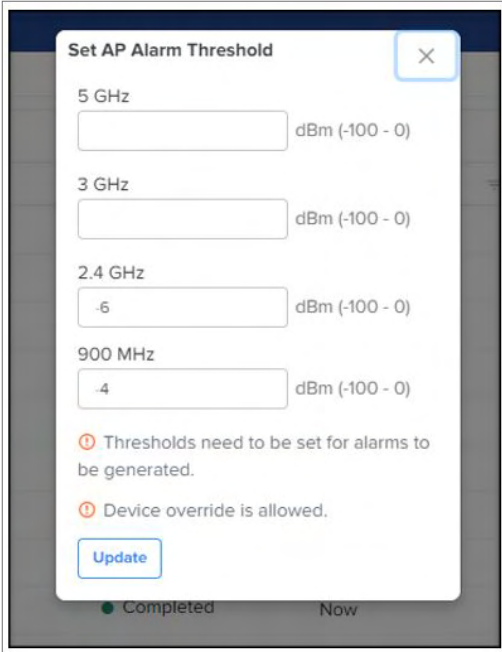
- b. The dashboard automatically generates the appropriate graph for AP and SM based on the device type.
- c. The default data path for displayed graphs is **Combined**, and users can customize it to their preferences.
- d. The dashboard displays **Noise Floor**, which provides noise floor information for both **Path A** and **Path B**. These two graphs are displayed for both AP and SM that are part of the scan.



- e. **Unmapped APs** display any APs that are not assigned to a tower.
- f. Click **Delete**  icon on the top right corner to delete a job.

To set Alarm Threshold:

1. Navigate to **Network Services > Spectrum Analyzer**.
2. Click on the **Set Alarm Threshold** on the top right corner of the Spectrum Analyzer page.



Set AP Alarm Threshold [X]

5 GHz
 dBm (-100 - 0)

3 GHz
 dBm (-100 - 0)

2.4 GHz
 dBm (-100 - 0)

900 MHz
 dBm (-100 - 0)

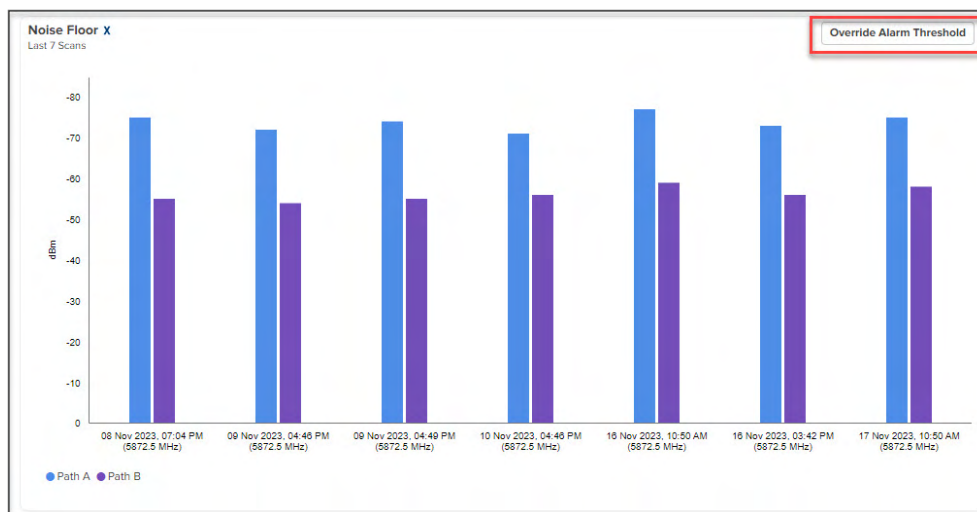
ⓘ Thresholds need to be set for alarms to be generated.

ⓘ Device override is allowed.

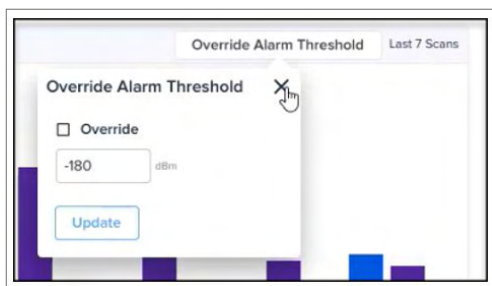
[Update](#)

Completed Now

3. Users can set band-specific alarms by configuring threshold values and alarm triggers for specific frequency bands (for example, 5 GHz, 3 GHz, 2.4 GHz, and 900 MHz).
4. These alarms are applied globally to all PMP devices operating in the same frequency band.
5. After configuration, the alarms are displayed on the alarm page, enabling easy monitoring and timely responses to network issues.
6. User can override alarm threshold for AP at the device level:
 - a. Navigate to **Dashboard > Override Alarm Threshold**.



- b. Before overriding, users can review the global alarm threshold values that apply to the entire network.



- c. Choose the specific AP device for which you want to set custom alarm thresholds.
- d. Configure and set individual threshold values for the selected device, overriding the global thresholds only for that specific device.


To create a new job:

1. Navigate to **Network Services > Spectrum Analyzer**.
2. Click on **Add New** on the top right corner of the Spectrum Analyzer page.

Table 163 Add Spectrum Scan parameters

Field	Description
Name	Job name to distinguish the analysis job within the Spectrum Analyzer.
Schedule	<p>Scheduling options, including:</p> <ul style="list-style-type: none"> • Now: Immediate execution of the spectrum analysis. • Daily: Set up a daily schedule for the analysis job. • Weekly: Configure a weekly schedule for the analysis job. • Monthly: Create a monthly schedule for the analysis job.
Scan Range	The desired scan range from a drop-down with two options:

Table 163 *Add Spectrum Scan parameters*

Field	Description
	<ul style="list-style-type: none">• Full Scan: Performs a comprehensive analysis of the entire spectrum.• Custom Scan: Set the Min Frequency and Max Frequency to precisely choose the frequency range for a more accurate spectrum analysis.
Scanning Bandwidth	<div>The specific scanning bandwidth from the available options to adjust the spectrum analysis.</div> <div>Note Scanning Bandwidth is not applicable for PMP 450m AP.</div>
Duration	The analysis duration in seconds, ranging from 10 to 1000 seconds.

3. After creating the job, it appears on the home page with a **Scheduled** status.

Administration

This section includes the following topics:

- [Managing Users](#)
- [Cloud Anchor Account](#)
- [Settings](#)
- [Audit Logs](#)

Users

This chapter provides the following details:

- [Managing Users](#)
- [Session Management](#)

Managing Users

cnMaestro allows you to add Users using the **Administration > Users** page.



Note

- cnMaestro X account supports up to 200 users.
- cnMaestro Essentials account supports only up to 10 users.

Figure 560 Adding Users

Username	Invited Email	Role	Email	Status
		Administrator		Active
		Super Administrator		Active
		Super Administrator		Active
		Super Administrator		Active
		Monitor		Active
		Super Administrator		Active
		Administrator		Active
		Administrator		Active
		Monitor		Active
		CPI		Invited

Role-Based Access

cnMaestro supports the following user Roles:

- **Super Administrator** – Super Administrators can perform all operations.
- **Administrator** – Administrators can modify cnMaestro application functionality, but they are not able to edit User, API, or Server configuration.
- **Operator** – Operators are able to configure device-specific parameters and view all configuration.
- **Monitor** - Monitors have only the view access.
- **CPI** - CPI can perform onboarding the devices using the CBRS tool and has the view access only.



Note

- cnMaestro allows one to limit the number of concurrent sessions for each Role and display current active user sessions.
- CPI role is authorized only when the **CBRS** is Enabled.

Role-Mappings

The table below defines how Roles are authorized to access specific features.

Table 164 *Role-Mappings*

Feature	Description
Access Control Policies	<p>Configure policies to control users connectivity to the network.</p> <ul style="list-style-type: none"> • Super Administrator - All • Administrator - All • Operator - All • Monitor - None • CPI - None
Application Operations	<p>Application level operations such as to create, update and delete operations for Networks, Towers/Sites. Bulk device configuration.</p> <ul style="list-style-type: none"> • Super Administrator - All • Administrator - All • Operator - None • Monitor - None • CPI - None
Application Settings	<p>Change global application configuration and onboarding key.</p> <ul style="list-style-type: none"> • Super Administrator - All • Administrator - All • Operator - None • Monitor - None • CPI - None
Assists	<p>Scan device configurations and generate assists scores, which in turn helps in isolating configuration issues in a deployment.</p> <ul style="list-style-type: none"> • Super Administrator - All • Administrator - All

Table 164 *Role-Mappings*

Feature	Description
	<ul style="list-style-type: none"> • Operator - All • Monitor - All (Fix Now is not allowed) • CPI - All (Fix Now is not allowed)
Citizen Broadband Radio Service Subscription (CBRS)	<p>Support CBRS-compliant devices in the 3.6 GHz band (from 3550 MHz to 3700 MHz)</p> <ul style="list-style-type: none"> • Super Administrator - All • Administrator - All • Operator - None • Monitor - None • CPI - All
cnArcher Installation Summary	<p>View installation summary of PMP ePMP, and cnRanger SMs installed using the cnArcher Mobile Application.</p> <ul style="list-style-type: none"> • Super Administrator - All • Administrator - All • Operator - All • Monitor - None • CPI - View
Configuration/Software Update	<p>Manage configuration/software update jobs.</p> <ul style="list-style-type: none"> • Super Administrator - All • Administrator - All • Operator - All • Monitor - None • CPI - None
Custom Applications	<p>Configure applications with a specific IP address or a domain name, and apply filter rules.</p> <ul style="list-style-type: none"> • Super Administrator - All • Administrator - All • Operator - All • Monitor - None • CPI - None
Device Operations	<p>Device operations such as reboot device, link test, connectivity test, tech support file download, and Wi-Fi performance test.</p> <ul style="list-style-type: none"> • Super Administrator - All • Administrator - All • Operator - All

Table 164 *Role-Mappings*

Feature	Description
	<ul style="list-style-type: none"> • Monitor - None • CPI - None
Device Overrides	<p>Per-device configuration, including updating AP Group and applying configuration.</p> <ul style="list-style-type: none"> • Super Administrator - All • Administrator - All • Operator - All • Monitor - None • CPI - None
EasyPass	<p>Create captive portal using EasyPass to allow clients to access the network through Free Tiers, Vouchers, or Paid Access types.</p> <ul style="list-style-type: none"> • Super Administrator - All • Administrator - All • Operator -View • Monitor - View (Sessions Only) • CPI - None
Floor Plan	<p>Floor Plan configuration</p> <ul style="list-style-type: none"> • Super Administrator - All • Administrator - All • Operator - View • Monitor - View • CPI - None
Global Configuration	<p>The ability to create and apply configuration for global features such as Templates, WLANs, AP Groups, and bulk sync configuration.</p> <ul style="list-style-type: none"> • Super Administrator - All • Administrator - All • Operator -View • Monitor - None • CPI - None
Guest Portal	<p>Guest Portal configuration.</p> <ul style="list-style-type: none"> • Super Administrator - All • Administrator - All • Operator -View • Monitor - View (Sessions Only) • CPI - None

Table 164 *Role-Mappings*

Feature	Description
LTE	Manage cnRanger LTE devices. <ul style="list-style-type: none">• Super Administrator - All• Administrator - All• Operator - View and Edit SIM credentials only• Monitor - None• CPI - None
Monitoring	Display of monitoring data at all levels. <ul style="list-style-type: none">• Super Administrator - All• Administrator - All• Operator - All• Monitor - View• CPI - View
Notifications	Alarms and Events management. <ul style="list-style-type: none">• Super Administrator - All• Administrator - All• Operator - All• Monitor - View• CPI - View
Onboarding	Device approval, modifying individual device configuration, and performing software update. <ul style="list-style-type: none">• Super Administrator - All• Administrator - All• Operator - All• Monitor - None• CPI - All
Reporting	Report generation. <ul style="list-style-type: none">• Super Administrator - All• Administrator - All• Operator - All• Monitor - All• CPI - All
Session Management	Capability to view and logout other users sessions. <ul style="list-style-type: none">• Super Administrator - All• Administrator - All

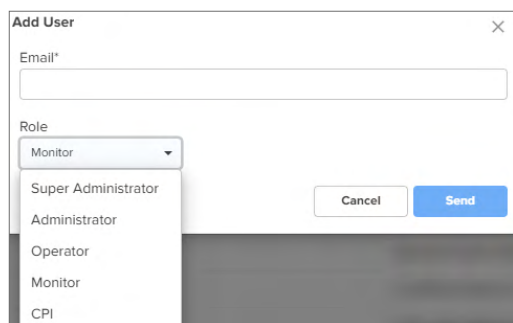
Table 164 *Role-Mappings*

Feature	Description
	<ul style="list-style-type: none">• Operator - None• Monitor - None• CPI - None
Software Upgrade	Upgrade the device with the latest software. <ul style="list-style-type: none">• Super Administrator - All• Administrator - All• Operator - All• Monitor - None• CPI - None
Spectrum Analyzer	Analyze and monitor wireless spectrum for optimizing network performance on PMP devices. <ul style="list-style-type: none">• Super Administrator - All• Administrator - All• Operator - All• Monitor - None• CPI - None
User Management	User management operations such as manage users and roles. <ul style="list-style-type: none">• Super Administrator - All• Administrator - View• Operator - None• Monitor - None• CPI - None

Creating Users and Configuring User Roles

To add an administrator:

1. Navigate to **Administration > Users** page.
2. Click **Add User** button. The following window is displayed:



The screenshot shows a modal window titled "Add User" with a close button (X) in the top right corner. Inside the window, there is an "Email*" label above a text input field. Below the input field is a "Role" label and a dropdown menu. The dropdown menu is open, showing a list of roles: "Monitor" (which is the selected option), "Super Administrator", "Administrator", "Operator", "Monitor", and "CPI". At the bottom right of the window, there are two buttons: "Cancel" and "Send".

3. Enter the email address in the **Email** box.

4. To configure the User Role, select any one of the role for the user from the **Role** drop-down list:

- Super Administrator
- Administrator
- Operator
- Monitor
- CPI

5. Click **Send** button to add this user.

To edit or delete a user, click the Edit icon or the Delete icon against the user in the **Administration > Users** page.

Whitelisting specific domains

Using the **Administration > Users** page, you can allow (or whitelist) a specific domain (for example, gmail.com). When users from the whitelisted (or allowed) domain are added, an invite email is sent directly to them. When the users accept the invite, they are allowed to access a particular cnMaestro UI account.

You can also blacklist or disallow a specific domain to prohibit all users of that domain from accessing the UI account.



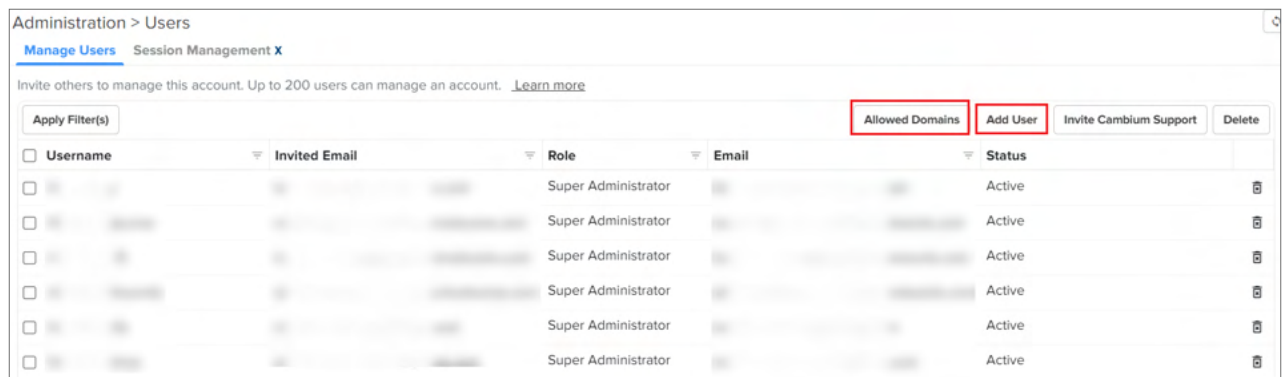
Note

- Domain whitelisting is not applicable to NFR User accounts.
- For users from the whitelisted domains, you can create the MSP user account.

To whitelist or blacklist a specific domain, perform the following steps:

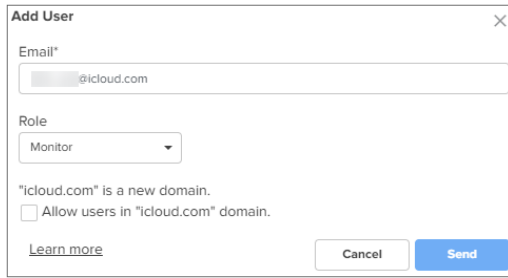
1. Navigate to **Administration > Users** page.

The **Manage Users** page appears.



2. To add a new domain (for example, a gmail ID), click on the **Add User** button.

The **Add User** window appears. You must set the fields, as described in the [Creating Users and Configuring User Roles](#) section. The **Add User** window also displays that the email ID used is a new domain, as shown in the following example (in this case, gmail.com is the new domain):



Add User

Email*

Role
 Monitor

"icloud.com" is a new domain.
☐ Allow users in "icloud.com" domain.

[Learn more](#) Cancel Send

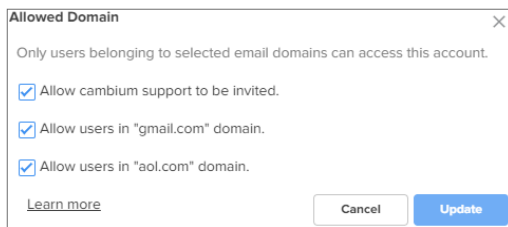
3. Select the **Allow users in "gmail.com" domain** check box (the domain name varies based on the email ID you add).

The new domain is added to the database.

When users who belong to this allowed domain (for example, gmail.com) are added (using the **Add User** button), an invite email is directly sent to the users. When the users accept the invite, they can access a particular cnMaestro UI account. The **Allow users in "gmail.com" domain** checkbox is available only when you are adding a new domain.

4. To blacklist or disallow a specific domain, click on the **Allowed Domains** button on the **Manage Users** page.

The **Allowed Domain** window appears with a list of whitelisted domains.



Allowed Domain

Only users belonging to selected email domains can access this account.

☒ Allow cambium support to be invited.

☒ Allow users in "gmail.com" domain.

☒ Allow users in "aol.com" domain.

[Learn more](#) Cancel Update

5. Uncheck the required domain check box to blacklist that specific domain.
6. 1. Select **Update**.

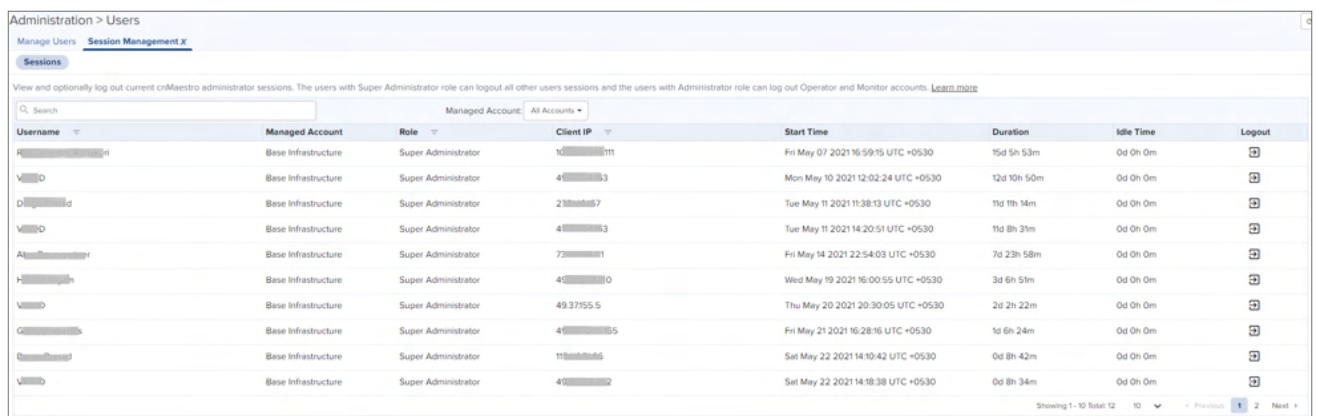
All users from that blacklisted domain are not allowed to access the UI. To allow the blacklisted domain, you must check the required domain check box on the **Allowed Domain** window.

Session Management

View and optionally log out current cnMaestro administrator sessions. The users with Super Administrator role can logout all other users sessions and the users with Administrator role can logout Operator and Monitor accounts.

Sessions

Displays the detailed information on the user sessions.



Username	Managed Account	Role	Client IP	Start Time	Duration	Idle Time	Logout
F...	Base Infrastructure	Super Administrator	10...	Fri May 07 2021 16:59:15 UTC +0530	15d 5h 53m	0d 0h 0m	[Logout]
V...	Base Infrastructure	Super Administrator	4...	Mon May 10 2021 12:02:24 UTC +0530	12d 10h 50m	0d 0h 0m	[Logout]
D...	Base Infrastructure	Super Administrator	2...	Tue May 11 2021 11:38:13 UTC +0530	11d 11h 14m	0d 0h 0m	[Logout]
V...	Base Infrastructure	Super Administrator	4...	Tue May 11 2021 14:20:51 UTC +0530	11d 8h 31m	0d 0h 0m	[Logout]
A...	Base Infrastructure	Super Administrator	7...	Fri May 14 2021 22:54:03 UTC +0530	7d 23h 58m	0d 0h 0m	[Logout]
H...	Base Infrastructure	Super Administrator	4...	Wed May 19 2021 16:00:55 UTC +0530	3d 6h 51m	0d 0h 0m	[Logout]
V...	Base Infrastructure	Super Administrator	49.37755.5	Thu May 20 2021 20:30:05 UTC +0530	2d 2h 22m	0d 0h 0m	[Logout]
C...	Base Infrastructure	Super Administrator	4...	Fri May 21 2021 16:28:16 UTC +0530	1d 6h 24m	0d 0h 0m	[Logout]
P...	Base Infrastructure	Super Administrator	11...	Sat May 22 2021 14:10:42 UTC +0530	0d 8h 42m	0d 0h 0m	[Logout]
V...	Base Infrastructure	Super Administrator	4...	Sat May 22 2021 14:18:38 UTC +0530	0d 8h 34m	0d 0h 0m	[Logout]

Showing 1-10 Total 12 Previous 1 2 Next

Cloud Anchor Account

This chapter provides the following details:

- [Manage Instances](#)
- [Inventory](#)
- [Administration](#)
- [Network Services](#)
- [Manage Subscriptions](#)

Manage Instances

Registration of On-Premise customer accounts to Cloud is addressed by this feature. This will allow us to do many synchronization things in On-Premises instances, similar to Cloud will have the inventory stats from instances.

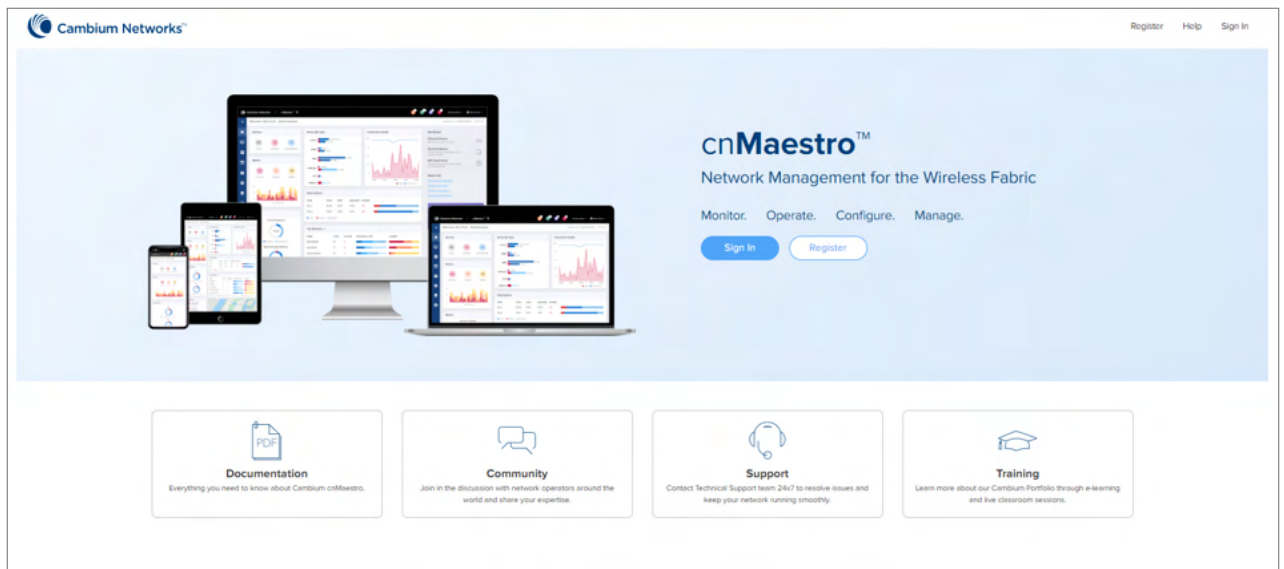
Manage Instances describes the following

- Onboarding
- On-Premises Instances
- Notifications

Onboarding

To onboard the devices to the Cloud Anchor Account, you need to create the Cloud account before connecting to cnMaestro On-Premises:

1. Log in to the cnMaestro UI, <https://cloud.cambiumnetworks.com>.



2. In **Account Type**, select **Anchor**.

Create a New Cloud Account

A Cloud Account allows you to manage your devices. Create an account for your company.

You can also be invited to manage an existing account - contact the administrator of the account to receive an email invitation.

Cambium ID*

Create a Cambium ID. For example: ACME_Broadband_Inc

The Cambium ID is a string that uniquely identifies this account. It consists of letters, numbers, and underscores, and it is used to onboard devices. It is also written to devices managed by cnMaestro (and can be accessed in their UI). Once set, the Cambium ID can only be changed by contacting Cambium Support.

Friendly Name*

A friendly name for this account. This could be the name of the company.

Country*

India

The country where devices in this account are located.

Time Zone

Est:GMT+12 (UTC 12:00)

The time zone used to calculate daily statistics.*

Account Type*

NMS
Use cnMaestro cloud for device management

Anchor
Host a copy of cnMaestro in your own data center, connected to this account.

Select the type of account. If you plan to host private copies of cnMaestro in your data center, then select the Anchor choice. This account will allow your local cnMaestro servers to connect to the cnMaestro Cloud to simplify firmware upgrades, license management etc.

Onboarding Key*

Please enter the Onboarding Key

Allow cnMaestro On-Premises instances to onboard into this account. You need to add the Cambium ID and onboarding key through cnMaestro On-Premises UI.

☐ I agree to the [cnMaestro Terms of Service](#).

[Create Account](#) [Cancel](#)

3. Enter the On-Premises **Onboarding Key**.
4. Click I agree to the cnMaestro **Terms of Service**.
5. Click **Create Account**.
6. When the Anchor Account is created, an Onboarding Key must be set to allow On-Premises instances to connect.
7. Navigate to the **Manage Instances** page as shown below and allows you to change the **Onboarding Key** and **Disable Onboarding**.

This key needs to be entered in the cnMaestro On-Premises UI to connect to the Anchor Account.

Manage Instances

[Onboarding](#) [On-Prem Instances](#) [Notifications](#)

Allow cnMaestro On-Premises instances to onboard into this account.
You need to add the Cambium ID and onboarding key through cnMaestro On-Premises instance UI.

Cambium ID: HKR_SRV_6_ANCHOR

[Change Onboarding Key](#) [Disable Onboarding](#)

On-Premises Instances

Once the On-Premises server has been onboarded with the Key, it will be included in the **On-Prem Instances** page. Multiple On-Premises installations can be added to a single Anchor Account.

Manage Instances

Onboarding **On-Prem Instances** Notifications

Search

Name	Subscription	Expiring In	Type	Active Version	Status	Last Connected	Onboarded	Uptime	
500-X-Trail-228	Essentials	N/A	OVA	5.0.0-b64	Online	Jan 18, 2024 21:...	0d 12h 11m ago	0d 15h 46m	
221-226-320	cnMaestro X	15 days	OVA	3.2.0-r7	Online	Jan 12, 2024 14:...	6d 19h 17m ago	6d 19h 32m	
310-...SRV-221-230	N/A	N/A	OVA	3.1.0-r3	Online	Jan 09, 2024 23:...	9d 11h 6m ago	31d 19h 16m	
NOC-222-410	cnMaestro X	15 days	OVA	4.1.0-r3	Online	Jan 12, 2024 14:31	6d 19h 36m ago	8d 20h 54m	
Restored-229	Essentials	N/A	OVA	5.0.0-b64	Online	Jan 18, 2024 18:...	0d 15h 40m ago	0d 15h 45m	
221-225	cnMaestro X	15 days	OVA	5.0.0-b64	Online	Jan 18, 2024 18:...	0d 15h 40m ago	0d 15h 46m	
231-NOC-410r3-upgraded	cnMaestro X	15 days	OVA	4.1.0-r3	Online	Jan 10, 2024 17:...	8d 17h 3m ago	15d 15h 17m	

Showing 1 - 7 Total: 7 10 < Previous 1 Next >

By clicking the instance host name, you can see the On-Premises server details such as General, Features, System, and CBRs:

Cambium Networks | cnMaestro™ X

Manage Instances

Onboarding **On-Prem Instances** Notifications

Search

Name	Subscription	Expiring
500-X-Trail-228	Essentials	N/A
221-226-320	cnMaestro X	15 days
310-...SRV-221-230	N/A	N/A
NOC-222-410	cnMaestro X	15 days
Restored-229	Essentials	N/A
221-225	cnMaestro X	15 days
231-NOC-410r3-upgraded	cnMaestro X	15 days

310-...SRV-221-230 Details

General Features System Devices

Name 310-...SRV-221-230

Status Online

Onboarded Jan 09, 2024 23:01

Uptime 31d 19h 17m

Last Connected Jan 09, 2024 23:01

Type OVA

Account View Access and Backhaul

Country India

CPI Users -

cnMaestro Users 1

Active OVA Version 3.1.0-r3

Active Package Version -

Showing 1 - 7 Total: 7 10 < Previous 1 Next >

Notifications

Notification page displays the history of the most recent events notification of On-Premises instances with **Severity, Source, Name, Raised Time, and Message**.

Manage Instances

Onboarding On-Prem Instances **Notifications**

Apply Filter(s) Export

Severity	Source	Name	Message	Raised Time
Notify	NOC-222-410	ONPREM_SUBSCRIPTION_FEATURE_STATE_CHANGE	Activated feature - cnMaestro X	18 Jan 2024, 10:39 PM
Critical	500-X-Trail-228	ONPREM_SUBSCRIPTION_FEATURE_STATE_CHANGE	Deactivated cnMaestro X. Data will be retained for 90 days	18 Jan 2024, 10:11 PM
Critical	Restored-229	ONPREM_SUBSCRIPTION_FEATURE_STATE_CHANGE	Deactivated cnMaestro X. Data will be retained for 90 days	18 Jan 2024, 10:10 PM
Notify	500-X-Trail-228	ONPREM_SUBSCRIPTION_FEATURE_STATE_CHANGE	Activated feature - cnMaestro X	18 Jan 2024, 10:02 PM
Notify	500-X-Trail-228	ONBOARDING	Onboarded.	18 Jan 2024, 09:56 PM
Notify	500-X-Trail-228	CLOUD_SYNC_STATUS_UP	Cloud sync is up	18 Jan 2024, 09:56 PM
Critical	500-X-Trail-228	ONPREM_SUBSCRIPTION_FEATURE_STATE_CHANGE	Deactivated cnMaestro X. Data will be retained for 90 days	18 Jan 2024, 09:51 PM
Notify	Restored-229	ONPREM_SUBSCRIPTION_FEATURE_STATE_CHANGE	Activated feature - cnMaestro X	18 Jan 2024, 09:38 PM
Critical	Restored-229	ONPREM_SUBSCRIPTION_FEATURE_STATE_CHANGE	Deactivated cnMaestro X. Data will be retained for 90 days	18 Jan 2024, 09:34 PM
Critical	NOC-222-410	ONPREM_SUBSCRIPTION_FEATURE_STATE_CHANGE	Deactivated cnMaestro X. Data will be retained for 90 days	18 Jan 2024, 09:22 PM

Showing 1 - 10 Total: 640 10 < Previous 1 2 3 4 5 ... 64 Next >

Click View Details to view the Event Details as shown below:

Event Details

X

Severity	Notify
Message	Activated feature - cnMaestro X
Event Time	18 Jan 2024, 10:02 PM
Source	500-X-Trail-228
Category	INFRASTRUCTURE
Offline Reason	-
Age	0d 12h 1m

<

>

Inventory

The **Inventory** page displays a list of devices under the selected Node. It presents health and maintenance information provides a tabular view that allows for sorting and filtering. When selected for a single device, it presents a detailed customized page of that device.

Inventory										
Apply Filter(s)		Managed Account: All Accounts				Import		Delete		Actions
Device	MAC Address	Managed Account	Type	IPv4 Add...	IPv6 Address	Status	Serial Number	Description	Onboard Duration	Active S/W Version
PMP 450i RV1		Base Infrastructure	PMP 450i AP	172.10.0.219	-	Online (2d 9h 46m)			0d 9h 1m	21.0
SM - PMP 450i		Base Infrastructure	PMP 450i SM	172.10.0.229	-	Online (0d 8h 48m)			0d 9h 4m	23.0
V5K DN-3039		MSP	60 GHz crWave V5000 DN	-	fd18:10f:5bb:18000:1	Online (2d 3h 30m)			0d 10h 34m	1.3.3
V5K DN-3050		MSP	60 GHz crWave V5000 DN	-	fd18:10f:5bb:18003:1	Online (2d 3h 30m)			0d 10h 34m	1.3.3
PoP 300C		MSP	60 GHz crWave V5000 DN (PoP)	-	fd18:10f:5bb:18002:1	Online (2d 3h 30m)			0d 10h 34m	1.3.3
V5K DN-3130		MSP	60 GHz crWave V5000 DN	-	fd18:10f:5bb:18001:1	Online (2d 3h 30m)			0d 10h 34m	1.3.3
V2k d		MSP	60 GHz crWave V3000 DN	-	fd18:10f:5bb:14:1	Online (2d 3h 30m)			0d 10h 34m	1.3.3
PoP V5K		MSP	60 GHz crWave V5000 DN (PoP)	-	fd18:10f:5bb:11:1	Online (1d 2h 59m)			0d 10h 34m	1.3.3
CN V1K		MSP	60 GHz crWave V1000 CN	-	fd18:10f:5bb:1:1	Online (1d 7h 36m)			0d 10h 34m	1.3.3
V1K CN-047		MSP	60 GHz crWave V1000 CN	-	fd18:10f:5bb:12:1	Online (2d 3h 30m)			0d 10h 34m	1.3.3

Administration

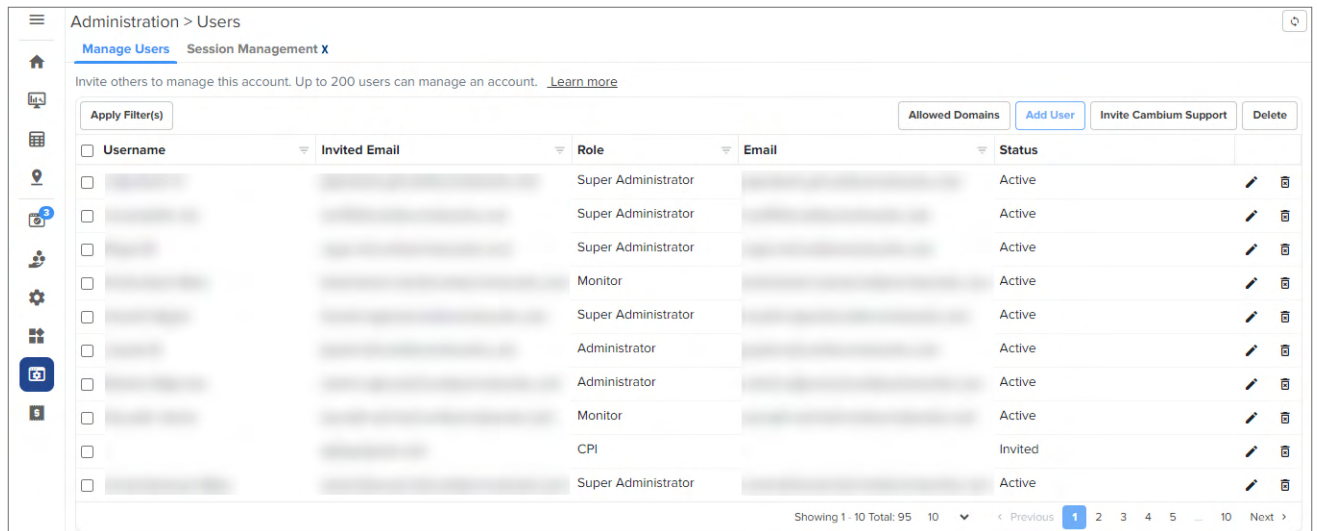
Administration provides the following details:

- Users
- Audit Logs

Users

cnMaestro allows to add Users using the **Administration > Users** page. A maximum of ten users are currently allowed in the system.

Figure 561 Adding Users



Username	Invited Email	Role	Email	Status
		Super Administrator		Active
		Super Administrator		Active
		Super Administrator		Active
		Monitor		Active
		Super Administrator		Active
		Administrator		Active
		Administrator		Active
		Monitor		Active
		CPI		Invited
		Super Administrator		Active

Role-Based Access

On successful authentication, every request from this user is processed in light of their Role.

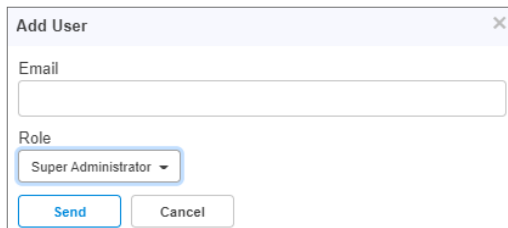
cnMaestro supports the user Role:

- **Super Administrator** – Super Administrators can perform all operations.

Creating Users and Configuring User Roles

To add an administrator:

1. Navigate to **Administration > Users** page.
2. Click **Add User** button. The following window is displayed:



Add User [X]
Email

Role
Super Administrator

3. Enter the ID in the **Email** text box.
4. Click **Send** button to add this user.

To delete, click the delete icon against the user in the **Administration > Users** page.

Session Management

View and optionally log out current cnMaestro administrator sessions. The users with Super Administrator role can logout all other users sessions and the users with Administrator role can log out Operator and Monitor accounts.

Administration > Users

Manage Users **Session Management X**

Sessions

View and optionally log out current cnMaestro administrator sessions. The users with Super Administrator role can logout all other users sessions and the users with Administrator role can log out Operator and Monitor accounts. [Learn more](#)

Q Search

Username	Role	Client IP	Start Time	Duration	Logout
auto admin	Super Administrator		Mon Dec 19 2022 13:13:45 UTC +0530	0d 7h 17m	
auto admin	Super Administrator		Mon Dec 19 2022 14:03:29 UTC +0530	0d 6h 28m	
	Super Administrator		Mon Dec 19 2022 13:14:34 UTC +0530	0d 7h 17m	
	Super Administrator		Mon Dec 19 2022 15:14:06 UTC +0530	0d 5h 17m	
	Super Administrator		Mon Dec 19 2022 12:18:11 UTC +0530	0d 8h 13m	
	Super Administrator		Mon Dec 19 2022 11:31:44 UTC +0530	0d 8h 59m	
	Super Administrator		Mon Dec 19 2022 12:13:17 UTC +0530	0d 8h 18m	
	Super Administrator		Mon Dec 19 2022 08:40:32 UTC +0530	0d 11h 51m	
	Super Administrator		Mon Dec 19 2022 10:31:47 UTC +0530	0d 9h 59m	
	Super Administrator		Tue Dec 13 2022 17:03:41 UTC +0530	6d 3h 27m	

Showing 1 - 10 Total: 11 10 < Previous 1 2 Next >

Network Services

Network Services provide the following details:

- CBRS
- Organization

CBRS

Citizens Broadband Radio Service subscription for the CBRS-compliant devices in 3.6 GHz band (3550 MHz to 3700 MHz).

For further information, refer to [CBRS](#).

Organization

An Organization allows multiple accounts to share CBRS billing and SAS ID. The Primary account owns this configuration, and the Secondary account can optionally share it. Both accounts must authorize the sharing.

For further information, refer to [Organization](#).

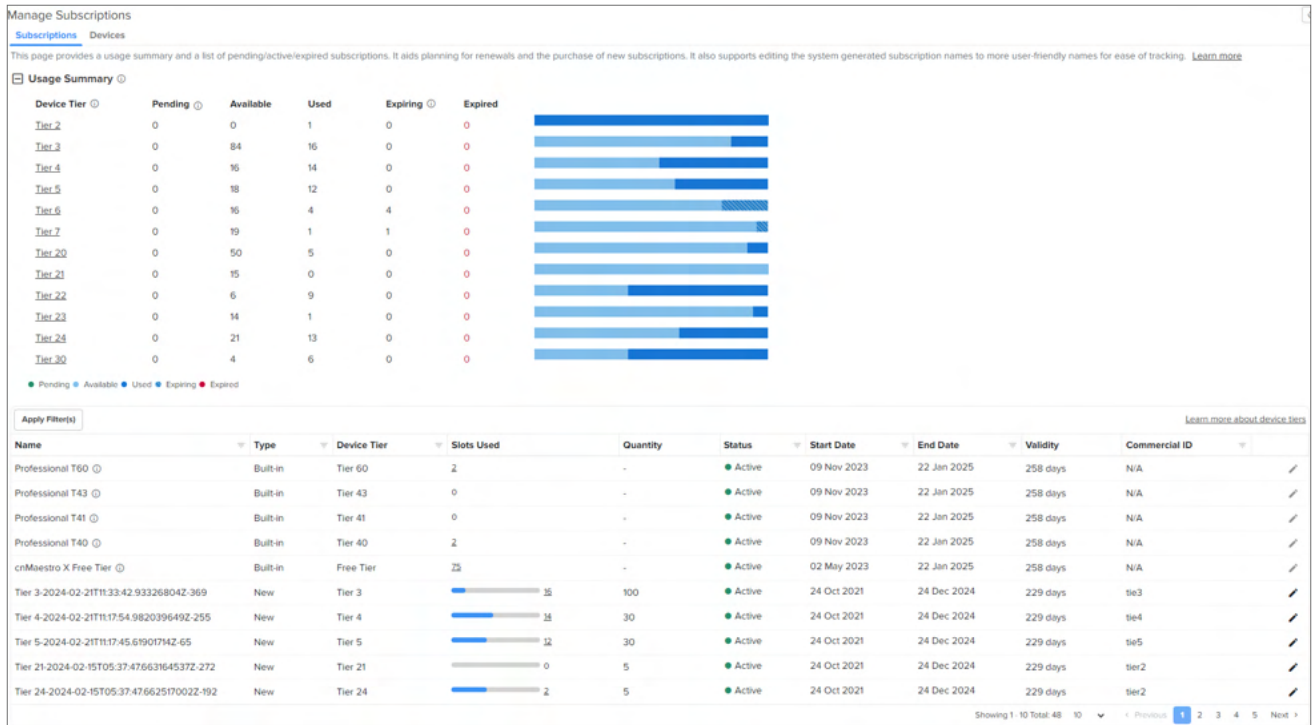
Manage Subscriptions

Manage Subscriptions provide the following details:

- Subscriptions
- Devices
- On-Premises Instances

Subscriptions

Subscriptions page describes about the usage summary and a list of pending, active, and expired subscriptions. It aids planning for renewals and the purchase of new subscriptions.



It also supports editing the system generated subscription names to more user-friendly names for ease of tracking.

To edit the **Subscriptions** perform the following steps:

1. click edit (✎) icon.

Edit window pops up as shown below.

Edit

Name

Tier 1-2022-09-27T06:06:28Z-490

Description

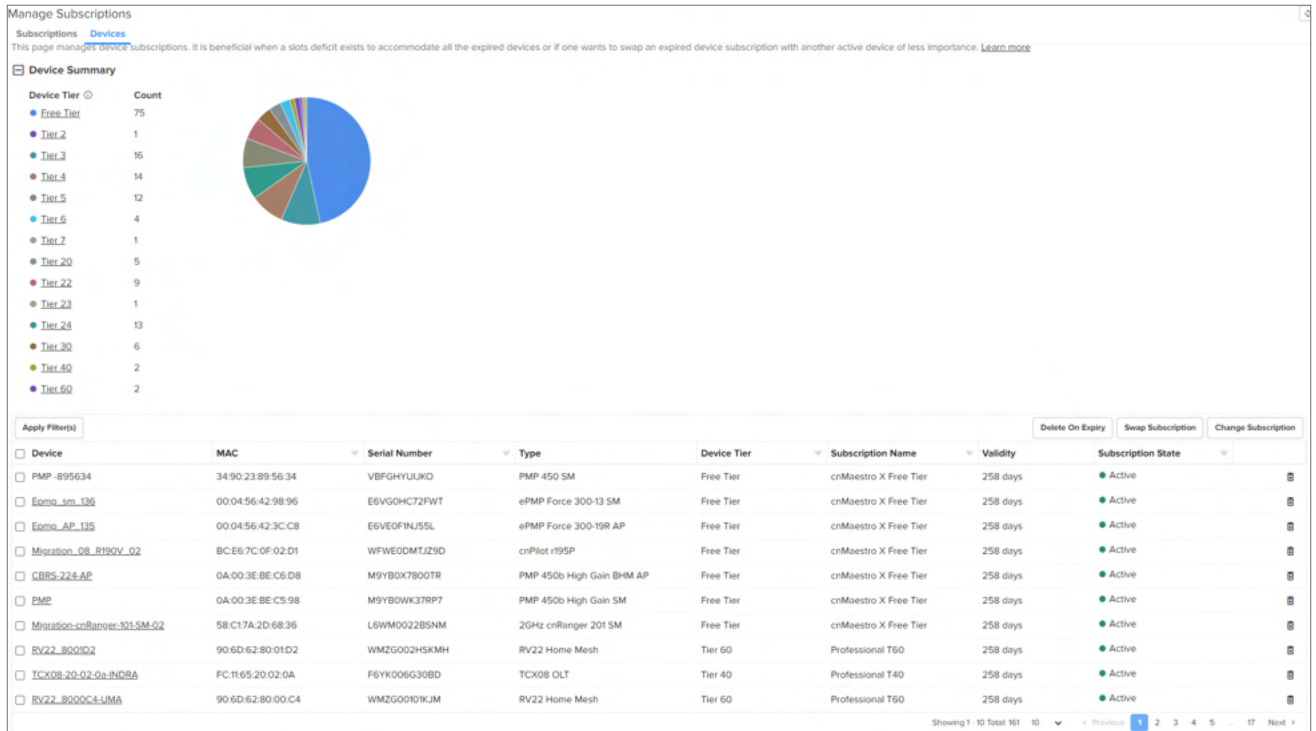
Save

Cancel

2. Enter **Name** and **Description**.
3. Click **Save**.

Devices

Devices page manages device subscriptions. It is beneficial when a slots deficit exists to accommodate all the expired devices or if one wants to swap an expired device subscription with another active device of less importance. For more info refer to Subscription Management.



Audit Logs



Note:

Audit Logs are supported only for cnMaestro X subscribers.

Audit Logs record administration activities through both the Web UI and the RESTful API. Audit Log entries usually include destination and source addresses, a timestamp and user login information. User can access Audit Logs in the **Administration > Audit Logs** page.

Figure 562 Audit Logs

Administration > Audit Logs x

Export

Result	Time	Type	Module	Action	Source	IP Address	Description
Success	10 May 2024, 02:35 AM	Operations	Infrastructure	Download			Successfully initiated Edge controller techdump for ec-2ae3ecc4f00d
Success	09 May 2024, 09:16 PM	Security	Administrator	Login			logged in successfully
Success	09 May 2024, 09:14 PM	Security	Administrator	Logout			logged out
Success	09 May 2024, 09:14 PM	Security	Administrator	Logout			session logout operation performed by successful
Success	09 May 2024, 09:14 PM	Security	Administrator	Logout			logged out
Success	09 May 2024, 08:54 PM	Operations	Device	Delete			Device deletion succeeded for MAC -
Success	09 May 2024, 08:53 PM	Operations	Device	Delete			Device deletion initiated for MAC -
Success	09 May 2024, 08:53 PM	Operations	Device	Delete			Device deletion succeeded for MAC -
Success	09 May 2024, 08:53 PM	Operations	Device	Delete			Device deletion initiated for MAC -
Success	09 May 2024, 08:53 PM	Operations	Device	Delete			Device deletion succeeded for MAC -

Showing 1 - 10 Total: 6779

The following table describes the Audit Logs parameters and their descriptions.

Table 165 Audit Log Parameters

Parameter	Description
Action	Displays the action performed by the user (create, delete, download, etc).

Table 165 *Audit Log Parameters*

Parameter	Description
Description	Textual description of the task.
Export	Enable export as CSV or PDF.
IP Address	IP address of the Web browser or API application.
Module	Module generating entry (AAA, administrator, alarm).
Result	The result of the audit log as Success or Failed .
Source	Administrator or API client name.
Time	The time when the action was performed.
Type	Type of the log entry (configuration, operation, onboarding, security).

Log Action

An action log contains a set of transactions. Each transaction contains one or more Actions. Each Action has a name and input parameters. Some Actions have output parameters.

The following Actions will be supported for individual Audit Log entries. Each activity performed in the server is detailed in this table.

Table 166 *Log Action Parameters*

Parameter	Description
Claim	Claim a device in the network operator.
Cloud-Connect	Provides the status of the On-Premises to Cloud account connection.
Create	Create an object in the network device.
Delete	Delete an object in the network device.
Download	Download a file.
Edit	Edit an existing device detail.
Link Test	Perform a Link Test.
Login	Login to a device.
Logout	Logout from a device.
Mail	Mail ID of a device.
Move	Move a device from the server.
Reboot	Reboot a device.
Reset	To reset a device
Upload	Upload a file on the server.

Audit Modules

Auditing activity is mapped to individual modules within cnMaestro. A breakdown of the available modules is listed below.

Module	Type (s)	Description
ACL	provisioning	Adding Editing Removing the ACL Entries.
administrator	provisioning operations security	User Management: Login, Users, Roles, Email, etc.

Module	Type (s)	Description
alarm	provisioning	Alarms and Alarm History.
api	provisioning	API Management: API Clients and Webhooks.
auditing	provisioning	Auditing Infrastructure.
auto-provision	provisioning	Auto-Provisioning.
CBRS	Services	CBRS.
Cloud- Sync	Services	Synchronizing the Cloud to On-Premises Instances.
data-tunnel	provisioning	Data Tunneling.
device	provisioning operations	Device management.
Email-Notifications	operations	Add or edit Email notification.
guest-portal	provisioning	Guest Portal.
infrastructure	provisioning	Site, Network, Tower Management.
jobs	provisioning operations	Jobs Infrastructure.
license	licensing	Update license details.
MSP	operations	Operations covering Managed Services and Managed Account.
onboard	provisioning operations	Onboarding Queue.
report	provisioning operations	Data Reports.
Profile	provisioning	Create or update a profile.
SIM	provisioning	SIM claim and delete.
system	provisioning operations security	System Services: VM management, change log level, system upgrade, system monitoring, software images, system settings.
template	provisioning	Template-Based Configuration.
tools	provisioning operations	Technical support dump, networking operations, etc.
webhooks	provisioning	Webhooks configuration and management.
Wi-Fi	provisioning operations security	AP Groups, WLANs: edit W-Fi configuration objects.

Settings

Email Notifications

The Email Notifications feature allows the Super Administrator and the Administrator users to add subscribers (Email IDs) for receiving different types of alerts by means of Emails.



Note

- Only 2 email recipients can be added per cnMaestro Essentials account.
- Up to 10 email recipients can be added per MSP, Base Infra, and system level scope.

For example, if there is one MSP, you can create 10 recipients at MSP, 10 at Base Infra, and 10 at system level (All accounts scope).

The severity of alerts are classified as follows:

- Critical
- Major
- Minor

The content of the email alert will be in JSON or HTML format. The subscriber will get email alert only when the global setting is enabled.

Figure 563 *Email notifications page*

Administration > Settings

General **Notifications** Software Images

Settings

☒ Enable email notification

Configure Email IDs to subscribe for email notifications for alarms.

Subscribers Scope: All Accounts [Add Recipient](#)

Email	Content Type	Severity	Status	Scope	Last Modified	Ignore Notification
	html	Major	Active	All Accounts	May 07 2024 14:44:24	PMP SM Offline, cnPilot Home Offline, ePMP ...
	json	Major	Active	All Accounts	May 07 2024 14:44:24	PMP SM Offline, cnPilot Home Offline, ePMP ...
	html	Minor	Active	All Accounts	May 07 2024 14:44:24	PMP SM Offline, cnPilot Home Offline, ePMP ...
	html	Minor	Active	All Accounts	May 07 2024 14:44:24	PMP SM Offline, cnPilot Home Offline, ePMP ...
	json	Major	Active	All Accounts	May 07 2024 14:44:24	
	json	Minor	Active	@MSP	May 07 2024 14:44:24	
	html	Major	Active	All Accounts	May 07 2024 14:44:24	PMP SM Offline, cnPilot Home Offline, ePMP ...
	html	Major	Active	All Accounts	May 07 2024 14:44:24	PMP SM Offline, cnPilot Home Offline, ePMP ...

Showing 1 - 8 Total: 8 10 < Previous 1 Next >

Adding Recipient to Subscriber Table

1. Navigate to **Administration > Settings > Notifications** page.

Figure 564 Adding Subscribers

The screenshot shows the 'Administration > Settings' page with the 'Notifications' tab selected. Under 'Settings', the 'Enable email notification' checkbox is checked. Below this, a section titled 'Configure Email IDs to subscribe for email notifications for alarms.' contains a 'Subscribers' table. The table has columns: Email, Content Type, Severity, Status, Scope, Last Modified, and Ignore Notification. A 'Scope' dropdown is set to 'All Accounts'. A red box highlights the 'Add Recipient' button in the top right corner of the table area.

Email	Content Type	Severity	Status	Scope	Last Modified	Ignore Notification
	html	Major	Active	All Accounts	May 07 2024 14:44:24	PMP SM Offline, cnPilot Home Offline, ePMP ...
	json	Major	Active	All Accounts	May 07 2024 14:44:24	PMP SM Offline, cnPilot Home Offline, ePMP ...
	html	Minor	Active	All Accounts	May 07 2024 14:44:24	PMP SM Offline, cnPilot Home Offline, ePMP ...
	html	Minor	Active	All Accounts	May 07 2024 14:44:24	PMP SM Offline, cnPilot Home Offline, ePMP ...
	json	Major	Active	All Accounts	May 07 2024 14:44:24	
	json	Minor	Active	@MSP	May 07 2024 14:44:24	
	html	Major	Active	All Accounts	May 07 2024 14:44:24	PMP SM Offline, cnPilot Home Offline, ePMP ...
	html	Major	Active	All Accounts	May 07 2024 14:44:24	PMP SM Offline, cnPilot Home Offline, ePMP ...

2. Click **Add Recipient**.

The following window is displayed:

The 'Add Email Subscriber' dialog box is shown. It contains the following fields and options:


- ☒ Active
- Severity: Major (dropdown menu)
- All alarms of chosen severity or greater will be sent.
- Email: Enter Email ID (text input)
- Content Type: ☒ HTML ☐ JSON
- Managed Account: All Accounts (dropdown menu)
- Ignore Notification: ☒ cnPilot Home Offline, ☒ ePMP SM Offline, ☒ PMP SM Offline
- Buttons: Cancel, Add

3. Enter the Email ID of the subscriber in the **Email** textbox.
4. Select the severity level from the **Severity** list.
5. Select the Managed Account type from the **Managed Account** list.
6. Choose **HTML** or **JSON** radio button for the **Content Type**.
7. Select the appropriate option (s) for **Ignore Notification**.
8. Click **Add** and the entry reflects in the subscriber table.

All alarms of chosen severity and above are sent through email as explained below:

- If severity **Critical** is selected, then we receive only critical alarms.
- If severity **Major** is selected, then we receive critical and major alarms.
- If severity **Minor** is selected, then we receive critical, major, and minor alarms.


HTML Email Example


CLEAR

1

Notification Details

Type	Account	Name	Message
Time	Tower/Site	Type IP Address	
CLEAR 14:10 (UTC +05:30)	Base Infrastructure	cnPilot R201P12345678 cnPilot r201P 10.110.224.74	Device is offline.



MAJOR


1

Notification Details

Type	Account	Name	Message
Time	Tower/Site	Type IP Address	
MAJOR 14:02 (UTC +05:30)	Base Infrastructure	cnPilot R201P12345678 cnPilot r201P 10.110.224.74	Device is offline.

JSON Email Example


cnMaestro Notifications <[redacted]@gmail.com>



[External] cnMaestro Notification

```
[
{
  "acknowledged_by": "",
  "code": "STATUS",
  "duration": 360122,
  "id": "5bec030f3f8f840c1a079ffe",
  "mac": "0A:00:3E:60:34:2D",
  "message": "Device is offline",
  "managed_account": "Base Infrastructure",
  "name": "Status",
  "ip": "10.110.208.30",
  "network": "default",
  "severity": "major",
  "site": "sid",
  "source": "PMP 450m AP",
  "source_type": "pmp",
  "status": "active",
  "time_raised": 1542193635297,
  "tower": "",
  "isSite": null,
  "mode": "ap"
}
]
```

Account Type

cnMaestro supports three separate account types, based upon the composition of devices installed. The type is set when the account is created initially, but it can be changed later through the **Administration > Settings** page.

For more information, refer [Navigating the cnMaestro UI](#).

Managing Device software images under Automatically Update Device Software section

cnMaestro cloud allows one to update the device software during onboarding and for managed devices.

Adding update device software is a manual process as follows:

1. Navigate to **Administration > Settings > Software Images > Automatically Update Device Software** tab.
2. Select the version file and then click **onboarding/Managed Devices** checkbox.



Note

Enable the onboarding checkbox, in order to avoid the failure of onboarding devices with minimum supported version rather than the recommended version.

3. Enable the checkbox as follows:

- Enable **Managed Devices** flag only for Wi-Fi devices (E-Series, R-Series and XE/XV/X7-Series).
- Enable **Sequential Site Update** and **Both Partitions** flag only for only E-Series and XE/XV/X7-Series devices.

4. click **Apply Settings**.



Note

- Once auto software update job for managed devices is triggered, it will automatically abort any manually scheduled software update jobs.
- In order to avoid failures in onboarding devices having minimum supported version other than recommended version, enable the onboarding check.

Figure 565 Software Images

Administration > Settings

General Notifications **Software Images**

Automatically Update Device Software View Update Jobs

Enable automatic software update for devices during onboarding and for managed devices.
 ⚠ Once auto software update job for managed devices is triggered, it will automatically abort any manually created running/scheduled software update jobs.

Device Type	Version	Onboarding Devices	Managed Devices	Sequential Site Update	Both Partitions
Enterprise Wi-Fi (E-Series)	4.2.31r9	<input checked="" type="checkbox"/>	<input type="checkbox"/> Now 12:57 PM	<input type="checkbox"/>	<input type="checkbox"/>
Enterprise Wi-Fi (XE/XV/X7-Series)	6.6.1 b2 (Beta)	<input checked="" type="checkbox"/>	<input type="checkbox"/> Now 12:07 PM	<input type="checkbox"/>	<input type="checkbox"/>
cnVision	4.6.2 (Recommended)	<input type="checkbox"/>	N/A	N/A	N/A
PON	1.2.0.42 (Beta)	<input type="checkbox"/>	N/A	N/A	N/A
PMP	23.0	<input checked="" type="checkbox"/>	N/A	N/A	N/A
cnMatrix	5.0.1 r4	<input type="checkbox"/>	N/A	N/A	N/A
cnPilot Home	4.8 R15	<input checked="" type="checkbox"/>	<input type="checkbox"/> Now 05:40 PM	N/A	N/A
cnRanger	1.0.0.0 r1	<input type="checkbox"/> ⚠	N/A	N/A	N/A
Enterprise Wi-Fi (Xirrus-Series)	8.7.0 r8167	<input type="checkbox"/>	N/A	N/A	N/A
NSE	1.0 r55 (Recommended)	<input type="checkbox"/>	N/A	N/A	N/A
cnWave 5G Fixed	3.1.2	<input type="checkbox"/>	N/A	N/A	N/A
ePMP	5.7.2 RC8 (Beta)	<input type="checkbox"/>	N/A	N/A	N/A

Apply Settings

Appendix

This section includes the following topics:

- [Network Port Requirements](#)
- [XMS-Enterprise to cnMaestro X](#)
- [Converting Tier 2 Unused Slots](#)

Network Port Requirements

Network Port Requirements for Outbound

The following table provides information about network port requirements for outbound:

Table 167 *Outbound Port Details*

Port Number	Port Type	Purpose
443	TCP	HTTPS Web Access and Device communication

XMS-Enterprise to cnMaestro X

This section describes the process of migration from XMS-Enterprise (XMS-E) to cnMaestro X.

Before you begin migration, upgrade the following to the latest version:

- XMS-E to version 8.4.0
- Xirrus APs to version 8.7.0

Perform the following steps for migration:

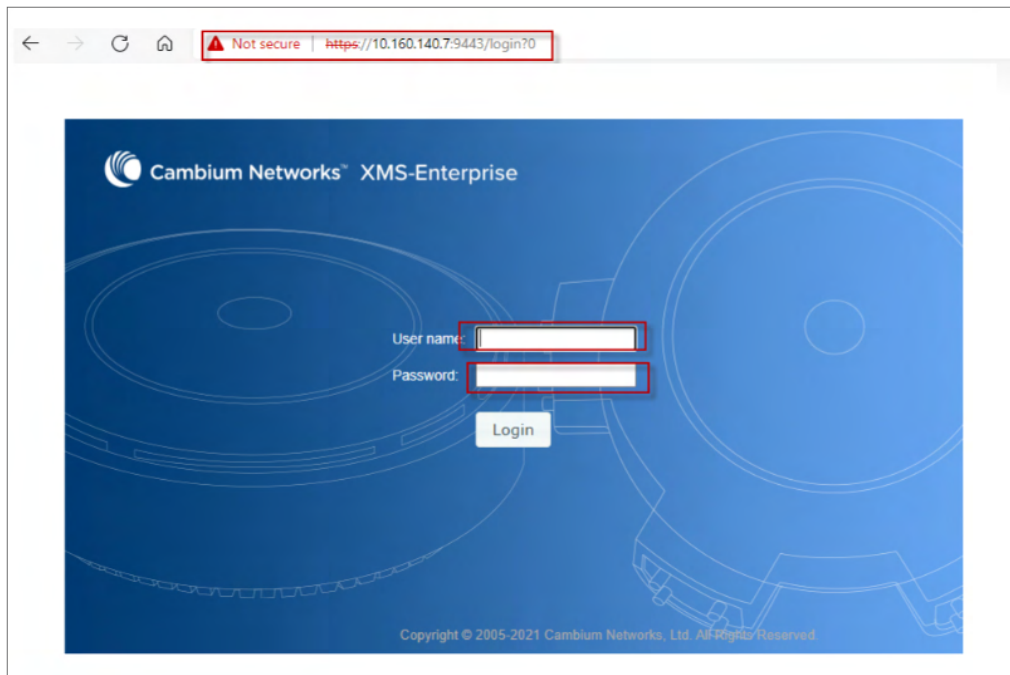
1. In XMS-E, perform the following actions:
 - [Export Golden Configuration](#)
 - [Migrate to cnMaestro X](#)
2. In cnMaestro X, perform the following actions:
 - [Create Wi-Fi AP Group](#)
 - [Approve APs into Wi-Fi AP Group](#)
 - [Import and Apply AP configuration](#)

XMS-E System

To login to XMS-E, complete the following steps:

1. Launch the Web login page.
2. Enter the username and password.

3. Click **Login**.

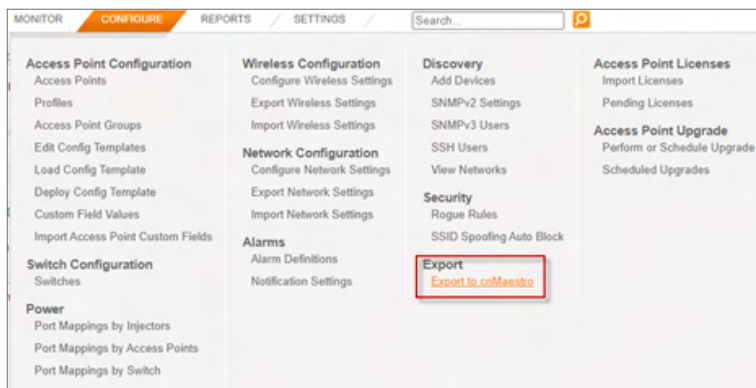


Export Golden Configuration

Export Golden Configuration for one of the APs. It is saved as a zipped file in the local file system.

To start export golden configuration in XMS-E, navigate to **Configure** tab > **Export**.

1. Select **Export to cnMaestro**.

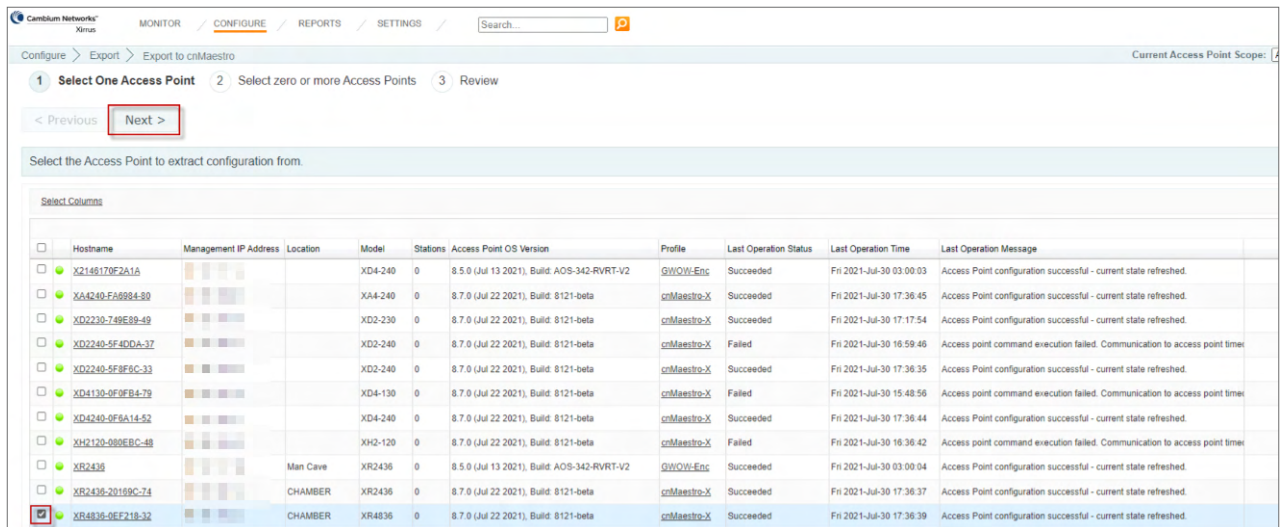


2. Select the AP to create the golden configuration for a group of APs and click **Next**.

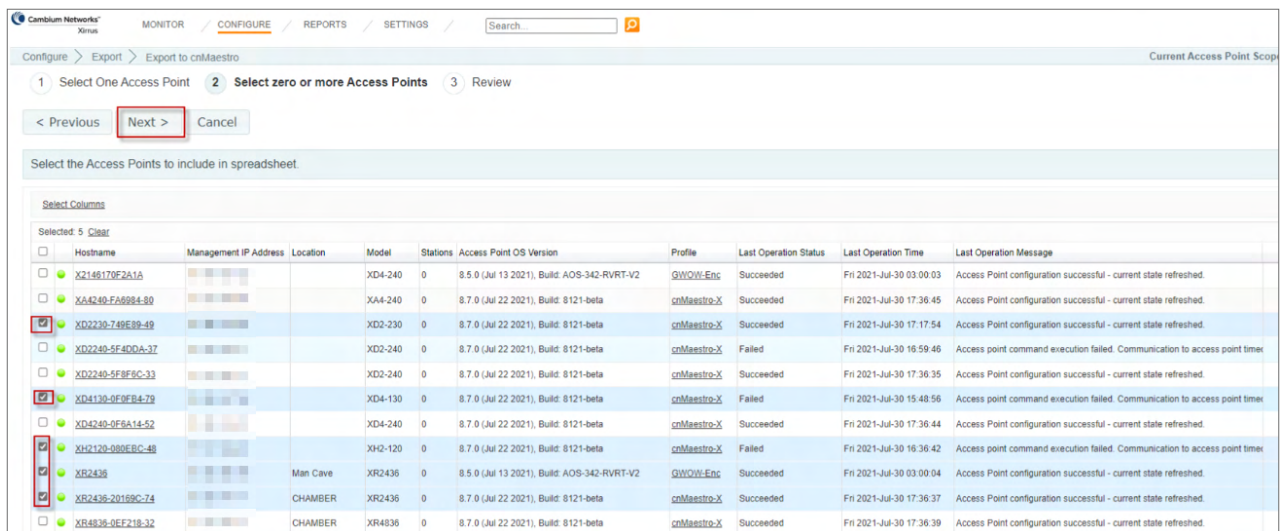


Note

- Select the AP with the maximum radios and the highest capability.
- During the migration of an AP from XMS-E to cnMaestro, the AP configurations are not modified.



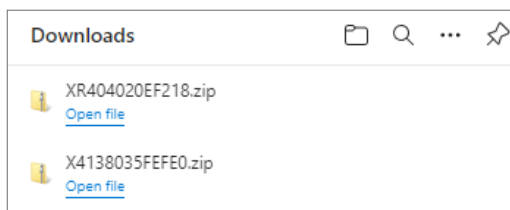
3. Select group of APs to be added to the spreadsheet and click **Next**.



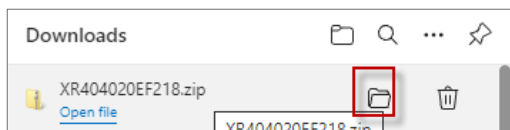
4. Click **Export**.

In Local System unzip the directory and files to local directory.

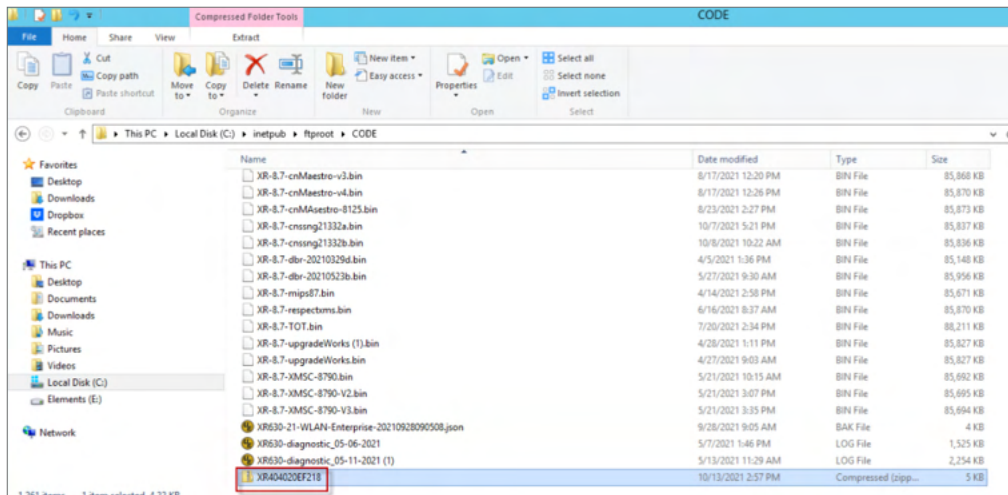
5. Download the zip files from the browser window.



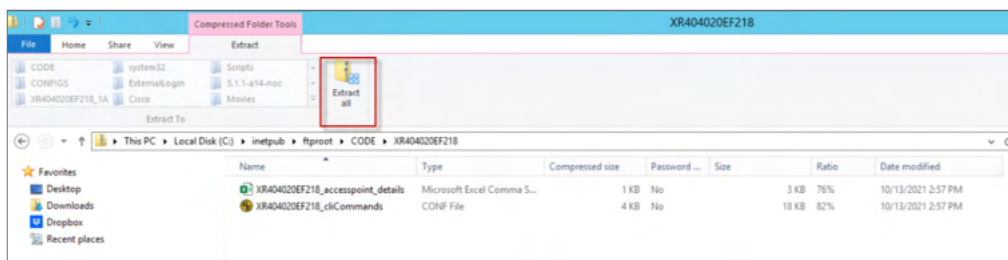
6. Go to the folder where the zipped files are saved and extract the contents to a folder.



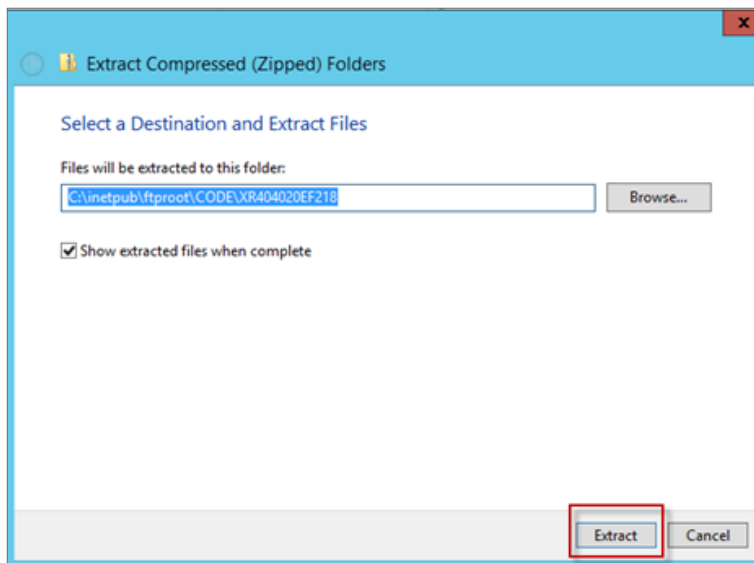
7. Open the directory path where the file has been stored and double-click on the zipped file.



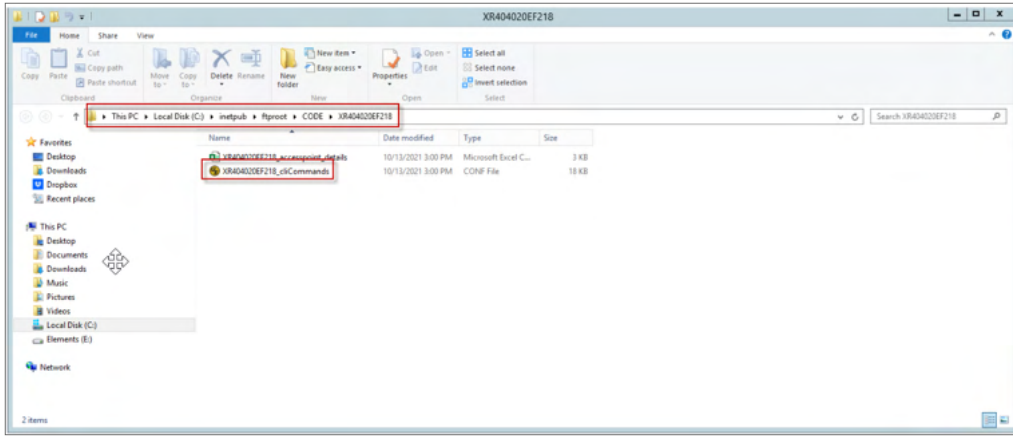
8. Click **Extract all**.



9. Extract the folder to the path.



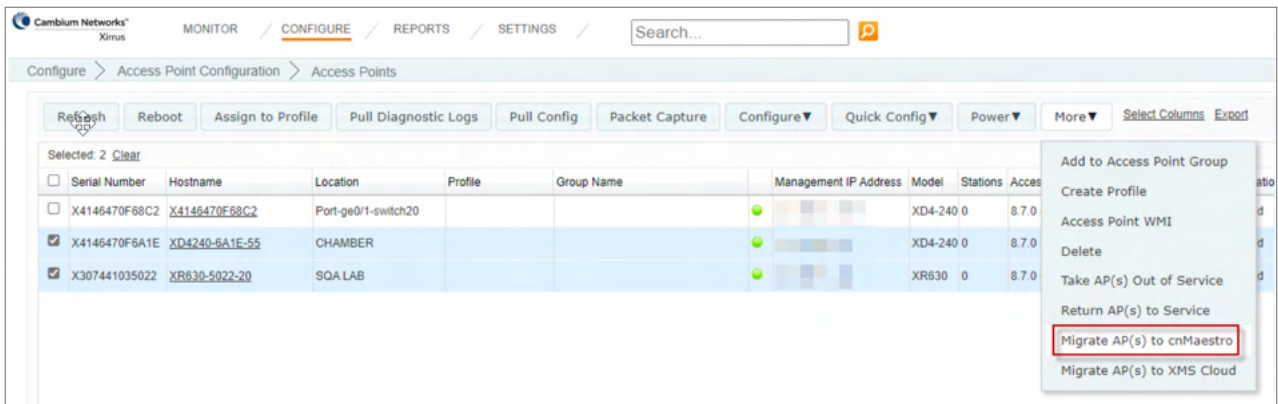
10. Make a note of the folder or file location as you will require this file later.



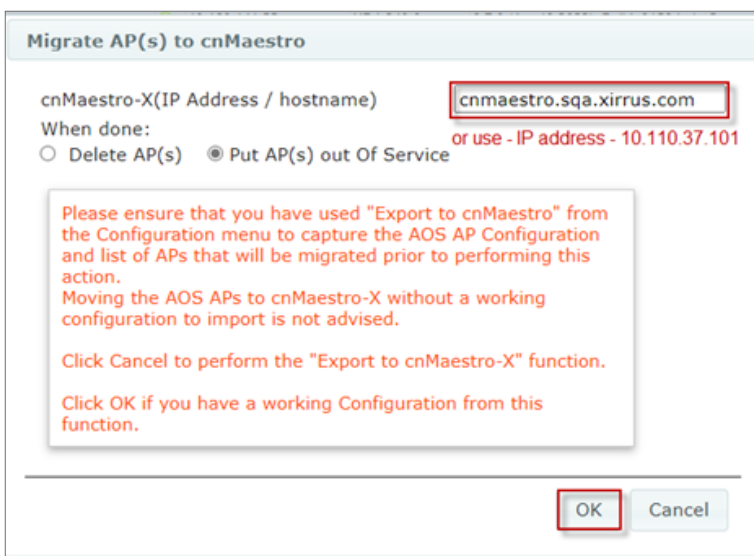
Migrate to cnMaestro X

Select APs to migrate to cnMaestro X. Perform the following steps:

1. Navigate to the **More** menu > select **Migrate APs to cnMaestro**.



2. Enter the IP address or Hostname mapped in DNS for cnMaestro X.
3. Select **Delete AP** or **Put AP(s) out of Service** and click **OK**.



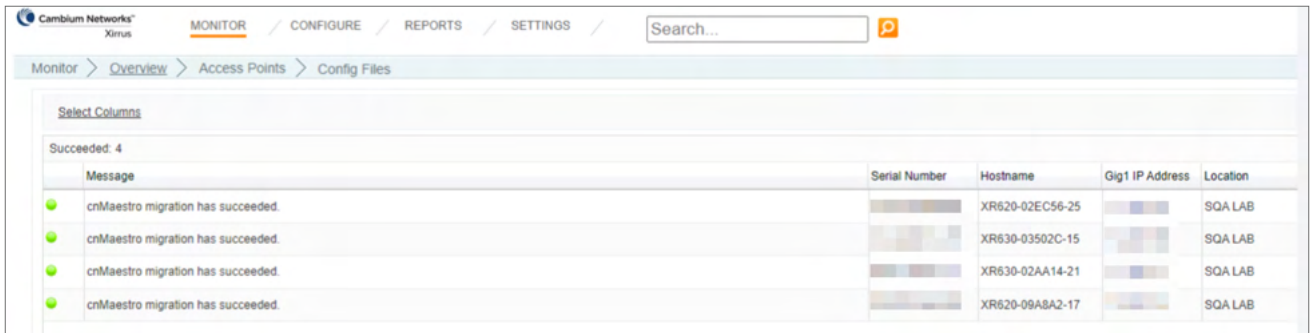
Note

- Out of service APs are not removed from XMS-E, so if there is an issue, select the **Return APs to**

Service option and they will return to XMS-E.

- You must reset using the `snmp trap host 1 Xirrus-XMS AP CLI` command on the AP for the return to service to work.
- If you select **Delete APs**, they will be removed and you must rediscover them on the network to return them to XMS-E.
- You should also remove the Device Network from the Device discovery section to clean up XMS-E.

A success message from XMS-E for each of the APs migrated to cnMaestro X is displayed.



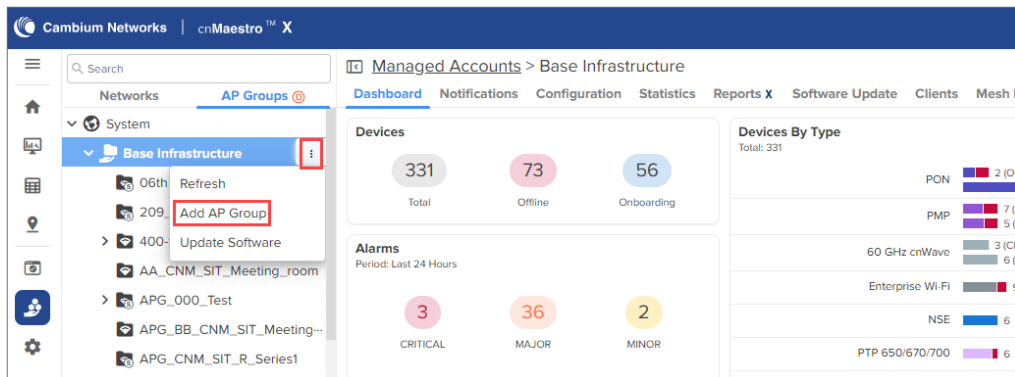
The screenshot shows the 'Monitor' tab in the Xirrus interface. A message box displays 'Succeeded: 4' with four green checkmarks, each followed by the text 'cnMaestro migration has succeeded.' Below the messages is a table with columns: Serial Number, Hostname, Gig1 IP Address, and Location. The table lists four APs, all with 'SQA LAB' as the location.

Serial Number	Hostname	Gig1 IP Address	Location
XR620-02EC56-25			SQA LAB
XR630-03502C-15			SQA LAB
XR630-02AA14-21			SQA LAB
XR620-09A8A2-17			SQA LAB

Create Wi-Fi AP Group

Create Wi-Fi AP Group and Import CLI command file from exported directory.

1. Navigate to **Wi-Fi AP Group > Base Infrastructure** > click action () icon to add **Add AP Group**.



2. In the **Basic Information** page, select Type as **Enterprise Wi-Fi (Xirrus-Series)** from the drop-down.
3. Select the **Auto-Sync**.
4. Click **Save**.

AP Groups > Add New

Basic

Full Configuration

Basic Information

Type
Enterprise Wi-Fi (Xirrus-Series)

Name*

Scope
Shared Shared Scope means the AP Group is accessible to all Managed Accounts

☐ Auto Sync Automatically push configuration changes to devices sharing this AP Group

Description

Save Close

- In the **Full Configuration** page, click the **Import** option.

AP Groups > Add New

Full Configuration

The format in the device configuration file must match the format in the web UI or the "View Device Configuration" link

⚠ Settings entered are not validated or error-checked (However, dollar (\$), period (.) or space characters are not allowed in a variable name and it should not be more than 64 characters long), and they may overwrite configuration made in previous screens, so please use them with caution. You are responsible for ensuring the resulting AP Group is valid and safe to use.

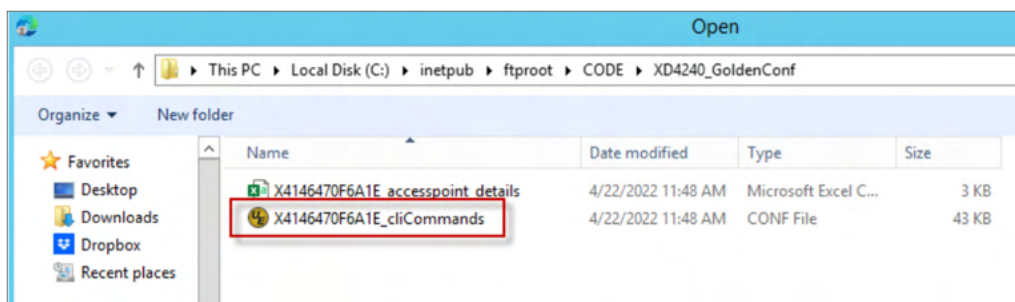
Import Config

Configuration file
Import.conf

Import

Save Close

- Select the CLI command file from the unzipped directory.



- Click **Import**.



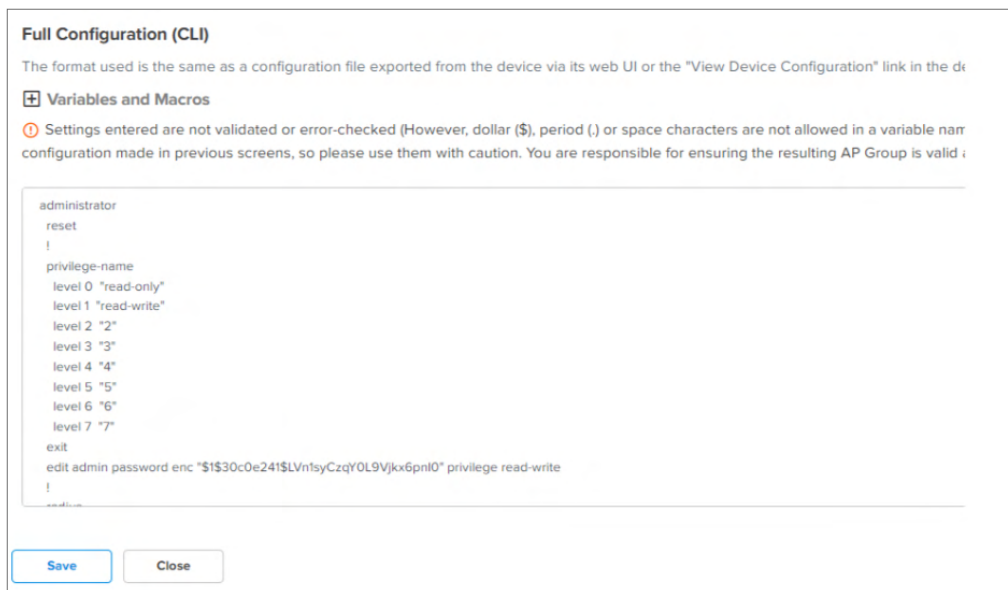
Import Config

Configuration file

X4146470F6A1E_cliCommands.conf Import.conf

Import

The configuration file is displayed.



Full Configuration (CLI)

The format used is the same as a configuration file exported from the device via its web UI or the "View Device Configuration" link in the device details page.

Variables and Macros

Settings entered are not validated or error-checked (However, dollar (\$), period (.) or space characters are not allowed in a variable name). Configuration made in previous screens, so please use them with caution. You are responsible for ensuring the resulting AP Group is valid.

```

administrator
reset
!
privilege-name
level 0 "read-only"
level 1 "read-write"
level 2 "2"
level 3 "3"
level 4 "4"
level 5 "5"
level 6 "6"
level 7 "7"
exit
edit admin password enc "$1$30c0e24$LVnfsyCzqY0L9VjKx6pnl0" privilege read-write
!
end

```

Save **Close**

8. Click **Save**.

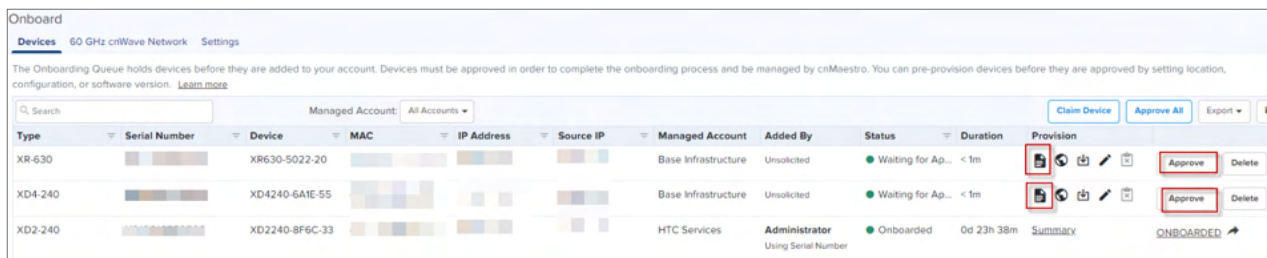
Approve APs into Wi-Fi AP Group

APs pending for approval in cnMaestro X based on the **Migrate APs to cnMaestro X** steps as described above.

You can claim APs to approve from the **Onboard > Devices** page.

Perform the following steps to approve APs from the **Onboard > Devices** page.

1. Navigate to the **Onboard > Devices** page and click **Approve All** (to approve all devices at once) or **Approve** (to approve devices individually.)



Onboard

Devices 60 GHz cnWave Network Settings

The Onboarding Queue holds devices before they are added to your account. Devices must be approved in order to complete the onboarding process and be managed by cnMaestro. You can pre-provision devices before they are approved by setting location, configuration, or software version. [Learn more](#)

Managed Account: All Accounts

Type	Serial Number	Device	MAC	IP Address	Source IP	Managed Account	Added By	Status	Duration	Provision	Actions
XR-630		XR630-5022-20				Base Infrastructure	Unsolicted	Waiting for Ap...	< 1m		Approve Delete
XD4-240		XD4240-6A1E-55				Base Infrastructure	Unsolicted	Waiting for Ap...	< 1m		Approve Delete
XD2-240		XD2240-8F6C-33				HTC Services	Administrator	Onboarded	0d 23h 38m	Summary	ONBOARDED

2. Enter the required details, provision the device for location, and assign to an AP Group.

Edit Device Configuration: XR630-5022-20

Details Location Update Configure

Basic Details

Serial Number

MAC

Device Name
XR630-5022-20

Description

Save Cancel

Edit Device Configuration: XR630-5022-20

Details Location Update **Configure**

AP Group
Test AP Group

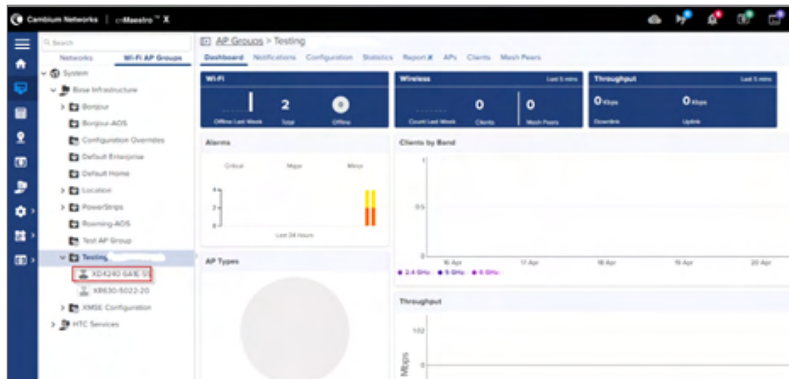
Configuration Variables (Advanced)

Save Cancel

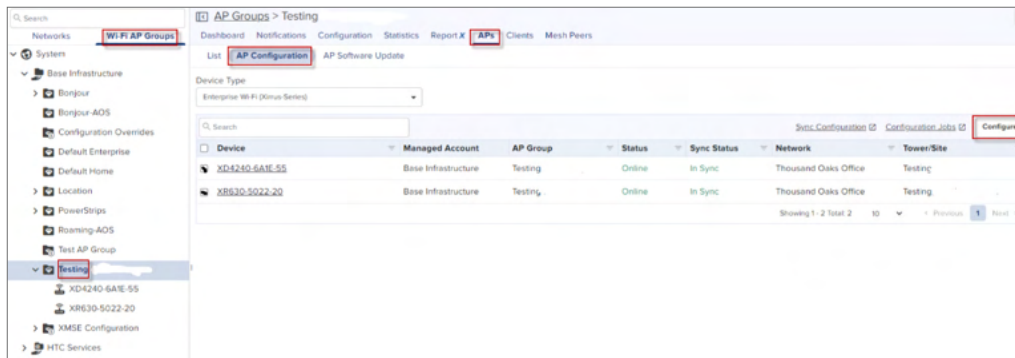
3. Click **Save**.
4. In the **Onboard > Devices** page, select **Approval All** (to approve all devices at once) or **Approve** (to approve devices individually.)

Import and Apply AP configuration

APs imported are ready for basic configuration. Import AP configuration using the CSV file from the exported directory.



1. Navigate to **Wi-Fi AP Group > select AP Group > AP Configuration**.
2. Select all APs to configure, click **Configure**.



3. In Device Override table, verify AP details and click **Import**.

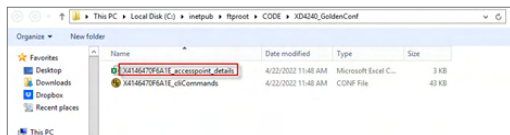


Note

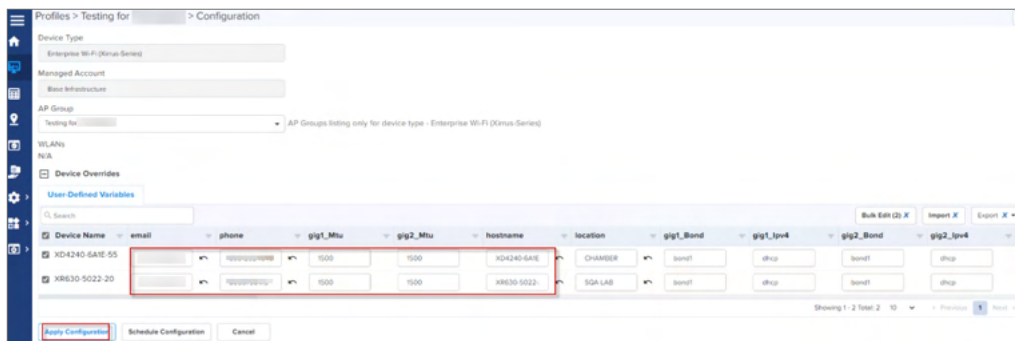
Email and Phone fields are auto populated from the .csv file.



4. Select the .csv import file from the unzipped directory folder and click **Apply**.



All the configuration values from the CSV file are populated for each AP. The data is auto populated to the **User Defined Variables** tab. The APs receive complete configurations including all IAP settings.



5. Click **Apply Configuration**.

Apply Configuration

☐ Stop update on critical error

Devices to update in parallel (1-500)

Notes

Apply Configuration to 2 device(s)

Cancel

When the APs are completely configured, **Sync Status** is displayed as **In Sync**.

Dashboard	Notifications	Configuration	Statistics	Report X	APs	Clients	Mesh Peers
List	AP Configuration	AP Software Update					
Device Type	Enterprise Wi-Fi (Xirrus-Series)						
Search							
Device	Managed Account	AP Group	Status	Sync Status			
<input type="checkbox"/> XD4240-6A1E-55	Base Infrastructure	Testing	Online	Not In Sync			
<input type="checkbox"/> XR630-5022-20	Base Infrastructure	Testing	Online	Not In Sync			

You have to refresh the page to view the updated **Sync Status**.

AP Groups > Testing AOS

Dashboard

Notifications

Configuration

Statistics

Report X

APs

Clients

Mesh Peers

List

AP Configuration

AP Software Update

Device Type

Enterprise Wi-Fi (Xirrus-Series)

Search

Sync Configuration

Configuration Jobs

Configure

<input type="checkbox"/>	Device	Managed Account	AP Group	Status	Sync Status	Network	Tower/Site
<input type="checkbox"/>	XD4240-6A1E-55	Base Infrastructure	Testing AOS	Online	In Sync	Thousand Oaks Office	Testing_for_
<input type="checkbox"/>	XR630-5022-20	Base Infrastructure	Testing AOS	Online	Not In Sync	Thousand Oaks Office	Testing_for_

Showing 1 - 2 Total: 2

10

< Previous

1

Next >

Converting Tier 2 Unused Slots

Cambium Networks has introduced new product family-based cnMaestro X SKUs and pricing for devices such as Fixed Wireless Broadband APs, cnRanger, cnReach, cnVision, PMP, ePMP, and PTP. Earlier, the Tier 2 subscription was used to control these devices (pricing). To simplify the purchase and onboarding for these devices, Cambium Networks has decided to remove the Tier 2 subscription and introduce new four tiers (Tier 21, Tier 22, Tier 23, and Tier 24).

The Tier 2 subscription is no longer valid now. Due to Tier 2 subscription removal, there can be unused Tier 2 slots in your account (purchased during the Tier 2 subscription). As a solution, Cambium Networks provides an option to convert these unused Tier 2 slots into new tiers based on the device family and requirements. You can manually convert the unused Tier 2 slots to Tier 21, Tier 22, Tier 23, and Tier 24 using the ⓘ icon located on the **Manage Subscriptions** page (cnMaestro UI). This solution helps in better mapping and device management.



Note

The Convert Tier 2 option is effective from March 1, 2024 for Fixed Wireless Broadband APs, cnRanger, cnReach, cnVision, and PTP devices. You must convert the unused Tier 2 slots in your account to the new Tier 2x slots before onboarding the devices.

When you convert the unused Tier 2 slots into new tiers, you cannot change the new tiers back to Tier 2.

You can convert the unused Tier 2 slots to new tiers, for example, as described in [Table 168](#).

Table 168 Example of converting unused Tier 2 slots

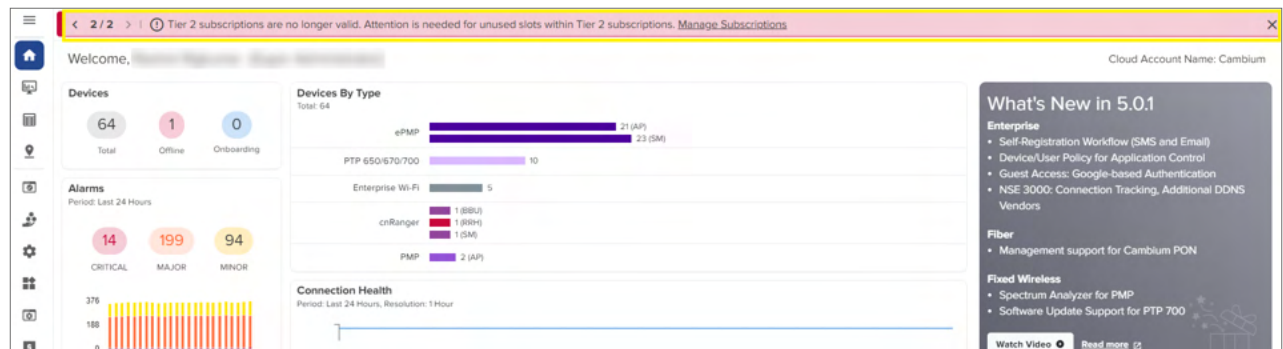
New Tier	Device Family and Type	
Tier 21	cnVision	FLEXr, HUB360
	ePMP	All AP Models
Tier 22	PMP	All AP Models except 450m and 450mv
Tier 23	PMP	450m
Tier 24	cnRanger	All BBU Models
	cnReach	All cnReach Models
	PTP	All PTP Models

To manually convert the unused Tier 2 slots for a device family, complete the following steps:

1. Log in to your respective cnMaestro UI account.

The **Home** page appears with a banner, as shown in [Figure 566](#).

Figure 566 The Tier 2 conversion-specific banner




2. From the home page, navigate to the **Manage Subscriptions** page.

The **Manage Subscriptions** page appears (as shown in [Figure 567](#)), displaying the same banner and details of tiers.

Figure 567 The Manage Subscriptions page with tier information

The screenshot shows the 'Manage Subscriptions' page. At the top, a notification bar states: 'Tier 2 subscriptions are no longer valid. Attention is needed for unused slots within Tier 2 subscriptions. Manage Subscriptions'. Below this, the 'Subscriptions' tab is active, showing a list of subscriptions. One subscription, 'Tier 2-2024-02-20T13:05:45.99997899Z-408', is highlighted with a red box and an information icon (i) in the right column. Below the subscription list, a table provides tier information:

Device Tier	Required	Available	Deficit	Upgradable
Tier 3	5	4	1	No
Tier 21	5	5	0	Yes
Tier 22	1	4	0	Yes
Tier 24	11	3	8	No

3. Select the Tier 2 subscription and click the corresponding  icon (as shown in [Figure 567](#)).

The Tier 2 subscription window appears with details of unused slots and options to convert to new tiers (Tier 21, Tier 22, Tier 23, and Tier 24).

Figure 568 The Convert Tier 2 window

The screenshot shows the 'Convert Tier 2-2024-02-26T07:40:38.788211254Z-323' window. It contains the following information:

- Effective March 1, 2024, Tier 2 for Fixed Wireless Broadband APs, cnRanger, cnReach, cnVision, and PTP devices will be replaced by four new Tiers 21, 22, 23, and 24.**
- The unused Tier 2 slots in your account must be converted to the new Tier 2x slots before onboarding AP/cnRanger/cnReach/cnVision/PTP devices, as mentioned below**
- Unused Tier 2 Slots:** 48
- Tier 21:** 0 ePMP Access Points and cnVision
- Tier 22:** 0 PMP 450i & 450v Access Points
- Tier 23:** 0 PMP 450m & 450mv Access Points
- Tier 24:** 0 PTP, cnReach & cnRanger
- Buttons:** Save, Cancel, Learn more

4. Check the unused slot count and enter a valid value (in integers) in Tier 21, Tier 22, Tier 23, or Tier 24 text boxes (based on your requirements).
5. Click the **Save** button (as shown in [Figure 568](#)) to apply the changes.

Cambium Networks

Cambium Networks delivers wireless communications that work for businesses, communities, and cities worldwide. Millions of our radios are deployed to connect people, places, and things with a unified wireless fabric that spans multiple standards and frequencies of fixed wireless and Wi-Fi, all managed centrally via the cloud. Our multi-gigabit wireless fabric offers a compelling value proposition over traditional fiber and alternative wireless solutions. We work with our Cambium certified Connected Partners to deliver purpose built networks for service provider, enterprise, industrial, and government connectivity solutions in urban, suburban, and rural environments, with wireless that just works.

Support website	https://support.cambiumnetworks.com
Support inquiries	
Technical training	https://learning.cambiumnetworks.com/learn
Main website	http://www.cambiumnetworks.com
Sales inquiries	solutions@cambiumnetworks.com
Warranty	https://www.cambiumnetworks.com/support/standard-warranty/
Telephone number list	http://www.cambiumnetworks.com/contact-us/
User Guides	http://www.cambiumnetworks.com/guides
Address	Cambium Networks Limited, Unit B2, Linhay Business Park, Eastern Road, Ashburton, Devon, TQ13 7UP United Kingdom



Cambium Networks and the stylized circular logo are trademarks of Cambium Networks, Ltd. All other trademarks are the property of their respective owners.

Copyright © 2024 Cambium Networks, Ltd. All rights reserved.

XV2-21X Wi-Fi 6 Access Point

802.11ax Dual-Radio Indoor Access Point

QUICK LOOK:

- Dual Radio Wi-Fi 6
- 5 GHz (2x2), 2.4 GHz (2x2)
- 1 GbE RJ45 interface
- Managed by cnMaestro™, Swift
- Limited lifetime warranty



Back panel with mounting bracket

Value-Tier Wi-Fi for any market

Cambium Networks XV2-21X Wi-Fi 6 Indoor access point delivers a high-performance to price ratio attractive to any market.

The XV2-21X can be adopted and managed by any of the Cambium Networks management systems, cnMaestro™ Cloud, cnMaestro™ X, cnMaestro™ on-premises, or Swift app-based management. Choose the management type you need, and change it at any time. Unlike other value-tier access points, the XV2-21X is never locked into just one management selection.

Designed for fast installation

The XV2-21X offers multiple installation methods included in the same shipping box. Mount the AP to a ceiling tile using the included steel plate, mount to an existing junction box with 83mm center-to-center holes, twist lock the AP onto a 36mm, 24mm and 14mm T-bar, or simply mount it to any flat surface using the included wall anchors. No accessory brackets are needed.

XV2-21X Wi-Fi 6 Access Point

Access Point Specifications

Note: Some features will be included on subsequent firmware releases.

FCC Ch 1–11, 36–48, 100–144, 149–165

ISED Ch 1–11, 36–48, 100–116, 149–165

ETSI Ch 1–13, 36–64, 100–140

ROW *Individual country limits may apply. Please contact sales for country specific regulations.*

Note: FCC, IC, EU DFS channels not supported in first release

Radios **5 GHz** 802.11 a/n/ac Wave 2/ax, 2x2:2
2.4 GHz 802.11 b/g/n/ax, 2x2:2

Wi-Fi 802.11 a/b/g/n/ac Wave 2/ax

SSID Security WPA3-SAE, WPA3-Enterprise, WPA2 (CCMP, AES, 802.11i), WPA2 Enterprise (802.1x/EAP), WEP, Open

Max PHY Rate **5 GHz radio** 2402 Mbps
2.4 GHz radio 573.5Mbps

Ports 1 x IEEE 10/100/1000 Mbps

Antenna **5 GHz** 6 dBi
2.4 GHz 5 dBi

Max EIRP **5 GHz** 33 dBm
2.4 GHz 32 dBm

Power Typical 11W, 802.3af powered device

Dimensions 155 mm x 155 mm x 37 mm
(6.1 in x 6.1 in x 1.46 in)

With Bracket:

155 x 155 x 46 mm
(6.1 x 6.1 x 1.81 in)

Weight 475g (1.05 lbs)

LEDs Multi-color status LEDs, dimmable, on/off

Ambient Operation Temperature 0°C to 50°C (32°F to 122°F)

Storage Temperature -40°C to 70°C (-40°F to 158°F)

Humidity 95% RH non-condensing

MTBF 1,980,244 hours at 50°C ambient (estimated)

Mount Options Wall or ceiling, T-bar with included locking bracket, ceiling tile plate

Certifications (Compliance) Passpoint 3.0,
802.11 a/b/e/g/i/k/n/r/u/v/w/ac/ax, PP2.0
FCC, IC, ETSI, CE, EN 60601-1-2, IEC60950,
IEC62368, UL2043, EN 61373

XV2-21X Wi-Fi 6 Access Point

Network Specifications

Note: Some features will be included on subsequent firmware releases.

Operational Modes	Controller-less standalone Cloud-managed cnMaestro, VM	RF Management	Multi-Modal RF optimization supporting AutoRF (cnMaestro) performed in the intelligent edge AP. Out of band RF spectrum analysis, RF monitor with chn/noise/interference
WLAN	16 WLAN profiles per radio 128 clients per radio, 16 SSIDs, WPA-TKIP, WPA2 AES, 802.1x 802.11w PMF	Network	TCP connection log, NAT logging firewall, DHCP server, L2, L3 or DNS based access control, VLAN Pooling, RADIUS attribute VID VLAN per SSID per user
Guest Access/Captive Portal	cnMaestro, On-AP hosted guest portal Social login, Voucher based login, SMS gateway, Payment gateway support. Supports radius based authentication. cnMaestro API support for external captive portal integration.	Band Steer Load Balance	Yes
Authentication Encryption	Hotspot 2.0, 802.1x EAP-SIM/AKA, EAP-PEAP, EAP-TTLS, EAP-TLS, MAC Authentication local database or RADIUS	Tunnel	L2TPv2, L2GRE, PPPoE
Scheduled WLAN	On/off by day, week, time of day	Network Tools	Wired and wireless remote packet capture, logging, ZapD
Data Limit	Client bitrate/time/throughput limit per SSID	Network and RF Management Tools	Wired and wireless remote packet capture, ZapD performance tool, rogue AP detection
Subscriber QoS	WMM	Services	L2-L7 application visibility & control, WiFi Calling control, WIDs/WIPs, NTP, Syslog, SNMP traps, DNS proxy, auto-off on WAN failure
Fast Roaming	802.11r, OKC, cnMaestro assisted roam	API	RESTful management and statistics API Presence location APIs
Mesh	Multi-hop, either band	IP	IPv4, IPv6
Channel Selection	Multi-modal channel selection with AutoChannel and autotune (cnMaestro)		

Standards

Wi-Fi Protocols	VHT MCS rates, 16/64/256/1024-QAM, 20/40/80/160 MHz
	TWT, Long OFDM Symbol, Transmit beamforming, Airtime Fairness, AMSDU, AMPDU, RIFS, STBC, LDPC, MIMO Power Save, MRC, BPSK, QPSK, CCK, DSSS, OFDM, OFDMA, UL/DL MU-MIMO
	IEEE 802.11 a/ac/ax/b/d/e/g/h/i/k/n/r/u/v

XV2-21X Wi-Fi 6 Access Point

Management



To serve a growing market for advanced management and services functionality, Cambium Networks offers cnMaestro™ in two different management tiers:

cnMaestro Essentials

License-free management that delivers a disruptive Total Cost of Ownership (TCO) for organizations of all sizes.

cnMaestro X

Paid subscription that includes:

- Advanced device management capabilities.
- Cambium Care Pro for 24x7 technical support.
- Accelerated access to L2 engineers and regular software updates.
- Upgrades for advanced features.

For More information, please visit:

cambiumnetworks.com/products/software/cnmaestro-essentials

cambiumnetworks.com/products/advanced-services/cnmaestro-x

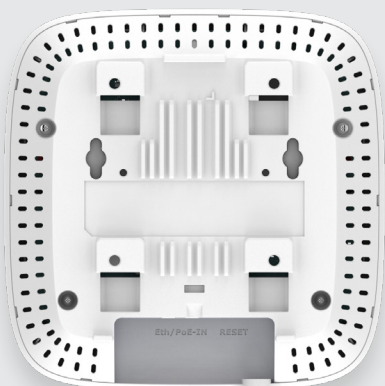
XV2-21X Wi-Fi 6 Access Point



Front Panel



Front Oblique



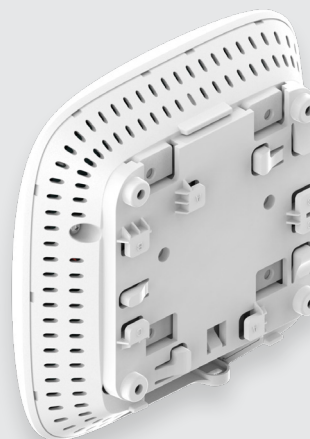
Back Panel



Bottom / Ports



Front Panel with
Mounting Bracket

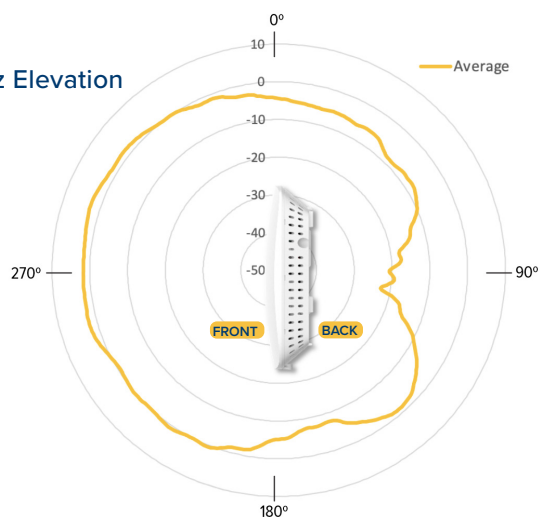


Back Panel with
Mounting Bracket

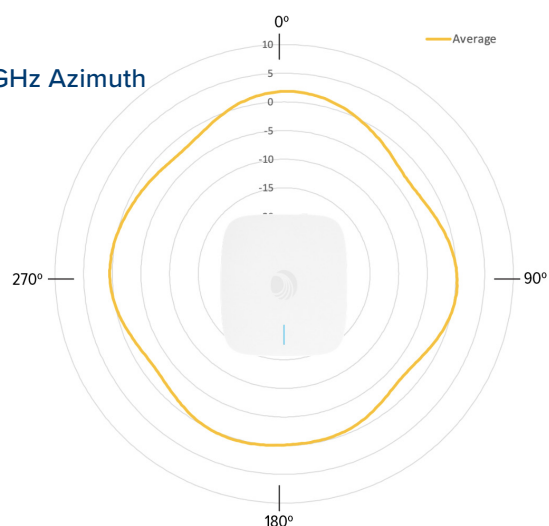
XV2-21X Wi-Fi 6 Access Point

Antenna Patterns

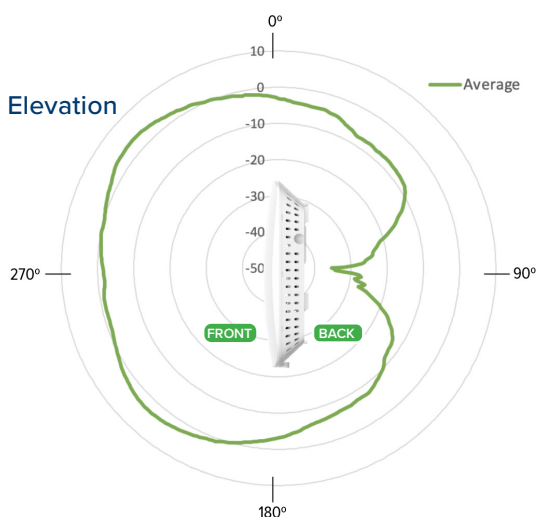
2.4 GHz Elevation



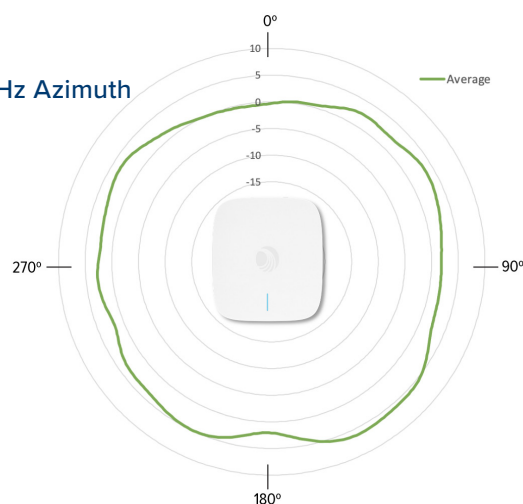
2.4 GHz Azimuth



5 GHz Elevation



5 GHz Azimuth



2.4 GHz Receive Sensitivity (dBm) Per Chain

HT20		HT40	
MCS0	-95.5	MCS0	-93
MCS7	-76.5	MCS7	-74
HE20		HE40	
MCS0	-95.5	MCS0	-92.5
MCS7	-76.5	MCS7	-73.5

2.4 GHz TX Power Target

Rate	Pout (dBm)
MCS0 HT20	27
MCS7 HT20	25
MCS8 VHT20	25
MCS9 VHT40	24
MCS11 HE40	23

5 GHz Receive Sensitivity (dBm) Per Chain

VHT20	VHT40	VHT80	VHT160
MCS0 -95.5	MCS0 -94	MCS0 -90	MCS0 -87.5
MCS7 -77	MCS7 -74	MCS7 -71.5	MCS7 -69
HE20	HE40	HE80	HE160
MCS0 -95.5	MCS0 -93.5	MCS0 -90.5	MCS8 -65
MCS7 -76.5	MCS7 -74	MCS7 -71.5	MCS11 -57

5 GHz TX Power Target

Rate	Pout (dBm)
MCS0 VHT20	27
MCS7 VHT20	24
MCS0 VHT40, VHT80	27, 27
MCS7 VHT40, VHT80	24, 24
MCS11, HE20, HE40, HE80, HE160	22, 22, 22, 21

XV2-21X Wi-Fi 6 Access Point

Cambium Ordering Information

Regulatory Model	XV2-21X
XV2-21X0A00-US	XV2-21X Indoor Dual radio WiFi 6 AP, 2x2, GbE, US
XV2-21X0A00-EU	XV2-21X Indoor Dual radio WiFi 6 AP, 2x2, GbE, EU
XV2-21X0A00-RW	XV2-21X Indoor Dual radio WiFi 6 AP, 2x2, GbE, RW
XV2-21X0A00-CA	XV2-21X Indoor Dual radio WiFi 6 AP, 2x2, GbE, CA
N000000L142A	N000000L142A PoE injector, 60W, 5 GbE, Indoor, Energy Level 6 Supply
N000000L034B	PoE, 30.5W, 56V, GbE DC Injector, Indoor, Energy Level 6 Supply, accepts C5 connector
N000900L017A	PoE, 15.4W, 56V, GbE DC Injector, Indoor, Energy Level 6 Supply, accepts C5 connector
XA-DROPTILE15	Recessed ceiling tile Installation Kit for 15mm T-bar, 20mm drop extension. 5 Pack
XA-DROPTILE24	Recessed ceiling tile Installation Kit for 24mm T-bar, 20mm drop extension. 5 Pack
AX-E510RBKT-WW	Shock mount bracket

cnMaestro X Ordering Information

MSX-SUB-XV2-21X-1	cnMaestro X for one XV2-21X AP. Creates one Device Tier 3 slot. Includes Cambium Care Pro support. 1-year subscription
MSX-SUB-XV2-21X-3	cnMaestro X for one XV2-21X AP. Creates one Device Tier 3 slot. Includes Cambium Care Pro support. 3-year subscription
MSX-SUB-XV2-21X-5	cnMaestro X for one XV2-21X AP. Creates one Device Tier 3 slot. Includes Cambium Care Pro support. 5-year subscription

XV2-21X Wi-Fi 6 Access Point

Cambium Care Ordering Information

CCADV-SUP-XV2-21X-1	Cambium Care Advanced, 1-year support for one XV2-21X Wi-Fi 6/6E AP. 24x7 TAC support, SW updates, and NBD advance replacement for HW
CCADV-SUP-XV2-21X-3	Cambium Care Advanced, 1-year support for one XV2-21X Wi-Fi 6/6E AP. 24x7 TAC support, SW updates, and NBD advance replacement for HW
CCADV-SUP-XV2-21X-5	Cambium Care Advanced, 3-year support for one XV2-21X Wi-Fi 6/6E AP. 24x7 TAC support, SW updates, and NBD advance replacement for HW
CCPRO-SUP-XV2-21X-1	Cambium Care Pro, 1-year support for one XV2-21X Wi-Fi 6/6E AP. 24x7 TAC support and SW updates
CCPRO-SUP-XV2-21X-3	Cambium Care Pro, 3-year support for one XV2-21X Wi-Fi 6/6E AP. 24x7 TAC support and SW updates
CCPRO-SUP-XV2-21X-5	Cambium Care Pro, 5-year support for one XV2-21X Wi-Fi 6/6E AP. 24x7 TAC support and SW updates
CCADV-UPG-XV2-21X-1	Cambium Care Advanced Add-on to cnMaestro X, 1-year support for one XV2-21X. 24x7 TAC support, SW updates, and NBDS advance replacement for HW
CCADV-UPG-XV2-21X-3	Cambium Care Advanced Add-on to cnMaestro X, 3-year support for one XV2-21X. 24x7 TAC support, SW updates, and NBDS advance replacement for HW
CCADV-UPG-XV2-21X-5	Cambium Care Advanced Add-on to cnMaestro X, 5-year support for one XV2-21X. 24x7 TAC support, SW updates, and NBDS advance replacement for HW

LIMITED WARRANTY

Cambium Networks XV2-21X Wi-Fi 6 Access Point includes a limited hardware warranty for a period of 5 years after end of sale.

ABOUT CAMBIUM NETWORKS

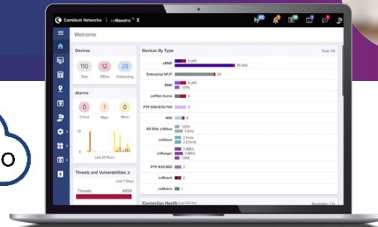
Cambium Networks empowers millions of people with wireless connectivity worldwide. Its wireless portfolio is used by commercial and government network operators as well as broadband service providers to connect people, places and things. With a single network architecture spanning fixed wireless and Wi-Fi, Cambium Networks enables operators to achieve maximum performance with minimal spectrum. End-to-end cloud management transforms networks into dynamic environments that evolve to meet changing needs with minimal physical human intervention. Cambium Networks empowers a growing ecosystem of partners who design and deliver gigabit wireless solutions that just work.

XV2-21X Wi-Fi 6 Access Point

802.11ax Dual-Radio Indoor Access Point

XV2-21X Quick Look:

- Dual-radio Wi-Fi 6
- 5 GHz (2x2), 2.4 GHz (2x2)
- 1 GbE RJ45 interface
- cnMaestro™ Network Management
- Limited lifetime warranty



Value-Tier Wi-Fi for Any Market

Cambium Networks' XV2-21X Wi-Fi 6 Indoor Access Point (AP) delivers a high performance-to-price ratio attractive to any market.

The XV2-21X can be adopted and managed by any of the Cambium management systems, including cnMaestro Essentials and cnMaestro X, available in cloud and on-premises versions. Choose the management type you need and change it at any time.

Unlike other value-tier access points, the XV2-21X is never locked into just one management selection.

Designed for Fast Installation

The XV2-21X offers multiple installation methods included in the same shipping box. Mount the AP to a ceiling tile using the included steel plate; mount to an existing junction box with 83 mm center-to-center holes; twist lock the AP onto a 36 mm, 24 mm, and 14 mm T-bar; or simply mount it to any flat surface using the included wall anchors. No additional accessory brackets are needed.



XV2-21X back panel with mounting bracket

XV2-21X Wi-Fi 6 Access Point

Specifications

Radios	5 GHz 802.11 a/n/ac/ax, 2x2:2 2.4 GHz 802.11 b/g/n/ax, 2x2:2	Power	Typical 11W, 802.3af powered device
Wi-Fi	802.11 a/b/g/n/ac/ax	Dimensions	155 mm x 155 mm x 37 mm (6.1 in x 6.1 in x 1.46 in) With Bracket: 155 x 155 x 46 mm (6.1 x 6.1 x 1.81 in)
SSID Security	WPA3-SAE, WPA3-Enterprise, WPA2 (CCMP, AES, 802.11i), WPA2 Enterprise (802.1x/EAP), OSEN, OWE, Open	Weight	475 g (1.05 lb)
Max PHY Rate	5 GHz radio 2402 Mbps 2.4 GHz radio 573.5 Mbps	Mount Options	Wall or ceiling, T-bar with included locking bracket, ceiling tile plate
Ports	1 x IEEE 10/100/1000 Mbps	Ambient Operation Temperature	0°C to 50°C (32°F to 122°F)
Antenna Gain	5 GHz 6 dBi 2.4 GHz 5 dBi	Storage Temperature	-40°C to 70°C (-40°F to 158°F)
FCC	Ch 1–11, 36–48, 52–64, 100–144, 149–165	Humidity	95% RH non-condensing
ISED	Ch 1–11, 36–48, 52–64, 100–116, 149–165	MTBF	831,902 hours at 50°C ambient
ETSI*	Ch 1–13, 36–48, 52–64, 100–140, 149–173	LEDs	Multi-color status LEDs, dimmable, on/off
ROW*	Ch 1–14, 36–48, 52–64, 100–144, 149–173	Certifications (compliance)	Wi-Fi Alliance, Passpoint 3.0, 802.11 a/b/e/g/i/k/n/r/u/v/w/ac/ax, FCC, IC, ETSI, CE, EN 60601-1-2, IEC60950, IEC62368, UL2043, EN 61373

*Individual country limits may apply. Please contact your regional sales manager for country-specific regulations. For Southeast Asia (SEA) countries, refer to the SEA Regulatory Details chart in this data sheet.

Standards

Wi-Fi Protocols	Data coding support 16/64/256/1024-QAM Channel width support under 5 GHz band: 20/40/80/160 MHz
	TWT, long OFDM symbol, transmit beamforming, airtime fairness, AMSDU, AMPDU, RIFS, STBC, LDPC, MIMO power save, MRC, BPSK, QPSK, CCK, DSSS, OFDM, OFDMA, UL/DL MU-MIMO
	IEEE 802.11 a/ac/ax/b/d/e/g/h/i/k/n/r/u/v/w

XV2-21X Wi-Fi 6 Access Point

Network Specifications

Operational Modes	Controllerless standalone cloud-managed cnMaestro, VM	RF Management	Multi-modal RF optimization supporting Auto-R for dynamic channel selection and dynamic power adjustment configured via cnMaestro, performed in the intelligent edge AP. RF monitor with channel utilization/packet error rate/interference.
WLAN	128 concurrent clients per radio, 256 per AP 16 SSID per AP		
Security, Authentication Encryption	Open, WPA2-AES with PSK, ePSK and Enterprise WPA3 with PSK (WPA3-SAE), ePSK, Enterprise, Enterprise-CNSA, OWE (Enhanced Open) OSEN and PMF (802.11 W) MAC authentication with local database or external database using RADIUS protocol 802.1X with EAP-TTLS, EAP-TLS/MSCHAPv2, PEAPv0/PEAPv1/EAP-PEAP/EAP-SIM/AKA/FAST Hotspot 2.0 WEB authentication	Band Steering	Yes
		Mesh	Multi-hop, either band
		Scheduled WLAN	On/off by day, week, time of day
		Data Limit	Client bitrate/time/throughput limit per SSID
		Network	TCP connection log, NAT logging firewall, DHCP server, DHCP Relay option 82, VLAN pooling, RADIUS attribute, VID VLAN per SSID per user, ePSK with VLAN assignment per PSK LLDP, IGMP v1, v2
Wi-Fi Quality of Service	802.11e / WMM (packet marking either with 802.1p or IP DSCP), WMM-PS, U-APSD Multicast to unicast conversion	Network Tools	Wired and wireless remote packet capture, logging, WAN speed test, ZapD, remote network connectivity tools
Service Availability	Critical network resource monitor with SSID shutdown	Tunnel	L2TPv2, L2GRE, PPPoE
Fast Roaming	802.11k/r/v, OKC, cnMaestro-assisted roam	IP	IPv4, IPv6
Guest Access/ Captive Portal Service (EasyPass)*	cnMaestro-hosted EasyPass portal Multiple authentication methods supported to onboard guest user: <ul style="list-style-type: none"> Radius-based authentication Click-through with simple terms and conditions acceptance Social login using Google®, Facebook® SMS-based authentication (X) Voucher-based access Microsoft® Azure AD and Google Workspace® (X) Sponsored guest access (X) Self-registration access (X) cnMaestro API support for external captive portal integration 802.11u, Hotspot 2.0	VLAN	802.11Q, max 4096
		Management Interfaces	HTTP / HTTPS web interface, SSH, Telnet SNMP V1, V2, V3 Syslog, SNMP traps, NTP
		Security	Rogue AP detection and termination(X), WIDs/WIPs, DoS protection L2–L7 firewall with application visibility(X) & control(X), DNS based access control(X). ACL and AirCleaner tools
		Services	Wi-Fi Calling control, NTP, Syslog, DNS proxy, SNMP traps, SNMPv1, SNMPv2c, SNMPv3, TCP and DNS logging
Accounting	RADIUS accounting, load balancing AAA servers, Dynamic Authorization COA, DM		
API	RESTful management and statistics API via cnMaestro X, presence location push APIs		

*X features available in cnMaestro X.

XV2-21X Wi-Fi 6 Access Point

Management



cnMaestro uses a distributed intelligence architecture with cloud-first management and edge-intelligent APs that self-optimize for the RF environment. cnMaestro delivers a single pane-of-glass management for Cambium broadband fixed wireless, cnMatrix Ethernet Switches, enterprise-grade Wi-Fi APs, NSE Service Edge, and residential service provider routers.

cnMaestro can be deployed on cloud or on-premises via a virtual machine.

To serve a growing market for advanced management and services functionality, Cambium Networks offers cnMaestro in two management tiers:

cnMaestro X

Paid subscription that includes:

- Advanced device management capabilities
- Deep packet inspection (DPI) application visibility and Control for 2,400+ apps
- RESTful management and statistics API
- Presence location push APIs
- Graphic reports
- Webhooks
- Cambium Care Pro for 24x7 technical support
- Accelerated access to L2 engineers and regular software updates

Assists

- Assesses the network's configuration and identifies weak security settings and proposes a fix to ensure the network configuration is up to the top security industry standards

cnMaestro Essentials

License-free cloud management that delivers a disruptive total cost of ownership (TCO) for organizations of all sizes. Includes EasyPass for OneClick or voucher-based connection as well as WiFi4EU access.

X Assurance

- Helps to quickly identify network-wide connectivity issues by isolating every element of the client's lifecycle, either radio or network related
- Gives an overview quality index of the network and highlights each element's contribution to easily identify the worst offender
- Provides insight of probable causes and proposes fixes for the administrator to apply
- Provides individual client connectivity visibility throughout the entire lifecycle of its connection to easily identify each connection's result and highlight the failure reason, should there be any

EasyPass Portal with Additional Options

- Self-registration: Form-based access
- Sponsored guest: Guest ambassador-based access
- Paid access: Monetize the Wi-Fi access
- Microsoft Azure: Corporate user login
- Google Login: Web login using Google accounts

**Find out more about
cnMaestro**

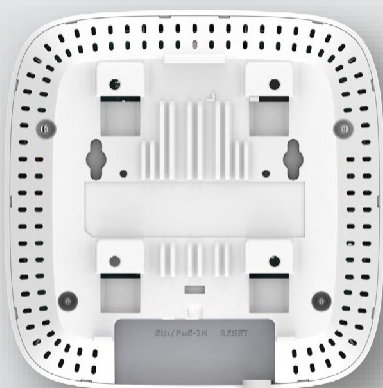
XV2-21X Wi-Fi 6 Access Point



Front



Front Oblique



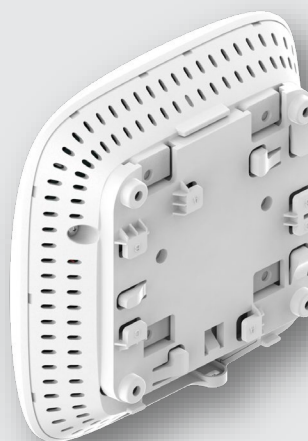
Back Panel



Bottom/Ports



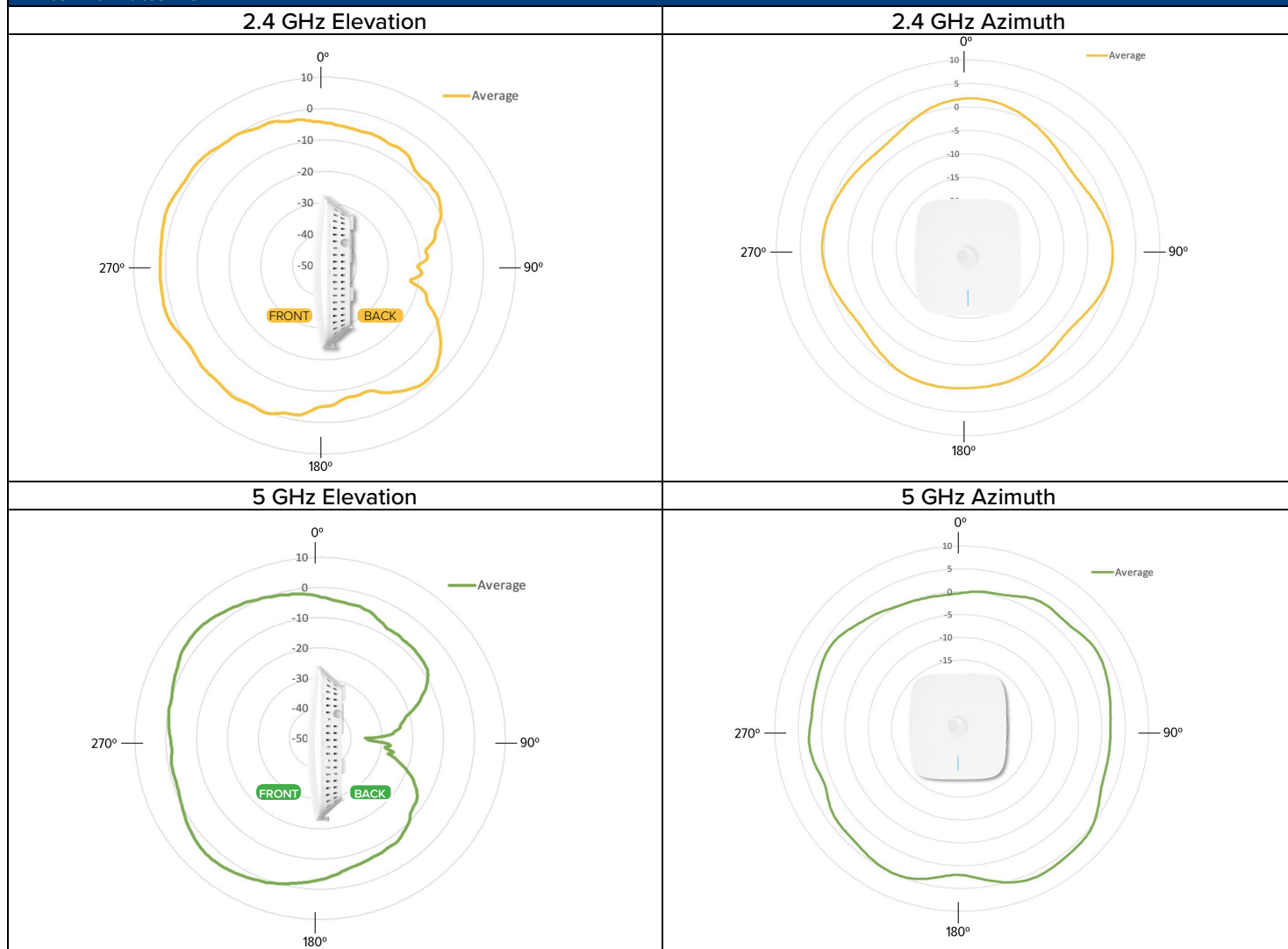
Front Panel with
Mounting Bracket



Back Panel with
Mounting Bracket

XV2-21X Wi-Fi 6 Access Point

Antenna Patterns



2.4 GHz Receive Sensitivity (dBm) per Chain

HT20		HT40	
MCS0	-95.5	MCS0	-93
MCS7	-76.5	MCS7	-74
HE20		HE40	
MCS0	-95.5	MCS0	-92.5
MCS7	-76.5	MCS7	-73.5

2.4 GHz TX Power Target

Rate	Pout (dBm)
MCS0 HT20	27
MCS7 HT20	25
MCS8 VHT20	25
MCS9 VHT40	24
MCS11 HE40	23

5 GHz Receive Sensitivity (dBm) per Chain

VHT20	VHT40	VHT80	VHT160
MCS0	-95.5	MCS0	-94
MCS7	-77	MCS7	-74
MCS0	-95.5	MCS0	-93.5
MCS7	-76.5	MCS7	-74
HE20		HE40	
MCS0	-95.5	MCS0	-90.5
MCS7	-76.5	MCS7	-71.5
HE80		HE160	
MCS0	-95.5	MCS0	-87.5
MCS7	-77	MCS7	-69
MCS0	-95.5	MCS0	-92.5
MCS7	-76.5	MCS7	-73.5

5 GHz TX Power Target

Rate	Pout (dBm)
MCS0 VHT20	27
MCS7 VHT20	24
MCS0 VHT40, VHT80	27, 27
MCS7 VHT40, VHT80	24, 24
MCS11, HE20, HE40, HE80, HE160	22, 22, 22, 21

XV2-21X Wi-Fi 6 Access Point

XV2-21X Ordering Information

Regulatory Model	XV2-21X
XV2-21X0A00-US	XV2-21X Indoor Dual radio WiFi 6 AP, 2x2, GbE, US
XV2-21X0A00-EU	XV2-21X Indoor Dual radio WiFi 6 AP, 2x2, GbE, EU
XV2-21X0A00-RW	XV2-21X Indoor Dual radio WiFi 6 AP, 2x2, GbE, RW
XV2-21X0A00-CA	XV2-21X Indoor Dual radio WiFi 6 AP, 2x2, GbE, CA
C000000L141A	PoE, 60W, 56V, 10GbE DC Injector, Indoor, Energy Level 6 Supply
N000000L034B	PoE, 30.5W, 56V, GbE DC Injector, Indoor, Energy Level 6 Supply, accepts C5 connector
N000900L017A	PoE, 15.4W, 56V, GbE DC Injector, Indoor, Energy Level 6 Supply, accepts C5 connector
XA-DROPTILE15	Recessed ceiling tile Installation Kit for 15mm T-bar, 20mm drop extension. 5 Pack
XA-DROPTILE24	Recessed ceiling tile Installation Kit for 24mm T-bar, 20mm drop extension. 5 Pack

cnMaestro X Subscriptions

MSX-SUB-XV2-21X-1	cnMaestro X for one XV2-21X AP. Creates one Device Tier 3 slot. Includes Cambium Care Pro support. 1-year subscription
MSX-SUB-XV2-21X-3	cnMaestro X for one XV2-21X AP. Creates one Device Tier 3 slot. Includes Cambium Care Pro support. 3-year subscription
MSX-SUB-XV2-21X-5	cnMaestro X for one XV2-21X AP. Creates one Device Tier 3 slot. Includes Cambium Care Pro support. 5-year subscription

Cambium Care Support

CCADV-SUP-XV2-21X-1	Cambium Care Advanced, 1-year support for one XV2-21X Wi-Fi 6/6E AP. 24x7 TAC support, SW updates, and NBD advance replacement for HW
CCADV-SUP-XV2-21X-3	Cambium Care Advanced, 3-year support for one XV2-21X Wi-Fi 6/6E AP. 24x7 TAC support, SW updates, and NBD advance replacement for HW
CCADV-SUP-XV2-21X-5	Cambium Care Advanced, 5-year support for one XV2-21X Wi-Fi 6/6E AP. 24x7 TAC support, SW updates, and NBD advance replacement for HW
CCPRO-SUP-XV2-21X-1	Cambium Care Pro, 1-year support for one XV2-21X Wi-Fi 6/6E AP. 24x7 TAC support and SW updates
CCPRO-SUP-XV2-21X-3	Cambium Care Pro, 3-year support for one XV2-21X Wi-Fi 6/6E AP. 24x7 TAC support and SW updates
CCPRO-SUP-XV2-21X-5	Cambium Care Pro, 5-year support for one XV2-21X Wi-Fi 6/6E AP. 24x7 TAC support and SW updates
CCADV-UPG-XV2-21X-1	Cambium Care Advanced Add-on to cnMaestro X, 1-year support for one XV2-21X. 24x7 TAC support, SW updates, and NBDS advance replacement for HW
CCADV-UPG-XV2-21X-3	Cambium Care Advanced Add-on to cnMaestro X, 3-year support for one XV2-21X. 24x7 TAC support, SW updates, and NBDS advance replacement for HW
CCADV-UPG-XV2-21X-5	Cambium Care Advanced Add-on to cnMaestro X, 5-year support for one XV2-21X. 24x7 TAC support, SW updates, and NBDS advance replacement for HW

XV2-21X Wi-Fi 6 Access Point

EIRP is limited to the countries listed below.

SE Asia Regulatory Details					
Country	2.4 GHz (EIRP)	5 GHz (EIRP)			
	2400–2483.5 MHz	5150–5250 MHz	5250–5350 MHz	5470–5725 MHz	5725–5825 MHz
Indonesia	27 dBm (500mW) indoor	23 dBm (200mW) indoor	23 dBm (200mW) indoor	Not supported	23 dBm (200mW) indoor,
	36 dBm (4W) outdoor				36 dBm (4W) outdoor
Vietnam	23 dBm (200mW)	23 dBm (200mW)	23 dBm (200mW)	30 dBm (1W)	30 dBm (1W)
Philippines	26 dBm (400mW)	26 dBm (400mW)	26 dBm (400mW)	26 dBm (400mW)	26 dBm (400mW)
Malaysia*	27 dBm (500mW)	30 dBm (1W) indoor	30 dBm (1W) indoor	5470–5650 MHz	30 dBm (1W)
		23 dBm (200mW) outdoor		30 dBm (1W)	
Singapore	23 dBm (200mW)	23 dBm (200mW)	23 dBm (200mW)	30 dBm (1W)	30 dBm (1W)
Thailand	20 dBm (100mW)	23 dBm (200mW)	23 dBm (200mW)	30 dBm (1W)	30 dBm (1W)

*Malaysia restricts the use of 5650 MHz–5725 MHz for regulatory reasons.

LIMITED WARRANTY

Cambium Networks XV2-21X Wi-Fi 6 Access Point includes a limited lifetime hardware warranty that extends 5 years after end of sale.

ABOUT CAMBIUM NETWORKS

Cambium Networks enables service providers, enterprises, industrial organizations, and governments to deliver exceptional digital experiences and device connectivity with compelling economics. Our ONE Network platform simplifies management of Cambium Networks' wired and wireless broadband and network edge technologies. Our customers can focus more resources on managing their business rather than the network. We make connectivity that just works.

cambiumnetworks.com

10222024

XV2-23T Wi-Fi 6 Outdoor Access Point

802.11ax Dual-Radio, 2x2

XV2-23T Quick Look:

Value tier outdoor Wi-Fi 6 access point designed for cost-effective upgrade to the latest 802.11ax standard in Wi-Fi technology.

- Dual-radio Wi-Fi 6
- 5 GHz (2x2), 2.4 GHz (2x2)
- One 1 GbE uplink
- Outdoor rated IP67 enclosure
- cnMaestro™ Network Management

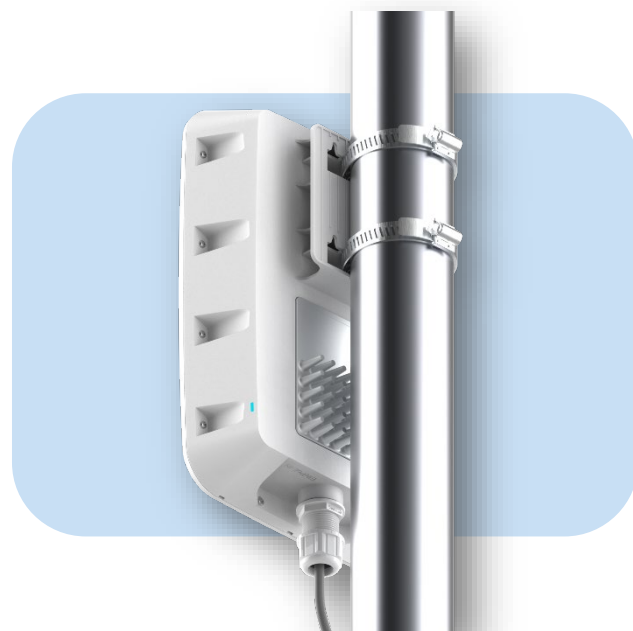


Value-Tier Wi-Fi for Any Market

The Cambium Networks' XV2-23T Wi-Fi 6 Outdoor Access Point (AP) delivers a high performance-to-price ratio attractive to any market. The XV2-23T can be onboarded and managed by your choice of Cambium management systems, including cnMaestro™ Essentials and cnMaestro X, available in cloud and on-premises versions. Choose the management type you need and change it at any time. Unlike other value-tier access points, the XV2-23T is never locked into just one management selection.

Designed for Fast Installation

The XV2-23T offers multiple installation methods included in the same shipping box. Mount the AP to a pole using the included clamps or to a flat surface using the integrated bracket. The XV2-23T is a compact size and high-performance outdoor Wi-Fi 6 AP.



XV2-23T Wi-Fi 6 Outdoor Access Point

Access Point Specifications

Radios	5 GHz 802.11 a/n/ac/ax, 2x2 2.4 GHz 802.11 b/g/n/ax, 2x2	Power	Typical 20W, 802.3af powered device
Wi-Fi	802.11 a/b/g/n/ac/ax	Dimensions	300 mm x 200 mm x 84 mm (11.8 in x 7.9 in x 3.3 in)
SSID Security	WPA3-SAE, WPA3-Enterprise, WPA2-PSK (CCMP, AES, 802.11i), WPA2-Enterprise (802.1X/EAP), OSEN, OWE, Open	Weight	1,200 g (2.65 lbs)
Ports	1 x IEEE 100/1000 Mbps Ethernet	Security	Kensington lock slot
Antenna Gain	5 GHz 10 dBi, Omni 2.4 GHz 7 dBi, Omni	Mount Options	Pole or wall mounting. Pole diameter: min 30 mm / max 75 mm
Max EIRP*	5 GHz 36 dBm 2.4 GHz 34 dBm	Ambient Operation Temperature	-40°C to 65°C (-40°F to 149°F)
Max PHY Rate	5 GHz radio 2,402 Mbps 2.4 GHz radio 573.5 Mbps	Storage Temperature	-40°C to 70°C (-40°F to 158°F)
Filter LTE Band	38, 40	Humidity	95% RH non-condensing
FCC	Ch 1–11, 36–48, 52–64, 100–144, 149–165	MTBF	5,077,102 hours @ 25°C 1,224,983 hours @ 65°C
ISED	Ch 1–11, 36–48, 52–64, 100–116, 149–165	LEDs	Multi-color status LEDs, dimmable, on/off
ETSI*	Ch 1–13, 36–64, 52–64, 100–140, 149–173	Certifications	WiFi Alliance 802.11a/b/g/n/ac/ax, PP2.0
ROW*	Ch 1–14, 36–48, 52–64, 100–144, 149–177	(compliance)	FCC, CE, IC, IEC60950, IEC62368, EN50121, EN61373

*Individual country limits may apply.

Standards

Wi-Fi Protocols	VHT MCS rates, 16/64/256/1024/4096-QAM, Channel width support in 5GHz: 20/40/80/160 MHz
	Transmit Beam steering, Airtime Fairness, AMSDU, AMPDU, RIFS, STBC, LDPC, MIMO Power Save, MRC, BPSK, QPSK, CCK, DSSS, OFDM, OFDMA, UL/DL MU-MIMO
	IEEE 802.11a/ac/ax/b/d/e/g/h/i/k/n/r/u/v/w

XV2-23T Wi-Fi 6 Outdoor Access Point

Network Specifications

Operational Modes	Controllerless standalone Cloud-managed cnMaestro or VM	RF Management	Multi-modal RF optimization supporting Auto-RF for dynamic channel selection and dynamic power adjustment configured via cnMaestro, performed in the intelligent edge AP. RF monitor with channel utilization/ packet error rate / interference.
WLAN	256 concurrent clients 16 SSIDs per AP	Band Steering	Yes
Security, Authentication Encryption	Open, WPA2-AES with PSK, ePSK and Enterprise WPA3 with PSK (WPA3-SAE), ePSK, Enterprise, Enterprise-CNSA, OWE (Enhanced Open) OSEN and PMF (802.11 W) MAC authentication with local database or external database using RADIUS protocol 802.1X with EAP-TTLS, EAP-TLS / MSCHAPv2, PEAPv0 / PEAPv1 / EAP-PEAP / EAP-SIM/AKA/AKA'/FAST Hotspot 2.0 WEB authentication	Mesh	Multi-hop, either band
Wi-Fi Quality of Service	WMM (packet marking either with 802.1p or IP DSCP), WMM-PS, U-APSD Multicast to unicast conversion	Scheduled WLAN	On/off by day, week, time of day
Service Availability	Critical network resource monitor with SSID shutdown	Data Limit	Client bitrate/time/throughput limit per SSID
Fast Roaming	802.11k/r/v, OKC, cnMaestro-assisted roam	Network	TCP connection log, NAT logging firewall, DHCP server, DHCP Relay option 82, VLAN pooling, RADIUS attribute, VID VLAN per SSID per user, ePSK with VLAN assignment per PSK LLDP, IGMP v1, v2
Guest Access/ Captive Portal Service (EasyPass)*	cnMaestro-hosted EasyPass portal Multiple authentication methods supported to onboard guest user: <ul style="list-style-type: none"> Radius-based authentication Click-through with simple terms and conditions acceptance Social login using Google®, Facebook® SMS-based authentication (X) Voucher-based access Microsoft® Azure AD and Google Workspace® (X) Sponsored guest access (X) Self-registration access (X) cnMaestro API support for external captive portal integration 802.11u, Hotspot 2.0	Network Tools	Wired and wireless remote packet capture, logging, WAN speed test, ZapD, remote network connectivity tools
Accounting	RADIUS accounting, load balancing AAA servers, Dynamic Authorization COA, DM	Tunnel	L2TPv2, L2GRE, PPPoE
API	RESTful management and statistics API via cnMaestro X, presence location push APIs	IP	IPv4, IPv6
		VLAN	802.11Q, max 4096
		Management Interfaces	HTTP / HTTPS web interface, SSH, Telnet
		Security	Rogue AP detection and termination(X), WIDs/WIPs, DoS protection L2–L7 firewall with application visibility(X) & control(X), DNS based access control(X). ACL and AirCleaner tools
		Services	Wi-Fi Calling control, NTP, Syslog, DNS proxy, SNMP traps, SNMPv1, SNMPv2c, SNMPv3, TCP and DNS logging

*X features available in cnMaestro X.

XV2-23T Wi-Fi 6 Outdoor Access Point

Management



cnMaestro uses a distributed intelligence architecture with cloud-first management and edge-intelligent APs that self-optimize for the RF environment. cnMaestro delivers a single pane-of-glass management for Cambium broadband fixed wireless, cnMatrix Ethernet Switches, enterprise-grade Wi-Fi APs, NSE Service Edge, and residential service provider routers.

cnMaestro can be deployed on cloud or on-premises via a virtual machine.

To serve a growing market for advanced management and services functionality, Cambium Networks offers cnMaestro in two management tiers:

cnMaestro X

Paid subscription that includes:

- Advanced device management capabilities
- Deep packet inspection (DPI) application visibility and Control for 2,400+ apps
- RESTful management and statistics API
- Presence location push APIs
- Graphic reports
- Webhooks
- Cambium Care Pro for 24x7 technical support
- Accelerated access to L2 engineers and regular software updates

Assists

- Assesses the network's configuration and identifies weak security settings and proposes a fix to ensure the network configuration is up to the top security industry standards

cnMaestro Essentials

License-free cloud management that delivers a disruptive total cost of ownership (TCO) for organizations of all sizes. Includes EasyPass for OneClick or voucher-based connection as well as WiFi4EU access.

X Assurance

- Helps to quickly identify network-wide connectivity issues by isolating every element of the client's lifecycle, either radio or network related
- Gives an overview quality index of the network and highlights each element's contribution to easily identify the worst offender
- Provides insight of probable causes and proposes fixes for the administrator to apply
- Provides individual client connectivity visibility throughout the entire lifecycle of its connection to easily identify each connection's result and highlight the failure reason, should there be any

EasyPass Portal with Additional Options

- Self-registration: Form-based access
- Sponsored guest: Guest ambassador-based access
- Paid access: Monetize the Wi-Fi access
- Microsoft Azure: Corporate user login
- Google Login: Web login using Google accounts

**Find out more about
cnMaestro**

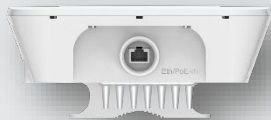
XV2-23T Wi-Fi 6 Outdoor Access Point



Front



Back



Bottom



Side

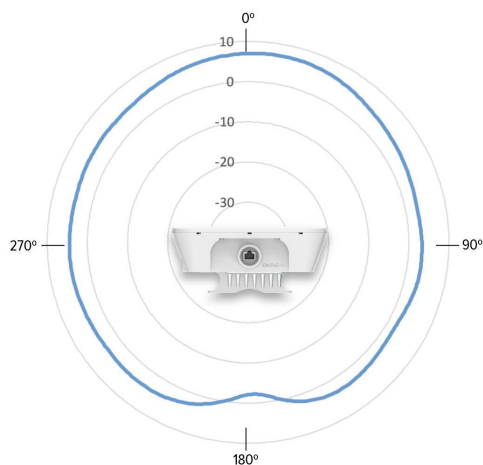


Front Oblique

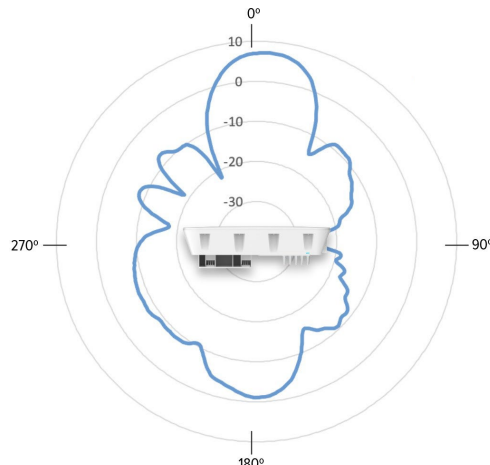
XV2-23T Wi-Fi 6 Outdoor Access Point

Antenna Patterns

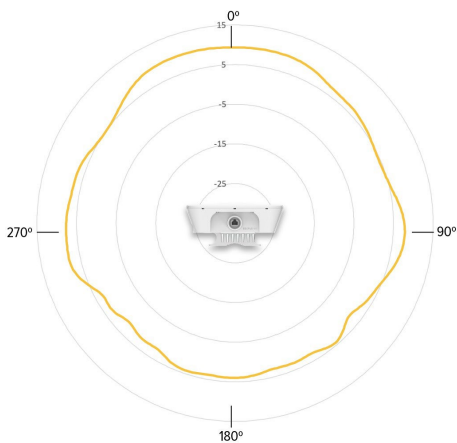
2.4 GHz Azimuth



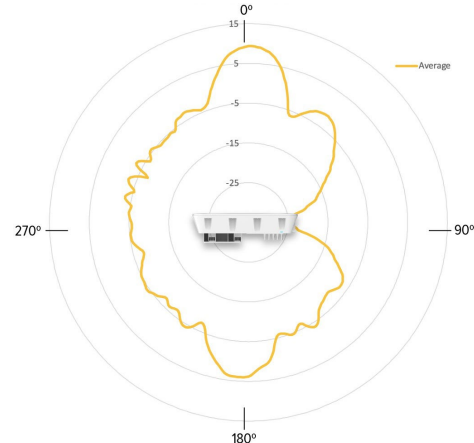
2.4 GHz Elevation



5 GHz Azimuth



5 GHz Elevation



2.4 GHz Receive Sensitivity (dBm) per Chain

802.11b		802.11g	
1 Mb	-99	1 Mb	-94.5
11 Mb	-91	11 Mb	-75.75
HT20		HT40	
MCS0	-95	MCS0	-92.5
MCS7	-76.5	MCS7	-73.5
HE20		HE40	
MCS0	-94.75	MCS0	-92
MCS11	-64.25	MCS11	-61.25

2.4 GHz TX Power Target

Rate	Pout (dBm)
802.11b 1Mb	27
802.11g 6Mb	27
MCS0 HT20, HT40	27, 27
MCS7 HT20, HT40	25, 25
MCS0 VHT20, VHT40	27, 27
MCS11 VHT20, VHT40	23, 23
MCS0 HE20, HE40	27, 27
MCS11 HE20, HE40	23, 23

5 GHz Receive Sensitivity (dBm) per Chain

VHT20	VHT40	VHT80	VHT160
MCS0	-95.5	MCS0	-90
MCS7	-77	MCS7	-71.5
HE20	HE40	HE80	HE160
MCS0	-95.5	MCS0	-90.5
MCS7	-76.5	MCS7	-71.5

5 GHz TX Power Target

Rate	Pout (dBm)
802.11a	27
MCS0 HT20, HT40	27, 27
MCS0 HT20, HT40	24, 24
MCS0 VHT40, VHT80, VHT160	27, 27, 27, 27
MCS11 VHT40, VHT80, VHT160	22, 22, 22, 21
MCS0 HE20, HE40, HE80, HE160	27, 27, 27, 27
MCS11, HE20, HE40, HE80, HE160	22, 22, 22, 21

XV2-23T Wi-Fi 6 Outdoor Access Point

XV2-23T Ordering Information

Regulatory Model	XV2-23T
XV2-23T0B00-US	XV2-23T Outdoor Dual radio Wi-Fi 6 AP, 2x2, 2.5 GbE, IP67, US
XV2-23T0B00-EU	XV2-23T Outdoor Dual radio Wi-Fi 6 AP, 2x2, 2.5 GbE, IP67, EU
XV2-23T0B00-RW	XV2-23T Outdoor Dual radio Wi-Fi 6 AP, 2x2, 2.5 GbE, IP67, RW
XV2-23T0B00-CA	XV2-23T Outdoor Dual radio Wi-Fi 6 AP, 2x2, 2.5 GbE, IP67, CA
C000000L141A	PoE, 60W, 56V, 10GbE DC Injector, Indoor, Energy Level 6 Supply, accepts C5 connector
N000000L034B	PoE injector, 30.5W, 56V, 5GbE DC Injector, Indoor, Energy Level 6 Supply, accepts C5 connector
N000900L017A	PoE, 15.4W, 56V, GbE DC Injector, Indoor, Energy Level 6 Supply, accepts C5 connector
AX-E510RBKT-WW	Shock mount bracket

cnMaestro X Subscriptions

MSX-SUB-XV2-23T-1	cnMaestro X for one XV2-23T AP. Creates one Device Tier 3 slot. Includes Cambium Care Pro support. 1-year subscription
MSX-SUB-XV2-23T-3	cnMaestro X for one XV2-23T AP. Creates one Device Tier 3 slot. Includes Cambium Care Pro support. 3-year subscription
MSX-SUB-XV2-23T-5	cnMaestro X for one XV2-23T AP. Creates one Device Tier 3 slot. Includes Cambium Care Pro support. 5-year subscription

Cambium Care Support

CCADV-SUP-XV2-23T-1	Cambium Care Advanced, 1-year support for one XV2-23T Wi-Fi 6/6E AP. 24x7 TAC support, SW updates, and NBD advance replacement for HW
CCADV-SUP-XV2-23T-3	Cambium Care Advanced, 3-year support for one XV2-23T Wi-Fi 6/6E AP. 24x7 TAC support, SW updates, and NBD advance replacement for HW
CCADV-SUP-XV2-23T-5	Cambium Care Advanced, 5-year support for one XV2-23T Wi-Fi 6/6E AP. 24x7 TAC support, SW updates, and NBD advance replacement for HW
CCPRO-SUP-XV2-23T-1	Cambium Care Pro, 1-year support for one XV2-23T Wi-Fi 6/6E AP. 24x7 TAC support and SW updates
CCPRO-SUP-XV2-23T-3	Cambium Care Pro, 3-year support for one XV2-23T Wi-Fi 6/6E AP. 24x7 TAC support and SW updates
CCPRO-SUP-XV2-23T-5	Cambium Care Pro, 5-year support for one XV2-23T Wi-Fi 6/6E AP. 24x7 TAC support and SW updates
CCADV-UPG-XV2-23T-1	Cambium Care Advanced Add-on to cnMaestro X, 1-year support for one XV2-23T. 24x7 TAC support, SW updates, and NBDS advance replacement for HW
CCADV-UPG-XV2-23T-3	Cambium Care Advanced Add-on to cnMaestro X, 3-year support for one XV2-23T. 24x7 TAC support, SW updates, and NBDS advance replacement for HW
CCADV-UPG-XV2-23T-5	Cambium Care Advanced Add-on to cnMaestro X, 5-year support for one XV2-23T. 24x7 TAC support, SW updates, and NBDS advance replacement for HW

LIMITED WARRANTY

Cambium Networks XV2-23T Wi-Fi 6 Access Point includes a limited lifetime hardware warranty for a period of 3 years.

ABOUT CAMBIUM NETWORKS

Cambium Networks enables service providers, enterprises, industrial organizations, and governments to deliver exceptional digital experiences and device connectivity with compelling economics. Our ONE Network platform simplifies management of Cambium Networks' wired and wireless broadband and network edge technologies. Our customers can focus more resources on managing their business rather than the network. We make connectivity that just works.

cambiumnetworks.com

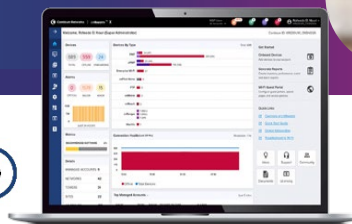
12062024

XE3-4 Wi-Fi 6/6E Indoor Access Point

802.11ax Tri-Radio 2x2/2x2/4x4 (2+2+4) Access Point with Software-Defined Radio

XE3-4 Quick Look:

- Tri-radio/tri-band Wi-Fi 6 and 6E
- 6.6 Gbps aggregate data rate
- Software-defined 5 GHz/6 GHz radio
- 2.5 GbE and 1 GbE uplink ports
- EasyPass with Microsoft Azure and Google G Suite integration



Designed for High-Density and Edge Services

The XE3-4 is a tri-radio Wi-Fi 6/6E, 2x2/2x2/4x4 (2+2+4) access point (AP) designed to deliver future-proof performance and value for building next-generation networks. Wi-Fi 6 delivers faster and more efficient wireless network connections than previous generation Wi-Fi technologies. Wi-Fi 6E extends the capacity of Wi-Fi into the 6 GHz band, more than tripling the wireless spectrum available. With a high-speed software-defined radio, the XE3-4 enables seamless transition to Wi-Fi 6E with the ability to easily change from dual-band to tri-band mode (2.4 GHz, 5 GHz, and 6 GHz) when sufficient 6 GHz clients are available.

The XE3-4 is fully backward compatible with existing Wi-Fi technology, enabling simultaneous support of new high-speed clients, legacy clients, low-bitrate IoT devices, and more in a single wireless infrastructure.

The XE3-4 comes with limited lifetime warranty providing return and repair service on the access point from date of purchase until end of life of the product.

Cloud and On-Premises Management

The XE3-4 is supported by Cambium ONE Network enterprise architecture managed by the cnMaestro™ Network Management System. cnMaestro uses a distributed intelligence architecture with cloud-first management and edge-intelligent Wi-Fi that self-optimizes for the RF environment. cnMaestro delivers a single-pane-of-glass management experience for enterprise Wi-Fi APs, cnMatrix™ Ethernet Switches, NSE Security Appliance/SD-WAN/Firewall, service provider residential routers, and Cambium's fixed wireless broadband and fiber.

cnMaestro Network Management

- Wi-Fi, switching, security, and fixed wireless broadband
- Help desk troubleshooting tools
- Real-time and historical device analytics
- EasyPass user and device onboarding portals
- Application visibility and control
- Graphical reports
- And more

XE3-4 Wi-Fi 6/6E Indoor Access Point

Access Point Specifications

Radios	5 GHz/6 GHz: 802.11a/n/ac/ax, 4x4:4 SW definable 5 GHz: 802.11 a/n/ac/ax, 2x2:2 2.4 GHz: 802.11 b/g/n/ax, 2x2:2 BLE 4.1	Power	32W 802.3bt powered device 25.5W 802.3at with USB, BT disabled Typical 22W (USB disabled)
Wi-Fi	802.11 a/b/g/n/ac/ax	Dimensions	215 mm x 215 mm x 42 mm (without bracket) (8.46 in x 8.46 in x 1.65 in)
SSID Security	WPA3-SAE, WPA3-Enterprise, WPA2-PSK (CCMP, AES, 802.11i), WPA2-Enterprise (802.1X/EAP), OSEN, OWE, Open	Weight	900 g (1.98 lb)
Ports	1 x IEEE 10/100/1000/2500 Mbps Ethernet 1 x IEEE 10/100/1000 Mbps Ethernet 1 x USB 2.0	Security	Kensington lock slot
Antenna Gain	6 GHz: 6.29 dBi, Omni 5 GHz: 6.12 dBi, Omni 2.4 GHz: 4.85 dBi, Omni	Mount Options	Wall or ceiling, T-bar with included locking bracket, ceiling tile plate
Max EIRP*	6 GHz: 30 dBm 5 GHz: 31 dBm 2.4 GHz: 29 dBm	Ambient Operation Temperature	0°C to 50°C (32°F to 122°F)
FCC	Ch 1–11, 36–64, 100–144, 149–165	Storage Temperature	-40°C to 70°C (-40°F to 158°F)
ISED	Ch 1–11, 36–64, 100–116, 149–165	Humidity	95% RH non-condensing
ETSI*	Ch 1–13, 36–64, 100–140, 149–173	MTBF	668,759 hours at 25°C 314,145 hours at 50°C
ROW*	Ch 1–14, 36–64, 100–144, 149–173	LEDs	Multi-color status LEDs, dimmable, on/off
6 GHz Channels		Certifications (Compliance)	Wi-Fi Alliance, Passpoint 3.0 FCC, IC, CE, EN 60601-1-2, EN 60950-1 IEC 62368-1 Safety, EN 60601-1-2 Medical EMC, EN 61000-4-2/3/5 Immunity, EN 50121-1 Railway EMC, EN 50121-4 Railway EMC, IEC 61373 Railway Shock & Vibration, UL 2043 Plenum EN 62311 Human Safety/RF Exposure, WEEE & RoHS
FCC/IC/ROW	Ch 1–233		
EU	Ch 1–93		

*Individual country limits may apply.

Max PHY Data Rate

Radio Type	Band	Number of Radios	Max Data Rate
4x4 SW-Defined	5 or 6 GHz	1	4.804 Gbps
2x2	5 GHz	1	1.201 Gbps
2x2	2.4 GHz	1	574 Mbps
Total		3	6.579 Gbps

Standards

Wi-Fi Protocols	Data Coding support 16/64/256/1024/4096-QAM, VHT MCS rates Channel width support 5GHz and 6GHz band: 20/40/80/160 MHz TWT, Long OFDM Symbol, transmit beamforming, Airtime Fairness, AMSDU, AMPDU, RIFS, STBC, LDPC, MIMO Power Save, MRC, BPSK, QPSK, CCK, DSSS, OFDM, OFDMA, UL/DL MU-MIMO IEEE 802.11 a/ac/ax/b/d/e/g/h/i/j/k/n/r/s/u/v/w
------------------------	---

XE3-4 Wi-Fi 6/6E Indoor Access Point

Network Specifications

Operational Modes	Controllerless standalone Cloud-managed cnMaestro or VM	RF Management	Multi-modal RF optimization supporting Auto-RF for dynamic channel selection & dynamic power adjustment configured via cnMaestro, performed in the intelligent edge AP RF monitor with channel utilization/packet error rate/interference.
WLAN	500 clients per radio 1,500 per AP 16 SSIDs per AP	Band Steering	Yes
Security, Authentication Encryption	Open, WPA-TKIP, WPA2-AES with PSK, ePSK and Enterprise WPA3 with PSK (WPA3-SAE), ePSK, Enterprise, Enterprise-CNSA, OWE (Enhanced Open) OSN and PMF (802.11 W) MAC authentication with local database or external database using RADIUS protocol 802.1X with EAP-TTLS, EAP-TLS / MSCHAPv2, PEAPv0 / PEAPv1 / EAP-PEAP / EAP-SIM/AKA/AKA'/FAST MAC auth fallback to guest portal Hotspot WEB authentication	Mesh	Multi-hop, all 3 bands
Wi-Fi Quality of Service	WMM (packet marking either with 802.1p or IP DSCP), WMM-PS, U-APSD Multicast to unicast conversion	Scheduled WLAN	On/off by day, week, time of day
Service Availability	Critical network resource monitor with SSID shutdown	Data Limit	Client bitrate/time/throughput limit per SSID
Fast Roaming	802.11k/r/v, OKC, cnMaestro-assisted roam	Network	LACP (802.3ad), TCP connection log, NAT logging firewall, DHCP server, DHCP Relay option 82, VLAN pooling, RADIUS attribute, VID VLAN per SSID per user, ePSK with VLAN assignment per PSK LLDP, IGMP v1, v2
Guest Access/ Captive Portal Service (EasyPass)*	cnMaestro-hosted EasyPass portal Multiple authentication methods supported to onboard guest user: <ul style="list-style-type: none"> Radius-based authentication Click-through with simple terms and conditions acceptance Social login using Google®, Facebook® SMS-based authentication (X) Voucher-based access Microsoft® Azure AD and Google Workspace® (X) Sponsored guest access (X) Self-registration access (X) cnMaestro API support for external captive portal integration 802.11u, Hotspot 2.0	Network Tools	Wired and wireless remote packet capture, logging, WAN speed test, ZapD, remote network connectivity tools
Accounting	RADIUS accounting, load balancing AAA servers, Dynamic Authorization COA, DM	Tunnel	L2TPv2, L2GRE, PPPoE
API	RESTful management and statistics API via cnMaestro X, presence location push APIs	IP	IPv4, IPv6
		VLAN	802.11Q, max 4096
		Management interfaces	HTTP/HTTPS web interface, SSH, Telnet
		Security	Rogue AP detection and termination (X), WIDs/WIPs, DoS protection L2–L7 firewall with application visibility (X) & control (X), DNS-based access control (X) ACL and AirCleaner tools
		Services	Wi-Fi Calling control, NTP, Syslog, DNS proxy, SNMP traps, SNMPv1, SNMPv2c, SNMPv3, TCP and DNS logging

*X features available in cnMaestro X.

XE3-4 Wi-Fi 6/6E Indoor Access Point

Management



cnMaestro uses a distributed intelligence architecture with cloud-first management and edge-intelligent APs that self-optimize for the RF environment. cnMaestro delivers a single pane-of-glass management for Cambium broadband fixed wireless, cnMatrix Ethernet Switches, enterprise-grade Wi-Fi APs, NSE Security Appliance/Firewall/SDWAN, and service provider routers.

cnMaestro can be deployed on cloud or on-premises via a virtual machine.

To serve a growing market for advanced management and services functionality, Cambium Networks offers cnMaestro in two management tiers:

cnMaestro X

Paid subscription that includes:

- Advanced device management capabilities
- Deep packet inspection (DPI) application visibility and control for 2,400+ apps
- RESTful management and statistics API
- Presence location push APIs
- Graphic reports
- Webhooks
- Cambium Care Pro for 24x7 technical support
- Accelerated access to L2 engineers and regular software updates

Assists

- Assesses the network's configuration and identifies weak security settings and proposes a fix to ensure the network configuration is up to the top security industry standards

X Assurance

- Helps to quickly identify network-wide connectivity issues by isolating every element of the client's lifecycle, either radio or network related
- Gives an overview quality index of the network and highlights each element's contribution to easily identify the worst offender
- Provides insight of probable causes and proposes fixes for the administrator to apply
- Provides individual client connectivity visibility throughout the entire lifecycle of its connection to easily identify each connection's result and highlight the failure reason, should there be any

EasyPass Portal with Additional Options

- Self-registration: Form-based access
- Sponsored guest: Guest ambassador-based access
- Paid access: Monetize the Wi-Fi access
- Microsoft Azure: Corporate user login
- Google login: Web login using Google accounts

cnMaestro Essentials

License-free cloud management that delivers a disruptive total cost of ownership (TCO) for organizations of all sizes. Includes EasyPass for OneClick or voucher-based connection as well as WiFi4EU access.

**Find out more about
cnMaestro**

XE3-4 Wi-Fi 6/6E Indoor Access Point



Front



Back



Left Side



Right Side



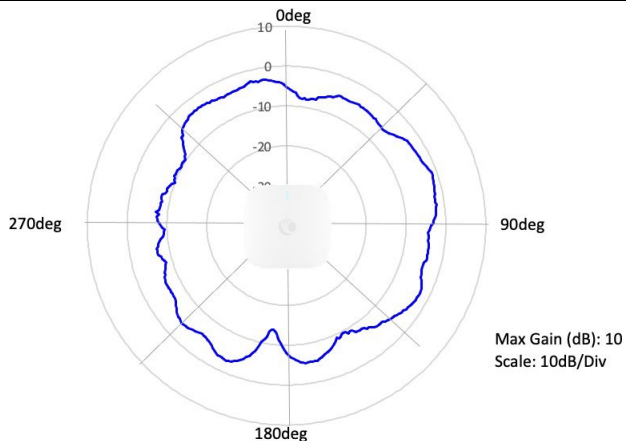
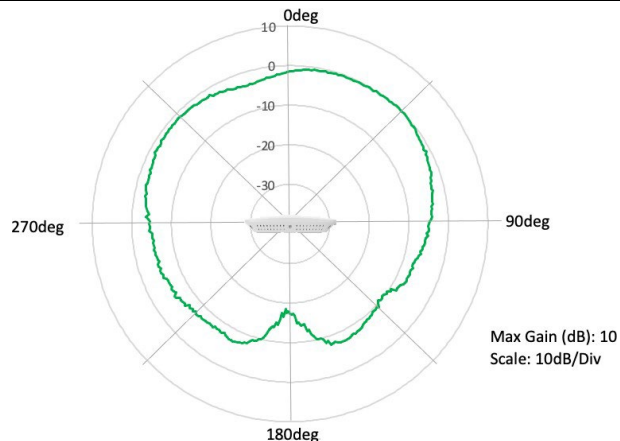
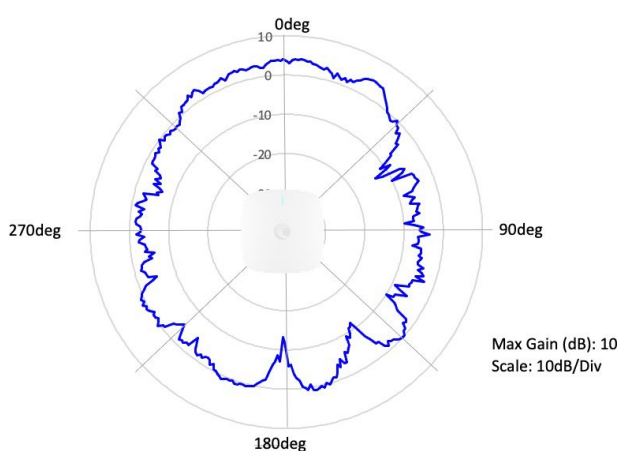
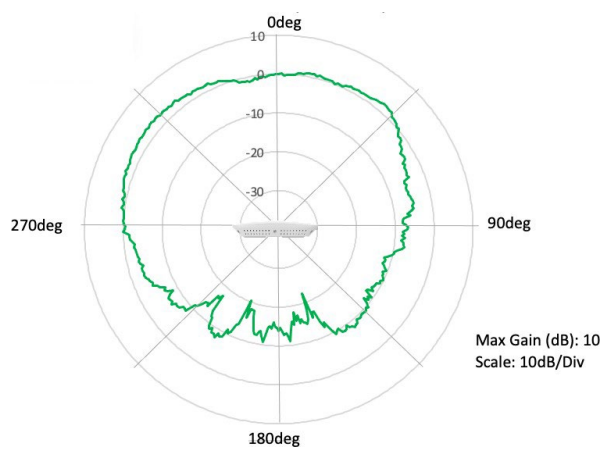
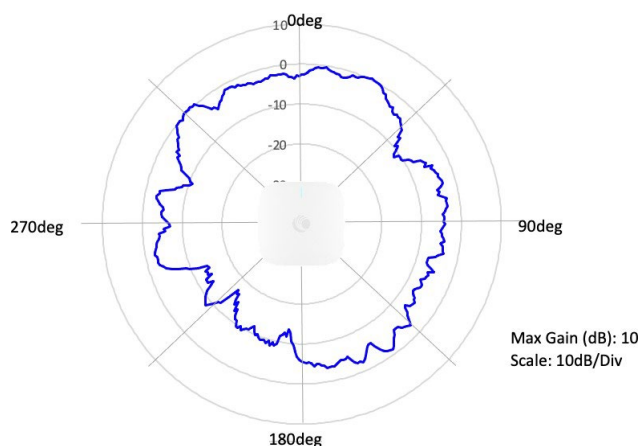
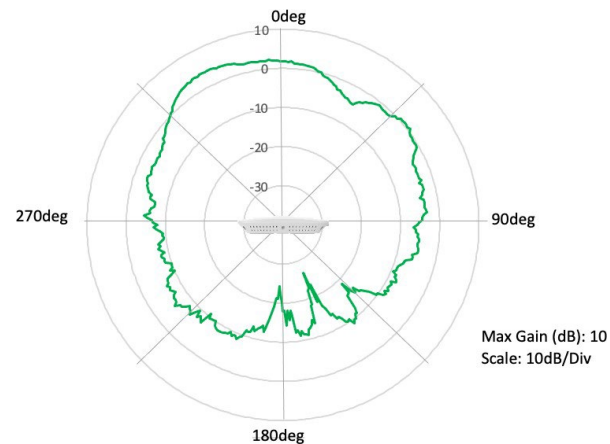
Back



Back

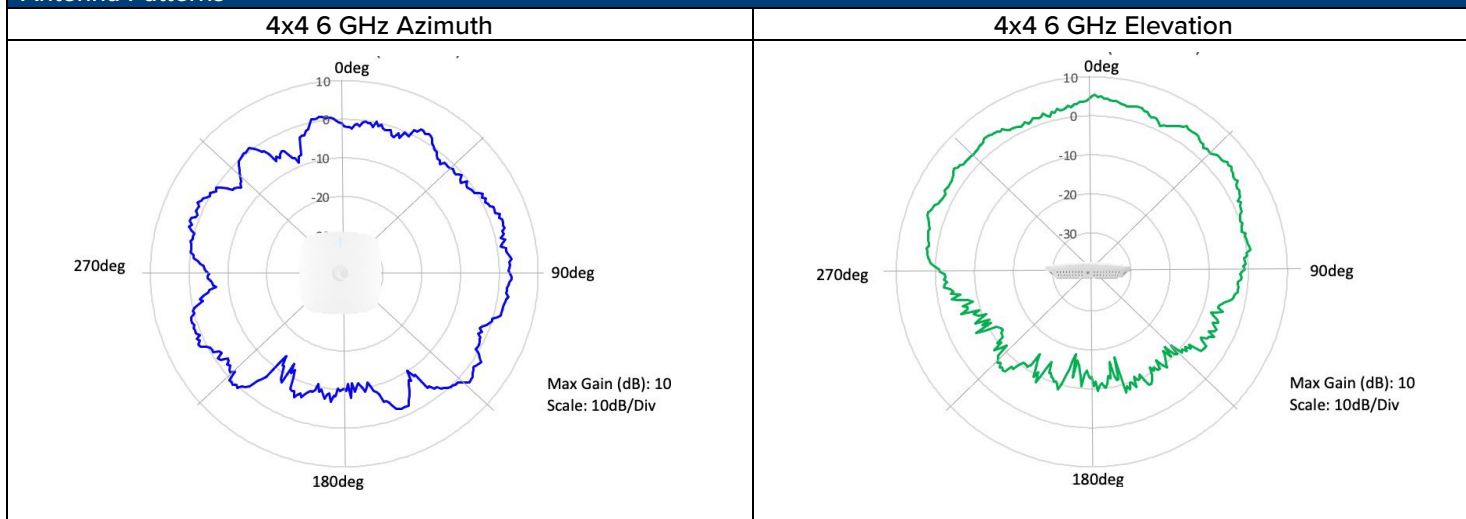
XE3-4 Wi-Fi 6/6E Indoor Access Point

Antenna Patterns

2x2 2.4 GHz Azimuth

2x2 2.4 GHz Elevation

2x2 5 GHz Azimuth

2x2 5 GHz Elevation

4x4 5 GHz Azimuth

4x4 5 GHz Elevation


XE3-4 Wi-Fi 6/6E Indoor Access Point

Antenna Patterns



XE3-4 Ordering Information

Regulatory Model	XE3-4
XE3-4X00B00-US	Indoor Tri-Radio Wi-Fi 6/6E Access Point. SDR 802.11ax 4x4/2x2, US
XE3-4X00B00-EU	Indoor Tri-Radio Wi-Fi 6/6E Access Point. SDR 802.11ax 4x4/2x2, EU
XE3-4X00B00-RW*	Indoor Tri-Radio Wi-Fi 6/6E Access Point. SDR 802.11ax 4x4/2x2, RW
XE3-4X00B00-CA	Indoor Tri-Radio Wi-Fi 6/6E Access Point. SDR 802.11ax 4x4/2x2, CA
C000000L141A	PoE, 60W, 56V, 10GbE DC Injector, Indoor, Energy Level 6 Supply, accepts C5 connector
N000000L034B	PoE injector, 30.5W, 56V, 5GbE DC Injector, Indoor, Energy Level 6 Supply, accepts C5 connector
AX-E510RBKT-WW	Shock mount bracket for cnPilot e510 and e505, Wi-Fi 6 XV3-8, XV2-2. XE3-4
AX-WALLBRKT-WW	Wall Mount L-Bracket for XV and XE series APs. Use to mount the AP horizontally.

cnMaestro X Subscriptions

MSX-SUB-XE3-4-1	cnMaestro X for one XE3-4 AP. Creates one Device Tier3 slot. Includes Cambium Care Pro support. 1-year subscription
MSX-SUB-XE3-4-3	cnMaestro X for one XE3-4 AP. Creates one Device Tier3 slot. Includes Cambium Care Pro support. 3-year subscription
MSX-SUB-XE3-4-5	cnMaestro X for one XE3-4 AP. Creates one Device Tier3 slot. Includes Cambium Care Pro support. 5-year subscription

*AP SKU that ends with 00-RW" does not support 6GHz. The SDR radio is locked to 5GHz mode and cannot be changed to 6GHz. Contact Cambium Networks customer support if you are operating a 00-RW product within a country that has allowed 6GHz operation.

XE3-4 Wi-Fi 6/6E Indoor Access Point

Cambium Care Support

CCADV-SUP-XE3-4-1	Cambium Care Advanced, 1-year support for one XE3-4 Wi-Fi 6/6E AP. 24x7 TAC support, SW updates, and NBD advance replacement for HW
CCADV-SUP-XE3-4-3	Cambium Care Advanced, 3-year support for one XE3-4 Wi-Fi 6/6E AP. 24x7 TAC support, SW updates, and NBD advance replacement for HW
CCADV-SUP-XE3-4-5	Cambium Care Advanced, 5-year support for one XE3-4 Wi-Fi 6/6E AP. 24x7 TAC support, SW updates, and NBD advance replacement for HW
CCPRO-SUP-XE3-4-1	Cambium Care Pro, 1-year support for one XE3-4 Wi-Fi 6/6E AP. 24x7 TAC support and SW updates
CCPRO-SUP-XE3-4-3	Cambium Care Pro, 3-year support for one XE3-4 Wi-Fi 6/6E AP. 24x7 TAC support and SW updates
CCPRO-SUP-XE3-4-5	Cambium Care Pro, 5-year support for one XE3-4 Wi-Fi 6/6E AP. 24x7 TAC support and SW updates
CCADV-UPG-XE3-4-1	Cambium Care Advanced Add-on to cnMaestro X, 1-year support for one XE3-4. 24x7 TAC support, SW updates, and NBDS advance replacement for HW
CCADV-UPG-XE3-4-3	Cambium Care Advanced Add-on to cnMaestro X, 3-year support for one XE3-4. 24x7 TAC support, SW updates, and NBDS advance replacement for HW
CCADV-UPG-XE3-4-5	Cambium Care Advanced Add-on to cnMaestro X, 5-year support for one XE3-4. 24x7 TAC support, SW updates, and NBDS advance replacement for HW

LIMITED WARRANTY

Cambium Networks XE3-4 Wi-Fi 6/6E Access Point includes a limited lifetime hardware warranty that extends 5 years after end of sale.

ABOUT CAMBIUM NETWORKS

Cambium Networks enables service providers, enterprises, industrial organizations, and governments to deliver exceptional digital experiences and device connectivity with compelling economics. Our ONE Network platform simplifies management of Cambium Networks' wired and wireless broadband and network edge technologies. Our customers can focus more resources on managing their business rather than the network. We make connectivity that just works.

cambiumnetworks.com



USER GUIDE

Enterprise Wi-Fi Access Point

Release 6.6.2



Reservation of Rights

Cambium reserves the right to make changes to any products described herein to improve reliability, function, or design, and reserves the right to revise this document and to make changes from time to time in content hereof with no obligation to notify any person of revisions or changes. Cambium recommends reviewing the Cambium Networks website for the latest changes and updates to products. Cambium does not assume any liability arising out of the application or use of any product, software, or circuit described herein; neither does it convey license under its patent rights or the rights of others. It is possible that this publication may contain references to, or information about Cambium products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that Cambium intends to announce such Cambium products, programming, or services in your country.

Copyrights

This document, Cambium products, and 3rd Party software products described in this document may include or describe copyrighted Cambium and other 3rd Party supplied computer programs stored in semiconductor memories or other media. Laws in the United States and other countries preserve for Cambium, its licensors, and other 3rd Party supplied software certain exclusive rights for copyrighted material, including the exclusive right to copy, reproduce in any form, distribute and make derivative works of the copyrighted material. Accordingly, any copyrighted material of Cambium, its licensors, or the 3rd Party software supplied material contained in the Cambium products described in this document may not be copied, reproduced, reverse engineered, distributed, merged or modified in any manner without the express written permission of Cambium. Furthermore, the purchase of Cambium products shall not be deemed to grant either directly or by implication, estoppel, or otherwise, any license under the copyrights, patents or patent applications of Cambium or other 3rd Party supplied software, except for the normal non-exclusive, royalty free license to use that arises by operation of law in the sale of a product.

Restrictions

Software and documentation are copyrighted materials. Making unauthorized copies is prohibited by law. No part of the software or documentation may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without prior written permission of Cambium.

License Agreements

The software described in this document is the property of Cambium and its licensors. It is furnished by express license agreement only and may be used only in accordance with the terms of such an agreement.

High Risk Materials

Cambium and its supplier(s) specifically disclaim any express or implied warranty of fitness for any high-risk activities or uses of its products including, but not limited to, the operation of nuclear facilities, aircraft navigation or aircraft communication systems, air traffic control, life support, or weapons systems ("High Risk Use").

This product is not restricted in the EU. Any High Risk is unauthorized, is made at your own risk and you shall be responsible for any and all losses, damage or claims arising out of any High-Risk Use.

Contents

Contents	3
About This User Guide	11
Overview of Enterprise Wi-Fi AP products	11
Intended audience	11
Purpose	11
Related documents	11
Supported hardware platforms	12
Premium feature list	13
Quick Start – Device Access	14
Powering up the device	14
PoE switches (802.3af/802.3at/802.3bt)	14
PoE adapter	15
DC power supply	16
Accessing the device	16
Device access using default or fallback IP	16
Device access using zeroconf IP	18
Device access using DHCP IP address	19
LED status	19
Onboarding the Device	21
Overview	21
Device onboarding and provisioning	21
cnMaestro	21
XMS-Cloud	22
Configuring the System	23
Basic	23
Power over Ethernet (PoE) in	25

Power over Ethernet (PoE) Out port	28
Link Layer Discovery Protocol (LLDP)	28
Management	30
Administrator Access	30
HTTPS Proxy server configuration	31
Time settings	32
Event logging	33
SNMP	33
Configuring the Radio	35
Overview	35
Configuring Radio parameters	35
Basic	35
Software-Defined Radio (SDR) capabilities	43
Enhanced Roaming	47
BSS Coloring	48
Target Wake Time (TWT)	48
Receive sensitivity configuration	48
Multicast-snooping and Multicast-to-Unicast conversion	48
Auto-RF	49
Overview	50
Dynamic Channel	50
Dynamic Power	51
Auto-RF behavior on device turn on	51
Configuring Dynamic Channel	51
Configuring Dynamic Power	53
Recommended Configuration	54
Configuring the Wireless LAN	56
Overview	56

Configuring the WLAN parameters	56
Basic	57
WLAN VLAN allowed list	70
ICMPv6 Router advertisement (RA) unicast conversion	70
802.11k/v	70
RADIUS server	71
Guest Access	75
Usage Limits	87
Scheduled Access	88
Access	90
Passpoint	93
RADIUS attributes	95
Enterprise PSK (ePSK)	97
Configuring ePSKs	97
ePSK registration for WPA3 clients	100
Creating a Personal Wi-Fi ePSK	108
RADIUS-based ePSK Premium feature	109
Configuring RADIUS-based ePSK	109
Groupwise Transient Key (GTK) per VLAN	111
Configuring the Network	112
Overview	112
Configuring Network parameters	112
IPv4 network parameters	112
Routes	118
IPv6 network parameters	119
General network parameters	122
Ethernet Ports	123
DHCP	126

Tunnel	127
Point-to-Point Protocol over Ethernet (PPPoE)	130
VLAN Pool	131
Wireless Wide Area Network (WWAN)	132
Configuring Access Control	134
Enabling Access Control Policy	134
User Group Policy	135
Device Policy	136
Managing Filters	138
Overview	138
Filter list	138
Filters	138
Configuring filter CLI	139
Device class filter	143
Wi-Fi Calling support	144
Air cleaner	144
Application control Premium feature	146
Deep Packet Inspection (DPI)	147
Custom Applications X	160
WIDS/WIPSPremium feature	163
Wireless Intrusion Detection Systems (WIDS)	163
Wireless flood detection	163
Neighbor AP detection	164
Rogue APs	164
Honeypot APs	164
Ad Hoc network detection	164
Wired Devices	165
Configuring WIDS	165

Wireless Intrusion Prevention System (WIPS)	166
Configuring Services	168
Overview	168
Configuring services	168
Lightweight Directory Access Protocol (LDAP)	168
NAT Logging	169
User Groups Premium feature	171
Real-Time Location System (RTLS)	172
Speed Test	176
DHCP Option-82	177
Bonjour Gateway	178
Link Aggregation Control Protocol (LACP)	180
Operations	182
Overview	182
Firmware upgrade	182
System	183
LED Test flashing pattern	184
Troubleshoot	186
Overview	186
Logging	186
Events	186
Debug Logs	187
Radio Frequency (RF)	188
Wi-Fi Analyzer	188
Packet capture	189
Performance	190
Speedtest on Access Point	190
Network Connectivity	191

XIRCON tool support	192
XIRCON tool support for Linux 1.0.0.40	193
Management Access	194
Local authentication	194
Device configuration	194
SSH Key authentication	194
Device configuration	194
SSH Key generation	195
RADIUS authentication	197
Device configuration	198
Mesh	199
Deployment scenarios	199
Mesh configurable parameters	201
Order of Mesh profile configuration	203
Mesh Auto Detect Backhaul	210
Scenario 1	210
Scenario 2	211
Scenario 3	211
Mesh Muti-Hop	214
Mesh Roaming	215
Mesh Base configuration	215
Mesh Client configuration	216
Mesh link-Sample configuration	217
VLAN 1 as the management interface	217
Non-VLAN 1 as the management interface	221
Typical use-cases	225
Additional mesh topology supported	226
Guest Access Portal - Internal	227

Introduction	227
Configurable parameters	228
Access policy	229
Splash page	229
Redirect parameters	230
Success message	231
Timeout	231
Whitelist	231
Configuration examples	231
Guest Access Portal - External	233
Introduction	233
Configurable parameters	233
Access policy	234
WISPr	234
External portal post through cnMaestro	234
External portal type	234
Redirect parameters	234
Success message	235
Timeout	235
Whitelist	235
Configuration examples	235
Guest Access – cnMaestro	237
Auto VLAN	238
Device Recovery Methods	239
Factory reset via 'RESET' button	239
Boot partition change via power cycle	239
Disable factory Reset Button	240
Command-Line Interface (CLI)	241

Show commands	241
Service commands	244
Service show	244
Service system	245
cnMaestro X Assurance	247
MarketApps	248
Target audience	248
Benefits	248
Glossary	249
Appendix	251
Supported RADIUS Attributes	252
WISPr VSAs (Vendor ID: 14122)	252
Cambium VSAs (Vendor ID: 17713)	253
Standard RADIUS attributes	256
RADIUS attributes in authentication and accounting packets with WPA2-Enterprise security	259
Supported CoA messages	261
Supported DFS channels	263
Supported 6 GHz countries	264
Priority order for parameters	267
Best practices for wireless clients seamless roaming across APs	268
External network recommendations	268
AP WLAN profile configuration recommendations	269
AP group configuration recommendations	271
Cambium Networks	273

About This User Guide

This section describes the following topics:

- [Overview of Enterprise Wi-Fi AP products](#)
- [Intended audience](#)
- [Purpose](#)
- [Related documents](#)
- [Supported hardware platforms](#)
- [Premium Feature List](#)

Overview of Enterprise Wi-Fi AP products

This User Guide describes the features supported by Enterprise Wi-Fi Access Point (AP), and provides detailed instructions for setting up and configuring Enterprise Wi-Fi AP.

Intended audience

This guide is intended for use by the system designer, system installer, and system administrator.

Purpose

Cambium Network's Enterprise Wi-Fi AP documents are intended to instruct and assist personnel in the operation, installation, and maintenance of Cambium's equipment and ancillary devices. It is recommended that all personnel engaged in such activities be properly trained.

Cambium disclaims all liability whatsoever, implied or expressed, for any risk of damage, loss, or reduction in system performance arising directly or indirectly out of the failure of the customer, or anyone acting on the customer's behalf, to abide by the instructions, system parameters, or recommendations made in this document.

Related documents

[Table 1](#) provides details of related documents for Enterprise Wi-Fi AP.

Table 1 *Related documents*

Document Name	Location
Enterprise Wi-Fi AP product details	https://www.cambiumnetworks.com/products/wifi/
Enterprise Wi-Fi AP Hardware and Installation Guide	https://support.cambiumnetworks.com/files
Enterprise Wi-Fi AP User Guide (This document)	https://support.cambiumnetworks.com/files

Document Name	Location
Enterprise Wi-Fi AP Release Notes	https://support.cambiumnetworks.com/files
Enterprise Wi-Fi AP Command-Line Interface Reference Guide	https://support.cambiumnetworks.com/files
Software Resources	https://support.cambiumnetworks.com/files
Community	http://community.cambiumnetworks.com/
Support	https://www.cambiumnetworks.com/support/contact-support/
Warranty	https://www.cambiumnetworks.com/support/warranty/
Feedback	support@cambiumnetworks.com

Supported hardware platforms

[Table 2](#) lists the existing hardware platforms in Enterprise Wi-Fi Access Points:



Warning

Release 6.x is no longer supported on Wi-Fi 5 APs. It was provided for the Wi-Fi 5 APs as a BETA release only. Any issues on these APs running release 6.x will not be supported by the Cambium Support team.

Table 2 Existing hardware platforms

Hardware Platform	Description
XE3-4	4x4:4; 2x2:2; 2x2:2 802.11a/b/g/n/ac wave 2/ax Tri-Radio Indoor Wi-Fi 6e Access Point with BLE IoT radio
XE3-4TN	4x4:4; 2x2:2; 2x2:2 802.11b/g/n/ac wave 2/ax Tri-Radio Outdoor Wi-Fi 6e Access point with BLE IoT radio
XE5-8	8x8:8; 4x4:4; 4x4:4; 4x4:4 802.11a/b/g/n/ac wave 2/ax Tri-Band AP with multi-radio SDR with BLE IoT radio
XV2-2	2x2:2; 2x2:2 802.11a/b/g/n/ac wave 2/ax Dual-Radio Indoor Access Point
XV2-2T0	2x2:2; 2x2:2 802.11a/b/g/n/ac wave 2/ax Dual-Radio Outdoor Access Point, Omni antenna, PoE out with BLE IoT radio
XV2-2T1	2x2:2; 2x2:2 802.11a/b/g/n/ac wave 2/ax Dual-Radio Outdoor Access Point, Sector antenna, PoE out with BLE IoT radio
XV2-21X	2x2:2; 2x2:2 802.11a/b/g/n/ac wave 2/ax Dual-Radio Indoor Wi-Fi 6 Access Point

Hardware Platform	Description
XV2-22H	2x2:2, 2x2:2 802.11a/b/g/n/ac wave 2/ax Dual-Radio Indoor Wi-Fi 6 Wall-Plate Access Point with BLE/Zigbee IoT radio
XV2-23T	2x2:2, 2x2:2 802.11a/b/g/n/ac wave 2/ax Dual-Radio Outdoor Wi-Fi 6 Access Point
XV3-8	8x8:8, 4x4:4 802.11a/b/g/n/ac wave 2/ax Tri-Radio Indoor Access Point with BLE IoT radio

Premium feature list

Release 6.0 and later releases of Enterprise Wi-Fi AP firmware support certain advanced features that are available only through a paid subscription to cnMaestro X or XMS-Cloud management. These features are identified with the label **Premium feature** in the documentation. With Release 6.5 and later releases, end users can access these features without a management subscription on a free trial basis and for a limited time. As Cambium Networks releases new versions, restrictions will be enforced on the use of these premium features only in conjunction with a current cnMaestro X or XMS-Cloud subscription. If the user does not have a current subscription at that time, the APs will stop enabling configurations, including these premium features.

Table 3 Premium feature list

Feature Name	Release Details
Wireless Intrusion Detection Systems (WIDS)	Release 6.4.2
RADIUS-based ePSK	Release 6.4
Stanley AeroScout Location Engine	Release 6.3
User Groups	Release 6.2
Advanced Filters (QoS, DSCP, Schedule, and Rate limit)	Release 6.0
Application Control	Release 6.0

Quick Start – Device Access

This chapter describes the following topics:

- [Powering up the device](#)
- [Accessing the device](#)
- [LED status](#)

Powering up the device

This section includes the following topics:

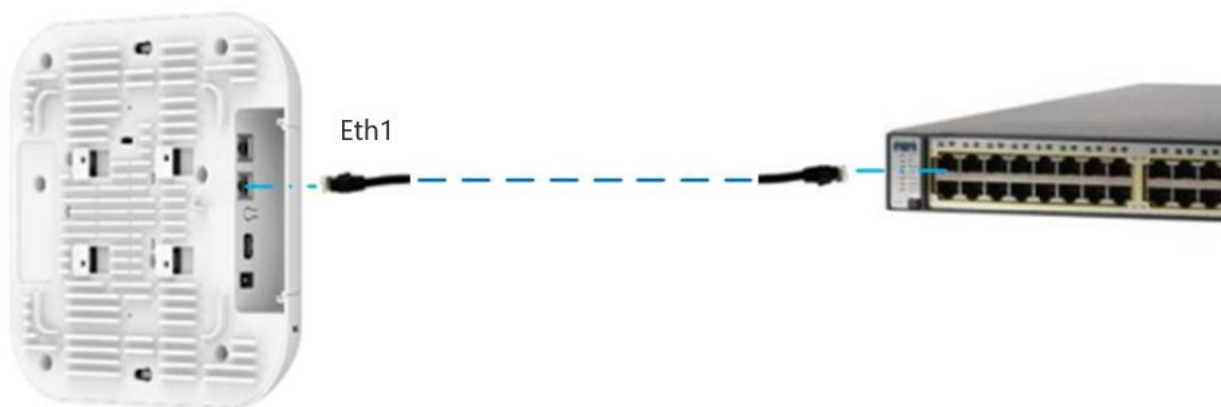
- [PoE switches \(802.3af/802.3at/802.3bt\)](#)
- [PoE adapter](#)
- [DC power supply](#)

Enterprise Wi-Fi AP product family can be powered using an Ethernet PoE Switch or a PoE midspan injector. Note that some APs can be powered by 802.3af, while others may require 802.3at or 802.3bt. Additionally, some APs can be powered with an external power supply. Refer to the related product datasheet to determine the options available.

PoE switches (802.3af/802.3at/802.3bt)

Enterprise Wi-Fi APs negotiate the power via the LLDP mechanism. [Figure 1](#) represents the Enterprise Wi-Fi AP Eth1 port connecting to a switch (PoE PSE Port).

Figure 1 Installation of Enterprise Wi-Fi AP to PSE port



[Table 4](#) provides detailed information on the AP modules that are enabled based on power negotiated via LLDP.

Table 4 Power management policy

Platform	IEEE 802.3af (12.95W @ PD)	IEEE 802.3at (25.5W @ PD)	IEEE 802.3bt Class - 0/1/2/3/4 (40W @ PD)	IEEE 802.3b Class - 5/6 (51W @ PD)	IEEE 802.3b Class - 7/8 (64W @ PD)
XV3-8	✓	✓	✓		
XV2-2	✓	✓			
XV2-2T0	✓	✓	✓	✓	
XV2-2T1	✓	✓	✓	✓	
XE5-8		✓	✓	✓	✓
XE3-4	✓	✓	✓		
XV2-21X	✓	✓			
XV2-23T	✓	✓			
XV2-22H	✓	✓			
XE3-4TN	✓	✓	✓	✓	✓

PoE adapter

To power up the device using a PoE adapter, perform the following steps:

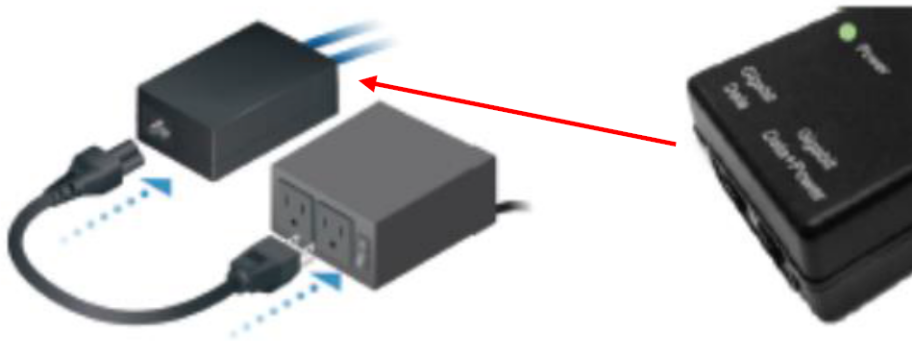
1. Connect the Ethernet cable from the Eth1/PoE-IN port of the device to the 5 Gigabit Data + Power port of the PoE adapter.
2. Connect an Ethernet cable from your LAN or computer to the 5 Gigabit Data port of the PoE adapter.

Figure 2 Installation of Enterprise Wi-Fi AP to a PoE adapter



3. Connect the power cord to the adapter, and then plug the power cord into a power outlet as shown in [Figure 3](#). Once powered ON, the Power LED should illuminate continuously on the PoE adapter.

Figure 3 Connecting PoE adapter to a power outlet



DC power supply

The Enterprise Wi-Fi AP XV3-8 has an option to power via a DC power adapter through the barrel connector. If the device is connected to both the DC power adapter and the PoE adapter, then the DC power adapter takes precedence.

Accessing the device

This section includes the following topics:

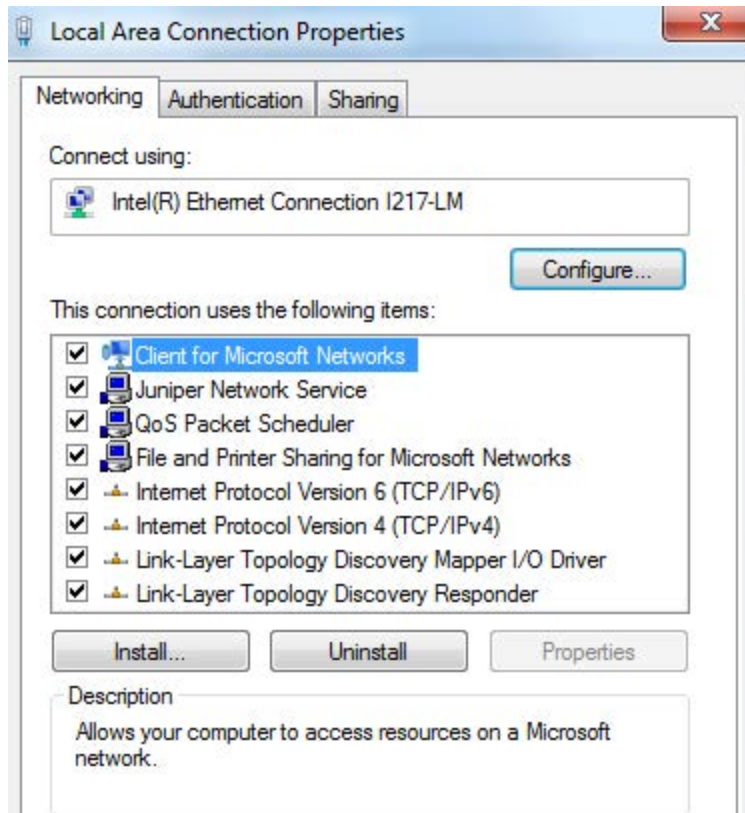
- [Device access using default or fallback IP](#)
- [Device access using zeroconf IP](#)
- [Device access using DHCP IP address](#)

Once the device is powered up, ensure it is operational by checking the LED status. The power LED on the AP should turn green, which indicates that the device is ready for access.

Device access using default or fallback IP

To configure the computer to access the device using the default or fallback IP, perform the following steps:

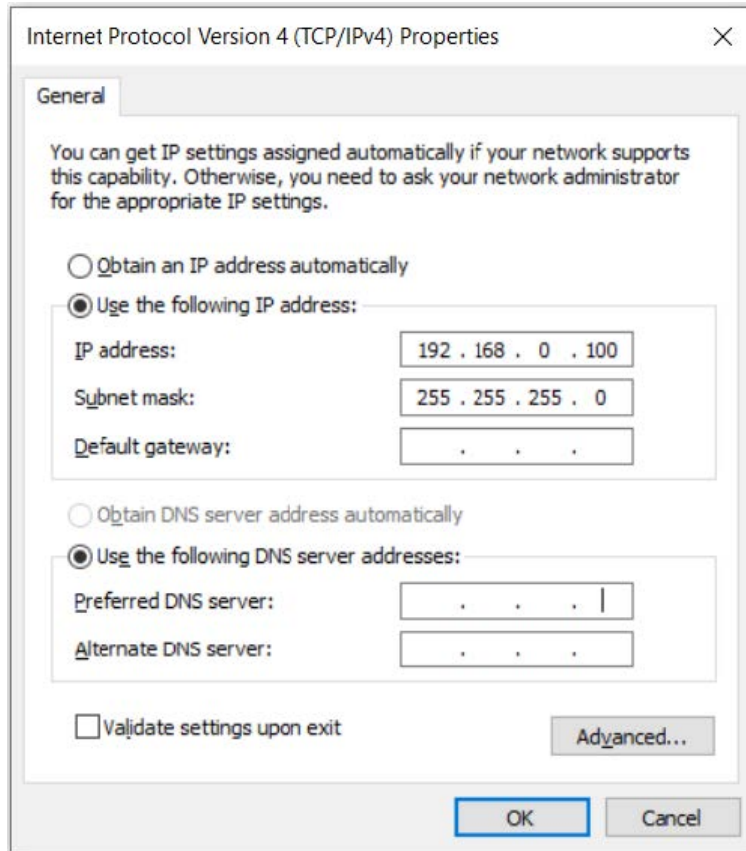
1. Open **Local Area Connection Properties** by performing one of the following steps:
 - In computers running Windows 7 operating system, go to **Control Panel > Network and Internet > Network Connections > Local Area Connection > Properties** (in the **Local Area Connection Status** window).
 - In computers running Windows 10 operating system, go to **Control Panel > Network and Internet > Network and Sharing Center > Local Area Connection > Properties** (in the **Local Area Connection Status** window).



The AP obtains its IP address from a DHCP server. A default IP address of 192.168.0.1/24 is used if an IP address is not obtained from the DHCP server.

2. Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

The **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box appears, as shown below:

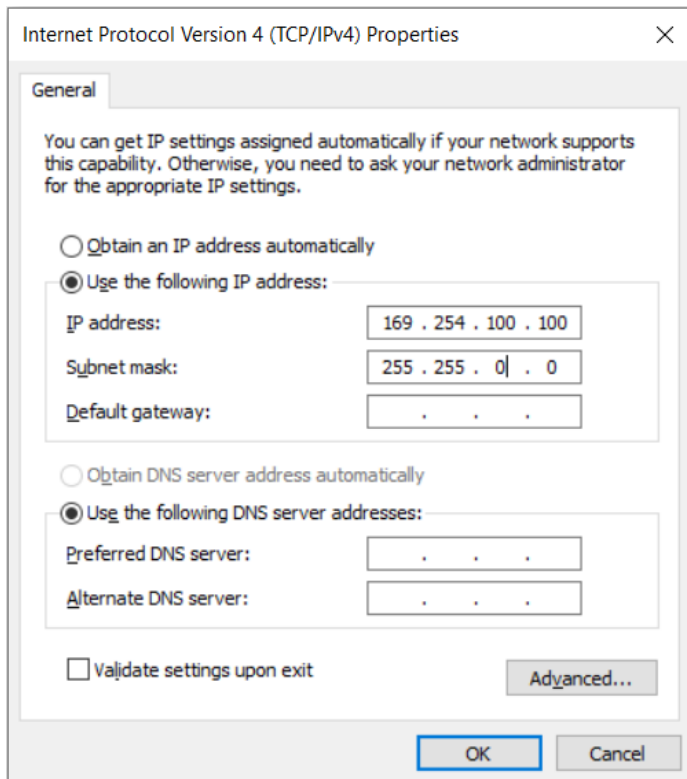


3. In the **Use the following IP address** section, ensure that an appropriate IP address and a subnet address are provided.
4. Click OK.
5. Ensure that your computer is set up to communicate with the required range of IP addresses.
6. Open a web browser and type the URL - <http://192.168.0.1> - to access the device UI. The Sign In page appears.
7. Type an appropriate username and password.
 - Default username: admin
 - Default password: admin
8. Click **Sign In**.

Device access using zeroconf IP

To configure the computer to access the device using the zeroconf IP, complete the following steps:

1. Convert the last two bytes of ESN of the device to decimal. If ESN is 58:C1:CC:DD:AA:BB, last two bytes of this ESN is AA:BB. Decimal equivalent of AA:BB is 170:187. Zeroconf IP of the device with ESN 58:C1:CC:DD:AA:BB is 169.254.170.187.
2. Configure Management PC with 169.254.100.100/16, as described below:



3. Access the device UI using <http://169.254.170.187> with default credentials as below:

- Username: admin
- Password: admin

Device access using DHCP IP address





To access the device using DHCP IP address, follow the below steps:

1. Plug in the device to the network.
2. Obtain the IP address of the device from the system administrator.
3. Access the device UI using <http://<IP address>> and default credentials, as listed below:
 - Username: admin
 - Password: admin

LED status

The Enterprise Wi-Fi AP features a single-color LED. The power LED glows amber when AP is turning on and turns green once the AP has successfully turned on. The network or status LED glows green if the connection to XMS or cnMaestro controller or manager is down. It turns blue once the AP is connected successfully to XMS or cnMaestro.

Table 5 Enterprise Wi-Fi AP LED status

LED Color	Status Indication
	<p>The device is turning on.</p> <div>  <div> <p>Note:</p> <p>If the LEDs remain amber for more than five minutes, it indicates that the device has failed to turn on.</p> </div> </div>
	<ul style="list-style-type: none"> • The device is successfully up and accessible. • Wi-Fi services are up, if configured.
	<ul style="list-style-type: none"> • XMS or cnMaestro connection is successful.

Onboarding the Device

This chapter describes the following topics:

- [Overview](#)
- [Device Onboarding and Provisioning](#)

Overview

By default, support is available for all the devices at <https://cloud.cambiumnetworks.com>, no user action is required to direct devices to contact either cnMaestro Cloud or XMS-Cloud. You can onboard and provision devices without any additional setup.

If you are using cnMaestro On-Premises, you must direct the devices to connect to the cnMaestro server using DHCP options or static URL configuration. For more information, refer to the *cnMaestro On-Premises User Guide*.

Device onboarding and provisioning

Enterprise Wi-Fi APs support the following onboarding methods:

- [cnMaestro](#)
- [XMS-Cloud](#)

cnMaestro

cnMaestro is a simple next-generation network management system for Cambium Networks wireless and wired solutions.

For onboarding devices to cnMaestro, refer to the *cnMaestro User Guide*.

Supported devices and minimum version

The following table lists the minimum release version of every Enterprise Wi-Fi APs that is required to be managed by cnMaestro Cloud and On-Premises. It also lists the minimum version of cnMaestro Cloud and On-Premises required to manage the respective APs.



Note

- The AP version is the minimum version required to manage the APs using cnMaestro Cloud and On-Premises.
- Similarly, the cnMaestro version is the minimum Cloud or On-Premises versions required to manage the APs.

Table 6 Supported minimum AP and cnMaestro versions

AP Model	Supported Minimum AP Version		Supported Minimum cnMaestro Version	
	cnMaestro Cloud	cnMaestro On-Premises	cnMaestro Cloud	cnMaestro On-Premises
XE3-4	6.6.0.3	6.6.0.3	3.1.0	3.1.0
XE3-4TN	6.6.0.3	6.6.0.3	3.2.0	3.2.0
XE5-8	6.6.0.3	6.6.0.3	3.1.1	3.1.1
XV2-2	6.6.0.3	6.6.0.3	2.4.1	2.4.1
XV2-2T0	6.6.0.3	6.6.0.3	3.1.0	3.1.0
XV2-2T1	6.6.0.3	6.6.0.3	3.1.1	3.1.1
XV2-21X	6.6.0.3	6.6.0.3	3.1.1	3.1.1
XV2-22H	6.6.0.3	6.6.0.3	3.1.1	3.1.1
XV2-23T	6.6.0.3	6.6.0.3	3.1.1	3.1.1
XV3-8	6.6.0.3	6.6.0.3	2.4.1	2.4.1

XMS-Cloud

XMS-Cloud makes it easy to manage networks from a single, powerful dashboard. Zero-touch provisioning and centralized, multi-tenant network orchestration simplifies network management functions. XMS-Cloud helps manage Cambium Enterprise Wi-Fi devices.

For onboarding devices to XMS-Cloud, refer to <https://www.youtube.com/watch?v=qD-nPsdRc4Y>.

Configuring the System

This chapter describes the following topics:

- [Basic](#)
- [Management](#)
- [Time settings](#)
- [Event Logging](#)
- [SNMP](#)

Basic

To configure the basic parameters for the AP, complete the following steps:

1. Navigate to **Configuration > Wi-Fi Profiles > AP Groups** page.
2. Click **Add New** and select **Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)** from the **Type** drop-down list.

By default, the **Basic** tab is displayed.



Note

- The following special characters are supported when creating the AP Group and WLAN passwords:
a-zA-Z_~*%#@!<>().[]^`\$1234567890.
- By default, the password is not configured. You must configure the password for AP Groups.
You can also rename the password after creating it.

[Table 7](#) lists the configurable parameters that are available in the **Basic** tab in the cnMaestro UI.

Table 7 Basic parameters

Parameter	Description	Range	Default
Name	Hostname of the device. Supported maximum length of the hostname: 64 characters	-	Enterprise Wi-Fi AP Model Number-Last 3 Bytes of ESN
Location	Location where the device is placed. Supported maximum length of location: 64 characters	-	-
Contact	Contact information for the device.	-	-

Parameter	Description	Range	Default
Country	<p>Country of operation of the device.</p> <p>To be set by the administrator only.</p> <p>The allowed operating channels and the respective transmit power levels depend on the country of operation. The list of countries supported depends on the SKU of the device (FCC and ROW).</p> <p>Note: Radios remain disabled unless this parameter is configured.</p>	-	-
Placement	<p>Enterprise Wi-Fi AP device supports both Indoor and Outdoor deployments. Based on deployment user can configure it as follows:</p> <ul style="list-style-type: none"> • Indoor: Only indoor channels for configured country code will be available and operational. • Outdoor: Only outdoor channels for configured country code will be available and operational. 	-	Indoor
PoE Output	Enable power over Ethernet to an auxiliary device connected to PoE OUT port.	-	Off
Dual 5 GHz radio	<p>Enable Dual 5 GHz radio.</p> <p>This parameter provides the flexibility of splitting 8x8 5 GHz radio into two 4x4 5 GHz radios.</p>	-	Disabled
LED	When enabled, turns on the device LEDs during operation.	-	Enabled
LLDP	Advertises device capabilities and information in the L2 network.	-	Enabled
Recommended Channel Distribution	<p>Allows unique distribution of channels across radios when multiple radios are configured with same frequency band.</p> <p>Note: This option is available only as a CLI-based configuration. Use the <code>channels-distribution</code> command.</p>	-	Enabled
Default Power Policy	Provision to configure current power policy.	-	Sufficient
Power Force Type	Provision to configure power force type.	-	None

Figure 4 The System page

AP Groups > Add New

Basic

Management

Radio

Network

Security

Access Control

Services

User-Defined Overrides

Basic Information

Type
Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)

Name*

Scope
Shared Shared Scope means the AP Group is accessible to all Managed Accounts

☒ Auto Sync Automatically push configuration changes to devices sharing this AP Group

Country* For appropriate regulatory configuration

Location Location where this device is placed (max 64 characters)

Contact Contact information for the device (max 64 characters)

Description

Placement
☒ Indoor ☐ Outdoor Configure the AP placement details

PoE Output
Off Enable Power over Ethernet to an auxiliary device connected to PoE OUT port

☒ LED Whether the device LEDs should be ON during operation

☒ LLDP Whether the AP should transmit LLDP packets

☒ Recommended Channel Distribution
Disabling the recommended channel distribution allows any approved channel on any radio in APs with multiple 5/6GHz radios such as the XE3-4, XE3-4TN, and XE5-8. By default allowed channels are restricted to optimize the performance of multiple radios on the same band. Use this with advice from an RF planning expert. (applies to XE3-4, XE3-4TN and XE5-8 APs which have more than two 5/6 GHz radios)

WLAN

Add WLAN Create WLAN

Order	WLAN
No WLAN Selected	

Save

Close

Power over Ethernet (PoE) in

Enterprise Wi-Fi APs first attempt to detect the type and classification of the Power Source (PS) using standard hardware handshake and control logic. Some PS devices, like the Cambium PoE power injectors, are passive and cannot be detected by the AP. Therefore, the APs also use LLDP power negotiation to

request a specific amount of PoE power from the PS. This feature in the Enterprise Wi-Fi APs is called LLDP power request and it is enabled by default.

The following table lists the PoE power requirements for the Enterprise Wi-Fi APs:



Caution

Although APs may operate in accordance with the power requirements mentioned in the **Hardware Power Requirement** column, caution is advised as the results may be unexpected.

Table 8 PoE power requirements for APs

Device	PoE Out	Hardware Power Requirement	Maximum Power Draw (Watts)	Minimum Power Required to boot (Watts)
XE3-4TN	Yes (Max 30W)	802.3at	64	15
XV2-2	No	802.3at	21	7.6
XV2-2T0	Yes (Max 30W)	802.3at	51	13.3
XV2-2T1	Yes (Max 30W)	802.3at	51	13.3
XV2-21X	No	802.3af	12.95	8
XV2-22H	Yes (Max 10W)	802.3af	22.95	8
XV2-23T	No	802.3af	12.95	8
XV3-8	No	802.3bt	35	22.9
XE3-4	No	802.3bt	32	15.6
XE5-8	No	802.3bt	60	32.9



Note

Accurate time on the AP is critical for features such as WLAN Scheduled Access and Syslogs.

Figure 5 Power policy configuration

The screenshot shows the configuration page for the 'Ent_Mesh_ZeroTouch_APGrp' under the 'Wi-Fi AP Groups' section. The left sidebar lists various configuration categories: System, Default Enterprise, Default Home, Ent_Mesh_ZeroTouch_APGrp (selected), Basic, Management, Radio, Network, Security, Services, and User-Defined Overrides. The main content area is titled 'User-Defined Overrides' and contains a text area for configuration settings. The text area contains the following content:

```

!
power policy limited
power force Unknown
!

```

Below the text area, there is a warning message: 'Settings entered are not validated or error-checked (However, dollar (\$), period (.) or space characters are not allowed in a variable name and it should not be more than 64 characters long), and they may overwrite configuration made in previous screens, so please use them with caution. You are responsible for ensuring the resulting AP Group is valid and safe to use.'

[Table 9](#) lists the Cambium PoE injectors and cnMatrix models supported on the APs.

Table 9 Supported Cambium PoE Injectors and cnMatrix models

AP Model	Cambium PoE Injector	cnMatrix Recommended Model
XE3-4TN	N000000L142A	EX3028R-P / EX3052R-P / EX2016M-P
XV2-2	N000000L142A	EX3028R-P / EX3052R-P / EX2016M-P
XV2-2T0	N000000L142A	EX3028R-P / EX3052R-P / EX2016M-P
XV2-2T1	N000000L142A	EX3028R-P / EX3052R-P / EX2016M-P
XV2-21X	N000000L142A / N000000L034B / N000900L017A	EX3028R-P / EX3052R-P / EX2016M-P / EX2052-P / EX2052R-P / EX2028-P / EX2010-P / EX1028-P / EX1010-P
XV2-22H	N000000L142A / N000000L034B	EX3028R-P / EX3052R-P / EX2016M-P / EX2052-P / EX2052R-P / EX2028-P / EX2010-P / EX1028-P / EX1010-P
XV2-23T	N000000L142A / N000000L034B / N000900L017A	EX3028R-P / EX3052R-P / EX2016M-P / EX2052-P / EX2052R-P / EX2028-P / EX2010-P / EX1028-P / EX1010-P
XV3-8	N000000L142A	EX3028R-P / EX3052R-P / EX2016M-P
XE3-4	N000000L142A	EX3028R-P / EX3052R-P / EX2016M-P
XE5-8	N000000L142A	EX3028R-P / EX3052R-P / EX2016M-P



Attention

Configure Power policy and power force type based on the input power source.

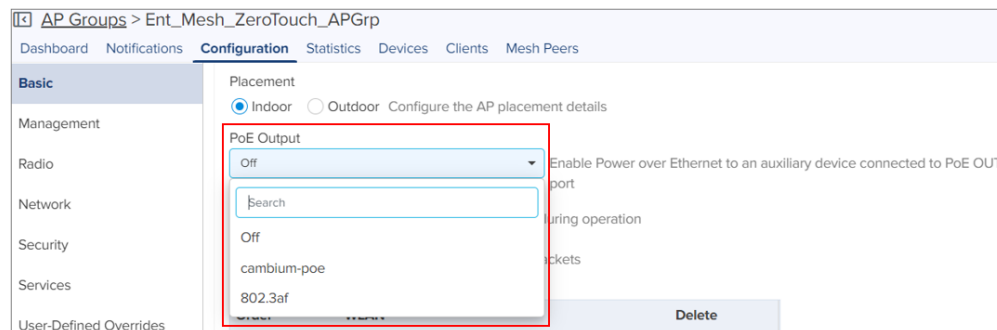
Power over Ethernet (PoE) Out port

PoE out provision is provided to power on devices that are compatible with IEEE 802.3 af/at PoE IN as per power consumption or Cambium 30V POE as shown in the below table.

Table 10 PoE-out capabilities

AP Model	10W	48V @ 15W	48V @ 30W	30V @ 30W	Default State
----------	-----	-----------	-----------	-----------	---------------

Figure 6 PoE Output cnMaestro configuration



Link Layer Discovery Protocol (LLDP)

LLDP is a Layer 2 network protocol used to share information, such as the device manufacturer, model, network capabilities, and IP address with other directly connected network devices. APs can both advertise their presence by sending LLDP announcements and can also collect and display information sent by neighbors.

LLDP settings are enabled by default on the AP. This implies that the power negotiation is also enabled over LLDP when an AP is powered by a Power over Ethernet (PoE) PSE switch port.

This window allows you to establish your LLDP settings.

Power negotiation

LLDP discovers a device port (connected to a PoE PSE switch, for example) that supplies power to the AP. The AP checks that the port can supply the maximum power that is required by the AP model. The AP sends the required maximum power (in watts) via LLDP frames to the PoE source and expects the PoE source to reply with the amount of power that can be allocated.

- If the AP receives a response confirming that the power allocated by the PoE PSE source is equal to or greater than the maximum power requested, the AP enables radios and other Model Specific peripherals (for example, USB port, Bluetooth).
- If the AP receives a power allocation that is less than the maximum but more than the minimum required to keep the radios operational, the AP issues a Syslog message and shuts down the other peripherals (for example, USB port, Bluetooth).

- If the AP receives less than the minimum power required for the radios to operate, the radios are shut down for five minutes. During this time, LLDP power negotiation continues to monitor the available power to ensure it meets the minimum requirement for the AP radios to function.
- Click to check power status: `show power`

This provides a more graceful way of handling an underpowered situation on a Wi-Fi device. When the radios are turned off, XMS can notify you so that you don't have to hunt down an intermittent problem.

CLI Configuration

Consider the following tasks to configure the CLI:

To enable:

```
ap(config)# lldp
ap(config)#
```

To disable:

```
ap(config)# no lldp
ap(config)#
```

To list LLDP configuration:

```
show lldp configuration
show lldp interfaces
```

Request power

To enable/disable power negotiation via LLDP:

```
ap(config)# lldp
request-power : Enable power negotiation (default:enabled)
tx-hold : Set transmit hold multiplier (default:4, used to calculate the time-
to-live (tx-interval * tx-hold))
tx-interval : Set LLDP packet transmit delay (in Sec, default:30 sec)
ap(config)# lldp request-power
<ENTER>
ap(config)# lldp request-power
```

Transmit hold

It is used to compute the Time To Live (TTL) value. This is the time during which the receiving device maintains information before the validity of information expires.

```
ap(config)# lldp
request-power : Enable power negotiation (default:enabled)
tx-hold : Set transmit hold multiplier (default:4, used to calculate the time-
to-live (tx-interval * tx-hold))
tx-interval : Set LLDP packet transmit delay (in Sec, default:30 sec)
ap(config)# lldp tx-hold
```

Specify transmit hold multiplier value (max 65535)

Transmit interval

It is the time interval between two regular LLDP packets transmissions. The AP sends out LLDP announcements, advertising its presence at this interval. The default value is 120 seconds.

```
ap(config)# lldp
request-power : Enable power negotiation (default:enabled)
tx-hold : Set transmit hold multiplier (default:4, used to calculate the time-
to-live (tx-interval * tx-hold))
tx-interval : Set LLDP packet transmit delay (in Sec, default:30 sec)
ap(config)# lldp tx-interval
Specify LLDP transmit delay in sec (max 65535)
```

Management

Administrator Access

To configure Administrator access parameters, complete the following steps:

1. Navigate to **Configuration > Wi-Fi Profiles > AP Groups** page.
2. Click **Add New** and select **Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)** from the **Type** drop-down list.
3. Click **Management** tab > **Administrator Access** section.

[Table 11](#) lists configurable fields that are displayed in the **Administrator Access** section.

Table 11 Administrator Access parameters

Parameter	Description	Range	Default
Admin Password	Password for authentication of UI and CLI sessions.	-	admin
Telnet	Enables Telnet access to the device CLI.	-	Disabled
SSH	Enables SSH access to the device CLI.	-	Enabled
SSH Key	Provision to login to device using SSH Keys. The user needs to add Public Key in this section. If configured, the user has to login to AP using Private Keys. This is applicable for both CLI and GUI.	-	Disabled
HTTP	Enables HTTP access to the device UI.	-	Enabled
HTTP Port	Provision to configure HTTP port number to access device UI.	1-65535	80
HTTPS	Enables HTTPS access to the device UI.	-	Enabled
HTTPS Port	Provision to configure HTTPS port number to access device UI.	1-65535	443

Parameter	Description	Range	Default
RADIUS Mgmt Auth	User has provision to control login to AP using RADIUS authentication. If enabled, every credential that is provided by the user undergo RADIUS authentication. If successful, allowed to login to UI of the device. This is applicable for both CLI and GUI.	-	Disabled
RADIUS Server	Provision to configure RADIUS IPv4 server for Management Authentication.	-	-
RADIUS Secret	Provision to configure RADIUS shared secret for Management authentication.	-	-

Figure 7 Administrator Access page

Administrator Access

Admin Password

.....
Show

Configure password for authentication of GUI and CLI sessions (max 32 characters)

⚠ Change your password, do not use default passwords!

☐ Telnet Enable Telnet access to the device CLI

☒ SSH Enable SSH access to the device CLI

SSH Key

Show

Use SSH keys instead of password for authentication

☒ HTTP Enable HTTP access to the device GUI

HTTP Port

80

Port for HTTP access to the device GUI (1-65535)

☒ HTTPS Enable HTTPS access to the device GUI

HTTPS Port

443

Port for HTTPS access to the device GUI (1-65535)

☐ RADIUS Mgmt Authentication Enable RADIUS authentication of GUI/CLI sessions

RADIUS Server

RADIUS server IP/Hostname

RADIUS Secret

Show

RADIUS server shared secret

HTTPS Proxy server configuration

The proxy management service is established in the AP to proxy management of traffic for remote management services originating from the AP.

For zero-touch configuration, refer to [DHCP Option 43 - Zero-touch onboarding](#).

CLI Configuration:

```

ap(config)# management proxy
https : Enable HTTPS proxy support
ap(config)# management proxy https
host : Configure HTTPS proxy host

```

```
password : Configure HTTPS proxy password
port : Configure HTTPS proxy port
username : Configure HTTPS proxy username
```

Time settings

Users can configure up to two NTP servers. These servers are used by the AP to set its internal clock to the respective time zones configured on the device. Upon turning on, the AP's clock resets to the default and resynchronizes the time, as the Enterprise Wi-Fi AP does not have battery backup. The servers can be specified as an IPv4 address or a hostname (for example, `pool.ntp.org`).

To configure time parameters, complete the following steps:

1. Navigate to **Configuration > Wi-Fi Profiles > AP Groups** page.
2. Click **Add New** and select **Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)** from the **Type** drop-down list.
3. Click **Management** tab > **Time Settings** section.

[Table 11](#) lists configurable fields that are displayed in the **Time Settings** section.

Table 12 Time Setting parameters


Parameter	Description	Range	Default
Time zone	<div>The time zone can be set according to the location where the AP is installed. Selecting the appropriate time zone from the drop-down list ensures that the device clock is synced with the wall clock time.</div> <div> Note Accurate time on the AP is critical for features such as WLAN Scheduled Access and Syslogs.</div>	-	-
NTP Server 1	Name or IPv4 address of a Network Time Protocol server 1.	-	-
NTP Server 2	Name or IPv4 address of a Network Time Protocol server 2.	-	-

Figure 8 Time setting page

Time Settings
Time Zone
 Configure Time Zone
NTP Server 1
 Name or IP Address of Network Time Protocol Server
NTP Server 2

Event logging

The Enterprise Wi-Fi AP devices support multiple troubleshooting methods. Event logging or Syslog is one of the standard troubleshooting processes. If you have a Syslog server in your network, you can enable it on an Enterprise Wi-Fi AP device. A maximum of two Syslog servers can be configured on an Enterprise Wi-Fi AP device. Events are sent to both configured Syslog servers if they are up and running.

To configure event logging, complete the following steps:

1. Navigate to **Configuration > Wi-Fi Profiles > AP Groups** page.
2. Click **Add New** and select **Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)** from the **Type** drop-down list.
3. Click **Management** tab > **Event Logging** section.

[Table 13](#) lists configurable fields that are displayed in the **Event Logging** section.

Table 13 Event logging parameters

Parameter	Description	Range	Default
Syslog Server 1	Hostname or IPv4 address of the Syslog server and respective port number.	-	514
Syslog Server 2	Hostname or IPv4 address of the Syslog server and respective port number.	-	514
Syslog Severity	Provision to configure severity of Logs that must be forwarded to the server. The Log levels supported are as per RFC.	-	Debug

Figure 9 Event logging page

Event Logging

Syslog Server1: Port: Name or IPv4/IPv6 address of syslog server

Syslog Server2: Port:

Syslog Severity: Specify severity of events forwarded to Syslog servers

SNMP

To configure SNMP, complete the following steps:

1. Navigate to **Configuration > Wi-Fi Profiles > AP Groups** page.
2. Click **Add New** and select **Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)** from the **Type** drop-down list.
3. Click **Management** tab > **SNMP** section.

[Table 13](#) lists configurable fields that are displayed in the **SNMP** section.

Table 14 SNMP parameters

Parameter	Description	Range	Default
Enable	Provision to enable SNMPv2 or SNMPv3 support on the device	-	-
SNMPv2c RO community	SNMP v2c read-only community string.	-	public
SNMPv2c RW community	SNMP v2c read-write community string.	-	private
Trap Receiver IP	Provision to configure SNMP trap receiver IPv4 server.	-	-
SNMPv3 Username	Enter the username for SNMPv3.	-	-
SNMPv3 Password	Enter the password for SNMPv3.	-	-
Authentication	Provision to choose the authentication type as MD5 or SHA.	-	MD5
Access	Provision to choose Access type as read-only or read-write.	-	RO
Encryption	Choose ON or OFF. APs use the AES algorithm for encryption.	-	ON



Note

The AP uses the AES algorithm for encryption. It uses the SNMPv3 password configuration parameter for encryption and authentication.

Figure 10 SNMP parameters

SNMP

☒ Enable Enable SNMP support on the device

SNMPv2c RO Community

public

SNMPv2c read-only community string (max 64 characters)

SNMPv2c RW Community

private

SNMPv2c read-write community string (max 64 characters)

Trap Receiver IP

xxxxxxxxxxxx

SNMP trap server IP address

SNMPv3 Username

SNMPv3 user name (max 32 characters)

SNMPv3 Password

Show

SNMPv3 password (8 to 32 characters)

Authentication

☒ MD5
 ☐ SHA

Access

☒ Read-Only
 ☐ Read-Write

Encryption

☒ On
 ☐ Off

Configuring the Radio

This chapter describes the following topics:

- [Overview](#)
- [Configuring Radio parameters](#)
- [BSS coloring](#)
- [Target Wake Time \(TWT\)](#)
- [Receive sensitivity configuration](#)
- [Multicast-snooping and Multicast-to-Unicast conversion](#)

Overview

Enterprise Wi-Fi AP devices support numerous configurable radio parameters to enhance the quality of service according to the deployment.

Configuring Radio parameters

The XV3-8 Tri-Band Indoor Wi-Fi 6 AP can operate in either Dual Band Simultaneous (DBS) or Single Band Simultaneous (SBS). This feature provides the flexibility of splitting 5 GHz radio into two independently configurable and operational radios. In DBS mode, 5 GHz radio operates as single radio with an 8x8 configuration. In SBS mode, 5 GHz Radio operates as split radio with each 4x4 configuration. Configurable parameters under the **Radio** profile are listed below.

- [Basic](#)
- [Software-Defined Radio \(SDR\) capabilities](#)
- [Enhanced Roaming](#)

Basic

To configure radio parameters, complete the following steps:

1. Navigate to **Configuration > Wi-Fi Profiles > AP Groups** page.
2. Click **Add New** and select **Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)** from the **Type** drop-down list.
3. Click **Radio** tab > **Basic** section.


[Table 15](#) lists the configurable fields that are displayed in the **Radio > Basic** section.

Table 15 Configure Radio parameters

Parameter	Description	Range	Default
Radio			
Enable	Enables the operation of radio.	-	Enabled
Band	Select the appropriate radio band, if the radio supports multiple bands.	-	-
Channel	Select the channel from the drop-down list. Channels in the drop-down list are populated based on the country configured.	Wi-Fi 6/6E APs <ul style="list-style-type: none"> • 2.4 GHz: 1 - 14 • 5 GHz: 36 - 173 • 6 GHz: 1 - 233 	Auto
Channel Width	Specifies the channel widths for the operation. The following widths are supported: <ul style="list-style-type: none"> • For 2.4 GHz: Only 20 MHz channel width is supported. • For 5 GHz: 20 MHz, 40 MHz, 80 MHz, and 160 MHz channel widths are supported. • For 6 GHz: 20 MHz, 40 MHz, 80 MHz, 160 MHz channel widths are supported. 	-	<ul style="list-style-type: none"> • 2.4 GHz: 20 MHz • 5 GHz: 40 MHz • 6 GHz: 80 MHz
Transmit Power	Total conducted transmit power, in decibel-milliwatt (dBm), of each radio based on coverage and SLA. The maximum transmit power of Enterprise Wi-Fi AP devices varies based on model number. Details of transmit power supported by each Enterprise Wi-Fi AP device are available at https://www.cambiumnetworks.com/products/wifi/ . Transmit power varies as per the country where the AP is deployed.. The default value is AUTO , which means radio transmit power is configured to the maximum as per the county configured.	<ul style="list-style-type: none"> • 2.4 GHz: 4 to 30 • 5 GHz: 4 to 30 • 6 GHz: 4 to 30 	Auto

Parameter	Description	Range	Default
Beacon Interval	Specifies the time duration (in milliseconds) between two consecutive Beacons.	50ms - 3400ms.	100
Minimum Unicast rate	Specifies the coverage area of the Enterprise Wi-Fi AP device. The higher the rate selected, the lesser the range. You can configure this value based on the SLA in the deployment. The drop-down list contains all values advertised by Enterprise Wi-Fi AP devices, including legacy, HE, HT, and VHT rates.	Standard 802.11b and 802.11g data rates	1Mbps
Candidate Channels	<p>Specifies selective channels based on user requirement. Options vary based on a band of operation and are as follows:</p> <ul style="list-style-type: none"> • For 2.4 GHz: <ul style="list-style-type: none"> ◦ All ◦ Specific • For 5 GHz: <ul style="list-style-type: none"> ◦ All ◦ Specific ◦ Prefer Non-DFS ◦ Prefer DFS • For 6 GHz: <ul style="list-style-type: none"> ◦ All ◦ Specific 	Wi-Fi 6/6E APs <ul style="list-style-type: none"> • 2.4 GHz: 1 - 14 • 5 GHz: 36 - 173 • 6 GHz: 1 - 233 	All
Mode	All Enterprise Wi-Fi AP devices support either 802.11ax, 802.11ac Wave 1, or 802.11ac Wave 2. Some legacy clients might not work as expected; therefore, this parameter can be tuned for backward compatibility based on wireless clients.	Wi-Fi 6/6E APs <ul style="list-style-type: none"> • 2.4 GHz: b/g/n/ax • 5 GHz: a/n/ac/ax 	All mode
Short Guard Interval	Standard 802.11 parameter to increase the throughput of an Enterprise Wi-Fi AP device.	-	Enabled
Off Channel Scan (OCS)			

Parameter	Description	Range	Default
Enable	Provision to enable OCS on a device to capture neighbor clients and APs.	-	-
Dwell-time	Configure the time period to spend scanning of Wi-Fi devices on a channel.	50-300	50ms
Auto-RF (Dynamic Power)			
Enable	Enable or disable dynamic power management.	-	-
Mode	Select the required dynamic power modes. Two modes are supported: <ul style="list-style-type: none"> • By-Channel • By-Band 	-	By-Channel
Minimum Transmit Power	The minimum transmit power that the AP can assign to radio when adjusting automatic cell sizes	5-15 dBm	8 dBm
Minimum Neighbour Threshold	The minimum number of neighbors to consider for power reduction by automatic cell logic.	1-10	2
Cellsize Overlap Threshold	Cell overlap will be allowed when the AP is determining automatic cell sizes.	0-100%	50%
Auto-RF (Dynamic Channel)			
Enable	Enable or disable the Dynamic Channel auto-RF functionality.		Disabled
Packet Error Rate	Enable channel change using unsuccessful packet transmissions by the AP.		
Packet Error Rate Threshold	Specifies the packet error rate threshold in percentage (%).	10-90%	30
Number of Packet Error Rate samples	Specifies the number of packet error rate samples needed to trigger a channel switch.	1-120	40
Channel Utilization	Enable channel change using the channel efficiency.		
Channel Utilization Threshold	Specifies the channel utilization threshold in percentage (%).	30-100%	70

Parameter	Description	Range	Default
Number of Channel Utilization samples	Specifies the number of channel utilization samples needed to trigger a channel switch.	5-300	100
Noise	Enable channel change with higher noise.		
Noise Threshold	Specifies the noise threshold in dBm.	-70 to -90 dBm	-70
Number of Noise samples	Specifies the number of noise samples needed to trigger a channel switch.	5-120	40
Auto-RF Iterations	<p>Specifies the number of times the Auto-RF channel change function must run, at the configured frequency, before stopping.</p> <p>The iteration count resets when the AP restarts or when the radio resets.</p> <p>The default value is 0. It indicates that the Auto-RF channel change function will run at the frequency configured in either of the following parameters without stopping:</p> <ul style="list-style-type: none"> • Enable time range for Auto-RF • Channel Hold Time <div>  <div> Note When the AP exceeds the configured iteration count, the Dynamic Channel Selection (DCS) method of channel selection takes over. </div> </div> <p>For more information on Auto-RF, see Auto-RF.</p>	0-100	0
Samples	Specifies the minimum number of samples required to run the channel selection.	1-20	3
Enable time range for Auto-RF	<p>Specifies the time range (in the 24 hour format) at which the Auto-RF channel change function must run everyday.</p> <p>When enabled, select the start and end time.</p>		

Parameter	Description	Range	Default
Channel Hold Time	Specifies the time (in minutes) for which the AP must hold the channel.	<ul style="list-style-type: none"> 1-44640 minutes for APs running version 6.6.0.1 and later 1-4320 minutes for APs running versions earlier than 6.6.0.1. 	1440

To configure **Auto-RF (Dynamic Channel)** using the CLI, execute the following commands:

```
ap(config-radio-1)# auto-rf dynamic-channel

acceptance-per-threshold : Configure Acceptance Packet Error Rate
(PER) threshold
channel-hold-time       : specifies how much time AP needs to hold the
channel. Default is 1440 mins
cmbnbnr-minsnr         : Configure the cambium neighbour minimum SNR to
consider as part of autorf cambium neighbour factor
congestion-channel-switch : Enable / Disable Congestion based channel
switch, disabled by default
congestion-threshold   : Configure Congestion threshold
count                  : Configure number of times autorf need to run;
'0' disables this feature
dcs-monitor-interval   : Configure dcs monitor interval in minutes.
dcs-trigger-threshold  : Configure dcs trigger threshold percentage
per-channel-switch     : Enable / Disable PER based channel switch,
disabled by default
samples                : Configure the minimum number of samples
required to run the channel selection
schedule-time          : Configure time range (24 hour format) at which
autorf algorithm need to run everyday
weightage-map-index    : Configure weightage map index
```

To configure **Auto-RF (Dynamic Power)** using the CLI, execute the following commands:

```
ap(config-radio-1)# auto-rf dynamic-power
```

cellsize-overlap-threshold : Cell overlap that will be allowed when the AP is determining automatic cell sizes

maximum-transmit-power : Maximum transmit power that the AP can assign to a radio when adjusting automatic cell sizes

minimum-neighbor-threshold : The Minimum number of neighbors to consider for power reduction by autocell logic

minimum-transmit-power : Minimum transmit power that the AP can assign to a radio when adjusting automatic cell sizes

mode : Set dynamic power mode by-channel/by-band

Figure 11 Radio parameters in the Basic page

Basic

Status

☒ Enabled ☐ Disabled Enable/Disable operation of this radio

Channel

Auto

Only 'Auto' value is allowed. Configure static channel under the 'Advanced Settings' section available on the Access Point level configuration page [Learn more](#)

Candidates Channel

All

Candidate channels is a list of channels on which AP can operate. List of channels depend on the band and country.

Channel Width

20

Operating width of the channel

Transmit Power

Auto

Radio transmit power in dBm (4 to 30; subject to regulatory limit)

Beacon Interval

100

Beacon interval in ms (50 to 3500) ⓘ

Minimum Unicast Rate

1

Configure the minimum unicast management rate (Mbps)

Multicast Data Rate

Highest Basic

Data-rate to use for transmission of multicast/broadcast packets

Mode

Default

Allow 802.11 b/g/n clients to connect

☐ Airtime Fairness Enable Airtime Fairness to improve performance of 11n and 11ac clients by throttling legacy clients

☒ Short Guard Interval Enable Short Guard interval to increase device throughput

Figure 12 Channel Scan - Off Channel Scan option

Channel Scan

☒ Off Channel Scan ☐ Continuous Background Scan ☐ None Enable/Disable operation of this radio

OCS periodically goes away from current operating channel (home channel) to other channels and collects data about neighboring clients, AP and RF characteristics.

Dwell time

50

Configure Off Channel Scan dwell time in milliseconds (50-300)

Figure 13 Channel Scan - Continuous Background Scan option

Channel Scan

☐ Off Channel Scan

☒ Continuous Background Scan

☐ None

Enable/Disable operation of this radio

Continuous background scan (CBS) reduces the dwell time, controls the channel switches and also monitors the voice data queues.

Rest TimeRest Time — Interval between scans on different channels (5-15).

Wait TimeConfigure wait time in minutes to wait after all channels are scanned and before starting a new scan (1-10)

Dwell Split Time

25

Configure dwell split time to spend on foreign channel

Dwell Rest TimeConfigure time interval between scans on same channel (100-1000)

☐ Channel Switch Announcement Use channel switch announcement as a part of channel change

Figure 14 Auto-RF - Dynamic Channel

Auto-RF

Auto-RF Dynamic Power option adjusts the radio transmit power based on the neighboring Cambium APs transmit power. Auto-RF Dynamic Channel changes the radio channel based on current operating channel RF conditions like channel utilization, interference, packet error rate, etc.

Mode Selection

Dynamic Channel

Dynamic Power

☒ Enable Enable Auto-RF to adjust dynamic channel selection based on RF conditions

☐ Packet Error Rate Enable channel change using unsuccessful packet transmissions by the AP

☐ Channel Utilization Enable channel change using the channel efficiency

☐ Noise Enable channel change with higher noise

Auto-RF IterationsConfigure number of times Auto-RF needs to run (0-100). 0 disables this feature

SamplesConfigure the minimum number of samples required to run the channel selection (1-20)

☐ Enable time range for Auto-RF. Configure time range (24 hour format) at which Auto-RF needs to run everyday.

Channel Hold TimeChannel hold time specifies how much time AP needs to hold the channel <1-44640> mins for build '6.6.0.1' and onwards. Range <1-4320> applies for AP running build below '6.6.0.1'.

Deprecated (Version 3.11.4 and 4.0)

Channel Selection Mode

Interference

Channel selection done based on interference

Channel Utilization ThresholdConfigure channel utilization threshold in %(20-40)

Figure 15 Auto-RF - Dynamic Power

Auto-RF

Auto-RF Dynamic Power option adjusts the radio transmit power based on the neighboring Cambium APs transmit power. Auto-RF Dynamic Channel changes the radio channel based on current operating channel RF conditions like channel utilization, interference, packet error rate, etc.

Mode Selection

Dynamic Channel

Dynamic Power

☐ Enable Enable Dynamic Power management

☐ By-Channel ☒ By-Band Set dynamic power mode by-channel / by-band

Maximum Transmit Power

Maximum transmit power that the AP can assign to a radio when adjusting automatic cell sizes. (5-30) dBm

Minimum Transmit Power

Minimum transmit power that the AP can assign to a radio when adjusting automatic cell sizes. (5-20) dBm

Minimum Neighbour Threshold

The Minimum number of neighbors to consider for power reduction by autotcell logic. (1-10)

Cellsize Overlap Threshold

Cell overlap that will be allowed when the AP is determining automatic cell sizes (0-100) %

Software-Defined Radio (SDR) capabilities



Note

- In XV3-8, radio 3 is available only in the SBS mode.
- In XE5-8, radio 5 is available only in the SBS mode.

Table 16 Supported radios

Access Point Model	Radio 1 (2.4 GHz)	Radio 2		Radio 3		Radio 4 (5 GHz)	Radio 5 (5 GHz)
		5 GHz	6 GHz	5 GHz	6 GHz		
XV3-8	✓	✓ (DBS)		✓ (SBS)			
XV2-2	✓	✓					
XV2-2T0	✓	✓					
XV2-2T1	✓	✓					
XE3-4	✓	✓		✓	✓		
XE3-4TN	✓	✓		✓	✓		
XE5-8	✓	✓	✓	✓	✓	✓ (DBS)	✓ (SBS)

Access Point Model	Radio 1 (2.4 GHz)	Radio 2		Radio 3		Radio 4 (5 GHz)	Radio 5 (5 GHz)
		5 GHz	6 GHz	5 GHz	6 GHz		
XV2-21X	✓	✓					
XV2-23T	✓	✓					
XV2-22H	✓	✓					

Table 17 Factory reset behavior of multi-radio APs

Access Point Model	Radio 1 (2.4 GHz)	Radio 2		Radio 3		Radio 4 (5 GHz)	Radio 5 (5 GHz)
		5 GHz	6 GHz	5 GHz	6 GHz		
XV3-8	ON	ON	NA	OFF	NA	-	-
XE3-4	ON	ON	NA	OFF	ON	-	-
XE3-4TN	ON	ON	NA	OFF	ON	-	-
XE5-8	ON	ON	OFF	OFF	ON	ON 4x4 SBS	ON 4x4 SBS

The **Radio** page allows the user to enable or disable the Software-Defined Radio (SDR) operations. It allows to configure **Software Defined Radios, Basic, Enhanced Roaming, Off Channel Scan, Auto-RF, and External Antennas**.



Note

The software-defined radio creation and channel listing are populated based on the country-specific restrictions, device type, and release version.

Software-Defined Radio

Software-Defined Radio (SDR) allows you to configure radio parameters for XV3-8, XE3-4, XE3-4TN, and XE5-8 device models. By default these device models are configured for radio bands as shown in the above

figure. The other radio bands for which the devices can be configured are as shown in [Table 18](#).

Table 18 Supported Radio bands for Enterprise Wi-Fi Series (XE, XV-Series)

Models	Radios	Supported Radio Bands	Channel Specification		
			Channel width	Default Channel width	Supported channel list
XV3-8	Radio 1	2.4 GHz	20/40	20	1 to 13
	Radio 2	5 GHz (8x8 - single radio) or 5 GHz (Split 4x4 dual radio)	20 / 40 / 80	40	100 to 165 in Split 4x4 dual radio
	Radio 3		20 / 40 / 80	40	36 to 64 in Split 4x4 dual radio
XE3-4	Radio 1	2.4 GHz	20/40	20	1 to 13
	Radio 2	5 GHz	20 / 40 / 80	40	36 to 64
	Radio 3	5 GHz	20 / 40 / 80 / 160	40	100 to 165
		6 GHz		160	Any 6 GHz channel
XE3-4TN	Radio 1	2.4 GHz	20/40	20	1 to 13
	Radio 2	5 GHz	20 / 40 / 80	40	36 to 64
	Radio 3	5 GHz	20 / 40 / 80 / 160	40	100 to 165
		6 GHz		160	Any 6 GHz channel
XE5-8	Radio 1	2.4 GHz	20/40	20	1 to 13
	Radio 2	5 GHz or 6 GHz	20 / 40 / 80 / 160	20*/80**	Refer to Table 19 for supported channel list in 5 GHz and 6 GHz.
	Radio 3	5 GHz or 6 GHz	20 / 40 / 80 / 160	20*/80**	
	Radio 4	5 GHz (8x8 - single radio) or 5 GHz (Split 4x4 dual radio)	20 / 40 / 80	20	
	Radio 5		20 / 40 / 80		
* 5 GHz **6 GHz					

**Note:**

- Split 4x4 is applicable only for 8x8 spatial streams supported devices. (Supported device models are XV3-8 and XE5-8).
- Dual 5 GHz Radio (Only supported for XV3-8 and XE5-8 Access Points) Splits 8x8 5 GHz radio into two 4x4 5 GHz radios.

Table 19 Supported Channel list 5 GHz or 6 GHz in XE5-8

Radio Index				Radio 1	Radio 2	Radio 3	Radio 4	Radio 5
8x8 mode of operation: Radio 4 & 5 as single radio with 8x8								
Radio 2	Radio 3	Radio 4 and 5						
5 GHz	5 GHz	5 GHz		NA	100 to 128	149 to 165	36 to 64	
6 GHz	5 GHz	5 GHz		NA	Any 6 GHz channel	100 to 165	36 to 64	
5 GHz	6 GHz	5 GHz		NA	100 to 165	Any 6 GHz channel	36 to 64	
6 GHz	6 GHz	5 GHz		NA	* 1 to 93	** 97 to 233 / 65 to 93	36 to 165	
Split 4x4 mode of operation: Radio 4 and 5 as individual radio with 4x4								
Radio 2	Radio 3	Radio 4	Radio 5					
5 GHz	5 GHz	5 GHz	5 GHz	NA	60 to 64	100 to 128	149 to 165	36 to 40
6 GHz	5 GHz	5 GHz	5 GHz	NA	Any 6 GHz channel	100 to 128	149 to 165	36 to 64
5 GHz	6 GHz	5 GHz	5 GHz	NA	100 to 128	Any 6 GHz channel	149 to 165	36 to 64
6 GHz	6 GHz	5 GHz	5 GHz	NA	* 1 to 93	** 97 to 233	100 to 165	36 to 64
Note: *FCC SKU 6GHz UNII-5 or 6 (1 - 93) EU SKU UNII-5 low (1 - 61) **FCC SKU 6GHz UNII-7 or 8 (97 - 233) EU SKU UNII-5 High (65 - 93)								

**Note**

You can use the `no channels-distribution` global configuration CLI command for all multi-radio platforms, such as XE3-4, XE3-4TN, and XE5-8 APs. When configured on device, default channel list can be overridden.

Off Channel Scan (OCS)

The following figure illustrates how to configure **Off Channel Scan** using the CLI:

```
ap(config)# wireless radio 2
ap(config-radio-2)# off-channel-scan

dwell-time : Configure Off-Channel-Scan dwelltime
interval : Configure Off-Channel-Scan interval
type : Configure active/passive Off-Channel-Scan

ap(config-radio-2)# off-channel-scan type
active : active off channel scan
passive : passive off channel scan
```

[Table 20](#) lists the fields that are required for configuring **Off Channel Scan**:

Table 20 Configuring Off Channel Scan

Parameter	Description	Range	Default
dwell time	Provision to configure Off Channel Scan dwell time. Needs to change 100 or more than 100+ ms for supporting passive scan method.	50-300	50ms

Enhanced Roaming

[Table 21](#) lists configurable fields that are displayed in the **Radio > Enhanced Roaming** tab.

Table 21 Configuring Radio > Enhanced Roaming parameters

Parameter	Description	Range	Default
Enhanced Roaming			
Enable	Provision to enable enhanced roaming on device.	-	Disabled
Roam SNR threshold	Enterprise Wi-Fi AP device triggers de-authentication of the wireless station when the wireless station is seen at configured SNR level or below.	1-100	15dB

☒ **Enhanced Roaming**

Please enable enhanced roaming only in networks with sufficient signal strength throughout the coverage area, otherwise clients could face connectivity issues

☐ Enable Enable active disconnection of clients with weak signal

Roam SNR Threshold

SNR below which clients will be forced to roam (1-100 dB)

BSS Coloring

Multiple APs operate on a shared channel by mitigating co-channel interference. This is achieved through a spatial reuse technique known as BSS Coloring, which enables devices in one BSS to ignore frames from other BSSs on the same channel that are typically some distance away.

Target Wake Time (TWT)

The Target Wake Time (TWT) feature, included in the IEEE 802.11ax amendment, provides a mechanism to schedule transmissions at a specific time or set of times for individual STAs to wake to exchange frames with AP. Using TWT, each STA negotiates awake periods with the AP to transmit and receive data packets allowing the STA to go to doze mode to minimize energy consumption and reduce contention within the basic service set (BSS).



Note

By default, BSS coloring and TWT are enabled.

Receive sensitivity configuration

This feature allows users to configure the receiver sensitivity per radio. The configuration hooks are exposed from both CLI and XMS-Cloud. cnMaestro does not expose any hooks for configuring receiver configuration. Receiver configuration determines the signal power required at the receiver to achieve the targeted or configured bit rate. Every RF receiver comes with a default sensitivity, which may not be sufficient for achieving the required RF performance in terms of meeting the bit rate. Therefore, reconfiguration of receiver sensitivity is suggested.

Multicast-snooping and Multicast-to-Unicast conversion

Multicast-to-Unicast conversion heavily depends on multicast (IGMP) snooping. With IGMP snooping enabled, the device monitors IGMP traffic on the network and forwards multicast traffic to only the downstream interfaces that are connected to interested receivers. The device conserves bandwidth by sending multicast traffic only to clients connected to devices that receive the traffic (instead of flooding the traffic to all the downstream clients in a VLAN).

The functionality to preserve both multicast and unicast MAC addresses during multicast enhancement implementation for packets in APs is introduced. The AP supports Directed Multicast Services (DMS) and Multicast Enhancement (ME). ME is a feature provided in APs that allows multicast frames to be sent as unicast frames to each member of the mentioned multicast group to improve the QoS of the transmission between the STA and the AP. The multicast frame is received at the host WLAN driver as an 802.3 (Ethernet) frame. This frame header contains the destination and source address, which are the multicast group address and client address, respectively. Iteratively, the Ethernet header is replaced with the unicast addresses of the clients present in the multicast group and sent out to the “air”. During this process, the multicast group address is completely lost from the frame.

CLI Configuration:

```
XV3-8-EC7708(config)# service show mcastsnoop br0 mdbtbl

-----Bridge Snooping Hash Table -- IPv4-----
NUM  GROUP                                FDB                                PORT  AGE

IPv4 Router Ports:      None

-----Bridge Snooping Hash Table -- IPv6-----
NUM  GROUP                                FDB                                PORT  AGE

IPv6 Router Ports:      None
XV3-8-EC7708(config)# service show mcastsnoop br0 acltbl

IGMP ACL TABLE:
PATTEN 01:224.000.000.001/255.255.255.255 - 00:00:00:00:00:00/00:00:00:00:00:00 -- SYSTEM WIDE MANAGEMENT
PATTEN 02:224.000.000.000/255.255.000.000 - 00:00:00:00:00:00/00:00:00:00:00:00 -- MANAGEMENT
PATTEN 03:239.255.000.000/255.255.000.000 - 00:00:00:00:00:00/00:00:00:00:00:00 -- MANAGEMENT
PATTEN 04:239.255.255.250/255.255.255.255 - 00:00:00:00:00:00/00:00:00:00:00:00 -- NON SNOOPING
PATTEN 05:224.000.000.251/255.255.255.255 - 00:00:00:00:00:00/00:00:00:00:00:00 -- NON SNOOPING
PATTEN 06:224.000.000.252/255.255.255.255 - 00:00:00:00:00:00/00:00:00:00:00:00 -- NON SNOOPING
PATTEN 07:000.000.000.000/000.000.000.000 - 01:00:5e:00:00:00/ff:ff:ff:00:00:00 -- MULTICAST

MLD ACL TABLE:
PATTEN 01:ff01:0000:0000:0000:0000:0000:0001/ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff - 00:00:00:00:00:00/00:00:00:00:00:00 -- SYSTEM WIDE MANAGEMENT
PATTEN 02:ff02:0000:0000:0000:0000:0000:0001/ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff - 00:00:00:00:00:00/00:00:00:00:00:00 -- SYSTEM WIDE MANAGEMENT
PATTEN 03:ff00:0000:0000:0000:0000:0000:0000/fff0:0000:0000:0000:0000:0000:0000:0000 - 00:00:00:00:00:00/00:00:00:00:00:00 -- MANAGEMENT
PATTEN 04:0000:0000:0000:0000:0000:0000:0000/0000:0000:0000:0000:0000:0000:0000:0000 - 33:33:00:00:00:00/ff:ff:00:00:00:00 -- MULTICAST
```

```
ap(config)# multicast-snoop
ap(config)# no multicast-snoop
ap(config)# save
ap(config)# wireless radio 1
ap(config-radio-1)# multicast-to-unicast
ap(config-radio-1)# multicast-to-unicast mode 802.3
ap(config-radio-1)# multicast-to-unicast mode amsdu
ap(config-radio-1)# multicast-to-unicast exclude-list 224.0.0.1
ap(config-radio-1)# show wireless radios multicast-to-unicast

=====
RADIO BAND MC2UC MC2UC-MODE EXCLUDE-LIST
=====

radio1 2.4GHz NO amsdu
radio2 5GHz YES amsdu
ap(config-radio-1)#
```

Auto-RF

This topic contains the following sections:

- [Overview](#)
- [Dynamic Channel](#)
- [Dynamic Power](#)

- [Auto-RF](#)
- [Configuring Dynamic Channel](#)
- [Configuring Dynamic Power](#)
- [Recommended Configuration](#)

Overview

Auto-RF allows APs to obtain various RF statistics and utilize them to provide wireless clients with a better RF environment by choosing the proper channel and transmitting power to each radio. This results in better application performance and improved quality of calls for the end user.

Auto-RF consists of the following two functionalities:

- [Dynamic Channel](#)—Enables radios to choose the best channel both at device turn on and subsequently if the channel or RF conditions change.
- [Dynamic Power](#)—Aids radios in determining the proper transmit power to deal with coverage gaps and reduce RF interference.

Dynamic Channel

Channel selection by APs can involve any of the following methods:

- [Auto Channel Selection \(ACS\)](#)
- [Dynamic Channel Selection \(DCS\)](#)

Auto Channel Selection (ACS)

Auto-RF runs independently on each device in a deployment. You can enable the feature in all the bands (2.4 GHz, 5 GHz, and 6 GHz (if AP supports)). In 2.4 GHz, channels 1, 6, and 11 are considered for channel selection. AP continuously executes the Continuous Background Scan (CBS) to collect samples and feed them to the ACS to choose the best channel based on the channel score. The packet queue is verified and the RF is monitored continuously to ensure that high priority traffic is delivered before starting the CBS. CBS is performed so that the device avoids background scan while voice and video traffic is transmitted. The scan is split into multiple slots to avoid diverting from the operating channel for a longer duration which will affect the performance of the AP.

Dynamic Channel Selection (DCS)

If the environment has lot of Wi-Fi interference or high packet error rate, Dynamic Channel Selection (DCS) takes over and initiates Packet Error Rate (PER) and Channel Utilization (CU) based channel switch methods. The AP monitors the error rate and Wi-Fi interference to see whether the threshold is crossed to initiate the channel switch. The AP sends the channel switch announcement in a beacon before any channel change occurs.

Dynamic Power

In multi-AP deployments, APs must automatically determine the cell size (coverage area), that is, increase or decrease transmit power to ensure the following:

- There are no coverage gaps—Increase transmit power
- There is no interference because of overlapping APs. Overlapping of APs creates interference and clients roam between multiple APs if they see more than one AP with a good transmit power. —
Decrease transmit power

Packets and scan results from CBS are parsed and neighbor entries are created which contains data about their transmission power and their neighbors. Periodically this data is processed and categorized to display how neighbors have seen their SNR.

Auto-RF behavior on device turn on

When the AP turns on the first time, it performs an initial scan (for about 0-300 seconds) to select the best operating channel. During this scan, CBS collects samples. The AP remains on the selected channel until one of the following scenarios occur:

- channel hold time expires
- configuration changes
- the radio restarts

After the hold time expires, the AP reinitiates the Automatic Channel Selection (ACS) algorithm to reassess and choose a new channel based on collected samples. If the current channel still has the highest score, it is retained. In cases of configuration changes or radio restarts, the collected samples are reset, but historical data remains, allowing CBS to automatically collect fresh samples.

Configuring Dynamic Channel

Dynamic channel configuration is achieved by the following methods:

- [ACS method](#)
- [DCS method](#)

ACS method

In the ACS method, to enable auto-RF Dynamic Channel in the cnMaestro UI, complete the following steps:

1. Go to **Configuration > Wi-Fi Profiles > AP Groups** page.
2. Click **Add New**.
3. Associate an existing WLAN and configure other AP group parameters.
4. Click **Radio** on the left menu.

5. In the required radio band tab, expand the **Auto-RF** section.
6. In the **Dynamic Channel** tab, select the **Enable** check box.

Once Auto-RF Dynamic Channel is enabled, ACS runs at regular intervals based on the **Samples** and **Channel Hold Time**, or the **Enable time range for Auto-RF** configuration parameters. For information on these parameters, see [Configuring the Radio](#).

DCS method

DCS configuration helps in avoiding instances when there is a spike in packet error rate (PER) or Channel Busy. The following are the default configuration parameters and their values:

- DCS trigger threshold—80%

CLI command—`auto-rf dynamic-channel dcs-trigger-threshold`

- DCS monitor interval—10 minutes

CLI command—`auto-rf dynamic-channel dcs-monitor-interval`

Both these parameters are available only as CLI commands that you can configure in the **AP Groups > User Overrides** section in cnMaestro.

Consider a scenario where the device detects that the PER or Congestion threshold is exceeded for a brief period in a day. If the threshold breach occurred because of a spike in PER or Congestion, the AP must not change the channel. You can avoid this scenario by configuring the DCS threshold and monitor interval. When configured, the AP switches to a different channel if the PER or Congestion threshold is breached continuously for the DCS duration and if the percentage of the breach exceeds the DCS threshold. DCS is enabled if either Channel Utilization (CU) or Packet Error Rate (PER) parameter is enabled.

Packet Error Rate (PER)

Consider a scenario where an AP must switch channels if the PER is more than 30% in a 10 minute interval. The AP monitors the PER, and if it exceeds 30% (default threshold) for 80% of the samples in a 10-minute interval, it will initiate a channel switch. However, when the PER threshold is breached, other configurations, such as sampling, channel hold time, and intervals are overridden. With the default DCS threshold and

interval configured, Auto-RF manages the channel switch when the above conditions are met. Hence, the AP changes channels if the PER remains consistently high (above 30%) for most of a 10-minute period.

Packet Error Rate Threshold	<input type="text" value="30"/>	Configure packet error rate threshold in %(10-90)
Number of Packet Error Rate samples	<input type="text" value="40"/>	Configure number of packet error rate samples, needed to trigger a channel switch (1-120)

Congestion channel switch

Consider a scenario where an AP must switch channels if the channel utilization exceeds a threshold of 70% (default) in a 10-minute interval. The AP monitors channel utilization, and if it exceeds 70% (default threshold) for 80% of the samples in a 10-minute interval, it will initiate a channel switch. However, when the congestion threshold is breached, other configurations, such as sampling, channel hold time, and intervals are overridden. With the default DCS threshold and interval configured, Auto-RF will handle the channel switch when the above conditions are met. Hence, the AP changes channels if channel utilization remains consistently high (above 70%) for most of a 10-minute period.

<input checked="" type="checkbox"/> Channel Utilization	Enable channel change using the channel efficiency	
Channel Utilization Threshold	<input type="text" value="70"/>	Configure Channel Utilization threshold in %(30-100)
Number of Channel Utilization samples	<input type="text" value="100"/>	Configure number of Channel Utilization samples, needed to trigger a channel switch(5-300)

Configuring Dynamic Power

To enable auto-RF Dynamic Power in the cnMaestro UI, complete the following steps:

1. Go to **Configuration > Wi-Fi Profiles > AP Groups** page.
2. Click **Add New**.
3. Associate an existing WLAN and configure other AP group parameters.
4. Click **Radio** on the left menu.
5. In the required radio band tab, expand the **Auto-RF** section.
6. In the **Dynamic Power** tab, select the **Enable** check box.

Mode Selection	
<input type="radio"/> Dynamic Channel	<input checked="" type="radio"/> Dynamic Power
<input type="checkbox"/> Enable Enable Dynamic Power management	
<input type="radio"/> By-Channel <input checked="" type="radio"/> By-Band Set dynamic power mode by-channel / by-band	

Dynamic Power can be configured in the following two modes:

- **By-Band:** Considers neighbor APs across all channels of same band for operating Auto-RF dynamic transmit power.

This is the default option in the Dynamic Power configuration.

- **By-Channel:** Considers only operating channel neighbor APs (that also within the same AP group) for operating Auto-RF dynamic transmit power.

When Auto-RF Dynamic Power is enabled, by default, CBS runs in the background with a 50% overlap threshold between APs. The default minimum transmit power is set to 8 dBm. The dynamic-power algorithm cannot reduce the transmit power below this level, even if there is overlap in AP signals. The **Minimum Neighbor Threshold** parameter defines the minimum number of neighboring APs required to enable dynamic power selection.

With Auto-RF Dynamic Power enabled, the system manages transmit power while maintaining a minimum level and considering AP overlap and neighbor requirements.

☐ By-Channel
 ☒ By-Band
 Set dynamic power mode by-channel / by-band

Maximum Transmit Power	<input type="text" value="30"/>	Maximum transmit power that the AP can assign to a radio when adjusting automatic cell sizes. (5-30) dBm
Minimum Transmit Power	<input type="text" value="8"/>	Minimum transmit power that the AP can assign to a radio when adjusting automatic cell sizes. (5-20) dBm
Minimum Neighbour Threshold	<input type="text" value="2"/>	The Minimum number of neighbors to consider for power reduction by autocell logic. (1-10)
Cellsize Overlap Threshold	<input type="text" value="50"/>	Cell overlap that will be allowed when the AP is determining automatic cell sizes (0-100) %

Recommended Configuration

For Auto-RF feature to function correctly, the following configuration is recommended:

- [Basic section](#)
- [Channel Scan section](#)

Basic section

Configure the following parameters in the **Radio > Basic** section with the recommended values:

- **Channel**—Auto
- **Transmit Power**—Auto
- **Channel Width**—20, 40, 80, or 160 MHz based on the deployment
- **Candidates Channel**—All.

If you want to restrict the APs to operate on specific channels, you must configure the required channels.

Basic

Status

☒ Enabled
 ☐ Disabled
 Enable/Disable operation of this radio

Channel

Auto

▼

Only 'Auto' value is allowed. Configure static channel under the 'Advanced Settings' section available on the Access Point level configuration page [Learn more](#)

Candidate Channels

All

▼

Candidate channels is a list of channels on which AP can operate. List of channels depend on the band and country.

Channel Width

20

▼

Operating width of the channel

Transmit Power

Auto

▼

Radio transmit power in dBm (4 to 30; subject to regulatory limit) ⓘ

Channel Scan section

Configure the following parameters in the **Radio > Channel Scan** section with the recommended values:

- Select the **Continuous Background Scan (CBS)** option—Selected by default.
- **Wait Time** in minutes
- **Rest Time**, **Dwell Split Time**, and **Dwell Rest Time** in milliseconds
- Select the **Channel Switch Announcement** check box to enable the AP to send notifications before any channel change.

Channel Scan

☐ Off Channel Scan
 ☒ Continuous Background Scan
 ☐ None
 Enable/Disable operation of this radio

Continuous background scan (CBS) reduces the dwell time, controls the channel switches and also monitors the voice data queues.

Rest Time

6

Rest Time — Interval between scans on different channels (5-15 seconds).

Wait Time

2

Configure wait time in minutes to wait after all channels are scanned and before starting a new scan (1-10 minutes)

Dwell Split Time

25

▼

Configure dwell split time to spend on foreign channel

Dwell Rest Time

100

Configure time interval between scans on same channel (100-1000 milliseconds)

☐ Channel Switch Announcement
 Use channel switch announcement as a part of channel change

Configuring the Wireless LAN

This chapter describes the following topics:

- [Overview](#)
- [Configuring the WLAN parameters](#)
- [Link Aggregation Control Protocol \(LACP\)](#)
- [RADIUS attributes](#)
- [Enterprise PSK \(ePSK\)](#)
 - [Configuring ePSKs](#)
 - [ePSK registration for WPA3 clients](#)
 - [Creating a Personal Wi-Fi ePSK](#)
- [RADIUS-based ePSK](#)

Overview

Enterprise Wi-Fi AP devices support up to 16 unique WLANs. Each of these WLANs can be configured as per the customer requirement and type of wireless station.

Configuring the WLAN parameters

To configure WLAN parameters, complete the following steps:

1. Navigate to **Configuration > Wi-Fi Profiles > WLANs** page.
2. Click **Add** and select **Enterprise Wi-Fi** from the **Type** drop-down list.

Following are the configurable parameters under the WLAN profile:

- [Basic](#)
- [Radius Server](#)
- [Guest Access](#)
 - [Internal Access Point](#)
 - [External Hotspot](#)
 - [cnMaestro](#)
- [Usage Limits](#)


- [Scheduled Access](#)
- [Access](#)
- [Passpoint](#)

Basic



[Table 22](#) lists configurable fields that are displayed in the **WLANs > Basic Settings** section.

Table 22 Basic parameters

Parameters	Description	Range	Default
WLAN > Basic Settings			
Enable	Enables a WLAN profile. Once enabled, a Beacon is broadcasted with the SSID and the corresponding parameters configured in a WLAN profile.	-	-
SSID	Unique network name that wireless stations scan and associate.	-	-
Mesh	<p>This parameter is required when a WDS connection is established with Enterprise Wi-Fi devices. This parameter supports the following options:</p> <ul style="list-style-type: none"> • Base: A WLAN profile configured with a mesh-base will operate as a normal AP. Its radio will beacon on startup so its SSID can be seen by radios configured as mesh-clients. • Client: A WLAN profile configured with mesh-client will scan all available channels on startup, looking for a mesh-base AP to connect. • Recovery: WLAN profile configured as mesh-recovery will broadcast a pre-configured SSID upon detection of mesh link failure after a successful connection. This needs to be exclusively configured on a mesh-base device. Meshclient will auto scan for mesh-recovery SSID upon failure of mesh link. • Off: Mesh support disabled on WLAN profile. 	-	Off (Access Profile Mode)
VLAN	Segregates wireless station traffic from AP traffic in the network. Wireless stations obtain an IP address from the subnet configured in the VLAN field of the WLAN profile.	1-4094	1
Security	<p>Determines key values that are encrypted based on the selected algorithm. Following security methods are supported:</p> <ul style="list-style-type: none"> • Open 	-	Open

Parameters	Description	Range	Default
	<p>This method is preferred when Layer 2 authentication is built into the network. With this configured on an Enterprise Wi-Fi AP device, any wireless station will be able to connect.</p> <ul style="list-style-type: none"> • OWE <p>This method ensures the communication between each pair of endpoints is protected from other endpoints.</p> <ul style="list-style-type: none"> • Osen <p>This method is extensively used when Passpoint 2.0 is enabled on Enterprise Wi-Fi AP devices. If Passpoint 2.0 is disabled, this security plays no role in wireless station association.</p> <ul style="list-style-type: none"> • >WPA2-Pre-Shared Keys <p>This mode is supported with AES and TKIP encryption. WPA-TKIP can be enabled from the CLI with the <code>allow-tkip</code> CLI option.</p> <ul style="list-style-type: none"> • WPA2 Enterprise <p>This security type uses 802.1x authentication to associate wireless stations. This is a centralized system of authentication methods.</p> <ul style="list-style-type: none"> • WPA2/WPA3 Pre-shared Keys <p>WPA3 comes with a transition mode where WPA2-only capable clients can connect to SSID. WPA2-only capable clients connect using the older PSK method while WPA3 capable clients connect using a more secure Simultaneous Authentication of Equals (SAE) method.</p> <ul style="list-style-type: none"> • WPA3 Pre-shared Keys <p>WPA3 replaces the Pre-Shared Key (PSK) exchange with SAE of Equals, which is more secure and provides forward-secrecy as well as resistance to offline dictionary attack.</p> <div>  <div> Note When you select WPA2/WPA3 Pre-shared Keys or WPA3 Pre-shared Keys, you can enable registration flow for WPA3 clients. </div> </div>		

Parameters	Description	Range	Default
	<p>To enable the registration flow, you must create an ePSK passphrase and follow the procedure for the clients to undergo the registration flow. For more information, see ePSK registration for WPA3 clients.</p> <ul style="list-style-type: none"> WPA3 Enterprise WPA3 also introduces Enterprise AES CCMP encryption. This level of security provides consistent cryptography and eliminates the mixing and matching of security protocols that are defined in the 802.11 standards. WPA3 Enterprise CNSA WPA3 also introduces a 192-bit cryptographic security suite. This level of security provides consistent cryptography and eliminates the mixing and matching of security protocols that are defined in the 802.11 standards. This security suite is aligned with the recommendations from the Commercial National Security Algorithm (CNSA) Suite and is commonly used in high-security Wi-Fi networks in government, defense, Finance, and industrial verticals. User Pre-shared keys The U-PSK (User-PSK) Authentication settings are only used in conjunction with XMS Cloud's EasyPass Onboarding Portals. The Cloud automatically configures this setting for an WLAN when you create an Onboarding portal and you assign that WLAN to the portal. Thus, you should not normally change this setting manually. Note that the User- PSK settings are only available on the WLAN profile. 		
Band	<p>Each SSID can be configured to be transmitted as per the deployment requirement. For a regular access profile, options are available to configure transmit mode of SSID:</p> <ul style="list-style-type: none"> 2.4 GHz 5 GHz 6 GHz 	-	all
Client Isolation	Enable this feature when there is a need for restriction of wireless station-to-station communication across the network or on an AP.		

Parameters	Description	Range	Default
	<div>  <div> <p>Note</p> <ul style="list-style-type: none"> For client isolation to work correctly, it is recommended that clients obtain their IP addresses through DHCP. You must manually update the default gateway addresses in the IP configuration of clients that are using static IP addresses. If the gateway MAC address changes due to hardware replacement or any other reason, you must restart the AP for the AP to learn the new gateway MAC address and to make sure the client isolation functions correctly. </div> </div> <p>The following options are available to configure based on requirement:</p> <ul style="list-style-type: none"> Disable <p>This option when selected disables the client isolation feature. i.e. any wireless station can communicate to other wireless stations.</p> Local <p>This options when selected enable the client isolation feature. This option prevents wireless station communications connected to the same AP.</p> Network Wide <p>This options when selected enable the client isolation feature. It prevents wireless stations communications connected to different AP deployed in the same L2 network.</p> <div>  <div> <p>Note</p> <ul style="list-style-type: none"> Network-wide mode is not supported when Redundancy Gateway protocol is used on deployment. In the Redundancy Gateway case, Network-wide static can be used to provide a list of Gateway MAC addresses. </div> </div> Network Wide Static 		




Parameters	Description	Range	Default
	<p>This option when configured enables client isolation feature across the network. Wireless stations can communicate only to statically added MAC list. Communication to rest other MAC addresses are blocked.</p> <div>  <div> Note <p>When Network Wide and Network Wide Static are selected, the user has the provision to add the whitelist MAC addresses to allow the communication. A maximum of 64 MAC addresses can be added.</p> </div> </div>		
cnMaestro Managed Roaming	Provision to enable centralized management of roaming for wireless clients through cnMaestro.	-	-
Hide SSID	This is the basic security mode of a Wi-Fi device. This parameter when enabled, will not broadcast SSID.	-	Disabled
Session Timeout	<p>This field applies to all wireless clients connected to the SSID. When a wireless station connects, a session timer is triggered. Once session time expires, the wireless station must undergo either re-authentication or re-association based on the state of the wireless station. By default, it is enabled.</p> <div>  <div> Note <p>Following priority takes precedence for the session timeout:</p> <ol style="list-style-type: none"> Configured from the RADIUS server Configured from the AP </div> </div>	60-604800	28800
Inactivity Timeout	<p>Inactivity timer triggers whenever there is no communication between Enterprise Wi-Fi AP device and wireless station associated to Enterprise Wi-Fi AP device. Once the timer reaches the configured Inactivity timeout value, APs send a de-authentication to that wireless station. By default, it is enabled.</p> <div>  <div> Note <p>Following priority takes precedence for the inactivity timeout:</p> <ol style="list-style-type: none"> Configured from the RADIUS server Configured from the AP </div> </div>	60-28800	1800

Figure 16 Basic parameters

WLANs > Add New

WLAN
AAA Servers
Guest Access
Access Control
Passpoint
ePSK

Basic Settings

SSID

☒ Enable

SSID* The SSID of this WLAN (up to 32 characters)

Mesh

Off Mesh Base/Client/Recovery mode

VLAN*

1 Default VLAN assigned to clients on this WLAN (1-4094)

Security

Open Set authentication and encryption type

Transition SSID

Configure the matching open/owe transition SSID

Band

☒ 2.4 GHz ☒ 5 GHz ☒ 6 GHz Define radio types (2.4 GHz, 5 GHz, 6 GHz) on which this WLAN should be supported

Client Isolation

Disable

When selected, it allows wireless clients connected to the same AP or different APs to communicate with each other in the same VLAN

☐ cnMaestro Managed Roaming
Enable centralized Guest Access Session management of roaming for wireless clients through cnMaestro

☐ Hide SSID Do not broadcast SSID in beacons

+ Advanced Settings

Save Close

Table 23 WLAN (Max clients) parameters

Number of clients	2.4 GHz	5 GHz	6 GHz	Concurrent
XV3-8	512	1024*	NA	1536
XE5-8	512	1024*	1024**	2560
XV2-2	512	512	NA	1024
XV2-2T0	512	512	NA	1024
XV2-2T1	512	512	NA	1024
XE3-4	512	512	512	1536
XE3-4TN	512	512	512	1536
XV2-21X	128	128	NA	256
XV2-23T	128	128	NA	256
XV2-22H	128	128	NA	256
e410/e430 and e510	256	256	NA	256
e600 and e700	512	512	NA	512

* Two 5 GHz radios are available in Single Band Simultaneous (SBS) mode.

** Two 6 GHz radios are available in XE5-8 platform.

Maximum wireless client

At present, the WLAN profile provides an option to configure the maximum wireless clients association limit. This configuration limits the maximum number of clients per SSID per radio. For example, if a user configures the maximum wireless client as 10, on a device capable of 2.4 GHz and 5 GHz radios, the total number of clients that can be associated is 10 across each radio. This has been enhanced in Release 6.5 to set the maximum clients limit per SSID irrespective of the number of radios to which SSID has been mapped.

Maximum clients per device

Most customers commonly use more than a single SSID. They prefer to set the maximum number of wireless clients connection per device, i.e. irrespective of the number of WLAN profiles and the number of radios, the maximum number of clients that can be associated is equivalent to the value configured for the parameter max-clients. This is a global configuration.

CLI configuration:

```
ap(config)# max-clients
0|<1-1536> '0' disables max client per device
```

Maximum clients per SSID

This option helps to limit the number of wireless clients connected to a WLAN profile (SSID) irrespective of the number of radios. This configuration is supported at the WLAN level. This can be enabled as follows:

CLI configuration:

```
ap(config)# wireless wlan 1
ap(config-wlan-1)# enforce-max-clients-per-ssid
```

Maximum clients per SSID per radio

This is the default configuration of the device. This configuration limits the maximum number of clients per SSID per radio. For example, if a user configures the maximum wireless client as 20, on a device capable of 2.4 GHz and 5 GHz radios, the total number of clients that can be associated is 20 across each radio. This configuration is supported at the WLAN level.

CLI configuration:

```
ap(config)# wireless wlan 1
ap(config-wlan-1)# max-associated-clients
<1-1536>
```

The default priority order can be:

1. Per device (Global limit)
2. Per SSID and (enforce at SSID level)
3. Per SSID per radio basis (present default option)

To keep backward compatibility with the existing deployments, the default option can be Per SSID per radio basis.

Opportunistic Wireless Encryption (OWE)

OWE is a Wi-Fi standard, which ensures that the communication between each pair of endpoints is protected from other endpoints. The OWE transition mode allows OWE-capable STAs to access the network in OWE authentication mode. The OWE transition mode is implemented as follows:

You must create two WLANs on an AP.

For example,

1. WLAN-1:
 open authentication
 owe-transition-ssid: Provides WLAN-2 owe security SSID
2. WLAN-2:
 owe authentication
 owe-transition-ssid: Provides WLAN-1 open security SSID

CLI configuration:

```
ap(config-wlan-1)# owe-transition-ssid
owe-transition-ssid : Configure the matching open/owe transition ssid
```



Note


The OWE transition mode SSIDs do not apply to 6 GHz radios.

Table 24 Advanced parameters

Parameters	Description	Range	Default
WLAN > Advanced			
VLAN Pooling	This parameter is required when a user requires to distribute clients across multiple subnets. Different modes of VLAN pooling is supported by Enterprise Wi-Fi AP devices, based on infrastructure available at the deployment site. Modes supported are as follows: <ul style="list-style-type: none"> • Disabled 	–	Disabled

Parameters	Description	Range	Default																														
	<p>This feature is disabled for this WLAN.</p> <ul style="list-style-type: none">• Radius Based <p>The user is expected to configure WPA2 Enterprise for this mode to support. During the association phase, AP obtains pool name from RADIUS transaction and based on the present distribution of wireless station across VLANs, AP selects appropriate VLAN and wireless station requests an IP address from the VLAN selected by Enterprise Wi-Fi AP device.</p> <ul style="list-style-type: none">• Static <p>For this mode to support, the user requires to configure VLAN Pool details available under Configure > Network > VLAN pool. During the association phase, AP obtains pool, and based on the present distribution of wireless station across VLANs, AP selects appropriate VLAN and wireless station requests an IPv4 address from the VLAN selected by the Enterprise Wi-Fi AP device.</p>																																
Max Clients	This specifies the maximum number of wireless stations that can be associated with a WLAN profile. This varies based on the Enterprise Wi-Fi AP device model number. Refer to Table 23 for more details.	1-512 (Refer Table 23)	256																														
UAPSD	<p>When enabled, Enterprise Wi-Fi AP devices support WMM Power Save / UAPSD. This is required where applications such as VOIP Calls, Live Video streaming are in use. This feature helps to prioritize traffic. Below is the default traffic priority followed by the Enterprise Wi-Fi AP device.</p> <table><tr><th>Priority</th><th>802.1D Priority (=UP)</th><th>802.1D Designation</th><th>Access Category</th><th>WMM Designation</th></tr><tr><td rowspan="7">lowest ↓ highest</td><td>1</td><td>BK</td><td rowspan="2">AC_BK</td><td rowspan="2">Background</td></tr><tr><td>2</td><td>-</td></tr><tr><td>0</td><td>BE</td><td rowspan="2">AC_BE</td><td rowspan="2">Best Effort</td></tr><tr><td>3</td><td>EE</td></tr><tr><td>4</td><td>CL</td><td rowspan="2">AC_VI</td><td rowspan="2">Video</td></tr><tr><td>5</td><td>VI</td></tr><tr><td>6</td><td>VO</td><td rowspan="2">AC_VO</td><td rowspan="2">Voice</td></tr><tr><td>7</td><td>NC</td></tr></table>	Priority	802.1D Priority (=UP)	802.1D Designation	Access Category	WMM Designation	lowest ↓ highest	1	BK	AC_BK	Background	2	-	0	BE	AC_BE	Best Effort	3	EE	4	CL	AC_VI	Video	5	VI	6	VO	AC_VO	Voice	7	NC	–	Disabled
Priority	802.1D Priority (=UP)	802.1D Designation	Access Category	WMM Designation																													
lowest ↓ highest	1	BK	AC_BK	Background																													
	2	-																															
	0	BE	AC_BE	Best Effort																													
	3	EE																															
	4	CL	AC_VI	Video																													
	5	VI																															
	6	VO	AC_VO	Voice																													
7	NC																																
QBSS	When enabled, appends QBSS IE in Management frames. This IE provides information on channel usage by AP, so that smart wireless stations can decide better AP for connectivity. Station count, Channel utilization, and Available admission capacity are the information available in this IE.	–	Disabled																														

Parameters	Description	Range	Default
DTIM interval	This parameter plays a key role when power save supported mobile stations are part of the infrastructure. This field when enabled controls the transmission of Broadcast and Multicast frames.	1-255	1
Monitored Host			
Host	This feature is required where there is an interrupted backbone network. Enterprise Wi-Fi AP device monitors the reachability of hostname/IP configured in this parameter and modifies the state of WLAN.	-	Disabled
Interval	The frequency of monitoring the network health based on the status of the keep-alive mechanism w.r.t configured monitored host.	60-3600 sec	300
Attempts	The number of packets in the keep-alive mechanism to determine the status.	1-20	1
DNS Logging Host	By enabling this feature, the Administrator can monitor the websites accessed by wireless stations connected to WLAN profile.	–	Disabled
Connection Logging Host	When enabled provides information of all IP connections accessed by a wireless station that is associated with WLAN and logs the connection data seamlessly onto an external syslog server.	–	Disabled
Band Steering	This feature when enabled steers wireless stations to connect to 5GHz. There are three modes supported by Enterprise Wi-Fi devices. The mode can be selected based on either deployment or wireless station type. Below is the order of modes, which forces the wireless station to connect to the 5 GHz band. <ul style="list-style-type: none"> • Low • Normal • Aggressive 	–	Disabled
Proxy ARP	Provision to avoid ARP flood in a wireless network. When enabled, AP responds to ARP requests for the wireless stations connected to that AP. This is for IPv4 infrastructure.	–	Enabled
Proxy ND	When enabled, AP responds to IPv6 Neighbor Discovery (ND) requests for the wireless stations connected to that AP.		
Unicast DHCP	Provision to transmit DHCP offer and ACK/NACK packets as Unicast packets to wireless stations.	–	Enabled

Parameters	Description	Range	Default
Insert DHCP Option 82	<p>When enabled, DHCP packets generated from wireless stations that are associated with APs are appended with Option 82 parameters. Option 82 provides a provision to append Circuit ID and Remote ID. Following parameters can be selected in both Circuit ID and Remote ID:</p> <ul style="list-style-type: none"> • Hostname • AP MAC • BSSID • SSID • VLAN ID • SITEID • Custom • All <div>  <div> Note <p>In case DHCP Option 82 is configured at the device-, WLAN profile-, and L3 interface-levels, the following priority order is considered:</p> <ol style="list-style-type: none"> 1. Device-level configuration 2. WLAN profile-level configuration 3. L3 interface-level configuration </div> </div>	–	Disabled
Tunnel Mode	This option is enabled when user traffic is tunneled to the DMZ network either using L2TP or L2GRE.	–	Disabled
Fast-Roaming Protocol	One of the important aspects to support voice applications on a Wi-Fi network (apart from QoS) is how quickly a client can move its connection from one AP to another. This should be less than 150 ms to avoid any call drop. This is easily achievable when the WPA2-PSK security mechanism is in use. However, in enterprise environments, there is a need for more robust security (the one provided by WPA2-Enterprise). With WPA2-Enterprise, the client exchanges multiple frames with the AAA server, and hence depending on the location of the AAA server the roaming time will be above 700 ms.	–	Disabled

Parameters	Description	Range	Default
	<p>Select any one of the following:</p> <ul style="list-style-type: none"> • OKC <p>This roaming method is a Cambium Networks proprietary solution to share the client authentication information with other Cambium Networks APs on the same network by sending encrypted information on wire on SSID VLAN. This information sharing does not require cnMaestro so even in cases where AP is not connected to cloud, the roaming will be seamless.</p> <ul style="list-style-type: none"> • 802.11r <p>Fast transition (FT) is an IEEE standard to permit continuous connectivity aboard wireless devices in motion, with fast and secure client transitions from one Basic Service Set (abbreviated BSS, and also known as a base station or more colloquially, an access point) to another, performed in a nearly seamless manner. The terms handoff and roaming are often used, although 802.11 transition is not a true handoff/roaming process in the cellular sense, where the process is coordinated by the base station and is generally uninterrupted.</p>		
RRM (802.11k)	<p>AP sends the SSID name of the neighbor APs (SSID configured on multiple APs) to 802.11k clients.</p> <p>The following parameter must be enabled:</p> <ul style="list-style-type: none"> • Enable RRM 	–	Disabled
802.11v	Provision to enable 802.11v BSS Transition Management.	–	Disabled
PMF (802.11w)	802.11w also termed as Protected Management Frames (PMF) Service, defines encryption for management frames. Unencrypted management frames make wireless connection vulnerable to DoS attacks as well as they cannot protect important information exchanged using management frames from eavesdroppers.	–	Optional
SA Query Retry Time	The legitimate 802.11w client must respond with a Security Association (SA) Query Response frame within a pre-defined amount of time (milliseconds) called the SA Query Retry time.	100-500	100ms
Association Comeback Time	This value is included in the Association Response as an Association Comeback Time information element. AP will deny association for the configured interval.	1-20	1 Sec

Figure 17 Advanced parameters

WLANs > Add New

WLAN

AAA Servers

Guest Access

Access Control

Passpoint

ePSK

Advanced Settings

Maximum Clients

127

Maximum number of clients assigned per Radio (1-512)

VLAN Pooling

Disabled

Configure VLAN Pooling

Session Timeout

28800

Session time in seconds (60 to 604800)

Inactivity Timeout

1800

Inactivity time in seconds (60 to 28800)

☐ Drop Multicast Traffic

Drop the send/receive of multicast traffic

☐ UAPSD

Enable WMM Power Save/UAPSD (for VoIP and streaming)

☐ QBSS

Append QBSS Load IE in management frame to improve AP selection

DTIM Interval

1

Configure Delivery Traffic Indication Message (1 – 255 beacon count)

Monitored Host

Host

IP Address or Hostname that should be reachable for this WLAN to be active

Interval

300

Duration in seconds (60-3600)

Attempts

5

Number of attempts to check the reachability of monitored host (1-20)

DNS Logging Host

Port

514

Syslog server where all client DNS requests will be logged

Connection Logging Host

Port

514

Syslog server where all client connection requests will be logged

Band Steering

Disable

Steer clients across all Bands.

☒ Proxy ARP

Respond to ARP requests automatically on behalf of clients

☐ Proxy ND

Respond to IPv6 Neighbor Discovery (ND) requests automatically on behalf of clients

☒ Unicast DHCP

Convert DHCP-OFFER and DHCP-ACK to unicast before forwarding to clients

☐ Insert DHCP Option 82

Enable DHCP Option 82

☐ Tunnel Mode

Enable tunnelling of WLAN traffic over configured tunnel

Fast Roaming Protocol

☐ OKC

☐ 802.11r

Configure roaming protocol (not applicable when authentication type is Open)

☒ RRM (802.11k)

Enable Radio Resource Measurements (802.11k)

☒ 802.11v

Enable 802.11v BSS Transition Management

Band steering also supports client load balancing based on the below CLI configuration:

```

ap(config)# wireless wlan 1
ap(config-wlan-1)# band-steer-load-balancing
client-counts : client counts for band steer to consider clients load
balancing
client-percentage : Client percentage for band steer to consider clients
load balancing

```

WLAN VLAN allowed list

This is an optional CLI to configure the allowed VLAN list upfront. It is needed in multiple VLAN scenarios such as Dynamic VLAN, ePSK-based VLAN, and RADIUS VLAN.

CLI configuration:

```

ap(config)# wireless wlan 1
ap(config-wlan-1)# vlans-allowed
{vlan_list} <e.g 1-10,15,100>
ap(config-wlan-1)# vlans-allowed 1-10

```

ICMPv6 Router advertisement (RA) unicast conversion

Convert ICMPv6 RA Multicast packets to Unicast for all stations. ICMPv6 RA unicast conversion is needed in multiple VLAN scenarios such as Dynamic VLAN, ePSK-based VLAN, and RADIUS-based VLANs.

This CLI configuration allows to configure the VLANs where ICMPv6 RA unicast conversion is needed.

CLI configuration:

```

ap(config)# wireless wlan 1
ap(config-wlan-1)# ipv6-router-advertisement-unicast
vlans : Configure vlans where IPV6 Router Advertisement unicast
conversion needed
ap(config-wlan-1)# ipv6-router-advertisement-unicast vlans
{vlan_list} <e.g 1-10,15,100>
ap(config-wlan-1)# ipv6-router-advertisement-unicast vlans 1-10

```

802.11k/v

802.11k

Radio Resource Measurement (RRM) defines and exposes radio and network information to facilitate the management and maintenance of a wireless network. 802.11k is intended to improve the way traffic is distributed within the network.

The client can request a neighbor report from the AP using the neighbor_report_req management message. The client may request neighbors with **matching** SSID or request for all neighbors in the vicinity. The AP

collects the neighbor information using proprietary methods and provides the list of neighbors to the client in the neighbor_report_rsp message.

802.11v

802.11v is deployed on the APs to govern the wireless networking transmission methods. It allows clients and APs to exchange information regarding the network topology, and RF environment. This facilitates the wireless devices to be RF-aware for participating in network-assisted power savings and network-assisted roaming methods.


The client may send solicited BSS Transition Management messages to AP before making roaming decisions. The idea is to identify the best APs to roam. The AP, after receiving the message from a client is expected to respond with the best APs in the vicinity to assist the client in roaming. The neighbor information is collected using proprietary methods.

RADIUS server

To configure a RADIUS server, complete the following steps:

1. Navigate to **Configuration > Wi-Fi Profiles WLAN** tab, select **Radius Server** tab and provide the details as given in [Table 25](#):

Table 25 RADIUS Server parameters

Parameters	Description	Range	Default
Authentication Server	<p>Provision to configure RADIUS Authentication server details such as Hostname/IPv4, Shared Secret, Port Number and Realm. A maximum of three RADIUS servers can be configured.</p> <div>Note<p>The Realm parameter can be left blank, unless you would like to use this server only for certain usernames where the network domain is included.</p><p>For example, in <username>@cambium.com or <domain-name>/<username>, the realms are @cambium.com and <domain-name>/, and this server will be selected only if the username has the appropriate realm.</p></div>	-	Disabled
Accounting Server	Provision to configure Accounting server details such as Hostname/IPv4, Shared Secret, Port Number. A maximum of three RADIUS servers can be configured.	-	Disabled
Timeout	This field indicates wait time period for a response from the AAA server.	1-30	3

Parameters	Description	Range	Default
Attempts	Parameter to configure many attempts that a device should send AAA request to server if no response is received within the configured timeout period.	1-3	1
Accounting Mode	<p>This field is enabled based on customer requirements. The accounting packet is transmitted based on the mode selected.</p> <ul style="list-style-type: none"> • Start-Stop Accounting packets are transmitted by AP to the AAA server when a wireless station is connected and then disconnects. • Start-Interim-Stop Accounting packets are transmitted by AP to the AAA server when a wireless station connects and then at regular intervals of configured Interim Update Interval and then when it disconnects. • None The accounting mode will be disabled. 	-	Disabled
Accounting Packet	When enabled, Accounting-On is sent for every client when connected.	-	Disabled
Sync Accounting Records	Provision to configure accounting records to be synced across neighboring APs.	-	-
Server Pool Mode	<p>Users can configure multiple Authorization and Accounting servers. Based on a number of wireless stations, the user can choose Failover mode.</p> <ul style="list-style-type: none"> • Load Balance—AP communicates with multiple servers and ensures that authorization and accounting are equally shared across configured servers. • Failover—AP selects the RADIUS server which is up and running based on the order of configuration. 	-	Failover
NAS-Identifier	This is a configurable parameter and is appended in the RADIUS request packet.	-	Hostname/ System Name
Dynamic Authorization	This option is required, where there is CoA request from AAA/RADIUS server.	-	Disabled

Parameters	Description	Range	Default
Dynamic VLAN	When enabled, AP honors the VLAN information provided in the RADIUS transaction. Wireless station requests IP address from the same VLAN learned through RADIUS.	-	Enabled
Called Station ID	<p>The following information can be communicated to the RADIUS server:</p> <ul style="list-style-type: none"> • AP-MAC • AP-MAC: SITE-NAME • AP-MAC: SSID • AP-MAC: SSID-SITE-NAME • AP-NAME • AP-NAME: SITE-NAME • AP-NAME: SSID • SITE-NAME • SSID • CUSTOM 	-	AP-MAC: SSID

Figure 18 The RADIUS Server parameters

WLANs > Add New

WLAN

AAA Servers
Guest Access
Access Control
Passpoint
ePSK

Warning: AAA Servers are configured separately for each WLAN.

Authentication Server

1. Host Secret Port* Realm

e.g. x.x.x.x/<url>
Show
1812

2. Host Secret Port* Realm

e.g. x.x.x.x/<url>
Show
1812

3. Host Secret Port* Realm

e.g. x.x.x.x/<url>
Show
1812

Timeout
3
Timeout in seconds for each request attempt (1-30)

Attempts
1
Number of attempts before giving up (1-3)

Accounting Server

1. Host Secret Port*

e.g. x.x.x.x/<url>
Show
1813

2. Host Secret Port*

e.g. x.x.x.x/<url>
Show
1813

3. Host Secret Port*

e.g. x.x.x.x/<url>
Show
1813

Timeout
3
Timeout in seconds for each request attempt (1-30)

Attempts
1
Number of attempts before giving up (1-3)

Accounting Mode
None
Configure accounting mode

☐ Accounting Packet Enable Accounting-On messages

☐ Sync Accounting Records Configure accounting records to be synced across neighboring AP's

Interim Update Interval
1800
Interval for RADIUS Interim-Accounting updates (10-65535 Seconds)

Advanced Settings

Server Pool Mode

☒ Load Balance Load balance requests equally among configured servers
☐ Failover Move down server list when earlier servers are unreachable

NAS-Identifier
AP-HOSTNAME
NAS-Identifier attribute for use in Request packets (defaults to system name)

☐ Dynamic Authorization Enable RADIUS dynamic authorization (COA, DM messages)

☒ Dynamic VLAN Enable RADIUS assigned VLANs

Called Station ID:
AP-MAC:SSID
Configure AP-MAC:SSID as Called-Station-Id in the RADIUS packet

Proxy Through Controller

cnMaestro On-Premises can act as a proxy server for a AAA request coming from Enterprise Wi-Fi Access Points. In this scenario, cnMaestro acts as Network Access Server (NAS) for the AAA server.

The AP sends AAA packets to cnMaestro On-Premises, and cnMaestro forwards them to the AAA server. When the Proxy Through Controller feature is enabled, CoA is supported other than AAA requests.

CLI configuration:

```
ap(config-wlan-1)# radius-server through-controller
```

Note: Applicable only with On-Premises controller

For activating Proxy Through Controller feature in cnMaestro On-Premises:

1. Go to **Administration > Settings**.
2. Enable **RADIUS Proxy** checkbox as shown in below figure.

Figure 19 RADIUS proxy



EAP-FAST support

EAP-FAST authentication occurs in two phases. In the first phase, EAP-FAST employs the TLS handshake to provide an authenticated key exchange and to establish a protected tunnel. Once the tunnel is established the second phase begins with the peer and server engaging in further conversations to establish the required authentication and authorization policies.

Guest Access

Internal Access Point

Below table lists configurable fields that are displayed in the **WLANs > Guest Access > Internal Access Point** page.

Table 26 Internal Access Point parameters

Parameters	Description	Range	Default
WLAN > Guest Access > Internal Access Point			

Parameters	Description	Range	Default
Enable	Enables the Guest Access feature.	-	Disabled
Access Policy	<p>There are four types of access types provided for the user:</p> <ol style="list-style-type: none"> 1. Clickthrough <p>This mode allows the users to get access data without any authentication mechanism. User can access the internet as soon as he is connected and accepts Terms and Conditions</p> 2. RADIUS <p>This mode when selected, the user has to provide a username and password, which is then redirected to the RADIUS server for authentication. If successful, the user is provided with data access.</p> 3. Local Guest Account <p>Users must configure username and password on the device, which has to be provided on the redirection page for successful authentication and data access.</p> 	-	Clickthrough
Redirect Mode	<p>This option helps the user to configure the HTTP or HTTPS mode of redirection URL.</p> <ol style="list-style-type: none"> 1. HTTP <p>AP sends an HTTP POSTURL to the associated client, in the <code>http://<Pre-defined-URL></code> format.</p> 2. HTTPS <p>AP sends HTTPS POSTURL to the success associated client, in the <code>https://<Pre-defined-URL></code> format.</p> 	-	HTTP
Redirect Hostname	Users can configure a friendly hostname, which is added to the DNS server and is resolvable to Enterprise Wi-Fi AP IP address. This parameter once configured will be replaced with an IP address in the redirection URL provided to wireless stations.	-	-

Parameters	Description	Range	Default
Title	Users can configure a Title to the splash page. Configured text in this parameter will be displayed on the redirection page. This text is usually Bold.	Up to 255 characters	Welcome To Cambium Powered Hotspot
Contents	Users can configure the contents of the Splash page using this field. Displays the text configured under the Title section of the redirection page.	Up to 255 characters	Enter username and password to get Web Access
Terms	Splash page displays the text configured when the user accepts the Terms and Agreement.	Up to 255 characters	-
Logo	Displays the logo image updated in URL http (s)://<ipaddress>/logo.png. Either PNG or JPEG format of the logo is supported.	-	-
Background Image	Displays the background image updated in URL http (s)://<ipaddress>/backgroundimage.png. Either PNG or JPEG format of the logo is supported.	-	-
Success Action	<p>Provision to configure redirection URL after successful login to captive portal services. Users can configure three modes of redirection URL:</p> <ol style="list-style-type: none"> 1. Internal Logout Page After successful login, the wireless client is redirected to the logout page hosted on AP. 2. Redirect user to External URL Here users will be redirected to the URL which is configured on the device in Redirection URL configurable parameter. 3. Redirect user to Original URL Here users will be redirected to the URL that is accessed by the user before successful captive portal authentication. 	-	Internal Logout page
Redirect user to External URL	<p>Provision to configure re-direction URL after successful login and additional information of AP and wireless station information can be appended in the URL.</p> <ul style="list-style-type: none"> • Prefix Query Strings in Redirect URL 	-	-

Parameters	Description	Range	Default
	<p>This option is selected by default. The following information is appended in the redirection URL:</p> <ul style="list-style-type: none"> • SSID • AP MAC • NAS ID • AP IP • Client MAC • Redirection URL • Users can provide either HTTP or HTTPS URL 		
Redirection user to Original URL	<p>Users will be redirected to the URL that is accessed by the user before successful captive portal authentication. There are additional parameter Prefix Query Strings in Redirection URL that is enabled by default and details given below:</p> <ul style="list-style-type: none"> • Prefix Query Strings in Redirect URL <p>This option is selected by default. The following information is appended in the redirection URL:</p> <ul style="list-style-type: none"> • SSID • AP MAC • NAS ID 	-	-
Success message	Provision to configure the text to display upon successful Guest Access authentication. This is applicable only when Success Action mode is Internal Logout Page.	-	-
Redirect	<ul style="list-style-type: none"> • If enabled, only HTTP URLs will be redirected to the Guest Access login page. • If disabled, both HTTP and HTTPS URLs will be redirected to the Guest Access login page. 	-	Enabled
Redirect User Page	IPv4 address configured in this field is used as logout URL for Guest Access sessions.	-	1.1.1.1
Proxy Redirection Port	The proxy port can be configured with which proxy server is enabled. This allows URLs accessed with proxy	1 - 65535	-



Parameters	Description	Range	Default
	port to be redirected to the login page.		
Session Timeout	<p>This is the duration of time, the client will be allowed to access the internet if quota persists, after which AP sends de-authentication. The wireless station has to undergo Guest Access authentication after session timeout.</p> <div>  <div> Note Following priority takes precedence for the session timeout: <ol style="list-style-type: none"> Configured from the RADIUS server Configured from the AP </div> </div>	60 - 2592000	28800
Inactivity Timeout	<p>Provision to configure timeout period to disconnect wireless stations that are associated but have no data traffic. AP starts a timer when there is no data received from a wireless station and disconnects when the timer reaches zero.</p> <div>  <div> Note Following priority takes precedence for the inactivity timeout: <ol style="list-style-type: none"> Configured from the RADIUS server Configured from the AP </div> </div>	60 - 2592000	1800
MAC Authentication Fallback	It is a mechanism in which wireless stations will be redirected to the Guest Access login page after any supported type of MAC address authentication fails.	-	Disabled
Whitelist	Provision to configure either IPv4 or URLs to bypass traffic, therefor user can access those IPs or URLs without Guest Access authentication.	-	-

Figure 20 The Internal Access Point parameters

The screenshot displays the 'WLANs > Add New' configuration page. The left sidebar shows a navigation menu with 'WLAN' selected. The main content area is titled 'WLAN' and contains several sections:

- Basic Settings:** Includes 'Enable' (checked), 'Portal Mode' (Internal Access Point selected), and 'Access Policy' (Clickthrough selected).
- Access Policy:** Details for the selected policy, including 'Access Policy' (Clickthrough), 'AP Server Protocol' (HTTP selected), and 'Redirect Hostname'.
- Title:** A text field for the title of the splash page.
- Contents:** A text area for the main content of the splash page.
- Terms:** A text area for the terms and conditions displayed in the splash page.
- Logo:** A text field for the logo to be displayed on the splash page.
- Background Image:** A text field for the background image to be displayed on the splash page.
- Success Action:** Includes 'Internal Logout Page' (selected), 'Redirect User to External URL', and 'Redirect User to Original URL'.
- Advanced Settings:** Includes 'Redirect' (checked), 'Redirect User Page' (1000), 'Redirection Port' (8080), 'Session Timeout' (3000), 'Inactivity Timeout' (300), 'MAC Authentication Fallback' (unchecked), and 'Extend Interface'.
- Pre-Login Allowed Domains:** A table with columns for 'IP Address / Domain Name' and 'Delete'.
- Captive Portal Bypass User Agent:** A table with columns for 'Index', 'User Agent String', 'HTTP Code', 'HTML Reply', and 'Delete'.

External Hotspot

Below table lists the configurable fields that are displayed in the **WLANs > Guest Access > External Hotspot** tab.

Table 27 External Hotspot parameters

Parameters	Description	Range	Default
WLAN > Guest Access > External Hotspot			
Access Policy	<p>There are four types of access types provided for the end user:</p> <ol style="list-style-type: none"> Clickthrough <p>This mode allows users to get access data without any authentication mechanism. The user can access the internet as soon as he is connected and accepts the Terms and Conditions.</p>	–	Clickthrough

Parameters	Description	Range	Default
	<p>2. RADIUS</p> <p>The user has to provide a username and password, which is then redirected to a RADIUS server for authentication. If successful, the user is provided with data access.</p> <p>3. Local Guest Account</p> <p>The user has to configure username and password on the device, which has to be provided on the redirection page for successful authentication and data access.</p>		
Redirect Mode	<p>Provision to configure the HTTP or HTTPS mode of redirection URL.</p> <p>1. HTTP</p> <p>AP sends an HTTP POSTURL to the associated client, in the <code>http://<Pre-defined-URL></code> format.</p> <p>2. HTTPS</p> <p>AP sends an HTTPS POSTURL to the associated client, in the <code>http://<Pre-defined-URL></code> format.</p>	–	HTTP
Redirect Hostname	Users can configure a friendly hostname, which is added to the DNS server and is resolvable to Enterprise Wi-Fi AP IP address. This parameter once configured will be replaced with an IP address in the redirection URL provided to wireless stations.	-	-
External Page URL	Users can configure a landing/login page that is posted to wireless stations that are not Guest Access authenticated.	–	–
External Portal Post Through cnMaestro	This is required when HTTPS is only supported by an external guest access portal. This option when enabled minimizes certification. The certificate is required to install only in cnMaestro On-Premises.	–	Disabled
External Portal Type	<p>Enterprise Wi-Fi AP products are supported by standard mode configuration.</p> <ul style="list-style-type: none"> • Standard 	–	Standard

Parameters	Description	Range	Default
	This mode is selected, for all third-party vendors whose Guest Access services are certified and integrated with Enterprise Wi-Fi AP products.		
Success Action	<p>Provision to configure redirection URL after successful login to captive portal services. User can configure three modes of redirection URL:</p> <ol style="list-style-type: none"> 1. Internal Logout Page After successful login, the wireless client is redirected to the logout page hosted on AP. 2. Redirect user to External URL Here users will be redirected to the URL which is configured on a device in Redirection URL configurable parameter. 3. Redirect user to Original URL Here users will be redirected to a URL that is accessed by the user before successful captive portal authentication. 	–	Internal Logout Page
Redirect user to External URL	<p>Provision to configure re-direction URL after successful login and additional information of AP and wireless station information can be appended in the URL.</p> <ul style="list-style-type: none"> • Prefix Query Strings in Redirect URL This option is selected by default. The following information is appended in the redirection URL: <ul style="list-style-type: none"> ◦ SSID ◦ AP MAC ◦ NAS ID ◦ AP IP ◦ Client MAC ◦ RedirectionURL ◦ Users can provide either HTTP or HTTPS URLs. 	–	–

Parameters	Description	Range	Default
Redirection user to Original URL	<p>Users will be redirected to the URL that is accessed by the user before successful captive portal authentication. There are additional parameter Prefix Query Strings in Redirection URL that is enabled by default and details given below:</p> <ul style="list-style-type: none"> Prefix Query Strings in Redirect URL <p>This option is selected by default. The following information is appended in the redirection URL:</p> <ul style="list-style-type: none"> SSID AP MAC NAS ID AP IP Client MAC 	–	–
Success message	Provision to configure the text to display upon successful Guest Access authentication. This is applicable only when Success Action mode is Internal Logout Page.	–	–
Redirection URL Query String	<p>The following information is appended in the redirection URL, if Prefix Query Strings in Redirect URL is enabled.</p> <ul style="list-style-type: none"> Client IP RSSI AP Location 	-	Disabled
Redirect	<ul style="list-style-type: none"> If enabled, only HTTP URLs will be redirected to the Guest Access login page. If disabled, both HTTP and HTTPs URLs will be redirected to the Guest Access login page. 	–	Enabled
Redirect User Page	The IP address configured in this field is used as logout/disconnect/redirect to captive portal URL for Guest Access sessions. The IP address configured should not be reachable to the internet.	–	1.1.1.1
Proxy Redirection Port	The proxy port can be configured with which proxy server is enabled. This allows URLs accessed with proxy port to be redirected to the login page.	1 - 65535	–



Parameters	Description	Range	Default
Session Timeout	<p>This is the duration of time, the client will be allowed to access the internet if quota persists, after which AP sends de-authentication. The wireless station has to undergo Guest Access authentication after session timeout.</p> <div>  <div> <p>Note</p> <p>Following priority takes precedence for the session timeout:</p> <ol style="list-style-type: none"> Configured from the RADIUS server Configured from the AP </div> </div>	60 - 2592000	28800
Inactivity Timeout	<p>Provision to configure timeout period to disconnect wireless stations that are associated but have no data traffic. AP starts a timer when there is no data received from a wireless station and disconnects when the timer reaches zero.</p> <div>  <div> <p>Note</p> <p>Following priority takes precedence for the inactivity timeout:</p> <ol style="list-style-type: none"> Configured from the RADIUS server Configured from the AP </div> </div>	60 - 2592000	1800
MAC Authentication Fallback	It is a mechanism in which wireless stations will be redirected to the Guest Access login page after any supported type of MAC address authentication failures.	–	Disabled
Extend Interface	Provision to support the Guest Access on the Ethernet interface.	–	Disabled

Figure 21 External Hotspot parameters

The screenshot displays the configuration interface for a new WLAN profile, specifically the 'Guest Access' tab under 'cnMaestro'. The interface is divided into several sections:

- Basic Settings:** Includes options to 'Enable' the profile, select the 'Portal Mode' (Internal Access Point, External Hotspot, or cnMaestro), and choose an 'Access Policy' (Clickthrough, RADIUS, LDAP, or Local Guest Account). It also allows selecting an 'AP Server Protocol' (HTTP or HTTPS) and setting a 'Redirect Hostname'.
- Advanced Settings:** Contains options for 'Success Action' (Internal Logout Page, Redirect User to External URL, or Redirect User to Original URL), 'Redirect' settings (HTTP-only), and 'Pre-Login Allowed Domains'.
- Pre-Login Allowed Domains:** A table for managing domains that are allowed to bypass the captive portal.
- Captive Portal Bypass User Agent:** A table for managing user agents that are allowed to bypass the captive portal.

cnMaestro

The following table lists configurable fields that are displayed in the **WLANs > Guest Access > cnMaestro** page:

Table 28 The cnMaestro parameters

Parameters	Description	Range	Default
WLAN > Guest Access > cnMaestro			
Guest Portal Name	Provision to configure the name of the Guest Access profile which is hosted on CnMaestro.	—	—
Redirect	<ul style="list-style-type: none"> If enabled, only HTTP URLs will be redirected to the Guest Access login page. If disabled, both HTTP and HTTPS URLs will be redirected to Guest Access login page. 	—	Enabled
Redirect User Page	The IP address configured in this field is used as a logout URL for Guest Access sessions. The IP address configured should be not	—	1.1.1.1


Parameters	Description	Range	Default
	reachable to the internet.		
Proxy Redirection Port	The proxy port can be configured with which proxy server is enabled. This allows URLs accessed with proxy port to be redirected to the login page.	1 - 65535	–
Inactivity Timeout	<p>Provision to configure timeout period to disconnect wireless stations that are associated but have no data traffic. AP starts a timer when there is no data received from a wireless station and disconnects when the timer reaches zero.</p> <div>  <div> Note Following priority takes precedence for the inactivity timeout: <ol style="list-style-type: none"> Configured from the RADIUS server Configured from the AP </div> </div>	60 - 2592000	1800
Whitelist	Provision to configure either IPs or URLs to bypass traffic, such that user can access those IPs or URLs without Guest Access authentication.	–	–

Figure 22 cnMaestro parameters

The screenshot displays the 'WLANs > Configuration' page in the cnMaestro interface. The left sidebar shows a navigation menu with options: WLAN, AAA Servers, Guest Access (selected), Access Control, Passpoint, and ePSK. The main content area is titled 'Guest Access' and contains several sections:

- Basic Settings:** Includes an 'Enable' checkbox, 'Portal Mode' (Internal Access Point, External Hotspot, cnMaestro), and 'Portal Name' (set to None).
- Advanced Settings:** Includes a 'Redirect' section with 'HTTP-only' checked, 'Redirect User Page' (1111), 'Redirection Port' (1 to 65535), 'Inactivity Timeout' (1800), 'MAC Authentication Fallback' (unchecked), and 'Extend Interface'.
- Pre-Login Allowed Domains:** A table with columns 'IP Address / Domain Name' and 'Delete'. It currently shows 'No IP Address or Domain Name Available'.
- Captive Portal Bypass User Agent:** A table with columns 'Index', 'User Agent String', 'HTTP Code', 'HTML Reply', and 'Delete'. It currently shows 'No User Agent rule available'.

Usage Limits

Below table lists configurable fields that are displayed in the **WLANs > Access Control > Usage Limits** section.

Table 29 Usage Limits parameters

Parameters	Description	Range	Default
Rate Limit per Client	Provision to limit throughput per client. Default allowed throughput per client is unlimited. i.e., maximum allowed by 802.11 protocols. The traffic from/to each client on an SSID can be rate-limited in either direction by configuring the client rate limit available in usage limits inside the WLAN Configuration. This is useful in deployments like public hotspots where the backhaul is limited and the network administrator would like to ensure that one client does not monopolize all available bandwidth.	–	0 [Unlimited]

Parameters	Description	Range	Default
Rate Limit per WLAN	Provision to limit throughput across WLAN irrespective of a number of associated wireless stations to WLAN. All upstream/downstream traffic on an SSID (aggregated across all wireless clients) can be rate-limited in either direction by configuring usage limits inside the WLAN configuration section of the GUI. This is useful in cases where multiple SSIDs are being used and say one is for corporate use, and another for guests. The network administrator can ensure that the guest VLAN traffic is always throttled, so it will not affect the corporate WLAN.	–	0 [Unlimited]


Figure 23 The Usage Limits parameters

The screenshot shows the 'WLANs > Add New' configuration page. On the left is a sidebar menu with options: WLAN, AAA Servers, Guest Access, Access Control (highlighted in blue), Passpoint, and ePSK. The main content area is titled 'Usage Limits' and contains two expandable sections. The first section, 'Rate Limit per Client', is expanded and shows input fields for 'Upstream' and 'Downstream' rates, both set to '0' Kbps. The second section, 'Rate Limit for WLAN', is also expanded and shows input fields for 'Upstream' and 'Downstream' rates, both set to '0' Kbps.

Scheduled Access

Below table lists configurable fields that are displayed in the **WLANs > Access Control > Scheduled Access** section.

Table 30 The Scheduled Access parameters

Parameters	Description	Range	Default
Scheduled Access	<p>Provision to configure the availability of Wi-Fi services for a selected time duration. Enterprise Wi-Fi AP has the capability of configuring the availability of Wi-Fi services on all days or a specific day (s) of a week. The time format is in Hours.</p> <div>  <div>Note</div> </div>	00:00 Hrs. - 23:59 Hrs.	Disabled

Parameters	Description	Range	Default
	From release version 6.3 onwards, users are allowed to configure up to a maximum of 12 scheduled access rules per day on a particular WLAN instead of one rule per day.		

Figure 24 The Scheduled Access parameters

WLANs > Add New

WLAN	Scheduled Access Sunday <input type="text"/> Start Time (HH:MM) <input type="text"/> End Time (HH:MM) Monday <input type="text"/> Start Time (HH:MM) <input type="text"/> End Time (HH:MM) Tuesday <input type="text"/> Start Time (HH:MM) <input type="text"/> End Time (HH:MM) Wednesday <input type="text"/> Start Time (HH:MM) <input type="text"/> End Time (HH:MM) Thursday <input type="text"/> Start Time (HH:MM) <input type="text"/> End Time (HH:MM) Friday <input type="text"/> Start Time (HH:MM) <input type="text"/> End Time (HH:MM) Saturday <input type="text"/> Start Time (HH:MM) <input type="text"/> End Time (HH:MM)
AAA Servers	
Guest Access	
Access Control	
Passpoint	
ePSK	

CLI Configuration:

```

ap(config)# wireless wlan 1
ap(config-wlan-1)# scheduled-access
all : all
friday : friday
monday : monday
saturday : saturday
sunday : sunday
thursday : thursday
tuesday : tuesday
wednesday : wednesday
weekday : weekday
weekend : weekend
ap(config-wlan-1)# scheduled-access all
Time period in HH:MM-HH:MM,HH:MM-HH:MM format

```

Access

Below table lists configurable fields that are displayed in the **WLANs > Access Control** tab.

Table 31 *The Access parameters*

Parameters	Description	Range	Default
DNS-ACL			
Precedence	Provision to configure index of ACL rule. Packets are validated and processed based on the Precedence value configured.	-	1
Action	Provision to configure whether to allow or deny traffic.	-	Deny
Domain	Provision to configure domain names and rules are applied based on Action configured.	-	-
MAC Authentication			
MAC Authentication Policy	<p>Enterprise Wi-Fi AP supports multiple methods of MAC authentication. Following are the details of each mode:</p> <ol style="list-style-type: none">Permit Wireless station MAC addresses listed will be allowed to associate to AP.Deny When the user configures a MAC address, those wireless stations shall be denied to associate and the non-listed MAC address will be allowed.RADIUS For every wireless authentication, AP sends a RADIUS request and if RADIUS acceptance is received, then the wireless station is allowed to associate. In case authentication fails, you can enable AP to assign the default WLAN VLAN to the clients. For this, you must configure the <code>failed-allow-traffic</code> CLI command. For more information, see Fallback to WLAN VLAN when RADIUS-based MAC authentication fails.cnMaestro This option is preferable when the administrator prefers a centralized MAC authentication policy. For every wireless authentication, AP a sends query to cnMaestro if it is allowed or disallowed to connect. Based on the configuration, wireless stations are either allowed or denied.	-	Deny

To configure **DNS ACL**:

1. Select **Precedence** from the drop-down list.
2. Select type of action from **Action** drop-down list.
3. Enter a domain name in the **Domain** textbox.
4. Click **Save**.

To configure **MAC Authentication**:

1. Select **MAC Authentication Policy** from the drop-down list.
2. Enter **MAC** in the textbox.
3. Enter **Description** in the textbox.
4. Click **Save**.

Figure 25 The Access parameters

WLANs > Add New

WLAN

AAA Servers

Guest Access

Access Control

Passpoint

ePSK

Access Control Lists

Policy Based ACL

① Policy Based ACLs are supported only by 6.x firmware. These are defined under Wi-Fi Profiles > Access Control Policies.

☒ Enable Access Control

Access Control Policy

None ▾

Legacy ACL

① Legacy ACLs are supported by both 4.x and 6.x firmware. For 6.x APs Policy Based ACLs are recommended.

[Add New](#)

Precedence...	Policy	Direction	Type	Rule	Description	Edit	Delete
No Rule Available							

MAC Authentication

Policy

☒ Deny ☐ Allow ☐ RADIUS ☐ cnMaestro

[Add New](#)

MAC	Description	Delete
No Rule Available		

DNS ACL

[Add New](#)

Precedence...	Policy	Domain	Edit	De
No Rule Available				

Sample DNS-ACL configuration

If any user wants to block Facebook or Youtube traffic and allow the rest of the traffic, the configuration is shown in below figure:

Figure 26 Sample DNS-ACL configuration

WLANs > Ent_Access_Profile_6GHz														
<div>Configuration Devices</div>														
WLAN	<div>DNS ACL</div> <table> <tr> <th>Precedence</th><th>Policy</th><th>Domain</th></tr> <tr> <td>1</td><td>deny</td><td>*facebook.com</td></tr> <tr> <td>2</td><td>deny</td><td>*youtbe.com</td></tr> <tr> <td>256</td><td>permit</td><td>*,*</td></tr> </table>		Precedence	Policy	Domain	1	deny	*facebook.com	2	deny	*youtbe.com	256	permit	*,*
Precedence	Policy	Domain												
1	deny	*facebook.com												
2	deny	*youtbe.com												
256	permit	*,*												
AAA Servers														
Guest Access														
Access Control														
Passpoint														
ePSK														

Fallback to WLAN VLAN when RADIUS-based MAC authentication fails

When a client passes RADIUS-based MAC authentication, the RADIUS server assigns the configured VLAN. However, if clients fail the authentication, you can configure the AP to assign the default WLAN VLAN. This enables the AP to allow limited access to clients, or redirects the clients to a captive portal page, that are not available in the RADIUS MAC authentication list. Once the captive portal authentication is successful, the RADIUS server dynamically disconnects the client and assigns the RADIUS VLAN when the clients try to connect later.

To assign the default WLAN VLAN to such clients, you must include the `mac-authentication radius failed-allow-traffic` CLI command in the **AP Groups > User Overrides** section in cnMaestro.

This feature is only available for RADIUS-based MAC authentication. The use case for this feature is to provide limited access to clients not included in the approved RADIUS MAC authentication list, such as granting access to a walled garden, the internet, or redirecting the clients to go through the captive portal authentication.

Figure 27 failed-allow-traffic in RADIUS-based MAC authentication

AP Groups > Add New	
Basic	User-Defined Overrides Advanced configuration settings entered below will be applied on top of the AP Group settings sent to the device. This allows you to apply configuration not supported in the previous screens. If there are conflicts, the below settings will take precedence. The format used is the same as a configuration file exported from the device via its web UI or the "View Device Configuration" link in the device level configuration page.
Management	
Radio	
Network	<div>Variables and Macros</div> <p>Settings entered are not validated or error-checked (However, dollar (\$), period (.) or space characters are not allowed in a variable name and it should not be more than 64 characters long), and they may overwrite configuration made in previous screens, so please use them with caution. You are responsible for ensuring the resulting AP Group is valid and safe to use.</p>
Security	
Access Control	
Services	
User-Defined Overrides	<pre>! wireless wlan-1 mac-authentication radius failed-allow-traffic !</pre>

Passpoint

Below table lists configurable fields that are displayed in the **WLANs > Passpoint** tab.

Table 32 Passpoint parameters

Parameters	Description	Range	Default
Passpoint parameters			
Enable	Passpoint (Release 2) enables secure hotspot network access, online sign-up, and policy provisioning.	–	Disabled
DGAF	Downstream Group Addressed Forwarding when enabled the WLAN does not transmit any multicast and broadcast packets.	–	Disabled
ANQP Domain ID	ANQP domain identifier is included when the HS 2.0 indication element is in Beacon and Probe Response frames.	0-65535	0
Comeback Delay	Comeback Delay in milliseconds.	100-2000	0
Access Network Type	The configured Access Network Type is advertised to STAs. Following are the different network types supported: <ul style="list-style-type: none"> • Private • Chargeable Public • Emergency Services • Free Public • Personal Device • Private with Guest • Test • Wildcard 	–	Private
ASRA	This indicates that the network requires a further step for access.	–	Disabled
Internet	The network provides connectivity to the Internet if not specified.	–	Disabled
HESSID	Configures the desired specific HESSID network identifier or the wildcard network identifier.	–	–
Venue Info	Configure venue group and venue type.	–	–
Roaming Consortium	The roaming consortium and/or SSP whose security credentials can be used to authenticate with the AP.	–	–
ANQP Elements	Select any one of the following: <ul style="list-style-type: none"> • 3GPP Cellular Network Information • Connection Capability • Domain Name List • Icons • IP Address Type information • NAI Realm List 	–	–

Parameters	Description	Range	Default
	<ul style="list-style-type: none"> • Network Authentication Type • Operating Class Indication • Operator Friendly Names • OSU Provider List • Venue Name Information • WAN Metrics 		

Figure 28 Passpoint parameters

WLANs > Add New

WLAN

AAA Servers

Guest Access

Access Control

Passpoint

ePSK

Basic Settings

☐ Enable Passpoint (Release 2) enables a secure hotspot network access, online sign up and Policy Provisioning

☐ DGAF
Downstream Group Addressed Forwarding. When enabled the WLAN doesn't transmit any multicast and broadcast packets

ANQP Domain ID
0
ANQP domain identifier (0-65535) included when the HS 2.0 Indication element is in Beacon and Probe Response frames

Comeback Delay
0
Comeback delay in milliseconds. Supported range is 100-2000 ms, use 0 to disable

Access Network Type
Private The configured Access Network Type is advertised to STAs.

☐ ASRA Additional Step Required for Access, indicate that the network requires a further step for access

☐ Internet The network provides connectivity to the Internet, otherwise unspecified

HESSID
Configure the desired specific HESSID network identifier or the wildcard network identifier

Venue Group
-- select -- Configure Venue group and Venue type

Venue Type
-- select --

☒ **Roaming Consortium**
The roaming consortium and/or SSP whose security credentials can be used to authenticate with the AP

[Add New](#)

Roaming Consortium
No Entries

ANQP (Access Network Query Protocol)

☒ 3GPP Cellular Network Information

☒ Connection Capability

☒ Domain Names

☒ NAI (Network Access Identifier) Realm List

☒ Operator Friendly Names

☒ IP Address Type Information

☒ Network Authentication

☒ Operating Class Indication

☒ Venue Name Information

☒ WAN Metrics

RADIUS attributes

The table below shows the RADIUS attributes describes their interpretation.

Table 33 Radius attributes parameters

Type	Attribute Name	Attribute Number	Purpose
Standard	Acct-Interim-Interval	85	Specifies the interval between accounting interim updates

Type	Attribute Name	Attribute Number	Purpose
Standard	Acct-Session-Id	44	Session identification (RFC 5176)
Standard	Calling-Station-Id	31	Session identification (RFC 5176)
Standard	Class	25	Accounting classification
Standard	Event-Timestamp	55	Replay protection (RFC 5176)
Standard	Filter-ID	11	<ul style="list-style-type: none"> Assign station to a user group Re-assign station to a different user group (RFC 5176)
Standard	Framed-IP-Address	8	Session identification (RFC 5176)
Standard	Idle-Timeout	28	Specifies the amount of time a station may remain idle before its session is terminated
Standard	NAS-IP-Address	4	NAS identification (RFC 5176)
Standard	NAS-Identifier	32	NAS identification (RFC 5176)
Standard	Session-Timeout	27	Specifies the interval at which session is terminated
Standard	Termination-Action	29	Specifies the action to take when the session is terminated
Standard	Tunnel-Type	64	Dynamic VLAN assignment (1 of 3 required), should be set to VLAN (Integer = 13)
Standard	Tunnel-Medium-Type	65	Dynamic VLAN assignment (2 of 3 required), should be set to 802 (Integer = 6)
Standard	Tunnel-Private-Group-ID	81	Dynamic VLAN assignment (3 of 3 required), should be set to the VLAN ID or name
Standard	User-Name	1	<ul style="list-style-type: none"> Station username update Session identification (RFC 5176)
Microsoft Vendor-Specific	MS-MPPE-Send-Key	16	Session key distribution
Microsoft Vendor-Specific	MS-MPPE-Recv-Key	17	Session key distribution
Cambium	Cambium-Vlan-	157	Radius based VLAN pool

Type	Attribute Name	Attribute Number	Purpose
Vendor-Specific	Pool-Id		
Nas Port ID	NAS-Port-Id	87	NAS identification (RFC 5176)

Enterprise PSK (ePSK)

By using the ePSK feature, users can configure and support individual PSKs for different clients. This feature can be configured under a given WLAN configuration in cnMaestro UI. For on devices, only CLI support is available.

This feature also supports individual VLAN assignments for a given key which helps to put client traffic on different VLANs for limiting broadcast traffic.



Note:

- Maximum key limit for cnMaestro Essentials: 300 per account
- Maximum key limit for cnMaestro X: 2000 per WLAN and 50000 per account

Configuring ePSKs

To create an ePSK, complete the following steps:

1. Navigate to **Configuration > Wi-Fi Profiles**.
2. Select **WLAN** tab and click **Add**.
3. Select **Enterprise Wi-Fi** from the **Type** drop-down list and enter details in the **Basic Information** section.
4. In the **Basic Settings** section, ensure the **WPA2 Pre-Shared Keys** option is selected in the **Security** drop-down list.
5. Click **Save**.
6. Click the **ePSK** tab and select the **Local** option in the **Mode** field.
7. Select the type of **Passphrase Strength** as one of the following options:
 - **Easy**—Supports a maximum of eight alphanumeric characters
 - **Strong**—Supports a maximum of 16 alphanumeric and special characters
 - **Number**—Supports a maximum of eight integers
8. Click **Add New**.

The **Add ePSK** window is displayed.

9. Select **Mode** type as one of the following options and configure the corresponding parameters:

- **Single mode**—Only one entry is created in this mode

Add ePSK

Mode
☒ Single ☐ Bulk

User Name *

The number of characters allowed is between 1 and 31

Expiry by
None

Passphrase

The number of characters allowed is between 8 and 32

MAC Address

VLAN

VLAN ID should be in between 1 and 4094

Save



Note:

The **Passphrase** field is optional and is automatically generated based on the selected **Passphrase Strength**.

- **Bulk mode**—Multiple entries are created in this mode depending on the count configured

Add ePSK

Mode
☐ Single ☒ Bulk

Count*

This allows values between 2 and 2000

User Name Prefix*

Username and Passphrase will be auto generated i.e prefix-1

Expiry by
None

VLANs

Use comma "," separated VLANs. To provide a range use "-".

Save

WLANs > Default Enterprise

Configuration Devices

WLAN

AAA Servers

Guest Access

Access Control

Passpoint

ePSK

☐ Base WLAN for Personal Wi-Fi SSID **X**
Turning on this setting will disable this WLAN's SSID. Use the Wi-Fi AP device configuration tab i.e. Advanced Settings -> WLANs section to enable it with a personalized SSID name.

Mode
☒ Local ☐ RADIUS **X** Configure LOCAL DB based ePSK or RADIUS based ePSK. Please configure AAA server when RADIUS based ePSK is selected.

Passphrase Strength
☐ Easy ☒ Strong ☐ Number This allows Alphanumeric and Special Characters (up to 16 Characters)

Add New Import Export Delete

<input type="checkbox"/>	User Name	MAC Address	Passphrase	Creation Date	Expiration Date	Status	VLAN		
<input type="checkbox"/>	admin	N/A	12345678	Wed, Aug 30, 2023	-	Active	N/A		
<input type="checkbox"/>	test-1	N/A	#N\$V6i9YzAZBjHS*	Wed, Aug 30, 2023	Aug 30 2024 16:5...	Active	10		
<input type="checkbox"/>	test-10	N/A	<1LJNh8BtBgtap	Wed, Aug 30, 2023	Aug 30 2024 16:5...	Active	20		
<input type="checkbox"/>	test-100	N/A	pH4cFsvF8a"Z"Rek	Wed, Aug 30, 2023	Aug 30 2024 16:5...	Active	20		
<input type="checkbox"/>	test-1000	N/A	%j8JIBH5&[q4]	Wed, Aug 30, 2023	Aug 30 2024 16:5...	Active	20		
<input type="checkbox"/>	test-101	N/A	uFdFA99>ZM16E%	Wed, Aug 30, 2023	Aug 30 2024 16:5...	Active	10		
<input type="checkbox"/>	test-102	N/A	kgwHF<T2yu2e:GS	Wed, Aug 30, 2023	Aug 30 2024 16:5...	Active	20		
<input type="checkbox"/>	test-103	N/A	gy2mWfYjBjAE13fb	Wed, Aug 30, 2023	Aug 30 2024 16:5...	Active	10		
<input type="checkbox"/>	test-104	N/A	joch_~4jKRvUfJc	Wed, Aug 30, 2023	Aug 30 2024 16:5...	Active	20		
<input type="checkbox"/>	test-105	N/A	ZA6bSQ>8POTCp&n	Wed, Aug 30, 2023	Aug 30 2024 16:5...	Active	10		

Showing 1 - 10 Total: 1001 10 < Previous 1 2 3 4 5 ... 101 Next >

10. To automatically expire ePSK details after a specific duration. The following options are available:



Note:

This feature is available from cnMaestro 4.1.0 and later versions only.

- **None**—ePSK details never expire. Select **None** to never expire the ePSK credentials.
- **Date and Time**— ePSK expires after the specified date and time (in dd/mm/yyyy hh:mm AM/PM format)

Supported minimum time is 12 A.M. on the next day and the maximum is five years.

Expiry by

Date and Time 12/04/2024 03:05 PM

Set expiration time for the created ePSK. Expired ePSKs will not be pushed to the APs when the configuration is pushed manually or applied automatically by Auto Sync.

- **Duration**— ePSK expires after the specified (in hours, days, months, or years) in the **Expiry by** drop-down.

Supported minimum duration is one hour and the maximum is five years. No decimal values are supported, for example, 1.5 hours.

Expiry by Expiry in

Duration 1 Years

Set expiration time for the created ePSK. Expired ePSKs will not be pushed to the APs when the configuration is pushed manually or applied automatically by Auto Sync.



Note:

- The configured expiry time appears in the **Expiration Date** column on the **WLANs > <WLAN name>** page.

- The **Status** column on the **WLANS** > <WLAN name> page displays the status of the ePSK details—**Active**, **Expired**, or **None**. **None** is displayed only when older ePSK keys are imported to cnMaestro.
- Expired ePSK details are deleted from the AP only when the next configuration sync functionality is initiated or when there is a configuration change in the AP.

ePSK registration for WPA3 clients

For the ePSK feature, when you configure WPA3-WPA2 (mixed mode)-PSK or WPA3-PSK as the WLAN security, the clients connection in the WPA3 mode must go through an additional registration phase. This is different from the flow when you configure WPA2-PSK as the WLAN security, where users can authenticate by using only a passphrase.

When clients use WPA3-PSK security, Simultaneous Authentication of Equals (SAE) is the authentication mechanism where an extra authentication is added, which is more secure than WPA2. For WPA2-PSK clients, the passphrase is matched against a database to identify the user. However, this is not possible for WPA3-PSK clients because of the extra authentication in WPA3-SAE. When WPA2-PSK security is used, the Pairwise Master Key (PMK) is the same for every connection made by the client. This is due to the underlying weaknesses in WPA2-PSK, which make it easier to validate the passphrase. In contrast, when WPA3-PSK security is used, a new PMK is generated each time a client joins the network. Therefore, registration will help us to know the passphrase upfront when a client tries to connect. This mandates the users to register themselves with the ePSK passphrase to bind the client MAC with the passphrase to successfully connect to the Wi-Fi network.

For WPA3 clients to connect to the network using ePSK flow:

1. First connect to the WLAN with the WLAN passphrase.

A simple password is recommended to be configured, for example, `signmeup`, or any other appropriate passphrase.

2. Register themselves with the WPA3-ePSK unique passphrase.

After the MAC binding is complete, users can use the WPA3-ePSK unique passphrase for subsequent WLAN connections.

This section describes the following topics:

- [ePSK with WPA3 feature recommendations](#)
- [Scenarios while registering clients](#)
- [Enabling ePSK registration flow using the AP CLI](#)
- [Configuring ePSK registration for WPA3 clients](#)
- [Registration flow screenshots](#)
- [Recommended best practices](#)

ePSK with WPA3 feature recommendations

The following are the recommendations for this feature:

- This feature is supported only on cnMaestro Cloud 5.1.0 onwards.
- Supported AP firmware version is 6.6.1 or 7.0 and above.
- Security mode must be configured to either **WPA2/WPA3 Pre-shared Keys** or **WPA3 Pre-shared Keys**.
- APs must be managed from cnMaestro Cloud for client registration.
- The WLAN VLAN must be able to provide DHCP to clients and must have internet connectivity.
- This feature is not supported on Enterprise Wi-Fi 5 APs and Xirrus APs.

Scenarios while registering clients

When a client connects to the WLAN, the following scenarios are possible:

- When a client connects for the first time using WPA2 security and ePSK passphrase (either on 2.4 GHz or 5 GHz radios), the AP performs an ePSK lookup. The following are the outcome:
 - If a match is found, the MAC binding is created with the respective ePSK key.
AP shares this MAC binding information with the other APs in the network.
 - If a match is not found, the connection fails.
- If the WPA2 client is connected using the WLAN passphrase, client registration steps are performed to bind the passphrase to the client.
- When a client connects for the first time using WPA3 security, the following two possibilities may occur:
 1. If MAC binding is not available for the client on the AP, the following procedure must be completed for successful registration of clients:
 - a. User must authenticate using the configured *WLAN* passphrase, for example, *signmeup*.
If the user tries to sign in with some other password other than the configured *WLAN* password (*signmeup*), the connection fails.
 - b. If the connection with the configured password (*signmeup*) is successful, the AP redirects the client to the registration page.
This is the only traffic allowed for the client with this *WLAN* passphrase.
 - c. User must now enter the configured *ePSK* passphrase and register.
The AP redirects the client to the registration page with instructions.

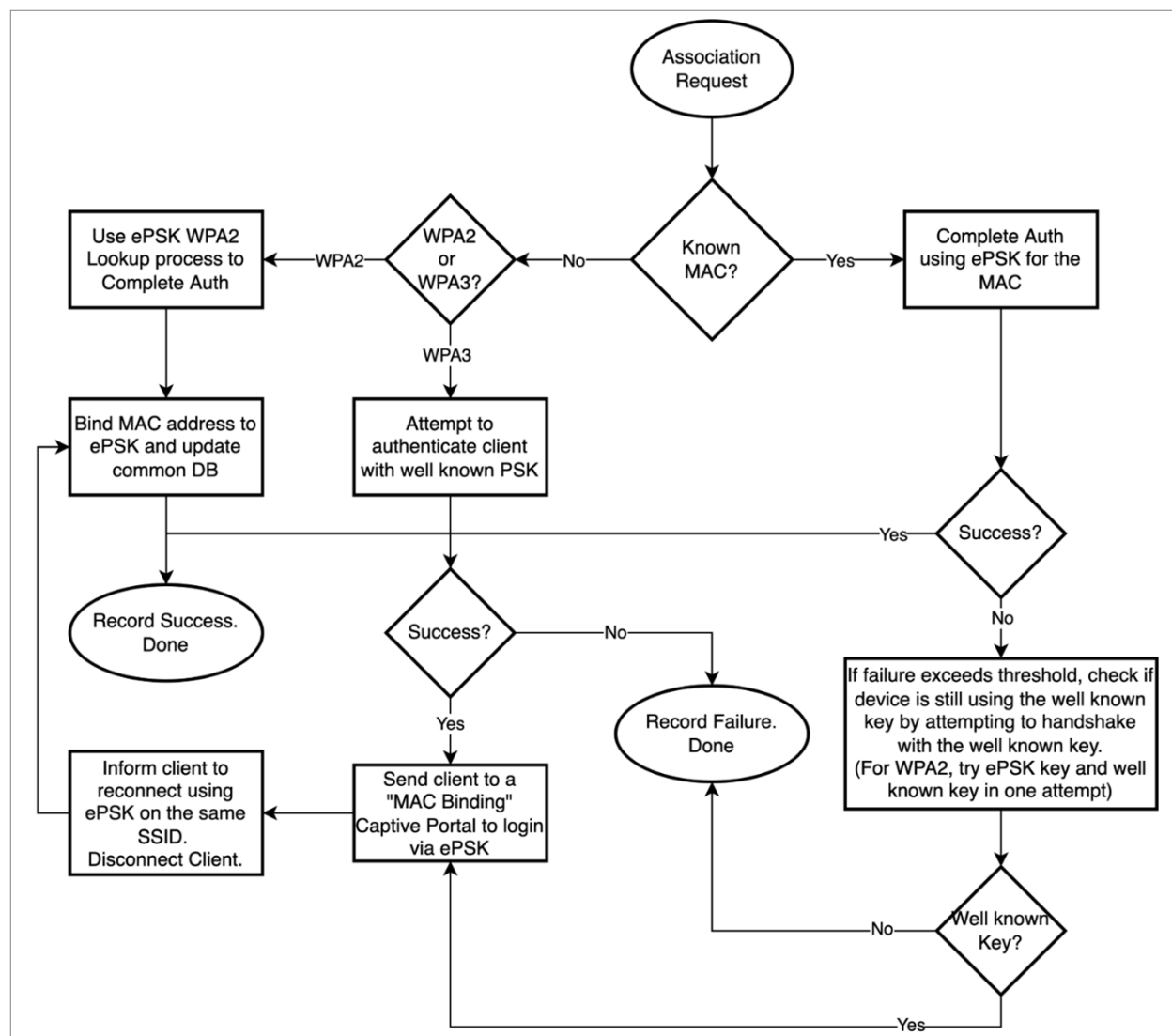
- d. Users must select the checkbox after reading the instructions (provided for different clients, such as Android, Windows, and iOS), and then disconnect from the network.
- e. User must forget the WLAN/SSID and reconfigure using the ePSK passphrase.

User then reconnects with ePSK passphrase and gets authenticated.

For a more detailed information, see [Registration flow screenshots](#).

2. When MAC binding is available for the client on the AP, users can authenticate the client with the passphrase present in the MAC binding, that is the ePSK passphrase.

Figure 29 Client registration flow for WPA3 clients



Enabling ePSK registration flow using the AP CLI

To enable ePSK registration for WPA3 clients in the AP CLI, execute the following commands:

```
ap(config)# wireless wlan 1
ap(config-wlan-1)# epsk-registration-flow
```

Configuring ePSK registration for WPA3 clients

To enable WPA3-ePSK registration, you must create a WLAN profile and add ePSK entries in the ePSK grid.

To create WLAN profile and add ePSK entries, complete the following steps:

1. Navigate to **Configuration > Wi-Fi Profiles** page.
 2. Select **WLANs** tab and click **Add**.
 3. Select **Enterprise Wi-Fi** from the **Type** drop-down list and configure the WLAN parameters.
 4. In the **Basic Settings** section, ensure either the **WPA2/WPA3 Pre-shared Keys** or **WPA3 Pre-shared Keys** option is selected in the **Security** drop-down list.
 5. Enter the WLAN passphrase.
 6. Click **Save**.
- When ePSK passphrase is not configured in the **WLANs > ePSK** page, the following message is displayed explaining the registration flow.

Figure 30 Message on the ePSK page when no ePSK entries are added

WLANs > Add New


WLAN

☐ Base WLAN for Personal Wi-Fi SSID **x**
Turning on this setting will disable this WLAN's SSID. Use the Wi-Fi AP device configuration tab i.e. Advanced Settings -> WLANs section to enable it with a personalized SSID name.

Mode
☒ Local ☐ RADIUS **x** Configure LOCAL DB based ePSK or RADIUS based ePSK. Please configure AAA server when RADIUS based ePSK is selected.

Passphrase Strength
☐ Easy ☒ Strong ☐ Number This allows Alphanumeric and Special Characters (up to 16 Characters)

ePSK

☐ This WLAN uses WPA3 security. Client registration flow is required and will be enabled when ePSK entries are added. Use the QR code to guide users for registering their clients. Note that the WLAN Passphrase will be used to verify that the client is attempting registration. Ensure that the client will get DHCP IP on the WLAN VLAN and will be able to reach cnMaestro Cloud. 

[Add New](#) [Import](#) [Export](#) [Delete](#)

<input type="checkbox"/>	User Name	MAC Address	Passphrase	Creation Date	Expiration Date	Status	VLAN
No Data Available							

Showing 0 - 0 Total: 0 10 < Previous Next >

[Save](#) [Close](#)

- For existing WLANs where ePSK entries are present and when **WPA2/WPA3 Pre-shared Keys** or **WPA3 Pre-shared Keys** option is selected in the **Security** drop-down list, the following messages appear respectively

Figure 31 When **WPA3 Pre-shared Keys** option is selected

The screenshot shows the WLAN configuration interface. The 'SSID' section has 'Enable' checked and 'ePSK WPA3' entered. The 'Mesh' dropdown is set to 'Off'. The 'VLAN' is set to '1'. The 'Security' dropdown is set to 'WPA3 Pre-Shared Keys'. A message below the dropdown states: 'For best client experience with ePSK, use WPA2/WPA3-PSK or WPA2-PSK security mode. Registration flow is enabled for WPA3 clients. [Learn more](#) on how to enable WPA3 with ePSK.' The 'Passphrase' field contains 'wlanpassword'.

Figure 32 When **WPA2/WPA3 Pre-shared Keys** option is selected

The screenshot shows the WLAN configuration interface. The 'SSID' section has 'Enable' checked and 'ePSK WPA3' entered. The 'Mesh' dropdown is set to 'Off'. The 'VLAN' is set to '1'. The 'Security' dropdown is set to 'WPA2/WPA3 Pre-Shared Keys'. A message below the dropdown states: 'Registration flow for ePSK is enabled for WPA3 clients. [Learn more](#) on how to enable WPA3 with ePSK.' The 'Passphrase' field contains 'wlanpassword'.

7. Click the **ePSK** tab and add the passphrase.

After the ePSK passphrase is added, the following message is displayed explaining the registration flow.

Figure 33 Message on the ePSK page when ePSK entries are added

The screenshot shows the ePSK management page. At the top, there's a 'Passphrase Strength' section with 'Strong' selected. A message box states: 'This WLAN uses WPA3 security. Client registration flow is active. Use the QR code to guide users for registering their clients. Note that the WLAN Passphrase will be used to verify that the client is attempting registration. Ensure that the client will get DHCP IP on the WLAN VLAN and will be able to reach cnMaestro Cloud.' Below this is a table with columns: User Name, MAC Address, Passphrase, Creation Date, Expiration Date, Status, and VLAN. There is one entry for 'ePSK' with a passphrase 'epskpassword@1234'. At the bottom, it says 'Showing 1 - 1 Total: 1'.

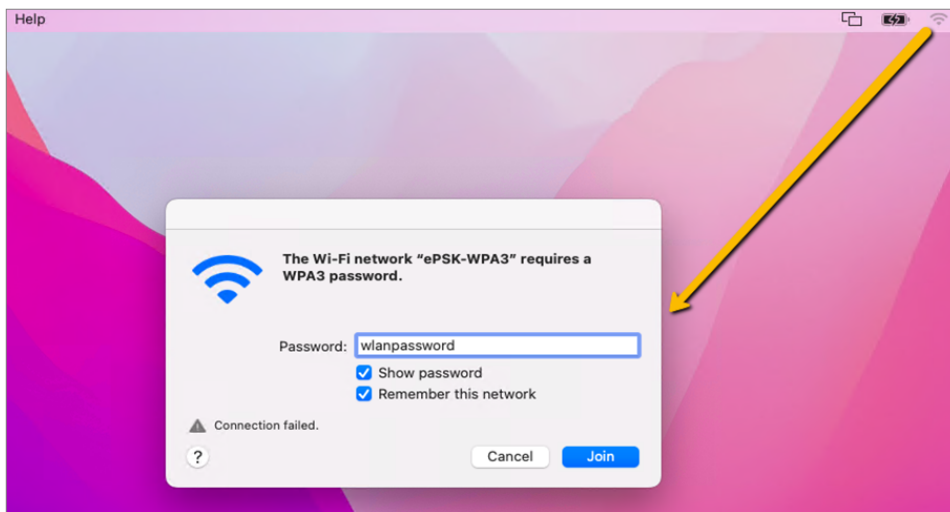
User Name	MAC Address	Passphrase	Creation Date	Expiration Date	Status	VLAN
ePSK	N/A	epskpassword@1234	Thu, Jun 13, 2024	Jun 13 2025 12:47:05	Active	1

Registration flow screenshots

To register the clients to the network using the ePSK passphrase, users must complete the following steps:

1. Connect the client to the network using the WLAN passphrase.

Figure 34 Using WLAN passphrase for connecting to network



2. Click **Join**.

Clients are redirected to the **Client Registration** page for providing the ePSK passphrase.

3. Enter the ePSK passphrase in the **Passphrase** field and click **Register**.

Figure 35 Using ePSK passphrase for client registration

Join "ePSK-WPA3"

Client Registration

Passphrase*

epskpassword@1234

Enter your unique Wi-Fi password

Register

How to get passphrase?

To connect to this secure Wi-Fi network, you must first register your client once using this form. Please use the unique Wi-Fi password provided by your administrator here. This unique password is different from the general password you used to reach this form. If you need help or forgot your unique Wi-Fi password, please reach out to your administrator for assistance.

qa-us-e1-guest.cloud.cambiumnetworks.com Cancel

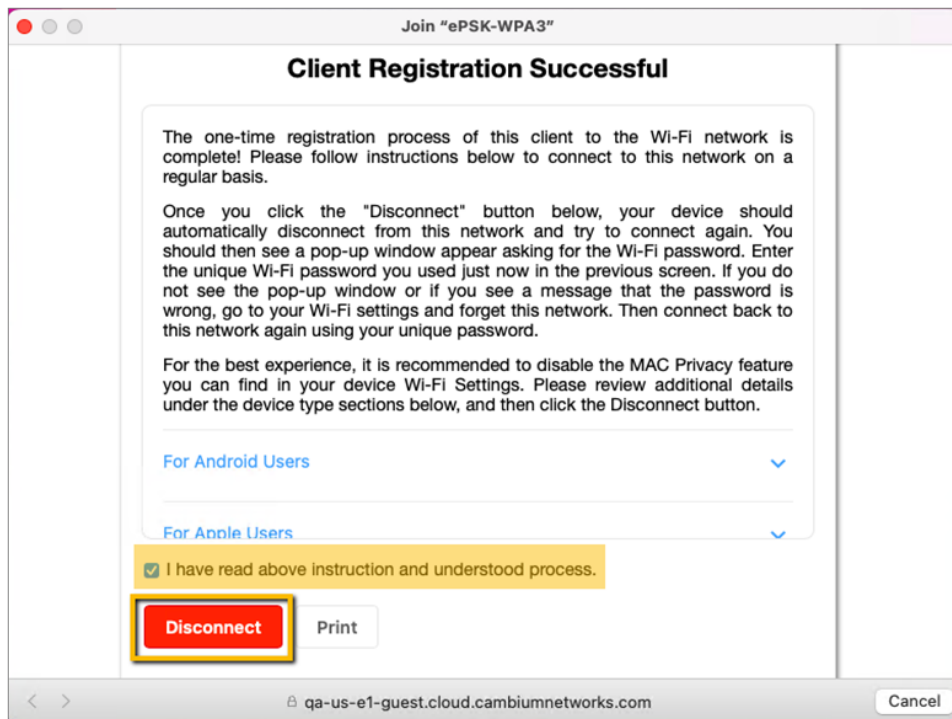
The registration success page is displayed along with a set of instructions.

4. Read the instructions (provided for different devices, such as Android, Windows, and iOS) and select the checkbox for confirmation.

The instructions provide details of the next steps for different devices.

The **Disconnect** button is enabled.

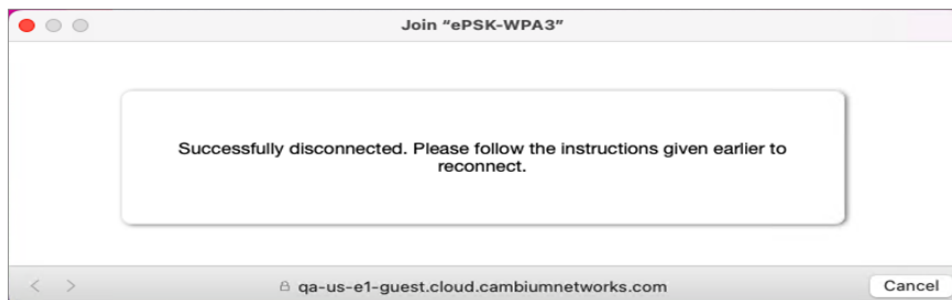
Figure 36 Registration success page with instructions



5. Click **Disconnect**.

The client is disconnected and a disconnect success message is displayed.

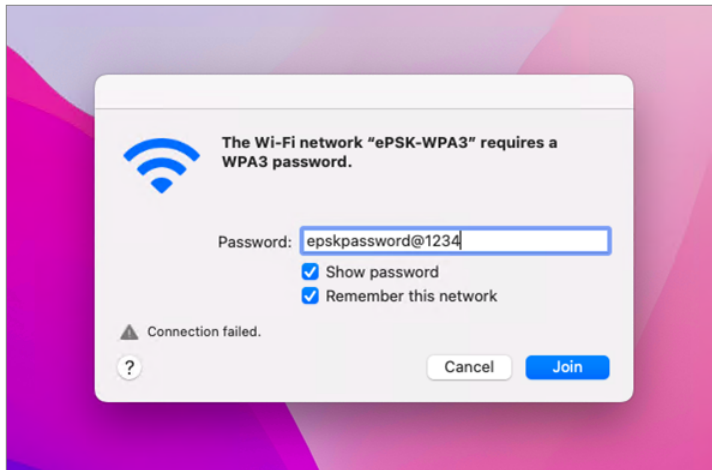
Figure 37 Disconnect success page



6. Reconnect to the network using the ePSK passphrase that you provided in the **Client Registration** page earlier.

The client connects to the network with the mapped VLAN.

Figure 38 Using ePSK passphrase for connecting to network



Recommended best practices

Following are some of the best practices you can follow while configuring ePSK registration for WPA3 clients:

- WPA3 PSK is not recommended for unmanaged (BYOD) clients (For example, multi-dwelling unit (MDU), hospitality, and educational institutions).

In MDUs, with IoT clients, making WPA3 mandatory with a single SSID may not be a successful deployment.

- WPA2/WPA3 PSK is recommended for unmanaged clients and to transition from the current (WPA2-PSK).
- Most of the WPA3-capable clients favor WPA3 PSK when available. This behavior is different among other clients, where some fallback to WPA2 and some which do not.
- When the SSID is mapped to 2.4 GHz and 5 GHz radios, WPA2 PSK or WPA2/WPA3 PSK security is recommended.
- When the SSID is mapped to 2.4 GHz, 5 GHz, and 6 GHz radios, or only the 6 GHz radio, then WPA3 PSK security is recommended.

Creating a Personal Wi-Fi ePSK



Note

This feature is available from cnMaestro 4.1.0 and later versions only.

In Multiple Dwelling Units (MDU), personal Wi-Fi allows a user to connect all the personal devices to a unique SSID associated with a VLAN.

To configure personal W-Fi on the AP, complete the following steps in the cnMaestro UI:

1. Add and enable the SSID details (to be used as personal Wi-Fi) in the **WLANS** tab, under **Manage and Operation > Networks > <network name> > Configuration > Device Configuration > Advanced Settings** section.
 - a. Select the **Enable SSID** checkbox.
 - b. In the **Passphrase** field, configure the passphrase.
 - c. Configure the VLAN with which the SSID must be associated.
2. Enable personal Wi-Fi on the ePSK page for the WLAN profile by selecting the **Base Personal SSID** checkbox.

By default, this feature is disabled. Once enabled, the **Enable** checkbox (under **WLANS > WLAN > Basic Settings > SSID**) is cleared. Also, the local and RADIUS ePSKs are disabled.

For more information on configuring personal Wi-Fi, refer to the *cnMaestro User Guide*.

RADIUS-based ePSK Premium feature

Cambium Networks ePSK feature is an extension of WPA2 PSK where multiple passphrases can be assigned to a single SSID. The Wi-Fi clients can have unique passphrases that can be used by each client using this feature. The same feature has been now extended to RADIUS.

The RADIUS server can provide the matching PMK for a given client, and corresponding standard RADIUS attributes can be enforced for a client session. This requires custom development on the RADIUS server.



Note

ePSK feature is not supported with WPA3.

Configuring RADIUS-based ePSK

To configure RADIUS-based ePSK, complete the following steps:

1. Navigate to **Configuration > Wi-Fi Profiles**.
2. Select **WLAN** tab and click **Add**.
3. Select **Enterprise Wi-Fi** from the **Type** drop-down list and enter details in the **Basic Information** section.
4. In the **Basic Settings** section, ensure the **WPA2 Pre-Shared Keys** option is selected in the **Security** drop-down list.
5. Click **Save**.
6. Click the **ePSK** tab and select the **RADIUS^X** option in the **Mode** field.

WLANs > Add New

WLAN
AAA Servers
Guest Access
Access Control
Passpoint
ePSK

☐ **Base WLAN for Personal Wi-Fi SSID X**
Turning on this setting will disable this WLAN's SSID. Use the Wi-Fi AP device configuration tab i.e. Advanced Settings -> WLANs section to enable it with a personalized SSID name.
Mode
☐ Local ☒ **RADIUS X** Configure LOCAL DB based ePSK or RADIUS based ePSK. Please configure AAA server when RADIUS based ePSK is selected.

You must configure AAA servers when configuring RADIUS-based ePSK. See *cnMaestro User Guide* for information on configuring AAA servers.

WLANs > Add New

WLAN
AAA Servers
Guest Access
Access Control
Passpoint
ePSK

Warning: AAA Servers are configured separately for each WLAN.

Authentication Server

Host	Secret	Port*	Realm
1. Host eg. xxx.xurp	<input type="password"/> <input type="button" value="Show"/>	1812	
2. Host eg. xxx.xurp	<input type="password"/> <input type="button" value="Show"/>	1812	
3. Host eg. xxx.xurp	<input type="password"/> <input type="button" value="Show"/>	1812	

Timeout: Timeout in seconds for each request attempt (1-30)

Attempts: Number of attempts before giving up (1-3)

Accounting Server

Host	Secret	Port*
1. Host eg. xxx.xurp	<input type="password"/> <input type="button" value="Show"/>	1813
2. Host eg. xxx.xurp	<input type="password"/> <input type="button" value="Show"/>	1813
3. Host eg. xxx.xurp	<input type="password"/> <input type="button" value="Show"/>	1813

Timeout: Timeout in seconds for each request attempt (1-30)

Attempts: Number of attempts before giving up (1-3)

Accounting Mode: Configure accounting mode

☐ Accounting Packet Enable Accounting On messages

☐ Sync Accounting Records Configure accounting records to be synced across neighboring APs

Interim Update Interval: Interval for RADIUS Interim-Accounting updates (10-65535 Seconds)

Advanced Settings

Server Pool Mode

☒ Load Balance Load balance requests equally among configured servers

☐ Failover Move down server list when earlier servers are unreachable

NAS-Identifier: NAS-identifier attribute for use in Request packets (defaults to system name)

☐ Dynamic Authorization Enable RADIUS dynamic authorization (COA, DM messages)

☒ Dynamic VLAN Enable RADIUS assigned VLANs

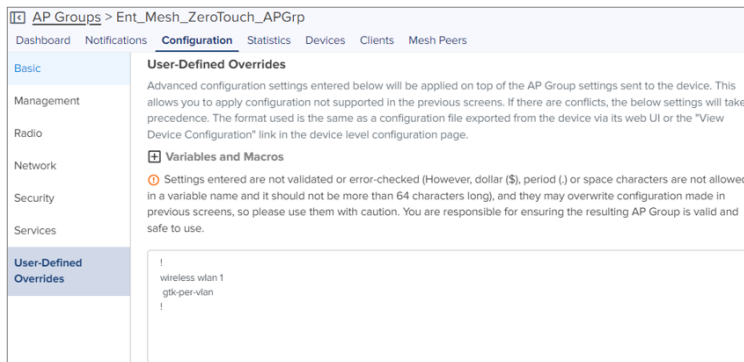
Called Station ID: Configure AP-MAC:SSID as Called-Station-Id in the RADIUS packet

Groupwise Transient Key (GTK) per VLAN

The APs support dynamic VLAN via ePSK/RADIUS based/VLAN-pool feature on a given WLAN profile. The client traffic is tagged as per the VLAN assigned dynamically. The unicast traffic works fine as each client generates a unique PTK. However, the AP provides common GTK for all the clients associated with the WLAN profile irrespective of the VLAN that belongs to. This causes all clients irrespective of the VLAN assigned can receive broadcast/multicast data traffic of other VLAN traffic.

The solution is to generate the GTK per VLAN and forward it to clients as part of the WPA2 handshake. So that the broadcast/multicast data traffic is encrypted using GTK based on the VLAN tag of the packet. The maximum number of GTKs supported is 127 per radio. By default it is disabled.

cnMaestro configuration:



The screenshot shows the 'AP Groups' configuration page for 'Ent_Mesh_ZeroTouch_APGrp'. The left sidebar contains a menu with 'Basic', 'Management', 'Radio', 'Network', 'Security', 'Services', and 'User-Defined Overrides' (which is currently selected). The main content area is titled 'User-Defined Overrides' and contains a warning message: 'Advanced configuration settings entered below will be applied on top of the AP Group settings sent to the device. This allows you to apply configuration not supported in the previous screens. If there are conflicts, the below settings will take precedence. The format used is the same as a configuration file exported from the device via its web UI or the "View Device Configuration" link in the device level configuration page.' Below this is a section for 'Variables and Macros' with a warning icon and text: 'Settings entered are not validated or error-checked (However, dollar (\$), period (.) or space characters are not allowed in a variable name and it should not be more than 64 characters long), and they may overwrite configuration made in previous screens, so please use them with caution. You are responsible for ensuring the resulting AP Group is valid and safe to use.' At the bottom, there is a text input field containing the following configuration lines: '! wireless wlan 1', 'gtk-per-vlan', and '!'.

AP Groups > Ent_Mesh_ZeroTouch_APGrp	
Dashboard Notifications Configuration Statistics Devices Clients Mesh Peers	
Basic	User-Defined Overrides
Management	Advanced configuration settings entered below will be applied on top of the AP Group settings sent to the device. This allows you to apply configuration not supported in the previous screens. If there are conflicts, the below settings will take precedence. The format used is the same as a configuration file exported from the device via its web UI or the "View Device Configuration" link in the device level configuration page.
Radio	Variables and Macros
Network	Settings entered are not validated or error-checked (However, dollar (\$), period (.) or space characters are not allowed in a variable name and it should not be more than 64 characters long), and they may overwrite configuration made in previous screens, so please use them with caution. You are responsible for ensuring the resulting AP Group is valid and safe to use.
Security	
Services	
User-Defined Overrides	! wireless wlan 1 gtk-per-vlan !

Configuring the Network

This chapter describes the following topics

- [Overview](#)
- [Configuring Network parameters](#)

Overview

This chapter gives an overview of the Enterprise Wi-Fi AP configuration parameters related to LAN, VLAN, Routes, DHCP server, ACL, and Firewall.

Configuring Network parameters

Enterprise Wi-Fi AP network configuration parameters are segregated into the following sections:

- [VLAN](#)
- [Routes](#)
- [Ethernet Ports](#)
 - [Port Control—802.1X Authentication](#)
- [DHCP](#)
- [Tunnel](#)
- [PPPoE](#)
- [VLAN Pool](#)
- [Wireless Wide Area Network \(WWAN\)](#)

IPv4 network parameters

VLAN



Note

By default, the XRP messages are sent through the native VLAN. From release version 6.6.2 onwards, a new CLI command (`roam management-vlan`) is added to enable XRP messages to be sent through any VLAN other than the native VLAN. When configured, the roaming VLAN must have an L3 interface on the AP.

To configure network parameters, complete the following steps:

1. Navigate to **Configuration > Wi-Fi Profiles > AP Groups** page.
2. Click **Add New** and select **Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)** from the **Type** drop-down list.

- Click **Network** tab > **VLANs** section.

Figure 39 *Network > VLANs section*

- Click **Add New** and configure the IPv4 parameters described in the following table.

Table 34 *VLAN IPv4 parameters*

Parameters	Description	Range	Default
VLAN > IPv4			
Address	Provision to configure the mode of IPv4 address configuration for an interface selected. Two modes are supported: <ul style="list-style-type: none"> DHCP—This is the default mode in which the Enterprise Wi-Fi AP device tries to obtain an IPv4 address from the DHCP server. Static IP—Users must explicitly configure the IPv4 address and Netmask for a VLAN selected. 	—	DHCP
NAT	This option enables wireless traffic gets NAT'ed with APs respective uplink interface IP. This option is recommended when DHCP pools are configured in AP.	—	Disabled
Zeroconf IP	Zeroconf IP is recommended to be enabled. This interface is available only in the VLAN1 configuration section. If VLAN 1 is not allowed in Ethernet interfaces, this IP will not be accessible.	—	Enabled
DHCP Relay Agent	This option is enabled when DHCP server is hosted on a VLAN which is not same as client that is requesting the DHCP IP. Enabling this appends Option 82 in the DHCP packets. Following information is allowed to configure: <ul style="list-style-type: none"> DHCP Option 82 Circuit ID <p>Configurable parameters under this option are as follows:</p> <ul style="list-style-type: none"> Hostname APMAC BSSID SSID 	—	Disabled


Parameters	Description	Range	Default
	<ul style="list-style-type: none"> ◦ Custom • DHCP Option 82 Remote ID Configurable parameters under this option are as follows: <ul style="list-style-type: none"> ◦ Hostname ◦ APMAC ◦ BSSID ◦ SSID ◦ Custom <div>  <div> Note In case DHCP Option 82 is configured at the device-, WLAN profile-, and L3 interface-levels, the following priority order is considered: <ol style="list-style-type: none"> 1. Device-level configuration 2. WLAN profile-level configuration 3. L3 interface-level configuration </div> </div>		
Request Option All	This configuration decides the interface on which Enterprise Wi-Fi AP will learn the following: <ul style="list-style-type: none"> • IPv4 default gateway • DHCP client options like Option 43 and Option 15 (Controller discovery like controller host name / IPv4 address) • DNS Servers • Domain Name 	–	Enabled on VLAN1

Figure 40 VLAN IPv4 parameters

Add VLAN

VLAN ID

1

Please enter VLAN ID (1 to 4094)

IPv4

IP Address

☒ DHCP
 ☐ Static IP

xxxxxx.xxxx.xx

xxxxxx.xxxx.xx

Netmask

xxxxxx.xxxx.xx

NAT

When NAT is enabled, IP addresses under this Switched Virtual Interface are hidden

Zeroconf IP Support 169.254.x.x local IP address

DHCP Relay Agent

xxxxxx.xxxx.xx

Enable relay agent and assign DHCP server

DHCP Option 82 Circuit ID

None

DHCP Option 82 Remote ID

None

Request Option All

Enable DHCP request option all on this interface

IPv6

General

Add

DHCP Client Options

Enterprise Wi-Fi AP devices learn multiple DHCP options for all VLAN interfaces configured on the device. Based on configured criteria, values of these options are used by the system. The below table lists the different DHCP options.

Table 35 DHCP Options

Options	Description	Usage	Reference CLI
Option 1	The subnet mask option specifies the client's subnet mask as per RFC 950.	Based on the state of “Request Option All”, the device chooses a subnet mask from the respective VLAN interface.	show ip route
Option 3	This option specifies a list of IP addresses for routers on the client's subnet.	Based on the state of “Request Option All”, the device chooses a route learned from the respective VLAN interface. The only first route is honored.	show ip route

Options	Description	Usage	Reference CLI
Option 6	The domain name server option specifies a list of Domain Name System (STD 13, RFC 1035) name servers available to the client. Servers SHOULD be listed in order of preference.	Based on the state of “Request Option All”, the device chooses a subnet mask from the respective VLAN interface. the top two DNS servers are honored by Enterprise Wi-Fi AP devices.	<code>show ip name-server</code>
Option 15	This option specifies the domain name that the client should use when resolving hostnames via the Domain Name System.	More details are provided in Option 15.	<code>show ip dhcp-client info</code>
Option 26	This option specifies MTU size in a network.	More details are provided in Configuring the Network .	<code>show ip dhcp-client info</code>
Option 28	This option specifies the broadcast address that the client should use.	A broadcast address learned for all VLAN interfaces are used respectively as per standards	<code>show ip dhcp-client-info</code>
Option 43	This option is used to help the AP in obtaining the cnMaestro IP address from the DHCP server while a DHCP request to get an IP address is sent to the DHCP server.	More details are provided in Option 43 (cnMaestro On-Premises 2.4.0 User Guide).	<code>show ip dhcp-client info</code>
Option 51	This option is used in a client request to allow the client to request a lease time for the IP address. In a server reply, a DHCP server uses this option to specify the lease time it is willing to offer.	Enterprise Wi-Fi AP renew leases for all VLAN interfaces configured based on lease time that has been learned from the DHCP server.	<code>show ip dhcp-client info</code>
Option 54	DHCP clients use the contents of the server identifier field as the destination address for any DHCP messages unicast to the DHCP server.	Enterprise Wi-Fi AP learns DHCP server IP for all VLAN interfaces configured.	<code>show ip dhcp-client info</code>
Option 60	This option is used by DHCP clients to optionally identify the vendor type and configuration of a DHCP client.	For Enterprise Wi-Fi AP device, value is updated as Cambium-Wi-Fi-AP.	<code>show ip dhcp-client info</code>

DHCP Option 43—Zero-touch onboarding

This option is used to help the AP in obtaining the cnMaestro/XMS IP address from the DHCP server while a DHCP request to get an IP address is sent to the DHCP server.

This option is used to learn HTTPS proxy server address from the DHCP server as well.

DHCP Option 43 format

If HTTP proxy needs to be configured, then the following format must be used:

The cnMaestro/XMS URL and HTTPS proxy URL can be packed into Option 43 payload in a key-value pair separated by ',' like <key=value,key=value>. Key and its value are separated by '=' character.

For example,

0=CMBM;1=cloud.cambiumnetworks.com;2=http://user:userpass@IP/URL:port, where identifiers are listed below:

- 0 is for header CMBM - **Mandatory**
- 1 is for the server's URL
- 2 is for HTTP proxy URL



Note

If only cnMaestro URL configuration is needed then Option 43 payload can contain only that too without key-value format as described above.

Routing and DNS

Table 36 AP Groups > Network > VLAN > Routes > IPv4 Routing and DNS parameters


Parameters	Description	Range	Default
Default Gateway	Provision to configure the default gateway. If this is provided, Enterprise Wi-Fi AP device installs this gateway as this is the highest priority.	–	–
DNS Server	Provision to configure Static DNS server on Enterprise Wi-Fi AP device. A maximum of two DNS servers can be configured.	–	–
Domain Name	Provision to configure Domain Name. If this is provided, Enterprise Wi-Fi AP device installs this Domain Name as this is the highest priority.	–	–
DNS Proxy	Enterprise Wi-Fi AP device can act as DNS proxy server when this parameter is enabled. <div>Note DNS Proxy is allowed only when NAT mode is enabled for the WLAN.</div>	–	Disabled

Figure 41 IPv4 Routing and DNS parameters

AP Groups > Add New

Basic

Management

Radio

Network

Security

Access Control

Services

User-Defined Overrides

Routes

☒ **IPv4 Routing and DNS**

Default Gateway
 IP address of default gateway

Domain Name
 Domain name

DNS Server 1
 Primary domain name server

DNS Server 2
 Secondary domain name server

☐ DNS Proxy

Routes

Below table lists the fields that are displayed in **Configure > Network > Routes** tab:

Table 37 IPv4 Gateway Source Precedence, Route entries, and Port forwarding parameters

Parameters	Description	Range	Default
Gateway Source Precedence	Provision to prioritize default gateway and DNS servers when Enterprise Wi-Fi AP device has learned from multiple ways. Default order is Static and DHCP.	—	Static
Add Multiple Route Entries	The user has provision to configure static Routes. Parameters that are required to configure static Routes are as follows: <ul style="list-style-type: none"> • Destination IP • Mask • Gateway 	—	—
Port Forwarding	This feature is required when wireless stations are behind NAT. Users can access the services hosted on wireless stations using this feature. Following configurable parameters are required to gain access to services hosted on wireless stations which are behind: <ul style="list-style-type: none"> • Port • IP Address • Type 	—	—

Figure 42 IPv4 Gateway Source Precedence, Route entries, and Port forwarding parameters

IPv6 network parameters

VLAN

Table 38 VLAN IPv6 parameters

Parameters	Description	Range	Default
Address	Provision to configure the mode of IPv6 address configuration for an interface selected. Five modes are supported: <ul style="list-style-type: none"> Disabled AutoConfig Static Stateless DHCPv6 Stateful DHCPv6 	–	AutoConfig
Request Option All	This configuration decides the interface on which AP will learn the following: <ul style="list-style-type: none"> IPv6 default gateway 	–	Enabled on VLAN1

Parameters	Description	Range	Default
	<ul style="list-style-type: none"> DHCP client options like Option 52 and Option 24 (Controller discovery like controller hostname / IPv6 address) DNS Servers Domain Name 		

Figure 43 VLAN IPv6 parameters

Routing & DNS

Table 39 IPv6 Routing and DNS parameters

Parameters	Description	Range	Default
Default Gateway	Provision to configure the default gateway. If this is provided, Enterprise Wi-Fi AP device installs this gateway as this is the highest priority.	–	–
DNS Server	Provision to configure Static DNS server on Enterprise Wi-Fi AP device. A maximum of two DNS servers can be configured.	–	–
Domain Name	Provision to configure Domain Name. If this is provided, Enterprise Wi-Fi AP device installs this Domain Name as this is the highest priority.	–	–
IPv6 Preference	When enabled, IPv6 is preferred over IPv4 based on DNS response.	–	Disabled

Figure 44 IPv6 Routing and DNS parameters

Routes

Table 40 IPv6 Gateway Source Precedence and Multiple Route Entries parameters

Parameters	Description	Range	Default
Gateway Source Precedence	Provision to prioritize default gateway and DNS servers when Enterprise Wi-Fi AP device has learned from multiple ways. Default order is Static and AUTO-CONFIG/DHCP.	–	Static
Add Multiple Route Entries	The user has provision to configure static Routes. Parameters that are required to configure static Routes are as follows: <ul style="list-style-type: none"> Destination IP/prefix Gateway 	–	–

Figure 45 IPv6 Gateway Source Precedence and Multiple Route Entries parameters

AP Groups > Add New

Basic
Management
Radio
Network
Security
Access Control
Services
User-Defined Overrides

Routes

- IPv4 Routing and DNS
- IPv6 Routing and DNS
- IPv4 Gateway Source Precedence
- IPv6 Gateway Source Precedence**

1 Static

2 Auto-config/DHCPv6

IPv4 Multiple Route Entries

IPv6 Multiple Route Entries

Add New

Destination IP	Gateway
No Multiple Routes configured	

Port Forwarding

General network parameters

Table 41 VLAN - General parameters

Parameters	Description	Range	Default
Management Access	Provision to restrict the access of devices in all modes CLI (Telnet, SSH), GUI (HTTP, HTTPS), and SNMP. Users can configure restriction of device access as follows: <ul style="list-style-type: none"> Block Allow from Wired Allow from both Wired and Wireless 	—	Allow from both Wired and Wireless

Select Management Access to configure restriction of the device from the drop-down list.

Figure 46 VLAN - General parameters

Add VLAN

VLAN ID

Please enter VLAN ID (1 to 4094)

☐ IPv4

☐ IPv6

☒ **General**

Management Access

Allow from Wired and Wireless

CLI/GUI/SNMP access via this interface

Add

Ethernet Ports

Below table lists the fields that are displayed in **AP Groups > Network > Ethernet Ports** tab.

Table 42 Ethernet Ports 1 to 4 parameters

Parameters	Description	Range	Default
Ethernet Port <1-4>	Enterprise Wi-Fi AP devices Ethernet port is provisioned to operate in the following modes: <ul style="list-style-type: none"> Access Single VLAN—Single VLAN traffic is allowed in this mode. Trunk Multiple VLANs—Multiple VLANs are supported in this mode. 	–	Access Single VLAN
VLAN	VLAN ID to be associated with the Ethernet port.	1 to 4094	1
Port Speed	Specifies the port speed in Mbps. Following values are supported: <ul style="list-style-type: none"> Auto 10 Mbps 100 Mbps 1000 Mbps 2500 Mbps 5000 Mbps 	–	Auto
Port Duplex	Specifies the type of duplex communication configured for the port.	–	Full Duplex

Parameters	Description	Range	Default
	Following values are supported: <ul style="list-style-type: none"> • Full Duplex • Half Duplex 		
Tunnel Mode	Only applicable for Ethernet ports 2, 3, and 4. Specifies whether tunneling of wired traffic is enabled or not.		

Figure 47 Ethernet Ports parameters

Port Control—802.1X Authentication

802.1X authentication on Ethernet ports enhance the network security of the AP. The AP supports 802.1X port-based authentication in the single-host authentication mode. In this mode, only one client is allowed to access the network after successful 802.1X port-based authentication. After successful authentication, the port VLAN is assigned based on RADIUS assigned VLAN.



Note

- 802.1X port-based authentication does not support CoA messages.

802.1X port-based authentication requires a RADIUS AAA server for authentication and accounting.

The following table lists the parameters for configuring the RADIUS AAA server on Ethernet ports available on the **AP Groups > Network > Ethernet Ports > RADIUS Server** page.

Table 43 RADIUS Server parameters

Parameters	Description	Range	Default
Authentication Server	Specifies the authentication server details, such as: <ul style="list-style-type: none"> • Host—IPv4 or IPv6 address or hostname of the server • Secret—Text string that is used to encrypt data in RADIUS packets shared between the AP and the sever. Format—Text string • Port—Port number of the authentication server. Default—1812 A maximum of three RADIUS authentication servers can be configured.	-	Disabled
Accounting Server	Specifies the accounting server details, such as: <ul style="list-style-type: none"> • Host—IPv4 or IPv6 address or hostname of the server 	-	Disabled

Parameters	Description	Range	Default
	<ul style="list-style-type: none"> • Secret—Text string that is used to encrypt data in RADIUS packets shared between the AP and the sever. Format—Text string • Port—Port number of the accounting server. Default—1813 <p>A maximum of three RADIUS accounting servers can be configured.</p>		
Timeout	Time (in seconds) to wait for a response from the RADIUS server.	1–30	3
Attempts	Number of retry attempts for contacting the RADIUS server.	1–3	1
Accounting Mode	<p>Specifies the accounting mode to be used. The following modes are supported:</p> <ul style="list-style-type: none"> • Start-Stop—Accounting packets are transmitted by APs to the AAA server when a wireless client is connected and when the client disconnects. • Start-Interim-Stop—Accounting packets are transmitted by APs to the AAA server when a wireless client connects, then at regular intervals (configured in the Interim Update Interval field) and also when the client disconnects. • None—Disables the accounting mode. This is the default mode. 	-	None (Disabled)
Server Pool Mode	<p>Users can configure multiple Authorization and Accounting servers. Based on a number of wireless stations, the user can choose Failover mode.</p> <ul style="list-style-type: none"> • Load Balance—AP equally distributes the requests between the configured RADIUS servers, • Failover—AP selects the RADIUS server that is functional based on the order of configuration. 	-	Failover
Interim update interval	<p>Time (in seconds) to wait for sending RADIUS interim accounting update packets.</p> <p>Note: This interval is applicable only when you select the Start-Interim-Stop option in the Accounting Mode parameter.</p>	10–65535	1800
Dynamic Authorization	This option is required, where there is CoA request from AAA/RADIUS server.	-	Disabled

Figure 48 RADIUS Server parameters

AP Groups > Add New

Basic
Management
Radio
Network
Security
Access Control
Services
User-Defined Overrides

RADIUS Server

Authentication Server

1. Host Secret Port*
2. Host Secret Port*
3. Host Secret Port*

Timeout
3 Timeout in seconds for each request attempt (1-30)
Attempts
1 Number of attempts before giving up (1-3)

Accounting Server

1. Host Secret Port*
2. Host Secret Port*
3. Host Secret Port*

Timeout
3 Timeout in seconds for each request attempt (1-30)
Attempts
1 Number of attempts before giving up (1-3)

Accounting Mode

None Configure accounting mode

Server Pool Mode

☒ Load Balance Load balance requests equally among configured servers
☐ Failover Move down server list when earlier servers are unreachable

Interim Update Interval

1800 Interval for RADIUS Interim-Accounting updates (10-65535 Seconds)

☒ Dynamic Authorization Enable RADIUS dynamic authorization (COA, DM messages)

DHCP

Below table lists the fields that are displayed in the **AP Groups > Network > DHCP** page.

Figure 49 DHCP Pool parameters

AP Groups > Add New

Basic
Management
Radio
Network
Security
Access Control

DHCP Pool

Add New

DHCP Pool	Address Range	Default Router	Domain Name	DNS Address	Network	Lease
No DHCP Pool configured						

Table 44 DHCP parameters

Parameters	Description	Range	Default
DHCP Pool	Specifies the DHCP pool ID.	1 to 16	–

Parameters	Description	Range	Default
Address Range	Indicates the start and end addresses for the DHCP Pool.	—	—
Default Router	Specifies the default router IP address.	—	—
Domain Name	Specifies the domain name for the DHCP pool.	—	—
DNS Address	Specifies the primary and secondary addresses of the DNS server for a DHCP pool.	—	—
Network	Specifies the network IP address and subnet mask for the DHCP pool.	—	—
Lease	Duration (in days, hours, and minutes) for which the IP address must be leased to the client.	—	1 day
Add Bind List			
	<p>For every DHCP pool configured, the user can bind MAC and IP from the address pool defined, so that the wireless station gets the same IP address every time they connect. Following parameters are required to bind IP address:</p> <ul style="list-style-type: none"> • MAC Address • IP Address 	—	—

Figure 50 Add DHCP window

The screenshot shows the 'Add DHCP' configuration window. It includes the following sections and fields:

- DHCP Pool:** A text field for 'Pool Number'.
- Address Range:** Two text fields for 'Start' and 'End' IP addresses.
- Default Router:** A text field.
- Domain Name:** A text field.
- DNS Address:** Two text fields for 'Primary' and 'Secondary' addresses.
- Network:** Two text fields for 'IP' and 'Mask'.
- Lease:** Three text fields for 'Lease time (days hours minutes)'.
- Bind List:** A section with two text fields for 'MAC' and 'IP' addresses, and an 'Add' button.
- Footer:** A message 'No Bind List configured' and an 'Add' button.

Tunnel

The following table lists the fields that are displayed in **AP Groups > Network > Tunnel** page.

Figure 51 Tunnel - L2TP parameters

AP Groups > Add New

Basic
Management
Radio
Network
Security
Access Control
Services
User-Defined Overrides

Tunnels

Basic Settings

Tunnel Encapsulation
L2TP

L2TP

Remote IP
 IP address or domain

Username

Password
 Show

Authentication Type
Default

TCP MSS
 ☒ TCP Maximum Segment Size (422-1410 bytes)

☒ PMTU Discovery Enable Path Maximum Transmission Unit discovery to avoid IP fragmentation

L2GRE

Figure 52 Tunnel - L2GRE parameters

AP Groups > Add New

Basic
Management
Radio
Network
Security
Access Control
Services
User-Defined Overrides

Tunnels

Basic Settings

Tunnel Encapsulation
L2GRE

L2TP

L2GRE

Remote IP
 IP address or domain

DSCP
 Differentiated Service Code Point

TCP MSS
 ☒ TCP Maximum Segment Size (472-1460 bytes)

☒ PMTU Discovery Enable Path Maximum Transmission Unit discovery to avoid IP fragmentation

MTU
 Configure MTU for L2GRE tunnel (850-1460 bytes)

☐ Cambium GRE Enable Cambium Generic Routing Encapsulation

☐ GRE in UDP Enable GRE in UDP encapsulation

Table 45 Tunnel parameters

Parameters	Description	Range	Default
Tunnel Encapsulation	Provision to enable tunnel type. Following tunnel types are supported by Enterprise Wi-Fi AP devices: <ul style="list-style-type: none"> • L2TP • L2GRE • OFF 	–	OFF
L2TP			
Remote IP	Configure L2TP end point. IPv4 address or Primary hostname of the endpoint is supported.	–	–
Username and Password	Credentials required for L2TP authentication.	–	admin/admin
Authentication Type	Provision to select the PPP authentication method. Following are the options available: <ul style="list-style-type: none"> • DEFAULT • CHAP • MS-CHAP • MS-CHAPv2 • PAP 	–	DEFAULT
TCP MSS	TCP Maximum Segment Size (MSS) in bytes.	422- 1410	1400
PMTU Discovery	Provision to enable to discover PMTU in network.	–	Enabled
L2GRE-1 You can configure a maximum of two L2GRE tunnels. Configure L2GRE-1 tunnel by configuring the below parameters in the AP Groups > Network > Tunnel tab. However, configuring L2GRE-2 tunnel is allowed only using the device CLI. The following parameters for L2GRE-1 are also applicable for L2GRE-2.			

Parameters	Description	Range	Default
Remote IP	Configure L2GRE endpoint. IPv4 address or primary hostname of an endpoint is supported.	–	–
DSCP	Users can configure priority of GRE packets.	–	0
TCP MSS	TCP Maximum Segment Size (MSS) in bytes.	472-1460	1410
PMTU Discovery	Provision to enable to discover PMTU in a network.	–	–
MTU	Maximum Transmission Unit in bytes.	850-1460	1460
GRE in UDP	GRE protocol is designed to establish a tunnel between any third-party vendor which complies with RFC 8086.	–	Disabled

Point-to-Point Protocol over Ethernet (PPPoE)

PPPoE provides the ability to establish a connection to ISP with user authentication. Below table lists the fields that are displayed in **AP Groups > Network > PPPoE** page.

Figure 53 PPPoE parameters

AP Groups > Add New

Basic
Management
Radio
Network
Security
Access Control
Services
User-Defined Overrides

PPPoE

Basic Settings

☐ Enable

VLAN ID

Vlan ID assigned to PPPoE

Service Name

Configure PPPoE service-name parameters (max 32 characters)

Authentication Info

Username

Password

MTU

Configure MTU for PPPoE connection (500-1492 bytes)

☒ TCP MSS Clamping Enable TCP Maximum Segment Size Clamping to avoid packet fragmentation

☐ Management Access Enable CLI/GUI/SNMP access via this interface

Table 46 PPPoE parameters

Parameters	Description	Range	Default
Enable	Provision to enable PPPoE client.	–	Disabled
VLAN ID	Users can configure VLAN ID where PPPoE clients should obtain an IP address.	–	–
Service Name	Configure PPPoE service name.	–	–
Authentication Info	Provision to configure credentials required for PPPoE authentication.	–	admin/admin
MTU	Maximum Transmission Unit.	500-1492	1492
TCP-MSS Clamping	Configure PPPoE endpoint. Either IP or hostname of an endpoint is supported.	–	Enabled
Management Access	If enabled, the user can access the device either using UI or SSH with PPPoE IP.	–	Disabled

VLAN Pool

The following table lists the fields that are displayed in **AP Groups > Network > VLAN Pool** page.

Table 47 The VLAN Pool parameters

Parameters	Description	Range	Default
VLAN Pool Name	Name for the VLAN pool.	–	–
VLAN ID List	List of VLAN IDs for the VLAN pool. You can configure either a single VLAN ID or multiple VLAN IDs. Multiple VLAN IDs can be configured either separated by comma or hyphen. For example, 2-7, 45, 67.	–	–

Figure 54 The VLAN Pool parameters

AP Groups > Add New

Management
Radio
Network
Security
Access Control
Services

☐ VLAN Pool

VLAN Pool Name VLAN ID List

No VLAN Pool configured

Wireless Wide Area Network (WWAN)

The following table lists the fields that are displayed in **Configure > Network > WWAN** tab.



Note

This feature is supported in XV2-2, XV3-8, XE3-4, and XE5-8 platforms only.

Table 48 WWAN parameters

Parameters	Description	Range	Default
WWAN	Provision to enable wireless WAN using a USB cellular dongle for internet access.	–	–
Failover Only	Failover only can be configured in two modes: <ul style="list-style-type: none">• Enabled: Ethernet will be the primary connection and WWAN will be backup.• Disabled: 3G/4G (WWAN) will be the only working connection. Note: Cellular link can be configured as backup only to Ethernet connection.	–	Enabled
APN	Provision to configure network provider APN address.	–	–
Authentication Info	Provision to configure credentials required for WWAN authentication.	–	admin/admin
Monitor Host	Running a check in the background that constantly monitors a user configured IP address (example: 8.8.8.8) for reachability through ping.	–	–

Figure 55 WWAN parameters

AP Groups > Add New

Basic
Management
Radio
Network
Security
Access Control
Services
User-Defined Overrides

☒ **WWAN**
WWAN
☐ Enable Wireless WAN using a USB cellular dongle for internet access

Failover Only
☒ Use WWAN as backhaul only when failover is triggered

APN
 Configure network provider APN address

Authentication Info
Username

Password

Monitor Host
 Host to monitor in order to trigger WWAN failover

Supported hardware

Cambium Networks currently support the following models, where local laws permit:

- Huawei
 - E8372
 - E3372
- Alcatel
 - Link Key 4G IK40V (recommended)
- ZTE
 - MF833V

Configuring Access Control

The Access Control page allows the users to enable or assign access control policies and configure user group policies and device policies. It offers visibility into the configured rules, ensuring efficient and secure network management.

Figure 56 Access Control page

The screenshot shows the 'Access Control' page in a management interface. The left sidebar contains a navigation menu with options: Basic, Management, Radio, Network, Security, **Access Control**, Services, and User-Defined Overrides. The main content area is titled 'AP Groups > GE_TEST' and includes tabs for Dashboard, Notifications, Configuration (active), Statistics, Reports, Devices, Clients, and Mesh Peers. The 'Access Control' section is expanded, showing three sub-sections: 'Access Control' with an 'Enable Access Control' checkbox and a dropdown for 'Access Control Policy' (set to 'None'); 'User Group Policy' with an 'Apply Filter(s)' button and a table with columns 'Policy Name', 'RADIUS Filter-ID', 'Access Control Policy', and 'VLAN'; and 'Device Policy' with an 'Apply Filter(s)' button and a table with columns 'Policy Name', 'Device Class', 'Device Type', and 'Access Control Policy'. Both tables show 'No Data Available'. At the bottom of each table, there is a pagination bar indicating 'Showing 0 - 0 Total: 0 10' and navigation links for 'Previous' and 'Next'.



Note

If an Access Control Policy is assigned at the AP group level, it does not appear under User Group or Device Group policies.

This chapter describes the following topics

- [Enabling Access Control Policy](#)
- [User Group Policy](#)
- [Device Policy](#)

Enabling Access Control Policy

Users have the provision to enable or disable access control policies under **Access Control** tab.

Figure 57 Enabling Access Control Policy

The screenshot shows the 'Access Control' section of the management interface. It includes a checkbox labeled 'Enable Access Control' which is checked. Below it is a dropdown menu for 'Access Control Policy' with the value 'test' selected. To the right of the dropdown is a button labeled 'View Rules' which is highlighted with a red rectangle.

Users can select the available access control policies listed in the Wi-Fi profiles in the **Access Control Policy** drop-down list. They can also view the configured rules associated with these policies by clicking **View Rules**. This provides a comprehensive view of the policies and rules within the network.

Figure 58 Access Control Policy Rules

Name	Status	Action	Type	Application / Category	Protocol	Source IP Mask	Destination IP Mask	Schedule
Iperf_app	Enabled	Allow	Layer7-filter	Iperf	-	-	-	-
speedtest_APP	Enabled	Allow	Layer7-filter	speedtest.net	-	-	-	-
allow_instagram	Enabled	Allow	Layer7-filter	Instagram	-	-	-	-
ap_gp_deny_ndtv	Enabled	Deny	Layer7-filter	NDTV	-	-	-	-
Ap_Gp_allow_whatsapp	Enabled	Allow	Layer7-filter	WhatsApp	-	-	-	-
Ap_GP_Allow_Facebook	Enabled	Allow	Layer7-filter	Facebook	-	-	-	-

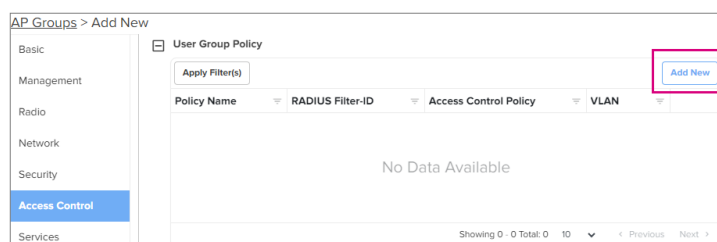
User Group Policy

User group policies allow you to categorize users into specific roles with customized access permissions and restrictions, facilitating a fine-tuned control over network access.

To add a new to User Group Policy, perform the following steps:

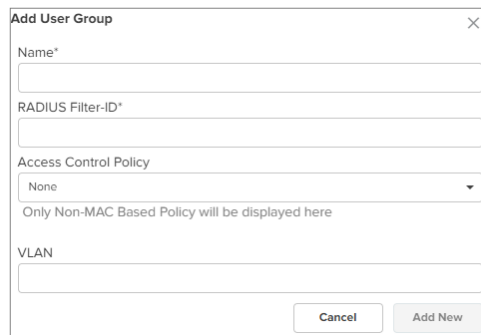
1. Navigate to **Configuration** > Wi-Fi Profiles > AP Groups > **Access Control** page.
2. Click **Add** to create a new AP group.
3. Click the **Access Control** tab in the **Add New** page.
4. Click **Add New** in the **User Group Policy** section.

Figure 59 User Group Policy



5. Complete the details in the **Add User Group** window.

Figure 60 Add User Group



The 'Add User Group' dialog box contains the following fields and controls:

- Name***: A text input field.
- RADIUS Filter-ID***: A text input field.
- Access Control Policy**: A dropdown menu with 'None' selected. Below it, a note states: 'Only Non-MAC Based Policy will be displayed here'.
- VLAN**: A text input field.
- Buttons**: 'Cancel' and 'Add New' buttons at the bottom right.



Note

- The user must assign an Access Control Policy or VLAN to create a User Group Policy.
- A maximum of 64 User Group Policies are supported.
- Users can select Access Control Policies with non-MAC filters only from the **Access Control Policy** drop-down list.
- Mapping an Access Control Policy to a User Group Policy enables its use for the AP group, and vice versa. However, the same Access Control Policy cannot be shared between the User Group Policy and the AP group. You can apply it either to the User Group Policy or to the AP group only.

Device Policy

Device Policy allows users to apply specific rules and access control policies based on the type and characteristics of devices, offering customized control over device behavior within the network.

To add a new Device Policy, perform the following steps:

1. Navigate to **Configuration > Wi-Fi Profiles > AP Groups** tab.
2. Click **Add** to create a new AP group.
3. Click the **Access Control** tab in the **Add New** page.
4. Click **Add New** in the **Device Policy** section.

Figure 61 Device Policy

The screenshot shows the 'AP Groups > Add New' page. On the left is a sidebar with navigation links: Management, Radio, Network, Security, Access Control (highlighted), Services, User-Defined, and Overrides. The main content area is titled 'Device Policy' and contains an 'Apply Filter(s)' button. Below this is a table with columns: Policy Name, Device Class, Device Type, and Access Control Policy. The table is currently empty, displaying 'No Data Available'. At the bottom right of the table area, there is a pagination bar showing 'Showing 0 - 0 Total: 0' and buttons for 'Previous' and 'Next'. A red rectangular box highlights the 'Add New' button located at the top right of the table area.

5. Complete the details in the **Add Device Policy** window.

Figure 62 Add Device Policy

The screenshot shows the 'Add Device Policy' dialog box. It has a title bar with a close button (X). The form contains the following fields:

- 'Name*' with an empty text input field.
- 'Device Class*' with a dropdown menu showing 'Any'.
- 'Device Type*' with a dropdown menu showing 'Any'.
- 'Access Control Policy*' with a dropdown menu showing 'None'.

Below the 'Access Control Policy*' dropdown, there is a note: 'Only Non-MAC Based Policy will be displayed here'. At the bottom of the dialog are two buttons: 'Cancel' and 'Add New'.



Note

- A maximum of 64 Device Policies are supported.
- Users can select Access Control Policies with non-MAC filters only from the **Access Control Policy** drop-down list.

Managing Filters

This chapter describes the following topics:

- [Overview](#)
- [Filter list](#)
- [Device class filter](#)
- [Wi-Fi Calling support](#)
- [Air cleaner](#)
- [Application control Premium feature](#)

Overview

Filters are used to define the rules used for blocking or passing traffic and also to change QoS/DSCP and rate-limiting for selected traffic.

The Wireless AP's integrated firewall uses stateful inspection to accelerate the decision of whether to allow or deny traffic user connections managed by the firewall are maintained statefully. Once user flow is established through the AP, it is recognized and passes through without the application of all defined filtering rules. Stateful inspection runs automatically on the AP.

Filter list

Filters are organized in groups, called filter lists. A filter list allows users to apply a uniform set of filters to SSIDs. AP supports 16 filter lists and each filter list supports 50 filter rules in precedence order.

Filters

These settings create and manage filters with precedence that belong to the current filter list, based on the filter criteria you specify.

Filters can be configured in Layer 2 and Layer 3 or application/category control (Layer 7). Layer 2 rule takes high precedence over Layer 3 application control and Layer 2 supports MAC/IP/protocol-based rules.

Filters are an especially powerful feature when combined with the intelligence provided by the **Application Control Windows**.

Based on Application Control's analysis of your wireless traffic, you can create filters to enhance wireless usage for your business needs:

1. Usage of non-productive and risky applications like BitTorrent can be restricted.
2. Traffic for mission-critical applications like VoIP and WebEx may be given higher priority (QoS).

3. Non critical traffic from applications like YouTube may be given lower priority (QoS) or bandwidth allowed may be capped per station or for all stations.

Configuring filter CLI

By configuring the filter CLI, the user can define ACL rules for blocking or passing traffic, DSCP/QoS rules for modifying packets, and rate-limiting for selected traffic.

1. Create filter list/filter profile using global filter command (Filter: configure filter parameters).

```
ap(config)# filter
filter-list : Configure filter list
global-filter : Configure Global filter parameters
```

2. Global-filter is for global rules in AP. Global-filter includes the below options:

```
ap(config-global-filter)#
air-cleaner : Configure Preset air cleaner filters
application-control : Enable application control
clear : Clear command
disable : Disable filter list
filter : Configure filter rules in precedence order
stateful : Enable stateful filtering
apply : Apply configuration that has just been set
exit : Exit from filter list configuration
no : Delete/disable filter list parameters
save : Save configuration to Flash so it persists across reboots
show : Show command
```

- **Stateful filtering** : Stateful operation of the integrated firewall can be Enabled or Disabled. By default, it is enabled.
- **Application Control** [Premium feature](#): Operation of the Application Control feature may be Enabled or Disabled.
- **Disable**: Disable or enable filter list.

3. Each filter list includes below options:

```
clear          : Clear command
disable        : Disable filter list
filter         : Configure filter rules in precedence order
name          : Name of filter list

apply         : Apply configuration that has just been set
exit          : Exit from filter list configuration
no            : Delete/disable filter list parameters
save          : Save configuration to Flash so it persists across reboots
show          : Show command
```



Note

Global-filter rules will take precedence over filter-list rules

- Global filter and filter-list can include 50 filter rules with precedence order.

```
ap(config-filter-list-1)# filter precedence {1-50}
```

4. Then create filter rule from precedence level (1 to 50).

```
(config-list-1-filter-precedence-1)# exit
(config-filter-list-1)# filter precedence 1
(config-list-1-filter-precedence-1)#

application-control : Configure application control filters
category-control   : Configure application category control filters
clear              : Clear command
disable            : Disable filter
layer2-filter       : Configure Layer2 filter
layer3-filter       : Configure Layer3 filter
logging            : Enable filter logging
rate-limit         : Set traffic limit for this filter
schedule           : Schedule Layer3 rules
wlan-to-wlan       : Restrict 'in' direction rule's egress direction as wlan

apply             : Apply configuration that has just been set
exit              : Exit from custom filter configuration
no                : Disable the filter options
save              : Save configuration to Flash so it persists across reboots
show              : Show command
```



Note

The filter type is either Layer 2 or Layer 3 or application control can be added in one precedence level.

5. Layer 3 filter has the below provisions.

```
(config-list-1-filter-precedence-1)# layer3-filter

deny          : Drop packet matching the rule
permit        : Allow packet matching the rule
set-dscp       : Set DSCP value to packet matching the rule
set-qos        : Set QoS value (0-3) to packet matching the rule
```

- **QoS [Premium feature](#)**: Set packets QoS level (0 to 3). Level 0 has the lowest priority; level 3 has the highest priority
- **DSCP [Premium feature](#)**: Differentiated Services Code Point or DiffServ (DSCP). DSCP level (0 to 63). Level 0 has the lowest priority and level 63 has the highest priority.
- **Rate limit [Premium feature](#)**: Filters support rate limiting per station or all stations and support Kbps/Mbps/pps.
- **Schedule [Premium feature](#)**: Filter support scheduling the activation of the layer3 /application control rules based on the day and local time selected.
- **Disable**: Each filter and filter list can be turned on/off.



Note:

Application Control, QoS, DSCP, Schedule and Rate limit are [Premium features](#).

6. Each layer 3 rule category has below types

```
(config-list-1-filter-precedence-1)# layer3-filter set-dscp

ip          : IPV4 address based rule
ip6         : IPV6 address based rule
proto       : Protocol based rule
proto6      : IPv6 Protocol based rule
```

7. For proto or port number-based rule, select proto.

```
(config-list-1-filter-precedence-1)# layer3-filter set-dscp proto

layer3-filter set-dscp proto (tcp|udp|icmp|igmp|srp|sctp|any) (SOURCE-IP[{mask|prefix-length}]|any) (SOURCE-PORT|any) (DESTINATION-IP[{mask|prefix-length}]|any) (DESTINATION-PORT|any) (in|out|any) (DSCP{0-63}) <(optional)//Filter_name>
```



Note

All fields are mandatory. If no parameter to configure, give 'any'. Direction is the direction of the rule. if it is 'in', the rule is applicable for traffic from the wireless side. If it is 'out', the rule is applies for traffic to wireless.

8. For non-protocol or port number-based rules, select IP.

```
(config-list-1-filter-precedence-1)# layer3-filter set-dscp ip  
  
layer3-filter set-dscp ip (SOURCE-IP[{mask|prefix-length}]|any) (DESTINATION-IP[{mask|prefix-length}]|any) (in|out|any) (DSCP{0-63}) <(optional)//Filter_name>
```

9. Layer 2 filter has below options:

```
(config-list-1-filter-precedence-11)# layer2-filter  
  
deny          : Drop packet matching the rule  
permit        : Allow packet matching the rule
```

10. Each layer 2 rule category has below two cases.

```
(config-list-1-filter-precedence-11)# layer2-filter permit  
  
mac           : Mac or IP based Rule with out Protocol  
proto         : Mac or IP based rule with Protocol
```

Layer 2 rule supports IP, MAC, Port, or Protocol-based rules.

11. ap(config-list-1-filter-precedence-1) # layer2-filter permit mac

```
(config-list-1-filter-precedence-1)# layer2-filter permit mac  
  
layer2-filter permit mac (SOURCE-MAC/IPv4/IPv6{(optional)//{mask|prefix-length}}|any)  
(DESTINATION-MAC/IPv4/IPv6{(optional)//{mask|prefix-length}}|any) (in|out|any) <(optional)//Filter_name>
```

Example:

```
e.g. layer2-filter permit mac 00-01-02-03-04-05 00-01-02-09-08-07 any //filter_to_allow_guest  
'!' for not e.g. layer2-filter permit mac 00-01-02-03-04-05 !00-01-02-09-08-07 out  
layer2-filter permit mac !1.1.1.1/8 any any
```

12. ap(config-list-1-filter-precedence-1) # layer2-filter permit proto

```
(config-list-1-filter-precedence-1)# layer2-filter permit proto  
  
layer2-filter permit proto (tcp|udp|arp|icmp|igmp|srp|sctp|any) (SOURCE-MAC/IPv4/IPv6[{mask|prefix-length}]|any) (SOURCE-PORT|any) (DESTINATION-MAC/IPv4/IPv6[{mask|prefix-length}]|any) (DESTINATION-PORT|any) (in|out|any) <(optional)//Filter_name>
```

Example:

```
e.g layer2-filter permit proto tcp any any any 10000 any //filter_permit_guest  
'!' for not e.g layer2-filter permit proto tcp any any !00-00-11-11-11-11 10000 out  
layer2-filter permit proto tcp 1.1.1.1 1000 00:11:22:33:44:44/ff-ff-ff-00-00-00 5000 any
```

Sample configuration

```

filter global-filter
  stateful
  application-control

filter filter-list 1
  filter precedence 1
    layer3-filter set-qos ip any 9.9.9.9 in 2
    rate-limit all Mbps 500
    exit
  filter precedence 2
    layer3-filter deny ip 5.5.5.5 6.6.6.6 any
    exit
  filter precedence 3
    layer3-filter permit ip any any any
    exit
  filter precedence 4
    layer3-filter permit ip 9.9.9.9 any any
    exit

```

13. To attach the filter list into the WLAN profile, filter-list < filter-list ID>.

```

wireless wlan 1
  ssid cambium-guest
  no shutdown
  vlan 1
  filter-list 1

```

14. To show filter statistics:

```

(config)# show filter-statistics

Filter ID | global

```

Device class filter

This feature applies wireless policies to the client-based device class (notebook, phone, tablet, and laptop) and its type (Windows, Mac, and Android).

CLI configuration:

```

ap(config)# device-class-filter 1
ap(config-device-class-filter-1)# class
ap : Configure filter rules for the AP device class
appliance : Configure filter rules for the appliance device class
desktop : Configure filter rules for the desktop device class
game : Configure filter rules for the game device class
notebook : Configure filter rules for the notebook device class

```

```

phone : Configure filter rules for the phone device class
player : Configure filter rules for the player device class
tablet : Configure filter rules for the tablet device class
ap(config-device-class-filter-1)# class notebook
all : Configure filter rules for all notebook device classes
chrome : Configure filter rules for the Chrome-OS device type
linux : Configure filter rules for the Linux device type
mac : Configure filter rules for the Mac device type
windows : Configure filter rules for the Windows device type
ap(config-device-class-filter-1)# class notebook linux
ap(config-device-class-filter-1)# filter-list
Filter list ID <1-16> or Name

```

Wi-Fi Calling support

Cambium Networks Access Point has the inbuilt application visibility engine, which can detect Wi-Fi calling and provide better call quality by reducing the latency, jitter, and roaming delays for voice calls over Wi-Fi.

When the Access Point detects the Wi-Fi calling traffic, it classifies and puts the traffic in the voice priority queue for achieving better call quality.

CLI configuration:

```

filter precedence 5
application-control wificall set-qos 3

```



Note

Filter precedence can be from 1 to 50.

Air cleaner

The Air Cleaner feature offers several predetermined filter rules that eliminate a great deal of unnecessary wireless traffic.

Configuration CLI:

```

ap(config)# filter global-filter
ap(config-global-filter)# air-cleaner
all : All air cleaner filters
arp : Eliminate station to station ARPs over the air
broadcast : Eliminate broadcast traffic from the air
dhcp : Eliminate stations serving DHCP addresses from the air
multicast : Eliminate chatty multicast traffic from the air

```

When we configure the Air Cleaner rule, pre-defined filter rules will get populated automatically as shown below:

```
ap(config-global-filter)# air-cleaner all
ap(config-global-filter)# show config filter
!
!
filter global-filter
stateful
application-control
air-cleaner all
filter precedence 1
layer2-filter deny proto arp any any in //Air-cleaner-Arp.1
wlan-to-wlan
exit
filter precedence 2
layer2-filter deny proto udp any any FF:FF:FF:FF:FF:FF 67 out //Air-
cleaner-Dhcp.1
exit
filter precedence 3
layer2-filter deny proto udp any any FF:FF:FF:FF:FF:FF 68 in //Air-
cleaner-Dhcp.2
exit
filter precedence 4
layer2-filter permit proto arp any FF:FF:FF:FF:FF:FF any //Air-cleaner-
Bcast.1
exit
filter precedence 5
layer2-filter permit proto udp any any FF:FF:FF:FF:FF:FF 67 any //Air-
cleaner-Bcast.2
exit
filter precedence 6
layer2-filter permit proto udp any any FF:FF:FF:FF:FF:FF 68 any //Air-
cleaner-Bcast.3
exit
filter precedence 7
layer2-filter permit proto udp any any FF:FF:FF:FF:FF:FF 22610 any
//Air-cleaner-Bcast.4
exit
filter precedence 8
layer2-filter deny mac any FF:FF:FF:FF:FF:FF any //Air-cleaner-Bcast.5
```

```
exit
filter precedence 9
layer2-filter permit mac any 01:00:5E:00:00:FB any //Air-cleaner-mDNS.1
exit
filter precedence 10
layer2-filter deny mac any multicast any //Air-cleaner-Mcast.1
exit
```

**Note**

In Mesh link configuration, the Air Cleaner rules need customization like disabling Precedence 2 and Precedence 3 (DHCP rules).

Application control [Premium feature](#)

The Application Control feature provides real-time visibility of application usage by users across the wireless network. Network usage has changed enormously in the last few years, with the increase in smartphone and tablet usage stressing networks. Increasing traffic from legitimate business needs such as cloud- and web-based applications, streaming media, and VoIP must be handled with an adequate quality of experience. To achieve this purpose Application Control filters are used to define the rules used for blocking or passing and change QoS/DSCP and rate-limiting for the specific Application or a specific category of application. For more details, refer to the Application Control Filters section in the user guide

Application Control can track application usage over time to monitor trends. Usage may be tracked by AP, VLAN, or station. Many hundreds of applications are recognized and grouped into a number of categories. The distributed architecture of Cambium Enterprise APs allows Application Control to scale naturally as you grow the network.

This topic describes the following content:

- [Deep Packet Inspection \(DPI\)](#)
 - [Application control policy](#)
 - [Risk and productivity](#)
 - [Selection criteria](#)
 - [DPI CLI configuration](#)
 - [Global application policy](#)
 - [SSID application policy](#)
- [Custom Applications X](#)

Deep Packet Inspection (DPI)

The AP uses Deep Packet Inspection (DPI) to determine what applications are being used and by whom, and how much bandwidth they are consuming. These applications are rated by their degree of risk and productiveness. Filters can be used to implement per-application policies that keep network usage focused on productive uses.

Application control policy

When you find risky or unproductive applications consuming bandwidth on the network, you can easily create Filters to control them. You may use filters to:

- Block problematic traffic, such as BitTorrent or Y8.
- Prioritize mission-critical traffic: By increasing the QoS assigned to the traffic, applications like VoIP and WebEx may be given higher priority (QoS).
- Lower the priority of less productive traffic: Use filters to decrease the QoS assigned to traffic for applications like YouTube and Facebook.
- A nonproductive specific application can be rate-limited to avoid impact on the productive application. (for example, YouTube streaming can be rate-limited to avoid impact on applications like VoIP)

Risk and productivity

Application control ranks applications in terms of their levels of risk and productivity.

Productivity: Indicates how appropriate an application is useful for business purposes. The higher the rating number, the more business-oriented an application is:

1. Primarily recreational
2. Mostly recreational
3. Combination of business and recreational purposes
4. Mainly used for business
5. Primarily used for business

Risk: indicates how likely an application is to pose a threat to the security of your network. The higher the rating number, the riskier of an application is:

1. No threat
2. Minimal threat
3. Some risk: maybe misused
4. High risk: maybe malware or allow data leaks
5. Very high risk: threat circumvents firewalls or avoids detection

Selection criteria

From the AP CLI, the below options are available to view the Application Statistics:

- **Application:** This gives detailed information about the application seen from the wireless traffic.
- **Category:** This gives the combined statistics of the application which belongs to a particular category (for example, Games, Network monitor).

```
(config)# show application-statistics by-application
```

Applications Count = 24
Application Statistics for All Applications

Protocol or Application	Productivity Index & Risk	TX Packets	TX Bytes	RX Packets	RX Bytes
Ad Analytics	4 1	4	220	3	231
Amazon	2 1	75	31437	69	8337
Bonjour	4 1	15	1737	14	1664
DoubleClick	1 1	84	30190	65	12228
Google Ads	3 1	103	47136	78	12223
Google Analytics	4 1	13	3750	15	1711
Google APIs	3 1	4713	6288091	892	153251
Google	3 1	2544	3248915	568	48664
Google Play	3 1	350	396456	181	15261
Mozilla	3 1	54	44708	48	5854
NetBIOS NS	1 3	0	0	12	936
NTP	1 3	2	152	2	152
OCSP	3 1	63	6404	71	5247
OpenX	1 1	32	8374	27	3507
Quantcast	1 1	14	4733	17	2341
Rapleaf	3 1	19	6745	19	2288
Reddit	3 1	1227	1477596	752	74695
Scorecard Research	1 1	26	5876	27	2748
SSDP	4 1	329	146086	20	4000
SSL	3 3	226	136435	176	22509
TCP	3 1	2376	1617471	1665	330377
Twitter	3 4	79	53301	68	7532
Wikipedia	3 3	19	3126	28	3873
YouTube	1 4	95	26393	99	12233

```
ap(config)# show application-statistics by-category
```

Application Category Statistics for All Applications

```
=====
```

Application	Productivity Index & Risk	TX Packets	TX Bytes	RX Packets	RX Bytes
-------------	---------------------------	------------	----------	------------	----------

```
-----
```

File-Transfer	1 1	81	17881	0	0
Mail	3 1	1351	1057897	1318	155897
Messaging	2 2	633	245164	558	68508
Network-Monitoring	3 4	43	2580	1	60
Networking	3 1	51911	4422799	2524	1488418
Proxy	2 2	8637	7892737	6454	1008520
Social-Networking	2 3	52038	68131289	19772	2285979
Streaming-Media	2 3	15030	18700791	9156	1366044


```
Web-Services 2 2 38872 26757562 32219 7094216
```

- **SSID:** This gives the application list seen on a particular SSID. The SSID number is the BSS index configured.

```
ap(config)# show application-statistics by-application ssid 1
```

```
Applications Count = 79
```

```
Application Statistics for wlan index 1
```

```
=====
```

```
Protocol or Productivity TX TX RX RX
```

```
Application Index & Risk Packets Bytes Packets Bytes
```

```
-----
```

```
Ad Analytics 4 1 221 113639 204 27874
```

```
Admeta 4 1 20 8577 17 3470
```

```
Aggregate Knowledge 4 1 72 25718 67 11423
```

```
Amazon 2 1 1245 773227 1307 413188
```

```
Amazon Web Services 1 2 2102 2543236 1522 111343
```

```
Amp 4 1 163 144673 157 16258
```

```
AOL Ads 3 1 21 11459 24 3769
```

```
Appier 4 1 39 13552 26 5046
```

```
AppNexus 1 1 172 72763 167 62363
```

```
Bing 3 1 17 8140 12 1175
```

```
Bluekai 1 1 35 13127 23 2856
```

```
Bonjour 4 1 0 0 1067 332560
```

```
Casale 3 1 97 36559 85 12244
```

```
CloudFlare 3 2 31 12537 20 2286
```

```
Captive Network Ass 2 1 18 1194 10 918
```

```
Connexity 3 1 22 13348 27 3954
```

```
Contextweb 4 1 81 41240 100 20963
```

```
Criteo 4 1 376 171618 396 60013
```

```
Crashlytics 1 1 74 29571 82 10660
```

```
Doubleclick 1 1 3549 2691946 2587 759544
```

```
DHCP 4 1 52 17212 0 0
```

```
Dotomi 4 1 59 21308 64 8324
```

```
Drawbridge 4 1 28 6164 23 4780
```

```
Facebook 2 1 6053 5188935 4732 1217723
```

Facebook Messages 2 2 202 71996 150 18393
 Facebook Video 2 3 44585 61497202 14049 941942
 Flurry 3 1 17 5694 27 15624
 Font Awesome 4 1 94 98415 88 5341
 gmail 3 1 1351 1057897 1318 155897
 Google Ads 3 1 1356 903620 1066 123597
 Google Analytics 4 1 475 165753 407 91298
 Google APIs 3 1 5437 2829186 4775 1605169
 GoogleDuo 4 1 84 22238 82 23226
 Google 3 1 5381 3955811 4385 799374
 Google Play 3 1 980 242763 880 254459
 Google Video 2 2 0 0 20 23771
 hotstar 1 4 100 64443 82 21328
 HTTP 3 1 1184 371037 1100 173347
 HTTP 2.0 3 1 1410 360603 1271 232993
 HTTP VIDEO 3 2 3801 5360601 1841 105901
 HWCDN 3 1 213 259756 200 12745
 ICICI Bank 2 2 29 33613 21 2025
 ICMP 3 4 5 300 1 60
 Instagram 1 1 322 330979 242 33346
 Krux 1 1 71 31719 53 6993
 Lotame 1 1 109 63865 84 10168
 MDNS 3 1 0 0 86 21324
 Media Innovation Gr 3 1 45 14819 40 5662
 Media Math 1 1 25 5413 8 1034
 Mixpanel 3 1 451 139375 496 275463
 NrData 4 1 371 56753 341 108525
 NTP 1 3 1 76 1 76
 OpenX 1 1 113 20680 86 12298
 Outbrain 3 1 34 16363 46 6344
 OwnerIQ 3 1 38 8977 29 5783
 Paytm 2 3 2015 2201287 1177 146483
 Psiphon 2 2 8562 7869967 6392 983509
 PubMatic 3 1 331 103338 262 57072
 Quantcast 1 1 47 23413 47 9495
 Quic 3 1 0 0 817 1052805
 Rampleaf 3 1 66 28602 65 8000
 Rubicon Project 1 1 17 9524 24 7846

```

Scorecard Research 1 1 96 35762 90 12758
Smart AdServer 3 2 35 13345 45 6116
SpotXchange 3 2 59 14418 49 14522
SSDP 4 1 0 0 287 43911
SSL 3 3 6029 4347809 5173 1029629
Taboola 3 2 2177 2715316 1082 123164
TCP 3 1 169 37436 194 26160
The Trade Desk 3 1 101 67145 67 13168
Turn 1 1 71 31424 81 9438
Twitter 3 4 867 1040706 593 73816
UDP 3 1 0 0 62 10664
Ultrasurf 2 2 31 10286 19 1848
WhatsApp Media Mess 2 2 145 167080 135 10680
WhatsApp 2 2 404 55846 341 34602
Xiaomi 3 1 1244 718018 1376 285219
Yahoo 3 3 204 77608 251 48694
YouTube 1 4 11031 13254451 7129 1156065

```

- **Display for Station:** This gives detailed information about a particular station. Provide the station MAC address the user wants to check for statistics.

- Tx means downlink traffic concerning AP and Rx mean uplink traffic with respect to AP.

```
(config)# show application-statistics by-application station D4-6A-6A-E7-D0-15
```

Applications Count = 24
Application Statistics for station D4-6A-6A-E7-D0-15

Protocol or Application	Productivity Index & Risk		TX Packets	TX Bytes	RX Packets	RX Bytes
Ad Analytics	4	1	4	220	3	231
Amazon	2	1	75	31437	69	8337
Bonjour	4	1	0	0	15	1810
DoubleClick	1	1	84	30190	65	12228
Google Ads	3	1	103	47136	78	12223
Google Analytics	4	1	13	3750	15	1711
Google APIs	3	1	4713	6288091	892	153251
Google	3	1	2544	3248915	568	48664
Google Play	3	1	387	404916	215	20326
Mozilla	3	1	117	67446	104	12051
NetBIOS NS	1	3	0	0	12	936
NTP	1	3	2	152	2	152
OCSP	3	1	63	6404	71	5247
OpenX	1	1	32	8374	27	3507
Quantcast	1	1	14	4733	17	2341
Rapleaf	3	1	19	6745	19	2288
Reddit	3	1	1235	1478487	761	77186
Scorecard Research	1	1	26	5876	27	2748
SSDP	4	1	0	0	28	5600
SSL	3	3	226	136435	176	22509
TCP	3	1	2770	1675214	2075	424531
Twitter	3	4	79	53301	68	7532
Wikipedia	3	3	19	3126	28	3873
YouTube	1	4	113	32330	116	15918

Below CLI command gives a list of stations present along with station count per VLAN.

```
(config)# show application-statistics debug
```

=====Station Count 1=====

MAC	IP	VLAN	SSID
	10.10.0.113	1	TIGER_XV3_8_OPEN_SSID

====vlan count 1=====

VLAN	STA_COUNT
1	1

```
ap(config)# show application-statistics debug
```

=====Station Count 3=====

MAC	IP	VLAN	SSID
9A-FD-AA-B4-9C-8E	0.0.0.0	0	
FC-D9-08-A4-D4-55	0.0.0.0	0	
52-78-93-70-38-35	0.0.0.0	0	

====vlan count 1=====

VLAN	STA_COUNT
------	-----------

- Display for VLAN: This gives information about the particular VLANs.

```
(config)# show application-statistics by-application vlan 1
Applications Count = 24
Application Statistics for VLAN 1
=====
```

Protocol or Application	Productivity Index	Risk	TX Packets	TX Bytes	RX Packets	RX Bytes
Ad Analytics	4	1	4	220	3	231
Amazon	2	1	75	31437	69	8337
Bonjour	4	1	0	0	15	1810
Doubleclick	1	1	84	30190	65	12228
Google Ads	3	1	103	47136	78	12223
Google Analytics	4	1	13	3750	15	1711
Google APIs	3	1	4713	6288091	892	153251
Google	3	1	2544	3248915	568	48664
Google Play	3	1	393	405374	221	20638
Mozilla	3	1	117	67446	104	12051
NetBIOS NS	1	3	0	0	12	936
NTP	1	3	3	228	3	228
OCSP	3	1	63	6404	71	5247
OpenX	1	1	32	8374	27	3507
Quantcast	1	1	14	4733	17	2341
Rapleaf	3	1	19	6745	19	2288
Reddit	3	1	1249	1481150	779	79476
Scorecard Research	1	1	26	5876	27	2748
SSDP	4	1	0	0	32	6400
SSL	3	3	226	136435	176	22509
TCP	3	1	2910	1694616	2219	455285
Twitter	3	4	79	53301	68	7532
Wikipedia	3	3	19	3126	28	3873
YouTube	1	4	115	32434	119	16137

```
ap(config)# show application-statistics by-application vlan 1
Applications Count = 79
Application Statistics for VLAN 1
=====
```

Protocol or Application	Productivity Index	Risk	TX Packets	TX Bytes	RX Packets	RX Bytes
Ad Analytics	4	1	221	113639	204	27874
Admeta	4	1	20	8577	17	3470
Aggregate Knowledge	4	1	72	25718	67	11423
Amazon	2	1	1245	773227	1307	413188
Amazon Web Services	1	2	2102	2543236	1522	111343

Amp 4 1 163 144673 157 16258
AOL Ads 3 1 21 11459 24 3769
Appier 4 1 39 13552 26 5046
AppNexus 1 1 172 72763 167 62363
Bing 3 1 17 8140 12 1175
Bluekai 1 1 35 13127 23 2856
Bonjour 4 1 0 0 1067 332560
Casale 3 1 97 36559 85 12244
CloudFlare 3 2 31 12537 20 2286
Captive Network Ass 2 1 18 1194 10 918
Connexity 3 1 22 13348 27 3954
Contextweb 4 1 81 41240 100 20963
Criteo 4 1 376 171618 396 60013
Crashlytics 1 1 74 29571 82 10660
Doubleclick 1 1 3549 2691946 2587 759544
DHCP 4 1 52 17212 0 0
Dotomi 4 1 59 21308 64 8324
Drawbridge 4 1 28 6164 23 4780
Facebook 2 1 6053 5188935 4732 1217723
Facebook Messages 2 2 202 71996 150 18393
Facebook Video 2 3 44585 61497202 14049 941942
Flurry 3 1 17 5694 27 15624
Font Awesome 4 1 94 98415 88 5341
gmail 3 1 1351 1057897 1318 155897
Google Ads 3 1 1356 903620 1066 123597
Google Analytics 4 1 475 165753 407 91298
Google APIs 3 1 5437 2829186 4775 1605169
GoogleDuo 4 1 84 22238 82 23226
Google 3 1 5381 3955811 4385 799374
Google Play 3 1 980 242763 880 254459
Google Video 2 2 0 0 20 23771
hotstar 1 4 100 64443 82 21328
HTTP 3 1 1184 371037 1100 173347
HTTP 2.0 3 1 1410 360603 1271 232993
HTTP VIDEO 3 2 3801 5360601 1841 105901
HWCDN 3 1 213 259756 200 12745
ICICI Bank 2 2 29 33613 21 2025
ICMP 3 4 5 300 1 60

```

Instagram 1 1 322 330979 242 33346
Krux 1 1 71 31719 53 6993
Lotame 1 1 109 63865 84 10168
MDNS 3 1 0 0 86 21324
Media Innovation Gr 3 1 45 14819 40 5662
Media Math 1 1 25 5413 8 1034
Mixpanel 3 1 451 139375 496 275463
NrData 4 1 371 56753 341 108525
NTP 1 3 1 76 1 76
OpenX 1 1 113 20680 86 12298
Outbrain 3 1 34 16363 46 6344
OwnerIQ 3 1 38 8977 29 5783
Paytm 2 3 2015 2201287 1177 146483
Psiphon 2 2 8562 7869967 6392 983509
PubMatic 3 1 331 103338 262 57072
Quantcast 1 1 47 23413 47 9495
Quic 3 1 0 0 817 1052805
Rapleaf 3 1 66 28602 65 8000
Rubicon Project 1 1 17 9524 24 7846
Scorecard Research 1 1 96 35762 90 12758
Smart AdServer 3 2 35 13345 45 6116
SpotXchange 3 2 59 14418 49 14522
SSDP 4 1 0 0 287 43911
SSL 3 3 6029 4347809 5173 1029629
Taboola 3 2 2177 2715316 1082 123164
TCP 3 1 169 37436 194 26160
The Trade Desk 3 1 101 67145 67 13168
Turn 1 1 71 31424 81 9438
Twitter 3 4 867 1040706 593 73816
UDP 3 1 0 0 62 10664
Ultrasurf 2 2 31 10286 19 1848
WhatsApp Media Mess 2 2 145 167080 135 10680
WhatsApp 2 2 404 55846 341 34602
Xiaomi 3 1 1244 718018 1376 285219
Yahoo 3 3 204 77608 251 48694
YouTube 1 4 11031 13254451 7129 1156065

```

- **Time frame:** This gives information about the application seen in last the duration (for example, 1 day).

- For low-risk numbers, the productivity is high and vice versa. (example, for GitHub (shown in the below figure) the risk index number is 1 and the productive index is 4, this means the application is low risk and more productive).

```
(config)# show application-statistics by-application time-frame 86000
Applications Count = 24
Application Statistics for All Applications
```

Protocol or Application	Productivity Index & Risk		TX Packets	TX Bytes	RX Packets	RX Bytes
Ad Analytics	4	1	4	220	3	231
Amazon	2	1	75	31437	69	8337
Bonjour	4	1	17	1956	15	1810
Doubleclick	1	1	84	30190	65	12228
Google Ads	3	1	103	47136	78	12223
Google Analytics	4	1	13	3750	15	1711
Google APIs	3	1	4713	6288091	892	153251
Google	3	1	2544	3248915	568	48664
Google Play	3	1	393	405374	221	20638
Mozilla	3	1	117	67446	104	12051
NetBIOS NS	1	3	0	0	12	936
NTP	1	3	3	228	3	228
OCSP	3	1	63	6404	71	5247
OpenX	1	1	32	8374	27	3507
Quantcast	1	1	14	4733	17	2341
Rapleaf	3	1	19	6745	19	2288
Reddit	3	1	1262	1482390	795	82476
Scorecard Research	1	1	26	5876	27	2748
SSDP	4	1	585	259542	36	7200
SSL	3	3	226	136435	176	22509
TCP	3	1	3006	1709704	2311	467655
Twitter	3	4	79	53301	68	7532
Wikipedia	3	3	19	3126	28	3873
YouTube	1	4	128	38033	130	19369

```
ap(config)# show application-statistics by-application time-frame 86000
Applications Count = 6
Application Statistics for All Applications
=====
Protocol or Productivity TX TX RX RX
Application Index & Risk Packets Bytes Packets Bytes
-----
Bonjour 4 1 3599 704477 1067 332560
DHCP 4 1 76 25156 0 0
ICMP 3 4 43 2580 1 60
MDNS 3 1 4414 633504 86 21324
NetBIOS NS 1 3 4785 376002 0 0
UDP 3 1 38944 2648192 62 10664
```



```
ap(config)#
```

DPI CLI configuration

Users can enable Application Control globally by using the below commands:

To enable DPI support:

```
ap(config)# filter global-filter
ap(config-global-filter)# application-control
ap(config-global-filter)#
```

To disable DPI support:

```
ap(config)# filter global-filter
ap(config-global-filter)# no application-control
ap(config-global-filter)#
```

Global application policy

Per application policy

```
(config)# filter global-filter
(config-global-filter)# filter precedence 1
(config-global-filter-precedence-1)# application-control

050plus      : 050Plus
12306cn      : 12306.cn
123movie     : 123movies
126com       : 126.com
17173       : 17173.com
1fichier     : 1fichier
2345com      : 2345.com
247inc       : [24]7 Inc.
247media     : 24/7 Media
2channel     : 2channel
33across     : 33Across
360antiv     : 360 AntiVirus
39net        : 39.net
3comtsmx     : 3COM-TSMUX
3pc          : 3PC
4399com      : 4399.com
4chan        : 4chan
4shared      : 4Shared
51com        : 51.com
56com        : 56.com
58com        : 58.com.cn
914cg        : 914CG
9gag         : 9GAG
about        : about.com
abscbn       : ABS-CBN
acas         : ACA Services
accweath     : accuweather.com

XV3-8-441BCC(config-global-filter-precedence-1)# application-control youtube

deny         : Block this application
permit       : Allow this Application
set-dscp     : set dscp priority
set-qos      : set qos priority

XV3-8-441BCC(config-global-filter-precedence-1)# ication-control youtube permit

permit       : Allow this Application
```

Set per category policy

```
ap(config-global-filter-precedence-1)# category-control
```

```
collab : Collaboration
database : Database
filexfer : File-Transfer
games : Games
mail : Mail
message : Messaging
monitor : Network-Monitoring
network : Networking
other : Other
proxy : Proxy
remote : Remote-Access
social : Social-Networking
stream : Streaming-Media
vpn_tun : VPN-Tunneling
web_srvc : Web-Services
ap(config-global-filter-precedence-1)# category-control games permit
ap(config-global-filter-precedence-1)#
```

SSID application policy

```
ap(config)# filter filter-list 1
ap(config-filter-list-1)# filter precedence 1
ap(config-list-1-filter-precedence-1)# application-control facebook deny
ap(config-list-1-filter-precedence-1)#
ap(config-list-1-filter-precedence-1)# wireless wlan 1
ap(config-wlan-1)# filter-list 1
ap(config-wlan-1)#
```

CLI Configuration

```

!
filter global-filter
  stateful
  application-control
  filter precedence 1
    category-control games permit
  exit

filter filter-list 1
  filter precedence 1
    application-control facebook deny
  exit

!
lldp
lldp tx-interval 100
power policy sufficient
logging syslog 7
!
(config-filter-list-1)#

```

Custom Applications X

Custom applications allow you to configure applications with a specific IP address or a domain name, and apply filter rules, such as enable or disable traffic from these applications. By default, these applications are applied on the devices along with the AP group configuration.

After creating the custom application, when you click **Apply**, cnMaestro creates a job for devices in the AP group that has auto sync enabled. Devices in AP groups that do not have auto sync enabled, are marked as **Not in Sync**, and users must manually apply the configuration on to the devices.

To disable cnMaestro from applying the custom application configuration on the devices, clear the **Enable Custom Application** check box from the **AP Groups > Services** tab > **Application Visibility X** section.

To add a new custom application, complete the following steps:

1. Navigate to **Configuration > Wi-Fi Profiles > Custom Applications X**.

Configuration > Wi-Fi Profiles

AP Groups WLANs Association ACL Access Control Policies **Custom Applications X**

ⓘ Configure Custom Applications corresponding to an FQDN or IP Address to capture statistics or control web access. Applications are pushed to the devices along with AP Groups by default. After creating them, click the Apply button to create Auto Sync Jobs for devices under AP Groups with Auto Sync enabled. Devices under AP Groups without Auto Sync enabled will be marked as Not in Sync, and configuration needs to be pushed manually. Disable the flag "Enable Custom Application" from AP Group -> Services Tab to stop applying them.

Apply Filter(s) Managed Account: All Accounts Add New Import Delete Export

<input type="checkbox"/> Application Name	Managed Account	Enabled	Category	Productivity Index	Risk Index	FQDN/IP Address	
<input type="checkbox"/> test	Base Infrastructure	Disabled	Remote Access	Medium	High	5.6.7.8	
<input type="checkbox"/> hghkhsdckjldkj	Base Infrastructure	Enabled	Streaming Media	Medium	High	3.3.3.3	
<input type="checkbox"/> test_test	Base Infrastructure	Enabled	Custom	Low	Low	1.1.1	

Showing 1 - 3 Total: 3 10 < Previous 1 Next >

2. Click **Add New** on the **Custom Applications X** page.

The **Add Custom Application(s)** window is displayed.

Add Custom Application(s)

This interface allows to add multiple custom applications, which will be saved and pushed to the device.

Name*

Scope
Base Infrastructure
Category*
Custom

FQDN/IP Address*
Productivity Index*
Low
Risk Index*
Low

Add

No Data

Cancel
Save and Apply

Configure the following parameters:

Table 49 Custom Application Parameters


Parameter	Description
Name	<p>Specifies the name for the custom application.</p> <p>Supports a maximum of 20 characters.</p>
Scope	<p>Specifies the availability of the custom application across managed accounts.</p> <p>The following values are supported:</p> <ul style="list-style-type: none"> Base Infrastructure—Custom application is available only for the global account. It is not shared with other managed accounts. Shared—Custom application is shared across all managed accounts. It can be mapped to devices in the managed account, but it cannot be modified. To modify the configuration, it must be copied into the managed account and then updated. Managed Account—Custom application is available only for that specific managed account. <div>  <div> Note <p>Once the scope has been configured on a custom application, it cannot be modified.</p> </div> </div>
Category	<p>Specifies the category to which the application must belong.</p> <p>Select the appropriate category from the drop-down list.</p>
FQDN/IP Address	<p>Specifies the IPv4 address or the domain name of the custom application.</p>
Productivity Index	<p>Indicates how appropriate an application is useful for business purposes. The higher the rating number, the more business-oriented an application is.</p>

Table 49 *Custom Application Parameters*

Parameter	Description
Risk Index	Indicates how likely an application is to pose a threat to the security of your network. The higher the rating number, the riskier of an application is.
Enable	Select the check box to enable this custom application.

3. Click **Add**.
4. To apply this configuration on the AP, click **Save and Apply**.

**Note**

WIDS and WIPS are beta features.

This section describes the following topics:

- [Wireless Intrusion Detection Systems \(WIDS\)](#)
 - [Wireless flood detection](#)
 - [Neighbor AP detection](#)
 - [Rogue APs](#)
 - [Honeypot APs](#)
 - [Ad Hoc network detection](#)
 - [Wired Devices](#)
 - [Configuring WIDS](#)
- [Wireless Intrusion Prevention System \(WIPS\)](#)

Wireless Intrusion Detection Systems (WIDS)

Wireless Intrusion Detection Systems (WIDS) is a powerful feature within cnMaestro that helps administrators monitor and protect their wireless networks from unauthorized access and potential security threats. WIDS works by continuously scanning the wireless spectrum to detect and mitigate potential intrusions, ensuring the integrity and security of your network infrastructure.

Wireless flood detection

Wireless flood detection helps in identifying and mitigating flood attacks in wireless networks. A flood attack occurs when a rogue client sends a large number of packets of a specific type to the AP to disrupt the normal working of the AP. This feature can detect the following types of flood attacks:

- Association
- Authentication
- Disassociation
- Deauthentication
- Extensible Authentication Protocol over LAN (EAPoL)

CLI configuration:

```

ap(config)# wids
association-flood : Detect floods of client associations from clients
authentication-flood : Detect floods of client authentication from
clients
deauthentication-flood : Detect floods of clients deauthentications from
clients
disassociation-flood : Detect floods of client disassociations from
clients
eap-flood : Detect floods of EAP messages from clients
num-of-minutes : Configure time duration for flood detection
num-of-packets : Configure threshold of flood packets

```

Neighbor AP detection

The AP can detect all neighbor APs. By default, all neighbors in the home channel are detected. To detect neighbors in all channels, go to **Radio > Basic > Off Channel Scan** and select the **Enable** check box.



Note

Off Channel Scan is not required for XV3-8 platforms because they have inbuilt radio for monitoring.

Rogue APs

Rogue APs are unauthorized APs that are not onboarded to cnMaestro, which may include Cambium or non-Cambium devices causing interference. The authorized or onboarded APs scan all available channels and collect details about neighboring APs. They send this information to cnMaestro for monitoring and management.

CLI configuration:

To enable rogue AP detection:

```

ap(config)# wids
rogue-ap-detection : Enable unsanctioned AP detection

```

Honeypot APs

Honeypot APs are unauthorized APs that advertise the same SSID as managed or onboarded APs. Detecting and monitoring these APs is crucial to prevent threats to the network infrastructure.

Ad Hoc network detection

A wireless Ad Hoc network is a type of Local Area Network (LAN) that is built spontaneously to enable two or more wireless devices to be connected to each other without requiring typical network infrastructure equipment, such as a wireless router or AP.

CLI configuration:

To enable ad hoc network detection:


```
ap(config)# wids
ad-hoc-detection : Detect ad-hoc networks
```

To display ad hoc networks:

```
ap(config)# show wids adhoc-networks
```

Wired Devices

The Wired Devices section within cnMaestro provides administrators with insights into the wired devices connected to the network infrastructure. This feature allows administrators to monitor and manage wired devices effectively to ensure optimal network performance and security.

CLI configuration:

To enable wired devices discovery:

```
ap(config)# wids
wired-neighbour-discovery : Enable wired neighbour discovery
```

Configuring WIDS

To enable WIDS feature perform the following steps on the cnMaestro UI:

1. Navigate to **Configuration > Wi-Fi Profiles > AP Groups** tab.
2. Select the **AP Group** and navigate to the **Security** page.
3. Select the **Enable Wireless Intrusion Detection System (WIDS)** checkbox.

Figure 63 Configuring WIDS

4. In the **Wireless Flood Detection** section, configure the number of packets and duration from the **Packets** and **Per Minutes** drop-down lists.

This indicates the number of flood attack packets that cnMaestro must detect in the specified duration to identify and report the type of attack.

5. Select the type of flood attack detection types that you want to configure in the **Wireless Flood Detection** section.

Table 50 Wireless Flood Detection parameters

Field	Description
Association	Detect floods of client associations from clients.
Authentication	Detect floods of client authentication from clients.
Deauthentication	Detect floods of client deauthentications from clients.
Disassociation	Detect floods of client disassociations from clients.
EAP	Detect floods of EAP messages from clients.

Wireless Intrusion Prevention System (WIPS)

WIPS is a critical feature within cnMaestro designed to enhance the security of wireless networks. When enabled, WIPS triggers Wi-Fi devices to deauthenticate rogue APs and clients by sending spoofed

deauthentication messages to the rogue APs and clients. You can also trigger Wi-Fi devices to deauthenticate honeypot APs and clients by enabling this feature.

CLI configuration:

To configure AP to detect honeypot and rogue APs, and send deauth requests to respective connected clients:

```
ap(config)# wips
deauth-honeypot-clients : Detect honeypot APs and send deauth to
respective clients
deauth-rogue-ap-clients : Detect rogue APs and send deauth to respective
clients
```

Configuring Services

This chapter describes the following topics:

- [Overview](#)
- [Configuring services](#)

Overview

This chapter gives an overview of Enterprise Wi-Fi AP configurable parameters related to User Groups, Location API, Speed Test, BT Location API, Bonjour Gateway, LACP, and RTLS.

Configuring services

This section provides information on how to configure the following services on Enterprise Wi-Fi AP.

To configure the services for the AP, complete the following steps:

1. Navigate to **Configuration > Wi-Fi Profiles > AP Groups** page.
2. Click **Add New** and select **Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)** from the **Type** drop-down list.
3. Click **Services** tab and configure the following services:
 - [Lightweight Directory Access Protocol \(LDAP\)](#)
 - [NAT Logging](#)
 - [User Groups](#)
 - [Wi-Fi API](#)
 - [Bluetooth API](#)
 - [Speed Test](#)
 - [DHCP Option 82](#)
 - [Bonjour Gateway](#)
 - [Link Aggregation Control Protocol \(LACP\)](#)
 - [Real-Time Location System \(RTLS\)](#)

Lightweight Directory Access Protocol (LDAP)

The following table lists the fields that are displayed in the **AP Groups > Services > Network > LDAP** page.

Table 51 LDAP parameters

Parameters	Description	Range	Default
Server Host	IP address or hostname of the LDAP server.	–	–
Server Port	Port number of the LDAP server.	–	–

To configure the above parameter, navigate to the **Configure > Services > LDAP** tab and provide the details as given below:

1. Enter the IP address of the LDAP server in the **Server Host** text box.
2. Enter the Port address of the LDAP server in the **Server Port** text box.
3. Click **Save**.

Figure 64 LDAP parameters

The figure shows two screenshots of the LDAP configuration interface. The top screenshot shows the 'Network' tab with the 'LDAP' sub-tab selected. It contains two input fields: 'Server Host' with a hint 'LDAP server IP address' and 'Server port' with a hint 'LDAP server port'. The bottom screenshot shows the 'LDAP' tab with two input fields: 'Server Host' with a hint 'Configure LDAP server IP address' and 'Server Port' with a hint 'Configure LDAP server port address'.

NAT Logging

NAT logging is same as the internet access log that is generated when NAT is enabled on AP. Each internet access log PDU consists of one or more internet access log data in TLV format. The packet format for the internet access log PDU is defined as below:

Table 52 PDU type code: 0x82

Type	Mandatory	Length	Default Value
0x01	N	32 Bytes	Includes IPv4 internet access log data structure.

Type 0x01 TLV includes the internet access log data structure as below:

Table 53 NAT Logging packet structure

Length	Description
4 Bytes	NAT records UNIX time stamp which generates time in seconds from 1970-01-01 (00:00:00 GMT until now).
6 Bytes	The MAC address of the client.
1 Bytes	Reserved for future use.
1 Bytes	The protocol type. The supported protocol types are: <ul style="list-style-type: none"> • 0x06 TCP • 0x11 UDP
2 Bytes	The VLAN ID where the client is connected. If there is no VLAN ID, the value will be 0.
4 Bytes	The client internal or the private IP address.
2 Bytes	The internal port of the client.
4 Bytes	The Internet IP address which is translated by NAT.
2 Bytes	The Internet port which is translated by NAT.
4 Bytes	The IP address of the visited server.
2 Bytes	The port address of the visited server.

Below table lists the fields that are displayed in **AP Groups > Services > Network > NAT Logging** page.

Table 54 NAT Logging parameters

Parameters	Description	Range	Default
Enable	Provision to enable/disable NAT logging services.	–	–
Server IP	Provision to configure IP/Hostname of NAT logging server.	–	–
Server Port	Provision to configure custom port number for NAT Logging services.	–	–
Interval	Provision to configure frequency of logging.	5-3600	5

Figure 65 NAT Logging parameters

The screenshot shows the configuration interface for NAT Logging. It includes a sidebar with 'Network' and 'NAT Logging' sections. The 'NAT Logging' section is expanded, showing a checkbox for 'Enable' which is checked. Below it are input fields for 'Server IP', 'Server Port', and 'Interval'. The 'Interval' field is set to '5'. Each input field has a descriptive label to its right.

User Groups Premium feature

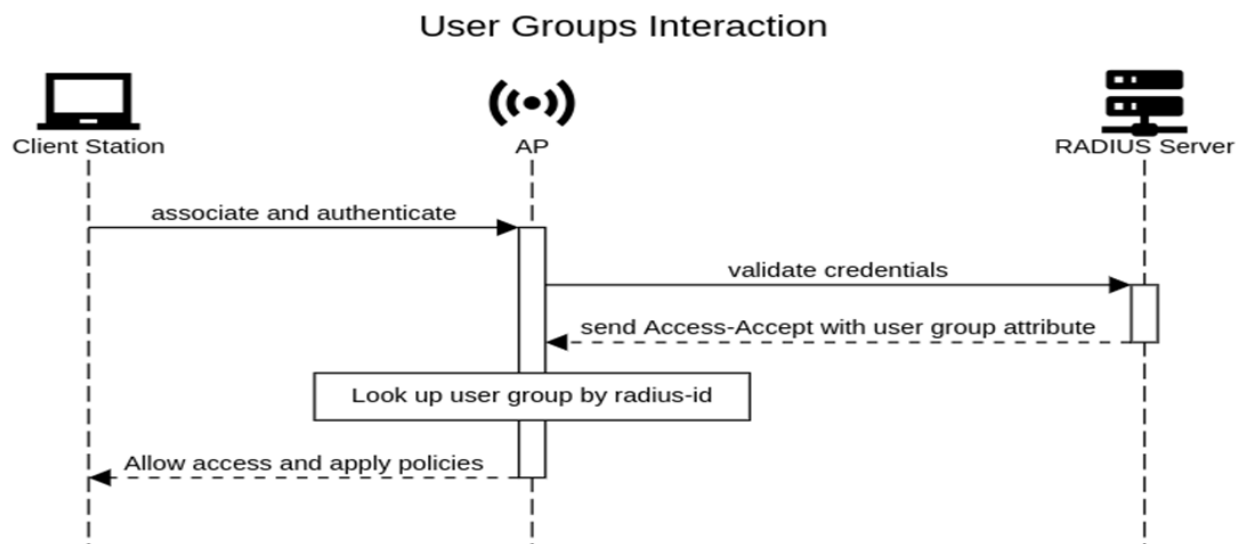
Some policies, like VLAN, require many RADIUS attributes to be sent by the RADIUS server and processed by the AP. Some wireless network administrators do not have administrative access to the RADIUS server, so making changes to wireless policies would require waiting for the RADIUS administrator to make changes.

To simplify wireless administration and streamline changes, a feature called User Groups is provided that allows the wireless administrator to apply a set of wireless policies to a user based on a single RADIUS attribute. This eliminates the need for administrative rights on the RADIUS server and simplifies applying complex policies to end-user stations.

A user group can also be assigned to a station based on the device type. This approach is dependent on the accuracy and completeness of device identification functionality, which is not guaranteed to be accurate or exhaustive.

The User Group feature is natively supported by XMS Cloud.

Figure 66 User Groups interaction



CLI Configuration:

```
ap(config)# group
Specify user group number <1-16>
ap(config)# group 1
ap(config-group-1)#
clear : Clear command
filter-list : Filter list selection for this user group
radius-id : Radius Filter-ID (Attribute Type 11) mapped to this user group
shutdown : Disable the user group
vlan : Set the vlan id for client traffic on this user group
apply : Apply configuration that has just been set
```

exit : Exit from user group configuration
no : Disable user group parameters
save : Save configuration to Flash so it persists across reboots
show : Show command
ap(config-group-1)#

Example:

```
!
group 1
 radius-id student
 vlan 40
 filter-list 1
!
group 2
 radius-id teacher
 vlan 30
 filter-list 2
!
```

User group properties and actions

A user group supports the following properties and actions:

Command	Description
shutdown	Disable this User Group
radius-id	Radius Filter-ID (Attribute Type 11) mapped to this User Group
no shutdown	Enable this User Group
no group <index>	Delete User Group

User group policies

The policies available in a user group configuration are a subset of those for an SSID. The most commonly used policies are filter-list and VLAN.

Policy	Description
filter-list <index>	Filter List setting for this User Group
vlan	VLAN associated with this User Group

Real-Time Location System (RTLS)

RTLS is a method to send the discovered (probed) clients list to a specified server address. The reports are sent as HTTP Post to the HTTP server every interval. The discovered client entries are deleted from the list if the entry is aged out. The client aging timeout is 2 times of location API interval configured. If there are no

new probe requests from the client within 2 x location API interval time, then the client entry will be removed from the list.

The following RTLS systems are available:

- [Wi-Fi API](#)
- [Bluetooth API](#)
- [Stanley AeroScout Premium feature](#)

Wi-Fi API

Below table lists the fields that are displayed in the **AP Groups > Services Network > RTLS (Real-Time Location System) > Wi-Fi API** page.

Table 55 Wi-Fi API parameters

Parameters	Description	Range	Default
Enable	Provision to enable or disable Wi-Fi API services.	-	-
Server URL	Provision to configure HTTP or HTTPS server to send a report with the port number.	-	-
Interval	Provision to configure the custom frequency of information to be shared on server.	2-3600	5
Ignore Anonymized MACs	Avoid populating locally administrated MAC addresses in the Wi-Fi API client list.	-	-

Figure 67 Wi-Fi API parameters



Note

For further details about this feature and sample reference output, go to <https://support.cambiumnetworks.com/files/cnpilot-tech-ref/> and download **Wireless client Presence and Locationing API** document.

Bluetooth API

XV3-8/XV2-2T APs with an integrated Bluetooth Low Energy (BLE) radio can detect and locate nearby BLE devices. This data is then provided via API to third-party applications. Examples of such devices include smartwatches, battery-based beacons, Apple iBeacons, fitness monitors, and remote sensors.

Organizations can create use cases for indoor wayfinding and mapping, asset tracking, and more.

Below table lists the fields that are displayed in the **AP Groups > Services Network > RTLS (Real-Time Location System) > Bluetooth API** page..

Figure 68 Bluetooth API

RTLS (Real-Time Location System)

☒ Wi-Fi API

☐ Bluetooth API

☐ Enable

Server URL Port

Interval Configure Bluetooth API interval (10-3600 seconds)

Table 56 Bluetooth API parameters

Parameters	Description	Range	Default
Enable	Enable or disable Bluetooth API services.	-	-
Server URL and Port	Configure HTTP or HTTPS server and the port number, to send a report.	-	-
Interval	Configure the custom frequency of information to be shared on server.	2-3600	5

Sending report

After enabling BLE Scanning on AP it will start processing:

1. Convert the scanned data to a JSON array.
2. Send that data in one single HTTP/HTTPS POST.

To configure the BT Location-API in the CLI:

```
ap(config)# location-api
ignore-anonymized-mac : Ignore MAC addresses that are anonymized
interval : Configure reporting interval in secs
server : HTTP/HTTPS server to send report to with the port number
```

To disable the BT Location-API:

```
ap(config)# no location-bt-api
```

Bluetooth API data elements

Table 57 Bluetooth API data elements

Parameters	Description
apMac	MAC address of the observing AP.
API Version	API Version applied for particular data format.
AP Name	Host name of the observing AP.
Timestamp	Observation time in seconds seen by AP.
BT MAC	BLE device MAC seen by AP.
UUID	BLE device UUID seen by AP.
RSSI	BLE device RSSI as seen by AP.

HTTP POST body format:

```
{
  u'ap_mac': '00-04-56-A5-5A-EC',
  'version': '2.2',
  'ap_name': 'XV3-8-EC7708',
  'ble_discoverd_clients': {Array of 0-250 devices}
}
```

Bluetooth API Data Format

```
{
  bt_rssi': u' -80 dBm ',
  bt_mac': 14-8F-21-FD-37-18', u
  'bt_uuids': Garmin International, Inc. (0xfelf)\n',
  'bt_timestamp': u' 1.811127'
}
```

Stanley AeroScout [Premium feature](#)

The Location Engine delivers accurate and reliable location data for assets and customers with STANLEY Healthcare Wi-Fi tags. It is an integral component of STANLEY Healthcare's AeroScout RTLS solutions. The AeroScout Location Engine determines location using signal strength measurements (RSSI) collected by the Cambium Wi-Fi Access Points, that can simultaneously serve location sensors and provide network access. AeroScout utilizes a location engine to determine the position of Wi-Fi tags.

CLI Configuration:

```
ap(config)# rtls aeroscout
ble-tag : Enable Aeroscout BLE Tag
server : Configure Aeroscout Server IP or FQDN
```

```
server-port : Configure Aeroscout Server Port (Default port:12092)
wifi-tag : Enable Aeroscout WiFi Tag
```

Below table lists the fields that are displayed in the **AP Groups > Services Network > RTLS (Real-Time Location System) > Stanley AeroScout** page..

Figure 69 Stanley AeroScout

Table 58 Stanley AeroScout parameters

Parameters	Description	Range	Default
<ul style="list-style-type: none">• Enable Wi-Fi• Enable Bluetooth	Enable or disable Wi-Fi or Bluetooth Stanley AeroScout services.	-	-
Server URL and Port	Configure HTTP or HTTPS server and the port number, to send a report.	-	Port: 12092

Speed Test

Wi-Fiperf is a speed test service available on Enterprise Wi-Fi AP devices. This tool is interoperable with open source zapwireless tool (<https://code.google.com/archive/p/zapwireless/>).

The Wi-Fiperf speed test can be triggered by using zapwireless tool between two Enterprise Wi-Fi APs or between Enterprise Wi-Fi APs and other third-party devices (or PC) that is having zapwireless endpoint running.

Refer to <https://code.google.com/archive/p/zapwireless/> to download the zap wireless tool to generate zapwireless endpoint for third party device (or PC) and zap CLI to perform the test.

In this case, Wi-Fiperf endpoint should be enabled in Enterprise Wi-Fi AP through UI shown below.

To configure the above parameter, navigate to the **AP Groups > Services > Network > Speed Test** page.

Select the **Wi-Fiperf** checkbox to enable the speed test.

Figure 70 Speed Test parameters

☒ **Speed Test**

☐ **Wi-Fiperf** Enable Wi-Fiperf Endpoint

DHCP Option-82

DHCP Option 82 parameter enabled at the device level with VLAN IDs inserts the Option 82 parameters in all the DHCP client packets leaving the configured VLAN interfaces. This device-level configuration precedes the DHCP Option 82 configuration at the WLAN profile or the L3 interface levels.

In case DHCP Option 82 is configured at the device-, WLAN profile-, and L3 interface-levels, the following priority order is considered:

1. Device-level configuration
2. WLAN profile-level configuration
3. L3 interface-level configuration

The device-level configuration is recommended when it is desired to insert the DHCP Option 82 for the following options:

- Guest access enabled wired traffic
- Guest and without guest access enabled wireless DHCP client traffic

To configure the above parameter, navigate to the **AP Groups > Services > Network** page and provide the details in the **DHCP Option 82** section:

1. Select the **Enable** checkbox.
2. Select the circuit ID from the **Option 82 Circuit ID** drop-down list.

Following are the supported values:

- **None**
- **All**
- **Hostname**
- **APMAC**
- **SSID**
- **VLANID**

- **SITEID**
- **Custom**

3. Select the remote ID from the **Option 82 Remote ID** drop-down list.

Following are the supported values:

- **None**
- **Hostname**
- **APMAC**
- **SSID**
- **VLANID**
- **SITEID**
- **Custom**

4. Enter the VLAN ID in the **VLAN ID** text box.

5. Click **Save**.

Figure 71 DHCP Option 82 parameter

☐ **DHCP Option 82**

☒ Insert DHCP Option 82 for all wireless and guest enabled wired clients.

Option 82 Circuit ID

None

Insert DHCP Option 82 circuitID information

Option 82 Remote ID

None

Insert DHCP Option 82 remoteID information

VLAN ID

Configure VLAN to have DHCP Option 82 (1-4094)

Bonjour Gateway

Bonjour enables the automatic discovery of devices such as printers, file servers, and other clients and services on a local network. Bonjour Gateway feature on Wi-Fi AP extends the scope of Bonjour service beyond the local network by forwarding Bonjour Multicast DNS (mDNS) packet across different VLANs, to make Bonjour services and devices available between the different wireless and local networks.

Below table lists the fields that are displayed in the **AP Groups > Services > Bonjour** page.

Figure 72 Bonjour page

Figure 73 Add Bonjour Gateway

Table 59 Bonjour Gateway parameters

Parameters	Description	Range	Default
Enable Bonjour Gateway	Provision to enable or disable Bonjour Gateway services.	-	-
Service Name	Provision for user-defined Bonjour rule name.	-	-
Proto	Select the required mDNS protocol.	-	-
From VLAN	VLAN in which mDNS/Bonjour service is running.	-	-
To VLAN	VLAN in which clients are listening.	-	-

CLI Configuration:

1. Enable Bonjour Gateway on AP.

```
ap(config)# Bonjour-gw
```

2. To configure Bonjour rule.

```
ap(config)# Bonjour-fw rules
```

```
bonjour-fw rules <sname> <proto> <vidfrom> <vidto>
```

3. To control mDNS repeated packet to WAN side.

```
ap(config)# bonjour-fw bonjour-forward-to-wan
all : Forward all bonjour mdns packets queries and response repeated
with vlan to WAN side
queries : Forward bonjour mdns Query packets repeated with vlan to
WAN side
responses : Forward bonjour mdns Response packets repeated with vlan
to WAN side
```



Note

1. By default, mDNS repeated will not send to the WAN side.
2. WAN side indicates Eth 1 interface, Mesh client interface in case of mesh client mode, tunnel interfaces like L2GRE, and L2TP.

Link Aggregation Control Protocol (LACP)

LACP provides the ability to group multiple physical ports as a logical port. This logical port is referred to as port-channel and supported only on XV3-8 devices. LACP is a dynamic protocol used to form and maintain the Link aggregation between two LACP supported devices.

LACP provides the following benefits:

- Increased Bandwidth: traffic may be balanced across the member ports to provide increased aggregate throughput.
- Link redundancy: the LACP bundle can survive the loss of one or more member links.

Configuration:

To add Ethernet to port channels:

```
ap(config)# interface portchannel 1
ap(config-portchannel-1)# exit
ap(config)# interface eth 1
ap(config-eth-1)# channel-group 1
ap(config-eth-1)# exit
ap(config)# interface eth 2
ap(config-eth-2)# channel-group 1
ap(config-eth-2)#
```


Port-channel configuration:

```
ap(config)# interface portchannel 1
ap(config-portchannel-1)#
advertise : Ethernet link speed advertisement
channel-group : Ethernet member channel group
clear : Clear command
duplex : Ethernet link duplex
shutdown : Shutdown interface
speed : Ethernet link speed
switchport : Configure switch port
tunnel-mode : Enable tunnelling of wired traffic over configured tunnel
apply : Apply configuration that has just been set
exit : Exit from interface configuration
no : Disable parameters
save : Save configuration to Flash so it persists across reboots
show : Show command
```

Syntax:

```
ap(config)# interface portchannel 1
ap(config-portchannel-1)# switchport mode trunk
ap(config-portchannel-1)# switchport trunk allowed vlan 1
ap(config-portchannel-1)# switchport trunk native vlan 1
ap(config-portchannel-1)#
```

Operations

This chapter describes the following topics:

- [Overview](#)
- [Firmware upgrade](#)
- [System](#)
- [Configuration](#)

Overview

This chapter gives an overview of Enterprise Wi-Fi AP administrative functionalities, such as firmware update, System, and Configuration.

Firmware upgrade

The running software on the Cambium Enterprise Wi-Fi AP can be upgraded to newer firmware. When upgrading from the UI, the user can upload the firmware file from the browser. The same process can be followed to downgrade the AP to a previous firmware version if required. Configuration is maintained across the firmware upgrade process.



Note

Once a firmware upgrade has been initiated, you must not restart the AP or power cycle until the process completes, as this might leave the AP inoperable.

To initiate a firmware update on the AP, complete the following steps:

1. Navigate to **Monitor and Manage > System > Software Update**.
2. Select **Enterprise Wi-Fi (XE/XV/X7-Series)** from the **Device Type** drop-down list.
3. Select the appropriate firmware version from the **Versions** drop-down list.
4. From the list of devices, select the devices for which you want to update the firmware.
5. Select the time when you want to perform the update from the **Update** section.
6. Select the appropriate options from the **Job Options** section.
7. If you select multiple devices, specify how many devices must be updated simultaneously in the text box.

A maximum of 500 devices can be updated simultaneously.
8. Click **Add Software Job to <no. of devices selected> devices**.

Figure 74 Software update

System

Dashboard
Notifications
Configuration
Statistics
Reports X
Software Update
Applications X
Clients
Mesh Peers
Analytics X
Assists X

Device Type

Enterprise Wi-Fi (XE/XV/X7 Series)

Versions

7.0-r5 (X7-35X Build)

Managed Account:

All Accounts

<input type="checkbox"/> Devices	Managed Account	Status	Client Count	Active	Inactive
<input type="checkbox"/> X7-35X-B000A0	Base Infrastructure	Offline (27d 14h 18m)	N/A	7.0-b12	7.0-a27
<input type="checkbox"/> X7-35X-B000B2	Base Infrastructure	Online (2d 3h 17m)	1	7.0-r5	7.0-r3
<input type="checkbox"/> X7-35X-B000B8	Base Infrastructure	Offline (27d 20h 13...	N/A	7.0-b14	7.0-b14
<input type="checkbox"/> X7-35X-B000D0	Base Infrastructure	Offline (3d 14h 18m)	N/A	7.0-r1	7.0-b18
<input type="checkbox"/> X7-35X-B000D4	Base Infrastructure	Offline (0d 10h 53m)	N/A	7.0-r3	7.0-b16
<input type="checkbox"/> X7-35X-B000E8	Base Infrastructure	Online (3d 16h 21m)	0	7.0-a0	7.0-b15
<input type="checkbox"/> X7-35X-B000EE	Base Infrastructure	Online (8d 3h 4m)	0	7.0-b18	7.0-b17
<input type="checkbox"/> X7-35X-B000F0_MC	Base Infrastructure	Offline (2d 19h 33m)	N/A	7.0-r3	7.0-r3
<input type="checkbox"/> X7-35X-B001A4	Base Infrastructure	Offline (2d 18h 44m)	N/A	7.0-r1	7.1-a0
<input type="checkbox"/> X7-35X-B001D6	Base Infrastructure	Online (4d 14h 59m)	0	7.1-a0	7.1-a0

Showing 1 - 10 Total: 28 10 < Previous 1 2 3 Next >

Update

☒ Now
☐ Schedule

☒ Job Options

☐ Stop update on critical error
☒ Retry skipped/offline device(s) on reconnect
☐ Update both partitions
☐ Perform sequential updates within a site
☐ Perform batch updates followed by reboot

10 Devices to update in parallel (1-500)

Notes

Add Software Job to 0 device(s)
View Update Jobs

System

This section provides multiple troubleshooting tools provided by Enterprise Wi-Fi AP.

[Table 60](#) lists the fields that are displayed in the **Operations > System** tab:

Table 60 System parameters

Parameters	Description	Range	Default
Reboot	Users will be prompted with a Reboot pop-up requesting a reboot. If yes, the device will go for a reboot.	—	—
Download Tech Support	Users will be prompted with permission to download tech support from AP. If yes, the file will be saved in your default download path configured on your system.	—	—

Parameters	Description	Range	Default
Disconnect All Clients	All clients connected to both the radios will be terminated by sending a de-authentication packet to each client connected to the radios.	–	–
Flash LEDs	LEDs on the device will toggle for the configured time period (in seconds).	1-120	10
Factory Default	A pop-up window appears requesting confirmation for factory defaults. If yes, the device will delete all configurations to factory reset and reboot.	–	–

To configure the above parameter, navigate to the **Operations > System** tab and provide the details as given below:

1. Click **Reboot** for rebooting the device.
2. Click **Download Tech Support** to generate tech support from the device and save it locally.
3. Click **Disconnect All Clients** to disconnect all wireless clients.
4. Select **Flash LEDs** value from the drop-down list to flash LEDs for the given duration of time.
5. Click **Factory Default** to delete all configurations on the device.

Figure 75 System parameters

System

Reboot
Download Tech Support
Disconnect All Clients

Flash LEDs
Flash LED (1-120) seconds

Factory Default

LED Test flashing pattern

The LED test flashing pattern for the Enterprise Wi-Fi AP is as follows:

Flashing pattern (For , XV3-8, XV2-2, XV2-2T0, XV2-2T1, XE5-8, and XE3-4): **Yellow -> Green -> Amber -> Blue**

Flashing pattern (For XV2-21X, XV2-23T, and XV2-22H): **Green -> Amber -> Blue**

CLI commands:

```
ap(config)# service flash-leds
```

Number of seconds to flash <1-120> (optional: default 10sec)
ap(config)# service test leds

Troubleshoot

Overview

This chapter provides detailed information about troubleshooting methods supported by Enterprise Wi-Fi APs. Troubleshooting methods supported by Enterprise Wi-Fi AP devices are categorized as below:

- [Logging](#)
 - [Debug Logs](#)
 - [Events](#)
- [Radio Frequency \(RF\)](#)
 - [Wi-Fi Analyzer](#)
- [Packet capture](#)
- [Performance](#)
 - [Connectivity](#)
 - [Speedtest on Access Point](#)
- [XIRCON tool support](#)
 - [XIRCON tool support for Linux 1.0.0.40](#)

Logging

Enterprise Wi-Fi AP devices support multi-level logging, which will ease debug issues.

Events

Enterprise Wi-Fi AP devices generate events that are necessary for troubleshooting across various modules. Below is the list of modules, Enterprise Wi-Fi AP device generates events for troubleshooting.

- Wireless station
 - Connectivity
- Configuration updates
- RADIUS
 - Authentication
 - Accounting

- CoA
- Roaming
 - Enhanced roaming
- Auto-RF
 - Channel change
- Reboot
- Guest Access

Events are available at **Troubleshoot > Logs > Events**.

Figure 76 Events parameters

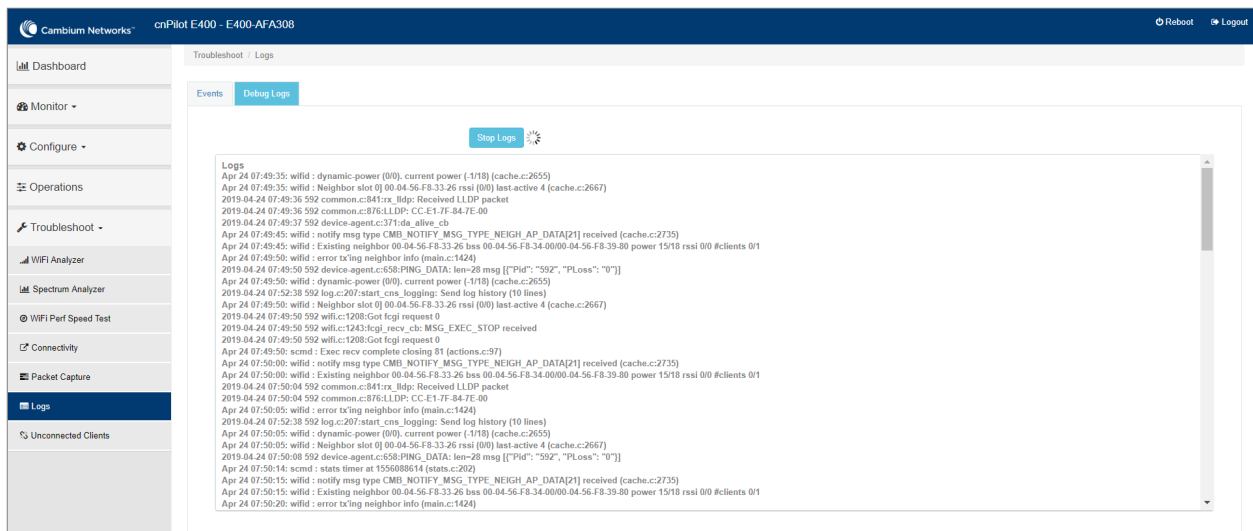
Date	Severity	Mnemonic	Message
Apr 23 07:47:12	Notice	NETWORK-RENEW-INTERFACE-IP	Renewed the interface IP on ethernet link [eth0] status move to up and running state
Apr 23 07:47:02	Notice	SYSTEM-CONFIG-APPLIED	System configuration change applied
Apr 23 07:45:50	Notice	NETWORK-RENEW-INTERFACE-IP	Renewed the interface IP on ethernet link [eth0] status move to up and running state
Apr 23 07:45:40	Notice	SYSTEM-CONFIG-APPLIED	System configuration change applied
Apr 23 07:45:28	Notice	SYSTEM-CONFIG-APPLIED	System configuration change applied
Apr 23 07:44:43	Notice	NETWORK-RENEW-INTERFACE-IP	Renewed the interface IP on ethernet link [eth0] status move to up and running state
Apr 23 07:44:32	Notice	SYSTEM-CONFIG-APPLIED	System configuration change applied
Apr 23 07:44:19	Notice	SYSTEM-CONFIG-APPLIED	System configuration change applied

Debug Logs

Enterprise Wi-Fi AP provisions enhanced debugging of each module as events generated by system and scope of debugging is limited. Debug logs can be triggered when the user clicks **Start Logs** and can be terminated when clicked on Stop Logs. By default, debug logs auto terminate after 1 minute when clicked on Start Logs.

Debug logs are available at **Troubleshoot > Logs > Debug Logs** tab.

Figure 77 Debug Logs parameters



Radio Frequency (RF)

Wi-Fi Analyzer

This tool provisions customers to scan the channels supported as per regulatory domain and provides information related to AP's presence in each channel. Wi-Fi analyzer graphs are available in two modes:

- Interference

This tool shares more information about each channel as below:

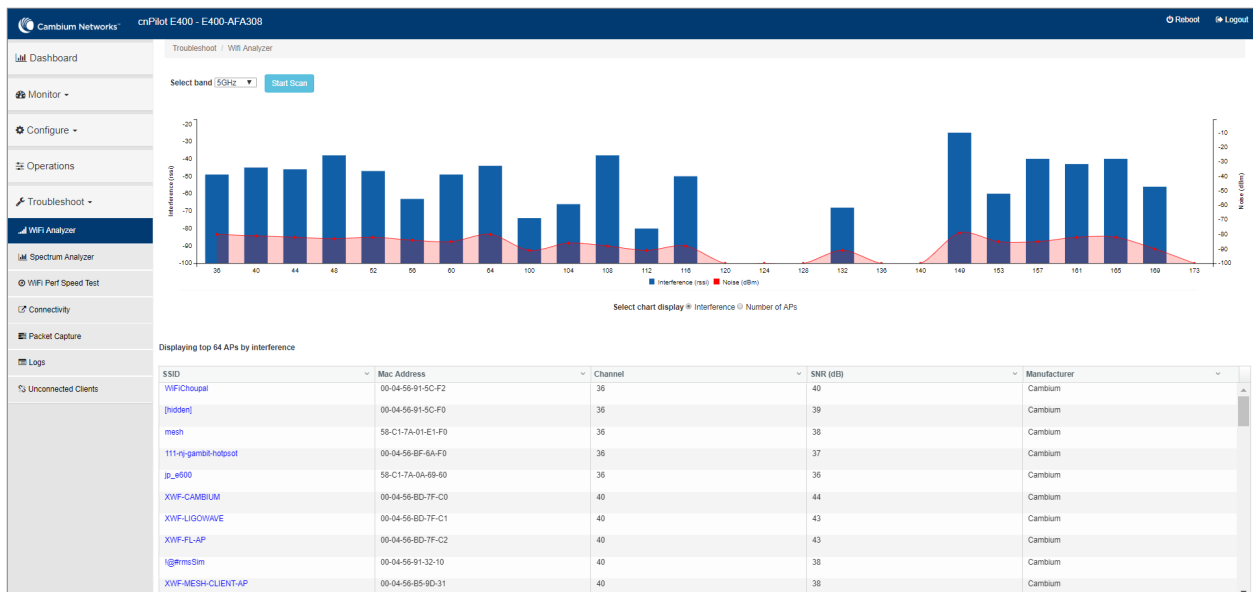
- Noise
- Interference measured in RSSI
- List of top 64 neighbor APs
- Number of APs

This tool shares more information about each channel as below:

- Noise
- Number of neighbor APs
- List of top 64 neighbor APs

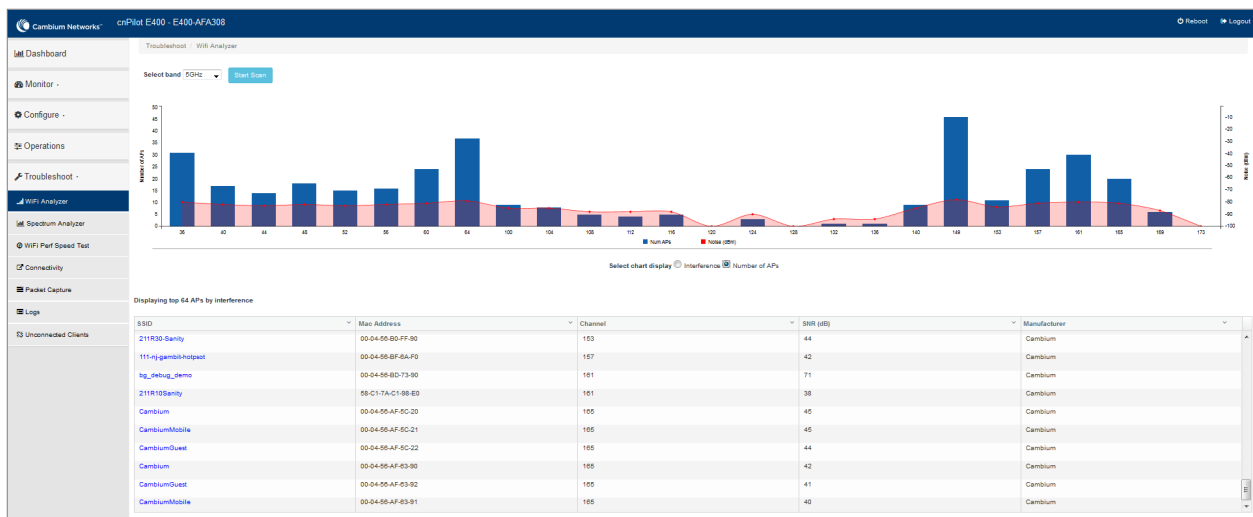
Channel analyzer is available at **Troubleshoot > Wi-Fi Analyzer > Interference Mode**.

Figure 78 Interference Mode



Channel analyzer is available at **Troubleshoot > Wi-Fi Analyzer > Number of APs Mode**:

Figure 79 Troubleshoot > Wi-Fi Analyzer > Number of APs Mode



Packet capture

Allows the administrator to capture packets from the APs UI, cnMaestro UI, or XMS-Cloud. The administrator can filter the packets being captured by specifying a particular MAC address, IP address, and port number. The user can trigger packet capture on one or more interfaces, simultaneously view the progress of the capture. The user can also download the captured pcap file on completion.

Enterprise Wi-Fi AP device allows packet capture on the following interfaces:

- Ethernet
- Radio
- Wireless LAN
- VLAN
- SSID
- Tunnel
- Bridge

Multiple options of filtering are provided and are available at **Troubleshoot > Packet Capture** page.

Figure 80 Packet Capture page

Interface: Ethernet Ex: 1

Source IP & Destination IP: Source IP Destination IP

Source MAC & Destination MAC: Source MAC Destination MAC

Direction: Both Count: Ex: 100 0 to 65535 (default 0 indicates unlimited) Duration: Ex: 120 Secs 1 to 600 (default 120) seconds

Snapslen: Ex: 9 0 to 1500 (default 0 indicates full packet length) File Size: Ex: 10 1 to 50 (default is 10 MB on 11ax APs) Filename: PCAP File Name 1 to 256 characters

Filter: Ex: icmp[empty] == 0

Start Capture

#	Interface	Status	Count	Duration	Size	Channel	Filename	Filter	StartTime	EndTime	Action
1	eth1	completed	731	15/120	854KB/10MB	NA	XV3-8-EC7708-eth1.pcap	icmp[empty] == 0	13-04-2021 19:22:55	13-04-2021 19:23:13	

Performance

Speedtest on Access Point

Speedtest can be used to measure speed across the WAN to Cambium hosted servers. The CLI output displays uplink and downlink speed in Mbps. You can also host your server in your data center and measure bandwidth to it using the ETSI option and specifying the URL. The server software can be obtained from the LibreSpeed project <https://github.com/librespeed/speedtest>.

Configuration:

Syntax:

```
ap(config)# speedtest etsi
<server url> <download MB> <upload MB> [simultaneous connections] [mbps]
```

Example:

```
XV3-8-EC7708(config)# speedtest etsi 10.110.211.19:9000 200 200
Your IP is 10.110.240.202 - private IPv4 access
Latency: 14.5ms Jitter: 1.3ms
Download: 169.53Mbps Upload: 93.93Mbps
```

Network Connectivity

This tool helps to check the accessibility of remote hosts from Enterprise Wi-Fi AP devices. The following tools are supported:

- Ping
- DNS Lookup
- Traceroute

Table 61 Troubleshoot: Connectivity

Parameters	Description	Range	Default
Ping			
IP Address or Hostname	Provide IPv4 address or Hostname to validate the reachability of the destined Host.	-	-
Number of Packets	Provide a number of request packets that are required to be transmitted to validate the reachability of the destined Host.	1-10	3
Buffer Size	Configure ICMP packet size.	1-65507	56
Ping Result	Displays the ICMP results.	-	-
DNS Lookup			
Host Name	Provide Hostname whose IP must be resolved.	-	-
DNS Test Result	Displays the IPs that are associated with configured Hostname.	-	-
Traceroute			
IP Address or Hostname	Provide IPv4 address or Hostname to validate the reachability of the destined Host.	-	-
Fragmentation	Provision to allow or deny fragment packets.	-	Off
Trace Method	Provision to configure payload mechanism to check the reachability of destined IPv4/Hostname.	-	ICMP Echo
Display TTL	Provision to customize TTL display.	-	On
Verbose	Provision to display the output of traceroute.	-	On
Traceroute Result	Displays the output of the traceroute command.	-	-

To configure the above parameter, navigate to the **Troubleshoot > Connectivity** tab and provide the details as given below:

To configure **Ping**:

1. Select **Test type** from the drop-down list.
2. Enter IP address or **Hostname** in the text box.
3. Enter the **Number of Packets** in the text box.
4. Select **Buffer Size** value from the drop-down list.
5. Click **Start Ping**.

To configure **DNS Lookup**:

1. Enter the **Hostname** in the text box.
2. Click **DNS Test**.

To configure Traceroute:

1. Enter **IP address** or **Hostname** in the text box.
2. Click **Fragmentation** to ON/Off.
3. Select **Trace Method** to either **ICMP Echo/UDP**.
4. Click **Display TTL** to ON/Off.
5. Click **Verbose** to ON/Off.
6. Click **Start Traceroute**.

Figure 81 Ping parameters

Figure 82 DNS Lookup parameters

Figure 83 Traceroute parameters

XIRCON tool support

The Xirrus console (Xircon) is a necessary tool for daily management, troubleshooting, and testing. Xirrus customers and field engineers used them for initial configuration, troubleshooting individual AP problems, changing IP addresses, and recovering units that would not boot. Since Cambium Networks acquired Xirrus and we expect the XV series APs to be deployed along with legacy Xirrus APs, limited Xircon support is added to the XV series APs.

The name "Xircon" refers to the feature in general, including the AP functionality, the communication protocol, and the client software used for discovering and controlling Xirrus APs.

- Xircon detects APs by listening for Xircon beacon packets. These packets are sent via UDP to a defined port and multicast address. These are the existing Multicast beacons sent by AOS.
- Control is established over unicast UDP on a different port from discovery. Only one client device can control an AP at any given time.

- Individual packets are RC4 encrypted. The payload includes a hash to ensure that any tampering or packet corruption is detected, and the packet discarded.
- Starting with Release 6.2, Enterprise Wi-Fi APs can be detected by Xirrus AOS APs and the Xircon client. It is not possible to establish a Xircon console connection to XV series APs – for that identify the IP address from Xircon and use standard SSH to connect.

XIRCON tool support for Linux 1.0.0.40

XIRCON tool support for Linux 1.0.0.40 has been added which is used to discover APs in the network If the IP address is not known.

Management Access

This chapter describes different methods of authenticating users to access device UI. Following are the authentication methods supported by Enterprise Wi-Fi AP devices:

- [Local authentication](#)
- [SSH Key authentication](#)
- [RADIUS authentication](#)

Local authentication

This is the default authentication mode enabled on the device. Only one username is supported which is `admin`. The default password for the `admin` username is `admin`. The user has a provision to configure or update password.

Device configuration

The below figure shows how to configure or update the default password of the `admin` user.

1. Navigate to **AP Groups > Management** section.
2. Enter the administrator password in the **Admin Password** field.
3. Click **Save**.

Figure 84 Configure/update default password of the `admin` user

SSH Key authentication

SSH keys are also used to connect remote machines securely. They are based on the SSH cryptographic network protocol, which is responsible for the encryption of the information stream between two machines. Ultimately, using SSH keys users can connect to remote devices without even entering a password and much more securely too. SSH works based on “public-key cryptography”. For simplicity, let us consider that SSH keys come in pairs. There is a private key, that is safely stored to the home machine of the user and a public key, which is stored to any remote machine (AP) the user wants to connect. So, whenever a user initiates an SSH connection with a remote machine, SSH first checks if the user has a private key that matches any of the public keys in the remote machine and if not, it prompts the user for a password.

Device configuration

SSH Key-based access method can be configured on the device from cnMaestro. Navigate to **AP Groups > Management** section and complete the following steps.

1. Select the **SSH** checkbox.
2. Provide the public key generated from the steps described in the [SSH Key generation](#) section.

Figure 85 Management parameters

AP Groups > Add New

Basic

Management

Radio

Network

Security

Access Control

Services

Administrator Access

Admin Password Configure password for authentication of GUI and CLI sessions (max 32 characters)

☐ Telnet Enable Telnet access to the device CLI

☒ **SSH** Enable SSH access to the device CLI

SSH Key Use SSH keys instead of password for authentication

☒ HTTP Enable HTTP access to the device GUI

SSH Key generation

Windows

You may use a tool, such as PUTTY to generate both public and private keys. Below is a sample demonstration of configuring Enterprise Wi-Fi AP device and logging using SSH key via UI.

1. Generate a key pair in PUTTY Key Generator as shown in .

Figure 86 Generating public/private Key

PuTTY Key Generator

File Key Conversions Help

Key

Please generate some randomness by moving the mouse over the blank area.

Actions

Generate a public/private key pair

Load an existing private key file

Save the generated key

Parameters

Type of key to generate: ☒ RSA ☐ DSA ☐ ECDSA ☐ ED25519 ☐ SSH-1 (RSA)

Number of bits in a generated key:

PuTTY Key Generator

File Key Conversions Help

Key

No key.

Actions

Generate a public/private key pair

Load an existing private key file

Save the generated key

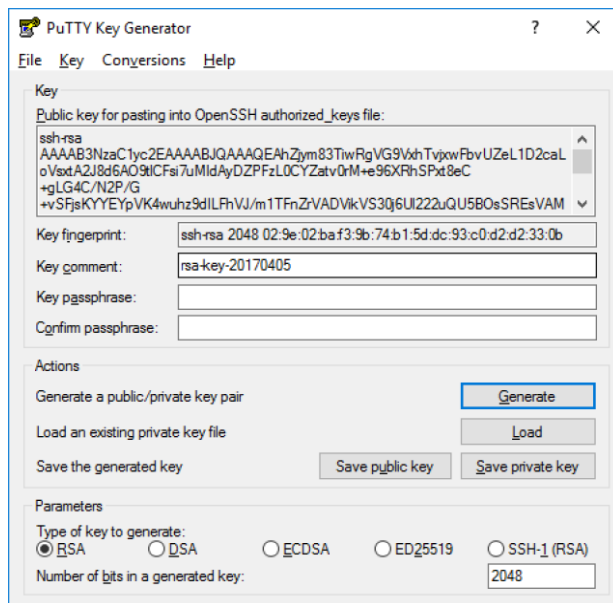
Parameters

Type of key to generate: ☒ RSA ☐ DSA ☐ ECDSA ☐ ED25519 ☐ SSH-1 (RSA)

Number of bits in a generated key:

2. Save the Public key and Private key once the key pair is generated as shown in .

Figure 87 Public and Private Key



3. Save the Public key generated in the step above as described in [Device configuration](#) section.
4. Login to device using private key generated above with username as `admin`.

Linux

If using a Linux PC and SSH from the Linux host, then you can generate the keys with the following steps:

1. Generate key pair executing below command on Linux console as shown in [Figure 88](#).

Figure 88 Public Key location path

```
pk@ubuntu:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/pk/.ssh/id_rsa):
Created directory '/home/pk/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/pk/.ssh/id_rsa.
Your public key has been saved in /home/pk/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:0qt4vJduO4uvsdptPkNzQ9uorlH7ydwE9fiEXOh0Kao pk@ubuntu
The key's randomart image is:
+---[RSA 2048]---+
|
|             ..|
|            .+.o|
|           . . .=*|
|          . S.. = o|
|         .oo*... o|
|        . .+E.. . .|
|       oo*X. + + |
|      ooBXOO. = . |
+-----[SHA256]-----+
pk@ubuntu:~$
```

2. The public key is now located in PATH as mentioned in [Figure 88](#).
PATH = "Enter the file to which to save the key"
3. The private key (identification) is now saved in PATH as mentioned in [Figure 89](#).
PATH = "Your identification has saved in <>"

Figure 89 Private Key saved path

```
pk@ubuntu:~$ cat /home/pk/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaClyc2EAAAADAQABAAQDfZq+gc13qG8DlckyfU2JqyW5pI9q8POMrVtrM9Vu5
P851kbIiCtsTmPm6Ewrfq/nhWWsn6k4p20pTZ/laX/Ww9BWf4jjw8nOqNY95z1JUD9mV48gqrOY8qbXv
5gybXLZ+A0LarSgDaeoasM34xiJEqL+/GWkJw9/ckyueliSwAeX8ki++zJeIOQZrJWcJ6mlYHZfd4Yyb
1LRg78L+q4YbHZAdkooUkTNXJ0kaBwR2i3OJjHxD1D+SRE3DrP9xAAD1lcB5MvgQNWeBJ4ale4rwkphP
QetH/lisY/DI9nkr8Hwul2JEDeMq5yII7Fdh6ALJb+b2mtZnbGBxdsM4HrTt pk@ubuntu
pk@ubuntu:~$
```

4. Save the public key generated in step above as described in the [Device configuration](#) section.
5. Login to device using private key generated above with username as admin.

RADIUS authentication

Device management access using RADIUS authentication allows multiple users to access using unique credentials and is secured.

Device configuration

Management access using the RADIUS authentication method can be configured on the device from cnMaestro. Navigate to **AP Groups > Management** and configure the following:

1. Select the **RADIUS Mgmt Authentication** check box.
2. Configure RADIUS IPv4/Hostname and shared secret in the **RADIUS Server** and **RADIUS Secret** parameters respectively.
3. Click **Save**.

Figure 90 RADIUS Server and RADIUS Secret parameters

AP Groups > Add New

Basic

Management

Radio

Network

Security

Access Control

Services

User-Defined Overrides

Administrator Access

Admin Password
[Text Field] Configure password for authentication of GUI and CLI sessions (max 32 characters)

☐ Telnet Enable Telnet access to the device CLI

☒ SSH Enable SSH access to the device CLI

SSH Key
[Text Field] Show Use SSH keys instead of password for authentication

☒ HTTP Enable HTTP access to the device GUI

HTTP Port
[Text Field: 80] Port for HTTP access to the device GUI (1-65535)

☒ HTTPS Enable HTTPS access to the device GUI

HTTPS Port
[Text Field: 443] Port for HTTPS access to the device GUI (1-65535)

☐ RADIUS Mgmt Authentication Enable RADIUS authentication of GUI/CLI sessions

RADIUS Server
[Text Field] RADIUS server IP/Hostname

RADIUS Secret
[Text Field] RADIUS server shared secret

Mesh

From Release 6.4 onwards, Enterprise Wi-Fi Access Points support mesh connections between radios. The suggested maximum hops are two. Mesh links can form between radios of the same band of operation (2.4 GHz, 5 GHz, and 6 GHz), but the two peers of the mesh link do not have to be of the same AP type. For example, a link between Wi-Fi 6 XV2-2 and XV3-8 is supported. Given the larger set of available channels and typically cleaner RF environment, Cambium Networks recommends using the 6 GHz radio for mesh backhaul if the AP is 6 GHz-capable, else use the 5 GHz band.

A mesh link can be created between two radios by configuring one of them as a Base and the other as a Client on the first WLAN of the AP. Typically, the wired connectivity AP would be configured as a Mesh Base (MB). The radio setup for the MB selects a channel and starts transmitting beacons as soon as the AP comes up. The Mesh Client (MC) radio setup scans all available channels, looking for an MB radio to connect with. The SSID in the mesh WLAN is how the client and base radios of a mesh link identify each other, the same SSID should be configured on the MB WLAN as well as the MC WLAN.

In addition to a simple topology between a base and a client, a star or hub-and-spoke mesh topology is also supported; practically a mesh radio can service up to 10-12 Mesh Clients connected to it. When a radio is configured with a mesh WLAN, on that WLAN other clients are allowed to connect, and the radio can service clients on other WLANs mapped to it. Note that a client radio starts rescanning all available channels as soon as it loses connectivity to the base. Other WLANs mapped to it are not operational during this scan period.

The mesh link can also be secured with WPA2/WPA3-Preshared-Keys (PSK). The same passphrase should be configured on both the MB as well as the MC. Standard 802.11 security handshakes and AES-CCM encryption are then used on the mesh link.

For WPA2-PSK, the maximum number of allowed characters is 64 whereas for WPA3-PSK, it is 63.

Deployment scenarios

Enterprise Wi-Fi APs support single and multi-hop mesh connections, although single hop mesh is highly advisable.

Enterprise Wi-Fi APs support the following deployment scenarios:

- Between Wi-Fi 6 APs
- Mixed deployment (between Wi-Fi 6 APs and Wi-Fi 5 APs)
- With third-party APs - TP-Link, MikroTik, and LigoWave

The following figures illustrate the working scenario of a wireless mesh network.

Figure 91 Single hop mesh connection in 5 GHz with two Mesh Clients

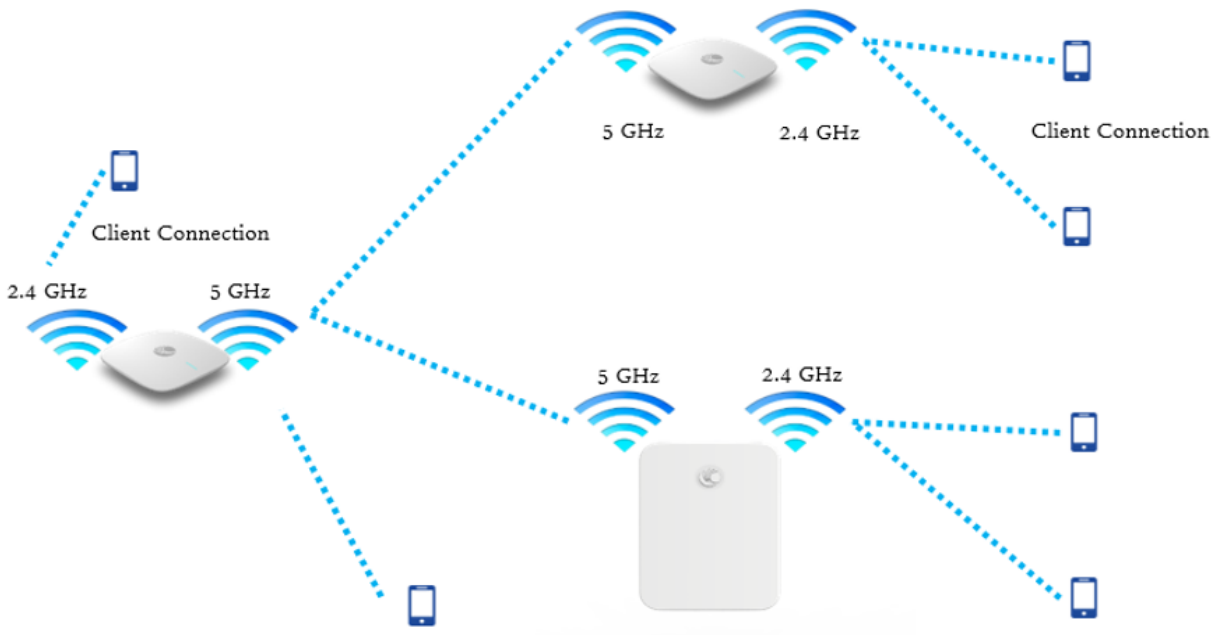


Figure 92 Single hop mesh connection in 5 GHz with two Mesh Clients and 2.4 GHz and 5 GHz as access

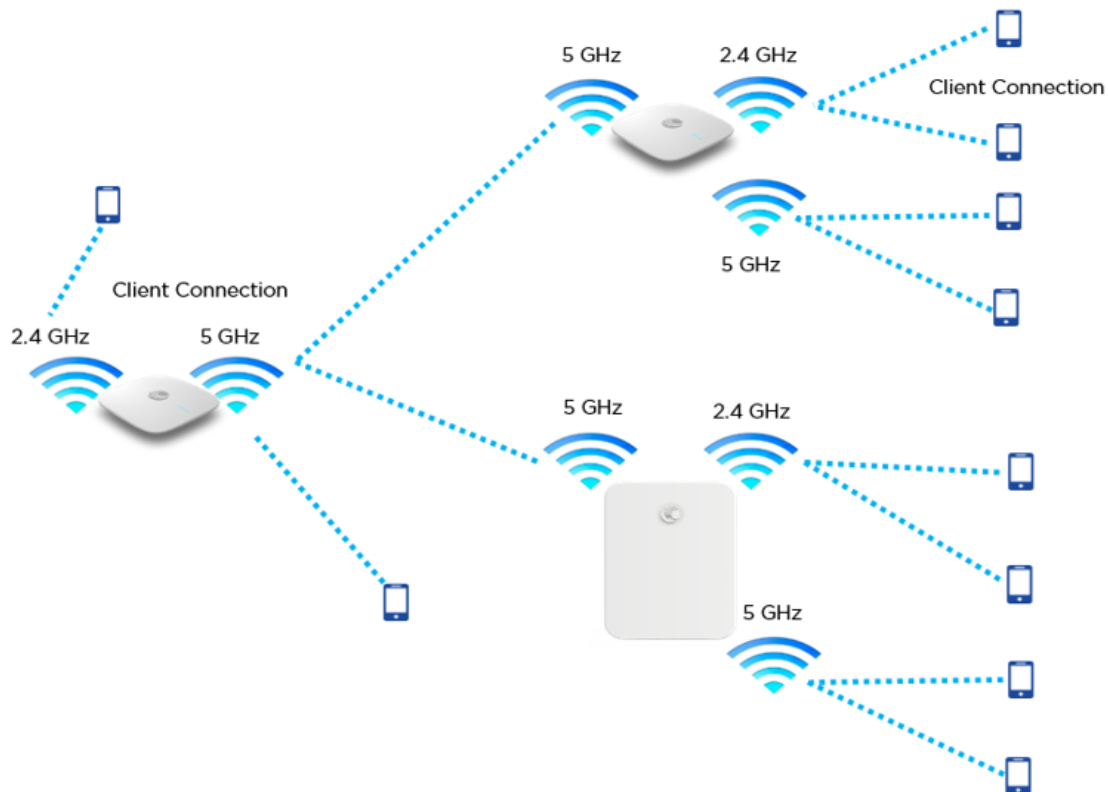
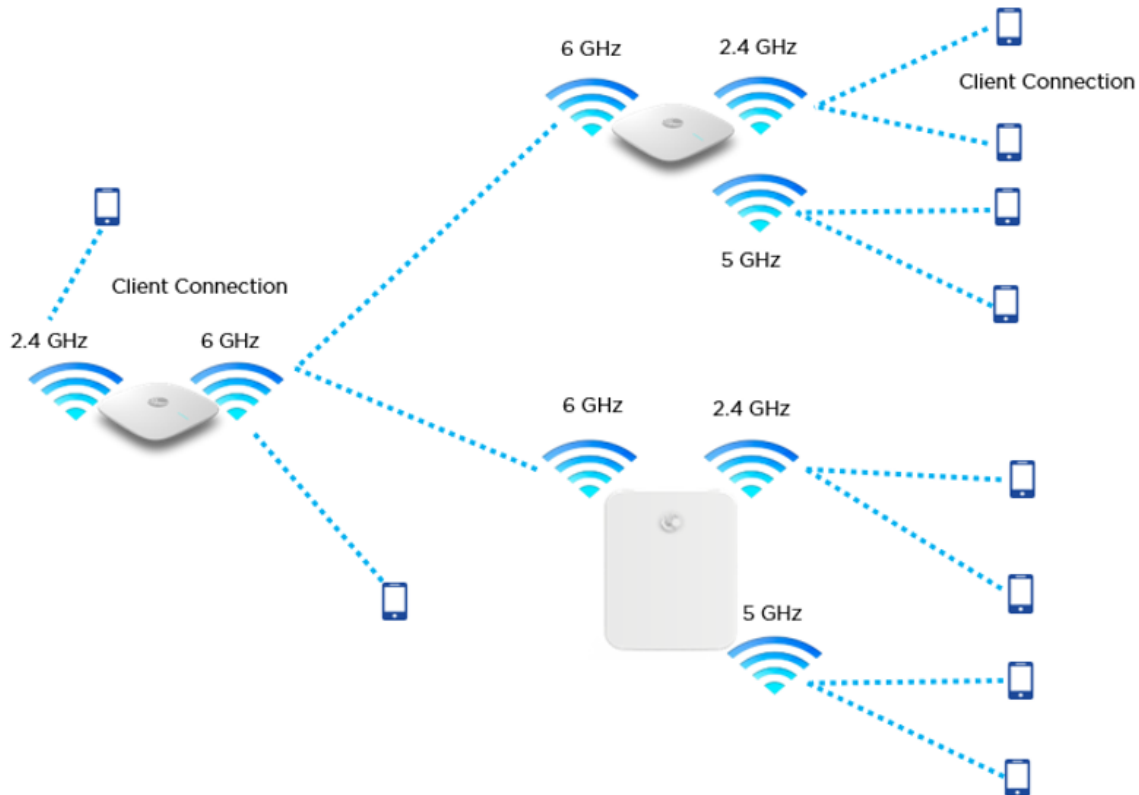


Figure 93 Single hop mesh Connection in 6 GHz with two Mesh Clients



For a stable mesh link to be established, Enterprise Wi-Fi mesh is configurable in the following three modes:

- Mesh Base (MB)

Enterprise Wi-Fi device that operates in MB mode is the key to Mesh topology. MB is usually connected to the wired network. The radio setup for MB selects a channel and starts transmitting beacons as soon as the AP comes up.

- Mesh Client (MC)

Enterprise Wi-Fi device that operates in MC mode, scans all available channels supported as per regulatory domain and establishes a link with MB.

- Mesh Recovery (MR)

When enabled, this mode helps maintain the mesh link if there is a disruption in the backhaul link established with MB and MC. Mesh link disruption can cause due to PSK mismatch or due to asynchronous configurations on MB and MC. This mode needs to be exclusively enabled on MB devices.

This mode can also help in the Zero Touch Configuration of the Enterprise Wi-Fi device.

Mesh configurable parameters

The below table lists the configurable parameters that are exclusive to mesh:

Table 62 Mesh configurable parameters

Parameter	Description	Range	Default
Mesh	<p>This parameter is required when a mesh connection is established with Enterprise Wi-Fi devices. Four options are available under this parameter:</p> <ol style="list-style-type: none"> 1. Base: A WLAN profile configured with a Mesh Base operates like a normal AP. Its radio beacon is on startup so its SSID can be seen by radios configured as Mesh Clients. 2. Client: A WLAN profile configured with a Mesh Client scans all available channels on startup, looking for a mesh-based AP to connect. 3. Recovery: A WLAN profile configured as mesh-recovery broadcast pre-configured SSID upon detection of mesh link failure after a successful connection. This needs to be exclusively configured on the mesh-base device. Mesh Client auto-scan for mesh-recovery SSID upon failure of mesh link. 	-	Off
SSID	SSID is the unique network name to which MC connects and establishes mesh links.	-	-
VLAN	Management VLAN to access all devices in a mesh topology.	1-4094	1
Security	For configurable parameters, refer to Chapter 6: Security section.	-	Open
Passphrase	A string that is a key value to generate keys based on the security method configured.	-	12345678
Radios	<p>Each SSID can be configured to be transmitted as per the deployment requirement. For a mesh WLAN profile, options available to configure the band:</p> <ul style="list-style-type: none"> • 2.4 GHz • 5 GHz • 6 GHz 	-	2.4 GHz
Hide SSID	This is the basic security mode of a Wi-Fi device. This parameter when enabled, will not broadcast SSID.	-	Disabled
SNR-threshold	Mesh Clients trigger a disconnect when SNR is below configured value. This is the applicable configuration on the MB.	1-100	Disabled
Mesh Recovery Interval	Configure the interval for the consecutive ping loss seen after which the mesh link is considered to be down and a reconnect is attempted. One can configure the duration and interval to be the same, in which case the first ping losses trigger the reconnect.	5-30 min	30

Parameter	Description	Range	Default
Mesh Auto Detect Backhaul	<ol style="list-style-type: none"> 1. Single Hop Both Mesh Client and MB profiles are configured on the devices. When enabled, this feature triggers when an MB losses Ethernet connectivity. Mesh Client profile automatically gets enabled and establishes a mesh link with the nearest MB. For the MB profile to get auto-disabled, uncheck Mesh Multi-Hop. 2. Multi-Hop Consider Mesh Client AP is connected to an MB AP which has an Ethernet backhaul connection. In case MB which has the backhaul connection loses the Ethernet connectivity, both APs disconnect from the network. When Auto detected Backhaul is enabled on the MB, it automatically enables the MC profile and connects to the nearest MB ensuring the connectivity for self as well as the client behind. Mesh Multi-Hop check should be enabled for this feature to be active. 3. Mesh Monitored Host This parameter is exclusive to Mesh Client devices when Auto-Detect Backhaul is enabled with an extended network via the Ethernet of the device. Configure IP or Hostname to check the link status. 	-	Disabled
Mesh Client Monitor	<ol style="list-style-type: none"> 1. Duration Duration in minutes of ping failure after which mesh connectivity is re-established. 2. Host Configure a server to monitor with ping to decide if mesh connectivity needs to be re-established. 	-	-
Mesh Vlan Tagging	Enable the VLAN tagging over the mesh link. This applies only to the Cambium mesh topology.	-	Enabled

Order of Mesh profile configuration

If a device is configured as Mesh Base/client/recovery, the recommended order of WLAN configuration should be as follows:

- WLAN profile 1: Mesh Base
- WLAN profile 2: Mesh Client

- WLAN profile 3: Mesh Recovery

Mesh Base (MB)

To configure the MB:

cnMaestro configuration:

The screenshot shows the 'WLANs > Ent_Mesh_Base' configuration page in the cnMaestro interface. The page is divided into two main sections: 'Basic Information' and 'Basic Settings'.

Basic Information:

- Type:** Enterprise Wi-Fi (dropdown menu)
- Name:** Ent_Mesh_Base (text input)
- Description:** (empty text input)

Basic Settings:

- SSID:**
 - ☒ Enable
 - SSID:** CAMBIUM_MESH_BASE (text input). The SSID of this WLAN (up to 32 characters)
- Mesh:**
 - Mode:** Base (dropdown menu). Mesh Base/Client/Recovery mode
- VLAN:**
 - VLAN:** 1 (text input). Default VLAN assigned to clients on this WLAN (1-4094)
- Security:**
 - Security:** WPA2 Pre-Shared Keys (dropdown menu). Set authentication and encryption type
 - Passphrase:** (password input field with a 'Show' button). WPA2 Pre-shared security passphrase or key
- Band:**
 - ☐ 2.4 GHz ☒ 5 GHz ☐ 6 GHz. Define radio types (2.4 GHz, 5 GHz, 6 GHz) on which this WLAN should be supported
- Client Isolation:**
 - Client Isolation:** Disable (dropdown menu). When selected, it allows wireless clients connected to the same AP or different APs to communicate with each other in the same VLAN
- Advanced Settings:**
 - ☐ Hide SSID. Do not broadcast SSID in beacons
 - ☒ Mesh Vlan Tagging. Enable the vlan tagging over mesh link
 - ☐ Mesh Auto Detect Backhaul. Enable the ethernet link status detection and try to connect over mesh link

CLI configuration:

```
ap(config-wlan-1)# Mesh Base
ap(config-wlan-1)# ssid CAMBIUM_MESH_BASE
ap(config-wlan-1)# security wpa2-psk
ap(config-wlan-1)# passphrase 12345678
ap(config-wlan-1)# VLAN 1
```



```
ap(config-wlan-1)# band 5GHz
```

Mesh Client (MC)

To configure the MC:

cnMaestro configuration:

WLANs > Ent_Mesh_Client

Configuration Devices

WLAN

Basic Information

Type*
Enterprise Wi-Fi

Name*
Ent_Mesh_Client

Description

Basic Settings

SSID
☒ Enable
SSID*
CAMBIUM_MESH_BASE The SSID of this WLAN (up to 32 characters)

Mesh
Client Mesh Base/Client/Recovery mode

VLAN*
1 Default VLAN assigned to clients on this WLAN (1-4094)

Security
Open Set authentication and encryption type

Transition SSID
Configure the matching open/owe transition SSID

Band
☐ 2.4 GHz ☒ 5 GHz ☐ 6 GHz Define radio types (2.4 GHz, 5 GHz, 6 GHz) on which this WLAN should be supported

☒ Mesh Vlan Tagging Enable the vlan tagging over mesh link

AP Groups > Ent_Mesh_ZeroTouch_APGrp

Dashboard Notifications Configuration Statistics Devices Clients Mesh Peers

Basic

Management

Radio

Network

Security

Services

User-Defined Overrides

User-Defined Overrides

Advanced configuration settings entered below will be applied on top of the AP Group settings sent to the device. This allows you to apply configuration not supported in the previous screens. If there are conflicts, the below settings will take precedence. The format used is the same as a configuration file exported from the device via its web UI or the "View Device Configuration" link in the device level configuration page.

Variables and Macros

ⓘ Settings entered are not validated or error-checked (However, dollar (\$), period (.) or space characters are not allowed in a variable name and it should not be more than 64 characters long), and they may overwrite configuration made in previous screens, so please use them with caution. You are responsible for ensuring the resulting AP Group is valid and safe to use.

```
!
wireless wlan 1
mesh-recovery-interval 5
mesh-client-monitor host 8.8.8.8
mesh-client-monitor duration 2
!
```

CLI configuration:

```

ap(config)# wireless wlan 1
ap(config-wlan-1)# mesh client
ap(config-wlan-1)# ssid CAMBIUM_MESH_BASE
ap(config-wlan-1)# vlan 1
ap(config-wlan-1)# security wpa2-psk
ap(config-wlan-1)# passphrase 12345678
ap(config-wlan-1)# band 5GHz
ap(config-wlan-1)# mesh-recovery-interval 30
ap(config-wlan-1)# mesh-client-monitor duration 5
ap(config-wlan-1)# mesh-client-monitor host 8.8.8.8

```

Mesh Recovery (MR)

To support plug and play Mesh deployment model, suggest configuring the MR profile on the MB AP. As a result, factory reset APs/New APs can establish a mesh connection to the MB right away (out of the box).

A recovery profile is also useful when an MC loses connectivity to a base due to misconfiguration or a bad connection that causes frequent drops.

To configure the MR:

cnMaestro configuration:

[WLANs](#) > Ent_Mesh_Recovery

Configuration **Devices**

WLAN

Access Control

Basic Information

Type*
Enterprise Wi-Fi

Name*
Ent_Mesh_Recovery

Description

Basic Settings

SSID

☒ Enable

Mesh

Recovery Mesh Base/Client/Recovery mode

VLAN*

1 Default VLAN assigned to clients on this WLAN (1-4094)

Transition SSID

Configure the matching open/owe transition SSID

Band

☐ 2.4 GHz ☒ 5 GHz ☐ 6 GHz Define radio types (2.4 GHz, 5 GHz, 6 GHz) on which this WLAN should be supported

CLI configuration:

```
ap(config-wlan-1)# mesh recovery
ap(config-wlan-1)# vlan 1
ap(config-wlan-1)# band 5GHz
```

Please refer to the [Cambium Zero touch White paper](#) on mesh for more information on Zero touch Mesh.

Mesh SNR-threshold

SNR-threshold configuration parameter is supported via CLI and can also be provisioned via cnMaestro on the MB WLAN profile. This parameter helps in maintaining the quality of the mesh link by denying MCs which has a low SNR value than the configured threshold.

cnMaestro configuration:

AP Groups > Ent_Mesh_ZeroTouch_APGrp

Dashboard Notifications Configuration Statistics Devices Clients Mesh Peers

Basic

Management

Radio

Network

Security

Services

User-Defined Overrides

User-Defined Overrides

Advanced configuration settings entered below will be applied on top of the AP Group settings sent to the device. This allows you to apply configuration not supported in the previous screens. If there are conflicts, the below settings will take precedence. The format used is the same as a configuration file exported from the device via its web UI or the "View Device Configuration" link in the device level configuration page.

Variables and Macros

Settings entered are not validated or error-checked (However, dollar (\$), period (.) or space characters are not allowed in a variable name and it should not be more than 64 characters long), and they may overwrite configuration made in previous screens, so please use them with caution. You are responsible for ensuring the resulting AP Group is valid and safe to use.

```
!
wireless wlan 7
mesh snr-threshold 60
!
```

CLI configuration:

```
ap(config-wlan-1)# mesh snr-threshold 60
```

Mesh Mode

Enterprise Wi-Fi APs support multi-radio, and by default channel distribution, is enabled. When channel distribution is enabled, each radio is mapped with a group of channels that it can operate.

When a device operates in MC, it will scan channels that are supported by the radio. Hence, there is a high possibility that MC will never connect to MB. Mesh mode configuration is supported at the RADIO level. To maintain the consistent link, the user has provision exclusively to configure mode on the radio to ensure that Mesh Clients are always connected to the network. To configure the Mesh mode:

cnMaestro configuration:

AP Groups > Ent_Mesh_ZeroTouch_APGrp

Dashboard Notifications **Configuration** Statistics Devices Clients Mesh Peers

Basic

Management

Radio

Network

Security

Services

User-Defined Overrides

Advanced configuration settings entered below will be applied on top of the AP Group settings sent to the device. This allows you to apply configuration not supported in the previous screens. If there are conflicts, the below settings will take precedence. The format used is the same as a configuration file exported from the device via its web UI or the "View Device Configuration" link in the device level configuration page.

Variables and Macros

Settings entered are not validated or error-checked (However, dollar (\$), period (.) or space characters are not allowed in a variable name and it should not be more than 64 characters long), and they may overwrite configuration made in previous screens, so please use them with caution. You are responsible for ensuring the resulting AP Group is valid and safe to use.

```
!
wireless radio 3
allowed-wlan-modes mesh
!
```

CLI configuration:

```
ap(config-radio-1) # allowed-wlan-modes mesh
```

Mesh ACL

ACL can be used to make sure that the Mesh Client connecting to the base AP is a known AP. The Mesh Client radio MAC address can be added to the Mesh Base AP to achieve this.

Following are the various modes of MAC authentication supported by Enterprise Wi-Fi APs:

- Allow

To enable this mode, add the list of MAC addresses either to be allowed or denied under “mac-authentication list <Radio MAC of Mesh Client>” and configure the device as below:

cnMaestro configuration:

MAC Authentication

Policy

☐ Deny ☒ Permit ☐ RADIUS ☐ cnMaestro

MAC	Description	Delete
00:04:56:11:22:33	Mesh client-Cambium	

[Add New](#)

Showing 1 - 1 Total: 1 10 < Previous 1 Next >

CLI configuration:

```
ap(config-wlan-1) # mac-authentication policy allow
```

- Deny

To enable this mode, add the list of MAC addresses either to be allowed or denied under “mac-authentication list <Radio MAC of Mesh Client>” and configure the device as below:

cnMaestro configuration:

MAC Authentication

Policy
☒ Deny ☐ Permit ☐ RADIUS ☐ cnMaestro

MAC	Description	Delete
00:04:56:11:22:33	Mesh client-Cambium	

[Add New](#)

Showing 1 - 1 Total: 1 10 < Previous 1 Next >

CLI configuration:

```
ap(config-wlan-1)# mac-authentication policy deny
```

- RADIUS

To enable this mode, configure the device (described in Chapter 7: Radius server section) on the MB WLAN profile as below:

cnMaestro configuration:

MAC Authentication

Policy
☐ Deny ☐ Permit ☒ RADIUS ☐ cnMaestro

Delimiter

☒ Password
☐ Upper Case

CLI configuration:

```
ap(config-wlan-1)# mac-authentication policy radius
```

- cnMaestro

To enable this mode, define the MAC addresses allowed or denied as described in the cnMaestro On-Premises User Guide Association ACL section and configure the device on the MB WLAN profile as below:

cnMaestro configuration:

MAC Authentication

Policy
☐ Deny ☐ Permit ☐ RADIUS ☒ cnMaestro

CLI configuration:

```
ap(config-wlan-1)# mac-authentication policy cnMaestro
```

Mesh Auto Detect Backhaul

Mesh Auto Detect backhaul is a mechanism to enable MB or MC WLAN profile based on the status of ethernet of a device that is operating in mesh mode. Enterprise Wi-Fi APs are multi-radio and multi-ethernet supported, hence there are multiple ways of configuring this feature based on the number of ethernet ports of a device.

In general, customers use a single AP group to configure any mesh devices in a network. When this feature is enabled, the device is intelligent enough to decide whether it has to operate in MB or MC mode. Below are different scenarios (AP2), where this feature can trigger a change in the mesh mode of the device.

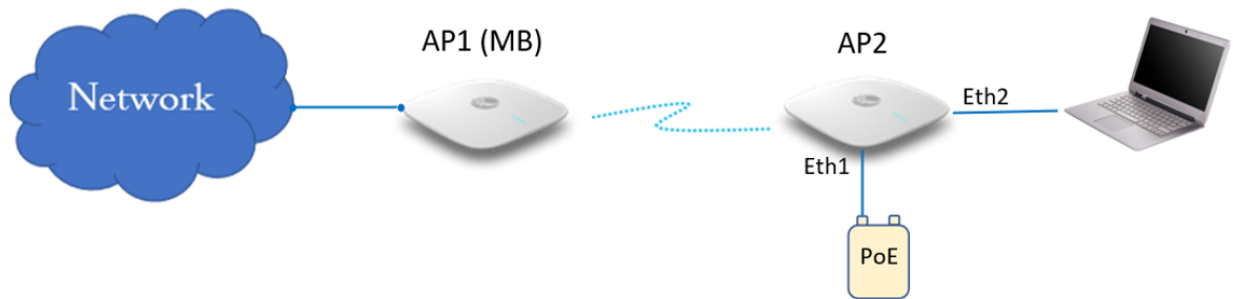
Scenario 1

When a single AP Group is used for both MB and MC, AP2 can decide its mesh mode based on eth1 and eth2 connections. To auto-trigger, the type of mesh mode below configuration needs to be pushed on all APs in the mesh link.

Based on eth1 and eth2 physical link and reachability to 8.8.8.8 determines the state of mesh mode of AP2. Below is a matrix that explains AP2 behavior:

Eth 1	Eth 2	8.8.8.8 Reachability	MB	MC
<ul style="list-style-type: none">ConnectedNo data enabled	Connected with no network reachability	No	Disabled	Enabled
<ul style="list-style-type: none">ConnectedNo data enabled	Connected with network reachability	Yes	Enabled	Disabled
<ul style="list-style-type: none">ConnectedData-enabled	Connected with no network reachability	No	Disabled	Enabled
<ul style="list-style-type: none">ConnectedData-enabled	Connected with no network reachability	Yes	Enabled	Disabled
<ul style="list-style-type: none">ConnectedData-enabled	Connected with network reachability	Yes	Enabled	Disabled

Figure 94 Deployment Scenario 1

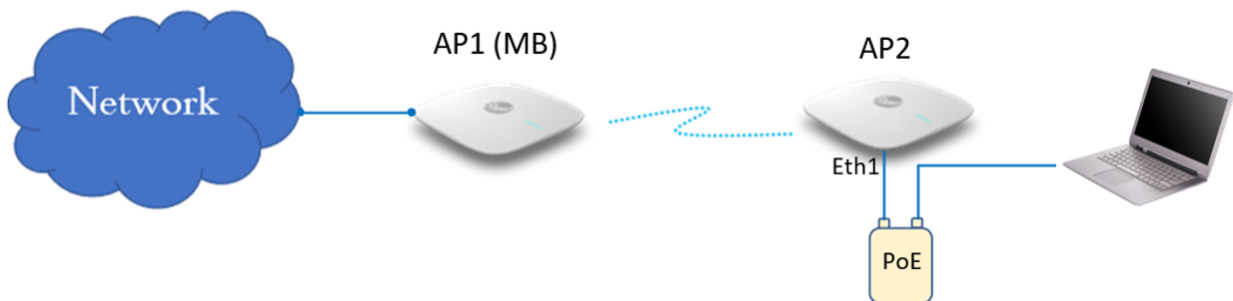


Scenario 2

When a single AP Group is used for both MB and MC, AP2 can decide its mesh mode based on eth1 connections. To auto-trigger, the type of mesh mode below configuration needs to be pushed on all APs in the mesh link.

Eth 1	8.8.8.8 Reachability	MB	MC
<ul style="list-style-type: none"> Connected No data enabled 	No	Disabled	Enabled
<ul style="list-style-type: none"> Connected Data-enabled 	No	Disabled	Enabled
<ul style="list-style-type: none"> Connected Data-enabled 	Yes	Enabled	Disabled

Figure 95 Deployment Scenario 2

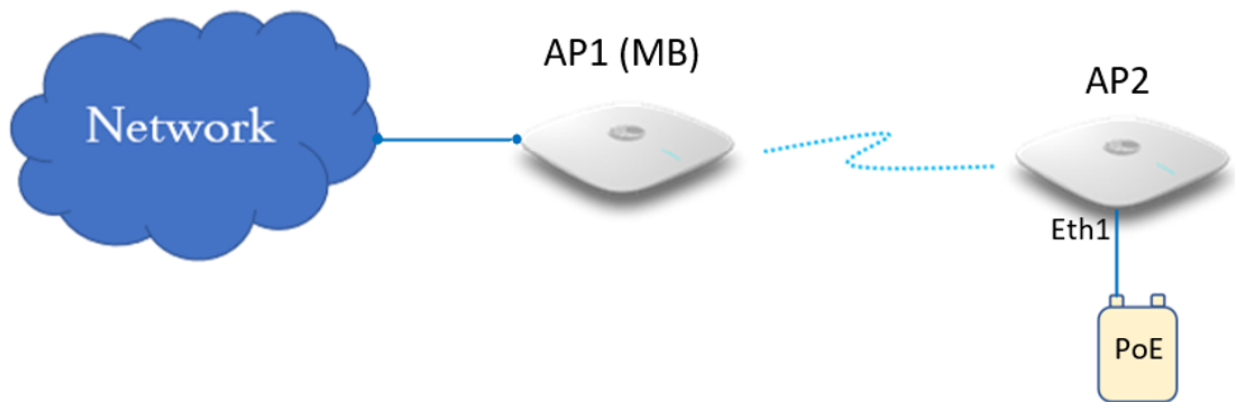


Scenario 3

When a single AP Group is used for both MB and MC, AP2 can decide its mesh mode based on eth1 connections. To auto-trigger, the type of mesh mode below configuration needs to be pushed on all APs in the mesh link.

Eth 1	8.8.8.8 Reachability	MB	MC
Connected	No	Disabled	Enabled

Figure 96 Deployment Scenario 3



To enable this configuration either from cnMaestro or CLI, follow the below guidelines:

cnMaestro configuration:

Mesh Client

WLANs > Ent_Mesh_Client

Configuration Devices

WLAN

Basic Settings

SSID

☒ Enable

SSID*

CAMBIUM_MESH_BASE The SSID of this WLAN (up to 32 characters)

Mesh

Client Mesh Base/Client/Recovery mode

VLAN*

10 Default VLAN assigned to clients on this WLAN (1-4094)

Security

WPA2 Pre-Shared Keys Set authentication and encryption type

Passphrase*

***** Show WPA2 Pre-shared security passphrase or key

Band

☐ 2.4 GHz ☒ 5 GHz ☐ 6 GHz Define radio types (2.4 GHz, 5 GHz, 6 GHz) on which this WLAN should be supported

☒ Mesh Vlan Tagging Enable the vlan tagging over mesh link

Advanced Settings

Mesh Monitored Host

8.8.8.8 IP or hostname that if not reachable a mesh recovery is attempted

Mesh Monitor Duration

30 Duration in minutes (5-60)

Mesh Recovery Interval

30 Interval in minutes after which a full recovery is attempted if the mesh base is not reachable (5-30)

Mesh Base

WLANs > Ent_Mesh_Base

Configuration Devices

WLAN

AAA Servers

Guest Access

Access Control

☒ Enable

SSID*
CAMBIUM_MESH_BASE The SSID of this WLAN (up to 32 characters)

Mesh
Base Mesh Base/Client/Recovery mode

VLAN*
10 Default VLAN assigned to clients on this WLAN (1-4094)

Security
WPA2 Pre-Shared Keys Set authentication and encryption type

Passphrase*
..... Show WPA2 Pre-shared security passphrase or key

Band
☐ 2.4 GHz ☒ 5 GHz ☐ 6 GHz Define radio types (2.4 GHz, 5 GHz, 6 GHz) on which this WLAN should be supported

Client Isolation
Disable
When selected, it allows wireless clients connected to the same AP or different APs to communicate with each other in the same VLAN

☐ Hide SSID Do not broadcast SSID in beacons

☒ Mesh Vlan Tagging Enable the vian tagging over mesh link

☒ Mesh Auto Detect Backhaul Enable the ethernet link status detection and try to connect over mesh link

☐ Mesh Multi Hop
Enable/Disable the multi-hop mesh link support. This configuration will be used if and only if mesh auto detect backhaul feature is enabled.

AP Groups > Ent_Mesh_ZeroTouch_APGrp

Dashboard Notifications Configuration Statistics Devices Clients Mesh Peers

Basic

Management

Radio

Network

Security

Services

User-Defined Overrides

User-Defined Overrides

Advanced configuration settings entered below will be applied on top of the AP Group settings sent to the device. This allows you to apply configuration not supported in the previous screens. If there are conflicts, the below settings will take precedence. The format used is the same as a configuration file exported from the device via its web UI or the "View Device Configuration" link in the device level configuration page.

Variables and Macros

ⓘ Settings entered are not validated or error-checked (However, dollar (\$), period (.) or space characters are not allowed in a variable name and it should not be more than 64 characters long), and they may overwrite configuration made in previous screens, so please use them with caution. You are responsible for ensuring the resulting AP Group is valid and safe to use.

```
!
wireless wlan 7
mesh client
band 5 ghz
fast-roaming 802.11r
mesh-auto-detect-backhaul monitor-host
!
```

CLI configuration:

Mesh Client

```
ap(config-wlan-1)# mesh client
ap(config-wlan-1)# ssid CAMBIUM_MESH_BASE
ap(config-wlan-1)# vlan 1
ap(config-wlan-1)# security wpa2-psk
ap(config-wlan-1)# passphrase 12345678
ap(config-wlan-1)# band 5GHz
ap(config-wlan-1)# mesh-client-monitor duration 5
ap(config-wlan-1)# mesh-client-monitor host 8.8.8.8
```

Mesh Base

```
ap(config-wlan-7)# mesh base
ap(config-wlan-7)# ssid CAMBIUM_MESH_BASE
ap(config-wlan-7)# vlan 1
ap(config-wlan-7)# security wpa2-psk
ap(config-wlan-7)# passphrase 12345678
ap(config-wlan-7)# band 5GHz
ap(config-wlan-7)# mesh-auto-detect-backhaul
ap(config-wlan-7)# mesh-auto-detect-backhaul monitor-host
```

Mesh Multi-Hop

This topology is not a recommended solution but can be deployed in foreseen situations. In this type of deployment, intermediate devices (AP2) in mesh links require both MB and MC to be enabled.

Figure 97 Multi-Hop deployment Scenario



cnMaestro configuration:

WLANs > Ent_Mesh_Base

Configuration Devices

WLAN

AAA Servers

Guest Access

Access Control

SSID

☒ Enable

SSID* CAMBIUM_MESH_BASE The SSID of this WLAN (up to 32 characters)

Mesh

Base Mesh Base/Client/Recovery mode

VLAN*

10 Default VLAN assigned to clients on this WLAN (1-4094)

Security

WPA2 Pre-Shared Keys Set authentication and encryption type

Passphrase*

***** Show WPA2 Pre-shared security passphrase or key

Band

☐ 2.4 GHz ☒ 5 GHz ☐ 6 GHz Define radio types (2.4 GHz, 5 GHz, 6 GHz) on which this WLAN should be supported

Client Isolation

Disable

When selected, it allows wireless clients connected to the same AP or different APs to communicate with each other in the same VLAN

☐ Hide SSID Do not broadcast SSID in beacons

☒ Mesh Vlan Tagging Enable the vlan tagging over mesh link

☒ Mesh Auto Detect Backhaul Enable the ethernet link status detection and try to connect over mesh link

☒ Mesh Multi Hop Enable/Disable the multi-hop mesh link support. This configuration will be used if and only if mesh auto detect backhaul feature is enabled.

CLI configuration:

```
ap(config-wlan-7)# mesh base
ap(config-wlan-7)# ssid CAMBIUM_MESH_BASE
ap(config-wlan-7)# vlan 1
ap(config-wlan-7)# security wpa2-psk
ap(config-wlan-7)# passphrase 12345678
ap(config-wlan-7)# band 5GHz
ap(config-wlan-7)# mesh-auto-detect-backhaul
ap(config-wlan-7)# mesh-auto-detect-backhaul monitor-host
ap(config-wlan-7)# mesh-auto-detect-backhaul multi-hop
```

Mesh Roaming

From Release 6.4 onwards Enterprise Wi-Fi APs support mesh roaming. For this functionality to be active, enable the below parameters (MB and MC) on mesh devices.

Mesh Base configuration

Enable 802.11r on the MB WLAN profile to support MC roaming.

cnMaestro configuration:

AP Groups > Ent_Mesh_ZeroTouch_APGrp

Dashboard Notifications **Configuration** Statistics Devices Clients Mesh Peers

Basic

Management

Radio

Network

Security

Services

User-Defined Overrides

Advanced configuration settings entered below will be applied on top of the AP Group settings sent to the device. This allows you to apply configuration not supported in the previous screens. If there are conflicts, the below settings will take precedence. The format used is the same as a configuration file exported from the device via its web UI or the "View Device Configuration" link in the device level configuration page.

Variables and Macros

ⓘ Settings entered are not validated or error-checked (However, dollar (\$), period (.) or space characters are not allowed in a variable name and it should not be more than 64 characters long), and they may overwrite configuration made in previous screens, so please use them with caution. You are responsible for ensuring the resulting AP Group is valid and safe to use.

```
!
wireless radio 2
mesh-client-bgscan
mesh-client-bgscan channel-list all-channels
mesh-client-bgscan roaming-rssi-threshold -65
mesh-client-bgscan long-interval 300
!
wireless wlan 1
mesh client
band 5 ghz
fast-roaming 802.11r
!
```

CLI configuration:

```
ap(config-radio-2)# mesh-client-bgscan
ap(config-radio-2)# mesh-client-bgscan channel-list all-channels
ap(config-radio-2)# mesh-client-bgscan roaming-rssi-threshold -65
ap(config-radio-2)# mesh-client-bgscan long-interval 300
ap(config-radio-2)# mesh-client-bgscan short-interval 60
```

Mesh link-Sample configuration

This section briefs about the configuration of the device to get a mesh link established with different deployment scenarios.

VLAN 1 as the management interface

Follow the below CLI commands to establish a mesh link with VLAN 1 as the management interface:

1. To configure MB and MR, following are the commands:

- WLAN MB profile

cnMaestro configuration:

WLANs > Ent_Mesh_Base

Configuration Devices

WLAN

AAA Servers

Guest Access

Access Control

SSID

☒ Enable

SSID*
CAMBIUM_MESH_BASE The SSID of this WLAN (up to 32 characters)

Mesh

Base Mesh Base/Client/Recovery mode

VLAN*
1 Default VLAN assigned to clients on this WLAN (1-4094)

Security

WPA2 Pre-Shared Keys Set authentication and encryption type

Passphrase*
..... Show WPA2 Pre-shared security passphrase or key

Band

☐ 2.4 GHz ☒ 5 GHz ☐ 6 GHz Define radio types (2.4 GHz, 5 GHz, 6 GHz) on which this WLAN should be supported

Client Isolation

Disable

When selected, it allows wireless clients connected to the same AP or different APs to communicate with each other in the same VLAN

☐ Hide SSID Do not broadcast SSID in beacons

☒ Mesh Vlan Tagging Enable the vlan tagging over mesh link

☐ Mesh Auto Detect Backhaul Enable the ethernet link status detection and try to connect over mesh link

CLI configuration:

```
ap(config-wlan-1)# mesh base
ap(config-wlan-1)# ssid CAMBIUM_MESH_BASE
ap(config-wlan-1)# security wpa2-psk
ap(config-wlan-1)# passphrase 12345678
ap(config-wlan-1)# VLAN 1
ap(config-wlan-1)# band 5GHz
```

- WLAN MR profile

cnMaestro configuration:

WLANs > Ent_Mesh_Recovery

Configuration Devices

WLAN

Access Control

Basic Information

Type*
Enterprise Wi-Fi

Name*
Ent_Mesh_Recovery

Description

Basic Settings

SSID

☒ Enable

Mesh
Recovery Mesh Base/Client/Recovery mode

VLAN*
1 Default VLAN assigned to clients on this WLAN (1-4094)

Transition SSID
Configure the matching open/owe transition SSID

Band
☐ 2.4 GHz ☒ 5 GHz ☐ 6 GHz Define radio types (2.4 GHz, 5 GHz, 6 GHz) on which this WLAN should be supported

CLI configuration:

```
ap(config-wlan-1)# mesh recovery
ap(config-wlan-1)# vlan 1
ap(config-wlan-1)# band 5GHz
```

2. To configure MC, following are the commands:

cnMaestro configuration:

WLANs > Ent_Mesh_Client

Configuration Devices

WLAN

Basic Settings

SSID
☒ Enable
 SSID* CAMBIUM_MESH_BASE The SSID of this WLAN (up to 32 characters)

Mesh
 Client Mesh Base/Client/Recovery mode

VLAN*
 1 Default VLAN assigned to clients on this WLAN (1-4094)

Security
 WPA2 Pre-Shared Keys Set authentication and encryption type

Passphrase*
 Show WPA2 Pre-shared security passphrase or key

Band
☐ 2.4 GHz ☒ 5 GHz ☐ 6 GHz Define radio types (2.4 GHz, 5 GHz, 6 GHz) on which this WLAN should be supported

☒ Mesh Vlan Tagging Enable the vlan tagging over mesh link

Advanced Settings

Mesh Monitored Host
 8.8.8.8 IP or hostname that if not reachable a mesh recovery is attempted

Mesh Monitor Duration
 30 Duration in minutes (5-60)

Mesh Recovery Interval
 30 Interval in minutes after which a full recovery is attempted if the mesh base is not reachable (5-30)

CLI configuration:

```

ap(config-wlan-1)# mesh client
ap(config-wlan-1)# ssid CAMBIUM_MESH_BASE
ap(config-wlan-1)# vlan 1
ap(config-wlan-1)# security wpa2-psk
ap(config-wlan-1)# passphrase 12345678
ap(config-wlan-1)# band 5GHz
ap(config-wlan-1)# mesh-recovery-interval
ap(config-wlan-1)# mesh-recovery-interval 30
ap(config-wlan-1)# mesh-client-monitor
ap(config-wlan-1)# mesh-client-monitor duration 5
ap(config-wlan-1)# mesh-client-monitor host 8.8.8.8

```

3. To configure the Management VLAN interface, following are the commands:

cnMaestro configuration:

The screenshot shows the 'Configuration' tab for 'Ent_Mesh_ZeroTouch_APGrp'. The left sidebar has 'Network' selected. The main area is titled 'Ethernet Ports' and contains four tabs: 'Ethernet Port 1' (active), 'Ethernet Port 2', 'Ethernet Port 3', and 'Ethernet Port 4'. Under 'Ethernet Port 1', the configuration includes: 'Ethernet Port 1' dropdown set to 'Trunk Multiple VLANs', 'Native VLAN' text box with '1', an unchecked 'Tagged' checkbox with the label 'Tag the native VLAN', 'Allowed VLANs' text box with '2-4094' and a hint 'Eg: 1-3 or 4,10,22', 'Port Speed' dropdown set to 'Auto', and 'Port Duplex' dropdown set to 'Full Duplex'.

CLI configuration:

```
ap(config)# interface vlan 1
ap(config-vlan-1)# ip address dhcp
ap(config-vlan-1)# exit
ap(config)# interface eth 1
ap(config-eth-1)# switchport mode trunk
ap(config-eth-1)# switchport trunk native vlan 1
ap(config-eth-1)# switchport trunk allowed vlan 2-4094
```

Non-VLAN 1 as the management interface

Follow the below CLI commands to establish a mesh link with non-VLAN 1 as the management interface:

1. To configure MB and MR, following are the commands:

- WLAN MB profile

cnMaestro configuration:

WLANs > Ent_Mesh_Base

Configuration Devices

WLAN

AAA Servers

Guest Access

Access Control

Basic Settings

SSID

☒ Enable

SSID* The SSID of this WLAN (up to 32 characters)

Mesh

Mesh Base/Client/Recovery mode

VLAN*

Default VLAN assigned to clients on this WLAN (1-4094)

Security

Set authentication and encryption type

Passphrase*

WPA2 Pre-shared security passphrase or key

Band

☐ 2.4 GHz ☒ 5 GHz ☐ 6 GHz Define radio types (2.4 GHz, 5 GHz, 6 GHz) on which this WLAN should be supported

Client Isolation

When selected, it allows wireless clients connected to the same AP or different APs to communicate with each other in the same VLAN

☐ Hide SSID Do not broadcast SSID in beacons

☒ Mesh Vlan Tagging Enable the vlan tagging over mesh link

☐ Mesh Auto Detect Backhaul Enable the ethernet link status detection and try to connect over mesh link

CLI configuration:

```
ap(config-wlan-1)# mesh base
ap(config-wlan-1)# ssid CAMBIUM_MESH_BASE
ap(config-wlan-1)# security wpa2-psk
ap(config-wlan-1)# passphrase 12345678
ap(config-wlan-1)# VLAN 10
ap(config-wlan-1)# band 5GHz
```

- WLAN MR profile

cnMaestro configuration:

WLANs > Ent_Mesh_Recovery

Configuration Devices

WLAN

Access Control

Basic Information

Type*
Enterprise Wi-Fi

Name*
Ent_Mesh_Recovery

Description

Basic Settings

SSID

☒ Enable

Mesh
Recovery Mesh Base/Client/Recovery mode

VLAN*
10 Default VLAN assigned to clients on this WLAN (1-4094)

Transition SSID
Configure the matching open/owe transition SSID

Band
☐ 2.4 GHz ☒ 5 GHz ☐ 6 GHz Define radio types (2.4 GHz, 5 GHz, 6 GHz) on which this WLAN should be supported

CLI configuration:

```
ap(config-wlan-1)# mesh recovery
ap(config-wlan-1)# vlan 10
ap(config-wlan-1)# band 5GHz
```

2. To configure MC, following are the commands:

cnMaestro configuration:

WLANs > Ent_Mesh_Client

Configuration Devices

WLAN

Basic Settings

SSID
☒ Enable
 SSID* CAMBIUM_MESH_BASE The SSID of this WLAN (up to 32 characters)

Mesh
 Client Mesh Base/Client/Recovery mode

VLAN* 10 Default VLAN assigned to clients on this WLAN (1-4094)

Security
 WPA2 Pre-Shared Keys Set authentication and encryption type

Passphrase* Show WPA2 Pre-shared security passphrase or key

Band
☐ 2.4 GHz ☒ 5 GHz ☐ 6 GHz Define radio types (2.4 GHz, 5 GHz, 6 GHz) on which this WLAN should be supported

☒ Mesh Vlan Tagging Enable the vlan tagging over mesh link

Advanced Settings

Mesh Monitored Host
 8.8.8.8 IP or hostname that if not reachable a mesh recovery is attempted

Mesh Monitor Duration
 30 Duration in minutes (5-60)

Mesh Recovery Interval
 30 Interval in minutes after which a full recovery is attempted if the mesh base is not reachable (5-30)

CLI configuration:

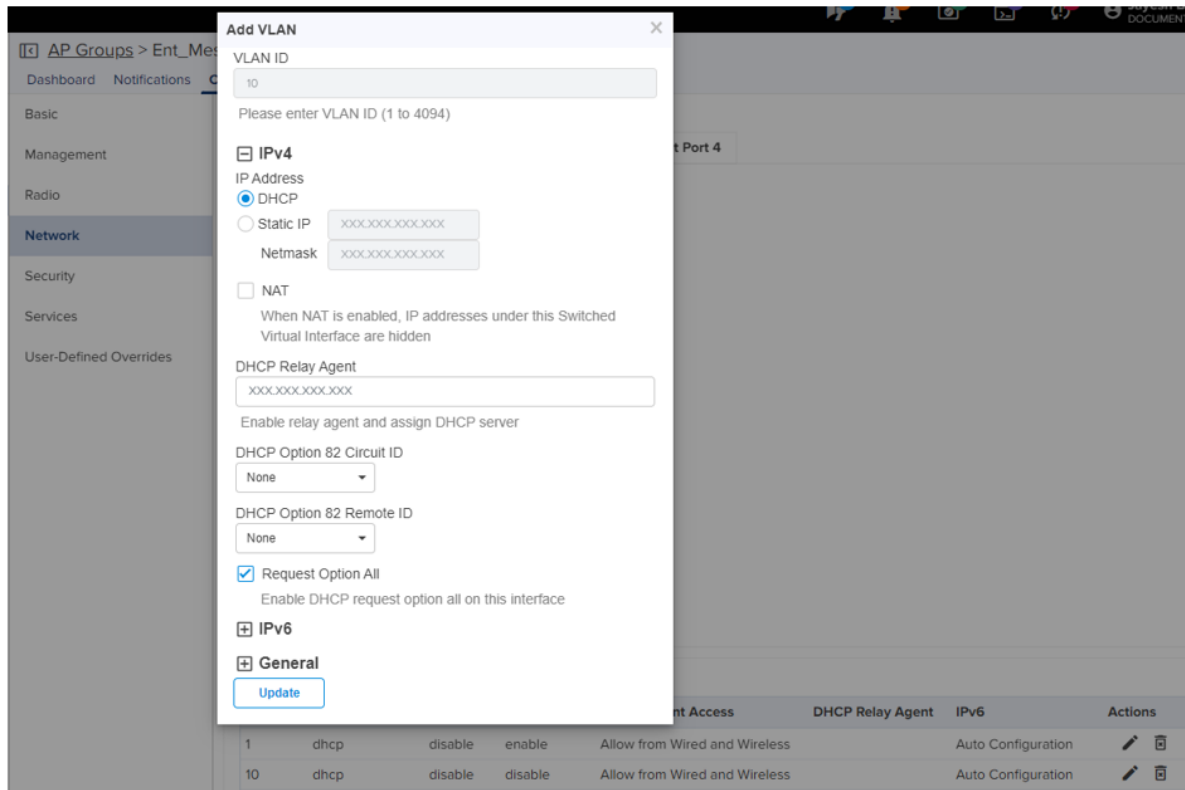
```

ap(config-wlan-1)# mesh client
ap(config-wlan-1)# ssid CAMBIUM_MESH_BASE
ap(config-wlan-1)# vlan 10
ap(config-wlan-1)# security wpa2-psk
ap(config-wlan-1)# passphrase 12345678
ap(config-wlan-1)# band 5GHz
ap(config-wlan-1)# mesh-recovery-interval
ap(config-wlan-1)# mesh-recovery-interval 30
ap(config-wlan-1)# mesh-client-monitor
ap(config-wlan-1)# mesh-client-monitor duration 5
ap(config-wlan-1)# mesh-client-monitor host 8.8.8.8

```

3. To configure the Management non-VLAN interface, the following are the commands:

cnMaestro configuration:



CLI configuration:

```
ap(config)# interface vlan 10
ap(config-vlan-10)# ip address dhcp
ap(config-vlan-10)# ip dhcp request-option-all
ap(config)# interface eth 1
ap(config-eth-1)# switchport mode trunk
ap(config-eth-1)# switchport trunk native vlan 1
ap(config-eth-1)# switchport trunk allowed vlan 2-4094
```

Typical use-cases

- Wi-Fi access in areas with no cable run
 - Add an AP indoor/outdoor APs for the areas that are difficult to reach
- Small retail location with one AP near an Ethernet outlet, and another in the middle of the lobby that has no easy cable run.

- Resolving coverage issues.
 - Plug coverage holes
- Extend range outdoors
 - An XV2-2T Hotspot in a parking lot outside a building, with XV2-2s providing Wi-Fi within the building

Additional mesh topology supported



Note

The following topology supports zero touch provisioning and single AP group configuration.



Wired devices behind mesh client AP

In this scenario, when wired devices are connected to the mesh client AP (AP2), the AP will support zero touch provisioning and both base and client APs will have the same configuration (AP group). Mesh AP must have the capability to connect a separate LAN segment (containing wired devices) to the WLAN.

When an AP, with factory default configuration, is connected in the above scenario, the device waits for 180 seconds to obtain the IP address from the wired side. If the device does not receive any IP address from the wired side, then mesh recovery is triggered. If the device restarts, the device waits for 360 seconds to obtain the IP address from the wired side. If the device does not receive any IP address from the wired side, then mesh recovery is triggered.

Guest Access Portal - Internal

Introduction

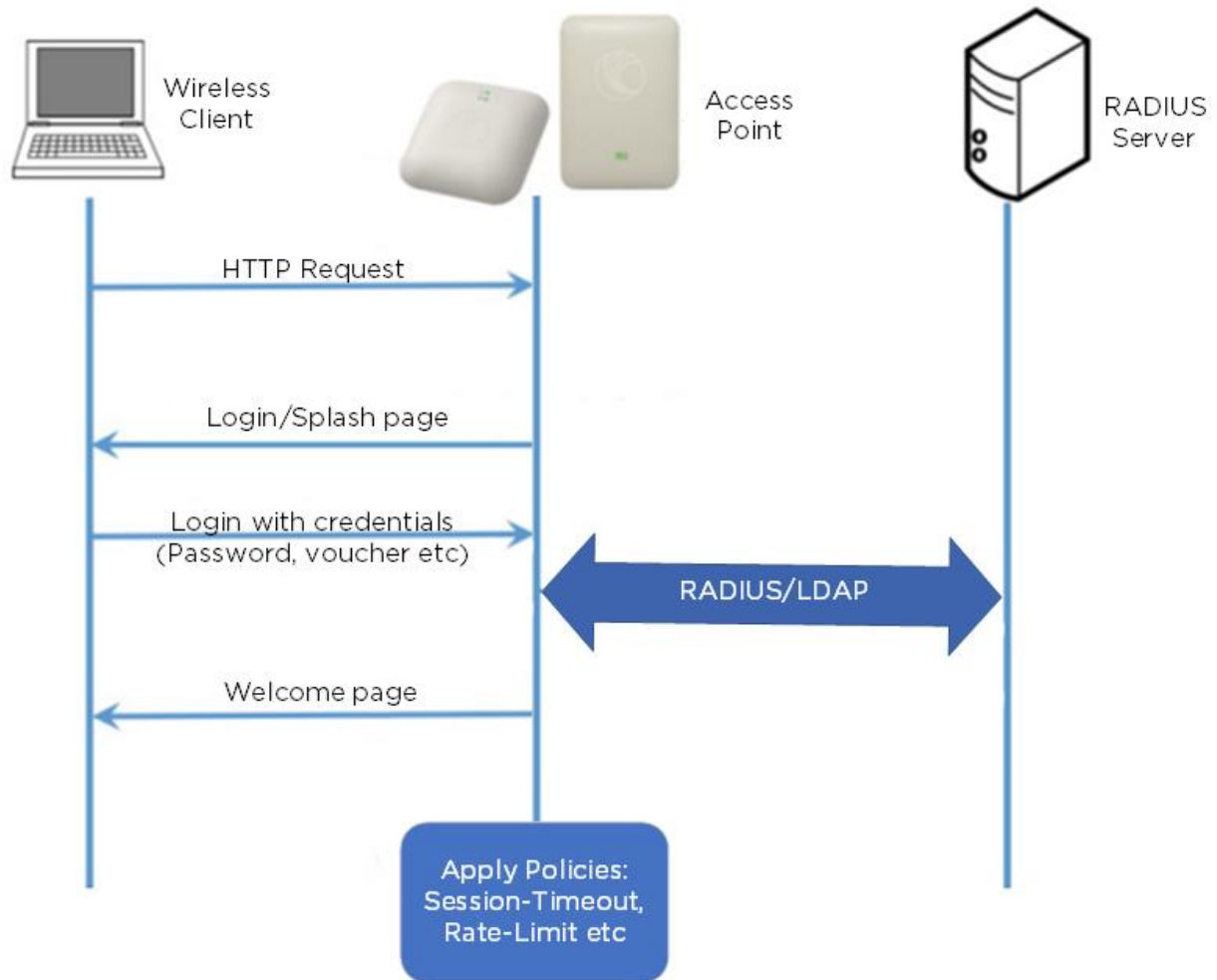
Guest Access Portal services offer a simple way to provide secure access to the internet for users and devices using a standard web browser. Guest access portal allows enterprises to offer authenticated access to the network by capturing and re-directing a web browser's session to a captive portal login page where the user must enter valid credentials to be granted access to the network.

Modes of Captive Portal Services supported by Enterprise Wi-Fi AP devices:

- **Internal Access:** Captive Portal server is hosted on the access point and is local to the AP.
- **External Access:** Enterprise Wi-Fi AP is integrated with multiple third-party Captive Portal services vendors. Based on the vendor, the device needs to be configured. For more information, see [Guest Access Portal - External](#).
- **cnMaestro:** Captive Portal services are hosted on cnMaestro where various features like Social login, Voucher login, SMS login, and Paid login are supported. For more information, see [Guest Access – cnMaestro](#).
- **EasyPass:** EasyPass Access Services enable you to easily provide secure and controlled access to users and visitors on your Wi-Fi network.

This chapter describes about Internal Captive Portal services supported by Enterprise Wi-Fi APs. The following figure displays the basic topology of testing the Internal Captive Portal Service.

Figure 98 Topology



Configurable parameters

The below figure displays multiple configurable parameters supported for Internal Guest Access hosted on AP. **Access Policy – Clickthrough.**

Figure 99 Guest Access Internal Access Point parameter

The screenshot shows the configuration page for 'WLANs > cm_test' under the 'Configuration' tab. The left sidebar lists various configuration areas: WLAN, AAA Servers, Guest Access (selected), Access Control, Passpoint, and ePSK. The main content area is titled 'Basic Settings' and includes the following sections:

- Basic Settings**
 - ☐ Enable
 - Portal Mode
 - ☒ Internal Access Point
 - ☐ External Hotspot
 - ☐ onMaestro
 - Access Policy
 - ☒ Clickthrough: Splash page where users accept terms and conditions to get on the network
 - ☐ RADIUS: Splash page with username and password, authenticated with a RADIUS server
 - ☐ LDAP: Redirect users to a login page for authentication by a LDAP server
 - ☐ Local Guest Account: Redirect users to a login page for authentication by local guest user account
 - AP Server Protocol
 - ☒ HTTP: Use unsecured HTTP protocol for AP guest access server
 - ☐ HTTPS: Use secured HTTPS protocol for AP guest access server
 - Redirect Hostname: Redirect Hostname for the splash page (up to 255 characters)
 - Title: Title text in splash page (up to 255 characters)
 - Contents: Main contents of the splash page (up to 255 characters)
 - Terms: Terms and conditions displayed in the splash page (up to 255 characters)
 - Logo: Logo to be displayed on the splash page (Eg: http://domain.com/logo.png)
 - Background Image: Background image to be displayed on the splash page (Eg: http://domain.com/backgroundimage)
 - Success Action
 - ☒ Internal Logout Page
 - ☐ Redirect User to External URL
 - ☐ Redirect User to Original URL
 - Success Message:
- Advanced Settings**
 - Redirect
 - ☒ HTTP-only: Enable redirection for HTTP packets only
 - Redirect User Page: 1111 Configure IP address for redirecting user to guest portal splash page
 - Redirection Port: Port number (1 to 65535)
 - Session Timeout: 28800 Session time in seconds (60 to 2592000)
 - Inactivity Timeout: 1800 Inactivity time in seconds (60 to 2592000)
 - ☐ MAC Authentication Fallback: Use guest-access only as fallback for clients failing MAC authentication
 - Extend Interface: Configure the interface which is extended for guest access

Access policy

Click through

When this policy is selected, the user will get a login page to accept **Terms and Conditions** to get access to the network. No additional authentication is required.

Splash page

Title

You can configure the contents of the splash page using this field. Contents should not exceed more than 255 characters.

Contents

You can configure the contents of the splash page using this field. Contents should not exceed more than 255 characters.

Terms and conditions

Terms and conditions to be displayed on the splash page can be configured using this field. Terms and conditions should not exceed more than 255 characters.

Logo

Displays the logo image updated in URL `http(s)://<ipaddress>/<logo.png>`. Either PNG or JPEG format of logo is supported.

Background image

Displays the background image updated in URL `http(s)://<ipaddress>/background/<image.png>`. Either PNG or JPEG format of logo is supported.

Redirect parameters

Redirect hostname

Users can configure a friendly hostname, which is added to the DNS server and is resolvable to Enterprise Wi-Fi AP IP address. This parameter once configured will be replaced with an IP address in the redirection URL provided to wireless stations.

Success action

Provision to configure redirection URL after successful login to captive portal services. Users can configure three modes of redirection URL:

- Internal logout Page

After successful login, the wireless client is redirected to the logout page hosted on AP.

- Redirect users to external URL

Here users will be redirected to the URL which we configured on a device as below:

- Redirect users to the Original URL

Here users will be redirected to a URL that is accessed by the user before successful captive portal authentication.

Redirect

By default, captive portal redirection is triggered when the user accesses either HTTP or HTTPS WWW. If enabled, redirection to Captive Portal Splash Page is triggered when an HTTP WWW is accessed by end-user.

Redirect Mode

There are two redirect modes available:

- **HTTP Mode**

When enabled, AP sends an HTTP POSTURL to the client.

- **HTTP(s) Mode**

When enabled, AP sends HTTPS POST URL to the client

Success message

This we can configure so that we can display success message on the splash page after successful authentication

Timeout

Session

This is the duration of time which wireless clients will be allowed internet after guest access authentication.

Inactivity

This is the duration of time after which wireless clients will be requested for re-login.

Whitelist

Provision to configure either Ips or URLs to bypass traffic, therefor users can access those IPs or URLs without Guest Access authentication.

Configuration examples

This section briefs about configuring different methods of Internal Guest Access captive portal services hosted on AP.

Access Policy – Clickthrough

Figure 100 Authentication – redirected splash page

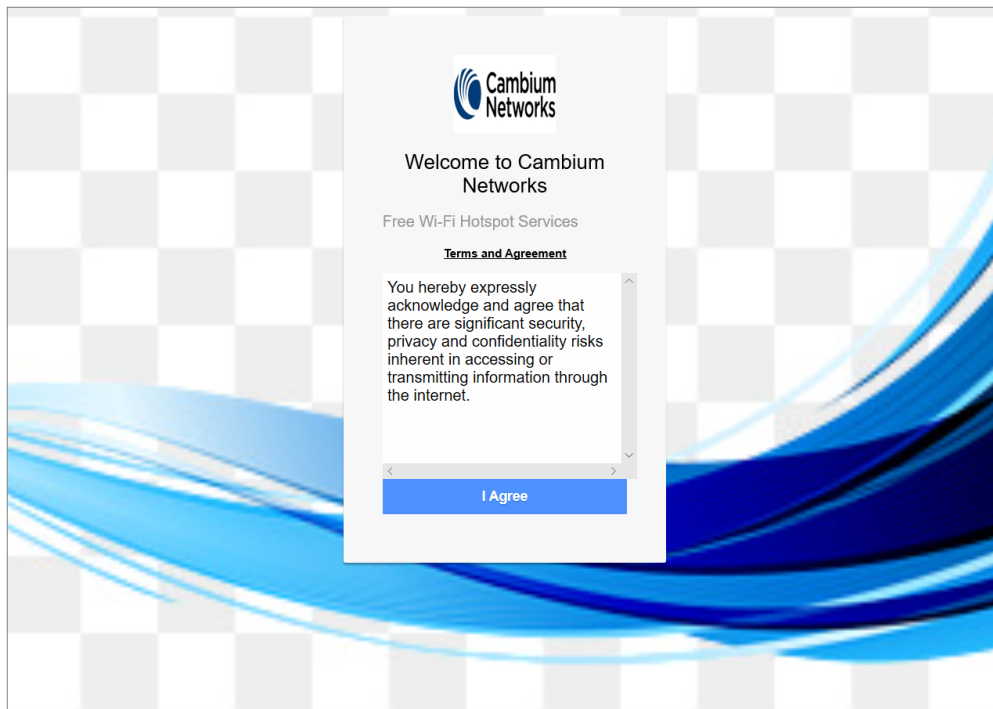
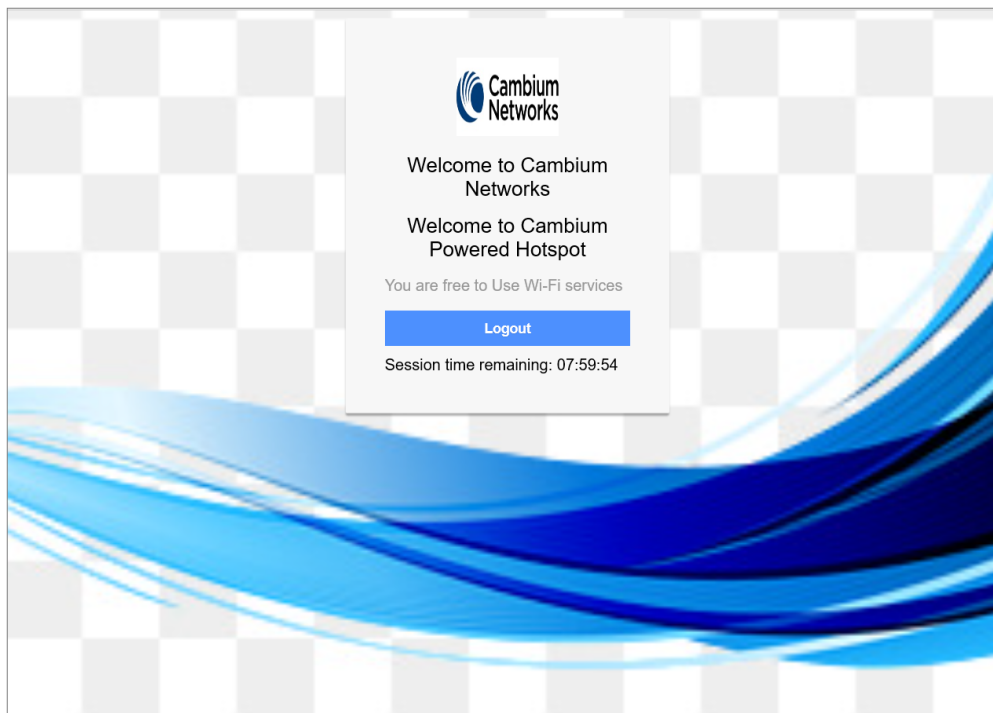


Figure 101 Successful login – redirected splash page



Guest Access Portal - External

Introduction

Guest access WLAN is designed specifically for BYOD (Bring Your Own Device) setup, where large organizations have both staff and guests running on the same WLAN or similar WLANs. Cambium Networks provides different options to the customers to achieve this based on where the captive portal page is hosted and who will be validating and performing the authentication process.

External Hotspot is a smart Guest Access provision supported by Enterprise Wi-Fi AP devices. This method of Guest Access provides the flexibility of integrating an external 3rd party Web/Cloud hosted captive portal, fully customized. More details on third-party vendors who are integrated and certified with Cambium are listed in the URL https://www.cambiumnetworks.com/wifi_partners/.

Configurable parameters

[Figure 102](#) displays multiple configurable parameters supported for External Guest Access hosted on AP.

Figure 102 External Hotspot parameter

The screenshot displays the 'Guest Access' configuration page for a WLAN named 'cm_test'. The left sidebar shows the navigation menu with 'Guest Access' selected. The main content area is divided into two sections: 'Basic Settings' and 'Advanced Settings'.

Basic Settings:

- Enable:** A checkbox that is currently unchecked.
- Portal Mode:** Three radio buttons: 'Internal Access Point' (unchecked), 'External Hotspot' (checked), and 'onMaestro' (disabled, indicated by a grey circle).
- Access Policy:** Four radio buttons: 'Clickthrough' (checked), 'RADIUS' (unchecked), 'LDAP' (unchecked), and 'Local Guest Account' (unchecked).
- AP Server Protocol:** Two radio buttons: 'HTTP' (checked) and 'HTTPS' (unchecked).
- Redirect Hostname:** A text input field with a placeholder 'Redirect Hostname for the splash page (up to 255 characters)'.
- WSPi Clients External Server Login:** A checkbox that is currently unchecked.
- External Page URL:** A text input field.
- External Portal Post Through onMaestro:** A checkbox that is currently unchecked.
- External Portal Type:** A dropdown menu set to 'Standard'.
- Success Action:** Three radio buttons: 'Internal Logout Page' (checked), 'Redirect User to External URL' (unchecked), and 'Redirect User to Original URL' (unchecked).
- Success Message:** A text input field.

Advanced Settings:

- Redirection URL Query String:** Three checkboxes: 'Client IP' (unchecked), 'RSSI' (unchecked), and 'AP Location' (unchecked).
- Redirect:** A checkbox 'HTTP-only' is checked.
- Redirect User Page:** A text input field containing '1111'.
- Redirection Port:** A text input field.
- Session Timeout:** A text input field containing '28800'.
- Inactivity Timeout:** A text input field containing '1800'.
- MAC Authentication Fallback:** A checkbox that is currently unchecked.
- Extend Interface:** A text input field.

Access policy

Clickthrough

When this policy is selected, the user will get a login page to accept **Terms and Conditions** to get access to the network. No additional authentication is required.

WISPr

WISPr clients external server login

Provision to enable re-direction of guest access portal URL obtained through WISPr.

External portal post through cnMaestro

This is required when HTTPS is only supported by an external guest access portal. This option when enabled minimizes certification. The certificate is required to install only in cnMaestro.

External portal type

Only standard mode configuration is supported by Enterprise Wi-Fi AP products.

Standard

This mode is selected, for all third-party vendors whose Guest Access services is certified and integrated with Enterprise Wi-Fi AP products.

Redirect parameters

Success action

Provision to configure redirection URL after successful login to captive portal services. Users can configure three modes of redirection URL:

- Internal logout Page

After successful login, the wireless client is redirected to the logout page hosted on AP.

- Redirect users to external URL

Here users will be redirected to the URL which we configured on the device as below:

- Redirect users to the original URL

Here users will be redirected to a URL that is accessed by the user before successful captive portal authentication.

Redirect

By default, captive portal redirection is triggered when the user accesses either HTTP or HTTPS WWW. If enabled, redirection to Captive Portal Splash Page is triggered when an HTTP WWW is accessed by end-user.

Redirect mode

There are two redirect modes available:

- HTTP Mode

When enabled, AP sends an HTTP POST URL to the client.

- HTTP(s) Mode

When enabled, AP sends HTTPS POST URL to the client

Success message

This we can configure so that we can display success message on the splash page after successful authentication

Timeout

Session

This is the duration of time which wireless clients will be allowed internet after guest access authentication.

Inactivity

This is the duration of time after which wireless clients will be requested for re-login.

Whitelist

Provision to configure either Ips or URLs to bypass traffic, therefor users can access those IPs or URLs without Guest Access authentication.

Configuration examples

This section briefs about configuring different methods of External Guest Access captive portal services hosted on AP.

Access Policy – Clickthrough

Figure 103 Authentication – redirected splash page

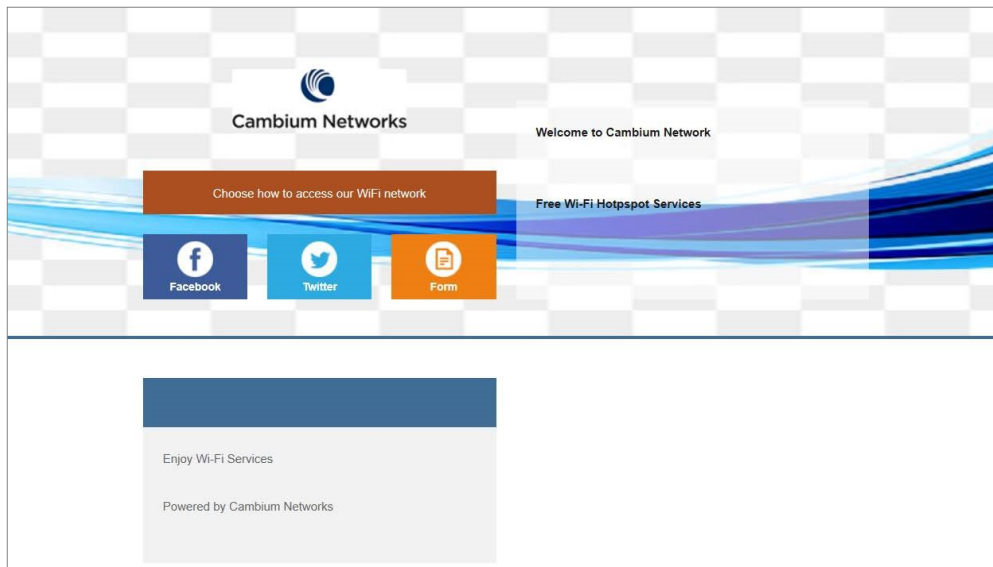
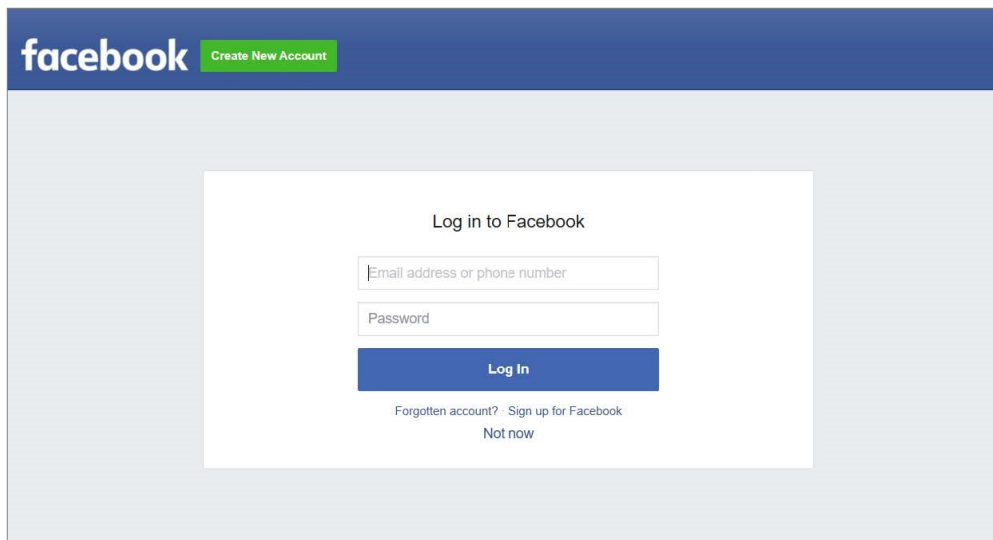


Figure 104 Successful Login – redirected splash page



Guest Access – cnMaestro

Cambium supports end-to-end Guest Access Portal services with a combination of Enterprise Wi-Fi AP and cnMaestro. cnMaestro supports various types of authentication mechanisms for wireless clients to obtain Internet access. For further information about Guest Access Portal:

- For On-Premises, go to <https://support.cambiumnetworks.com/files/cnmaestro/> and download the latest *cnMaestro On-Premises User Guide*.
- For cnMaestro Cloud, refer to the *cnMaestro Cloud User Guide*.

Auto VLAN

The Auto VLAN is intended to support zero-touch detection and configuration for connected Enterprise Wi-Fi APs. New Cambium vendor-specific LLDP TLVs are introduced starting with cnMatrix Release 3.1 to support “pushing” PBA policy data from Enterprise Wi-Fi APs to cnMatrix. The new PBA TLVs are implemented as an extension to the LLDP standard, using its flexible extension mechanism.

From a functional perspective, cnMatrix, acting as the upstream device, includes the PBA authentication TLV in the regularly generated LLDPDUs for a port. The downstream device receives the PBA authentication TLV, and, if policy action data (for example VLANs) is present to be pushed to cnMatrix, a PBA device settings TLV is constructed and added to the LLDPDU for the port.

The below table lists the fields that are required for configuring Auto-VLAN:

Table 64 Configuring Auto-VLAN parameters

Parameters	Description	Range	Default
lldp pba	New PBA TLVs is shared with cnMatrix switch.	–	Enabled
lldp pba-auth-key	The shared private key used during PBA TLV authentication can be updated or reset from its default value (by using the ‘no’ option).	–	Enabled with default key



Note

lldp pba-auth-key default value cannot be shared due to security concerns.

CLI configuration:

Syntax:

```
ap(config)# lldp
ap(config)# lldp pba-auth-key
```

Example:

```
ap(config)# lldp pba
ap(config)# lldp pba-auth-key 123456789
```

Device Recovery Methods

Factory reset via 'RESET' button

Table 65 Factory reset via RESET button

Access Point	Procedure	LED Indication
XV3-8	Press and hold the Reset button for 15 seconds	Both LEDs will be OFF and turned onto Amber
XE5-8	Press and hold the Reset button for 15 seconds	Both LEDs will be OFF and turned onto Amber
XV2-2	Press and hold the Reset button for 15 seconds	Both LEDs will be OFF and turned onto Amber
XV2-2T0	Press and hold the Reset button for 15 seconds	Both LEDs will be OFF and turned onto Amber
XV2-2T1	Press and hold the Reset button for 15 seconds	Both LEDs will be OFF and turned onto Amber
XE3-4	Press and hold the Reset button for 15 seconds	Both LEDs will be OFF and turned onto Amber
XE3-4TN	Press and hold the Reset button for 15 seconds	Both LEDs will be OFF and turned onto Amber
XV2-21X	Press and hold the Reset button for 15 seconds	Both LEDs will be OFF and turned onto Amber
XV2-23T	Press and hold the Reset button for 15 seconds	Both LEDs will be OFF and turned onto Amber
XV2-22H	Press and hold the Reset button for 15 seconds	Both LEDs will be OFF and turned onto Amber

Boot partition change via power cycle

Table 66 Boot partition change via power cycle

Access Point	Procedure
XV3-8	Follow power ON and off 9 times with an interval of 120 Sec (ON) and 5 Sec (OFF)
XE5-8	Follow power ON and off 9 times with an interval of 120 Sec (ON) and 5 Sec (OFF)
XV2-2	Follow power ON and off 9 times with an interval of 120 Sec (ON) and 5 Sec (OFF)

Access Point	Procedure
XV2-2T0	Follow power ON and off 9 times with an interval of 120 Sec (ON) and 5 Sec (OFF)
XV2-2T1	Follow power ON and off 9 times with an interval of 120 Sec (ON) and 5 Sec (OFF)
XE3-4	Follow power ON and off 9 times with an interval of 120 Sec (ON) and 5 Sec (OFF)
XE3-4TN	Follow power ON and off 9 times with an interval of 120 Sec (ON) and 5 Sec (OFF)
XV2-21X	Follow power ON and off 9 times with an interval of 120 Sec (ON) and 5 Sec (OFF)
XV2-23T	Follow power ON and off 9 times with an interval of 120 Sec (ON) and 5 Sec (OFF)
XV2-22H	Follow power ON and off 9 times with an interval of 120 Sec (ON) and 5 Sec (OFF)

Disable factory Reset Button

User can disable the physical Reset Button on the device by using the below CLI command:

```
ap(config)# no system hw-reset
```



Warning

The **Reset Button** is a key recovery option in situations when an AP gets misconfigured and you are unable to connect to the AP.

By disabling the **Reset Button**, you lose the ability to recover the AP in such scenarios.

Command-Line Interface (CLI)

The Enterprise Wi-Fi products support Command-Line Interface (CLI) which helps in configuring as well as monitoring the devices.

Show commands

The below table provides **Show commands** supported in Enterprise Wi-Fi AP:

Table 67 Show commands supported in Enterprise Wi-Fi AP

SL No	CLI Command	Description
Deep Packet Inspection (DPI)		
1	<code>show application-statistics by-application</code>	Displays statistics of each application that is accessed by the station connected to the AP.
2	<code>show application-statistics by-category</code>	Displays statistics of application category that is accessed by the station connected to the AP.
Network Information		
3	<code>show arp</code>	Displays list of ARP entries learned by AP.
4	<code>show conntrack</code>	Displays current connection track entries along with application ID Mapping.
5	<code>show route</code>	Displays IP route information.
6	<code>show dhcp-pool <Index number></code>	Displays the DHCP pool configuration.
7	<code>show interface brief</code>	Displays interface details such as IP, Netmask, and traffic statistics.
8	<code>show ip dhcp-client-info</code>	Displays the DHCP options learned by device across all interfaces.
9	<code>show ip domain-name</code>	Displays learned domain name information.
10	<code>show ip gw-source-precedence</code>	Displays the Precedence of gateway sources.
11	<code>show ip interface</code>	Displays IP interface parameters.
12	<code>show ip name-server</code>	Displays DNS server information.
13	<code>show ip neighbour</code>	Displays IPv4 neighbour entries.
14	<code>show ip route</code>	Displays IP route information.
15	<code>show ipv6 dhcp-client-info</code>	Displays learned DHCPv6 client information.

SL No	CLI Command	Description
16	show ipv6 domain-name	Displays learned domain name information.
17	show ipv6 gw-source-precedence	Displays the precedence of gateway sources.
18	show ipv6 interface brief	Displays IPv6 interface parameters.
19	show ipv6 name-server	Displays DNS server information.
20	show ipv6 neighbour	Displays neighbour entries.
21	show ipv6 route	Displays IP route information.
Radio Information		
22	show auto-rf channel-info	Displays Auto-RF channel information.
23	show auto-rf history	Displays Auto-RF history.
24	show wireless band-steer client-cache	Displays band steered client cache.
25	show wireless mesh ipv6	Displays IPv6 address of associated mesh clients .
26	show wireless mesh-xtnded-list	Displays mesh extended device list for 2.4 GHz when mesh-xtnded-dev-list is enabled.
27	show wireless neighbors 2.4GHz	Displays 2.4 GHz wireless neighbors.
28	show wireless neighbors 5GHz	Displays 5G Hz wireless neighbors.
29	show wireless neighbors 6GHz	Displays 6 GHz wireless neighbors.
30	show wireless neighbors autocell	Displays Auto-cell neighbors.
31	show wireless radios channels	Displays supported channels.
32	show wireless radios mu-mimo-statistics	Displays MU-MIMO statistics of Radios.
33	show wireless radios multicast-to-unicast	Displays multicast-to-unicast configuration.
34	show wireless radios ofdma-statistics	Displays OFDMA statistics of Radios.
35	show wireless radios rf-statistics	Displays statistics of Radios.
36	show wireless radios statistics	Displays statistics of Radios.
37	show wireless wlans aggregate-statistics	Displays aggregate statistics of wireless LANs.
38	show wireless wlans interface	Displays wireless WLAN interface details.

SL No	CLI Command	Description
39	<code>show wireless wlans monitor-host</code>	Displays monitor host information for wireless LANs.
40	<code>show wireless wlans statistics</code>	Displays statistics of wireless LANs.
Bonjour Information		
41	<code>show bonjour-services</code>	Displays Bonjour services available.
42	<code>show bonjour-statistics</code>	Displays Bonjour rule statistics.
System Information		
43	<code>show upgrade-status</code>	Displays last upgrade status.
44	<code>show version</code>	Displays device firmware information.
45	<code>show timezones</code>	Displays list of timezone locations.
46	<code>show management details</code>	Displays management status in detail.
47	<code>show mfgrom</code>	Displays manufacturing ROM details.
48	<code>show country-codes</code>	Displays a list of supported countries and corresponding country codes.
49	<code>show boot</code>	Displays device firmware active-backup versions.
50	<code>show cambium-id</code>	Displays configured Cambium-ID (if any).
51	<code>show clock</code>	Displays system time.
52	<code>show config all</code>	Displays current configuration including defaults.
53	<code>show config dhcp-pools all</code>	Displays DHCP pools configuration including defaults.
54	<code>show config filter</code>	Displays Filter configuration.
55	<code>show config wireless all</code>	Displays wireless configuration including defaults.
56	<code>show config system all</code>	Displays infra configuration including defaults.
57	<code>show config system interfaces</code>	Displays network interface configuration.
58	<code>show events</code>	Displays recent event messages.
Guest Access		
59	<code>show ext-guest clients</code>	Displays information of ext-guest clients.
Filters		
60	<code>show filter-statistics</code>	Displays filter statistics.

SL No	CLI Command	Description
LLDP		
61	show lldp chassis	Displays local chassis data.
62	show lldp configuration	Displays configuration.
63	show lldp interfaces	Displays interfaces data.
64	show lldp neighbors	Displays neighbors data.
65	show lldp statistics	Displays statistics.
66	show power	Displays power conditions.
67	show packet-capture status	Displays status of packet capture.
Real-Time Location System		
68	show rtls aeroscout ble-tag-summary	Displays AeroScout BLE-tag summary.
69	show rtls aeroscout configuration	Displays AeroScout Wi-Fi-tag configuration.
70	show rtls aeroscout wifi-tag-summary	Displays AeroScout Wi-Fi-tag summary.
Tunnel		
71	show tunnel-statistics	Displays tunnel statistics.
72	show tunnel-status details	Displays tunnel parameters.
73	show ip pppoe-client-info	Displays learned PPPoE client information.
74	show pppoe-status	Displays PPPoE status.

Service commands

Service show

The below table provides **Service show commands** supported in Enterprise Wi-Fi AP:

Table 68 Service show commands supported in Enterprise Wi-Fi AP

SL No	CLI Command	Description
1	service show bridge	Displays AP bridge table entries.
2	service show client-cache	Displays current client status and history of clients connected and respective parameters.
3	service show config	Displays configuration from data base.

SL No	CLI Command	Description
4	service show cores	Displays process cores (if any).
5	service show debug-logs <Process Names>	Displays debug logs of various processes.
6	service show df	Displays flash status.
7	service show dmesg	Displays system kernel logs.
8	service show epsk	Displays ePSK information.
9	service show ethtool	Displays information and statistics w.r.t Ethernet interfaces.
10	service show guest-portal whitelist wlan <wlan index>	Displays whitelist entries either configured or auto-selected by a device in a guest portal WLAN profile.
11	service show ifconfig	Displays status and statistics of all interfaces configured and supported on the device.
12	service show iperfd-logs	Display IPERF logs when iperfd daemon is enabled on device.
13	service show iwconfig	Displays status and statistics of all Wireless interfaces configured on the device.
14	service show last-reboot-reason	Displays the reason for the last reboot of the AP.
15	service show last-reboot-state watchdog	Displays if the last reboot reason is due to watchdog.
16	service show mcastsnoop	Displays multicast-snoop tables.
17	service show mdnsd-statistics	Displays mDNS packet stats on mdnsd.
18	service show memory	Displays memory information.
19	service show netstat	Displays network socket connections.
20	service show ps	Displays a list of processes.
21	service show ps-restart-history	Displays history of process restart on the AP.
22	service show route	Displays routing table.
23	service show top	Displays process activity status.

Service system

The below table provides **Service system** commands supported in Enterprise Wi-Fi AP:

Table 69 Service system commands supported in Enterprise Wi-Fi AP

SL No	CLI Command	Description
1	service boot backup-firmware	Helps to boot to other partition.
2	service clear-cores	Clear system core files (if any).
3	service clear-dhcp-pool	Clear DHCP pool allocated addresses.
4	service debug <process name>logging-level <logging-level>	Commands to enable debugging of processes at various logging levels.
5	service flash-leds	Flash system LEDs help identify this device visually.
6	service radio apstats	Displays aggregate statistics of all wireless interfaces.
7	service radio athstats	Displays aggregate Radio traffic statistics.
8	service radio iwpriv	Displays supported iwpriv commands.
9	service radio thermaltool	Displays radio current operating temperature.
10	service schedule reload	Reboot AP at the specified time.
11	service ssh host add	Add a host and key to the known hosts list.
12	service ssh host del	Delete a host and key from the known hosts list.
13	service system-trace	Start a trace session for troubleshooting.
14	service test leds	Displays test LEDs.
15	service test radio	Displays status and configured Radio.

cnMaestro X Assurance



Note

This feature is available from cnMaestro 4.1.0 and later versions only.

The cnMaestro X Assurance feature provides enhanced visibility into the health of Wi-Fi client connections, including root cause analysis of failures with possible recommended actions. It also provides analytics on aggregated data that can help to improve clients connectivity in the Wi-Fi network.



Note

This feature is currently available as a free trial to all cnMaestro X customers. In future, this feature will require a separate paid subscription.

The cnMaestro X Assurance feature analyzes the Wi-Fi client connection events and helps to troubleshoot common network connectivity and performance issues such as the following:

- Connectivity—Association, authentication, and network connectivity services, such as DHCP and DNS transaction failures.
- Poor Performance—Low RSSI, low data rate, AAA, DHCP, DNS transaction latency.

For more information, refer to the *cnMaestro User Guide*.

MarketApps

The MarketApps feature in cnMaestro offers customized solutions for efficiently managing Wi-Fi services in residential settings, such as multi-dwelling units (MDUs) and apartment complexes. It provides specialized tools (applications or Apps) that enhance operational efficiency and cater to the distinct requirements of both property managers and residents.

Target audience

- **Property managers**—The MarketApps feature empowers property managers to centrally administer Wi-Fi access across their properties. They can set up community-wide Wi-Fi networks and manage personal Wi-Fi networks for local residents.
- **Residents**—Residents can set up and manage their own Wi-Fi networks within the community, ensuring personalized and secure Internet access.
- **Solution providers**—Solution providers can utilize MarketApps to offer tailored Wi-Fi solutions, enhancing network performance and user satisfaction in multi-dwelling units and apartment complexes.

Benefits

- **Centralized management**—Property managers can oversee and control Wi-Fi access across multiple units or buildings from cnMaestro.
- **Customization**—Residents can set up personal Wi-Fi networks with customized SSIDs and passwords, enhancing their user experience.

To access MarketApps, navigate to **Network Services > MarketApps** in cnMaestro.

For more information on configuring and viewing MarketApps, refer to the *cnMaestro User Guide*.

CLI configuration

To enable MarketApps using AP CLI, execute the following command:

```
ap(config)# wireless wlan 2
ap(config)# epsk cnMaestro
```

Glossary

Term	Definition
AP	Access Point Module. One module that distributes network or Internet services to subscriber modules.
API	Application Program Interface
ARP	Address Resolution Protocol. A protocol defined in RFC 826 to allow a network element to correlate a host IP address to the Ethernet address of the host.
BT	Bluetooth
DFS	See Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol defined in RFC 2131. The protocol that enables a device to be assigned a new IP address and TCP/IP parameters, including a default gateway, whenever the device reboots. Thus, DHCP reduces configuration time, conserves IP addresses, and allows modules to be moved to a different network within the system.
Ethernet Protocol	Any of several IEEE standards that define the contents of frames that are transferred from one network element to another through Ethernet connections.
FCC	Federal Communications Commission of the U.S.A.
GPS	Global Positioning System. A network of satellites that provides absolute time to networks on earth, which use the time signal to synchronize transmission and reception cycles (to avoid interference) and to provide reference for troubleshooting activities.
UI	User interface.
HTTP	Hypertext Transfer Protocol, used to make the Internet resources available on the World Wide Web.
HTTPS	Hypertext Transfer Protocol Secure
HT	High Throughput
IP Address	The 32-bit binary number identifies a network element by both network and host. See also Subnet Mask.
IPv4	The traditional version of Internet Protocol, defines 32-bit fields for data transmission.
LLDP	Link Layer Discovery Protocol
MAC Address	Media Access Control address. The hardware address that the factory assigns to the module for identification in the Data Link layer interface of the Open Systems Interconnection system. This address serves as an electronic serial number.
MIB	Management Information Base. Space that allows a program (agent) in the network to relay information to a network monitor about the status of defined variables (objects).

Term	Definition
MIR	See Maximum Information Rate.
PPPoE	Point to Point Protocol over Ethernet. Supported on SMs for operators who use PPPoE in other parts of their network operators who want to deploy PPPoE to realize per-subscriber authentication, metrics, and usage control.
Proxy Server	Network computer that isolates another from the Internet. The proxy server communicates for the other computer, and sends replies to only the appropriate computer which has an IP address that is not unique or not registered.
PoE	Power over Ethernet.
SLA	Service Level Agreement
VLAN	Virtual local area network. An association of devices through software that contains broadcast traffic, as routers would, but in the switch-level protocol.
VPN	A virtual private network for communication over a public network. One typical use is to connect remote employees, who are at home or in a different city, to their corporate network over the Internet. Any of several VPN implementation schemes are possible. SMs support L2TP over IPSec (Level 2 Tunneling Protocol over IP Security) VPNs and PPTP (Point to Point Tunneling Protocol) VPNs, regardless of whether the Network Address Translation (NAT) feature enabled.

Appendix

This appendix contains the following topics:

- [Supported RADIUS Attributes](#)
- [Supported DFS channels](#)
- [Supported 6 GHz countries](#)
- [Priority order for parameters](#)
- [Best practices for wireless clients seamless roaming across APs](#)

Supported RADIUS Attributes

This topic lists the following RADIUS override attributes that are supported on Enterprise Wi-Fi APs:

- [WISPr VSAs \(Vendor ID: 14122\)](#)
- [Cambium VSAs \(Vendor ID: 17713\)](#)
- [Standard RADIUS attributes](#)
- [RADIUS attributes in authentication and accounting packets with WPA2-Enterprise security](#)
- [Supported CoA messages](#)

WISPr VSAs (Vendor ID: 14122)

[Table 70](#) lists the WISPr vendor-specific attributes (VSAs) supported on Enterprise Wi-Fi APs.

Table 70 WISPr VSAs

Attribute Value	Attribute Description	Attribute Type	RADIUS Message Types			Accounting Messages			WPA2 / WPA3 - Enterprise Authentication Support	Guest Access Support
			Request	Response / Challenge	Accept	Start	Interim	Stop		
2	WISPr-Location-Name	string	Yes	-NA-	No	Yes	Yes	Yes	Yes	Yes
7	WISPr-Bandwidth-Max-Up	integer	No	No	Yes	No	No	No	Yes	Yes
8	WISPr-Bandwidth-Max-Down	integer	No	No	Yes	No	No	No	Yes	Yes
9	WISPr-Session-Terminate-Time	string	No	No	Yes	No	No	No	Yes	Yes

[Table 71](#) lists the WISPr VSAs supported on Enterprise Wi-Fi APs with CoA support.

Table 71 WISPr VSAs with CoA

Attribute Value	Attribute Description	Attribute Type	RADIUS Message Types			Accounting Messages			CoA Support with Guest Access	CoA Support with WPA2 / WPA3 - Enterprise Authentication
			Request	Response / Challenge	Accept	Start	Interim	Stop		
2	WISPr-Location-Name	string	Yes	-NA-	No	Yes	Yes	Yes	-NA-	-NA-
7	WISPr-Bandwidth-Max-Up	integer	No	No	Yes	No	No	No	Yes	Yes
8	WISPr-Bandwidth-Max-Down	integer	No	No	Yes	No	No	No	Yes	Yes
9	WISPr-Session-Terminate-Time	string	No	No	Yes	No	No	No	Yes	Yes

Cambium VSAs (Vendor ID: 17713)

[Table 72](#) lists the Cambium Networks VSAs supported on Enterprise Wi-Fi APs.

Table 72 Cambium VSAs

Attribute Value	Attribute Description	Attribute Type	RADIUS Message Types			Accounting Messages			WPA2 / WPA3 - Enterprise Authentication Support	Guest Access Support
			Request	Response / Challenge	Accept	Start	Interim	Stop		
151	Cambium-Wi-Fi-Quota-Up	integer	No	No	Yes	No	No	No	-NA-	Yes
152	Cambium-Wi-Fi-Quota-Down	integer	No	No	Yes	No	No	No	-NA-	Yes
155	Cambium-Wi-Fi-Quota-Total	integer	No	No	Yes	No	No	No	-NA-	Yes
153	Cambium-Wi-Fi-Quota-Up-Gigaword	integer64	No	No	Yes	No	No	No	-NA-	Yes

Attribute Value	Attribute Description	Attribute Type	RADIUS Message Types			Accounting Messages			WPA2 / WPA3 - Enterprise Authentication Support	Guest Access Support
			Request	Response / Challenge	Accept	Start	Interim	Stop		
154	Cambium-Wi-Fi-Quota-Down-Gigaword	integer64	No	No	Yes	No	No	No	-NA-	Yes
156	Cambium-Wi-Fi-Quota-Total-Gigaword	integer64	No	No	Yes	No	No	No	-NA-	Yes
157	Cambium-VLAN-Pool-ID	string	No	No	Yes	No	No	No	Yes	No
159	Cambium-Traffic-Classes-Acct	TLV								
159.2	Cambium-Acct-Input-Octets	integer	No	No	No	No	Yes	Yes		
159.3	Cambium-Acct-Output-Octets	integer	No	No	No	No	Yes	Yes		
159.4	Cambium-Acct-Input-Packets	integer	No	No	No	No	Yes	Yes		
159.5	Cambium-Acct-Output-Packets	integer	No	No	No	No	Yes	Yes		
161	Cambium-ePSK	TLV							-NA-	Yes
161.1	Cambium-ePSK-Anonce	octet	Yes	-NA-	No				-NA-	Yes
161.2	Cambium-ePSK-M2	octet	Yes	-NA-	No				-NA-	Yes
161.3	Cambium-ePSK-BSSID	octet	Yes	-NA-	No				-NA-	Yes
161.4	Cambium-ePSK-AP-MAC	octet	Yes	-NA-	No				-NA-	Yes
161.5	Cambium-ePSK-SSID	string	Yes	-NA-	No				-NA-	Yes
161.6	Cambium-ePSK-PMK	string	No	-NA-	Yes				-NA-	Yes

[Table 73](#) lists the Cambium Networks VSAs supported on Enterprise Wi-Fi APs with CoA.

Table 73 Cambium VSAs with CoA

Attribute Value	Attribute Description	Attribute Type	RADIUS Message Types			Accounting Messages			CoA Support with Guest Access	CoA Support with WPA2 / WPA3 - Enterprise Authentication
			Request	Response / Challenge	Accept	Start	Interim	Stop		
151	Cambium-Wi-Fi-Quota-Up	integer	No	No	Yes	No	No	No	Yes	
152	Cambium-Wi-Fi-Quota-Down	integer	No	No	Yes	No	No	No	Yes	
155	Cambium-Wi-Fi-Quota-Total	integer	No	No	Yes	No	No	No	Yes	
153	Cambium-Wi-Fi-Quota-Up-Gigaword	integer64	No	No	Yes	No	No	No	Yes	
154	Cambium-Wi-Fi-Quota-Down-Gigaword	integer64	No	No	Yes	No	No	No	Yes	
156	Cambium-Wi-Fi-Quota-Total-Gigaword	integer64	No	No	Yes	No	No	No	Yes	
157	Cambium-VLAN-Pool-ID	string	No	No	Yes	No	No	No		
159	Cambium-Traffic-Classes-Acct	TLV								
159.2	Cambium-Acct-Input-Octets	integer	No	No	No	No	Yes	Yes		
159.3	Cambium-Acct-Output-Octets	integer	No	No	No	No	Yes	Yes		
159.4	Cambium-Acct-Input-Packets	integer	No	No	No	No	Yes	Yes		

Attribute Value	Attribute Description	Attribute Type	RADIUS Message Types			Accounting Messages			CoA Support with Guest Access	CoA Support with WPA2 / WPA3 - Enterprise Authentication
			Request	Response / Challenge	Accept	Start	Interim	Stop		
159.5	Cambium-Acct-Output-Packets	integer	No	No	No	No	Yes	Yes		
161	Cambium-ePSK	TLV							-NA-	-NA-
161.1	Cambium-ePSK-Anonce	octet	Yes	-NA-	No				-NA-	-NA-
161.2	Cambium-ePSK-M2	octet	Yes	-NA-	No				-NA-	-NA-
161.3	Cambium-ePSK-BSSID	octet	Yes	-NA-	No				-NA-	-NA-
161.4	Cambium-ePSK-AP-MAC	octet	Yes	-NA-	No				-NA-	-NA-
161.5	Cambium-ePSK-SSID	string	Yes	-NA-	No				-NA-	-NA-
161.6	Cambium-ePSK-PMK	string	No	-NA-	Yes				-NA-	-NA-

Standard RADIUS attributes

[Table 74](#) lists the standard RADIUS attributes supported on Enterprise Wi-Fi APs.

Table 74 Standard RADIUS attributes

Attribute Value	Attribute Description	Attribute Type	RADIUS Message Types			Accounting Messages			WPA2 / WPA3 - Enterprise Authentication Support	Guest Access Support
			Request	Response / Challenge	Accept	Start	Interim	Stop		
11	Filter-Id (text) - Group-ID	text	No	-NA-	Yes	No	No	No	Yes	
24	State	string	Yes	Yes	No				Yes	-NA-
25	Class	string	No	-NA-	Yes	Yes	No	No	Yes	Yes
27	Session-Timeout	integer	No	-NA-	Yes	No	No	No	Yes	Yes

Attribute Value	Attribute Description	Attribute Type	RADIUS Message Types			Accounting Messages			WPA2 / WPA3 - Enterprise Authentication Support	Guest Access Support
			Request	Response / Challenge	Accept	Start	Interim	Stop		
28	Idle-Timeout	integer	No	-NA-	Yes	No	No	No		Yes
64	Tunnel-Type	enum	No	-NA-	Yes	No	No	No	Yes	Yes
65	Tunnel-Medium-Type	enum	No	-NA-	Yes	No	No	No	Yes	Yes
81	Tunnel-Private-Group-Id	text	No	-NA-	Yes	No	No	No	Yes	Yes
85	Acct-Interim-Interval	integer	No	-NA-	Yes	No	No	No	Yes	Yes
	Disconnect		RADIUS packet							
40	Disconnect-Request	-	RADIUS packet	-NA-	-NA-	-NA-	-NA-	-NA-	-NA-	-NA-
41	Disconnect-ACK	-	RADIUS packet	-NA-	-NA-	-NA-	-NA-	-NA-		
42	Disconnect-NAK	-	RADIUS packet	-NA-	-NA-	-NA-	-NA-	-NA-		
43	CoA-Request	-	RADIUS packet	-NA-	-NA-	-NA-	-NA-	-NA-		
44	CoA-ACK	-	RADIUS packet	-NA-	-NA-	-NA-	-NA-	-NA-		
45	CoA-NAK	-	RADIUS packet	-NA-	-NA-	-NA-	-NA-	-NA-		

[Table 75](#) lists the standard RADIUS attributes supported on Enterprise Wi-Fi APs with CoA support.

Table 75 Standard RADIUS attributes with CoA

Attribute Value	Attribute Description	Attribute Type	RADIUS Message Types			Accounting Messages			CoA Support with Guest Access	CoA Support with WPA2 / WPA3 - Enterprise Authentication
			Request	Response / Challenge	Accept	Start	Interim	Stop		
11	Filter-Id (text) - Group-ID	text	No	-NA-	Yes	No	No	No	Yes	Yes
24	State	string	Yes	Yes	No					Yes
25	Class	string	No	-NA-	Yes	Yes	No	No	-NA-	-NA-
27	Session-Timeout	integer	No	-NA-	Yes	No	No	No	-NA-	-NA-
28	Idle-Timeout	integer	No	-NA-	Yes	No	No	No	-NA-	-NA-
64	Tunnel-Type	enum	No	-NA-	Yes	No	No	No	-NA-	-NA-
65	Tunnel-Medium-Type	enum	No	-NA-	Yes	No	No	No	-NA-	-NA-
81	Tunnel-Private-Group-Id	text	No	-NA-	Yes	No	No	No	No	Yes
85	Acct-Interim-Interval	integer	No	-NA-	Yes	No	No	No		
	Disconnect		RADIUS packet							
40	Disconnect-Request	-	RADIUS packet	-NA-	-NA-	-NA-	-NA-	-NA-	Yes	Yes
41	Disconnect-ACK	-	RADIUS packet	-NA-	-NA-	-NA-	-NA-	-NA-	Yes	Yes
42	Disconnect-NAK	-	RADIUS packet	-NA-	-NA-	-NA-	-NA-	-NA-	Yes	Yes

Attribute Value	Attribute Description	Attribute Type	RADIUS Message Types			Accounting Messages			CoA Support with Guest Access	CoA Support with WPA2 / WPA3 - Enterprise Authentication
			Request	Response / Challenge	Accept	Start	Interim	Stop		
43	CoA-Request	-	RADIUS packet	-NA-	-NA-	-NA-	-NA-	-NA-	Yes	Yes
44	CoA-ACK	-	RADIUS packet	-NA-	-NA-	-NA-	-NA-	-NA-	Yes	Yes
45	CoA-NAK	-	RADIUS packet	-NA-	-NA-	-NA-	-NA-	-NA-	Yes	Yes

RADIUS attributes in authentication and accounting packets with WPA2-Enterprise security

[Table 76](#) lists the RADIUS attributes supported in authentication and accounting packets with WPA2-Enterprise security.

Table 76 RADIUS attributes in authentication and accounting packets with WPA2-Enterprise security

Attribute Value	Attribute Description	Attribute Type	Access-Request	Access-Challenge	Access-Accept	Accounting-Start	Accounting-Interim	Accounting-Stop
1	User-Name	string	Yes	No	Yes	Yes	Yes	Yes
2	User-Password	string	Yes	No	No	No	No	No
4	NAS-IP-Address	ipv4addr	Yes	No	No	Yes	Yes	Yes
5	NAS-Port	integer	Yes	No	No	Yes	Yes	Yes
6	Service-Type	enum	Yes	No	No	Yes	Yes	Yes
8	Framed-IP-Address	ipv4addr	No	No	No	Yes	Yes	Yes
12	Framed-MTU	integer	Yes	No	No	Yes	Yes	Yes
24	State	string	Yes	Yes	No	No	No	No

Attribute Value	Attribute Description	Attribute Type	Access-Request	Access-Challenge	Access-Accept	Accounting-Start	Accounting-Interim	Accounting-Stop
25	Class	string	No	No	Yes	Yes	Yes	Yes
27	Session-Timeout	integer	No	No	Yes	No	No	No
28	Idle-Timeout	integer	No	No	Yes	No	No	No
30	Called-Station-Id	string	Yes	No	No	Yes	Yes	Yes
31	Calling-Station-Id	text	Yes	No	No	Yes	Yes	Yes
32	NAS-Identifier	string	Yes	No	No	Yes	Yes	Yes
40	Acct-Status-Type	enum	No	No	No	Yes	Yes	Yes
41	Acct-Delay-Time	integer	No	No	No	Yes	Yes	Yes
42	Acct-Input-Octets	integer	No	No	No	No	Yes	Yes
43	Acct-Output-Octets	integer	No	No	No	No	Yes	Yes
44	Acct-Session-Id	text	Yes	No	No	Yes	Yes	Yes
45	Acct-Authentic	enum	No	No	No	Yes	Yes	Yes
46	Acct-Session-Time	integer	No	No	No	No	Yes	Yes
49	Acct-Terminate-Cause	enum	No	No	No	No	No	Yes

Attribute Value	Attribute Description	Attribute Type	Access-Request	Access-Challenge	Access-Accept	Accounting-Start	Accounting-Interim	Accounting-Stop
50	Acct-Multi-Session-Id	text	Yes (Empty)	No	No	Yes	Yes	Yes
52	Acct-Input-Gigawords	integer	No	No	No	No	No	No
53	Acct-Output-Gigawords	integer	No	No	No	No	No	No
55	Event-Timestamp	time	No	No	No	Yes	Yes	Yes
61	NAS-Port-Type	integer	Yes	No	No	Yes	Yes	Yes
77	Connect-Info	text	Yes	No	No	Yes	Yes	Yes
79	EAP-Message	concat	Yes	Yes	Yes	No	No	No
80	Message-Authenticator	string	Yes	Yes	Yes	No	No	No
85	Acct-Interim-Interval	integer	No	No	Yes	No	No	No
87	NAS-Port-Id	text	Yes	No	No	Yes	Yes	Yes

Supported CoA messages

[Table 77](#) lists the supported CoA messages.

Table 77 CoA messages

CoA Message	Supported by MAB (Wired Clients)	Supported by the AP
Disconnect client	Yes	Yes
Update VLAN	Yes	Yes

CoA Message	Supported by MAB (Wired Clients)	Supported by the AP
Session Timeout	No	Yes
Accounting Interval	Yes	Yes
Quota Limit	No	Yes



Note

Following are the mandatory parameters to be included in the CoA message:

- When sent through cnMaestro—User-Name, Calling-Station-Id, and Session ID
- When sent directly through the AP—User-Name, Calling-Station-Id, and NAS-Identifier

Supported DFS channels

[Table 78](#) lists the DFS channel support for various platforms in conformance with FCC standards.

Table 78 DFS channel support for FCC

AP Model	5250-5350 MHz (U-NII-2A)	5470-5725 MHz (U-NII-2C)	5725-5850 MHz (U-NII-3)
XE3-4TN	Yes	Yes	Yes
XV2-22H	Yes	Yes	Yes
XV2-21X	Yes	Yes	Yes
XV2-23T	Yes	Yes	Yes
XE3-4	Yes	Yes	Yes
XE5-8	Yes	Yes	Yes
XV2-2	Yes	Yes	Yes
XV3-8	Yes	Yes	Yes
XV2-2T0	Yes	Yes	Yes
XV2-2T1	Yes	Yes	Yes

[Table 79](#) lists the DFS channel support for various platforms in conformance with IC standards.

Table 79 DFS channel support for IC

AP Model	5250-5350 MHz (U-NII-2A)	5470-5725 MHz (U-NII-2C)	5725-5850 MHz (U-NII-3)
XE3-4TN	Yes	Yes	Yes
XV2-22H	Yes	Yes	Yes
XV2-21X	Yes	Yes	Yes
XV2-23T	Yes	Yes	Yes
XE3-4	Yes	Yes	Yes
XE5-8	Yes	Yes	Yes
XV2-2	Yes	Yes	Yes
XV3-8	Yes	Yes	Yes

AP Model	5250-5350 MHz (U-NII-2A)	5470-5725 MHz (U-NII-2C)	5725-5850 MHz (U-NII-3)
XV2-2T0	Yes	Yes	Yes
XV2-2T1	Yes	Yes	Yes

[Table 80](#) lists the DFS channel support for various platforms in conformance with CE standards.

Table 80 DFS channel support for CE

AP Model	5250-5350 MHz (U-NII-2A)	5470-5725 MHz (U-NII-2C)	5725-5850 MHz (U-NII-3)
XE3-4TN	Yes	Yes	Yes
XV2-22H	Yes	Yes	Yes
XV2-21X	Yes	Yes	Yes
XV2-23T	Yes	Yes	Yes
XE3-4	Yes	Yes	Yes
XE5-8	Yes	Yes	Yes
XV2-2	Yes	Yes	No
XV3-8	No	Yes	No
XV2-2T0	Yes	Yes	Yes
XV2-2T1	Yes	Yes	Yes

Supported 6 GHz countries

[Table 81](#) lists the countries where 6 GHz band is available and the frequencies supported.



Note

Availability of these channels is subjected to respective country regulations.

6 GHz frequency is supported only on the following Enterprise Wi-Fi APs:

- XE3-4
- XE3-4TN
- XE5-8

Table 81 List of countries where 6 GHz band is supported

Country	XE3-4		XE5-8			
	Frequencies Supported	Channels Supported	Frequencies Supported	Channels Supported (No Channel Distribution)	Channels Supported (With Channel Distribution Enabled)	
					Radio 2	Radio 3
Australia (AU)	5945-6425 MHz	1-93	5945-6425 MHz	1-93	1-61	65-93
Brazil (BR)	5945-7125 MHz	1-233	5945-7125 MHz	1-233	1-93	129-233
Canada (CA)	5945-7125 MHz	1-233	5945-7125 MHz	1-233	1-93	97-233
Colombia (CO)	5945-7125 MHz	1-233	5945-7125 MHz	1-233	1-93	129-233
France (FR)	5945-6425 MHz	1-93	5945-6425 MHz	1-93	1-61	65-93
Germany (DE)	5945-6425 MHz	1-93	5945-6425 MHz	1-93	1-61	65-93
Ireland (IE)	5945-6425 MHz	1-93	5945-6425 MHz	1-93	1-61	65-93
Italy (IT)	5945-6425 MHz	1-93	5945-6425 MHz	1-93	1-61	65-93
Jordan (JO)	5945-6425 MHz	1-93	5945-6425 MHz	1-93	1-61	65-93
South Korea (KR)	5945-7125 MHz	1-233	5945-7125 MHz	1-233	1-93	97-233
Netherlands (NL)	5945-6425 MHz	1-93	5945-6425 MHz	1-93	1-61	65-93
New Zealand (NZ)	5945-6425 MHz	1-93	5945-6425 MHz	1-93	1-61	65-93
South Africa (ZA)	5945-6425 MHz	1-93	5945-6425 MHz	1-93	1-61	65-93
Spain (ES)	5945-6425 MHz	1-93	5945-6425 MHz	1-93	1-61	65-93

Country	XE3-4		XE5-8			
	Frequencies Supported	Channels Supported	Frequencies Supported	Channels Supported (No Channel Distribution)	Channels Supported (With Channel Distribution Enabled)	
					Radio 2	Radio 3
Sweden (SE)	5945-6425 MHz	1-93	5945-6425 MHz	1-93	1-61	65-93
United Kingdom (GB)	5945-6425 MHz	1-93	5945-6425 MHz	1-93	1-61	65-93
United States (US)	5945-7125 MHz	1-233	5945-7125 MHz	1-233	1-93	129-233

Priority order for parameters

This section provides information on the order of priority for the following parameters:

- **Session timeout and inactivity timeout**—Following priority is considered when configuring session timeout and inactivity timeout:
 - a. Configured from the RADIUS server
 - b. Configured from the AP



Note

- Inactivity timeout is triggered when there is no data packets from the client to the AP.
- A five minute static idle time is configured from the driver, which is triggered when there are no wireless packets from the client.

- **VLAN assignment**—Following priority is considered when assigning VLANs to clients:
 - a. RADIUS dynamic VLAN for guest access clients
 - b. RADIUS dynamic VLAN (Filter-ID/RADIUS-ID)
 - c. RADIUS dynamic VLAN
 - d. RADIUS-based ePSK
 - e. RADIUS-based dynamic VLAN Pool
 - f. Local ePSK VLAN setting
 - g. VLAN pool (Static)
 - h. SSID/WLAN profile VLAN
- **User group filter**—Following priority is considered for assigning policy:
 - a. Global policy
 - b. User Group policy
 - c. Device Group policy
 - d. SSID/WLAN policy

Best practices for wireless clients seamless roaming across APs



Note

- Inactivity timeout is triggered when there is no data packets from the client to the AP.
- A five minute static idle time is configured from the driver, which is triggered when there are no wireless packets from the client.

This appendix explains the recommended configuration for Cambium Networks APs and external network to facilitate a seamless roaming across the APs for the wireless clients. Additionally, this appendix also lists the recommended network best practices for minimizing broadcast and multicast packets processing.

This appendix contains the following topics:

- [External network recommendation](#)
- [AP WLAN profile configuration recommendations](#)
- [AP group configuration recommendations](#)

External network recommendations

The Cambium APs work in the distributed architecture mode and it is important to facilitate AP-to-AP communication for the wireless clients seamless roaming. The APs use the Cambium proprietary XRP protocol to exchange clients information with the neighboring APs.

Following are the recommendations:

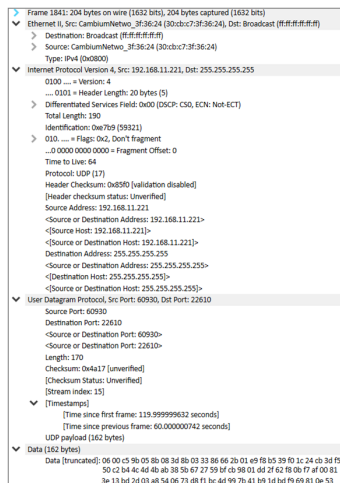
- The intermediate network switches, to which the APs are connected, must not block the following XRP messages:

XRP message packet information

- Source MAC—APs ethernet MAC
- Destination MAC—Ethernet broadcast
- Source IP Address—APs exit interface IP address
- Destination IP Address—255.255.255.255 Broadcast IP address
- Protocol—UDP with a random source port and a fixed destination port

A sample pcap capture of the XRP message is displayed in [Figure 105](#).

Figure 105 Sample XRP message



- APs send the XRP messages on the ethernet port's native VLAN.
- All the APs must be part of the same native VLAN.
- Make sure that the APs have the L3 interface for the native VLAN with a valid IP address.

AP WLAN profile configuration recommendations

If the WLAN profile is configured with WPA2 and WPA3 security, it is recommended to enable the following:

- 802.11r fast roaming
- OKC



Note

A few clients use 802.11k and 802.11v protocols for fast roaming. We can enable the same.

Figure 106 Enabling OKC and 802.11r

WLANs > NORMAL BROWSING

Configuration Devices

WLAN

Band Steering: Disable

Proxy ARP: ☒ Respond to ARP requests automatically on behalf of clients

Proxy ND: ☐ Respond to IPv6 Neighbor Discovery (ND) requests automatically on behalf of clients

Unicast DHCP: ☒ Convert DHCP-OFFER and DHCP-ACK to unicast before forwarding to clients

Insert DHCP Option 82: ☒ Enable DHCP Option 82

Option82 Circuit ID: BSSID

Option82 Remote ID: APMAC

Tunnel Mode: ☐ Enable tunnelling of WLAN traffic over configured tunnel

Fast Roaming Protocol

☒ OKC ☒ 802.11r Configure roaming protocol (not applicable when authentication type is Open)

☒ Over-the-DS

Re-association Timeout: 20 Number of seconds (1-100)

☒ RRM (802.11k) Enable Radio Resource Measurements (802.11k)

☒ 802.11v Enable 802.11v BSS Transition Management

PMF (802.11w): Optional

- Enable client isolation with the **Network Wide** option to prevent clients communicating with other clients on the same L2 network.

Figure 107 Enabling Client Isolation

WLANs > Default Enterprise

Configuration Devices

WLAN

Basic Settings

SSID: ☒ Enable

SSID*: cnPilot The SSID of this WLAN (up to 32 characters)

Mesh: Off Mesh Base/Client/Recovery mode

VLAN*: 1 Default VLAN assigned to clients on this WLAN (1-4094)

Security: WPA2 Pre-Shared Keys Set authentication and encryption type

Passphrase*: Show WPA2 Pre-shared security passphrase or key (must contain 8 to 63 ascii or 64 hex digits)

Change your password, do not use default passwords!

Band: ☒ 2.4 GHz ☒ 5 GHz ☒ 6 GHz Define radio types (2.4 GHz, 5 GHz, 6 GHz) on which this WLAN should be supported

Client Isolation: Network Wide

When selected, it prevents wireless clients connected to the same AP or different APs from communicating with each other which are in the same VLAN. Clients are allowed to communicate to gateway mac address automatically and also mac addresses listed in below MAC address table

Client Isolation MAC List: e.g. xxxxxxxxxx Add Import .csv

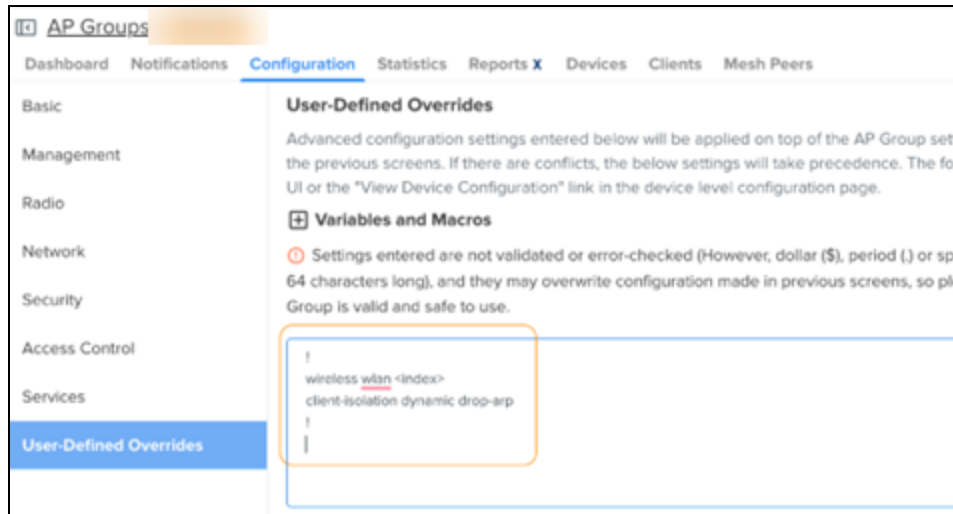
Save



Note

From AP version 6.6.0.2 onwards, the AP drops the ARP packets when the client isolation feature is enabled. To enable this in APs running firmware version lesser than 6.6.0.2, execute the `client-isolation dynamic drop-arp` CLI command from the AP group **User-Defined Overrides** section.

Figure 108 Enabling Client Isolation in User-Defined Overrides



AP group configuration recommendations

- In large public Wi-Fi and campus deployments, it is common to see large number of network discovery protocols, such as mDNS, LLMNR, SSDP and other service discovery packets coming from the wireless clients.

Disable these packets using **Access Control Policy**.

- If IPv6 is not required, disable IPv6 packets from the wireless clients using **Access Control Policy**.
- Use **Air Cleaner Rules** to:
 - prevent unauthorized rogue DHCP server from wireless clients
 - prevent unwanted DHCP client packets from wired network side
 - drop L2 broadcast packets
 - drop IPv4 and IPv6 multicast packets
 - drop ARP discovery packets from one SSID to another SSID interface
 - disable mDNS packets in the default Air Cleaner rules



Note

Allow the mDNS packet to enable Bonjour discovery service to work.

- Sample AP group policy with **Air Cleaner Rules**.

Figure 109 Sample AP group policy with Air Cleaner Rules

View Access Control Policy Rules

Air Cleaner Rules

Apply Filter(s)

Name	Status	Action	Direction	Source ...	Source Mask	Destination ...	Destination Mask	Protocol	Source Port	Destination Port
Air-cleaner-Arp.1	Enabled	Deny	In	any	FF:FF:FF:FF:FF:FF	any	FF:FF:FF:FF:FF:FF	ARP	any	any
Air-cleaner-Dhcp.1	Enabled	Deny	Out	any	FF:FF:FF:FF:FF:FF	FF:FF:FF:FF:FF:FF	FF:FF:FF:FF:FF:FF	UDP	any	67
Air-cleaner-Dhcp.2	Enabled	Deny	In	any	FF:FF:FF:FF:FF:FF	FF:FF:FF:FF:FF:FF	FF:FF:FF:FF:FF:FF	UDP	any	68
Air-cleaner-Bcast.1	Enabled	Allow	Any	any	FF:FF:FF:FF:FF:FF	FF:FF:FF:FF:FF:FF	FF:FF:FF:FF:FF:FF	ARP	any	any
Air-cleaner-Bcast.2	Enabled	Allow	Any	any	FF:FF:FF:FF:FF:FF	FF:FF:FF:FF:FF:FF	FF:FF:FF:FF:FF:FF	UDP	any	67
Air-cleaner-Bcast.3	Enabled	Allow	Any	any	FF:FF:FF:FF:FF:FF	FF:FF:FF:FF:FF:FF	FF:FF:FF:FF:FF:FF	UDP	any	68
Air-cleaner-Bcast.4	Enabled	Allow	Any	any	FF:FF:FF:FF:FF:FF	FF:FF:FF:FF:FF:FF	FF:FF:FF:FF:FF:FF	UDP	any	22610
Air-cleaner-Bcast.5	Enabled	Deny	Any	any	FF:FF:FF:FF:FF:FF	FF:FF:FF:FF:FF:FF	FF:FF:FF:FF:FF:FF	ANY	any	any
Air-cleaner-mDNS.1	Enabled	Allow	Any	any	FF:FF:FF:FF:FF:FF	01:00:5E:00:00:FB	FF:FF:FF:FF:FF:FF	ANY	any	any
Air-cleaner-Mcast.1	Enabled	Deny	Any	any	FF:FF:FF:FF:FF:FF	multicast	FF:FF:FF:FF:FF:FF	ANY	any	any

MAC Filtering Rules

Apply Filter(s)

Name	Status	Action	Type	Application / Category	Protocol	Sour...	Source IP Mask	Destination ...	Destination IP Mask
BLOCK DROPBOX DISCOVERY	Enabled	Deny	Layer3-filter	-	UDP	any	any	255.255.255.255	any
BLOCK LLNMR	Enabled	Deny	Layer3-filter	-	UDP	any	any	224.0.0.252	any
BLOCK SSDP	Enabled	Deny	Layer3-filter	-	UDP	any	any	239.255.255.250	any

IP and Application Filtering Rules

Apply Filter(s)

Sample user-defined rule for blocking IPv6 traffic and allowing the rest of the traffic.

```
!
filter global-filter
filter precedence 14
enable
layer3-filter deny proto6 any any any any any any //BLOCK IPv6
TRAFFIC
exit
filter precedence 15
enable
layer3-filter permit ip any/any any/any any //ALLOW TRAFFIC
exit
!
```

Cambium Networks

Cambium Networks delivers wireless communications that work for businesses, communities, and cities worldwide. Millions of our radios are deployed to connect people, places, and things with a unified wireless fabric that spans multiple standards and frequencies of fixed wireless and Wi-Fi, all managed centrally via the cloud. Our multi-gigabit wireless fabric offers a compelling value proposition over traditional fiber and alternative wireless solutions. We work with our Cambium certified Connected Partners to deliver purpose built networks for service provider, enterprise, industrial, and government connectivity solutions in urban, suburban, and rural environments, with wireless that just works.

Support website	https://support.cambiumnetworks.com
Support enquiries	
Technical training	https://learning.cambiumnetworks.com/learn
Main website	http://www.cambiumnetworks.com
Sales enquiries	solutions@cambiumnetworks.com
Warranty	https://www.cambiumnetworks.com/support/standard-warranty/
Telephone number list	http://www.cambiumnetworks.com/contact-us/
User Guides	http://www.cambiumnetworks.com/guides
Address	Cambium Networks Limited, Unit B2, Linhay Business Park, Eastern Road, Ashburton, Devon, TQ13 7UP United Kingdom



Cambium Networks and the stylized circular logo are trademarks of Cambium Networks, Ltd. All other trademarks are the property of their respective owners.

Copyright © 2024 Cambium Networks, Ltd. All rights reserved.



Wi-Fi CERTIFIED™ Certificate

This certificate lists the features that have successfully completed Wi-Fi Alliance interoperability testing. Learn more: www.wi-fi.org/certification/programs



Certification ID: WFA125208

Product Info

Date of Certification	June 1, 2023
Company	Cambium Networks Ltd.
Product Name	Cambium XV2-21X Indoor Wi-Fi 6 Access Point
Product Model Variant	XV2-21X
Model Number	XV2-21X
Category	Routers
Sub-category	Enterprise/Service Provider Access Point, Switch/Controller or Router

Summary of Certifications

CLASSIFICATION	CERTIFICATION
Access	Passpoint® Release 3
Connectivity	2.4 GHz Spectrum Capabilities 5 GHz Spectrum Capabilities Wi-Fi CERTIFIED 6® Wi-Fi CERTIFIED™ a Wi-Fi CERTIFIED™ ac Wi-Fi CERTIFIED™ b Wi-Fi CERTIFIED™ g Wi-Fi CERTIFIED™ n
Optimization	WMM® Wi-Fi Agile Multiband™
Security	Protected Management Frames WPA2™-Enterprise 2018-04 WPA2™-Personal 2021-01 WPA3™-Enterprise 2022-12 WPA3™-Personal 2022-06
Spectrum & Regulatory Features	Spectrum & Regulatory



Wi-Fi CERTIFIED™ Certificate

Certification ID: WFA125208



Role: Access Point

Page 2 of 3

Wi-Fi Components

Wi-Fi Component Operating System

Linux

Wi-Fi Component Firmware

6.5.2-a0

RF Architecture

Bands Supported	Transmit (Tx)	Receive (Rx)
2.4 GHz	2	2
5 GHz	2	2

Certifications

2.4 GHz Spectrum Capabilities

20 MHz Channel Width in 2.4 GHz

5 GHz Spectrum Capabilities

20 MHz Channel Width in 5 GHz

40 MHz Channel Width in 5 GHz

80 MHz Channel Width in 5 GHz

Passpoint® Release 3

Online Sign Up and Policy provisioning

Online Sign Up using single SSID

Roaming Consortium Selection

Venue Information

Terms and Conditions

Protected Management Frames

Spectrum & Regulatory

802.11d

802.11h

WMM®

WPA2™-Enterprise 2018-04

EAP methods

WPA2™-Personal 2021-01

WPA3™-Enterprise 2022-12

EAP methods

192-bit security

WPA3™-Personal 2022-06

Wi-Fi Agile Multiband™

Wi-Fi CERTIFIED 6®

A-MPDU with A-MSDU

Basic Trigger frame in HE MU PPDU

Beamforming sounding

BSRP Trigger frame

Compressed Block Ack Rx (buffer size 256)

Compressed Block Ack Tx (buffer size 256)



Wi-Fi CERTIFIED™ Certificate

Certification ID: WFA125208



Role: Access Point

Page 3 of 3

Wi-Fi CERTIFIED 6® (continued)

DL OFDMA
Individual Target Wake Time
LDPC Rx
LDPC Tx
MCS 8-9 Rx
MCS 8-9 Tx
MCS 10-11 Rx
MCS 10-11 Tx
MU EDCA Parameter Set element
MU-BAR Trigger frame
MU-RTS Trigger frame
Operating mode indication
SU beamformer
SU-MIMO
TXOP RTS Threshold
UL OFDMA

Wi-Fi CERTIFIED™ n (continued)

A-MPDU Tx
OBSS on Extension Channel
Short Guard Interval
STBC

Wi-Fi CERTIFIED™ a

Wi-Fi CERTIFIED™ ac

Extended 5 GHz Channel Support
A-MPDU with A-MSDU
LDPC Rx
LDPC Tx
MCS 8-9 Rx
Short Guard Interval
STBC
SU beamformer

Wi-Fi CERTIFIED™ b

Wi-Fi CERTIFIED™ g

Wi-Fi CERTIFIED™ n



Wi-Fi CERTIFIED™ Certificate

This certificate lists the features that have successfully completed Wi-Fi Alliance interoperability testing. Learn more: www.wi-fi.org/certification/programs



Certification ID: WFA126875

Product Info

Date of Certification	June 14, 2023
Company	Cambium Networks Ltd.
Product Name	Cambium XV2-23T Two Radio Dual Band Wi-Fi 6 2x2 Outdoor Access Point
Product Model Variant	XV2-23T
Model Number	XV2-23T
Category	Routers
Sub-category	Enterprise/Service Provider Access Point, Switch/Controller or Router

Summary of Certifications

CLASSIFICATION	CERTIFICATION
Access	Passpoint® Release 3
Connectivity	2.4 GHz Spectrum Capabilities 5 GHz Spectrum Capabilities Wi-Fi CERTIFIED 6® Wi-Fi CERTIFIED™ a Wi-Fi CERTIFIED™ ac Wi-Fi CERTIFIED™ b Wi-Fi CERTIFIED™ g Wi-Fi CERTIFIED™ n
Optimization	WMM® Wi-Fi Agile Multiband™
Security	Protected Management Frames WPA2™-Enterprise 2018-04 WPA2™-Personal 2021-01 WPA3™-Enterprise 2022-12 WPA3™-Personal 2022-06
Spectrum & Regulatory Features	Spectrum & Regulatory



Wi-Fi CERTIFIED™ Certificate

Certification ID: WFA126875



Role: Access Point

Page 2 of 3

Wi-Fi Components

Wi-Fi Component Operating System

Linux

Wi-Fi Component Firmware

6.5.2-a0

RF Architecture

Bands Supported	Transmit (Tx)	Receive (Rx)
2.4 GHz	2	2
5 GHz	2	2

Certifications

2.4 GHz Spectrum Capabilities

20 MHz Channel Width in 2.4 GHz

5 GHz Spectrum Capabilities

20 MHz Channel Width in 5 GHz

40 MHz Channel Width in 5 GHz

80 MHz Channel Width in 5 GHz

Passpoint® Release 3

Online Sign Up and Policy provisioning

Online Sign Up using single SSID

Roaming Consortium Selection

Venue Information

Terms and Conditions

Protected Management Frames

Spectrum & Regulatory

802.11d

802.11h

WMM®

WPA2™-Enterprise 2018-04

EAP methods

WPA2™-Personal 2021-01

WPA3™-Enterprise 2022-12

EAP methods

192-bit security

WPA3™-Personal 2022-06

Wi-Fi Agile Multiband™

Wi-Fi CERTIFIED 6®

A-MPDU with A-MSDU

Basic Trigger frame in HE MU PPDU

Beamforming sounding

BSRP Trigger frame

Compressed Block Ack Rx (buffer size 256)

Compressed Block Ack Tx (buffer size 256)



Wi-Fi CERTIFIED™ Certificate

Certification ID: WFA126875



Role: Access Point

Page 3 of 3

Wi-Fi CERTIFIED 6® (continued)

DL OFDMA
Individual Target Wake Time
LDPC Rx
LDPC Tx
MCS 8-9 Rx
MCS 8-9 Tx
MCS 10-11 Rx
MCS 10-11 Tx
MU EDCA Parameter Set element
MU-BAR Trigger frame
MU-RTS Trigger frame
Operating mode indication
SU beamformer
SU-MIMO
TXOP RTS Threshold
UL OFDMA

Wi-Fi CERTIFIED™ n (continued)

A-MPDU Tx
OBSS on Extension Channel
Short Guard Interval
STBC

Wi-Fi CERTIFIED™ a

Wi-Fi CERTIFIED™ ac

Extended 5 GHz Channel Support
A-MPDU with A-MSDU
LDPC Rx
LDPC Tx
MCS 8-9 Rx
Short Guard Interval
STBC
SU beamformer

Wi-Fi CERTIFIED™ b

Wi-Fi CERTIFIED™ g

Wi-Fi CERTIFIED™ n



Wi-Fi CERTIFIED™ Certificate

This certificate lists the features that have successfully completed Wi-Fi Alliance interoperability testing. Learn more: www.wi-fi.org/certification/programs



Certification ID: WFA129114

Product Info

Date of Certification	February 15, 2024
Company	Cambium Networks Ltd.
Product Name	XE3-4 Three Radio Tri Band Wi-Fi 6E 4x4 Indoor Access Point
Product Model Variant	XE3-4
Model Number	XE3-4
Category	Routers
Sub-category	Enterprise/Service Provider Access Point, Switch/Controller or Router

Summary of Certifications

CLASSIFICATION	CERTIFICATION
Access	Passpoint® Release 3
Connectivity	2.4 GHz Spectrum Capabilities 5 GHz Spectrum Capabilities 6 GHz Spectrum Capabilities Wi-Fi CERTIFIED 6® Wi-Fi CERTIFIED™ a Wi-Fi CERTIFIED™ ac Wi-Fi CERTIFIED™ b Wi-Fi CERTIFIED™ g Wi-Fi CERTIFIED™ n Wi-Fi Enhanced Open™ 2023-12
Optimization	WMM® Wi-Fi Agile Multiband™
Security	Protected Management Frames WPA2™-Enterprise 2018-04 WPA2™-Personal 2021-01 WPA3™-Enterprise 2022-12 WPA3™-Personal 2022-06



Wi-Fi CERTIFIED™ Certificate

Certification ID: WFA129114



Summary of Certifications (continued)

Page 2 of 4

CLASSIFICATION

CERTIFICATION

Spectrum & Regulatory
Features

Spectrum & Regulatory



Wi-Fi CERTIFIED™ Certificate

Certification ID: WFA129114



Role: Access Point

Page 3 of 4

Wi-Fi Components

Wi-Fi Component Operating System

Linux

Wi-Fi Component Firmware

6.6.0.1

RF Architecture

Bands Supported	Transmit (Tx)	Receive (Rx)
2.4 GHz	2	2
5 GHz	2	2
6 GHz	4	4

Certifications

2.4 GHz Spectrum Capabilities

20 MHz Channel Width in 2.4 GHz

5 GHz Spectrum Capabilities

20 MHz Channel Width in 5 GHz

40 MHz Channel Width in 5 GHz

80 MHz Channel Width in 5 GHz

6 GHz Spectrum Capabilities

20 MHz Channel Width in 6 GHz

40 MHz Channel Width in 6 GHz

80 MHz Channel Width in 6 GHz

160 MHz Channel Width in 6 GHz

Passpoint® Release 3

Roaming Consortium Selection

Terms and Conditions

Venue Information

Protected Management Frames

Spectrum & Regulatory

802.11d

802.11h

WMM®

WPA2™-Enterprise 2018-04

EAP methods

WPA2™-Personal 2021-01

WPA3™-Enterprise 2022-12

EAP methods

192-bit security

WPA3™-Personal 2022-06

Wi-Fi Agile Multiband™



Wi-Fi CERTIFIED™ Certificate

Certification ID: WFA129114



Role: Access Point

Page 4 of 4

Wi-Fi CERTIFIED 6®

A-MPDU with A-MSDU
Basic Trigger frame in HE MU PPDU
Beamforming sounding
BSRP Trigger frame
Compressed Block Ack Rx (buffer size 256)
Compressed Block Ack Tx (buffer size 256)
DL MU-MIMO
DL OFDMA
Individual Target Wake Time
LDPC Rx
LDPC Tx
MCS 8-9 Rx
MCS 8-9 Tx
MCS 10-11 Rx
MCS 10-11 Tx
MU EDCA Parameter Set element
MU-BAR Trigger frame
MU-RTS Trigger frame
Operating mode indication
SU beamformer
SU-MIMO
TXOP RTS Threshold
UL OFDMA
Wi-Fi 6E

Wi-Fi CERTIFIED™ a

Wi-Fi CERTIFIED™ ac

A-MPDU with A-MSDU
DL MU-MIMO
Extended 5 GHz Channel Support
LDPC Rx
LDPC Tx
MCS 8-9 Rx

Wi-Fi CERTIFIED™ ac (continued)

Short Guard Interval
STBC
SU beamformer

Wi-Fi CERTIFIED™ b

Wi-Fi CERTIFIED™ g

Wi-Fi CERTIFIED™ n

A-MPDU Tx
OBSS on Extension Channel
Short Guard Interval
STBC

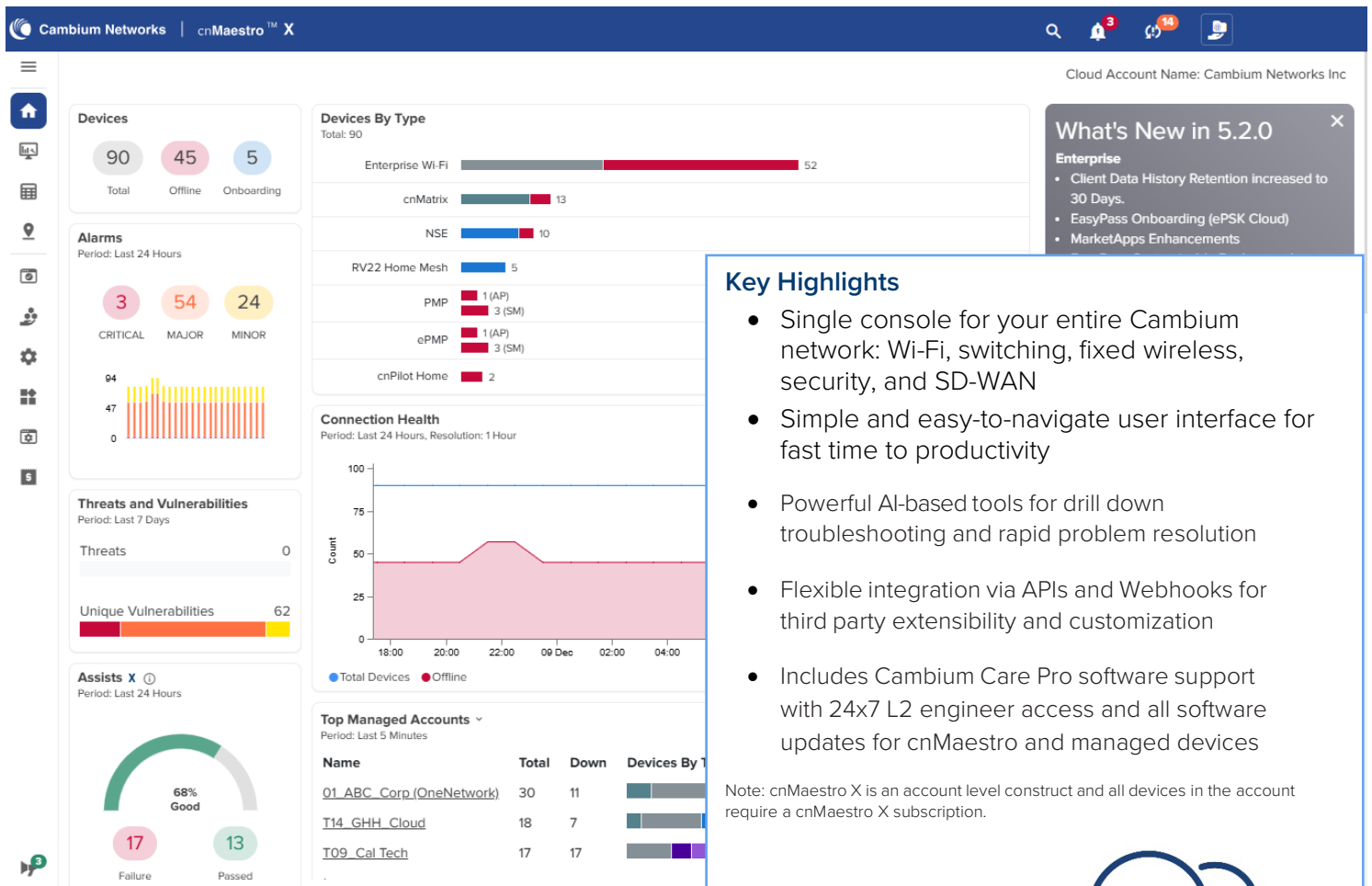
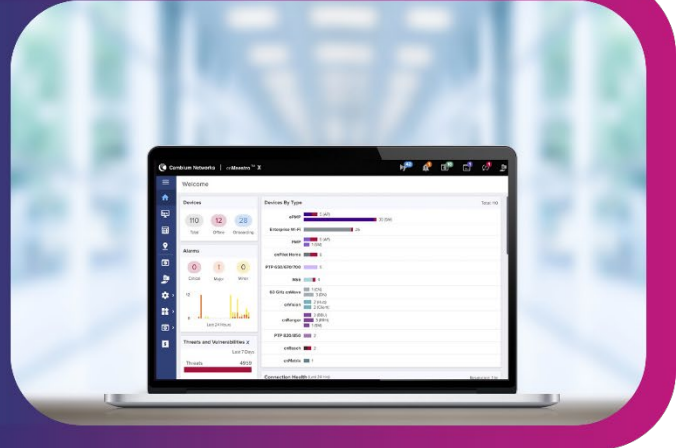
Wi-Fi Enhanced Open™ 2023-12

cnMaestro™ X Management System

cnMaestro Quick Look

A simple, yet sophisticated AI-based network management system for Cambium Networks wireless and wired solutions.

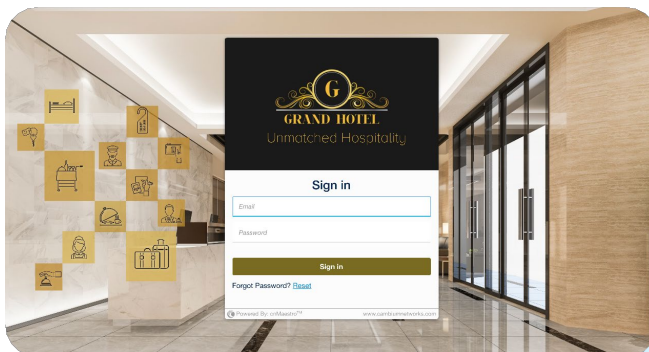
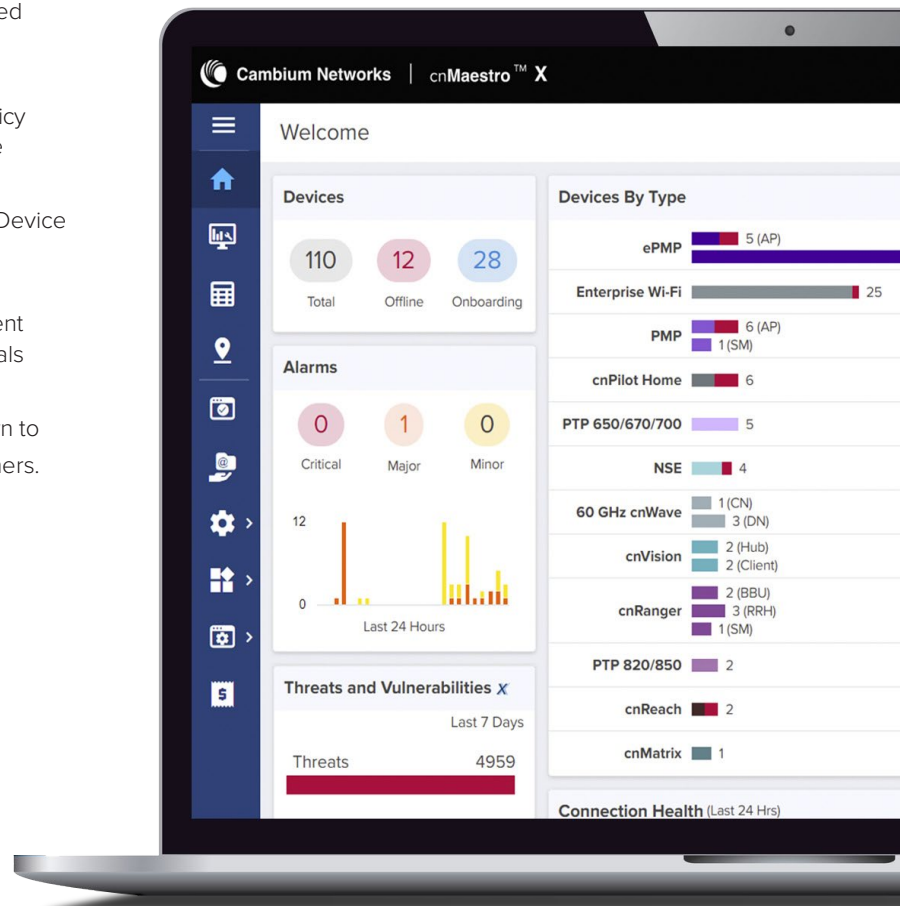
- Elastic scalability in a single-pane-of-glass experience for Cambium's ONE Network
- Secure, end-to-end network management with zero-touch provisioning
- Simplified operations and ongoing maintenance for the network administrator



cnMaestro™ X Management System

Advanced Functionality in cnMaestro X

- X Assurance provides AI-powered analytics to identify and fix wireless network issues, helping IT admins improve user experience by proactively finding root cause of problems.
- EasyPass offers diverse Wi-Fi onboarding options for employees, guests, attendees, and IoT, featuring advanced captive portals and one-year client login history.
- Application visibility and control provides analytics and policy control for 2400+ applications at the Wi-Fi and WAN edge
- Advanced cnMatrix switch features including QinQ, Auto Device Recovery (ADR) and cable diagnostics
- Customizable MSP dashboard with ability to create different brands with multi-tier customizations including guest portals
- Consolidated MSP tenant statistics with ability to drill down to manage a specific tenant without impacting data from others. Support for up to 200 managed tenants.
- Restful APIs and Webhooks for integration with existing OSS/BSS systems and event monitoring
- Assists function scans device configurations to identify potential vulnerabilities and recommends improvements to save time troubleshooting.
- Long-term historical data retention: 2-year data for FWB and 1-year data for Enterprise and IIoT devices
- RADIUS, TACACS+, LDAP, and AD Login for user administration



cnMaestro X allows MSPs to create a custom branding experiences for their customers.

cnMaestro™ X Management System

Key Functionalities

- Zero-touch provisioning: Create, provision, monitor and manage the entire network of wireless and wired devices from a single dashboard login with key performance metrics, alarms, and alerts. The cloud-first UI design is easy to learn and apply across the portfolio and helps network administrators simplify operations and deliver an optimal client experience.
- With centralized visibility and control for Cambium Networks' wireless and wired products, network administrators can quickly and easily deploy networks with minimal training. Whether you work on small sites or large distributed networks with thousands of sites, cnMaestro makes deployment and operations easy. Administrators have access to information needed to enforce policies and optimize performance. Remote support capability is integrated into the architecture, along with powerful help desk tools to debug remote issues without going onsite. Troubleshooting tools such as ping, traceroute, throughput, and live packet captures are included, dramatically reducing resolution times and enabling remote troubleshooting.
- Deployment flexibility and TCO: Choice of public cloud, private cloud, or on-premises deployment with best TCO. cnMaestro helps reduce operating costs and accelerate return on investment. cnMaestro does not require Wi-Fi controllers, thereby reducing the complexity and cost of deploying Wi-Fi networks.
- Built for scale and security at all levels: Devices connect to cnMaestro Cloud using SSL-enabling deployments without changes to the firewall configuration. Cambium Intelligent edge architecture enables fault-tolerant networks where the network continues to operate even when the cloud is unreachable due to a WAN outage. With cnMaestro X, you can manage networks with up to thousands of sites, and up to 25,000 devices.
- Tailored views for enterprise, access and backhaul, and IIoT: The access and backhaul view provides visualization and control of devices from service provider towers to the network edge.
- Supports network hierarchy, enabling easy configuration, monitoring, and debugging at network nodes to reduce operational costs. This is especially critical for large networks or small distributed networks with small on-site IT staff.
- Provides a bird's-eye view of network health with insights on performance, connectivity, and client experience. Administrators can quickly identify potential trouble spots and drill down from network to client-level details.
- Extensible platform for managing third-party endpoints.
- cnMaestro X supports the following Cambium solutions:
 - » Wi-Fi 6/6E/7 Access Points (APs)
 - » cnPilot™ E-series and R-series APs
 - » Xirrus XD, XH, XA, and XR 11ac APs
 - » cnMatrix™ EX1000/2000/3000, and TX1000/2000 Series Switches
 - » Network Service Edge (NSE)
 - » cnWave™ 60 GHz and 28 GHz
 - » PTP (point-to-point)
 - » PMP and ePMP™ (point-to-multipoint)
 - » PON
 - » cnReach
 - » cnRanger™

cnMaestro On-Premises Server Requirements	Resources	Enterprise	Fixed Wireless	Enterprise and Fixed Wireless
	8vCPUs, 16 GB RAM, 250 GB Hard Disk	10,000 Enterprise devices (Wi-Fi, cnMatrix, NSE)	20,000 Fixed Wireless devices (PMP, ePMP, PTP, cnReach, cnRanger)	10,000 total devices – Fixed Wireless and Enterprise (PMP, ePMP, PTP, PON, Wi-Fi, cnMatrix, NSE)
	16vCPUs, 32 GB RAM, 500 GB Hard Disk	25,000 Enterprise devices (Wi-Fi, cnMatrix, NSE)	40,000 Fixed Wireless devices (PMP, ePMP, PTP, cnReach, cnRanger)	25,000 total devices Fixed Wireless and Enterprise (PMP, ePMP, PTP, PON, Wi-Fi, cnMatrix, NSE)

cnMaestro™ X Management System

Product Summary *Features marked X require cnMaestro X subscription*

Onboarding & Provisioning

- Zero-touch onboarding
- Template configuration
- Object configuration (enterprise)
- Claim PMP SMs associated with AP
- cnMaestro Installer installation summary upload (PMP & ePMP) **X**
- Mass provisioning for ePMP/PMP/cnWave 60 GHz (using LINKPlanner) **X**
- Webhooks support **X**

Network Services

- Branded tenant login page **X**
- Support for software-defined radios (SDR) on XV3-8, XE3-4, & XE5-8 Wi-Fi 6 APs
- ePSK Types
 - o ePSK Local – ePSKs are cached locally on the Wi-Fi APs
 - 2,000 per WLAN (Wi-Fi 6+)
 - 300 per WLAN (Wi-Fi 5)
 - o ePSK RADIUS – ePSKs are limited via external radius server **X**
 - o ePSK Cloud – ePSKs are unlimited & cloud managed (Wi-Fi 6+) **X**
- Personal Wi-Fi **X**
- Number of guest portals: 500 **X**
- EasyPass
 - o One-click
 - o Sponsored guest **X**
 - o Voucher
 - o Paid **X**
 - Payment gateway **X**
 - » PayPal
 - » IPPay
 - » QuickPay
 - » mPesa
- o WiFi4EU
- o Azure guest portal **X**
- o Google authentication **X**
- o Self-registration: SMS & email **X**
- o Onboarding **X**
- o Combined options
- Max number of login events: Unlimited event records for 30 days **X**
- Max number of guest client sessions at a time: 10,000 **X**
- Max number of managed devices: **X**
 - 25,000 for enterprise
 - 40,000 for FWB
- Application visibility & control of over 2,400 different applications across the Wi-Fi access network **X**

Wi-Fi

- Simplified wireless LAN view
- Stateful firewall support
- Dynamic channel listing based on country, release, & SKU
- AP group & WLAN configuration
- Site support for collocated APs
- WIDS support **X**

X Assurance **X**

- Client connection lifecycle monitoring & analysis
- Root cause analysis of connection & service failures
- Network-wide client health monitoring & scoring

NOTE: X Assurance is available in cnMaestro X Cloud, but not in cnMaestro X On-Premises.

Troubleshooting & Forensics

- Tower-to-edge view
- Technical support dump export
- Rogue AP detection
- Wi-Fi packet capture
- ePMP/PMP link test
- Cambium Care Pro – 24/7 technical support, accelerated access to L2 engineers, & software updates/upgrades **X**

Security

- Communication over SSL
- No Inbound internet access
- Not-in-traffic path
- Disaster recovery

Deployment

- Cloud-hosted, delivered as a service
- Customer-hosted VMware OVA
- Amazon Marketplace AMI

Visualization

- Full Visibility across network
- Supports ePMP, cnMatrix, enterprise & residential Wi-Fi, PMP, PTP, cnReach, cnRanger
- Multiple product views
 - o Access & backhaul view
 - o Enterprise wireless view
 - o Industrial internet view
- Hierarchical device tree
- PMP/ePMP sector display
- Spectrum analyzer: PMP **X**
- cnWave 60GHz Interference Scan **X**

Configuration & Monitoring

- Redundant cloud services
- Scheduled system backup
- Automatic bulk software update
- Dedicated device dashboards
- Statistics & trending
- Email alerts
- Supporting concurrent device jobs **X**
- Configuration lock **X**
- Managed service provider accounts **X**
- Support for up to 200 accounts
- High availability (1+1) for On-Premises **X**
- Monitor Wi-Fi performance from client or AP to cnMaestro (On-Premises NMS; Cloud NMS – N/A) **X**
- Assists for cnMatrix, Wi-Fi, cnPilot-R, PMP, ePMP, cnWave 5G Fixed, & PTP 670/700 **X**

Data & Reporting

- Statistics reports exported in CSV
- Export UI tables in CSV or PDF **X**
- RESTful monitoring/provisioning API **X**
- Graphical reports **X**
- Long-term data retention **X**
 - o 2 years for FWB
 - o 1 year for enterprise & IIoT

Administration

- Management users: 200 **X**
- Role-based access
- Auto-provisioning **X**
- RADIUS, TACACS+, LDAP, & AD login **X**
- Advanced troubleshooting **X**
 - o Audit logs
 - o Audit syslog & event syslog (On-Premises NMS; Cloud NMS – N/A)
- Advanced monitoring **X**
 - o Session management
 - o User authentication (On-Premises NMS; Cloud NMS – N/A)
- cnWave 60 GHz MAP features
 - o Extensive network map RF link visualization **X**
 - o Auto-manage route
- Open ID/SAML authentication **X**

MarketApps **X**

- Managed Wi-Fi
- Self-Service Personal Wi-Fi

cnMatrix

- Zero-touch remote provisioning
- Policy-based automation (PBA) on EX2000/EX3000
- Cambium Sync on TX series
- DHCP client/server
- Automated voice VLAN
- Assists **X**
- QinQ **X**
- Auto-device recovery
- Cable diagnostics **X**
- PBA on EX1000 **X**
- MAC lists & location services for PBA **X**

Network Service Edge (NSE)

- Site-to-site VPN
- WAN flow preferences
- DHCP/RADIUS/DNS services
- Load balancing
- WAN QoS
- Firewall
- LAN vulnerability assessment
- Granular content filtering
- WAN failover policy & IP groups
- High Availability

cnMaestro™ X Management System

cnMaestro X Part Numbers

Tier	Product		cnMaestro X Subscription SKU
Free Tier	ePMP Hotspot	1000 Hotspot	No subscription needed
	cnPilot Home	All R-Series APs	
	cnRanger	All SM Models	
	cnVision	MAXr, MAXrp, MICRO, MINI	
	cnWave 60 GHz	All Client Nodes	
	ePMP	All SM Models	
	PMP	All SM Models	
Tier 3	Enterprise Wi-Fi	All cnPilot E-Series, XE/XV/X7-Series and Xirrus (AOS) APs	MSX-SUB-[Model]-1/3/5*
Tier 5	60 GHz cnWave	All Distribution Nodes	MSX-SUB-T5-1/3/5
Tier 6	cnWave 5G Fixed	All CPE Models	MSX-SUB-T6-1/3/5
Tier 7	cnWave 5G Fixed	All BTS Models	MSX-SUB-T7-1/3/5
Tier 20	cnMatrix	All cnMatrix Switches	MSX-SUB-[Model]-1/3/5*
Tier 21	cnVision	FLEXr, HUB360	MSX-SUB-EPMP-1/3/5
	ePMP	All AP Models	
Tier 22	PMP	All AP Models except 450m and 450mv	MSX-SUB-PMP450i-1/3/5
Tier 23	PMP	450m	MSX-SUB-PMP450m-1/3/5
Tier 24	cnRanger	All BBU Models	MSX-SUB-PTP-1/3/5
	cnReach	All cnReach Models	
	PTP	All PTP Models	
Tier 30	NSE 3000 Security	NSE 3000	No subscription needed
Tier 30	NSE 3000 Security Plus	NSE 3000	NSE-SUB-3000-1/3/5**

*cnMatrix Switches and Wi-Fi APs:

These products use model-based SKUs for subscription.

For Wi-Fi access points, the corresponding cnMaestro X SKU follows a specific format:

The base part of the SKU will be ""MSX-SUB-"" followed by the model name of the access point (e.g., XV2-21X).

The ending part will be ""-1/3/5"", indicating the subscription term duration (1, 3, or 5 years).

Similarly, for cnMatrix switches, the cnMaestro X SKU follows the same format based on the switch model name (e.g., EX3024F)

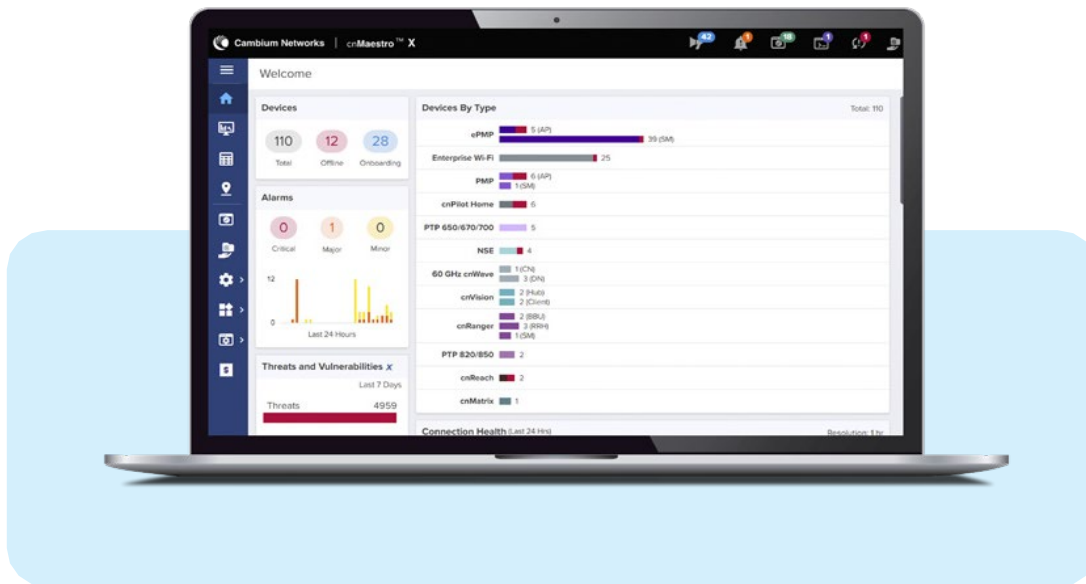
For example:

The SKU for 3-year cnMaestro X subscription for XV2-21X AP and a 5-year cnMaestro X subscription for an EX3024F switch would be:

SKU	Description
MSX-SUB-XV2-21X-3	cnMaestro X for one XV2-21X AP. Creates one Device Tier3 slot. Includes Cambium Care Pro support. 3-year subscription
MSX-SUB-EX3024F-5	cnMaestro X for one EX3024F. Creates one Device Tier20 slot. Includes Cambium Care Pro support. 5-year subscription

** Unlike other products, NSE3000 & RV22 devices need a subscription to be used on either cnMaestro X or cnMaestro Essentials.

cnMaestro™ X Management System



GET STARTED at

cloud.cambiumnetworks.com

Free 90-day trial of cnMaestro X:

cambiumnetworks.com/cnmaestro-x

ABOUT CAMBIUM NETWORKS

Cambium Networks enables service providers, enterprises, industrial organizations, and governments to deliver exceptional digital experiences and device connectivity with compelling economics. Our ONE Network platform simplifies management of Cambium Networks' wired and wireless broadband and network edge technologies. Our customers can focus more resources on managing their business rather than the network. We make connectivity that just works.

cambiumnetworks.com

02102025