



USER GUIDE

cnMaestro Cloud

Release 5.2.1



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.

Accuracy

While reasonable efforts have been made to assure the accuracy of this document, Cambium Networks assumes no liability resulting from any inaccuracies or omissions in this document, or from use of the information obtained herein. 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 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.

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
Introduction	19
Supported Devices and Features	19
Devices and minimum software versions	19
Supported browsers	22
Network connectivity	22
cnMaestro features	22
Quick Start	30
Create and manage accounts	30
Create a Cambium Support Center login	30
Create a cnMaestro account	33
Log on to cnMaestro	35
Claim and onboard devices	38
Claim devices by serial number	38
Claim devices by Cambium ID	40
Creating a Cloud Account	45
Overview	45
Creating a Support Center User ID	45
Creating a Cloud NMS Account	46
Creating an Anchor Account	49
Multiple Cloud Accounts	51
Account selection	51
Concurrent access	52
Managing users	52
Organization	54
cnMaestro X	54
NSE subscription	55
cnMaestro X Trial self-activation	55
cnMaestro X activation	56
Slot Deficit	60
Subscription Management	62
Manage Subscriptions	63
Usage Summary	64
Device Tiers	65

Devices	65
Expiry Notification	70
Retention of Data After Expiry and Reinstatement of Service	72
Overdraft Subscription	72
Download a Bill of Material (BoM)	73
cnMaestro X features behavior state	75
Navigating the cnMaestro UI	82
Account View	83
Home page	84
Page structure	84
Page navigation	85
Access and Backhaul View	86
Overview	86
Enterprise Account view	93
Overview	93
System	93
Devices	93
AP Groups	94
WLANs	95
Switch Groups	95
NSE Groups	96
Sites	96
Side menu	96
Section tabs	97
System status	97
Data Tables and Chart UI Controls	98
Logout	98
Device Onboarding	98
Onboarding Overview	99
Claiming Devices	99
Claiming Devices with Serial Number	100
Claiming Devices with Cambium ID	103
Onboarding Queue	104
Serial Number flow	104
Cambium ID flow	104
Onboarding fields	105

Onboarding Configuration	106
Onboarding Actions	107
60 GHz E2E Controller Onboarding	107
Header Notification	108
Zero Touch Configuration	108
Claiming Your First Wi-Fi AP (Cloud)	108
Claiming a single Wi-Fi AP from the Home page	109
Claiming a single Wi-Fi AP using the AP Group menu	110
Claiming multiple Wi-Fi APs from the AP Group	112
Claiming multiple Enterprise devices from the Enterprise Site dashboard	113
Claiming multiple Enterprise devices using CSV import	114
Points to consider when importing enterprise devices using CSV import option	116
Miscellaneous Onboarding Issues	117
Configuring Devices after Onboarding	117
Deleting Devices	117
Transferring Device Ownership	117
Onboarding Examples	117
Onboarding Existing Networks	117
Onboarding New Devices	117
Device-Specific Onboarding Instructions	118
Onboarding cnMatrix	119
Onboarding cnRanger	120
Onboarding cnReach	121
Onboarding cnPilot R-Series	122
Onboarding cnVision	123
Onboarding Enterprise AP	124
Onboarding ePMP 1000	125
Onboarding PMP	126
Onboarding PTP 650/670/700	127
Onboarding Xirrus device	128
Onboarding a cnWave 5G Fixed BTS device	129
Onboard Edge Controller	134
Onboard PTP 820/850 devices	134
Onboarding the NSE 3000 Devices	135
Onboarding Home Mesh Routers	137
Onboarding PON devices	137

Onboarding 60 GHz cnWave devices	138
Deleting Devices in Bulk	143
Device-specific restrictions	144
Deleting devices in bulk	145
Viewing the status of device deletion and retrying	146
Monitoring	149
Network Monitoring	149
Assists X	149
Dashboard	158
Notifications	162
Events	164
Alarms	173
Alarm History	176
Wi-Fi Events	178
Configuration	178
Statistics and Details	180
Statistics page	180
Details page	190
Performance	219
Map	234
Map Navigation	236
Mode	237
Sector Visualization	237
Tools	242
60 GHz cnWave Tools	242
cnMatrix Tools	242
cnPilot Home Tools	249
cnRanger Tools	252
cnReach Tools	253
cnVision Tools	254
Edge Controller Tools	255
Enterprise Wi-Fi Tools	256
ePMP Tools	262
PMP Tools	264
cnWave 5G Fixed Tools	266
RV22 Home Mesh Tools	269

Wireless Intrusion Detection System (WIDS)	273
Wireless Intrusion Prevention System (WIPS)	282
Network Service Edge (NSE 3000)	283
Dashboard	284
Notifications	284
Configuration	285
Advanced Settings	286
Factory Reset	288
User-Defined Overrides	289
Configuration Lock	290
Security	291
Threats	291
Vulnerabilities	293
Network	300
LAN	300
Routes	301
WAN	301
VPN Sites	302
Debug Tools	303
Clients	306
Device-level information	306
Network- and Site-level information	308
Client Dashboard	311
Certificate	314
Wireless LAN Dashboards	315
Wi-Fi Monitoring	315
Dashboard	315
Clients	316
Client Dashboard	321
Renaming Client Host-names	322
Details	323
Mesh Peers	326
Site Dashboard	327
RF Quality	332
Floor Plan	333
WLANs Dashboard	338

Fiber OLT and ONU	342
Dashboard	343
Notifications	347
Configuration	348
Details	349
Performance	350
ONU	350
Ports	352
Software Update	353
ONU Dashboard	354
Inventory	357
Inventory Export	358
Bulk Delete	358
Bulk Reboot	359
Schedule Reboot	360
Import Device Configuration	360
Sample Configuration File	361
Sample Configuration File (60 GHz cnWave)	361
Uploading a Configuration File	362
Reports	364
Data Reports	365
Devices Report	366
Audit Logs Report	376
Performance Report	377
Active Alarms Report	384
Alarm History Report	385
Events Report	386
Wireless Clients Report	387
Wi-Fi Events Report	388
Guest Access Login Events	389
Report Jobs	390
Graphical Reports	391
Create Graphical Report Templates	393
Generate Reports Based on Templates	397
Provisioning	399
Software Update	399

Software Update Overview	399
Create Software Update Job	400
Software Update Jobs and Parameters	408
Viewing Running Jobs in header	410
Fixed Wireless Configuration	410
Overview	410
Configuration Templates	411
Configuration Variables	411
Macros	412
Variable Caching	412
Device Type-Specific Configurations	412
Variable validation	412
Sample Templates	412
Template file creation	412
Template	413
BTS and CPE Configuration	415
Configuration Template for PTP 820/850	416
Configuration Update	419
Device Selection	419
Device Type	419
Device Table	420
Configuration Update Steps	421
Configuration Jobs	421
Configuration Update at Onboarding	422
Wi-Fi Configuration	422
Enterprise Wi-Fi AP	423
Configuring Enterprise Wi-Fi APs using Wi-Fi Profiles	423
Pre-Defined Overrides	470
User-Defined Overrides	471
User-Defined Variables	472
Bulk Overrides	473
Synchronize (Sync) Configuration	480
Configuration Job Status	481
Factory Reset	482
Association ACL	484
Overview	484

Configuring Association ACL	484
Access Control Policies	485
Configuring Access Control Policies for AP Groups and WLANs	485
Custom Applications	487
cnMatrix Switches	489
Switch Group Configuration	489
Synchronize (Sync) Configuration	499
Policy Based Automation (PBA)	501
Switches	505
Switch Ports	512
Device Details	521
60 GHz cnWave Network Configuration	524
Managing E2E Network	524
Site Configuration	594
Node Configuration	597
PoP Node	603
DN/CN Node	625
Managing NSE 3000 using cnMaestro	636
Claiming an NSE 3000 device associated with a site	636
High availability support for NSE 3000	638
Licensing	638
Constraints on NSE 3000 devices	639
Creating an HA pair in cnMaestro	639
Onboarding an NSE 3000 device as an HA spare	639
Claiming an NSE 3000 device as an HA spare	642
Moving the HA pair (in the tree)	643
Deleting an NSE 3000 device from the HA pair	643
Deprecation of device overrides	643
Upgrading the firmware	644
Viewing aggregated data of HA pair	644
Creating Wireguard clients for NSE HA pair	645
Configuring NSE 3000	645
Basic	646
Management	647
Network	649
Groups	662

WAN	664
Firewall	677
DNS	687
Threat Protection	691
VPN	694
User-Defined Overrides	705
Configuring WAN in the device UI	706
Configuring Auto VPN	709
Hub and Spoke mode	710
Mesh mode	710
Disabling or Enabling the Security Plus License Mode for NSE	720
Disabling the Security Plus mode	722
Enabling the Security Plus mode	724
Configuring Advanced Features	726
Lock Device Configuration	726
Strict Device Password Policy	726
Auto-Provisioning	727
Creating Auto-Provisioning Rule	727
Managing Home Mesh Router	728
Configuring Home Mesh Router	730
Configuring WLAN Profiles (SSIDs)	730
Configuring AP Groups	734
Onboarding the Home Mesh Router to cnMaestro	747
cnMaestro Subscriber application branding	747
Adding a Home Site	748
Managing subscribers (end-customer)	749
Adding a Subscriber Service Profile	750
Adding a subscriber	751
Claiming the Home Mesh Router	754
Setting up the Home Mesh Router	756
Setting up the Home Mesh Router—Standalone mode	756
Setting up the Home Mesh Router—Wireless Mesh Mode	757
Wireless mesh: 1-1 deployment	757
Wireless mesh: 1-1-1 deployment	758
Wireless mesh: 1-2 deployment	760
Wireless and wired mixed mesh 1-2 deployment	761

Setting up the Home Mesh Router—Wired Mesh Mode	763
Wired mesh: 1-1 deployment	763
Wired mesh: 1-1-1 deployment	764
Wired mesh: 1-2 deployment	764
Viewing router system information and network traffic status	765
Viewing, editing, and blocking connected clients	767
Viewing connected clients	767
Editing a client's host name	768
Blocking clients	768
Monitoring and troubleshooting the Home Mesh Router	768
Monitoring the Home Mesh Router	769
Home Site Dashboard	769
Notifications	769
Software Update	772
Performance	772
Troubleshooting the Home Mesh Router	775
Status	775
Debug	776
Network Connectivity	776
Wi-Fi Analyzer	777
Speed Test	778
Packet Capture	780
Upgrading the Home Mesh Router firmware	781
Assurance X	783
Analyzing Connection Failures of Wi-Fi Clients and Poor Performance of Wi-Fi Networks	783
Overview	783
Use cases	787
Resolve connectivity issues	787
Address poor performance of applications	787
Identify OS, SSID, and AP-specific issues	787
Accessing the Assurance X page	788
Accessing Site-level consolidated details at the System- and MSP-levels	791
Setting filters to view the connection data	791
Suppressed clients	794
Viewing the connection events	798
Dashboard page	798

Assurance X page	799
System-level Assurance	821
Managed Services	823
Managed Accounts	823
Overview	823
Managed Accounts	823
Accounts	824
Managed Account Service	824
Account Service Users (Administrators)	825
Configuring Managed Account Services	827
Enable Managed Accounts	827
Creating Managed Account Services	829
Creating Account	831
Validating Account Users	832
Managed Account Administration	835
Overview	835
System Dashboard	837
Account Administration	838
Device Management	838
Disabling the Managed Accounts feature	840
Managing subscribers (end-customer)	840
Adding a Subscriber Service Profile	840
Adding a subscriber	842
Claiming the Home Mesh Router	845
Network Services	848
API Client	849
Overview	849
API Clients	849
RESTful API Specification	850
Authentication	850
Swagger API	854
Introduction	854
API Session	856
Introduction	856
Retrieve Access Token	856
Access Resources	857

API Details	857
HTTP Protocol	857
REST Protocol	858
Parameters	860
Access API	864
Token (basic request)	864
Token (alternate request)	865
Validate Token	866
API Changes	867
Sunsetted APIs/Fields	867
Deprecated APIs/Fields	867
Devices, Statistics, and Performance APIs	868
Overview	868
cnMaestro v2 API	868
Devices API Response (v2 Format)	868
Statistics API Response (v2 Format)	872
Performance API Response (v2 Format)	884
Client API Response (v2 Format)	891
External Guest Access Login API	893
60 GHz cnWave RESTful API	894
EasyPass	898
Guest/Public Access	900
Employee/Student Access	900
Combined	901
Implementation of EasyPass portals for various types of users	902
EasyPass configuration	902
Creating a portal	903
Configuring common parameters	907
Accessing the common tabs	924
Creating One Click portal	928
Creating Self Registration X portal	929
Creating Sponsored Guest X portal	938
Creating Voucher portal	939
Creating Paid X portal	940
Creating WiFi4EU portal	940
Creating Microsoft Azure X portal	941

Creating Google Login X portal	943
Creating Onboarding X portal	945
Adding a new user	948
Importing user data using a CSV file	950
Creating One Click + Voucher portal	952
Creating One Click + Paid X portal	952
Creating Voucher + Paid X portal	952
MarketApps X	953
Overview	953
Target audience	954
Benefits	954
Prerequisites	954
Key features	954
Adding a new MarketApps App	955
Managed Wi-Fi app	956
Basic tab	956
Settings tab	957
Design tab	960
Self-Service Personal Wi-Fi app	962
Basic tab	963
Personal Wi-Fi configuration	963
How to configure units by property managers	964
Units managed in the Managed Wi-Fi app	965
Units managed in Self-Service Personal Wi-Fi App	981
Installer App	986
Basic tab	987
Settings tab	987
Design tab	988
Accessing the Installer App interface	989
Citizens Broadband Radio Service (CBRS)	998
Enabling CBRS in Cloud	999
Management Tool	1005
Domain Proxy View	1025
Searching a Domain Proxy Sector	1025
Domain Proxy Sector view	1025
Searching a Domain Proxy in Non Sector View	1026

Actions for Existing CBRS On-Premises Users	1028
Link an Anchor Account to this Account	1029
Convert this Account to Anchor Account	1030
Organizations for CBRS	1031
Create an Organization	1032
Primary Account	1032
Secondary Account	1034
Removing Accounts	1037
Remove through Primary Account	1037
Remove Organization from Secondary Account	1039
Disable Secondary Account services	1041
Edit Services	1045
Share CBRS Configuration with the On-Premises Instance	1049
Organization History	1050
LTE	1050
Adding SIM Cards	1050
Managing Edge Controller	1053
Topology Sync	1054
Edit	1054
Delete	1054
Dashboard	1055
Configuration	1056
Rules	1056
Blacklist	1059
Advanced Settings	1060
Tools	1061
Diagnostics	1061
Operations	1064
Services	1064
Monitoring	1065
Installation Summary	1065
Configuration	1068
Photos and Location	1068
Link Test Result	1068
AP Scan Result	1068
Spectrum Analyzer X	1069

Administration	1076
Users	1076
Managing Users	1076
Role-Based Access	1076
Creating Users and Configuring User Roles	1081
Whitelisting specific domains	1082
Assigning roles for IdP-based domain users	1084
Advantages	1084
Prerequisite tasks	1084
Assigning roles for IdP-based domain users	1085
Session Management	1085
Sessions	1086
Cloud Anchor Account	1086
Manage Instances	1086
Onboarding	1086
On-Premises Instances	1088
Notifications	1089
Inventory	1089
Administration	1089
Users	1090
Session Management	1091
Network Services	1091
CBRS	1091
Organization	1091
Manage Subscriptions	1091
Subscriptions	1092
Devices	1092
Audit Logs	1093
Settings	1096
Email Notifications	1096
Adding Recipient to Subscriber Table	1097
Account Type	1099
Managing Device software images under Automatically Update Device Software section	1099
Updating Company Information	1100
Updating information through the Company Information page	1103

Appendix	1104
Guest Access	1104
Configuration	1105
Creating the Guest Access Portal in cnMaestro	1105
Mapping the device to Guest Access Portal in cnMaestro	1126
Access Types	1128
Guest Access using Social Login	1129
Guest Access Portal Logout	1140
SMS Authentication	1141
Generic SMS Gateway configuration	1141
Network Port Requirements	1147
Network Port Requirements for Outbound Access	1147
XMS-Enterprise to cnMaestro X	1148
XMS-E System	1148
Export Golden Configuration	1149
Migrate to cnMaestro X	1152
Create Wi-Fi AP Group	1153
Approve APs into Wi-Fi AP Group	1155
Import and Apply AP configuration	1156
Converting Tier 2 Unused Slots	1158
Cambium Networks	1161

Introduction

cnMaestro is Cambium Networks next-generation network management platform. It is available in two versions: **cnMaestro Essentials** and **cnMaestro X**.

- cnMaestro Essentials is free and provides basic network management support for Cambium Networks devices.
- cnMaestro X is a paid service that includes advanced features such as long-term statistics.
- Both versions are available in cloud and on-premises deployments.

This section covers the following topics:

- [Supported Devices and Features](#)
- [Quick Start](#)
- [Creating a Cloud Account](#)
- [cnMaestro X](#)
- [UI Navigation](#)
- [Device Onboarding](#)

Supported Devices and Features

Devices and minimum software versions

The following table lists the device model and the minimum software version supported by cnMaestro (not the recommended software version).

Table 1 *Supported devices and minimum software versions*

Device	Minimum Software Version
60 GHz cnWave V1000	1.1
60 GHz cnWave V2000	1.2.2
60 GHz cnWave V3000	1.1
60 GHz cnWave V5000	1.1
cnMatrix	2.1-r5
cnPilot e400/e500	3.11.4.1-r3
cnPilot e425H/e505	4.1-r3
cnPilot e430W/e410/e600	3.11.4.1-r3
cnPilot e501S	3.11.4.1-r3
cnPilot e502S	3.11.4.1-r3
cnPilot e510	3.11.4.1-r3
cnPilot e700	3.11.4.1-r3
cnPilot r190V/r190W	4.6-R16
cnPilot r195P	4.7-R6
cnPilot r195W	4.6-R16

Table 1 *Supported devices and minimum software versions*

Device	Minimum Software Version
cnPilot r200/r200P/r201/r201P	4.6-R16
cnRanger Sierra 800	1.1-r3
cnRanger Tyndall 101	1.1-r3
cnRanger Tyndall 201	2.0-r1
cnReach N500	5.2.19h
cnVision Client	4.6
cnVision Hub	4.6
cnWave 5G Fixed B1000	2.0
cnWave 5G Fixed C100	2.0
ePMP 1000	4.5.0
ePMP 2000	4.5.0
ePMP 3000	4.5.0
ePMP 3000L	4.5.0
ePMP 4600	5.4.0
ePMP 4600L	5.4.0
ePMP Elevate	3.2
ePMP Elevate SXGLIT5/LHG5	4.5.0
ePMP Elevate XM/XW	4.5.0
ePMP Force 130 2.4 GHz	4.5.0
ePMP Force 130 5 GHz	4.5.0
ePMP Force 180/200	4.5.0
ePMP Force 190	4.5.0
ePMP Force 200L	4.7.0
ePMP Force 300	4.5.0
ePMP Force 300-13	4.5.0
ePMP Force 300-13L	4.5.0
ePMP Force 300-13LC	4.5.0
ePMP Force 300-19	4.5.0
ePMP Force 300-19R	4.5.0
ePMP Force 300-22L	4.6
ePMP Force 300-25L	4.6
ePMP Force 300 CSM	4.3.2
ePMP Force 400	5.1.0.18
ePMP Force 425	5.1.0.18
ePMP Force 4500	5.4.0
ePMP Force 4525	5.4.0
ePMP Force 4600C	5.4.0
ePMP Force 4625	5.4.0

Table 1 *Supported devices and minimum software versions*

Device	Minimum Software Version
ePMP MP 3000	4.5.0
ePMP PTP 550	4.5.0
ePMP PTP 550E	4.5.0
NSE 3000	1.0
PMP 450i	22.1.2
PMP 450 MicroPoP Omni	22.1.2
PMP 450 MicroPoP Sector	22.1.2
PMP 450b Retro	22.1.2
PMP 450v	23.0
PON (OLT and ONU)	1.1.0
PTP 650	01-50
PTP 670 (650 Emulation)	01-50, 03-12
PTP 670, PTP 700	03-11
PTP 820, PTP 850	11.9
XV3-8	6.6.0.3
XV2-2	6.6.0.3
XV2-2T0	6.6.0.3
XV2-2T1	6.6.0.3
XV2-22H	6.6.0.3
XV2-21X	6.6.0.3
XV2-23T	6.6.0.3
XE3-4	6.6.0.3
XE3-4TN	6.6.0.3
XE5-8	6.6.0.3
X7-35X	7.0
RV22 Home Mesh Router	1.0.0

Table 2 *Supported Xirrus device models*

Device Model	Minimum Software Version
Wave 2 APs: <ul style="list-style-type: none"> • XA4-240 • XD2-230 • XD2-240 • XD4-240 • XH2-240 	8.7.0
Wave 1 APs: <ul style="list-style-type: none"> • XD4-130 • XH2-120 • XR-630 	8.7.0

Table 2 *Supported Xirrus device models*

Device Model	Minimum Software Version
<ul style="list-style-type: none"> XR-620 	
Wave 1/2 Modular 4-radio: <ul style="list-style-type: none"> XR-2436/Wave 2 XR-2426 XR-4436 XR-4426 XR-2226 XR-2236 XR-2247 XR-2447 XR-4447 	8.7.0
Wave 1 Modular 8-radio: <ul style="list-style-type: none"> XR-4836/Wave 2 XR-4826 	8.7.0

Supported browsers

The following table lists browsers supported by cnMaestro on different operating systems:

Table 3 *Supported browsers*

Operating System	Browser	Version
Linux	Chrome	49 and above
	Firefox	45 and above
macOS	Safari	9 and above
MS Windows	Chrome	49 and above
	Firefox	45 and above
	Microsoft Edge	44.17763.1.0 and above

Network connectivity

Cambium devices use <https://cloud.cambiumnetworks.com> over port 443 to access cnMaestro in the cloud. The devices initiate the connection, and they can be located in a private subnet behind a NAT firewall.

cnMaestro features

The following table lists the features shared between the on-premises and cloud deployments.



Note

Features marked with an **X** mark indicate that they require a cnMaestro X subscription.

Table 4 Features supported by cnMaestro

Feature	Description	Cloud	On-Premises
Account Recovery	Ability to resolve password and account recovery issues locally.		✓
Advanced Troubleshooting	Display tower-to-edge status in a single graphic, which is used to: <ul style="list-style-type: none"> View Wi-Fi client details and health. Troubleshoot client connectivity directly on the AP. 	✓	✓
Access Control Policies	Configure policies that define who can connect to the network, and when they are allowed to connect and access a specific device.	✓	✓
Automated Frequency Coordination (AFC) X	Manage and allocate radio frequencies efficiently for a specific region or country.	✓	
Assurance X	View the health of Wi-Fi client connections, including root cause analysis of failures and possible remediations.	✓	
AP Group Configuration	Support configuration of Enterprise Wi-Fi and cnPilot Home devices.	✓	✓
AP Group Dashboard	Display aggregate Wi-Fi AP statistics for the configured AP Group.	✓	✓
API Client X	Create API clients and access tokens to programmatically manage deployments using customer's own client applications.	✓	✓
Applications X	View details of applications accessed by users in a particular site.	✓	✓
Auto-Provisioning X	New devices, such as cnPilot Home (R-Series), cnVision, Enterprise Wi-Fi, Enterprise Wi-Fi (Xirrus-Series), ePMP, and PMP, can automatically be approved and onboarded using the subnet.	✓	✓
Assists X	Assists scans the configurations and generates assists scores.	✓	✓
Association ACL	Configure a MAC association list that is used to allow or deny client associations with the APs.	✓	✓
Audit Logs X	Record administrator activities.	✓	✓
60 GHz cnWave Auto Manage Routes	Support automated IPv6 routes for Distribution Node (DN) and Client Node (CN) based on topology and status of Point of Presence (PoP) Node.	✓	✓
Automatic Device Software Updates	Automatically update device software during onboarding or reconnection.	✓	✓
Backup and Restore	Backup or restore configuration and monitoring data from cnMaestro.		✓
Bulk Acknowledge Alarms	Acknowledge multiple alarms and clear them in a single action.	✓	✓
Bulk Image Upgrade	Schedule software image upgrades across sectors and device groups.	✓	✓
Certificate Management	SSL certificate management is available for the UI and Guest Access Portal.		✓
Citizen Broadband Radio Service Subscription (CBRS)	Support CBRS-compliant devices in the 3.6 GHz band (from 3550 MHz to 3700 MHz).	✓	✓

Table 4 Features supported by cnMaestro

Feature	Description	Cloud	On-Premises
Client -Application Visibility X	Allows methods to control or block applications, or terminate based on consumption of applications.	✓	✓
Client - Renaming the host-name	Rename wireless and wired client host-names to more appropriate names for easy reference.	✓	✓
Cloud Connectivity	Automatically download device software from the cloud.	✓	✓
Cloud Synchronization	Allows connection to the Cloud Anchor account and also push announcements form Cloud Anchor account to On-Premises instances.		✓
Configuration Backup	Backup configuration from fixed wireless devices (cnVision, PMP and ePMP) and cnReach devices that are currently online.		✓
Current Best Route(s) X	<p>View the best route from a CN or DN to PoP.</p> <p>The Current Best Route(s) X map view displays statistics of the following parameters for uplink and downlink of wireless link of a node:</p> <ul style="list-style-type: none"> • Golay • SNR • MCS • RSSI • Throughput (Mbps) • Airtime (%) • Link Fade Margin (LFM) <p>Applicable only to 60 GHz cnWave devices.</p>	✓	✓
Custom Applications X	Configure applications with a specific IP address or a domain name, and apply filter rules.	✓	✓
Deployment—cnMaestro	<p>The Cloud version is fully hosted and maintained by Cambium Networks at https://cloud.cambiumnetworks.com.</p> <p>The cnMaestro On-Premises version is released as an OVA (Open Virtualization Archive) file that needs to be installed on either VMware or VirtualBox.</p>		✓
Device Auto Refresh X	Device Auto Refresh allows to refresh data automatically in the E2E Network.		✓
Device Connectivity	<p>In the Cloud version, all devices can be accessed through https://cloud.cambiumnetworks.com.</p> <p>In the cnMaestro On-Premises version, all devices contact the local cnMaestro server. The devices must be configured to access the server before they can be managed. Alternatively, DHCP options can be configured to provide the cnMaestro URL when the device boots up.</p>	✓	✓
Device Image	In the Cloud, device images are automatically available.	✓	✓

Table 4 Features supported by cnMaestro


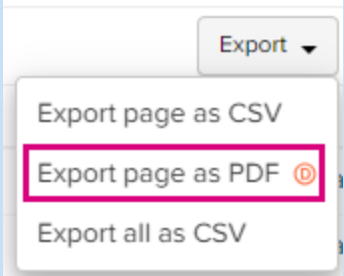
Feature	Description	Cloud	On-Premises
Management	In the cnMaestro On-Premises device, new images need to be downloaded from Support Center and added to the cnMaestro server. Device image can be downloaded from the anchor.		
Device Inventory	Aggregate inventory data for a group of devices at the System, Network, Tower, Sector, or Site level in CSV format. <div>  <div> <p>Note</p> <p>The Export page as PDF option is deprecated from cnMaestro release 5.2.0 onwards. This option will be completely removed from the UI from release 5.3.0.</p>  </div> </div>	✓	✓
EasyPass	Create captive portal to allow clients to access the network through the following portal types: <ul style="list-style-type: none"> One Click Paid X Self Registration X Sponsored Guest X Voucher WiFi4EU—Available only in the European Union 	✓	✓
EasyPass—Microsoft Azure, Google Login	Create captive portal to allow clients to access the network through the following portals: <ul style="list-style-type: none"> Microsoft Azure X and Google Login X portals. 	✓	
Edge Controller	Configure Edge Controllers to discover PTP 820/850 devices in a network using SNMP protocol.	✓	✓
Email Notifications	Send email when the alarm status changes.	✓	✓
Enterprise View	Display a simplified UI tailored for Enterprise Wi-Fi.	✓	✓
Hierarchical Dashboards	Visualize devices from tower to edge through customized dashboards for each device type.	✓	✓
Installation Summary X	Displays the installation summary of the following devices installed using the Cambium Networks Installer application: <ul style="list-style-type: none"> PMP SMs 	✓	✓

Table 4 Features supported by cnMaestro


Feature	Description	Cloud	On-Premises
	<ul style="list-style-type: none"> ePMP SMs cnMatrix Enterprise Wi-Fi APs 		
Interference Scan X	<p>Applicable only to 60 GHz cnWave devices.</p> <p>End-to-end, Controller-coordinated scan that aims at performing real-time measurements of interference affecting a specific interfered link (referred to as the victim link). The Controller filters the network topology to identify potential interfering links (known as aggressor links).</p>	✓	✓
IPv6 Support	Provide IPv6 support for cnPilot Enterprise, cnPilot Home (R-Series), and ePMP devices.	✓	✓
High Availability (HA)	Support the High Availability of Layer 2 through an Active-Standby (1+1) architecture.	✓	✓
Home Mesh Routers	Onboard and manage Home Mesh Routers (RV22).	✓	
Link Throughput Test X	<p>Test the throughput between the link end points.</p> <p>Applicable only to 60 GHz cnWave devices.</p>	✓	✓
Local and Authentication Server Administrators	<p>Multiple types of administration access for local administrators (with a username and password maintained by cnMaestro) or authentication services (including TACACS+, RADIUS, LDAP X, Active Directory, OpenID Connect, and SAML).</p> <div>  <div> Note LDAP is a cnMaestro X feature. </div> </div>		✓
Long Term Historical Data X	<p>Display long-term performance graphs for the following:</p> <ul style="list-style-type: none"> Fixed Wireless Broadband up to 2 years. Wi-Fi APs, IIoT, and cnMatrix up to 1 year. 	✓	✓
LTE	Manage cnRanger LTE devices.	✓	✓
Managed Services X	Allow cnMaestro account owners to split their installation into separate Managed Accounts. Each Managed Account contains independent administration and configuration.	✓	✓
Maps and Map Modes—Street View	Leverage maps to position devices and visualize their health and connectivity. Change the map mode to display various wireless key performance indicators.	✓	✓
Maps and Map Modes—Satellite and Terrain X		✓	✓
MarketApps X	<p>Simplifies management and deployment of Wi-Fi services for property managers, residents, field installers, and service providers with the help of the following applications for the Multi-Dwelling Unit (MDU) market::</p> <ul style="list-style-type: none"> Managed Wi-Fi 	✓	

Table 4 *Features supported by cnMaestro*

Feature	Description	Cloud	On-Premises
	<ul style="list-style-type: none"> Self-Service Personal Wi-Fi Installer App 		
Mesh Peers	Displays details of available mesh clients.	✓	✓
Multiple Administrators	Invite colleagues by email to manage the account with an assigned role.	✓	✓
Multiple UI Views	<p>Support the following tailored views in the cnMaestro UI:</p> <p>Access and Backhaul View: Used for managing Fixed Wireless and Wi-Fi deployments, including the following:</p> <ul style="list-style-type: none"> 60 GHz cnWave cnMatrix cnPilot Home (cnPilot R-Series) cnRanger cnVision cnWave 5G Fixed Enterprise Wi-Fi (E-Series and XE/XV/X7-Series) and cnPilot Enterprise APs Enterprise Wi-Fi (Xirrus-Series) ePMP NSE PMP PON PTP 650/670/700 PTP 820/850 RV22 Home Mesh <p>Enterprise View: Used for managing Wi-Fi deployments, including the following:</p> <ul style="list-style-type: none"> cnMatrix Enterprise Wi-Fi (E-Series and XE/XV/X7-Series) and cnPilot Enterprise APs Enterprise Wi-Fi (Xirrus-Series) NSE <p>Industrial Internet View: Used for managing Fixed Wireless, Wi-Fi, and IIoT deployments, including the following:</p> <ul style="list-style-type: none"> 60 GHz cnWave cnMatrix 	✓	✓

Table 4 *Features supported by cnMaestro*

Feature	Description	Cloud	On-Premises
	<ul style="list-style-type: none"> • cnPilot Home (cnPilot R-Series) • cnRanger • cnReach • cnVision • cnWave 5G Fixed • Enterprise Wi-Fi (E-Series and XE/XV/X7-Series) and cnPilot Enterprise APs • Enterprise Wi-Fi (Xirrus-Series) • ePMP • NSE • PMP • PON • PTP 650/670/700 • PTP 820/850 • RV22 Home Mesh 		
Multi-Floor Plans	Multiple floor plans for Sites.	✓	✓
Notifications	Communicate immediate status with stateful alarms and events. Notifications help troubleshoot customer issues.	✓	✓
Node Throughput Test X	Test the throughput between a node and PoP. Using this option, you can conduct a throughput test for each hop seamlessly. Applicable only to 60 GHz cnWave devices.	✓	✓
NSE	Onboard and Manage Network Service Edge (NSE) devices.	✓	
Onboarding	In the Cloud version, devices onboard using either the device Manufacturer Serial Number (MSN) or through the Cambium ID or Onboarding Key (entered on the device). In the cnMaestro On-Premises version, all the cloud modes of onboarding or devices contacting cnMaestro are added to the Onboarding Queue, where they are approved and managed.	✓	✓
On-Premises Console	Configure networking parameters and update the system password using the CLI available through the virtual machine console.		✓
Organization X	Allow users to manage multiple accounts through a single CBRS payment subscription.	✓	✓
PON (OLT/ONU)	Onboard and manage Passive Optical Network (PON) devices, including Optical Line Terminal (OLT) and Optical Network Unit (ONU).	✓	✓
RADIUS Proxy	Proxy RADIUS packets are sent through cnMaestro (On-Premises) instead of directly to the RADIUS server from the AP.		✓

Table 4 Features supported by cnMaestro

Feature	Description	Cloud	On-Premises
Reports X (Data, Graphical, and Graphical Report Template)	<ul style="list-style-type: none"> Export Active Alarms, Alarm History, Audit Logs, Devices, Events, Guest Access Login Events, Performance, Wi-Fi Events, and Wireless Clients data in CSV format. Generate various data in graphical format and export the details in a PDF file. 	✓	✓
RESTful API X	Support HTTPS RESTful API for inventory, monitoring, performance, notification, and basic provisioning.	✓	✓
Role-Based Access	Assign the following roles to users: <ul style="list-style-type: none"> Super Administrator Administrator Operator Monitor CPI 	✓	✓
Scheduled Configuration Update	Specify a time to configure devices.	✓	✓
Scheduled Software Update	Specify a time to install device software.		✓
cnMaestro Software Upgrade	Enable three types of software upgrade: <ul style="list-style-type: none"> Virtual machine upgrade requires the customer to replace the entire virtual machine with a new instance. The configuration and the data are exported from the old instance and imported to the new. Package upgrade only updates the cnMaestro software. It does not require a virtual machine reinstallation. OVA upgrade only overwrites the OS partition. 		✓
Server Management	Monitor virtual machine parameters such as disk, memory, and CPU utilization through the UI. This feature is available only on cnMaestro On-Premises.		✓
Site Dashboard	Aggregate Wireless LAN AP statistics by location.	✓	✓
SNMP X	Basic SNMP for inventory and alarms.		✓
Spectrum Analyzer X	Analyze and monitor the wireless spectrum for optimizing network performance on PMP devices.	✓	✓
Statistics and Trending	Present historical radio and network statistics.	✓	✓
Syslog	Forward audit and event logs to a configured external Syslog server.		✓
Switch Groups	Support shared configuration across cnMatrix switches.	✓	✓
System Events	System events for cnMaestro On-Premises server instance.		✓
System Log	Forward events to a remote system log server. This feature is available only on cnMaestro Cloud.		✓

Table 4 Features supported by cnMaestro

Feature	Description	Cloud	On-Premises
Template-Based Configuration	Schedule configuration of single devices or a group of devices across your network by using templates for cnPilot Home (R-Series), cnMatrix, cnReach, cnVision, ePMP, PMP, and PTP 820/850 devices.	✓	✓
Topology Scan X	Toposcan Discovery tool allows a user to select a DN and scan for nodes on the same channel sector.		✓
User Session Management X	Track current cnMaestro users and support forced logoff.	✓	✓
Webhooks X	Send alarm notifications to the external servers.		✓
Wi-Fi Speed Test	Test the speed between the Wi-Fi APs and cnMaestro.		✓
WLANs Dashboard X	View details of all WLANs that are applied on devices at a given site. Also view the details of APs connected to these WLANs.	✓	✓
Zero Touch Onboarding	Allow cnVision Client, PMP SMs, and ePMP SMs to automatically appear in the onboarding queue if the parent AP is already onboarded.	✓	✓

Quick Start

This section guides users through the initial process of creating an account; logging into cnMaestro; and claiming and onboarding devices.

You must perform the following procedures to create an account and onboard devices.

- **For account management:**

1. [Create a Cambium Support Center login](#) (if you do not have one already).
2. [Create a cnMaestro account](#).
3. [Login to cnMaestro](#).

- **For claiming devices:**

1. [Claim devices using a Manufacturer Serial Number \(MSN\)](#).
2. [Claim devices using a Cambium ID](#).

Create and manage accounts

To access cnMaestro, you must create a Cambium Support Center account, which sets your username and password.

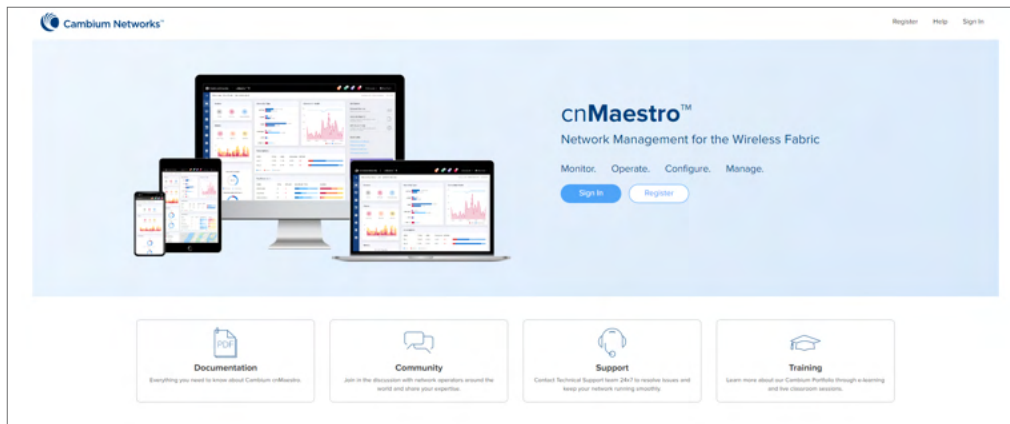
Create a Cambium Support Center login

cnMaestro uses an existing Cambium Support Center account. If you do not have an account, you must create one.

To create a Cambium Support Center account, perform the following steps:

1. Open a web browser and enter <https://cloud.cambiumnetworks.com> into the address bar.
The cnMaestro Main login page appears, as shown in [Figure 1](#).
2. Click **Register**.

Figure 1 The main login page



A registration form appears, as shown in [Figure 2](#).

Figure 2 Initial registration form

The image shows the initial registration form. It has the Cambium Networks logo at the top left. The main heading is 'Create an account'. Below it, a sub-heading says 'A Cambium Account will allow you to:'. This is followed by a bulleted list of benefits: joining discussions, accessing learning, joining the Open Beta program, downloading firmware, managing license keys, and using cnMaestro. Below the list, a paragraph explains that a confirmation email will be sent. A link 'log in over here' is provided for existing users. There is a text input field labeled 'Email' with a red asterisk, and a blue 'Register' button at the bottom.

3. Enter your email address and click the **Register** button.
An email from Cambium Support Center is sent with a link for validation.
4. Check email and click the validation link, as shown in [Figure 3](#).

Figure 3 Email from Cambium Support to validate account

From: support@cambiumnetworks.com <support@cambiumnetworks.com>
Sent: Monday, November 18, 2019 10:15 AM
To: k [REDACTED]
Subject: Cambium Networks Support Site Registration

Hi,

We've received a request to create an account on the Cambium Networks support site for [REDACTED]. If you made this request, you can visit this page to complete your registration:

<https://nam05.safelinks.protection.outlook.com/?url=http%3A%2F%2F100.26.63.226%2Fregister%2F1244c57f3e4f44e2a70e8c87ce0b4552&data=02%7C01%7Cgnana.prakash%40cambiumnetworks.com%7Ca37ffa9b71ee414c44b108d76be241b3%7C0e263e36340946228ac818d993e76eb6%7C0%7C0%7C637096491810918686&sd=CK%2FzPKq040f2%2FuV8PKzi%2Bc4Zih9rH%2Fug5Hiaf5WGH4%3D&reserved=0>

If you didn't make this request, then we're sorry for bothering you!

Regards,

Cambium Networks



Note

If you do not receive the email, check your email's spam folder.

The **Finish registering** form appears, as shown in [Figure 4](#).

Figure 4 *Finish registering form*

Cambium Networks

Finish registering

Thanks for being patient. We just need a few more details and then you're done.

Your Full Name*

Company Name*

Country*

Please select a country ▼

Street Address*

Town / City*

State / Province*

Zip / Postal Code*

Password*

Passwords must be at least 8 characters long, and they cannot have appeared in any data breaches. See [this Knowledge Base article](#) for more information about our password requirements.

Register

5. In the registration form, you must enter details such as your name, company name, country name, and password.
6. Click **Register** to complete the process.

Create a cnMaestro account

Use the Cambium Support Center account to log on to cnMaestro and create a cnMaestro account.

1. Navigate to <https://cloud.cambiumnetworks.com>.
2. Log in to cnMaestro using your Cambium Support Center account credentials.

The **Create a New Cloud Account** window appears, as shown in [Figure 5](#).

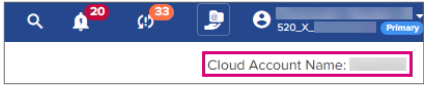
Figure 5 *Creating a new Cloud account*

3. Enter the required details as described below:

Table 5 *NMS Cloud management fields*

Parameter	Description
Cambium ID	The Cambium ID identifies this account externally. Once created, it can only be changed by contacting Cambium Support.
Country	The Country determines where to store the device data. Cambium has data centers in North America, Europe, and Asia. If your devices are located in more than one region, you should create a separate account for a country in each region.
Time Zone	The Time Zone aggregates daily device statistics. Daily statistics are collected starting at 12:00 AM in the time zone selected.
Account Type	The Account Type is either NMS or Anchor . Select NMS to manage devices through cnMaestro Cloud. Select Anchor if installing cnMaestro On-Premises.
Account View	Select the Account View based on the devices you intend to manage. Select Enterprise if only cnMaestro Enterprise devices will be managed (these include the cnMatrix, Enterprise Wi-Fi (E-Series, XE/XV/X7-Series) and cnPilot Enterprise, Enterprise Wi-Fi (Xirrus-Series), and NSE). The Account View can be changed later by navigating to Administration > Settings > General .
Primary Contact Details	
Full Name	User's full name to appear in the cnMaestro account.
Position	Designation of the user in the company. Select from the dropdown list.
Email	Email ID of the user.
Phone Number	Phone number of the user. Select the country code from the dropdown list and provide a valid phone number.
Company Details	
Company Name	Name of the company. This name will appear as the Cloud Account Name in the cnMaestro home page.

Table 5 NMS Cloud management fields

Parameter	Description
	
Company Website	URL of the company website.
Market Vertical	Type of market or industry the company caters to. For example, Government, Defense, Education. Select from the dropdown list.
Company Type	Nature of work that the company does. For example, Defense, Manufacturer, Distributor. Select from the dropdown list.
Headquarters Address	Address of the company headquarters.

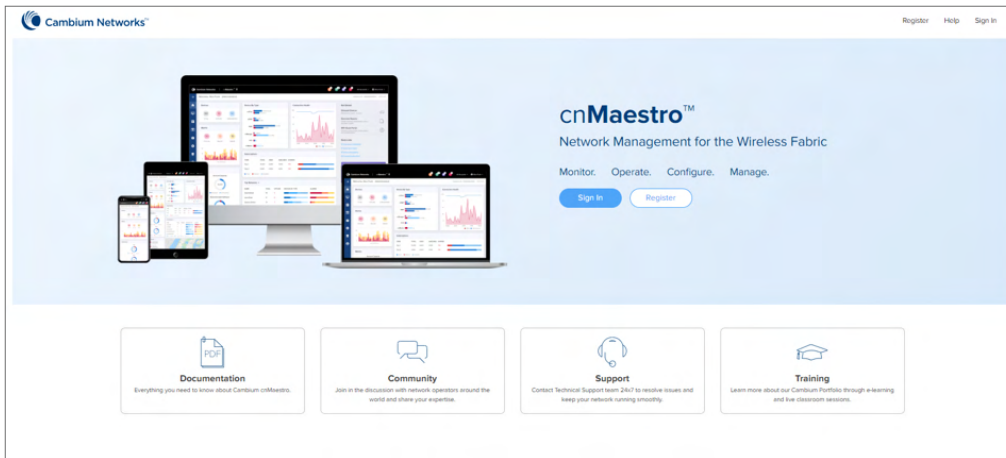
4. Select **I agree to the cnMaestro Terms of Service**.
5. Click **Create Account** to complete the process.

Log on to cnMaestro

To log on to the cnMaestro, perform the following steps:

1. Open a web browser and enter <https://cloud.cambiumnetworks.com> into the address bar.
The cnMaestro Main login page appears, as shown in [Figure 6](#).

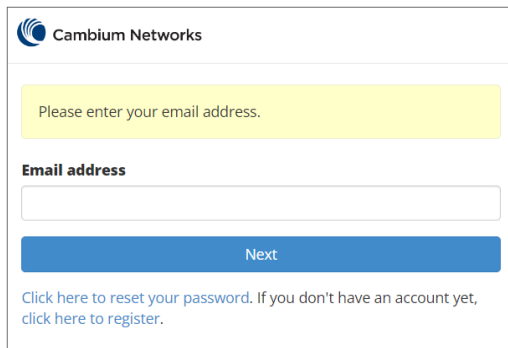
Figure 6 Main login page



2. Click **Sign In**.

Please enter your email address page appears as shown in [Figure 7](#).

Figure 7 *Email address page*

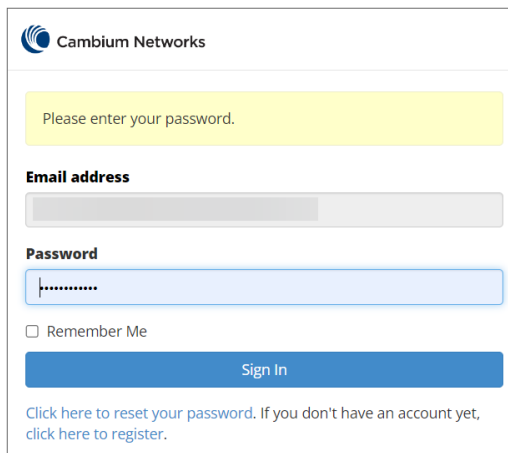


The screenshot shows the 'Email address' page of the Cambium Networks login interface. At the top left is the Cambium Networks logo. Below it is a yellow instruction box that says 'Please enter your email address.' Underneath is a label 'Email address' followed by a text input field. A blue 'Next' button is positioned below the input field. At the bottom, there is a link that reads 'Click here to reset your password. If you don't have an account yet, click here to register.'

3. Enter your **Email address**.
4. Click **Next**.

Please enter your password page appears as shown in [Figure 8](#).

Figure 8 *Password page*

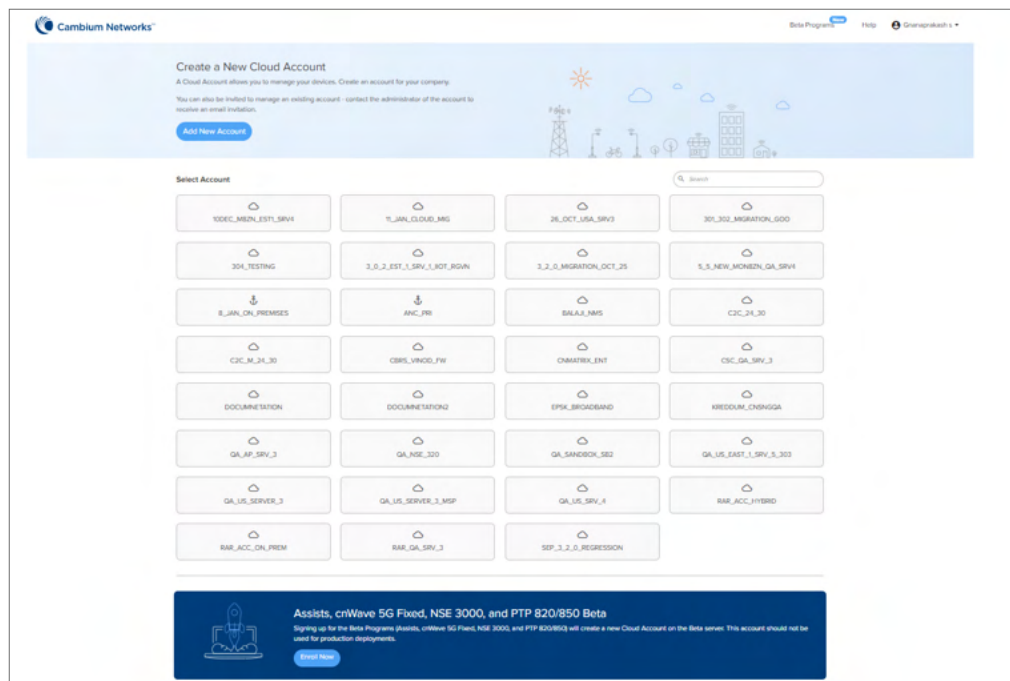


The screenshot shows the 'Password' page of the Cambium Networks login interface. At the top left is the Cambium Networks logo. Below it is a yellow instruction box that says 'Please enter your password.' Underneath is a label 'Email address' followed by a disabled text input field. Below that is a label 'Password' followed by a password input field with masked characters. A checkbox labeled 'Remember Me' is located below the password field. A blue 'Sign In' button is positioned below the 'Remember Me' checkbox. At the bottom, there is a link that reads 'Click here to reset your password. If you don't have an account yet, click here to register.'

5. Click **Sign in**.

Select Account page appears as shown in [Figure 9](#).

Figure 9 Select account page

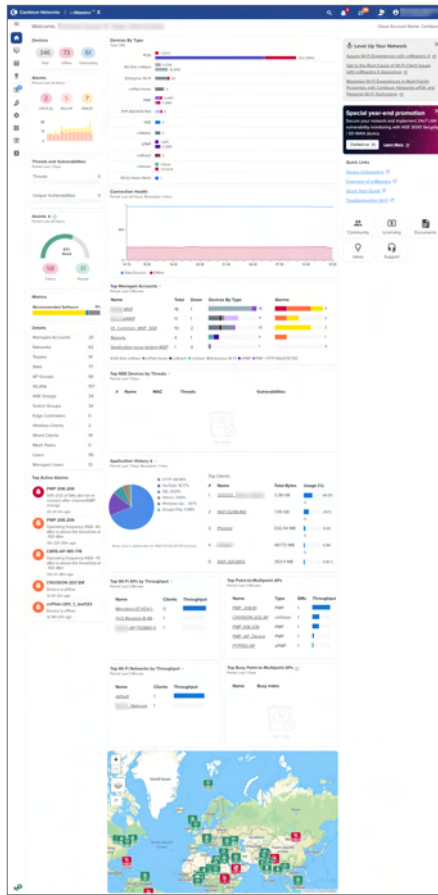


In **Select Account** page you can use search option to search the account.

6. Click the selected account.

The cnMaestro **Home** page appears, as shown in [Figure 10](#).

Figure 10 cnMaestro Home page



Claim and onboard devices

To manage devices in cnMaestro, it is necessary to claim and onboard them.

Claiming specifies who owns a device. After a device is claimed, it is listed in the Onboarding Queue, where it can be pre-provisioned or approved. Once devices are approved, they are managed by cnMaestro.

Claim devices by serial number

You can claim a device by using the Manufacturer Serial Number (MSN). The system prompts the user to validate the devices before applying them. After being claimed, devices are placed into the Onboarding Queue, where they can be pre-provisioned to update software or configuration before onboarding.

To claim and onboard a device, perform the following steps:

1. From the Home page of cnMaestro, navigate to **Onboard > Device** tab.

The Onboard page appears with details of the devices and their serial numbers, as shown in [Figure 11](#).

Figure 11 Onboard page

Type	Serial Number	Name	MAC	Tier	IP Address	Source IP	Managed Account	Onboarding Mode	Status	Onboarding Status	Subscription Status	Duration
PMP 450 SM		PMP-677823		N/A	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	Will attempt after appr...	1d 1h 52m
PMP 450 SM		PMP-43BE5D		N/A	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	Will attempt after appr...	2d 2h 0m
crMatrix		crMatrix-F5AAE0		Tier 20	N/A	N/A	Application issue tes	Using Serial Number	Offline	Waiting for Device	Completed	0d 22h 37m
ePMP		ePMP Force 300...		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	Completed	5d 22h 10m
ePMP		ePMP Force 300...		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	Completed	5d 22h 10m
PMP 450 SM		PMP-894356		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	Completed	5d 22h 10m
PMP 450 AP		PMP-678954		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	Completed	5d 22h 10m
PMP 450i SM		PMP-4546A7		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	Completed	5d 22h 10m
PMP 450i High ...		PMP 450i SM BE...		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	Completed	5d 22h 10m
PMP 450i High ...		PMP 450i SM BE...		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	Completed	5d 22h 10m

- Click **Claim Devices** located at the right side of the Onboard page (as shown in [Figure 11](#)).

The **Claim Devices with Serial Number** page appears, as shown in [Figure 12](#).

- Enter the Serial Number(s) of the device(s) in the text box, as shown in [Figure 12](#).

If MSP is enabled, select the **Managed Account** from the drop down and Enter the Serial Number(s) of the device(s) in the text box.



Note

You can also place a cursor in the text box and use a barcode scanner to quickly claim the devices.

Figure 12 Claim Devices with Serial Number page

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

Enter / Place a cursor in the box and use a barcode scanner to quickly claim devices.

Clear Claim Devices

- Click **Claim Devices**.
- To onboard the device when it contacts cnMaestro, click the **Approve Device** (🔒) icon or **Approve All** at the right side of the Onboard page, as shown in [Figure 13](#).

Figure 13 Onboarding Queue

Type	Serial Number	Name	MAC	Tier	IP Address	Source IP	Managed Account	Onboarding M...	Status	Onboarding Status	Duration
cnPilot e600		Migration_10_E...		Tier 3	10.110.209.190	115.110.225.242	Base Infrastructure	Using Serial Number	Online	Waiting for Approval	0d 10h 20m
cnMatrix TX2012R-P		Migration-cnMat...		Tier 20	10.110.209.111	115.110.225.242	Base Infrastructure	Using Serial Number	Online	Waiting for Approval	1d 19h 42m
PMP 450 SM		PMP-347867		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	0d 0h 50m
PMP 450i AP		PMP-449086		Tier 2	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	0d 0h 50m
PMP 450 SM		PMP-438E49		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	0d 0h 59m



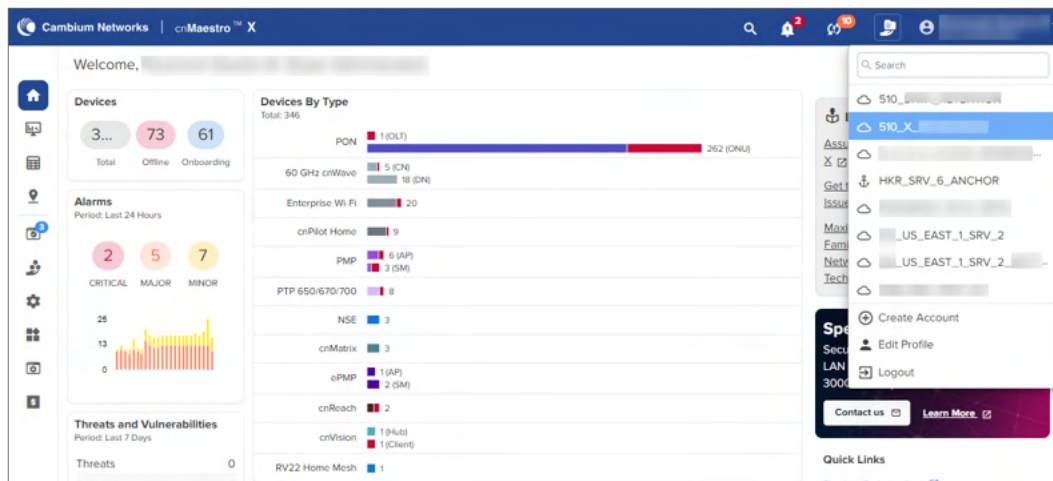
Note

If you do not click the **ApproveDevice** button, the device remains in the Onboarding Queue.

Claim devices by Cambium ID

The Cambium ID, set during the Cloud account creation can also be used to claim devices. You can see the Cambium ID on the user dropdown, as shown in [Figure 14](#).

Figure 14 Cambium ID



A Cambium ID with an Onboarding Key is:

- Required to claim legacy devices that do not have a 12-character serial number (these devices are usually 5+ years old).
- Optional for devices that have 12-character serial numbers (though generally not used).

The administrator must approve all devices added to the Onboarding Queue using the Cambium ID.

Cambium ID configuration

You must configure the Onboarding Key in order to claim devices with Cambium ID, as shown in [Figure 15](#).

Figure 15 Cambium ID configuration

Onboard

Devices 60 GHz cnWave Edge Controller PON Settings

You can add devices to your account by logging into the Device UI directly and entering the Cambium ID and Onboarding Key (these were set when you created your Company Account, and they can be modified below). ePMP 1000, PMP 430/450 and ePMP 1000 Hotspot must be claimed using this method. ⓘ

Cambium ID: [REDACTED]

☒ Allow device to be claimed using Cambium ID

Enabling this feature allows a device to be claimed by entering the Cambium ID and Onboarding Key on the device. This information can be set on the device via its user interface (or SNMP or CLI on some devices). Each user can have their own Onboarding Key. [Learn more](#)

The following users can claim devices using the cnMaestro Cambium ID and the user's Onboarding Key.

User: [REDACTED]	Onboarding Key: [REDACTED]	Delete
User: [REDACTED]	Onboarding Key: [REDACTED]	Delete
User: [REDACTED]	Onboarding Key: [REDACTED]	Delete
User: [REDACTED]	Onboarding Key: [REDACTED]	Delete
User: [REDACTED]	Onboarding Key: [REDACTED]	Delete

Save Cancel Add New

Onboarding Key configuration

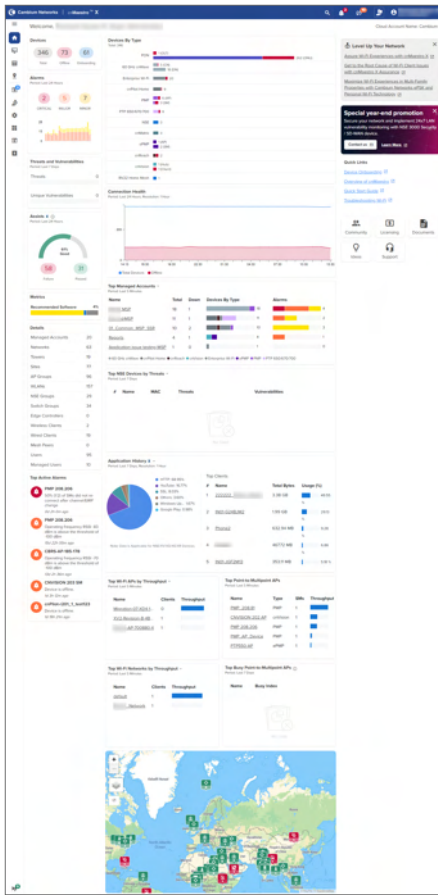
Each Onboarding Key is mapped to an individual User account. This mapping allows Cambium Cloud to know who is onboarding a device, and the key can be revoked if needed.

To configure the Onboarding Key, perform the following steps:

1. Log on to your cnMaestro account.

The Home page appears, as shown in [Figure 16](#).

Figure 16 Home page



- From the Home page, navigate to the **Onboard > Settings** tab.

Figure 17 Onboard settings page

Onboard

Devices
60 GHz cnWave
Edge Controller
PON
Settings

You can add devices to your account by logging into the Device UI directly and entering the Cambium ID and Onboarding Key (these were set when you created your Company Account, and they can be modified below). ePMP 1000, PMP 430/450 and ePMP 1000 Hotspot must be claimed using this method. ⓘ

Cambium ID:

☒ Allow device to be claimed using Cambium ID

Enabling this feature allows a device to be claimed by entering the Cambium ID and Onboarding Key on the device. This information can be set on the device via its user interface (or SNMP or CLI on some devices). Each user can have their own Onboarding Key. [Learn more](#)

The following users can claim devices using the cnMaestro Cambium ID and the user's Onboarding Key.

User: <input type="text"/>	Onboarding Key: <input type="password"/>	<input type="button" value="Delete"/>
User: <input type="text"/>	Onboarding Key: <input type="password"/>	<input type="button" value="Delete"/>
User: <input type="text"/>	Onboarding Key: <input type="password"/>	<input type="button" value="Delete"/>
User: <input type="text"/>	Onboarding Key: <input type="password"/>	<input type="button" value="Delete"/>
User: <input type="text"/>	Onboarding Key: <input type="password"/>	<input type="button" value="Delete"/>

Save
Cancel
Add New

- Select the **Allow device to be claimed using Cambium ID** checkbox.
Enabling this feature allows one to add Onboarding Keys mapped to individual Users.
- Click **Add New** to add a User and Onboarding Key.

A new row appears as shown in [Figure 18](#).

Figure 18 *New onboarding key*

Onboard

Devices60 GHz cnWaveEdge ControllerPONSettings

You can add devices to your account by logging into the Device UI directly and entering the Cambium ID and Onboarding Key (these were set when you created your Company Account, and they can be modified below). ePMP 1000, PMP 430/450 and ePMP 1000 Hotspot must be claimed using this method. ⓘ

Cambium ID:

☒ Allow device to be claimed using Cambium ID

Enabling this feature allows a device to be claimed by entering the Cambium ID and Onboarding Key on the device. This information can be set on the device via its user interface (or SNMP or CLI on some devices). Each user can have their own Onboarding Key. [Learn more](#)

The following users can claim devices using the cnMaestro Cambium ID and the user's Onboarding Key.

User: <input type="text"/>	Onboarding Key: <input type="text"/>	<input type="button" value="Delete"/>
User: <input type="text"/>	Onboarding Key: <input type="text"/>	<input type="button" value="Delete"/>
User: <input type="text"/>	Onboarding Key: <input type="text"/>	<input type="button" value="Delete"/>
User: <input type="text"/>	Onboarding Key: <input type="text"/>	<input type="button" value="Delete"/>
User: <input type="text"/>	Onboarding Key: <input type="text"/>	<input type="button" value="Delete"/>
User: <input type="text"/>	Onboarding Key: <input type="text"/>	<input type="button" value="Delete"/>
User: <input type="text"/>	Onboarding Key: <input type="text"/>	<input type="button" value="Delete"/>
User: <input type="text"/>	Onboarding Key: <input type="text"/>	<input type="button" value="Delete"/>
User: <input type="text"/>	Onboarding Key: <input type="text"/>	<input type="button" value="Delete"/>
User: <input type="text"/>	Onboarding Key: <input type="text"/>	<input type="button" value="Delete"/>

5. Select the **User** from the dropdown.
6. Enter the **Onboarding Key**.
7. Click **Save**.

Onboard device using Onboarding Key

The Cambium ID and Onboarding Key are entered into the Device UI (see the User Guide for the individual devices to determine where; the section below demonstrates the process for cnPilot). Once entered, the Device sends these credentials to Cambium Cloud, where it is mapped to the Onboarding Queue of the Cambium ID account.


Device UI

To configure the Onboarding Key using cnPilot Device UI, perform the following steps:


1. Log on to the Device UI.


The **Sign In** page appears, as shown in [Figure 19](#).

Figure 19 *Login page*

 Cambium Networks™ cnPilot E600 - E600-A65C72

Login

 Username

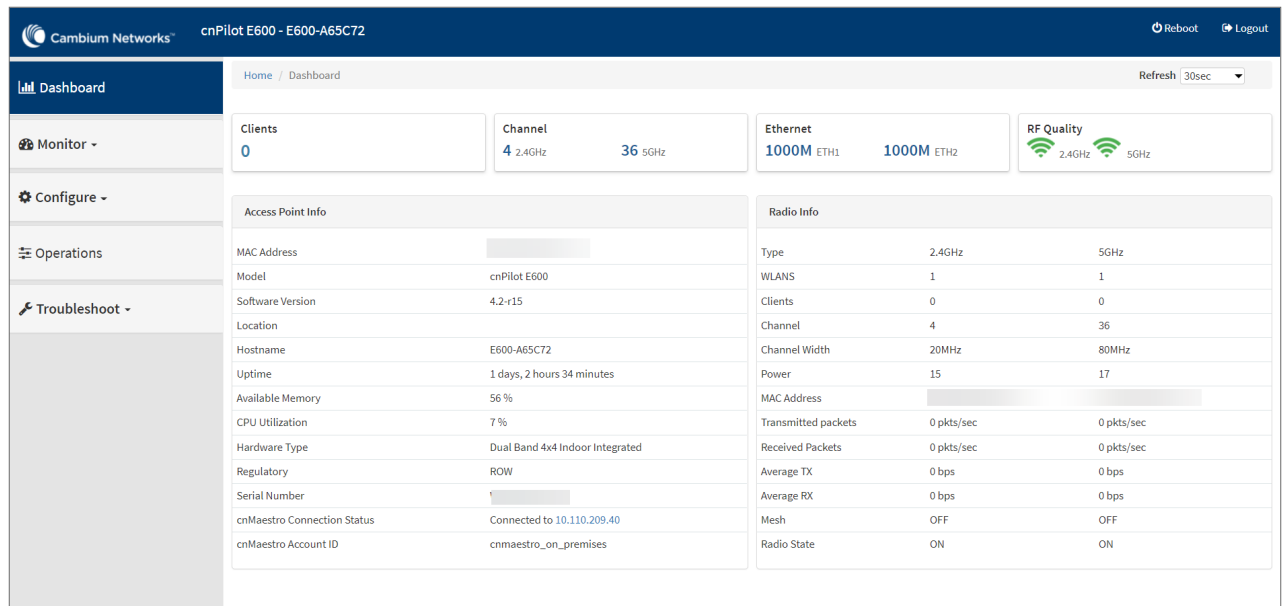
 Password

Sign In

2. Enter your **Username** and **Password**.
3. Click **Sign In**.

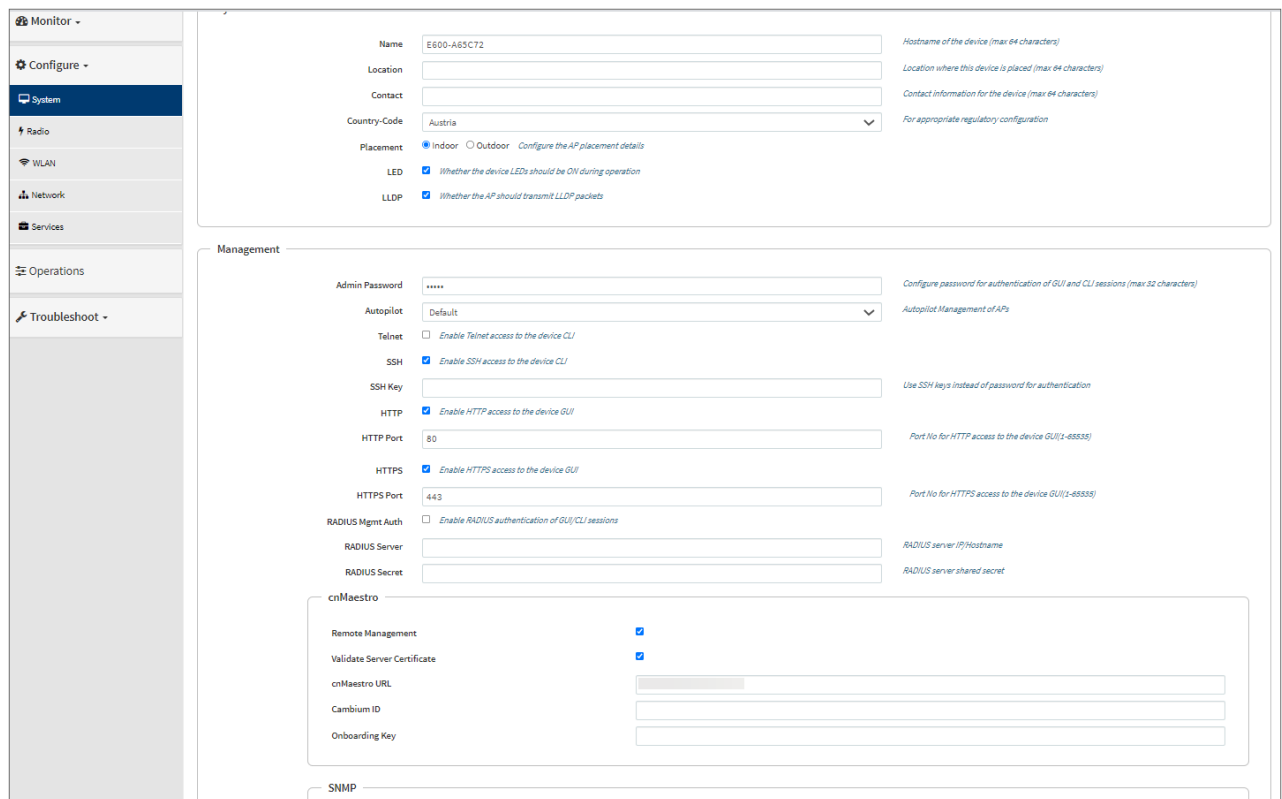
The device home page appears, as shown in [Figure 20](#).

Figure 20 Device home page



- From the Home page, navigate to **Configure > System > Management**.
System configuration page appears, as shown in [Figure 21](#).

Figure 21 cnMaestro configuration



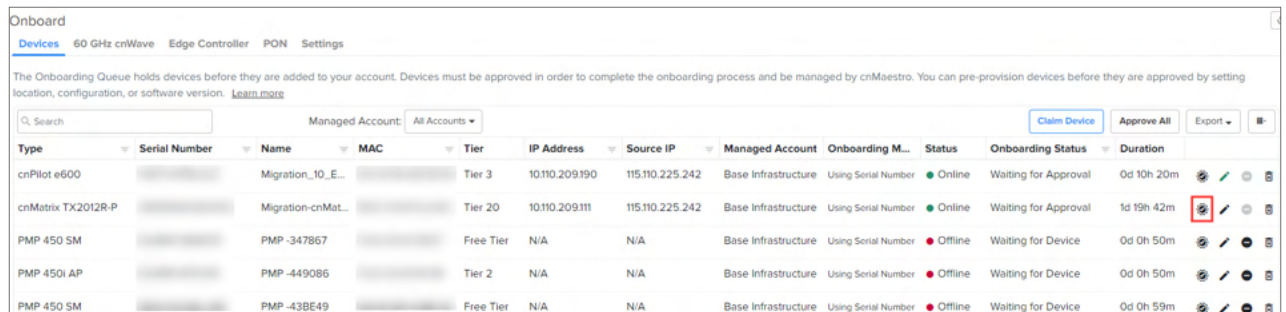
- Enter URL in **cnMaestro URL** to connect the server (by default it will be cloud.cambiumnetworks.com), as shown in [Figure 21](#).
- Enter the **Cambium ID**.


7. Enter the **Onboarding Key**.

8. Click **Save**.

Once in the Onboarding Queue, the devices can be provisioned and managed by clicking the **Approve Device** button, as shown in [Figure 22](#).

Figure 22 *Device approval*



Type	Serial Number	Name	MAC	Tier	IP Address	Source IP	Managed Account	Onboarding M...	Status	Onboarding Status	Duration	
cnPilot e600		Migration_10_E...		Tier 3	10.110.209.190	115.110.225.242	Base Infrastructure	Using Serial Number	Online	Waiting for Approval	0d 10h 20m	
cnMatrix TX2012R-P		Migration-cnMat...		Tier 20	10.110.209.111	115.110.225.242	Base Infrastructure	Using Serial Number	Online	Waiting for Approval	1d 19h 42m	
PMP 450 SM		PMP-347867		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	0d 0h 50m	
PMP 450i AP		PMP-449086		Tier 2	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	0d 0h 50m	
PMP 450 SM		PMP-438E49		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	0d 0h 59m	

Creating a Cloud Account

This section provides an overview of cnMaestro Cloud Accounts. This section includes the following:

- [Overview](#)
- [Creating a Support Center User ID](#)
- [Creating a Cloud NMS Account](#)
- [Creating an Anchor Account](#)
- [Multiple Cloud Accounts](#)

Overview

There are two types of accounts for cnMaestro cloud management.

Table 6 *Account types*

Account	Description
Cloud NMS	Cloud NMS accounts allow users to manage their devices through https://cloud.cambiumnetworks.com . Devices can be claimed, onboarded, and fully managed through the cloud service.
Cloud Anchor	Cloud Anchor Accounts are needed for on-premises installations of cnMaestro. After cnMaestro is deployed in a local data center, it connects to a Cloud Anchor Account. See the following section for more details on Creating an Anchor Account .

Both Cloud NMS and Cloud Anchor Accounts require a Support Center ID to login.

Creating a Support Center User ID

New Cambium Cloud users need to register with Cambium Support Center to create a Support Center ID.

1. Navigate to <https://cloud.cambiumnetworks.com> and click **Sign In**.
2. In the **Sign In** page, click **Register**.

3. Enter your email address in the text box and click **Register**.
4. An email will be sent to the address provided. Open the email and click the link.
5. Fill in details on the registration completion form, such as your name, the name of your company, and a password.
6. Click **Sign in** to log into the UI.

Creating a Cloud NMS Account

If you do not have a Cloud NMS Account, you will be asked to create one after logging in and accessing cnMaestro Cloud. The NMS Account allows you to access cnMaestro functionality and start claiming devices.

1. Log in to the cnMaestro UI <https://cloud.cambiumnetworks.com>.
2. Click **Add New Account**. You will be redirected to the **Create a New Cloud Account** page.
3. Enter details such as **Cambium ID**, **Friendly Name**, **Country**, **Time Zone**, **Account Type**, and **Account View**. The **Account Type** should be set to **NMS**.
4. Enable **I agree to the cnMaestro Terms of Service**.
5. Click **Create Account**.

Figure 23 Create Cloud NMS account

The required fields are defined below:

Table 7 NMS Cloud management fields

Parameter	Description
Cambium ID	The Cambium ID identifies this account externally. Supported characters—alphabets, integers, and underscore only. Once created, it can only be changed by contacting Cambium Support.
Country	Determines where the devices in this account are located. Cambium has data centers in North America, Europe, and Asia. If your devices are located in more than one region, you must create a separate account for a country in each region.
Time Zone	Specifies the time zone used to calculate device statistics.

Table 7 NMS Cloud management fields

Parameter	Description
	Daily statistics are collected at 12 AM in the configured time zone.
Account Type	<p>Specifies the type of cnMaestro account you want to use to manage devices.</p> <p>Following options are supported:</p> <ul style="list-style-type: none"> • NMS—Manage devices through cnMaestro Cloud • Anchor—Manage devices locally on your own data center through cnMaestro On-Premises
Account View	<p>Specifies the cnMaestro account view based on the devices you intend to manage.</p> <ul style="list-style-type: none"> • Access and Backhaul <ul style="list-style-type: none"> ◦ 60 GHz cnWave ◦ cnMatrix ◦ cnPilot Home (cnPilot R-Series) ◦ RV22 Home Mesh ◦ cnRanger ◦ cnVision ◦ cnWave 5G Fixed ◦ Enterprise Wi-Fi (E-Series and XE/XV/X7-Series) and cnPilot Enterprise (ePMP 1000 Hotspot) ◦ Enterprise Wi-Fi (Xirrus-Series) ◦ ePMP ◦ NSE ◦ PMP ◦ PON ◦ PTP 650/670/700 ◦ PTP 820/850 • Enterprise— <ul style="list-style-type: none"> ◦ cnMatrix ◦ Enterprise Wi-Fi (E-Series and XE/XV/X7-Series) and cnPilot Enterprise (ePMP 1000 Hotspot) ◦ Enterprise Wi-Fi (Xirrus-Series) ◦ NSE • Industrial internet— <ul style="list-style-type: none"> ◦ 60 GHz cnWave ◦ cnMatrix ◦ cnPilot Home (cnPilot R-Series)

Table 7 NMS Cloud management fields

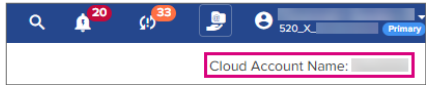
Parameter	Description
	<ul style="list-style-type: none"> ◦ RV22 Home Mesh ◦ cnRanger ◦ cnReach ◦ cnVision ◦ cnWave 5G Fixed ◦ Enterprise Wi-Fi (E-Series and XE/XV/X7-Series) and cnPilot Enterprise (ePMP 1000 Hotspot) ◦ Enterprise Wi-Fi (Xirrus-Series) ◦ ePMP ◦ NSE ◦ PMP ◦ PON ◦ PTP 650/670/700 ◦ PTP 820/850 <p>You can change this view later by navigating to the Administration > Settings > General page.</p>
Primary Contact Details	
Full Name	User's full name to appear in the cnMaestro account.
Position	Designation of the user in the company. Select from the dropdown list.
Email	Email ID of the user.
Phone Number	Phone number of the user. Select the country code from the dropdown list and provide a valid phone number.
Company Details	
Company Name	<p>Name of the company.</p> <p>This name will appear as the Cloud Account Name in the cnMaestro home page.</p> 
Company Website	URL of the company website.
Market Vertical	<p>Type of market or industry the company caters to.</p> <p>For example, Government, Defense, Education.</p> <p>Select from the dropdown list.</p>
Company Type	<p>Nature of work that the company does.</p> <p>For example, Defense, Manufacturer, Distributor.</p>

Table 7 NMS Cloud management fields

Parameter	Description
	Select from the dropdown list.
Headquarters Address	Address of the company headquarters.

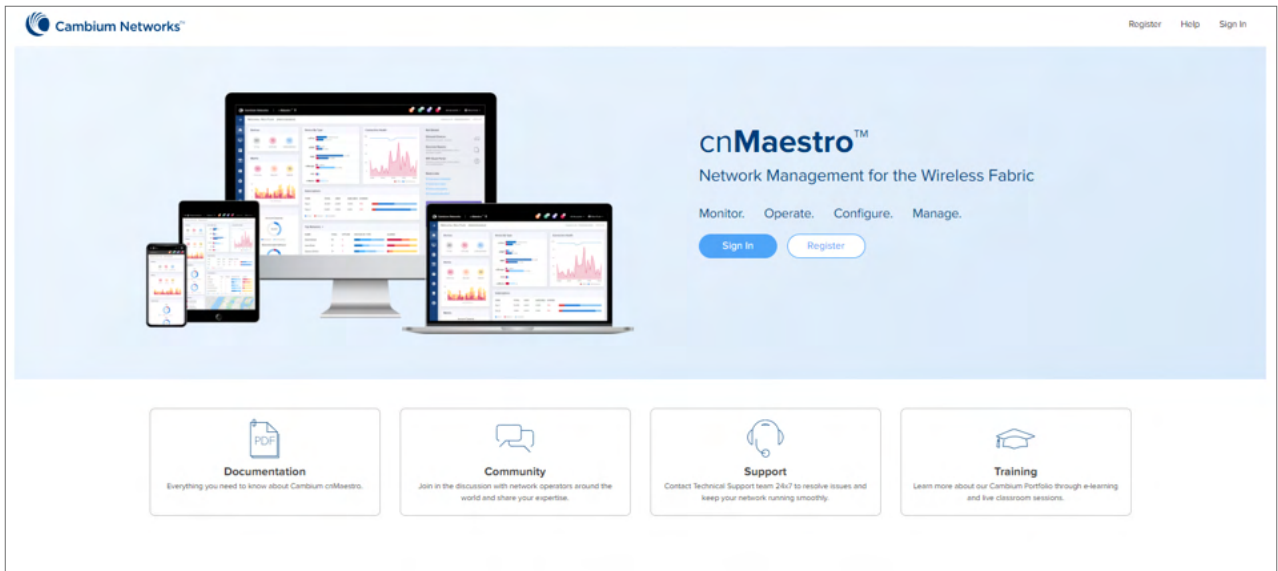
6. Click the dropdown next to the username or search option to view the created Cloud account.

Once you have created a Cloud NMS Account, you will be directed to the home page on subsequent login.

Creating an Anchor Account

An Anchor Account is required only if installing cnMaestro On-Premises.

1. Log in to the cnMaestro UI <https://cloud.cambiumnetworks.com>.



2. In **Account Type**, select **Anchor**.

Cambium Networks Help

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* The country where devices in this account are located.

Time Zone* 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](#)

- Once the Anchor Account is created, an Onboarding Key must be set to allow On-Premises instances to connect.
- Navigate to the **Manage Instances** page as shown below and edit the **Onboarding Key**. 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: ANCHOR_SRV6_QA_TEST

[Change Onboarding Key](#) [Disable Onboarding](#)

- Once the On-Premises server has been onboarded with the Key, it will be included in the **Instances** page. Multiple On-Premises installations can be added to a single Anchor Account.

Manage Instances

[Onboarding](#) [On-Prem Instances](#) [Notifications](#)

Q Search

Name	Subscription	Expiring In	Type	Status	Last Connected	Onboarded	Uptime
CnMaestro-46	cnMaestro X	28 days	-	Online	Nov 01, 2022 11:22	1d 3h 54m ago	2d 1h 15m

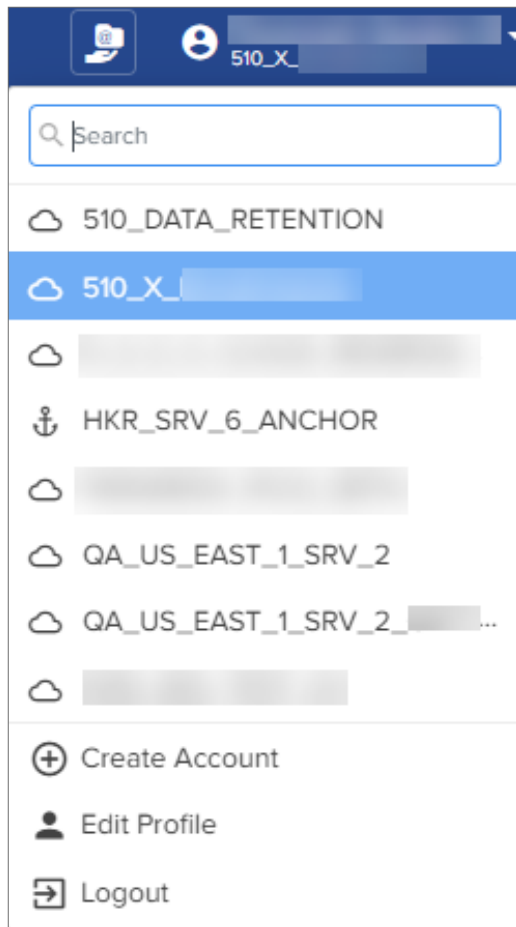
Showing 1 - 1 Total: 1 10 < Previous 1 Next >

Clicking the instance host name displays the server information collected.

Multiple Cloud Accounts

Individuals can belong to multiple Cambium Cloud accounts. To create another Cloud Account (NMS or Anchor), select **Create Account** from the dropdown in the top-right corner. Enter the ID name in the **Search** field to filter the particular ID.

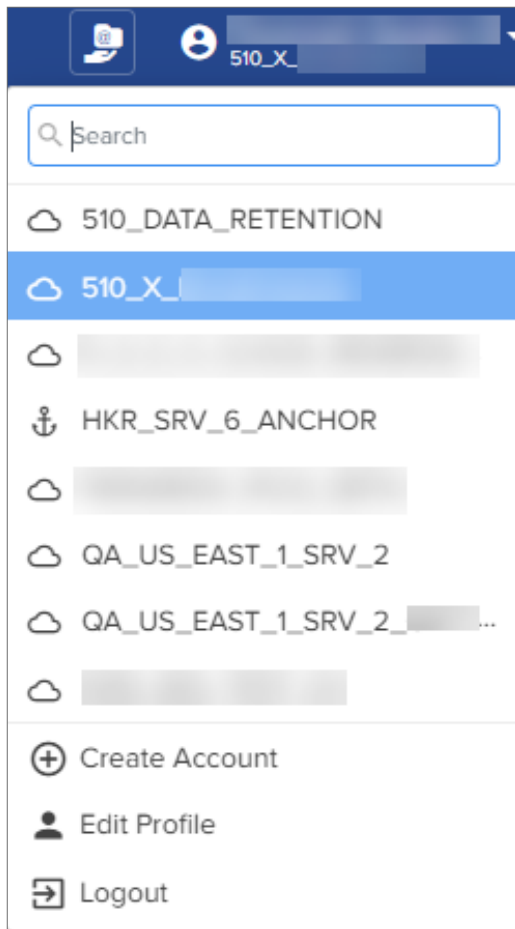
Figure 24 Multiple Cloud Management Accounts



Account selection

To switch between accounts, use the dropdown in the top-right corner of the UI. It displays all accounts to which the user has access.

Figure 25 *Account selection*



Concurrent access

The same user can access multiple accounts simultaneously; however, each account needs to be opened in a separate browser window or tab.

Managing users

A user can add additional administrators to their cloud management accounts and assign roles such as **Super Administrator**, **Administrator**, **Operator**, **Monitor**, and **CPI**.

Figure 26 *Managing 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

Creating Users and Configuring User Roles

To add a user:

1. Navigate to **Administration > Users Page > Manage Users**.
2. Click **Add User**.

Add User

Email*

Role: Monitor

[Learn more](#) Cancel Send

3. Enter the Email address in the **Email** text box.
4. To configure user role, select from the **Role** dropdown:
 - Super Administrator
 - Administrator
 - Operator
 - Monitor
 - CPI

For more details on user Roles, refer to [Role-Based Access](#).

5. Click **Send**.
6. Cambium Cloud sends an email with directions on how to access the Cloud management account.



Note

The email does not need to match the email address of an existing Cambium user.

7. The email contains a link that directs you to the Cambium Cloud website <https://cloud.cambiumnetworks.com>.
8. Login using an existing Cambium Support Center account or create a new Cambium Support Center account.

Organization

Organizations allow multiple Cloud NMS Accounts and Anchor Accounts to consolidate CBRS billing into one Primary Account.

- Primary Account: provides services such as Shared SAS ID and Unified Payments to multiple accounts.
- Secondary Account: shares services such as CBRS billing SAS ID; the Secondary Account is linked with the Primary Account.

Organizations are currently only used with CBRS. Refer [CBRS](#) on how they can simplify CBRS management across multiple accounts.

General details of Organizations include:

1. One Organization can include accounts created in different countries and regions.
2. The maximum number of accounts managed by an Organization is 5.
3. There is one required Primary Account in an Organization and optionally multiple Secondary Accounts.
4. Removing the Primary Account will dissolve the Organization.
5. Both NMS and Anchor Accounts can be included in an Organization, and either can be Primary.

cnMaestro X

cnMaestro works in two different modes: Essentials, and X. cnMaestro Essentials is free and supports basic network management functionality. cnMaestro X is paid and requires subscriptions.

New accounts are created with cnMaestro Essentials capabilities. cnMaestro X features can be activated with the **Entitlement ID** provided by Cambium Networks. For more details, refer to [cnMaestro Features](#). You can purchase the **Entitlement ID** from an authorized **Cambium Reseller or Distributor**. The subscriptions are available for 1 year, 3 years, and 5 years per device type and device count. Pricing is based on [Device Tiers](#). You need an **Entitlement ID** with equal or more device counts for each tier shown in the [Device Summary](#).

cnMaestro X part numbers are available at <https://www.cambiumnetworks.com/products/software/cnmaestro-x/>. Once your order is processed, you will receive an email from Cambium containing your **Entitlement ID**.

Figure 27 Example of Entitlement ID

Cambium Networks software entitlement

licensing@cambiumnetworks.com

To [redacted]
Cc [redacted]

Wed 23-12-2020 20:12

↩ Reply ↩ Reply All → Forward ⋮

🔗 If there are problems with how this message is displayed, click here to view it in a web browser.

Cambium Networks is pleased to deliver this entitlement document that you may use to redeem the order for the products listed below. To redeem this entitlement, please go to the [Cambium Support Center](#) and click on the "Licensing" link, then click on "Activate Entitlements".

You will need to have valid Cambium login credentials in order to access this area of the site. If you don't have these credentials, click on "Register" at the top of the page. You will then receive an email outlining how to register.

If you need assistance with this process, please [contact](#) Cambium Networks Support.

Entitlement Details		
Entitlement ID:	[redacted]	Creation Date: 12/23/2020
Contact:	[redacted]	
Cambium Order Reference:	Testing 123	
Your Order Reference:		

Product Details		
Product Number	Description	Quantity
MSX-SUB-T1-5 1	cnMaestro X for FWB SM; Tier1 5-year subscription per device	20
MSX-SUB-T2-5 1	cnMaestro X for FWB AP/PTP/IOT; Tier2 5-year subscription per device	20
MSX-SUB-T3-5 1	cnMaestro X for Enterprise W-Fi; Tier3 5-year subscription per device	20



Note

- If you are creating new accounts after cnMaestro 3.0.0, then you can request a 90-day free trial

either through the link available on the cnMaestro home page or <https://www.cambiumnetworks.com/cnmaestro-x/>.

For more information about cnMaestro X trial, see [cnMaestro X Trial self-activation](#).

- The 90 days free trial gets activated automatically for the accounts created before cnMaestro 3.0.0.

NSE subscription

- The NSE device subscription is supported in cnMaestro Essentials as well as cnMaestro X in the cnMaestro Cloud deployment.
- You can avail the Entitlement ID for NSE with the required device slots according to the [Device Tiers](#) by contacting the reseller or distributor.
- When you move other devices from cnMaestro Essentials to cnMaestro X, you can continue to use the same NSE subscription.
- When you have only Free Tier devices and a subscription for NSE, you can manually upgrade to cnMaestro X and downgrade to Essentials on your own.

cnMaestro X Trial self-activation

cnMaestro Essentials users can try cnMaestro X features, for free, as part of the cnMaestro X Trial mode for a duration of 90 days. New users who meet the following criteria can self-activate the trial:

- There must no subscriptions in the Essentials account.
- Users must not have used cnMaestro X earlier.

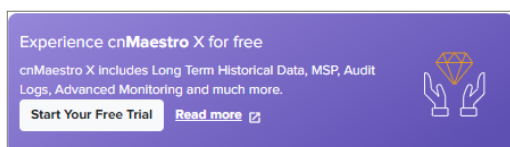
If the users have already used cnMaestro X earlier, then downgraded to Essentials, and now want to try cnMaestro X trial, then they must contact the Cambium Support team by filling the form at <https://www.cambiumnetworks.com/cnmaestro-x/>.

- Users must not have activated cnMaestro X Trial earlier.

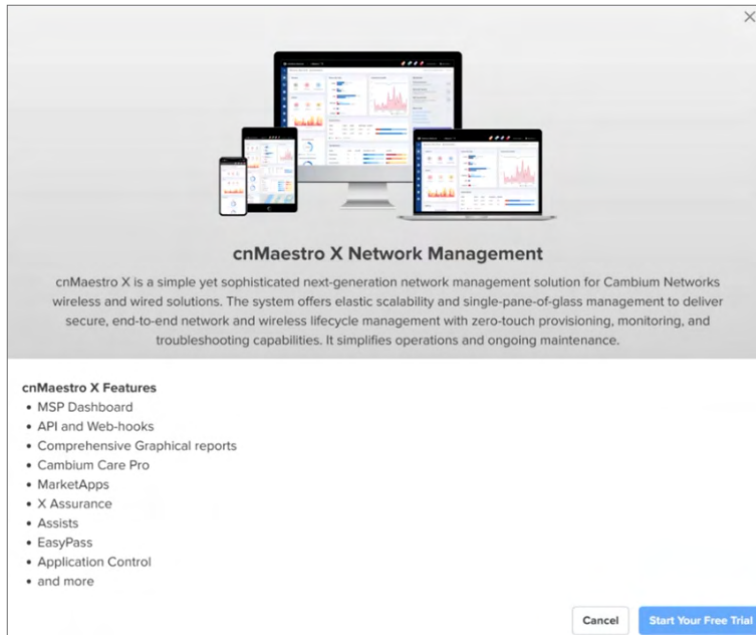
If the trial was activated earlier and users want to try cnMaestro X Trial again, users must contact the Cambium Support team by filling the form at <https://www.cambiumnetworks.com/cnmaestro-x/>.

To self-activate the free cnMaestro X Trial, complete the following steps:

1. Navigate to cnMaestro Essentials account homepage.
2. Click **Start your Free Trial** in the **Experience cnMaestro X for free** banner on the right pane.

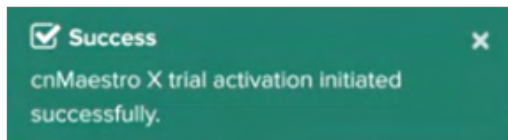


The cnMaestro X Network Management pop-up is displayed.

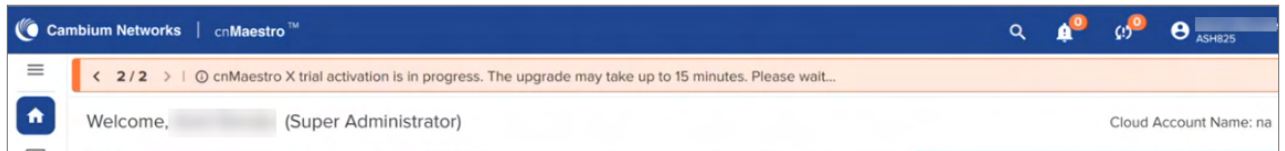


3. Click **Start Your Free Trial**.

A success message is displayed at the top of the homepage.



A banner also appears mentioning that the trail activation has started.



cnMaestro X activation

To activate the cnMaestro X account, perform the steps below:

1. Navigate to <https://support.cambiumnetworks.com/entitlements>, or from the cnMaestro home page click the **Licensing** tile.
2. In the Licensing page under **Entitlements** select **Activate Entitlements**.
3. Enter the **Entitlement ID** received from licensing@cambiumnetworks.com.
4. Click **Check**.

Cambium Networks | Support Center

Submit a request

[Knowledge Base](#)
[Downloads](#)
[Warranty](#)
[Licensing](#)
[Beta](#)
[FAQ](#)
[My Requests](#)

Licensing

Entitlements

Activate Entitlements

Previous Activations

Saved Entitlements

Fixed Wireless License Keys

cnVision

ePMP 1000/2000/3000

PMP / PTP 450

PTP 300/400/500/600/800

PTP 550

PTP 650

PTP 670

PTP 700

PTP 810

PTP 820 / 850

Entitlement Activation

Enter as many entitlement IDs as you like, one per line, then press **Check**.

Check

Entitlement ID:

Save

Part Number	Description	Available Quantity
MSX-SUB-T1-1	cnMaestro X for FWB; Free Tier 1-year subscription per device	6 of 6 Activate
MSX-SUB-T2-1	cnMaestro X for FWB; Tier 2 1-year subscription per device	6 of 6
MSX-SUB-T3-3	cnMaestro X for Enterprise Wi-Fi; Tier 3 3-year subscription per device	12 of 12
MSX-SUB-T100-1	cnMaestro X for Third Party; Tier 100 1-year subscription per device	1 of 1

- Once the **Entitlement ID** is validated, the **Activate** button is enabled.



Note

All subscribed part numbers must be activated under each **Entitlement ID**.

The part numbers subscribed with **MSX** must be activated together.

- Click **Activate**.
- Select the Cambium ID from the list and click **Next**.

Cambium Networks | Support Center

Submit a request

john@camn.com

[Knowledge Base](#)
[Downloads](#)
[Warranty](#)
[Licensing](#)
[Beta](#)
[FAQ](#)
[My Requests](#)

Licensing

Entitlements

Activate Entitlements

Previous Activations

Saved Entitlements

Fixed Wireless License Keys

cnVision

ePMP 1000/2000/3000

PMP / PTP 450

PTP 300/400/500/600/800

PTP 550

PTP 650

PTP 670

PTP 700

PTP 810

PTP 820 / 850

You are about to activate the following items:

Part Number	Description	Available Quantity
MSX-SUB-T1-1	cnMaestro X for FWB; Free Tier 1-year subscription per device	6
MSX-SUB-T2-1	cnMaestro X for FWB; Tier 2 1-year subscription per device	6
MSX-SUB-T3-3	cnMaestro X for Enterprise Wi-Fi; Tier 3 3-year subscription per device	12
MSX-SUB-T100-1	cnMaestro X for Third Party; Tier 100 1-year subscription per device	1

Select cnMaestro Account

is a member of the following **cnMaestro** accounts:

Cambium ID	Account Name	Type
10NOVSHEMNA_QA	camnium	cnMaestro X Trial Next
240_300_AFTER_MIG	camnium	cnMaestro X Trial Next
242_TO_300_MIGRATION	Cambium Networks	cnMaestro X Trial Next
27_NOV_ESS_PRO_MON8ZN	CMBM CONNECT	cnMaestro X Next
300_ENTERPRISEVIEW	camniumnetworks.com	cnMaestro X Next
30_NOV_MON8ZN	camnium	cnMaestro Essentials Next
3_DEC_MON8ZN	camnium	cnMaestro Essentials Next
ABCD_1234	camnium	cnMaestro Essentials Next
C2C_24_30	Cambium Networks	cnMaestro X Trial Next
C2C_IR_TRY_01	Cambium Networks	cnMaestro X Trial Next
C2C_M_24_30	Cambium Networks	cnMaestro X Trial Next
C2C_M_RETRY_01	Cambium Networks	cnMaestro Essentials Next
EMS_CHECKING	camnium	cnMaestro X Next
EPSK_BROADBAND	Cambium Networks	cnMaestro Essentials Next

8. The **Ready to Upgrade** page displays.

The screenshot shows the 'Licensing' page in the Cambium Networks Support Center. The page has a navigation bar with links: Knowledge Base, Downloads, Warranty, Licensing, Beta, FAQ, and My Requests. A 'Submit a request' button and a user profile dropdown are in the top right. The main content area is titled 'Licensing' and includes an 'Entitlements' sidebar on the left with options: Activate Entitlements, Previous Activations, and Saved Entitlements. The 'Fixed Wireless License Keys' section lists various keys like cnVision, ePMP 1000/2000/3000, PMP / PTP 450, PTP 300/400/500/600/800, PTP 550, PTP 650, PTP 670, PTP 700, PTP 810, and PTP 820 / 850. The 'Account Details' section shows: Cambium ID: EPSK_BROADBAND, Name: Cambium Networks, and Type: cnMaestro Essentials. The 'Ready to Upgrade' section displays a progress bar with tiers: Tier1: 0, Tier2: 6, Tier3: 12, and Tier100: 1. Below this is an 'Entitlement' table with columns: Part Number, Description, and Quantity.

Part Number	Description	Quantity
MSX-SUB-T1-1	cnMaestro X for FWB; Tier 1 1-year subscription per device	6
MSX-SUB-T2-1	cnMaestro X for FWB; Tier 2 1-year subscription per device	6
MSX-SUB-T3-3	cnMaestro X for Enterprise Wi-Fi; Tier 3 3-year subscription per device	12
MSX-SUB-T100-1	cnMaestro X for Third Party; Tier 100 1-year subscription per device	1

An 'Activate' button is located below the table.

9. 1. Click **Activate**.



Note

If a Slot Deficit error occurs (meaning there are more devices than slots available) occurs, refer to [Slot Deficit](#).

10. The **Previous Activations** page displays the **Complete** activation list.

The screenshot shows the 'Licensing' page with the 'Previous Activations' tab selected in the sidebar. The main content area displays a table of previous activations. At the top, there is a search bar with the text 'Serial Number, Part Number or Description', a '10 results' dropdown, and a 'Search' button. Below the search bar is a pagination control showing '1 2 3'. The table has columns: Date, Description, Serial Number, and License. All entries in the 'License' column are marked as 'Complete'.

Date	Description	Serial Number	License
2020-12-18	cnMaestro X for Third Party; Tier 100 1-year subscription per device	-	Complete
2020-12-18	cnMaestro X for Enterprise Wi-Fi; Tier 3 3-year subscription per device	-	Complete
2020-12-18	cnMaestro X for FWB AP/PTP/IOT; Tier 2 1-year subscription per device	-	Complete
2020-12-18	cnMaestro X for FWB SM; Tier 1 1-year subscription per device	-	Complete
2020-12-18	cnMaestro X for Enterprise Wi-Fi; Tier 3 10-year subscription per device	-	Complete
2020-12-18	cnMaestro X for Third Party; Tier 100 1-year subscription per device	-	Complete
2020-12-18	cnMaestro X for Enterprise Wi-Fi; Tier 3 10-year subscription per device	-	Complete
2020-12-18	cnMaestro X for Third Party; Tier 100 1-year subscription per device	-	Complete
2020-12-18	cnMaestro X for Third Party; Tier 100 1-year subscription per device	-	Complete
2020-12-18	cnMaestro X for FWB SM; Tier 1 1-year subscription per device	-	Complete

At the bottom of the table, there is another pagination control showing '1 2 3'.

11. Click any licensed description which is marked **Complete**.

Cambium Networks | Support Center

[Submit a request](#)

[Knowledge Base](#)
[Downloads](#)
[Warranty](#)
[Licensing](#)
[Beta](#)
[FAQ](#)
[My Requests](#)

Licensing

Entitlements

[Activate Entitlements](#)

[Previous Activations](#)

[Saved Entitlements](#)

Fixed Wireless License Keys

cnVision

ePMP 1000/2000/3000

PMP / PTP 450

PTP 300/400/500/600/800

PTP 550

PTP 650

PTP 670

PTP 700

PTP 810

PTP 820 / 850

Activation Request: cnMaestro X for Enterprise Wi-Fi; Tier 3 10-year subscription per device

State: Complete

Date: 2020-12-18

Entitlement ID: [\[Link\]](#)

Quantity: 1

Cambium ID: EPSK_BROADBAND

Account Name: Cambium Networks

The Subscription is activated with the number of requested slots.

In the cnMaestro page, a notification displays for a successful update, and the user is asked to wait for 15 minutes.

Subscriptions

[Manage Subscriptions](#)
[Devices](#)

This page provides a usage summary and a list of pending/active/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. [Learn more](#)

[Learn more about device keys](#)

Name	Type	Device Tier	Slots Used	Status	Start Date	End Date	Validity	Commercial ID	Description
cnMaestro X Free Tier	Built-in	Free Tier	5	Active	Dec 21, 2020	Apr 24, 2023	1 year	N/A	cnMaestro X Free Tier
Tier100 2022 01 19 10:30:252 81	Trial	Tier100	0	Active	Jan 19, 2022	Jan 18, 2023	269 days	qpyvsngh@cnmaestronetworks.com	
Tier1 2022 01 19 10:30:252 147	Trial	Free Tier	15	Active	Jan 19, 2022	Jan 18, 2023	269 days	qpyvsngh@cnmaestronetworks.com	
Tier2 2022 01 19 10:30:252 437	Trial	Tier2	5	Active	Jan 19, 2022	Jan 18, 2023	269 days	qpyvsngh@cnmaestronetworks.com	
Tier3 2022 01 19 10:30:252 123	Trial	Tier3	25	Active	Jan 19, 2022	Jan 18, 2023	269 days	qpyvsngh@cnmaestronetworks.com	
Tier4 2022 01 19 10:30:252 31	Trial	Tier4	0	Active	Jan 19, 2022	Jan 18, 2023	269 days	qpyvsngh@cnmaestronetworks.com	
Tier5 2022 01 19 10:30:252 115	Trial	Tier5	0	Active	Jan 19, 2022	Jan 18, 2023	269 days	qpyvsngh@cnmaestronetworks.com	
Tier15 2022 04 01 18:35:162 299	Trial	Tier15	0	Active	Apr 02, 2022	Jan 17, 2023	268 days	qpyvsngh@cnmaestronetworks.com	
Tier100 2021 11 19 12:19:582 385	Trial	Tier100	0	Expired	Nov 19, 2021	Feb 16, 2022	-	qpyvsngh@cnmaestronetworks.com	
Tier2 2021 11 19 12:19:582 339	Trial	Tier2	0	Expired	Nov 19, 2021	Feb 16, 2022	-	qpyvsngh@cnmaestronetworks.com	

Showing 1 - 10 Total: 38

The user account upgrades to a cnMaestro X account.

Cambium Networks | Support Center Submit a request jishma asmi

Knowledge Base Downloads Warranty Licensing Beta FAQ My Requests

Licensing

Entitlements

Activate Entitlements

Previous Activations

Saved Entitlements

Account Details

Cambium ID: EPSK_BROADBAND
Name: Cambium Networks
Type: cnMaestro Essentials

Not enough slots

To upgrade to cnMaestro X, you **must** have an active subscription for every device in your account.

Tier	Required	Already Activated	Available on Entitlement	OK to Upgrade?
Free Tier	6	0	0	No (6 slot deficit)
Tier2	6	0	0	No (6 slot deficit)
Tier3	11	0	1	No (10 slot deficit)
Tier100	1	0	0	No (1 slot deficit)

! This entitlement is not sufficient to upgrade your account to cnMaestro X. You can activate this entitlement, and the subscriptions will be added to your account, but you will not be able to access cnMaestro X features until you have added enough subscriptions to make up the deficit.

Entitlement

Part Number	Description	Quantity
MSX-SUB-T3-10	cnMaestro X for Enterprise Wi-Fi; Tier 3 10-year subscription per device	1

Activate

Fixed Wireless License Keys

cnVision

ePMP 1000/2000/3000

PMP / PTP 450

PTP 300/400/500/600/800

PTP 550

PTP 650

PTP 670

PTP 700

PTP 810

PTP 820 / 850

3. If the user activates even with the slot deficit warning.

- Activation process completes.

Cambium Networks | Support Center Submit a request jishma asmi

Knowledge Base Downloads Warranty Licensing Beta FAQ My Requests

Licensing

Entitlements

Activate Entitlements

Previous Activations

Saved Entitlements

Activation Request: cnMaestro X for Enterprise Wi-Fi; Tier 3 10-year subscription per device

State: Complete
Date: 2020-12-18
Entitlement ID:
Quantity: 1
Cambium ID: EPSK_BROADBAND
Account Name: Cambium Networks

Fixed Wireless License Keys

cnVision

ePMP 1000/2000/3000

PMP / PTP 450

PTP 300/400/500/600/800

PTP 550

PTP 650

PTP 670

PTP 700

PTP 810

PTP 820 / 850

- cnMaestro X upgrade will be pending, since there are not enough slots to match the devices in the account. Refer to **Not enough slots** in the **Manage Subscriptions** tab to identify the slot deficit.
- It also displays the notification message shown below.

1/2 | Your free trial will expire on 28-Apr-2024. No action is needed if you do not want to continue with cnMaestro X after the trial expires. After trial expiry, the account will gracefully downgrade to --

Manage Subscriptions

[Subscriptions](#) [Devices](#)

This page provides a usage summary and a list of pending/active/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. [Learn more](#) [Upgrade to X-NFR](#)

Not enough slots

To upgrade to cnMaestro X, you must have an active subscription for every device in your account. [Learn more](#)

Device Tier	Required	Available	Deficit	Upgradable
Tier 2	14	4	10	No
Tier 3	5	4	1	No
Tier 22	1	4	0	Yes
Tier 24	2	3	0	Yes

[Apply Filter\(s\)](#) [Learn more about device tiers](#)

Name	Type	Device Tier	Slots Used	Status	Start Date	End Date	Validity	Commercial ID
Professional T60	Built-in	Tier 60	0	Active	20 Dec 2023	28 Jan 2025	345 days	N/A
Professional T43	Built-in	Tier 43	0	Active	20 Dec 2023	28 Jan 2025	345 days	N/A
Professional T41	Built-in	Tier 41	0	Active	20 Dec 2023	28 Jan 2025	345 days	N/A
Professional T40	Built-in	Tier 40	0	Active	20 Dec 2023	28 Jan 2025	345 days	N/A
cnMaestro X Free Tier	Built-in	Free Tier	41	Active	20 Dec 2023	28 Jan 2025	345 days	N/A
Tier 30-2024-01-30T04:51:04.998813884Z-310	Trial	Tier 30	0	Active	30 Jan 2024	28 Apr 2024	70 days	harikumar.raman@cambiumnetworks.com
Tier 20-2024-01-30T04:51:04.99878656Z-144	Trial	Tier 20	0	Active	30 Jan 2024	28 Apr 2024	70 days	harikumar.raman@cambiumnetworks.com
Tier 7-2024-01-30T04:51:04.998762228Z-289	Trial	Tier 7	0	Active	30 Jan 2024	28 Apr 2024	70 days	harikumar.raman@cambiumnetworks.com
Tier 6-2024-01-30T04:51:04.998730059Z-40	Trial	Tier 6	0	Active	30 Jan 2024	28 Apr 2024	70 days	harikumar.raman@cambiumnetworks.com
Tier 5-2024-01-30T04:51:04.9987035Z-11	Trial	Tier 5	0	Active	30 Jan 2024	28 Apr 2024	70 days	harikumar.raman@cambiumnetworks.com

4. Once the user removes the deficit, the account automatically upgrades to cnMaestro X.

Subscription Management

A cnMaestro Essentials account can be identified as shown below.

Cambium Networks | cnMaestro™

Welcome, [User Name] Cloud Account Name: Cambium

Devices

346 Total, 73 Offline, 61 Onboarding

Alarms

Period: Last 24 Hours

2 CRITICAL, 5 MAJOR, 7 MINOR

Threats and Vulnerabilities

Period: Last 7 Days

Threats: 0

Devices By Type

Total: 346

- PON: 1 (OLT), 262 (ONU)
- 60 GHz crWave: 5 (CN), 18 (DR)
- Enterprise Wi-Fi: 20
- cnPilot Home: 9
- PMP: 6 (AP), 3 (SM)
- PTP 650/670/700: 8
- NSE: 3
- cnMatrix: 3
- ePMP: 1 (AP), 2 (SM)
- cnReach: 2
- cnVision: 1 (Hub), 1 (Client)
- RV22 Home Mesh: 1

Level Up Your Network

Assure Wi-Fi Experiences with cnMaestro X

Get to the Root Cause of Wi-Fi Client Issues with cnMaestro X Assurance

Maximize Wi-Fi Experiences in Multi-Family Properties with Cambium Networks ePSK and Personal Wi-Fi Technology

Special year-end promotion

Secure your network and implement 24x7 LAN vulnerability monitoring with NSE 3000 Security / SD-WAN device.

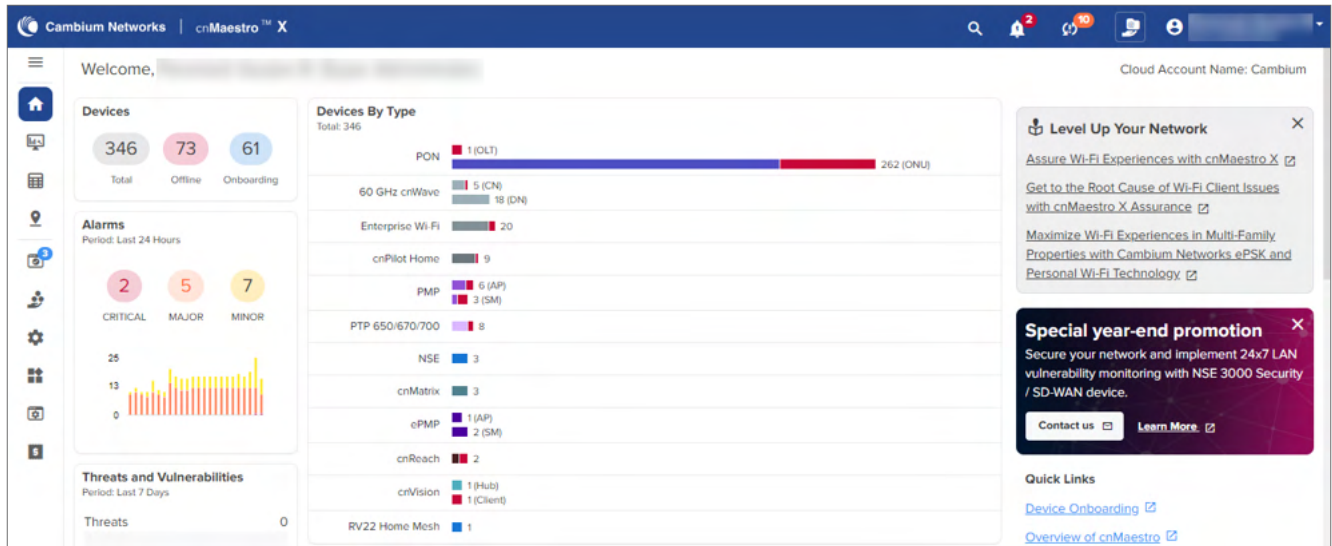
Contact us | Learn More

Quick Links

[Device Onboarding](#)

[Overview of cnMaestro](#)

If a subscription is active, the cnMaestro X banner will display, as shown in the figure below.



This topic contains the following sections:

- [Manage Subscriptions](#)
- [Usage Summary](#)
- [Device Tiers](#)
- [Devices](#)
- [Expiry Notification](#)
- [Retention of Data After Expiry and Reinstatement of Service](#)
- [Overdraft Subscription](#)
- [Download a Bill of Material \(BoM\)](#)

Manage Subscriptions

Users can view, edit, check the validity and status of subscriptions.

1. Navigate to the **cnMaestro > Manage Subscriptions > Subscriptions** page.

Manage Subscriptions

Subscriptions Devices

This page provides a usage summary and a list of pending/active/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. [Learn more](#) [Upgrade to X-NFR](#)

Not enough slots

To upgrade to cnMaestro X, you must have an active subscription for every device in your account. [Learn more](#)

Device Tier	Required	Available	Deficit	Upgradable
Tier 2	15	0	15	No
Tier 3	3	0	3	No
Tier 20	2	0	2	No
Tier 21	1	2	0	Yes
Tier 24	1	2	0	Yes

Apply Filter(s)

Name	Type	Device Tier	Slots Used	Status	Start Date	End Date	Validity	Commercial ID
Tier 23-	New	Tier 23		0/2 Pending	02 Feb 2024	09 Aug 2024	173 days	ss
Tier 22-	New	Tier 22		0/2 Pending	02 Feb 2024	09 Aug 2024	173 days	ss
Tier 21-	New	Tier 21		0/2 Pending	02 Feb 2024	09 Aug 2024	173 days	ss
Tier 24-	New	Tier 24		0/2 Pending	02 Feb 2024	09 Aug 2024	173 days	ss
Tier 2-2-	New	Tier 2	0	Pending	02 Feb 2024	09 Aug 2024	173 days	ss
Tier 2-2-	New	Tier 2		0/1 Expired	02 Feb 2024	16 Feb 2024	-	documentation
Tier 21-	New	Tier 21		0/1 Expired	02 Feb 2024	16 Feb 2024	-	slottwo45
Tier 2-2-	New	Tier 2	0	Expired	02 Feb 2024	16 Feb 2024	-	slottwo45
Tier 21-	New	Tier 21		0/1 Expired	02 Feb 2024	16 Feb 2024	-	slottwo
Tier 2-2-	New	Tier 2	0	Expired	02 Feb 2024	16 Feb 2024	-	slottwo

2. Click the **Edit** icon to edit the subscription **Name** and **Description** and click **Save**.

Edit

Name*

Tier 23-2024-02-12T06:54:12.008387242Z-6

Description

Save

Cancel

- Onboard devices according to the allotted slots.
- New devices are added to the subscription with the earliest expiration.

Usage Summary



Usage summary displays the number of slots that are **Pending**, **Available**, **Used**, **Expiring**, **Expired**, and **Overdraft**.

Device Tiers

Device Tiers display the classifications allotted for each device.

Device Tiers		
Q Search		
Tier	Family	Models
Free Tier	60 GHz cnWave	V1000, V2000, V3000
	cnPilot Enterprise (ePMP Hotspot)	1000 Hotspot
	cnPilot Home	All R-Series Access Points
	cnRanger	All SM Models
	cnVision	MAXr, MAXrp, MICRO, MINI
	ePMP	All SM Models
	PMP	All SM Models
Tier 3	Enterprise Wi-Fi	All E-Series, XE/XV/X7-Series and Xirus(AOS) Access Points
Tier 5	60 GHz cnWave	All Distribution Nodes
Tier 6	cnWave 5G Fixed	All CPE Models
Tier 7	cnWave 5G Fixed	All BTS Models
Tier 20	cnMatrix	All cnMatrix Switches
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
Tier 30	NSE	NSE3000
Tier 40	PON	Fiber OLT-8 Port
Tier 41	PON	Fiber ONT-GPON-Indoor, Fiber ONT-GPON-Outdoor, Fiber ONT-XGS-PON-Indoor, Fiber ONT-XGS-PON-Outdoor
Tier 43	PON	Fiber OLT-16 Port
Tier 60	RV22 Home Mesh	RV22

Unlisted devices do not require paid subscription. They are part of the Free Tier (Tier 0). All Tier 0 through Tier 7 devices can be used with an Essentials account. Tier 20 and Tier 30 require paid subscription even in Essentials mode.

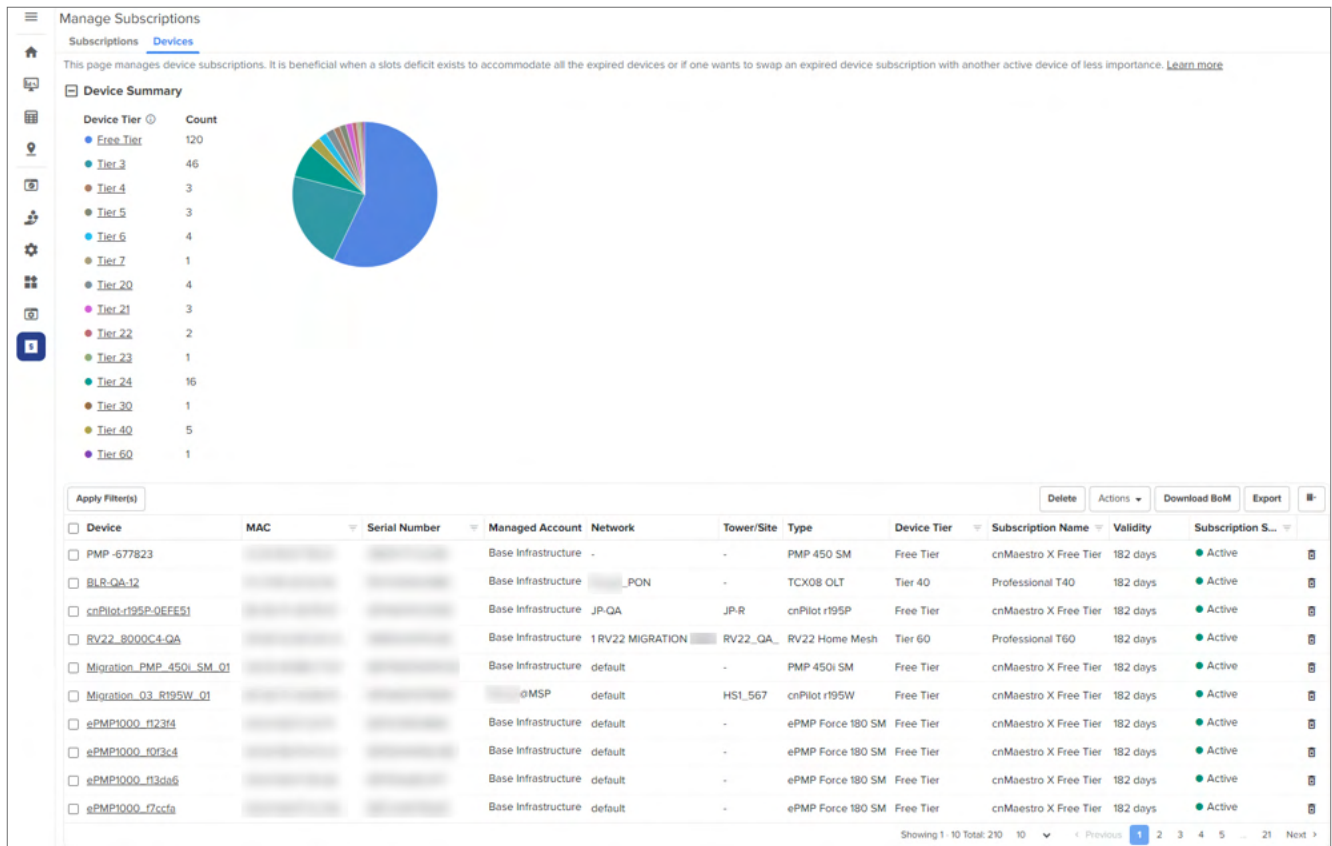


Note

To manage NSE devices under Essentials account, you need a subscription. If your account is upgraded to cnMaestro X, the Essentials NSE subscription will automatically be transferred to cnMaestro X. You will not need any additional subscription for NSE again.

Devices

The Devices page displays devices mapped to their subscription, and it allows changing or swapping a subscription. **Device Summary** displays device counts per tier.



Swap Subscription

Swap Subscription allows the user to swap one device subscription with another device of the same tier. It can be performed at any time.



Note

To manage NSE devices under Essentials account, you need a subscription. If your account is upgraded to cnMaestro X, the Essentials NSE subscription will automatically be transferred to cnMaestro X. You will not need any additional subscription for NSE again.

To swap subscriptions:

1. Navigate to the **Manage Subscriptions > Devices** and copy the **MAC address** to which the device subscription needs to be swapped.

Manage Subscriptions

Subscriptions **Devices**

This 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. [Learn more](#)

Device Summary

Device Tier Count

- Free Tier 120
- Tier 3 46
- Tier 4 3
- Tier 5 3
- Tier 6 4
- Tier 7 1
- Tier 20 4
- Tier 21 3
- Tier 22 2
- Tier 23 1
- Tier 24 16
- Tier 30 1
- Tier 40 5
- Tier 60 1

Apply Filter(s)

Device	MAC	Serial Number	Managed Account	Network	Tower/Site	Type	Device Tier	Subscription Name	Validity	Subscription S...
PMP-677823			Base Infrastructure	-	-	PMP 450 SM	Free Tier	cnMaestro X Free Tier	182 days	Active
BLR-QA-12			Base Infrastructure	Durga_PON	-	TCX08 OLT	Tier 40	Professional T40	182 days	Active
cnPilot-r195P-0EFE51			Base Infrastructure	JP-QA	JP-R	cnPilot r195P	Free Tier	cnMaestro X Free Tier	182 days	Active
RV22_8000C4-QA			Base Infrastructure	1 RV22 MIGRATION UMA	RV22_QA	RV22 Home Mesh	Tier 60	Professional T60	182 days	Active
Migration_PMP_450I_SM_01			Base Infrastructure	default	-	PMP 450I SM	Free Tier	cnMaestro X Free Tier	182 days	Active
Migration_03_R195W_01			eMSP	default	HS1_567	cnPilot r195W	Free Tier	cnMaestro X Free Tier	182 days	Active
ePMP1000_r123f4			Base Infrastructure	default	-	ePMP Force 180 SM	Free Tier	cnMaestro X Free Tier	182 days	Active
ePMP1000_r0f3c4			Base Infrastructure	default	-	ePMP Force 180 SM	Free Tier	cnMaestro X Free Tier	182 days	Active
ePMP1000_r13da6			Base Infrastructure	default	-	ePMP Force 180 SM	Free Tier	cnMaestro X Free Tier	182 days	Active
ePMP1000_r7ccfa	00-04-56-F7-CC-FA		Base Infrastructure	default	-	ePMP Force 180 SM	Free Tier	cnMaestro X Free Tier	182 days	Active

Showing 1 10 Total: 210 10 Previous 1 2 3 4 5 ... 21 Next

2. Select the device to be swapped to another subscription.

Manage Subscriptions

Subscriptions **Devices**

This 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. [Learn more](#)

Device Summary

Device Tier Count

- Free Tier 120
- Tier 3 46
- Tier 4 3
- Tier 5 3
- Tier 6 4
- Tier 7 1
- Tier 20 4
- Tier 21 3
- Tier 22 2
- Tier 23 1
- Tier 24 16
- Tier 30 1
- Tier 40 5
- Tier 60 1

Apply Filter(s)

Device	MAC	Serial Number	Managed Account	Network	Tower/Site	Type	Device Tier	Subscription Name	Validity	Subscription S...
PMP-677823			Base Infrastructure	-	-	PMP 450 SM	Free Tier	cnMaestro X Free Tier	182 days	Active
BLR-QA-12			Base Infrastructure	_PON	-	TCX08 OLT	Tier 40	Professional T40	182 days	Active
cnPilot-r195P-0EFE51			Base Infrastructure	JP-QA	JP-R	cnPilot r195P	Free Tier	cnMaestro X Free Tier	182 days	Active
RV22_8000C4-QA			Base Infrastructure	1 RV22 MIGRATION	RV22_QA	RV22 Home Mesh	Tier 60	Professional T60	182 days	Active
Migration_PMP_450I_SM_01			Base Infrastructure	default	-	PMP 450I SM	Free Tier	cnMaestro X Free Tier	182 days	Active
Migration_03_R195W_01			eMSP	default	HS1_567	cnPilot r195W	Free Tier	cnMaestro X Free Tier	182 days	Active
ePMP1000_r123f4			Base Infrastructure	default	-	ePMP Force 180 SM	Free Tier	cnMaestro X Free Tier	182 days	Active
ePMP1000_r0f3c4			Base Infrastructure	default	-	ePMP Force 180 SM	Free Tier	cnMaestro X Free Tier	182 days	Active
ePMP1000_r13da6			Base Infrastructure	default	-	ePMP Force 180 SM	Free Tier	cnMaestro X Free Tier	182 days	Active
ePMP1000_r7ccfa			Base Infrastructure	default	-	ePMP Force 180 SM	Free Tier	cnMaestro X Free Tier	182 days	Active

Showing 1 10 Total: 210 10 Previous 1 2 3 4 5 ... 21 Next

3. From the **Actions** dropdown list, click **Swap Subscription**.

Enter the **MAC Address** and click **Swap**.

Swap Subscription for "XV3-8-ED1368"

Enter MAC Address of the target device with an active subscription and belonging to the same tier - Tier 3.

MAC Address*

Cancel

Swap

A success notification is displayed on successful subscription swapping.

Change Subscription

Change Subscription changes the device from one subscription to another of the same tier when slots are available.



Note

Change subscription operation is not allowed for devices belonging to Free Tier, Tier 40, Tier 41, Tier 43, Tier 60.

To change subscription:

1. Navigate to the **Manage Subscriptions > Devices** and select the device.
2. From the **Actions** dropdown list, click **Change Subscriptions**.

Manage Subscriptions

Subscriptions

Devices

This 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. [Learn more](#)

Device Summary

Device Tier

Count

Free Tier

120

Tier 3

46

Tier 4

3

Tier 5

3

Tier 6

4

Tier 7

1

Tier 20

4

Tier 21

3

Tier 22

2

Tier 23

1

Tier 24

16

Tier 30

1

Tier 40

5

Tier 60

1

Apply Filter(s)

2 records from this grid are selected. [Select All 230 records](#) [Clear Selection](#)

Device	MAC	Serial Number	Managed Account	Network	Tower/Site	Type	Device Tier	Subscription Name	Validity	
<input type="checkbox"/> cnMaestro_SIT-e700			Application issue testing-MSP	default	New-Site	cnPilot e5--	Tier 3	Tier 3-2024-02-	153 days	
<input type="checkbox"/> cnMaestro_SIT-XV0			Application issue testing-MSP	default	New-Site	XV2-22H	Tier 3	Tier 3-2024-02-	153 days	Active
<input type="checkbox"/> XV2-2-S1MF03			Base Infrastructure	default	-	XV2-2	Tier 3	Tier 3-2024-02-	153 days	Active
<input type="checkbox"/> XV3-8-ED1368			Base Infrastructure	default	cm_site	XV3-8	Tier 3	Tier 3-2024-02-	153 days	Active
<input checked="" type="checkbox"/> XV2-22H-E94BCA			Base Infrastructure	default	cm_site	XV2-22H	Tier 3	Tier 3-2024-02-	153 days	Active

Delete

Actions

Export

Delete On Expiry

Swap Subscription

Change Subscription

3. **Change Subscription** window pops up, select the **Subscription** from the dropdown.

Change Subscription

Subscription

Tier 3-2024-02-21T11:33:42.93326804Z-369 (54 Available Slots)

153 days validity

Cancel

Change

4. Click **Change**.

A success notification is displayed on successful subscription change.

Delete on Expiry



Note

- Once a device state is changed to **Delete on Expiry**, this action cannot be undone.
- Tier 30 (NSE) devices also support **Delete on Expiry** in cnMaestro Essentials.

User can select the device and set the subscription state to **Delete on Expiry**, once the device is expired, it automatically is deleted from the device list.

To set the delete on expiry option:

1. Navigate to the **Manage Subscriptions > Devices** and select the device.

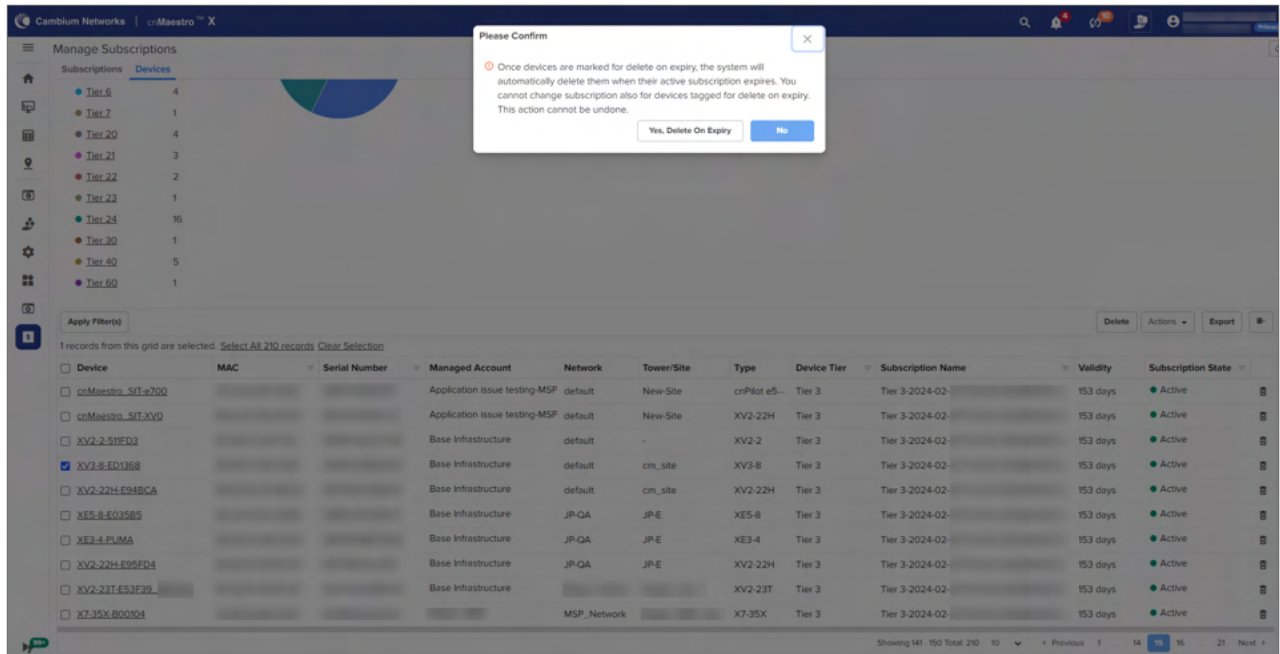
Device Summary

Device Tier	Count
Free Tier	120
Tier 3	46
Tier 4	3
Tier 5	3
Tier 6	4
Tier 7	1
Tier 20	4
Tier 21	3
Tier 22	2
Tier 23	1
Tier 24	16
Tier 30	1
Tier 40	5
Tier 60	1

Device	MAC	Serial Number	Managed Account	Network	Tower/Site	Type	Device Tier	Subscription Name	Validity	Subscription S...
<input type="checkbox"/> PMP-677823			Base Infrastructure	-	-	PMP 450 SM	Free Tier	cnMaestro X Free Tier	182 days	Active
<input type="checkbox"/> BLR-QA-12			Base Infrastructure	-PON	-	TCX08 OLT	Tier 40	Professional T40	182 days	Active
<input type="checkbox"/> cnPilot-r19SP-0EEF51			Base Infrastructure	JP-QA	JP-R	cnPilot r19SP	Free Tier	cnMaestro X Free Tier	182 days	Active
<input type="checkbox"/> RV22_8000C4-QA			Base Infrastructure	1 RV22 MIGRATION	RV22_GA_	RV22 Home Mesh	Tier 60	Professional T60	182 days	Active
<input type="checkbox"/> Migration_PMP_450i_SM_01			Base Infrastructure	default	-	PMP 450i SM	Free Tier	cnMaestro X Free Tier	182 days	Active
<input type="checkbox"/> Migration_03_R195W_01			@MSP	default	HS1_567	cnPilot r195W	Free Tier	cnMaestro X Free Tier	182 days	Active
<input type="checkbox"/> ePMP1000_1123f4			Base Infrastructure	default	-	ePMP Force 180 SM	Free Tier	cnMaestro X Free Tier	182 days	Active
<input type="checkbox"/> ePMP1000_10f3c4			Base Infrastructure	default	-	ePMP Force 180 SM	Free Tier	cnMaestro X Free Tier	182 days	Active
<input type="checkbox"/> ePMP1000_113da6			Base Infrastructure	default	-	ePMP Force 180 SM	Free Tier	cnMaestro X Free Tier	182 days	Active
<input type="checkbox"/> ePMP1000_17ccfa			Base Infrastructure	default	-	ePMP Force 180 SM	Free Tier	cnMaestro X Free Tier	182 days	Active

Showing 1 - 10 Total: 210

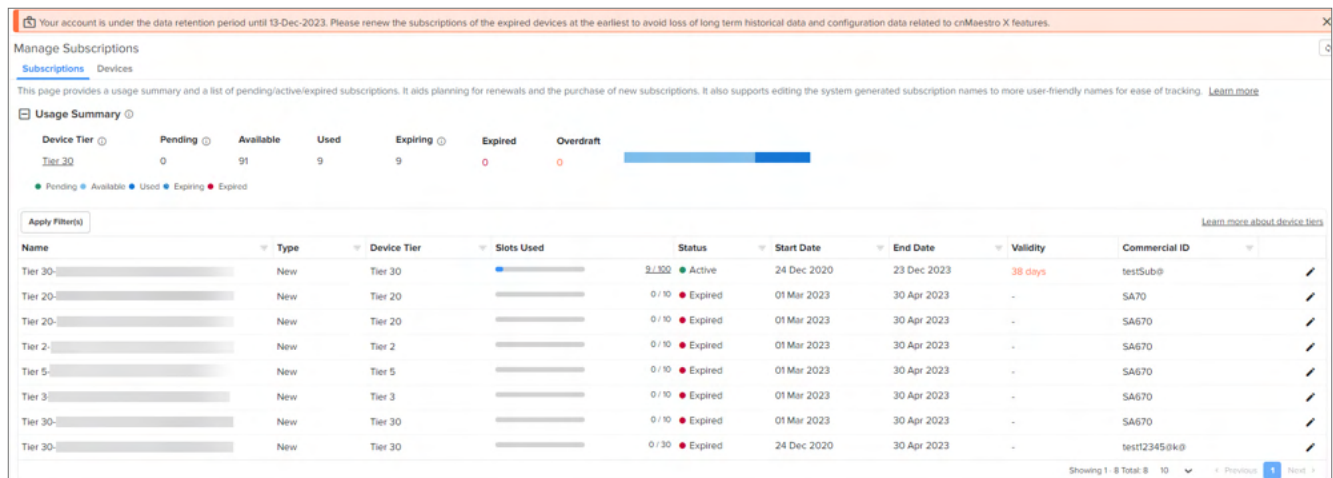
2. From the **Actions** dropdown list, click **Delete on Expiry**.
3. Click **Yes, Delete On Expiry** in the confirmation window.



4. The subscription state changes to **Delete on Expiry** from **Active**.

Expiry Notification

If the subscription validity is less than 90, in the **Validity** column the number of days left are highlighted in red color. Also, a notification message will be displayed as shown below.



The expired subscription slots are automatically moved to the active subscription, if the number of expired subscription slots is equal to or less than the number of available subscription slots.

Expired Device

Once the device expires, all device level features become inaccessible. The device should either be deleted from the account or added to a new subscription as shown below:



Note

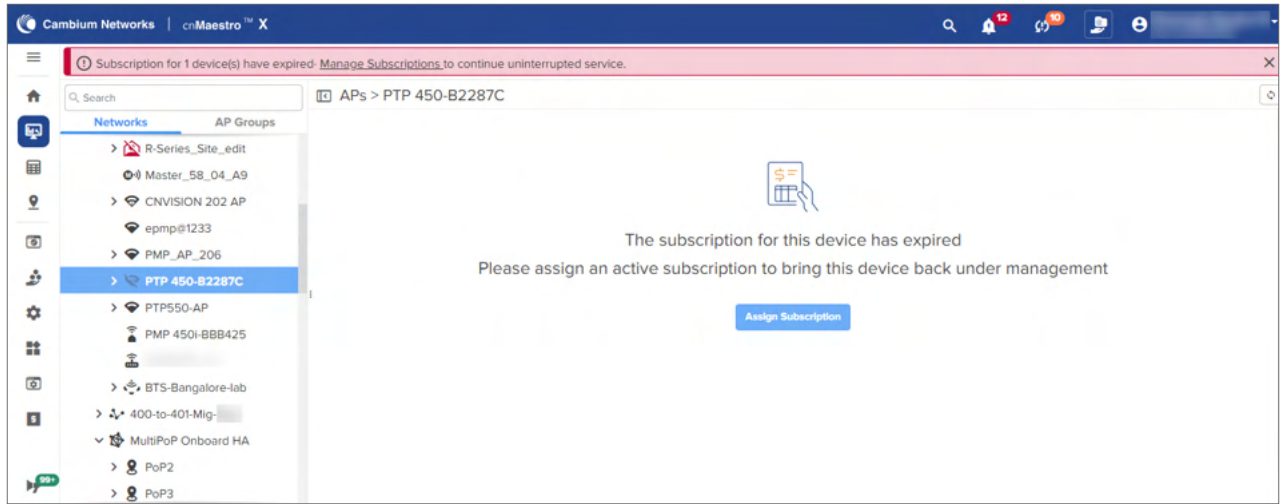
In the expired device dashboard:

- If any free slots are available Change Subscription will be enabled.
- If free slots are not available Swap Subscription will be enabled with the specific device MAC address.

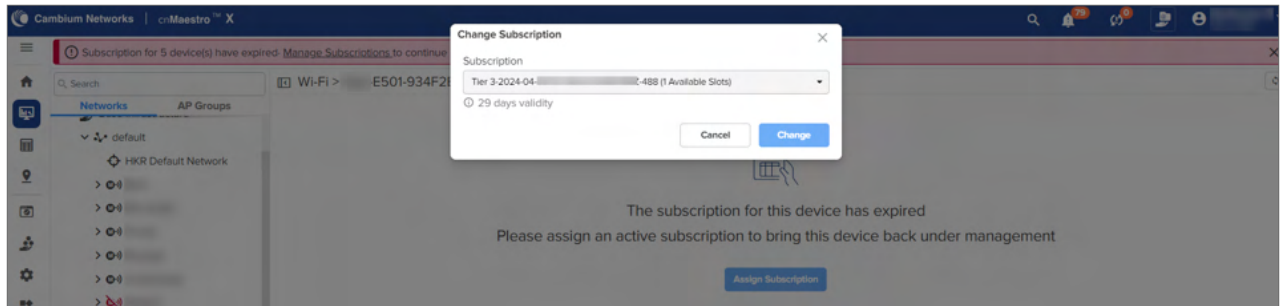
- If you have an X account with expired devices, you can downgrade to Essentials and manage all devices without X features. The activated subscriptions will be moved to pending state.

Change Subscription at device level

1. Navigate to **Manage > Network >** and select the expired device.

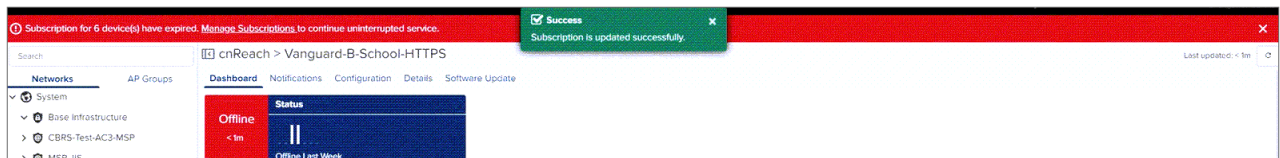


2. Click **Assign Subscription** and select the **Subscription** from the list.



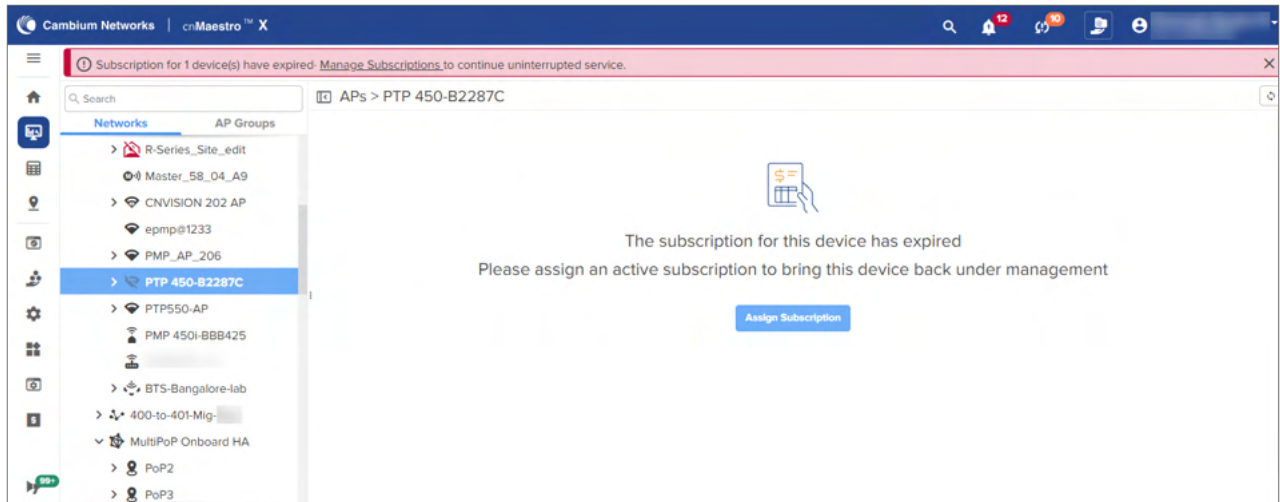
3. Click **Save**.

The following message displays if successful and the device becomes active.

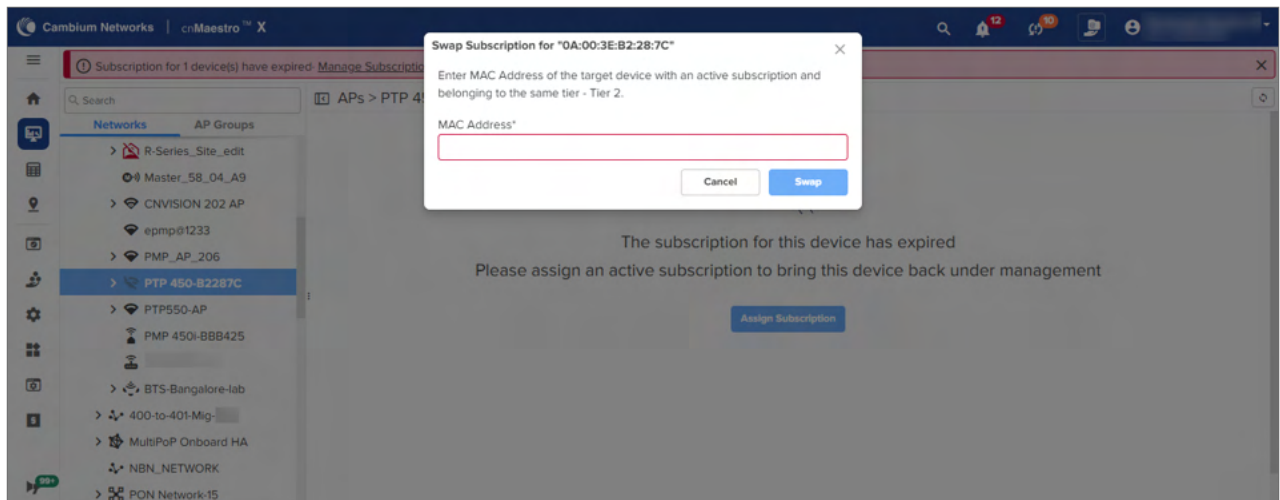


Swap Subscription at device level

1. Navigate to **Manage > Network >** and select the expired device.



2. Click **Assign Subscription**. The **Swap Subscription** window pops up.



3. Enter the **MAC address** and click **Swap**.

Retention of Data After Expiry and Reinstatement of Service

If subscriptions are not renewed in time, devices under those subscriptions will expire and are no longer managed by cnMaestro. Once all subscriptions are expired, the account transitions to cnMaestro Essentials with a data retention period for historical data of 90 days. All historical data beyond one week, and cnMaestro X specific configuration, will be retained until the data retention period of 90 days, after which it will be deleted. This is done to ensure no data loss if subscriptions are renewed before the data retention period ends.

Overdraft Subscription



Note

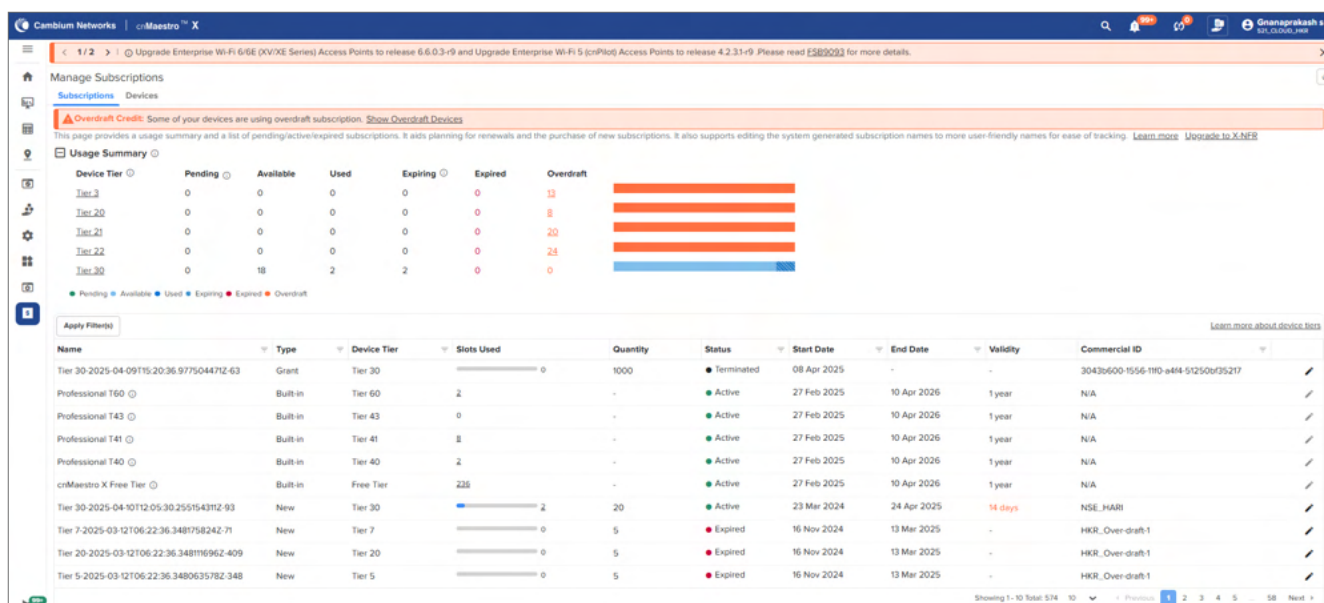
Overdraft support is available only in cnMaestro X and is applicable for NSE devices in an ESS account. A minimum of one active subscription is required to enable this feature.

In the **Manage Subscriptions > Devices** page, the Overdraft Subscription feature allows newly onboarded devices to operate temporarily without an active subscription when no available slots are found. The overdraft period is

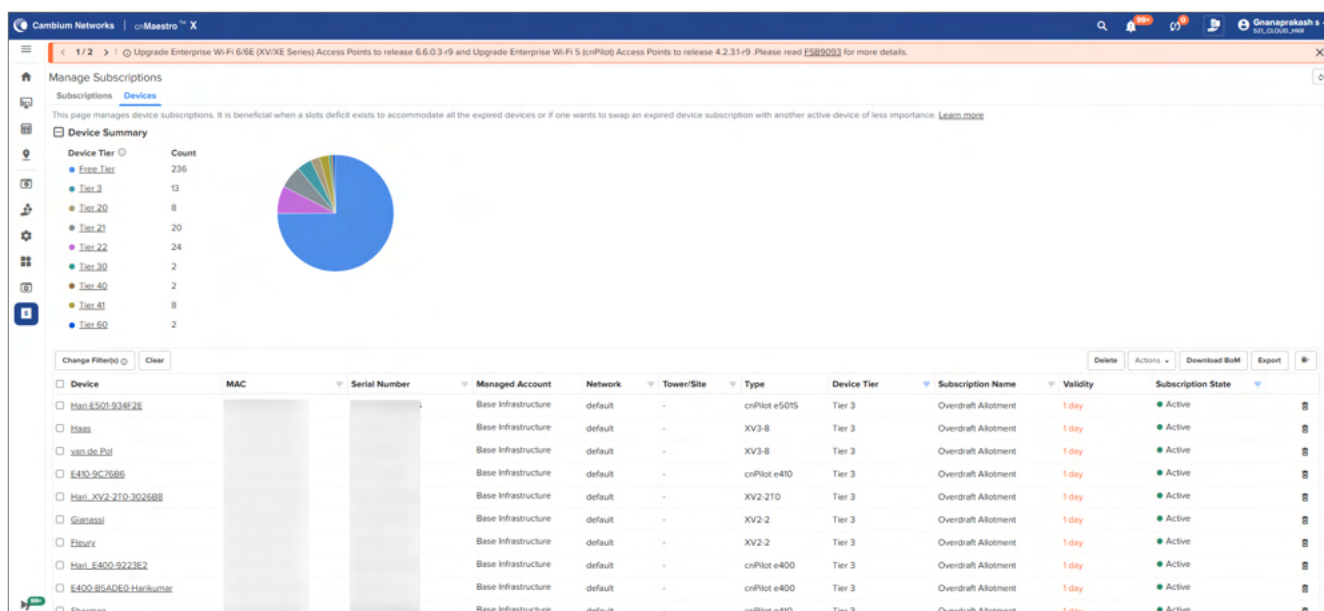
assigned automatically, and access is provided for a specific duration determined by the Cambium Networks support team.

Overdraft devices can be reassigned to other subscription slots using the Change Subscription feature and devices in standard subscriptions cannot be converted to overdraft by users. Once the overdraft period ends, the device automatically moves to an expired state and is no longer managed.

When a device is moved to overdraft, a banner is displayed on the Subscription Summary page as shown in the below figure. In the overdraft credit banner, click **Show Overdraft Devices** to view the list of devices in overdraft.

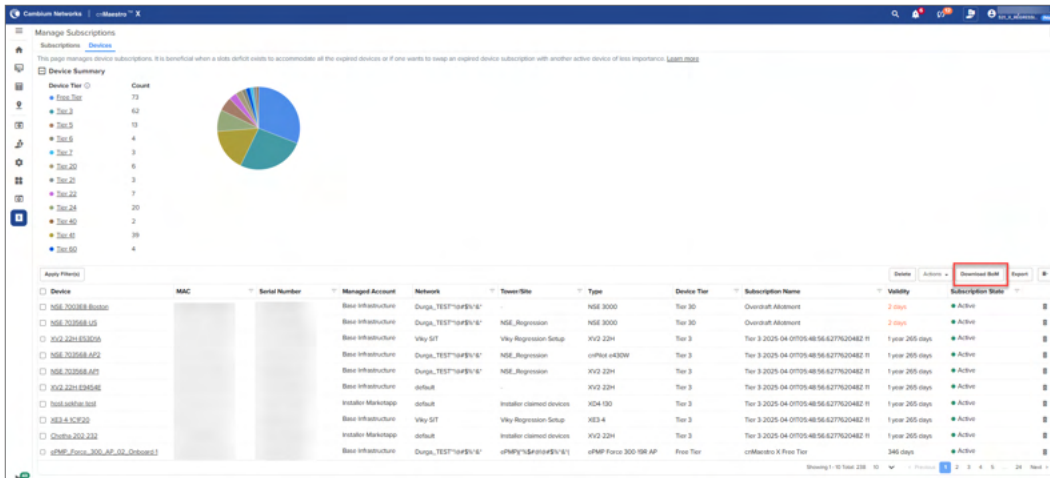


On the Devices page displays the **Overdraft Devices** as shown in the below figure.



Download a Bill of Material (BoM)

In the **Manage Subscriptions > Devices** page, the download BoM feature allows the users to generate a summary of the required subscriptions for an account to upgrade. The downloaded file is used to analyze and determine subscription requirements.



Perform the following steps to download the BoM:

1. Navigate to **Manage Subscriptions > Devices**.
2. Click **Download BoM**.

Download a Bill of Material (BoM) window appears, as shown in the figure below.

Download a Bill of Material(BoM)

This subscription requirement is summarized below. You can adjust the quantity if needed. Please download the BoM(CSV format) and share it with your partner to place an order. Download has an additional file capturing SKU missing devices.

Model	Class	Active	Overdraft	Expired	Requirement
1000	ePMP 1000	16	14	2	16
2000	ePMP 2000	1	1	0	1
3000	ePMP 3000	1	1	0	1
4000	ePMP 4000 - 6 GHz	1	1	0	1
450	PMP 450 AP(disconnected-onprem)	10	10	0	10
450i	PMP 450v 4x4 AP	12	12	0	12
450i AP	PMP 450i 5 GHz AP	1	1	0	1
450v	PMP 450v 4x4 AP	1	1	0	1
E400	cnPilot	2	2	0	2
E410	E410	5	5	0	5
EX2010	EX2010	5	5	0	5
EX2010	EX2010-P	3	3	0	3
MP3000	Micro-Pop	1	1	0	1
NSE3000	NSE 3000	2	2	0	2
XV2-2	XV2-2H	7	7	0	7
XV2-2	XV2-2T0	1	1	0	1
XV3-8	XV3-8	7	7	0	7

Cancel
Download

3. The subscription requirements are generated based on the device model and class.
4. Modify the subscription count, if required.
5. Click **Download** to download the BoM file in .CSV format.
- Success** window pops up.
6. If any missing materials are detected, it generates an additional Bill of Missing Material in .CSV format.

Once the BoM file is downloaded, share it with the Cambium Networks support team for validation and to proceed with the required subscriptions.

cnMaestro X features behavior state

cnMaestro X subscriptions can be purchased for 1 year, 3 years, and 5 years. Pricing is based on device tiers. Device slots are purchased for each device tier needed for a deployment. Devices require free slots in order to onboard.



Note

To manage NSE devices under Essentials account, you need a subscription. If your account is upgraded to cnMaestro X, the Essentials NSE subscription will automatically be transferred to cnMaestro X. Thereafter, no additional subscription for NSE is required.

The following table describes about the cnMaestro feature behavior state in different modes such as cnMaestro X, data retention period, and after data retention period.

Table 8 *cnMaestro X Feature behavior state matrix*

Feature	cnMaestro X	On Downgrading cnMaestro X to Essentials and Data Retention Period	After Data Retention Period
60 GHz cnWave	<p>Link Events</p> <ul style="list-style-type: none"> Maintains link events data up to 30 days. <p>Maps</p> <ul style="list-style-type: none"> Channel and Polarity in Device Overlay Golay, SNR, MCS, RSSI, Throughput(Mbps), Airtime % and Link Fade Margin in Link Overlay Auto Refresh option allows to add up to 10 devices Topology Scan Node Throughput test Link Throughput test Current Best Route(s) Interference Scan <p>High Availability</p> <ul style="list-style-type: none"> Allows configuring a secondary (backup or passive) E2E Controller from cnMaestro 	<p>Link Events</p> <ul style="list-style-type: none"> Only 7 days link events data is exposed Data will still be collected in retention period <p>Maps</p> <ul style="list-style-type: none"> Status and Sectors in Device Overlay 	<p>Link Events</p> <ul style="list-style-type: none"> Not accessible <p>Maps</p> <ul style="list-style-type: none"> Status in Link Overlay Status and Sectors in Device Overlay

Feature	cnMaestro X	On Downgrading cnMaestro X to Essentials and Data Retention Period	After Data Retention Period
Administrator Count	Administrator limit increased from 10 to 200.	New users cannot be added if the current count is 10 or more.	Deletes cnMaestro users with the lower privileges in Super Administrator > Administrator > Operator > Monitor to maintain 10 users.
API Clients	Create API clients and access tokens	Not accessible	Not accessible
Applications	View details of applications accessed by users in a particular site. This is available for Enterprise Wi-Fi and NSE devices.	<ul style="list-style-type: none"> Enterprise Wi-Fi—Not accessible NSE—Accessible and displays data 	<ul style="list-style-type: none"> Enterprise Wi-Fi—Not accessible NSE—Accessible and displays data
Application Visibility	Enables users to control or block applications, or terminate based on consumption of applications.	Not accessible	Not accessible
Assists	Assists helps to isolate configuration issues in a deployment.	Not accessible	Not accessible
Assurance	<ul style="list-style-type: none"> View client connection health and Wi-Fi client analytics data, available for the last 24 hours on Site > Dashboard Site > Assurance X tab displays client analytics events data Notification > Wi-Fi Events displays View Lifecycle Event button Client > Lifecycle tab must display if the client is connected to a analytics-enabled device Client dashboard > Client History graph displays lifecycle events Client dashboard displays Connection Success Rate widget 	Not accessible	Not accessible

Feature	cnMaestro X	On Downgrading cnMaestro X to Essentials and Data Retention Period	After Data Retention Period
Audit Logs	Audit Logs record user activity.	Audit log generation continues through the data retention period, but users cannot access the logs.	Not accessible
Auto-Provisioning	Allows configuring and approving of devices automatically based on IP address.	Not accessible	Not accessible
Base WLAN for Personal Wi-Fi SSID (Part of WLANs > ePSK configuration)	Allows user to configure personal SSID, password, and VLAN. This disables the local ePSK and the WLAN SSID.	Not accessible	Not accessible
Bulk Edit	<ul style="list-style-type: none"> Allows bulk edit of device configuration for Enterprise Wi-Fi devices. Allows bulk edit through import and export of CSV files. 	Not accessible	Not accessible
Client Dashboard	<ul style="list-style-type: none"> Displays Wi-Fi Client application and network statistics. Application statistics are only available for NSE, XV, XD, XE, and XR series devices. 	Not accessible	Not accessible
Configuration Lock	Prevents changes to Wi-Fi AP, cnMatrix, and NSE device configuration, even if the device is updated directly.	The lock is no longer enforced.	Not accessible
Custom Applications	Configure applications with a specific IP address or a domain name, and apply filter rules.	Not accessible	Not accessible
EasyPass	Create captive portal to allow clients to access the network through various portal types. Following portal types require an cnMaestro X subscription: Guest/Public Access	Configuration will be retained, but the cnMaestro X portal types will no longer be available.	cnMaestro X portal types will no longer be available.

Feature	cnMaestro X	On Downgrading cnMaestro X to Essentials and Data Retention Period	After Data Retention Period
	<ul style="list-style-type: none"> Self Registration Sponsored Guest Paid Employee/Student Access <ul style="list-style-type: none"> Microsoft Azure Google Login Onboarding Combined <ul style="list-style-type: none"> One Click + Paid Voucher + Paid 		
Email Notifications	Maximum upto 10 email recipients can be added per scope (All Accounts, Base Infra and per MSP)	<ul style="list-style-type: none"> All the configured email recipients are retained None of the email recipients are deleted. Only the 2 earliest added subscribers per scope would receive email notifications. 	Only the 2 earliest added recipients are retained. The remaining email recipients are deleted automatically.
ePSK Limit	ePSK limit increased from 300 to 2000.	New ePSK entries cannot be added if the current count is 300 or more.	Only 300 entries are retained, and the remaining entries will be deleted.
Guest Portal—Access	Connect a wireless service through following access methods: <ul style="list-style-type: none"> Paid access Enterprise: <ul style="list-style-type: none"> Microsoft Azure Sponsored Guests Self Registration Google Guests page— Allows to view details of self registered guests connecting to the wireless network. 	Configuration will be retained, but the feature will no longer be available.	Not accessible
Guest Portal—Design	Allows to create email templates to send email	Configuration will be retained, but the feature will no longer be available.	Not accessible

Feature	cnMaestro X	On Downgrading cnMaestro X to Essentials and Data Retention Period	After Data Retention Period
	confirmation and password for enterprise self registration and sponsored guests.		
Guest Portal	Allows 500 guest portals, 10,000 sessions, and 20,000 login event session records for a maximum of 1 year.	<ul style="list-style-type: none"> • If the count is more than 4 then, all portals are read-only. • Only portal delete option is available to the user. • All existing client sessions will continue without any disruption. 	Only 4 portals will be retained and rest will be deleted.
Graphical Reports Template	<ul style="list-style-type: none"> • Assurance (Only at the Site-level)—Top Access Points Reporting Client Disconnections, Top Client Connection Failures, Top Affected Client OS by Failure Count, Top Affected Client Types by Failure Count • Access Points—Top Access Points by Traffic Usage • Clients—6E Clients by Radio, Client Count by Band, Client Count by Manufacturers, Client Count by OS, Client Count over Time, Peak and Unique Clients, Top Access Points by Unique Clients, Top Application Category by Client Count, Top Applications by Client Count, Top Applications by Usage, Top Category by Usage, Top Client Types by Traffic Usage, Top Clients by Traffic Usage, Top Managed Accounts by Traffic Usage, Top 	Not accessible.	Not accessible.

Feature	cnMaestro X	On Downgrading cnMaestro X to Essentials and Data Retention Period	After Data Retention Period
	Sites by Client Count, Top Sites by Traffic Usage, Top SSIDs by Client Count, Top SSIDs by Traffic Usage		
Identity Provider (IdP) Role mapping	IDP Role-Mappings tab is visible to Super-Admin and Administrator roles. <ul style="list-style-type: none"> • Validate IdP role mapping key • View existing role mappings • Add, edit, delete role mappings. 	Not accessible	Not accessible
Installation Summary	Installation summary of PMP and ePMP SMs, cnMatrix, and Enterprise Wi-Fi APs installed using the Installer mobile application.	Not accessible	Not accessible
Layer 7 (Application Filtering) (Part of Wi-Fi Profiles > Access Control Policies > IP and Application Filtering Rules)	Filter individual applications or applications belonging to a category.	Not accessible	Not accessible
Long term Historical Data	Displays the devices performance graph: <ul style="list-style-type: none"> • Performance graphs for Wi-Fi APs and cnMatrix support historical data for 14 months. • Performance graphs for Fixed Wireless Broadband devices support historical data for 26 months. • All performance graphs for IIoT devices support historical data for 14 	Only 7 days of statistics will be exposed, but existing data will be maintained. During the retention period, data will be maintained.	Removes data beyond 7 days.

Feature	cnMaestro X	On Downgrading cnMaestro X to Essentials and Data Retention Period	After Data Retention Period
	months.		
Managed Services	Provides separate Managed Accounts – each with independent administration and configuration.	<ul style="list-style-type: none"> Managed Account users are logged out. Managed Services tab is hidden. Managed Account configuration changed to read-only. Managed Accounts > Users tab hidden. All managed accounts are changed to read-only. 	All managed services are deleted, and they will no longer be associated with any managed accounts.
MarketApps	Allows property managers, residents, and MSPs to administer and manage the Wi-Fi networks in multi-dwelling units and apartment complexes.	Not accessible	Not accessible
Multi-Floor Site Plan	Allows to create 50 floor plan per site.	<ul style="list-style-type: none"> All floor plans are viewable as read-only. Cannot create additional floor plans or edit any existing floor plans if more than one configured in a Site. Edit is available only when all additional floor plans are deleted. 	<ul style="list-style-type: none"> Additional floor plans is deleted and devices on those floors is unmapped. Only the latest floor is available.
Reports	Schedule Devices, Performance, Active Alarms, Alarm History, Events, Clients, Mesh Peers, and Guest Access Login Events Reports.	Reports tab will not be accessible, and all previously scheduled reports will be skipped.	All jobs will be terminated and Reports are not accessible.
Satellite View	It allows to view maps in Satellite view.	Not accessible	Not accessible
Session Management	Tracks the current cnMaestro user sessions and optionally allows to logout cnMaestro user sessions.	Not accessible	Not accessible
Spectrum Analyzer	Analyzes and monitors the wireless spectrum for	Not accessible	Not accessible

Feature	cnMaestro X	On Downgrading cnMaestro X to Essentials and Data Retention Period	After Data Retention Period
	optimizing network performance on PMP devices.		
Stanley-AeroScout	Delivers accurate and reliable location data for assets and customers with the STANLEY Healthcare Wi-Fi tags.	Not accessible	Not accessible
Terrain View	It allows to view maps in Terrain view.	Not accessible	Not accessible
Wireless Intrusion Detection System (WIPS)	Protect wireless networks from unauthorized access and potential security threats. <ul style="list-style-type: none"> WIDS data is processed APIs are supported 	Statistics is not available through API	Not accessible
Wireless Intrusion Prevention System (WIPS)	Enhances security of wireless networks by deauthenticating rogue APs and clients. <ul style="list-style-type: none"> WIDS data is processed APIs are supported 	Not accessible	Not accessible
WLANs Dashboard	View details of all WLANs that are applied on devices at a given site. Also view the details of APs connected to these WLANs.	Not accessible	Not accessible

Navigating the cnMaestro UI

cnMaestro provides a number of ways to navigate the UI.

This section includes the following topics:

- [Account View](#)
- [Home page](#)
- [Page structure](#)
- [Page navigation](#)
- [Access and Backhaul View](#)
- [Enterprise Account view](#)
- [Side menu](#)

- [Section tabs](#)
- [System status](#)
- [Data Tables and Chart UI Controls](#)
- [Logout](#)

Account View

cnMaestro supports three different account views, based upon the composition of devices.

- Access and Backhaul view
- Enterprise view
- Industrial Internet view

The account view is selected when the account is created but it can be changed later through the **Administration > Settings > General** page.

Figure 28 *Account View*

The screenshot shows the 'Administration > Settings' page with the 'General' tab selected. Under the 'Basic' section, the 'Time Zone' is set to 'Pacific/Midway (UTC -11:00)'. The 'Account View' section is expanded, showing three options: 'Access and Backhaul', 'Enterprise', and 'Industrial Internet'. The 'Industrial Internet' option is selected with a radio button. Below the 'Account View' section, there is a 'Zero Touch Onboarding Of SM Devices' section with a checkbox labeled 'Allow automatic onboarding of ePMP and PMP SM devices' which is currently unchecked. At the bottom of the page, there are 'Save' and 'Discard' buttons.

Access and Backhaul View

The Access and Backhaul View supports all Fixed Wireless and Wi-Fi deployments. The device types include 60 GHz cnWave, cnMatrix, cnPilot Home (cnPilot R-Series), cnRanger, cnVision, cnWave 5G Fixed, Enterprise Wi-Fi (E-Series and XE/XV/X7-Series), cnPilot Enterprise (ePMP 1000 Hotspot), Enterprise Wi-Fi (Xirrus-Series), ePMP, NSE, PMP, PTP 650/670/700, PTP 820/850, RV22 Home Mesh, and PON.

Enterprise View

The Enterprise View supports the Enterprise Wi-Fi portfolio, which includes the cnPilot Enterprise APs, cnMatrix, and Enterprise Wi-Fi APs (E-Series, and XE/XV/X7-Series), and Enterprise Wi-Fi (Xirrus-Series), and NSE. It provides a simplified UI for Wi-Fi components (hiding fixed wireless features such as Towers).

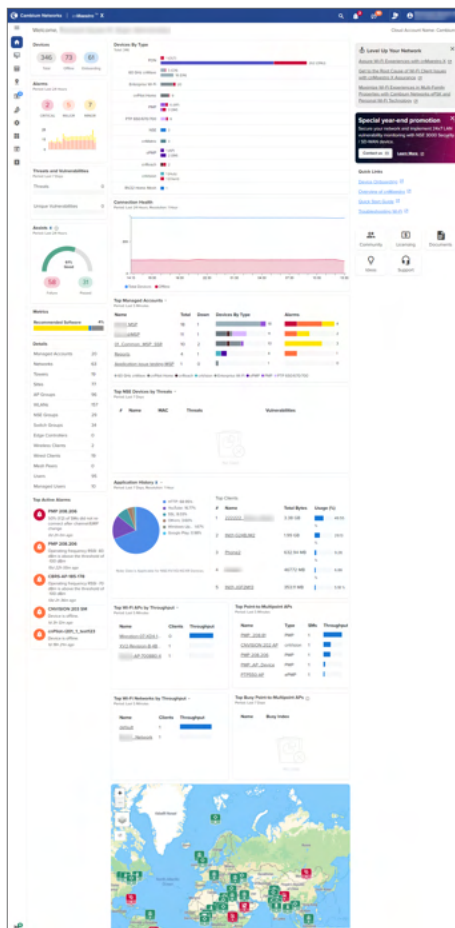
Industrial Internet View

Industrial Internet View provides a single interface for Fixed Wireless, Wi-Fi, and IIoT deployments. The device types include 60 GHz cnWave, cnMatrix, cnPilot Home (R-Series), cnRanger, cnVision, cnWave 5G Fixed, ePMP, PMP, cnReach, PTP 650/670/700, PTP 820/850, Enterprise Wi-Fi (E-Series, and XE/XV/X7-Series) and Enterprise (ePMP 1000 Hotspot), Enterprise Wi-Fi (Xirrus-Series), NSE, RV22 Home Mesh, and PON.

Home page

The **Home** page is displayed when the user logs into the cnMaestro. It provides links to the core functional areas in the UI, such as Cambium **Support Center**, **Community**, **Documents**, and **Licensing**. It can be accessed from any page in the UI by clicking the **Home** tab.

Figure 29 cnMaestro Home page



Page structure

cnMaestro follows a standard page structure, which consists of a left-side menu and a content area. In many pages, tabs provide additional content navigation.

Figure 30 cnMaestro page structure

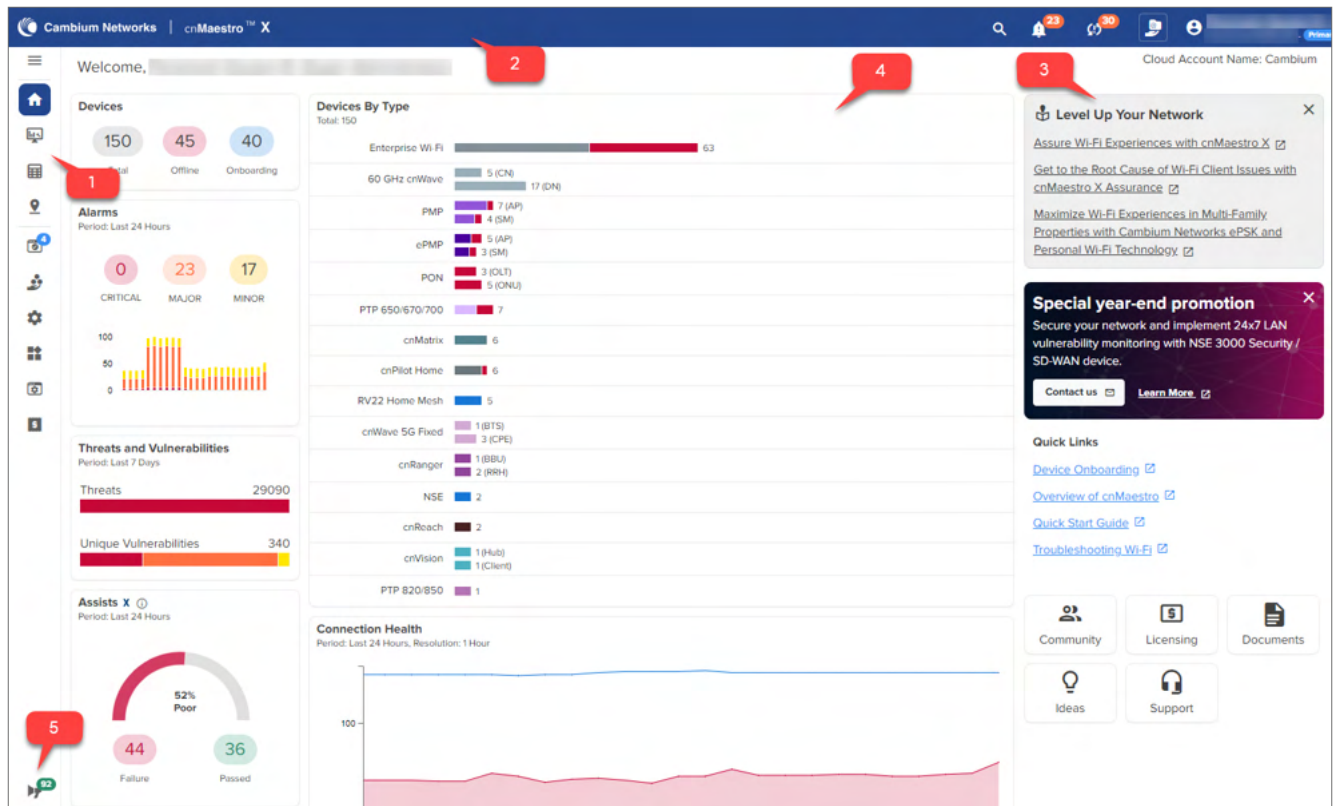
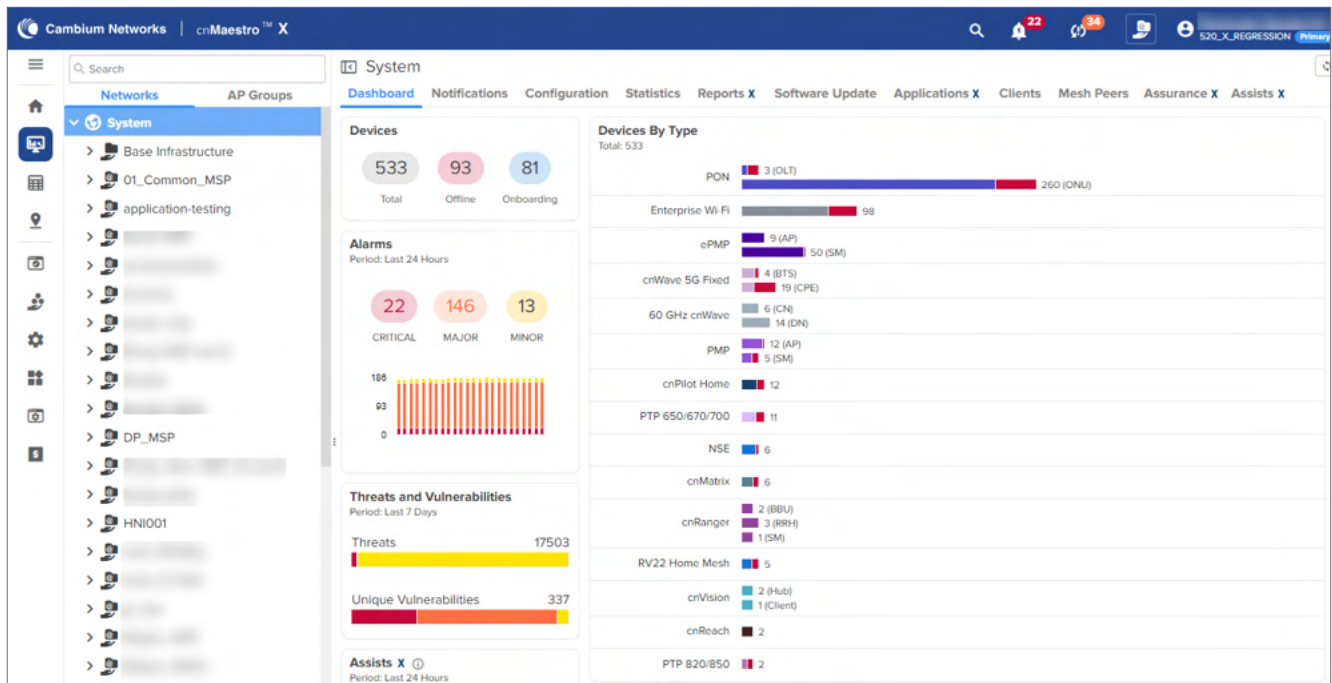


Table 9 UI description

Number	Elements	Description
1	Left menu	Shows the functional areas of the UI. This menu can be expanded or collapsed to view the submenu by clicking the top arrow.
2	Header	Shows the basic counters for Major Alarms , Devices Awaiting for Approval , Software Updates Jobs , and Out of Sync Devices .
3	Right menu	Provides links to Cambium Ideas , Support , Community , Documents , and Licensing .
4	Functional area	Shows the detailed view of the section selected in the left menu.
5	Announcements	Displays announcements about availability of newer firmware versions of devices.

Page navigation

The cnMaestro pages include items such as **Dashboard**, **Notifications**, **Configuration**, **Statistics**, **Reports X**, **Software Update**, **Applications X**, **Clients**, **Mesh Peers**, **Assurance X**, and **Assists X**. The content of a page differs depending upon its context. For example, a **Dashboard** page will be different at the **System/Network/Tower/Site/Device** levels. The context, or level in the hierarchy, is selected in the Device tree as shown in [Table 12](#).



Access and Backhaul View

Overview

The Access and Backhaul view leverages a hierarchical tree to display device installations. In this view, customers can group their fixed wireless devices into Networks, and display their Point-to-Multipoint devices in Tower-based sectors. Navigation is performed using the tree. The device tree is segmented into two tabs: Network and Wi-Fi AP Groups.

Networks tab

The **Network** tab displays a hierarchical view of the devices. It consists of Systems, Networks, Towers, Sites, and Devices. There is a strict ordering for how nodes can fit in the hierarchy, and as one navigates through and selects nodes, the pages display the node chosen.

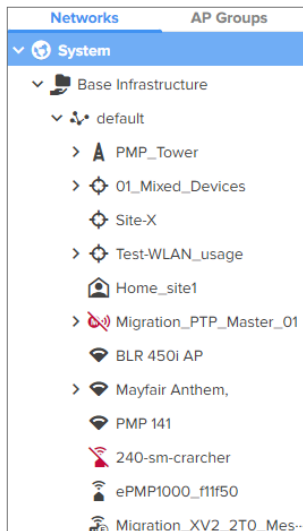
Selecting an arrow icon will expand the node and display the next level of hierarchy.



Note

- Towers are only visible in the Fixed Wireless view and 60 GHz cnWave devices are only visible in the 60 GHz cnWave E2E Network. cnMatrix devices are visible only in Access and Backhaul, and the Industrial Internet views.
- Japanese characters are supported in Network, Tower, and Site names.
- Select a node in the hierarchy tree and expand to open the node.
- Opening the node does not automatically select a node in the new hierarchy, instead you must click the desired node.
- PON devices are visible only in the PON networks.

Figure 31 *Networks*



The structured hierarchy has the following nodes:

Table 10 *Structured hierarchy nodes*

Icon	Name	Description
	60 GHz cnWave CN	CN is mapped to a Site in E2E Network.
	60 GHz cnWave DN	DN is mapped to a Site in E2E Network.
	60 GHz cnWave Onboard E2E Network	60 GHz cnWave devices are located within a Network deployed through the Onboard E2E controller.
	60 GHz cnWave External E2E Network	60 GHz cnWave devices are located within a Network deployed through the external E2E controller.
	60 GHz cnWave PoP	PoP is mapped to a Site in E2E Network and deployed through the External E2E controller.
	60 GHz cnWave PoP Onboard E2E Network	PoP is mapped to a Site in E2E Network and deployed through the Onboard E2E controller.
	60 GHz cnWave Unmanaged Node	60 GHz cnWave Unmanaged Node
	60 GHz cnWave Site	Sites are located within E2E Networks. A site maps to a single area and represents a location on a map that has 60 GHz cnWave devices.
	cnMatrix	cnMatrix devices are located within a Network . Optionally they can also be mapped standalone to a Tower or a Site .
	cnRanger RRH	cnRanger RRH access points are located in a Network and are mapped to a BBU .
	cnRanger Sierra 800	cnRanger Sierra 800 are located in a Network and are optionally mapped to a Tower .
	cnRanger SM	cnRanger SM devices are located in a Network and are optionally mapped to a RRH.

Table 10 *Structured hierarchy nodes*




















Icon	Name	Description
	cnReach	cnReach device which could have zero, one, or two radios, and support one or two roles, including Point-to-Point (PTP), Point-to-Multipoint (AP or EP) (PTMP), or IO Expander.
	cnPilot Home	Wi-Fi devices are generally matched to a local SM and inherit its Network . They can also be mapped standalone to a Network or a Site .
	cnVision Client	cnVision Client Subscriber Modules are located in a Network (if they are standalone, which is only used for bootstrapping) or they are associated with an AP. The SM will inherit the Network and Tower of the AP to which it is associated.
	cnVision Hub	cnVision Hub are located in a Network and are optionally mapped to a Tower .
	cnWave 5G Fixed BTS	cnWave 5G Fixed BTS devices are located within a Network.
	cnWave 5G Fixed CPE	cnWave 5G Fixed CPE devices connected through cnWave 5G Fixed BTS device in a Network.
	Enterprise Wi-Fi	Enterprise Wi-Fi devices are generally matched to a local SM and inherits its Network . They can also be mapped standalone to a Network or to a Site .
	ePMP AP	ePMP Access Points are located in a Network and are optionally mapped to a Tower .
	ePMP SM	ePMP Subscriber Modules are located in a Network (if they are standalone, which is only used for bootstrapping) or they are associated with an AP. The SM inherits the Network and Tower of the AP to which it is associated.
	Home Site	Home sites are located within networks and contain cnPilot Home Router (r-series) APs and Home Mesh routers.
	Network	All devices are placed within Networks . Networks represents the geographical regions or collections of devices with a shared responsibility. Accounts can have one network or many networks. Networks allow one to provide structure to accounts with many devices and also provides aggregation buckets for cnMaestro statistics (essentially the system pre-calculates statistics, so they are displayed quickly).
	NSE 3000	NSE device located in the Network .
	OLT	Optical Line Terminal (OLT) device located in the PON network
	ONU	Optical Network Unit (ONU) device located in the PON network.
	PMP AP	Point-to-Multipoint Access Points (PMP AP) are located in a Network and are optionally mapped to a Tower .
	PMP SM	Point-to-Multipoint Subscriber Modules (PMP SM) are located in a Network (if they are standalone, which is only used for bootstrapping) or they are associated with an AP. The SM will inherit the Network and Tower of the AP to which it is associated.
	PON Network	All PON devices are placed within PON networks.
	PON Site	PON sites are located within PON networks and hold OLT and ONU devices.
	PTP Master	Point-to-Point (PTP) Master device located in a network and optionally mapped to a Tower.

Table 10 *Structured hierarchy nodes*

Icon	Name	Description
	PTP Slave	Point-to-Point (PTP) Slave device located in a network and optionally mapped to a Tower.
	PTP 820/850	Point-to-Point (PTP 820/850) device located in a network.
	RV22 Home Mesh Router—Base	RV22 Home Mesh routers (deployed as a standalone or the base in a mesh setup) located in the network and are mapped to a home site.
	RV22 Home Mesh Router—Node	RV22 Home Mesh routers (deployed as the node in a mesh setup) located in the network and are mapped to a home site.
	Enterprise Site	Enterprise Sites are located within networks and hold Wireless Access Points. A site maps to a single area and represents a location on a map that has APs or a building.
	System	The System node is at the top level of the hierarchy, though it does not have an explicit node in the tree. It's pages are displayed when the user logs in for the first time, when one selects the System button in the hierarchical tree (displayed when Networks are shown) or selects the System node in the breadcrumbs. The System level aggregates data from all devices within the account.
	Tower	Towers are located within networks and hold cnRanger, cnReach, PTP, or Point-to-Multipoint APs. All the devices on a Tower are mapped to the same Network, and all their children devices such as Subscriber Modules or Home APs are also mapped to the same network.
	GPON port	GPON port of the PON OLT device. PON ONU devices are connected.
	XGSPON port	XGSPON port of the PON OLT device. PON ONU devices are connected.

Default network

cnMaestro has a default network into which unmapped devices will be placed. These can remain in the default network or moved to a named network. The default network cannot be deleted.

Tree menu

Each node in the device tree has a menu icon (≡) that supports node-specific actions.

For example, the system node lets you to **Add Network** or launch the **Update Software** page, while individual devices allow you to **Edit** their cnMaestro settings, **Reboot**, or even **Delete** the device from management (so it can be transferred to another account). The actions supported across the tree include the following:

Table 11 *Tree menu*

Action	Node	Description
Actions common to All Devices		
Add Network	System	Add a new Network as a child to the System node.
Add Site	Network	Add a new Site as a child to the Network node.
Add Tower	Network	Add a new Tower as a child to the Network node.
Claim Devices	Site	Claim devices in an Enterprise site.
Delete	Most Nodes	Delete a node from the tree. This is available for all nodes except System and the default network. Deleted devices will be removed entirely from the management

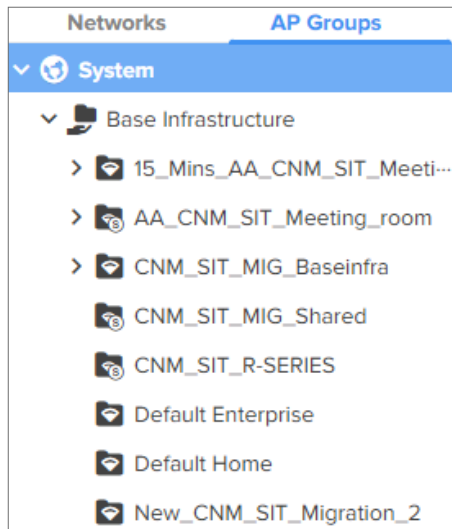
Table 11 *Tree menu*

Action	Node	Description
		system (along with their historical statistics). In order to delete a container, such as Network or Site, all nodes inside the container must be deleted first.
Edit	Most Nodes	Edit the cnMaestro settings, including node name and location. This is available for all nodes except System. For 60 GHz cnWave, edit option applies for E2E Network and nodes. Node name can be edited.
Flash LEDs	Enterprise Wi-Fi	The LEDs of the device enables to identify and locate the device.
Reboot	Devices	Reboot the device.
Refresh	All	Refresh the node in the tree. This refreshes the node and its children only, not the entire tree.
Update Software	All	Update device software.
Actions specific to 60 GHz cnWave Network		
Add Link	Network and Most Nodes	Add a new link to the System.
Add Node	Site	Add a new Node as a child to the Site.
Add Site	Network	Add a new Site to the E2E Network.
Refresh	Network	Refresh the network details
Download PoP(s) Onboarding Config	Network and PoP Nodes	Download PoP(s) Onboarding Configuration data.
Edit	Network	Edit name of the network
Hide or Show Sites	Network	Allows to hide or show sites in the E2E Controller Network tree menu.
Sync Topology	Network	To sync the Topology of E2E Network and cnWave 60GHz device.
Update Software	Network and Nodes	Allows the user to update the 60 GHz cnWave nodes software.
PON Network		
Sync Topology	Network	To sync the topology of PON devices (OLT/ONU).

Wi-Fi AP Groups tab

The **Wi-Fi AP Groups** tab displays the Wi-Fi AP Groups configured in cnMaestro (and the devices mapped to them). AP Groups allow you to share configuration across many access points. They also display the aggregated statistics for the devices managed and present them within the AP Groups dashboard.

Figure 32 *Wi-Fi AP Group tab*



Map navigation

Maps are presented in Main menu with dedicated Map display. Maps often show Towers and Devices located in proximity. You can double-click the map nodes to navigate to the Device, Site, or Tower. By selecting a node in the map, the Device tree gets updated to reflect that node.



Note

- Map view is supported for devices 60 GHz cnWave, cnRanger, cnPilot Home, cnMatrix, cnVision, ePMP, Enterprises Wi-Fi Series, PMP, PTP, and RV22 Home Mesh at the site- and device-levels.

Figure 33 Map navigation

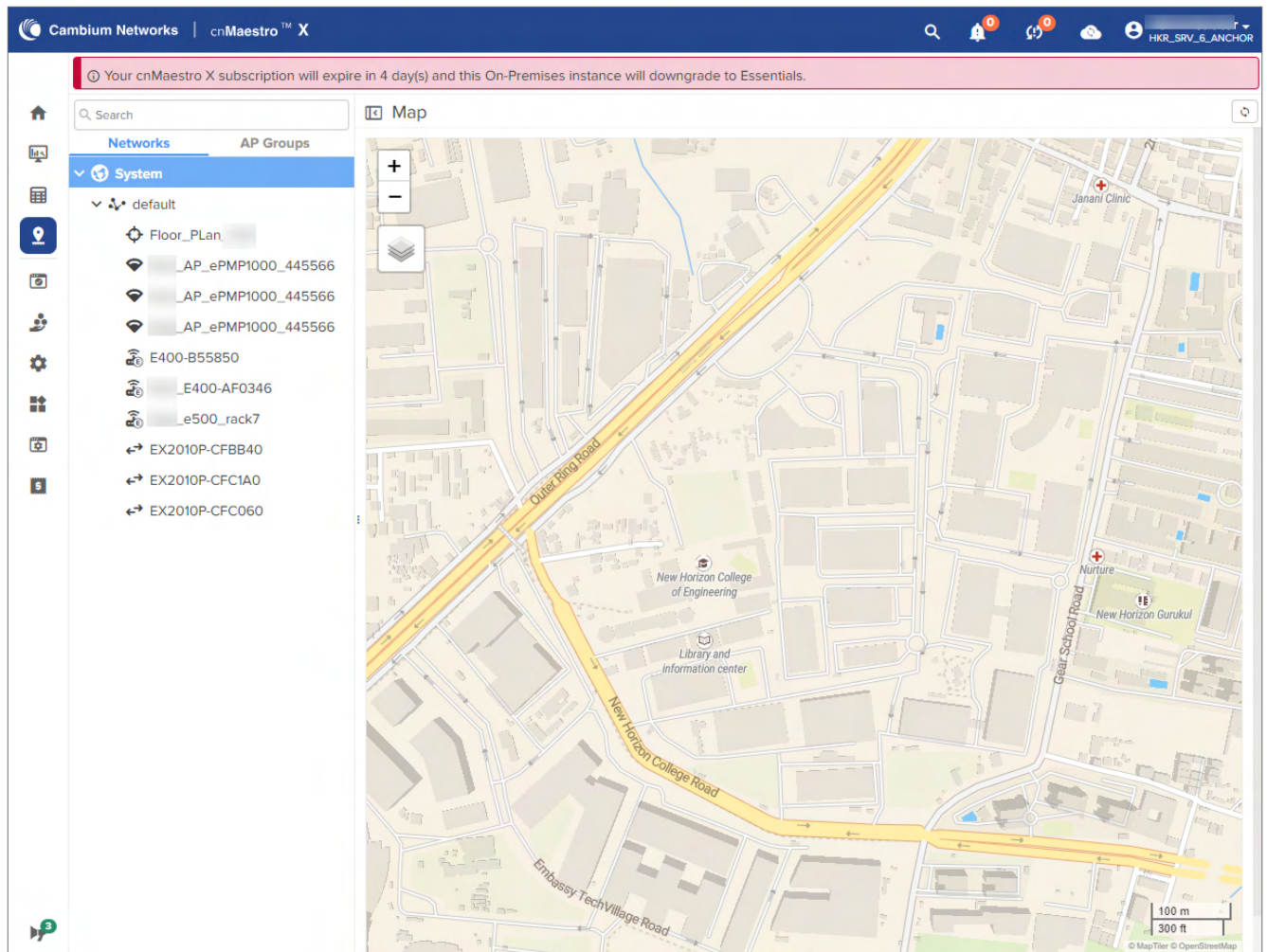


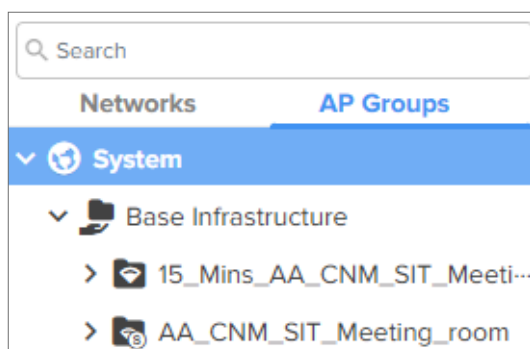
Table navigation

Some tables display **Networks**, **Towers**, **Site**, or **Devices** and allow the user to click the node and navigate to the location of the node in the tree.

Node search

Administrators can search for nodes within the device tree using the **Search** box. It allows the user to search based upon Device Name and MAC Address. Once the node is found and selected, one can navigate to it in the hierarchical tree.

Figure 34 Node search



Enterprise Account view

Overview

The Enterprise account differs from Access and Backhaul in that it is largely table-driven. It does not have the Quick Buttons or the Device Tree, instead, it has direct navigation for Devices, AP Groups, WLANs, Switch Groups, and Sites. Each of these is presented in tabular form.

System

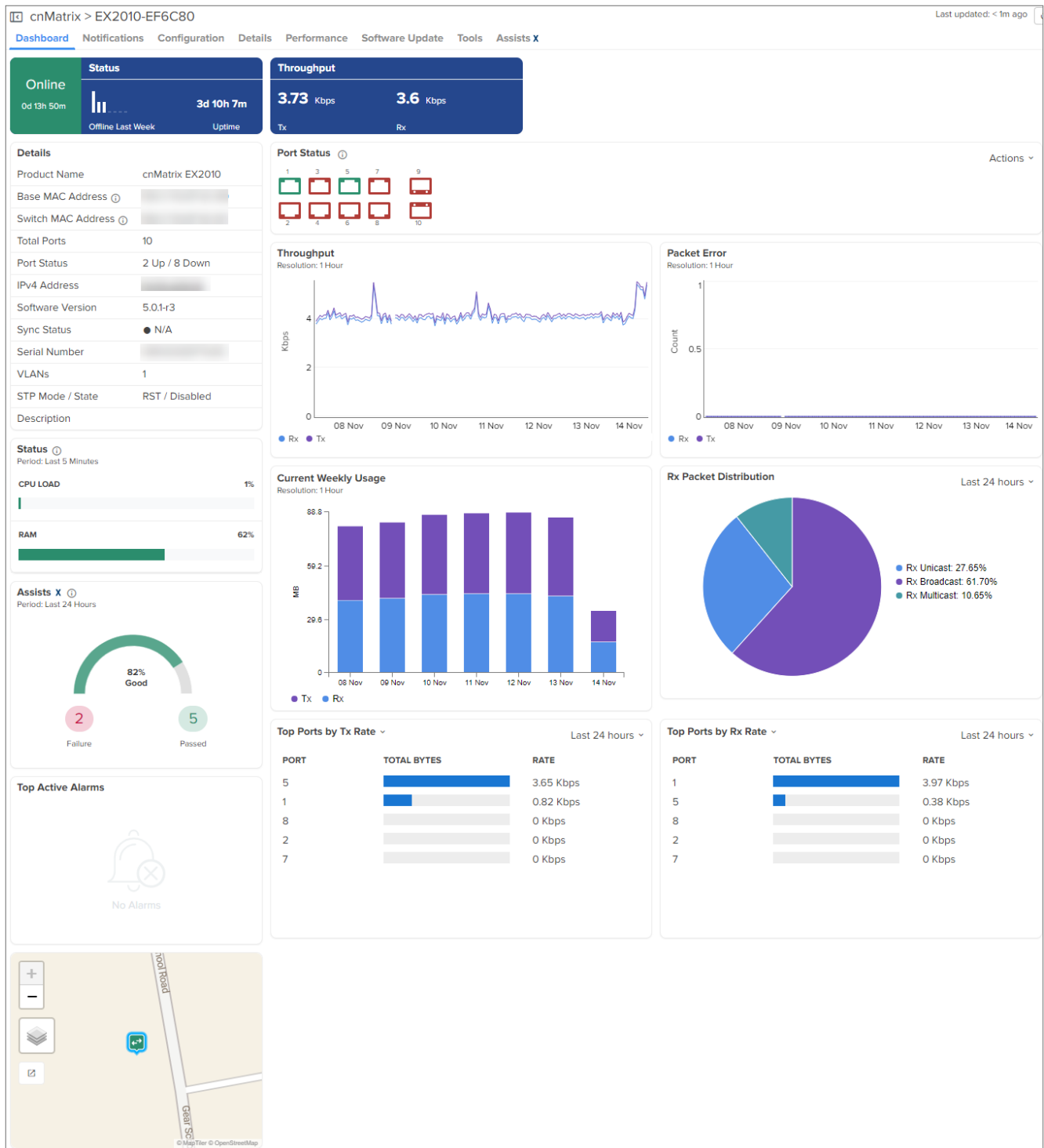
Global functionality is presented in the System menu. It aggregates data across the entire installation.

Devices

The Devices section provides a searchable table listing all the devices in the system.

Device	MAC Address	Managed Account	Type	IPv4 Add...	IPv6 Add...	Status	Serial Number	Description	Onboard Duration	Active S/W Version
<input type="checkbox"/> F425_200dc5		Base Infrastructure	ePMP Force 425 SM		-	Offline (0d 12h 15m)			0d 12h 28m	5.4.1-RC15
<input type="checkbox"/> F400_200d16		Base Infrastructure	ePMP Force 400C AP		-	Offline (0d 12h 15m)			0d 12h 31m	5.4.2
<input type="checkbox"/> XV2-22H-E0477		Base Infrastructure	XV2-22H		-	Offline (0d 12h 14m)			1d 7h 51m	6.6.0.2-b1
<input type="checkbox"/> XV2-22H-E53BE4		Base Infrastructure	XV2-22H		-	Offline (0d 12h 15m)			1d 14h 31m	6.6.0.1-r5
<input type="checkbox"/> XV2-2T0-3002D2		Base Infrastructure	XV2-2T0		-	Offline (0d 12h 15m)			1d 16h 59m	6.6.0.1-r5
<input type="checkbox"/> XV2-2-5342E5		Base Infrastructure	XV2-2		-	Offline (0d 12h 15m)			1d 17h 4m	6.6.0.1-r5
<input type="checkbox"/> XV2-23T-E5F987		Base Infrastructure	XV2-23T		-	Offline (0d 12h 15m)			2d 13h 32m	6.6.0.2-b1
<input type="checkbox"/> XV3-8-4EEEF0		Base Infrastructure	XV3-8		-	Offline (0d 12h 15m)			2d 13h 41m	6.6.0.1-r5

Selecting a device launches its management page.



AP Groups

AP Groups manage shared configuration across APs. AP Groups also aggregate data for all the APs that map to them. This includes consolidating statistics and events/alarms and presenting AP Group centered pages for Dashboard, Notifications, Configuration, Statistics, Report, Software Update, Clients, and Mesh Peers.

Figure 35 AP Groups

Configuration > Wi-Fi Profiles

AP Groups | WLANs | Association ACL | Access Control Policies | Custom Applications X

Change Filter(s) Clear Scope: All Accounts Add New Import Sync

Name	Type	AP Status	Scope	WLANs	Auto Sync	Last Updated	Last Updated By	Origin	
test	Enterprise Wi-Fi	0 of 1 offline	Base Infrastructure		OFF	25 Nov 2024, 01:35 AM		Custom	
ASK4_D_Clone	Enterprise Wi-Fi	0 of 1 offline	Shared		OFF	24 Nov 2024, 12:31 AM		Custom	
cm_test_group	Enterprise Wi-Fi	0 of 2 offline	Base Infrastructure		ON	22 Nov 2024, 05:02 PM		Custom	
jp-xe34	Enterprise Wi-Fi	1 of 1 offline	Shared	jp-xe34	OFF	22 Nov 2024, 03:39 PM		Custom	
diva_RCA_9th_floor	Enterprise Wi-Fi	2 of 5 offline		diva_sae_owe_rca_diva_wpa	ON	22 Nov 2024, 03:21 PM		Custom	
JP-662-Reg	Enterprise Wi-Fi	0 of 1 offline	Shared	JP-W7-11 JP-W7-12	OFF	22 Nov 2024, 12:48 PM		Custom	
Whats New 520 AP Group	Enterprise Wi-Fi	0 of 3 offline	Whats New Network	Whats New Network SSID_Wi	ON	22 Nov 2024, 03:30 AM		Custom	
cm_test	Enterprise Wi-Fi	0 of 12 offline	Base Infrastructure		ON	21 Nov 2024, 11:32 PM		Custom	
AutoRF	Enterprise Wi-Fi	0 of 7 offline	Shared		ON	21 Nov 2024, 04:24 PM		Custom	
diva_RCA_baseament	Enterprise Wi-Fi	4 of 4 offline		diva_wpa3_new_diva_rca	ON	19 Nov 2024, 03:27 PM		Custom	

Showing 1 - 10 Total: 188 10 < Previous 1 2 3 4 5 ... 19 Next >

WLANs

WLANs manage shared configuration across APs.



Note

You can connect to or share a WLAN network using the QR code for the WLAN. Click the View QR Code (📄) icon.

Figure 36 WLANs

Configuration > Wi-Fi Profiles

AP Groups | WLANs | Association ACL | Access Control Policies | Custom Applications X

Change Filter(s) Clear Device Type: All Scope: All Accounts Add New Import Sync

Name	Scope	Type	AP Status	AP Group	Guest Access	Last Updated	Last Updated By	Origin	
sit_enterprise_clone	Base Infrastructure	Enterprise Wi-Fi	0 of 1 offline	Nira_test	N/A	25 Nov 2024, 01:30 AM		Custom	
ASK4_Ocen_clone	Shared	Enterprise Wi-Fi	0 of 1 offline	ASK4_D_Clone	N/A	24 Nov 2024, 12:05 AM		Custom	
JP-W7-12	Shared	Enterprise Wi-Fi	0 of 1 offline	JP-662-Reg	N/A	22 Nov 2024, 05:57 PM		Custom	
diva_wpa2_ent_rca	Divakar	Enterprise Wi-Fi	2 of 5 offline	diva_RCA_9th_floor	N/A	22 Nov 2024, 02:55 PM		Custom	
jp-xe34	Shared	Enterprise Wi-Fi	1 of 1 offline	jp-xe34	N/A	22 Nov 2024, 02:42 PM		Custom	
511-Cloud-Regression-MSP	Megha_MSP	Enterprise Wi-Fi	0 of 1 offline	511-Cloud-Reg-MSP-Gro	cnMaestro (Self-Reg-MSP)	22 Nov 2024, 12:29 PM		Custom	
Whats New Resident Network	Whats New Network	Enterprise Wi-Fi	0 of 3 offline	Whats New 520 AP Group	N/A	22 Nov 2024, 03:36 AM		Custom	
Whats New Resident Network	Whats New Network	Enterprise Wi-Fi	0 of 3 offline	Whats New 520 AP Group	N/A	22 Nov 2024, 03:36 AM		Custom	
Whats New Resident Network	Whats New Network	Enterprise Wi-Fi	0 of 3 offline	Whats New 520 AP Group	N/A	22 Nov 2024, 03:36 AM		Custom	
Whats New Resident Network	Whats New Network	Enterprise Wi-Fi	0 of 3 offline	Whats New 520 AP Group	N/A	22 Nov 2024, 03:27 AM		Custom	

Showing 1 - 10 Total: 374 10 < Previous 1 2 3 4 5 ... 38 Next >

Switch Groups

Switch Groups provide shared configuration for cnMatrix devices, and a subset of parameters can be overridden for each device. Administrators can simultaneously edit individual/bulk ports across all physical switches mapped to a Switch Group.

Figure 37 Switch Groups

Configuration > Switch Groups

[Learn more](#) about Switch Groups.

Q Search Scope: All Accounts

Name	Offline Switches	Scope	Ports Up	VLANs	Active PoE Ports	Auto Sync	Last Updated	Last Updated By	Origin	
30thApr24	0 of 1 Offline	Shared	1 of 28	1,5-4000	0	ON	Apr 30 2024 16...		Custom	<input type="button" value="Share"/> <input type="button" value="Copy"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
DE	0 of 1 Offline	Base Infrastructure	1 of 10	1	0	ON	Apr 30 2024 10...		Custom	<input type="button" value="Share"/> <input type="button" value="Copy"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
Do-not-Use	0 of 0 Offline	Shared	0 of 0	1,5-10	0	ON	Apr 24 2024 14...		Custom	<input type="button" value="Share"/> <input type="button" value="Copy"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
22ndApr24	0 of 0 Offline	Shared	0 of 0	1,5-10	0	ON	Apr 22 2024 14...		Custom	<input type="button" value="Share"/> <input type="button" value="Copy"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

Showing 1 - 4 Total: 4 10 < Previous 1 Next >

NSE Groups

NSE 3000s are configured by creating configuration profiles called NSE Groups.

Figure 38 NSE Groups

Configuration > NSE Groups

Change Filter(s) Managed Account: All Accounts

Name	Device Status	Managed Account	Auto Sync	Last Updated	Last Updated By	Origin	
NSE-700880-163-NSE_Group-202404221755...	0 of 1 offline	Shared	ON	02 May 2024, 03:24 PM		Custom	<input type="button" value="Share"/> <input type="button" value="Copy"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
NSE_Group_1_Wrong_DNS	0 of 0 offline	Base Infrastructure	ON	30 Apr 2024, 04:48 PM		Custom	<input type="button" value="Share"/> <input type="button" value="Copy"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
NSE_Group_1_161_clone	0 of 0 offline	Base Infrastructure	ON	24 Apr 2024, 10:30 AM		Custom	<input type="button" value="Share"/> <input type="button" value="Copy"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
M	0 of 0 offline	_MSP	ON	23 Apr 2024, 04:58 PM		Custom	<input type="button" value="Share"/> <input type="button" value="Copy"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
NSE_MSP	0 of 0 offline	_MSP	ON	23 Apr 2024, 03:49 PM		Custom	<input type="button" value="Share"/> <input type="button" value="Copy"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
_MSP_New	0 of 0 offline	_MSP	ON	23 Apr 2024, 03:44 PM		Custom	<input type="button" value="Share"/> <input type="button" value="Copy"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
Test	0 of 0 offline	_MSP	ON	23 Apr 2024, 03:22 PM		Custom	<input type="button" value="Share"/> <input type="button" value="Copy"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
_NSE-NSE_Group-20240423145739	0 of 0 offline	_MSP	ON	23 Apr 2024, 03:06 PM		Custom	<input type="button" value="Share"/> <input type="button" value="Copy"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
_NSE_clone	0 of 0 offline	Shared	ON	23 Apr 2024, 03:00 PM		Custom	<input type="button" value="Share"/> <input type="button" value="Copy"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
_NSE	0 of 0 offline	Shared	ON	23 Apr 2024, 12:08 PM		Custom	<input type="button" value="Share"/> <input type="button" value="Copy"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

Showing 1 - 10 Total: 12 10 < Previous 1 2 Next >

Sites

Sites are similar to AP Groups in that they aggregate statistics from many APs. The difference is a Site represents APs installed at a single physical location (and mapped to a Floor Plan). Sites also have their own Dashboard and aggregation pages.

Side menu


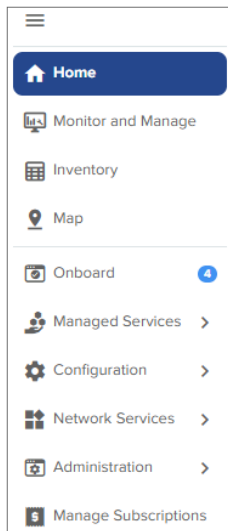
The side menu provides high-level navigation through the cnMaestro UI. Click the menu () icon in the left column to view the side menu names in the page.

Figure 39 *Side menu*



Section tabs

All management sections are displayed in the context of the managed item, including System, AP, AP Group, Switch Groups, and Site. The options vary depending upon the menu selected. A breakdown is below:

Table 12 *Section tabs*

Page	Tabs
System	Dashboard Notifications Configuration Statistics Report Software Update Applications Clients Mesh Peers Assurance Assists
Enterprise Sites	Dashboard Notifications Configuration Statistics Reports Floor Plan Devices Applications Clients Mesh Peers WIDS/WIPS Assurance Assists WLANs
Home Sites	Dashboard Notifications Configuration Reports Software Update Clients Assists
PON Sites	Dashboard Notifications Configuration OLTs ONUs Ports

System status

The UI header has the following System status icons.

Table 13 *System status icons*

Icon	Name	Description
	Announcements	Notifies the latest Device Software images, Package, or OVA to upload from Cloud.
	Major Alarms	The count of major alarms raised in the system.
	Out-of-Sync Devices	The number of Wi-Fi devices with unsynchronized configuration (which can occur when automatic synchronization is disabled in the AP Group or the configuration is changed directly on the device).

Clicking an icon navigates to the relevant management page.

Data Tables and Chart UI Controls

Familiarize with UI controls required for working with the data tables and chart UI pages. An example of the data tables is displayed below:

Configuration > Wi-Fi Profiles

AP Groups | WLANs | Association ACL | Access Control Policies | Custom Applications X

Change Filter(s) Clear Scope: All Accounts Add New Import Sync

Name	Type	AP Status	Scope	WLANs	Auto Sync	Last Updated	Last Updated By	Origin	
test	Enterprise Wi-Fi	0 of 1 offline	Base Infrastructure		OFF	25 Nov 2024, 01:35 AM		Custom	
ASK4_D_Clone	Enterprise Wi-Fi	0 of 1 offline	Shared		OFF	24 Nov 2024, 12:31 AM		Custom	
cm_test_Grow	Enterprise Wi-Fi	0 of 2 offline	Base Infrastructure		ON	22 Nov 2024, 05:02 PM		Custom	
jp-xe34	Enterprise Wi-Fi	1 of 1 offline	Shared	jp-xe34	OFF	22 Nov 2024, 03:39 PM		Custom	
diya_RCA_9th_floor	Enterprise Wi-Fi	2 of 5 offline		diya_sae_owe_rca_diya_wpa	ON	22 Nov 2024, 03:21 PM		Custom	
JP-662-Reg	Enterprise Wi-Fi	0 of 1 offline	Shared	JP-W7-11_JP-W7-12	OFF	22 Nov 2024, 12:48 PM		Custom	
Whats New 520 AP Group	Enterprise Wi-Fi	0 of 3 offline	Whats New Network	Whats New Network SSID_Wi	ON	22 Nov 2024, 03:30 AM		Custom	
cm_test	Enterprise Wi-Fi	0 of 12 offline	Base Infrastructure		ON	21 Nov 2024, 11:32 PM		Custom	
AutoRF	Enterprise Wi-Fi	0 of 7 offline	Shared		ON	21 Nov 2024, 04:24 PM		Custom	
diya_RCA_basement	Enterprise Wi-Fi	4 of 4 offline		diya_wpa3_new_diya_ga_rc	ON	19 Nov 2024, 03:27 PM		Custom	

Showing 1 - 10 Total: 188 10 < Previous 1 2 3 4 5 ... 19 Next >

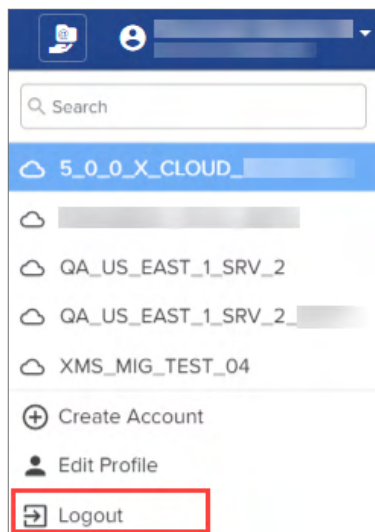


Note

Mouse Rollover Behavior—In the data tables, when some of the columns on the right side are hidden, if you move the mouse pointer over the row, the action icons on the right most side are displayed without having to move the scroll bar to the right.

Logout

Log out of cnMaestro by clicking on the user icon in the upper-right corner and selecting **Logout**. You can also navigate to: **Administration > Users > Session Management > Sessions**.



Device Onboarding

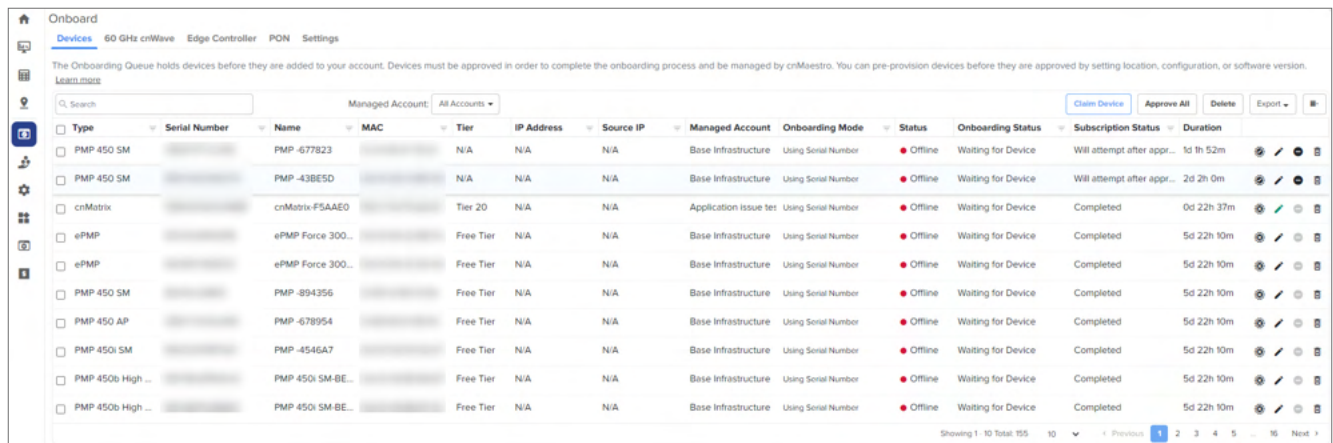
Onboarding is the process of adding a device into cnMaestro Cloud management.

This section includes the following:

- [Onboarding Overview](#)
- [Claiming Devices](#)
- [Onboarding Queue](#)
- [Zero Touch Configuration](#)
- [Claiming Your First Wi-Fi AP \(Cloud\)](#)
- [Claiming multiple Wi-Fi APs from the AP Group](#)
- [Claiming multiple Enterprise devices from the Enterprise Site dashboard](#)
- [Claiming multiple Enterprise devices using CSV import](#)
- [Miscellaneous Onboarding Issues](#)

Onboarding Overview

The Onboarding flow includes claiming the device (which maps it to the correct management account) and optionally pre-provisioning the device by selecting its software image and configuration. It also supports setting Device Name, Location, Software Version, and Configuration. When the onboarding process completes, the device will be under full cloud management.



The screenshot shows the 'Onboard' section of the interface. At the top, there are tabs for 'Devices', '60 GHz cnWave', 'Edge Controller', 'PON', and 'Settings'. Below the tabs, a message states: '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](#)'.

Below the message is a search bar and a 'Managed Account' dropdown set to 'All Accounts'. To the right are buttons for 'Claim Device', 'Approve All', 'Delete', and 'Export'. Below these is a table with the following columns: Type, Serial Number, Name, MAC, Tier, IP Address, Source IP, Managed Account, Onboarding Mode, Status, Onboarding Status, Subscription Status, and Duration.

Type	Serial Number	Name	MAC	Tier	IP Address	Source IP	Managed Account	Onboarding Mode	Status	Onboarding Status	Subscription Status	Duration
PMP 450 SM		PMP-677823		N/A	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	Will attempt after appr...	1d 1h 52m
PMP 450 SM		PMP-438E5D		N/A	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	Will attempt after appr...	2d 2h 0m
cnMatrix		cnMatrix-F5AAE0		Tier 20	N/A	N/A	Application Issue test	Using Serial Number	Offline	Waiting for Device	Completed	6d 22h 37m
ePMP		ePMP Force 300...		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	Completed	5d 22h 10m
ePMP		ePMP Force 300...		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	Completed	5d 22h 10m
PMP 450 SM		PMP-894356		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	Completed	5d 22h 10m
PMP 450 AP		PMP-678954		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	Completed	5d 22h 10m
PMP 450i SM		PMP-4546A7		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	Completed	5d 22h 10m
PMP 450b High ...		PMP 450i SM-BE...		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	Completed	5d 22h 10m
PMP 450b High ...		PMP 450i SM-BE...		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	Completed	5d 22h 10m

At the bottom right of the table, it says 'Showing 1 - 10 Total 155'. There are navigation buttons for 'Previous', '1', '2', '3', '4', '5', 'Next'.

Claiming Devices

A device is claimed when it is explicitly added to Cloud management using the Serial Number or Cambium ID. The difference between the two is the Serial Number is entered through the Cloud management UI and Cambium ID is entered via the Device UI or through SNMP.



Note

- Only serial numbers with a length of 12 characters can be claimed through the Cloud management UI.
- Devices with serial numbers less than 12 characters for example, 10 or 11 characters, need to be claimed on the device UI using the Cambium ID.

All claimed devices are placed in the onboarding queue. The devices need to be approved in order to become fully managed.

Claiming Devices with Serial Number

Claiming with Serial Number means entering the serial numbers of devices, one per line, and clicking the **Claim Devices** button. The system prompts the user to validate the devices before applying them. When complete, they will be placed into the onboarding queue, where they can be pre-provisioned to update software or configuration before onboarding.

Figure 40 Claiming Devices with Serial Number

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

Enter / Place a cursor in the box and use a barcode scanner to quickly claim devices.

Clear Claim Devices

To claim a device using the Serial Number:

1. Navigate to **Onboard** page > click **Claim Device**.

Onboard													
Devices 60 GHz cnWave Edge Controller PON 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													
Search Managed Account: All Accounts Claim Device Approve All Delete Export													
<input type="checkbox"/>	Type	Serial Number	Name	MAC	Tier	IP Address	Source IP	Managed Account	Onboarding Mode	Status	Onboarding Status	Subscription Status	Duration
<input type="checkbox"/>	PMP 450 SM		PMP-677823		N/A	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	Will attempt after appr...	1d 1h 52m
<input type="checkbox"/>	PMP 450 SM		PMP-438E5D		N/A	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	Will attempt after appr...	2d 2h 0m
<input type="checkbox"/>	cnMatrix		cnMatrix-F5AAE0		Tier 20	N/A	N/A	Application issue tes	Using Serial Number	Offline	Waiting for Device	Completed	0d 22h 37m
<input type="checkbox"/>	ePMP		ePMP Force 300...		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	Completed	5d 22h 10m
<input type="checkbox"/>	ePMP		ePMP Force 300...		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	Completed	5d 22h 10m
<input type="checkbox"/>	PMP 450 SM		PMP-894356		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	Completed	5d 22h 10m
<input type="checkbox"/>	PMP 450 AP		PMP-678954		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	Completed	5d 22h 10m
<input type="checkbox"/>	PMP 450i SM		PMP-4546A7		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	Completed	5d 22h 10m
<input type="checkbox"/>	PMP 450b High ...		PMP 450i SM-BE...		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	Completed	5d 22h 10m
<input type="checkbox"/>	PMP 450b High ...		PMP 450i SM-BE...		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	Completed	5d 22h 10m
Showing 1 - 10 Total: 55 10 Previous 1 2 3 4 5 ... 16 Next													

Claim Devices with Serial Number window appears.



Note

The user must manually select a PON network before approving the device.

2. Enter the serial number of the device.
3. Click **Claim Devices**.



Note

Slot availability is available only for cnMaestro X account users.

4. The device appears on the onboarding page.

While in the onboarding queue, the devices can be pre-provisioned with the following settings:

Figure 41 *Onboarding Queue Edit Device Configuration - Basic Details*

- **Details**—Displays basic details of the device, such as Serial Number, MAC address, device name and description.

You can edit only the device name and description parameters.

- **Location**—Displays details, such as network, tower/site to which you want to assign the device, and the location information.

You can edit all parameters in this tab.

- **Update**—Update the software version on the device in this tab.
- **Configure**—Decides the configuration type that must be used for configuring the device.

5. Click **Approve**.

If slots are available, then cnMaestro approves the devices and automatically onboards the devices. However, if there are no slots available, then a corresponding error message is displayed in the **Subscription Status** column.

New devices periodically query cnMaestro Cloud to see if they have been claimed (it generally takes between 1 to 15 minutes to show up in an account, depending upon when the device was last rebooted). Once a device has been added to a Cloud management account, it will be visible in the Onboarding Queue.



Note

Devices must be able to access <https://cloud.cambiumnetworks.com> to be claimed and onboarded. HTTPS proxies are currently not supported. If your device is not showing up in the Cloud management UI, you should verify network connectivity and reboot the device to prompt more frequent connection attempts.

• Not Enough Slots available in PTP 820/850 devices

User receive the license failure message in PTP 820/850 device dashboard, when no slots are available.

Network Services > Edge Controller > Centos-09

Dashboard Configuration Tools Monitoring

Online	Status	Managed Devices	Unmanaged Devices
38m ago	15d 2h 23m ago Uptime	1 Total	0 Total

Details

Host Name	centos09
Virtualization	oracle
Distribution	CentOS Stream 9
Architecture	x86-64
Number of CPUs	1
CPU Model	Intel(R) Core(TM) i3-8145U CPU @ 2.10GHz
Memory	5.54 GB
Timezone	Asia/Kolkata
Date & Time	21 Nov 2023, 07:23 PM
System Clock Sync	Enabled (chrony)
Topology Sync	Success (2m ago)
Version	1.0.0-r4

Disks

Disk 1	/dev/sda (12.6GB)
--------	-------------------

Network

Interface 1	
Status	Online
Name	enp0s3
IPv4 Address	10.110.221.8/24
IPv4 Gateway	10.110.221.254
IPv6 Address	
IPv6 Gateway	
MTU	1500

Licence Failures

MAC	IP Address	Reason
	10.120.109.204	Serial Number is claimed into another
	10.120.109.106	There are no slots available.
	10.120.109.107	There are no slots available.
	10.120.109.101	There are no slots available.

Approving Devices

Devices in the Onboarding Queue must be approved before they are updated and added to the Cloud Management. Click the approval button in the device to onboard. Unapproved devices will remain in the Onboarding Queue indefinitely.



Note

- Once approved, connected devices are onboarded and added to the account immediately, and all configuration or software updates are applied. Approved devices will be onboarded as soon as they connect.
- To pre-provision devices, you should make all your changes before approving them. After devices have been onboarded, additional configuration or software updates must be done through the standard management user interface.

Devices that have completed onboarding remain in the Onboarding Queue for one week.

Claiming Devices with Cambium ID

The Cambium ID is defined when the Cloud management is created. You can view it on the **Home** page; it uniquely identifies the account.

To claim a device with Cambium ID, you need to have access to the device. Cambium ID claiming is required for devices that do not have a 12-character Serial Number, and it is optional for devices with a 12-character Serial Number. There are two ways to claim a device with Cambium ID.

Table 14 *Types of Claiming Devices with Cambium ID*

Type	Description
Device UI	Enter the Cambium ID/Onboarding Key directly into the device UI. This prompts the device to access Cambium Cloud and be placed in the onboarding queue.
Device SNMP	The Cambium ID/Onboarding Key can also be entered into the device over SNMP. This allows one to quickly onboard existing devices using an SNMP manager. The correct OID will be dependent upon the device type. The string entered into the OID should be of the format “<Cambium ID>:<Onboarding Key>”.

The directions for each specific device type are presented later in this chapter. Once devices are added to the Onboarding Queue using Cambium ID, the administrator must approve them prior to them being onboarded.

Cambium ID Configuration

You must configure the Cloud Manager to support Cambium ID onboarding. Once enabled, Cambium ID onboarding will work for all device types.

Figure 42 *Cambium ID Configuration*

Onboard

Devices 60 GHz cnWave Edge Controller PON **Settings**

You can add devices to your account by logging into the Device UI directly and entering the Cambium ID and Onboarding Key (these were set when you created your Company Account, and they can be modified below). ePMP 1000, PMP 430/450 and ePMP 1000 Hotspot must be claimed using this method. ⓘ

Cambium ID: 5_0_0_X_CLOUD_REGRESSION

☒ Allow device to be claimed using Cambium ID

Enabling this feature allows a device to be claimed by entering the Cambium ID and Onboarding Key on the device. This information can be set on the device via its user interface (or SNMP or CLI on some devices). Each user can have their own Onboarding Key. [Learn more](#)

The following users can claim devices using the cnMaestro Cambium ID and the user's Onboarding Key.

User: [redacted]	Onboarding Key: [redacted]	[edit]	Delete
User: [redacted]	Onboarding Key: [redacted]	[edit]	Delete
User: [redacted]	Onboarding Key: [redacted]	[edit]	Delete
User: [redacted]	Onboarding Key: [redacted]	[edit]	Delete
User: [redacted]	Onboarding Key: [redacted]	[edit]	Delete
User: [redacted]	Onboarding Key: [redacted]	[edit]	Delete

Save Cancel Add New

Cambium ID Onboarding Key

An Onboarding Key must be associated with a Cambium ID before onboarding. This provides security and tracking benefits for onboarded devices. The Onboarding Key can be configured at **Onboard > Settings**.

Each onboarding key is mapped to an account administrator. This allows Cambium Cloud to know who is onboarding a device. Onboarding Keys can also be revoked if needed.

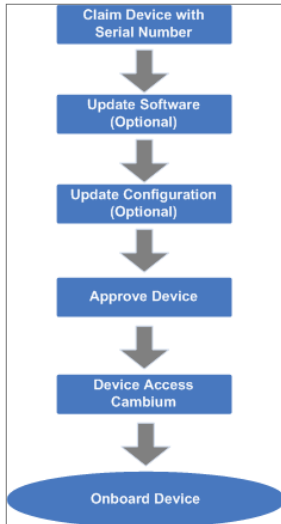
Onboarding Queue

The Onboarding Queue holds a list of pending and recent (last 24 hours) device onboards. It allows the administrator to pre-provision device software and configuration, as well as signal a device is ready to be onboarded. The process flows for how the Onboarding Queue is used are slightly different based upon how the device was claimed.

Serial Number flow

When onboarding with Serial Number, the device can be fully provisioned before it contacts Cambium Cloud and is placed in the Cloud Management. This allows it to be added immediately upon connection.

Figure 43 *Serial Number flow*



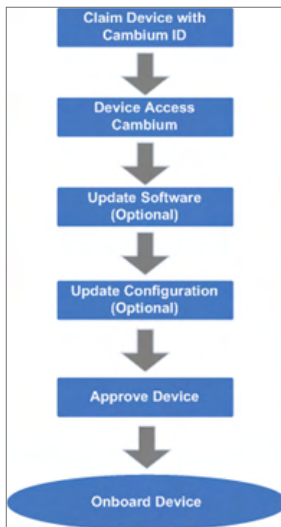
Note

When a user onboards using a Serial Number, the software update and configuration can be defined even before the device physically accesses the account.

Cambium ID flow

The flow is a little different when using Cambium ID. Here devices must connect to Cambium Cloud before they are added to Cloud Management. The administrator needs to then approve them in the Onboarding Queue after optionally updating the software version and device configuration.

Figure 44 Claiming Devices Using Cambium ID



Onboarding fields

The following table details the columns in the Onboarding Queue. Some of these fields will be unknown or uncertain until the physical device has contacted Cloud Management.

Table 15 Onboarding fields

Parameter	Description
Actions	Before a device is onboarded, it must be approved. There are two buttons available: <ul style="list-style-type: none">• Approve: Click Approve to enable the device for onboarding. If the device is connected, it will be onboarded immediately.• Delete: If the device has been added in error, you can delete it from the Onboarding Queue. This also disconnects the device and allows it to be added to another account. The Delete button is only enabled before the device has started the onboarding process.
Added By	The user who added this device for onboarding. Note: If the Device is claimed by a tenant user, the user information is not shown on the Onboarding page.
Configure	This highlights configuration that is applied to the device before onboarding. It is presented as a set of icons that represent: software update, configuration update, and map placement. The icons have the following colors: <ul style="list-style-type: none">• Gray: Indicates that nothing is applied.• Green: Indicates that the parameter is set and applied when onboarded.
Device	The name of the device. This is set manually, or, if unset, it will be read from the device.
Duration	Displays when the status last changed for the device.
IP Address	The IP address of the device. This is only available after the device contacts cnMaestro.
MAC Address	The MAC address of the device (if known).
Serial No	The Serial Number of the device.
Status	The current status of onboarding: <ul style="list-style-type: none">• Waiting for Approval: The device has contacted cnMaestro, but it has not been approved, so



Table 15 *Onboarding fields*

Parameter	Description
	it is in a waiting state. <ul style="list-style-type: none">• Waiting for Devices: The user has claimed the device, but the device has not connected.• Onboarded: The device has completed onboarding and must now be managed through normal Configuration and Software Update processes.
Type	The type of the device (if known or manually configured).

Onboarding Configuration

Before a device has been approved, the administrator can pre-provision the device. This is presented through a set of icons (depicted below), which represent configuration update, software download, and device map position.

The color icon indicates the following:

- **Gray:** No changes are made to the device configuration (.
- **Green:** Changes are applied successfully (.



Note

Onboarding configuration can be modified until the onboarding process has begun. The approval however needs to be turned off before any changes can be made.

Basic Details

The basic configuration includes Serial Number, MAC, Device Name, Mode, and Description. A Comment can also be specified to provide additional context to the device.

Configure Device

Configure Device follows the standard template system (see the section on Template Configuration for full details). The administrator can select an existing configuration template and set any required variables.

cnMatrix Configure Device

The administrator can select configuration method with the existing template or Switch Group.

User can configure the following Switch Group options while onboarding the devices:

- General
- IP Routes
- Spanning Tree
- VLANs



Note

If **Auto Generate IPv6 Addresses** is enabled, E2E Controller fetches the IPv6 addresses automatically.

For information about onboarding E2E devices, refer to [Onboarding 60 GHz cnWave devices](#).

For information about onboarding Edge Controller and PTP 820/850 devices, refer to [Onboard Edge Controller](#) and [Onboard PTP 820/850 devices](#).

Header Notification

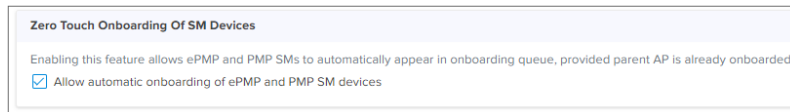
The header bar in cnMaestro displays the following UI controls:



These UI controls are located on the top right side of the UI page. The **Search** UI control allows you to provide keywords and search for the required knowledge base information (for example, onboarding devices to cnMaestro) available in Cambium community. The **Notifications** UI control provides the count of major alarms. The **Out of sync devices** UI control provides the count of devices that are out of sync. The **Administrator** UI control supports a dropdown list, which you can use to search and view account names, create account, edit profile, and log out.

Zero Touch Configuration

Zero Touch Configuration allows PMP SMs and also ePMP SMs to automatically appear in the Onboarding Queue, provided parent AP is already onboarded.



Claiming Your First Wi-Fi AP (Cloud)

Irrespective of the account type, the **Claim Your First Wi-Fi AP** option has been introduced to simplify the Wi-Fi AP deployment. This option allows the claiming of Wi-Fi APs. This option is available when no APs have been claimed for your device.

Consider the following points for using the **Claim Your First Wi-Fi AP** option:

- For the access and backhaul account type, navigate to the **Wi-Fi AP Group** tree view. You can see this option for claiming your first Wi-Fi AP.
- For the Wi-Fi account type, the **Wi-Fi AP Groups** tree menu (available on the Monitor and Manage page) is launched with the **Claim Your First Wi-Fi AP** option automatically (as shown in [Figure 45](#)).
- For Cloud users who want to claim Wi-Fi AP for a single device (after onboarding the device for the first time and if no AP has been claimed), navigate to the main **Home** page. You can locate the **Claim Your First Wi-Fi AP** widget on the right side of the **Home** page (as shown in [Figure 46](#)).

Figure 45 The Claim Your First Wi-Fi AP option

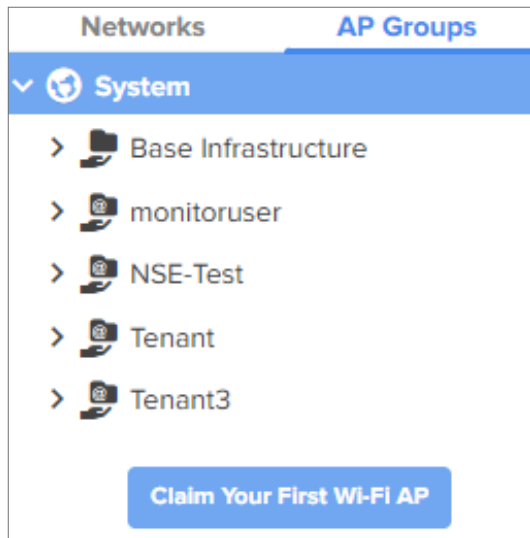
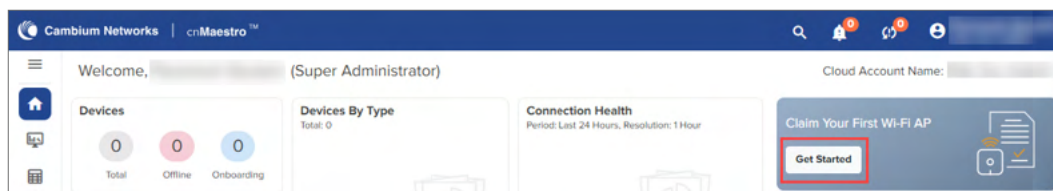


Figure 46 The Claim Your First Wi-Fi AP widget on the Home page



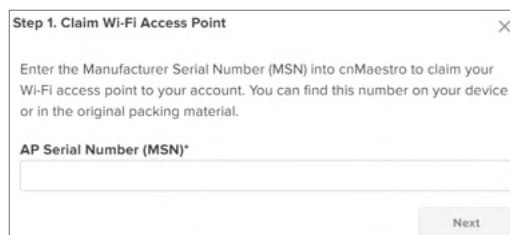
If there are any Enterprise Wi-Fi APs already claimed in an account, the **Claim Your First Wi-Fi AP** option will not be available on the cnMaestro **Home** and **Monitor and Manage** pages.

Claiming a single Wi-Fi AP from the Home page

To claim your first Wi-Fi AP for a single device, perform the following steps:

1. On the main **Home** page, locate the **Claim Your First Wi-Fi AP** widget on the right side of the page and click **Get Started** (as shown in [Figure 46](#)).

The **Claim Wi-Fi Access Point** screen appears.



2. Enter a valid value in the **AP Serial Number (MSN)** text box (for example, AxCx4040Q2V8) and click **Next**.

The **Configure Wireless LAN (Optional)** screen displays multiple settings, which are applicable to Wi-Fi APs (home and enterprise Wi-Fi).

Step 2. Configure Wireless LAN (Optional)

Please update the settings below, which will be applied to the default Home and Enterprise AP Groups. If this section is skipped, the default SSID will be "cnPilot" and passphrase will be "cambium123".

Country
 Argentina

WLAN SSID
 Select the SSID identifier for your network
 test11

WLAN Passphrase
 Select the passphrase used to authenticate wireless users
☐ Open (no security) ☒ WPA2 Pre-Shared Keys

Password:* Show

Confirm Password:* Show

Back Next

You can update the following settings based on your requirements.

- **Country:** Name of the country (used for the regulatory purpose).
- **WLAN SSID:** Unique name or ID that identifies your wireless network. Do not leave this field blank.
- **WLAN Passphrase:** The passphrase is supported only if the WPA2 Pre-Shared Keys option is selected as the security method. The minimum length of the passphrase is eight characters.

If you skip configuring this settings section, the default SSID and the security configuration of the device are retained.

3. Click **Next**.

The **Onboarding AP** screen displays the onboarding status (for example, waiting) for the device. If the device is successfully onboarded, the **Onboarding AP** screen displays the following message:

Step 3. Onboarding AP

Please turn on your AP and plug it into the internet. The AP must be able to reach <https://cloud.cambiumnetworks.com> in order to be onboarded.

✓

Device is onboarded and connected

You may now manage your AP in cnMaestro. You should be able to connect to your AP using the SSID "test11"

Exit

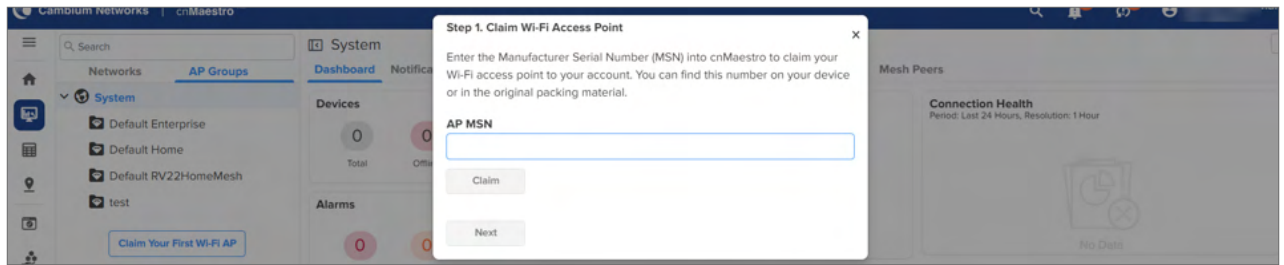
If the onboarding fails, the **Onboarding AP** screen displays a message indicating the failure status.

Claiming a single Wi-Fi AP using the AP Group menu

To claim your Wi-Fi AP using the **Wi-Fi AP Groups** tree menu, perform the following steps:

1. Navigate to **Monitor and Manage > Wi-Fi AP Groups** tree menu, and click **Claim Your First Wi-Fi AP** (as shown in [Figure 45](#)).

The **Claim Wi-Fi Access Point** screen appears.



2. Enter a valid value in the **AP MSN** text box and click **Claim**.

The device is successfully claimed.

3. Click **Next**.

The **Configure Wireless LAN (Optional)** screen displays the following fields for configuration: Country, WLAN SSID, and WLAN Passphrase.

4. Enter the configuration details.

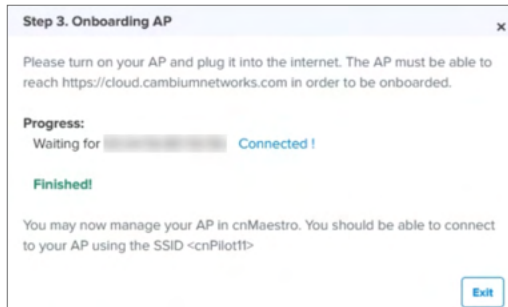
You can configure the following settings based on your requirements:

- **Country:** Name of the country (used for the regulatory purpose).
- **WLAN SSID:** Unique name or ID that identifies your wireless network. Do not leave this field blank.
- **WLAN Passphrase:** The passphrase is supported only if the WPA2 Pre-Shared Keys option is selected as the security method. The minimum length of the passphrase is eight characters.

If you skip configuring this settings section, the default SSID and the security configuration of the device are retained.

5. Click **Finish**.


The **Onboarding AP** page displays the onboarding status and configured actions for the device.

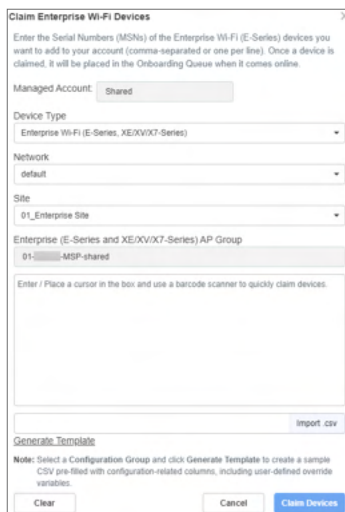


The device is mapped to the default Wi-Fi AP Group, and the configuration is updated in the Default Enterprise WLAN.

Claiming multiple Wi-Fi APs from the AP Group

To claim multiple Enterprise Wi-Fi APs from the AP Groups tree view, complete the following steps:

1. Navigate to the AP Groups tree view and click the actions  icon for the selected AP group.
2. Click **Claim Device(s)**.
3. In the **Claim Enterprise Wi-Fi Devices** pop-up dialog select the Network and Site under which these devices should be placed and by default devices claimed under this group will have its configuration settings.



4. Specify the Manufacturing Serial Numbers (MSNs) of the devices line-by-line or comma-separated, or click **Import .csv** to import the MSNs of the devices from a CSV file.

The CSV file can also include User-Defined variables that you configure in the AP Group. For more information, see [Claiming multiple Enterprise devices using CSV import](#).



Note

You can include the device host name in the CSV file while claiming Enterprise devices through the import CSV option.

Figure 47 Example CSV file to include the device name

	A	B
1	Serial Number	Device Name
2	W8TYHR3UI9OP	South-East-1
3	HRU38SJ30SLT	North-Pole
4	UIE83YGHBS23	Point-Nemo

- Click **Claim Devices** to add to the selected AP Group with the configuration applied.



Note

In cnMaestro On-Premises the procedure is the same as Cloud, but instead of MSN, the user should use the Device MAC Addresses.

Claiming multiple Enterprise devices from the Enterprise Site dashboard

To claim multiple Enterprise devices (NSE, cnMatrix, Wi-Fi AP) from the Site Dashboard, perform the following steps:

- Navigate to **Monitor and Manage > Networks** tree view.
- Click the actions (⚙️) icon for the required site and click **Claim Device(s)**.

The **Claim Enterprise Devices** window is displayed.

Figure 48 *Claim Enterprise Devices window*

Claim Enterprise Devices

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

Managed Account: Base Infrastructure

Site: 01_Enterprise Site

Device Type: All

NSE Group: Default NSE (Default)

Switch Group: None

Enterprise (E-Series and XE/XV/X7-Series) AP Group: None

Enter / Place a cursor in the box and use a barcode scanner to quickly claim devices.

Note: The Bulk CSV Import feature is currently available only for specific device types. To use this feature, please select either cnMatrix or Enterprise Wi-Fi from the Device Type dropdown menu.

Clear Cancel Claim Devices

- In the **Claim Enterprise Devices** window select the NSE group, Switch group, or the Enterprise AP Group that must be applied for the Enterprise devices.

The devices claimed under this site will have the configuration settings from the selected device group (NSE, switch, or AP).

- Specify the MSNs of the devices line-by-line or comma-separated, or click **Import .csv** to import the MSNs of the devices from a CSV file.

Click **Download Template** to download a sample CSV file.

For more information on claiming Enterprise devices using CSV files, see [Claiming multiple Enterprise devices](#)



Note

You can include the device host name in the CSV file while claiming Enterprise devices through the import CSV option.

Figure 49 Example CSV file to include the device name

	A	B
1	Serial Number	Device Name
2	W8TYHR3UI9OP	South-East-1
3	HRU38SJ30SLT	North-Pole
4	UIE83YGHBS23	Point-Nemo

- Click **Claim Devices** to add the devices to the selected device group and click **Apply Configuration**.

Claiming multiple Enterprise devices using CSV import

You can claim multiple Enterprise devices from an Enterprise site or from the AP group by either entering the serial numbers of the devices in the box provided, or by uploading a CSV file with the required information.



Note


- The CSV import option is available only for cnMatrix and Enterprise Wi-Fi APs.
CSV import option is not applicable to NSE devices.
- Also, by default, only one NSE device can be imported by adding the serial number in the box provided. To import multiple devices, High Availability (HA) must be enabled in the NSE devices.
Importing multiple NSE devices is allowed only by adding serial numbers in the box provided.

When claiming devices using the CSV files, by default, only the serial number and device name is allowed. However, if you select a particular device type (cnMatrix or Enterprise Wi-Fi) and a corresponding switch or AP group, you can also add additional details in the CSV file, based on the parameters that are present in the **User-Defined Overrides** section of the respective group.

For example, if the selected AP group contains parameters defined in the **User-Defined Overrides** section of the AP group, then these parameters appear in the CSV file as shown in the following image. The name of the selected AP group also is displayed in the CSV file.

A	B	C	D	E	F	G	H
Serial Number	Device Name	AP Group	hostname	ssid1	ssid2	channel1	channel-width
		AP-Group-01-shared					

The CSV import option for cnMatrix and Enterprise Wi-Fi APs is available from the following locations in the cnMaestro UI:

- Both cnMatrix and Wi-Fi AP devices
 - Monitor and Manage** > **Networks** tab > **<Enterprise-site-name>** > **Claim Device(s)** (from the actions  menu)
- Only Wi-Fi APs
 - Monitor and Manage** > **Networks** tab > **<Enterprise-site-name>** > **Devices** tab > **Claim New AP**

- **Monitor and Manage > AP Groups tab > <AP-group-name> > Claim Device(s)** (from the actions (⚙️) menu)
- **Monitor and Manage > AP Groups tab > <AP-group-name> > Devices tab > Claim New AP**

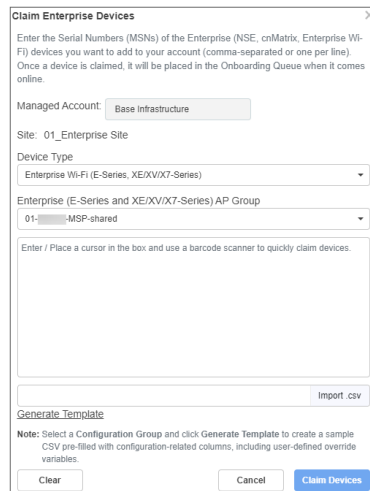
To import multiple Enterprise devices using the CSV import option, complete the following steps:

1. Navigate to any one of the pages mentioned above.

The **Claim Enterprise Devices** window is displayed as shown in the following images.

- At the enterprise site-level:

Wi-Fi APs



Claim Enterprise Devices

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

Managed Account: Base Infrastructure

Site: 01_Enterprise Site

Device Type: Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)

Enterprise (E-Series and XE/XV/X7-Series) AP Group: 01-MSP-shared

Enter / Place a cursor in the box and use a barcode scanner to quickly claim devices.

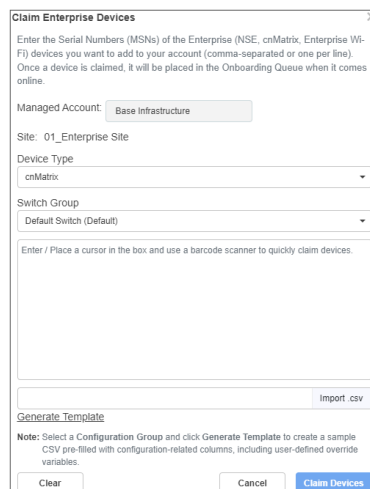
Import.csv

[Generate Template](#)

Note: Select a Configuration Group and click Generate Template to create a sample CSV pre-filled with configuration-related columns, including user-defined override variables.

Clear Cancel Claim Devices

cnMatrix devices



Claim Enterprise Devices

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

Managed Account: Base Infrastructure

Site: 01_Enterprise Site

Device Type: cnMatrix

Switch Group: Default Switch (Default)

Enter / Place a cursor in the box and use a barcode scanner to quickly claim devices.

Import.csv

[Generate Template](#)

Note: Select a Configuration Group and click Generate Template to create a sample CSV pre-filled with configuration-related columns, including user-defined override variables.

Clear Cancel Claim Devices

- At the AP group-level:

2. Select the appropriate options at the site- or AP group-level:

- At the enterprise site-level—Select the options from the **Device Type** and **Enterprise (E-Series and XE/XV/X7-Series) AP Group** dropdown lists.
- At the AP group-level—Select the options from the **Device Type**, **Network**, **Site**, and **Enterprise (E-Series and XE/XV/X7-Series) AP Group** dropdown lists.

3. Generate the CSV file with all selected columns, by clicking **Generate Template** and save the CSV file.

The CSV file contains columns corresponding to the variables that are defined in the **User-Defined Overrides** section of the switch or AP group, respectively.



Note

If no switch or AP group is selected, then CSV file will contain only the **Serial Number** and **Device Name** columns, which are the default columns.

4. Click **Import .csv** to import the CSV file with the information.
5. Click **Claim Devices**.

Points to consider when importing enterprise devices using CSV import option

- Only one AP group per CSV file is allowed. The same AP group is applied to all devices listed in the CSV file. Including multiple AP groups in the same CSV file causes an error.
- Invalid values (for example, unsupported channel numbers) will be accepted while uploading the CSV import, but the values will not be applied.
- Only hyphens (-) and underscores (_) are allowed in the **Device Name** column. All other special characters are not allowed.
- If user-defined variables are empty in the CSV file, and if the AP group configuration contains default values for these variables, then those values are assigned where applicable.
- You must specify the values for user-defined variables either in the CSV file or in the AP group (under **User-Defined Overrides** section).

The value of the variables must not be empty.

Miscellaneous Onboarding Issues

This topic provides information on some of the miscellaneous issues observed during the onboarding process.

Configuring Devices after Onboarding

When onboarding completes, the device will no longer be managed through the Onboarding Queue. Instead, Configuration and Software Upgrade must be performed through the standard cnMaestro UI sections.

Deleting Devices

While a device is in the Onboarding Queue, it can be removed from the account by deleting it from the queue. After Onboarding, the device needs to be manually deleted. The device can be deleted either by right-clicking the device node in the tree and selecting the **Delete** option or from the **Inventory** page.

Transferring Device Ownership

When a device is sold to a third-party, the device ownership needs to be transferred. This is done by deleting the device in one account, thereby opening it up to be claimed by another.



Note

For examples of onboarding and device-specific onboarding procedures, check [Onboarding Examples](#) and [Device-Specific Onboarding Instructions](#), respectively.

Onboarding Examples

This section covers the following topics:

- [Onboarding Existing Networks](#)
- [Onboarding New Devices](#)

Onboarding Existing Networks

Existing networks can be onboarded by setting Cambium ID on already-deployed devices over SNMP (see the section on Device-Specific Onboarding for details on the OID). These devices will contact Cambium Cloud and be mapped to the corresponding Cloud Management. To complete onboarding, the administrator should navigate to the Onboarding Queue and approve all devices.

Onboarding New Devices

New devices are onboarded either using Cambium ID (which is a requirement for serial numbers less than 12 characters in length) or through the Serial Number.

Claiming Devices using Cambium ID and Device UI

- Configure cnMaestro to support Cambium ID
First, make sure Cambium ID support is enabled, and a password field is set.
 1. Navigate to **Home > Onboard Devices** and click **Claim from Device**.
 2. Select **Allow device to be claimed using Cambium ID**.
 3. Click **Add New**.
 4. Choose the name of the user from the **Name** dropdown list.

5. Enter the key for the user in the **Onboarding Key** textbox. The minimum length of characters for the key is 8.
 6. Click **Save**.
- Set Cambium ID on the device UI
Launch the device UI and enter the Cambium ID and password. The example below defines how to set for ePMP.
 - Login to the device UI and navigate to **Configuration > System > cnMaestro tab**.
 - Enable the radio button for enabling **Remote Management**.
 - Enter the cnMaestro cloud URL in the **cnMaestro URL** textbox.
 - Enter Cambium ID in the **Cambium ID** textbox.
 - Enter the Onboarding key in the **Onboarding Key** textbox.
 - Click **Save** the device.
 - Approve the device for onboarding:
 1. Navigate to **Home > Onboard Devices** and click the **Onboard** tab.
 2. Find the device and onboard using the Cambium ID.
 3. You can able to see who onboarded the device.
 4. The Status field should display **Waiting for Approval**.
 5. Make any additional onboarding configuration changes you want.
 6. Approve the device by clicking the **Approve** button under **Actions**.
 7. The device status will change to **Onboarded** after onboarding finishes under the **Status**.

Claiming Devices Using Cambium ID and SNMP

Devices can be claimed over SNMP by using the Cambium ID and Onboarding Key. See [Claiming Devices with Cambium ID](#) section for devices you would like to onboard in this way.

Device-Specific Onboarding Instructions

This topic describes how to onboard the following Cambium devices to cnMaestro:

- [Onboarding cnMatrix](#)
- [Onboarding cnRanger](#)
- [Onboarding cnReach](#)
- [Onboarding cnPilot R-Series](#)
- [Onboarding cnVision](#)
- [Onboarding Enterprise AP](#)
- [Onboarding ePMP 1000](#)
- [Onboarding PMP](#)
- [Onboarding PTP 650/670/700](#)
- [Onboarding Xirrus device](#)
- [Onboarding a cnWave 5G Fixed BTS device](#)

- [Onboard Edge Controller](#)
- [Onboard PTP 820/850 devices](#)
- [Onboarding the NSE 3000 Devices](#)
- [Onboarding Home Mesh Routers](#)
- [Onboarding PON devices](#)
- [Onboarding 60 GHz cnWave devices](#)

Onboarding cnMatrix

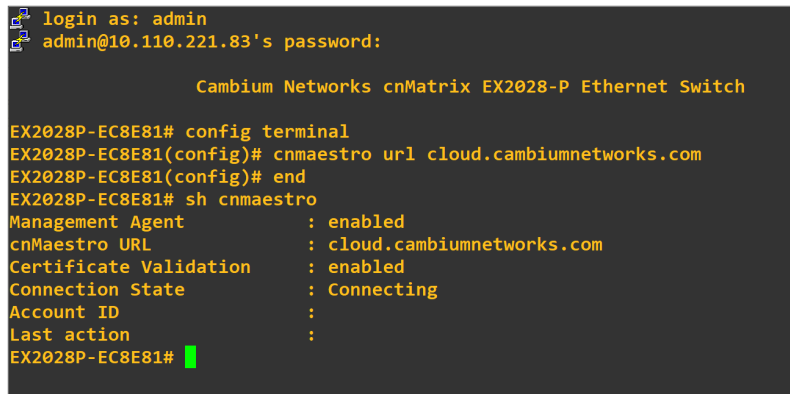
You can onboard cnMatrix through device CLI and using the device UI.

Execute the following command to onboard cnMatrix device connection to cnMaestro:

```
cnMatrix(config) # cnMaestro url cloud.cambiumnetworks.com
```

Execute the following command to view the status of cnMatrix device connection to cnMaestro:

```
cnMatrix(config) # show cnMaestro
```



```

login as: admin
admin@10.110.221.83's password:

      Cambium Networks cnMatrix EX2028-P Ethernet Switch

EX2028P-EC8E81# config terminal
EX2028P-EC8E81(config)# cnmaestro url cloud.cambiumnetworks.com
EX2028P-EC8E81(config)# end
EX2028P-EC8E81# sh cnmaestro
Management Agent      : enabled
cnMaestro URL         : cloud.cambiumnetworks.com
Certificate Validation : enabled
Connection State      : Connecting
Account ID            :
Last action           :
EX2028P-EC8E81#

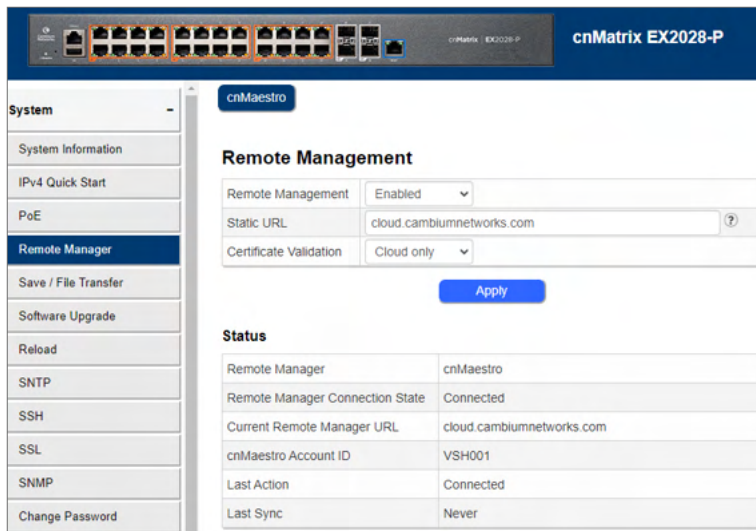
```

Onboarding cnMatrix through UI

In the cnMatrix device UI, complete the following steps:

1. Navigate to **System > Remote Management**.
2. Enter the details in **Remote Management** section.

3. Click **Apply**.



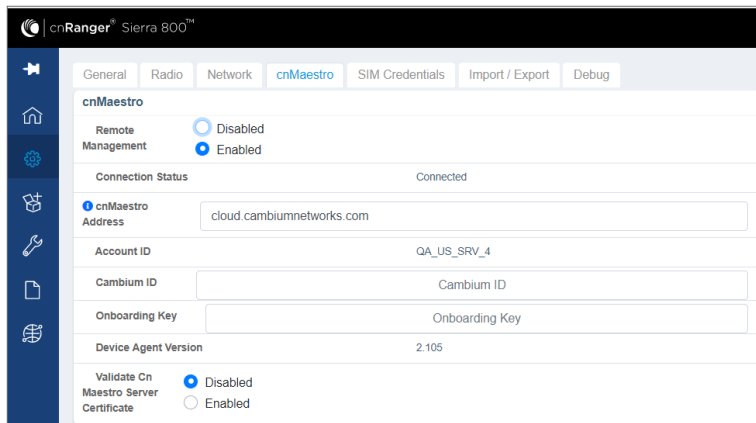
Status	
Remote Manager	cnMaestro
Remote Manager Connection State	Connected
Current Remote Manager URL	cloud.cambiumnetworks.com
cnMaestro Account ID	VSH001
Last Action	Connected
Last Sync	Never

Onboarding cnRanger

To view the status of Sierra 800 and Tyndall 101 connection to cnMaestro, complete the following steps.

Setting static URL for cnMaestro on Sierra 800

1. Navigate to **Configuration > cnMaestro**.
2. Under cnMaestro section, enter the URL in the cnMaestro Address.
3. Click **Save**.



Setting static URL for cnMaestro on Tyndall 101

1. Navigate to **Configuration > cnMaestro**.
2. Under cnMaestro section, enter the URL in the cnMaestro URL.

3. Click **Save**.

The screenshot shows the Cambium Networks cnMaestro interface. The top navigation bar includes tabs for General, Network, Radio, Scan Results, cnMaestro (selected), Import / Export, Port Mapping, and CBRS. The left sidebar contains icons for Home, Settings, and other functions. The main content area is divided into two sections: Status and Settings. The Status section shows the Connection Status as 'Connected', the Account ID as '3_0_2_EST_1_SRV_1_IJOT_RGVN', and the Device Agent Version as '2.106'. The Settings section includes a 'Remote Management' toggle set to 'Enabled', a 'cnMaestro Server Certificate Validation' toggle set to 'Disabled', a 'cnMaestro URL' field with 'cloud.cambiumnetworks.com', a 'Cambium ID' field with 'Cambium ID', and an 'Onboarding Key' field with 'Onboarding Key'.

Onboarding cnReach

Onboarding through UI

In the cnReach device UI, complete the following steps:

1. Navigate to **cnMaestro > Management Settings**.
2. Enable **cnMaestro Management** in Settings section.
3. Enter your **Cambium ID** and **Onboarding Key**.
4. Click **Save**.
5. Navigate to home page to view the status of the cnReach device connection to cnMaestro.

Figure 50 Onboarding cnReach through UI

The screenshot shows the 'cnMaestro Remote Management Settings' page. It is divided into two main sections: Status and Settings. The Status section shows 'Remote Management Status' as 'Enabled' with a status icon. Below this, there are fields for 'cnMaestro URL' (https:// cloud.cambiumnetworks.com), 'State' (Device Approval Pending), and 'Account ID'. A 'Force Reconnect' button is also present. The Settings section includes a 'cnMaestro Management' toggle set to 'On', a 'cnMaestro URL' field (https:// cloud.cambiumnetworks.com), and empty fields for 'Cambium ID' and 'Onboarding Key'. At the bottom, there are 'Save' and 'Commit' buttons.

To view the status of the cnReach connection in the cnMaestro:

Figure 51 Viewing the *cnReach* connection to *cnMaestro*

cnReach N500

Device Name	TestUpdate
Location	Boulder
Latitude	30.0
Longitude	30.0
Model	NB-N500910A-US
MSN	
Ethernet SN	
Ethernet Firmware	cn-EBX 5.2.17g

cnMaestro Device Management Status

cnMaestro Management: Enabled
Connection state: Device Approval Pending
cnMaestro URL: <https://cloud.cambiumnetworks.com>
Account ID: Warning: not set

Radio Information

SN: E501C1B8
Name: Radio One
Model: X9-X9B12
Firmware: 1.48.17487
Device Id: 456
Operating Mode End Point (EP)
Network type: Point-to-multipoint
Protocol type: Ethernet
Regulation: FCC

Onboarding cnPilot R-Series

Onboarding through UI

To view the status of the cnPilot R-Series device connection to cnMaestro, complete the following steps:

1. Navigate to **Administration > cnMaestro**.
2. Under cnMaestro configuration section.
3. Enter the URL in the **cnMaestro URL**.
4. Click **Save**.

Figure 52 Viewing the *cnPilot R-Series* device connection

Cambium Networks Firmware Version 4.6-R8
Current Time 2019-11-28 23:48:44
Admin Mode [Logout](#) [Reboot](#)

Status Network Wireless 2.4GHz Wireless 5GHz SIP FXS1 FXS2 Security Application Storage **Administration**

Management Firmware Upgrade Scheduled Tasks Certificates Provision SNMP TR069 Rflow **cnMaestro** Diagnosis

Operating Mode

cnMaestro Configuration

Configuration

Remote Management ☐ Disable ☒ Enable
IPv6 Preferred ☒ Disable ☐ Enable
Use Management Interface ☐ Disable ☒ Enable
cnMaestro URL
Connection Status Connected to cloud.cambiumnetworks.com

Credentials

Cambium ID
Onboarding Key
AccountID

Help

cnMaestro Configuration:
Device can be managed remotely using Cambium Remote Management server

Onboarding through SNMP

The following OIDs can be configured:

- cambium_id
- cambium_token
- cns_staic_url

Onboarding cnVision

Onboarding cnVision Client

In the cnVision Client device UI, complete the following steps:

1. Navigate to **Configuration > System**.
2. Under cnMaestro section, enter cnMaestro URL.
3. Click **Save**.

The screenshot shows the 'cnVision' interface for a 'Client_MICRO' device. The top navigation bar includes the Cambium Networks logo, the device name 'Client_MICRO', and the user 'Administrator'. The main content area is titled 'cnMaestro' and contains the following settings:

- Remote Management:** ☐ Disabled ☒ Enabled
- cnMaestro URL:** cloud.cambiumnetworks.com
- Cambium ID:** Cambium ID
- Onboarding Key:** *****

Below the cnMaestro section is the 'Account Management' section, which includes:

- Administrator Account:** ☐ Disabled ☒ Enabled. Username: admin, Password: *****
- Home User Account:** ☐ Disabled ☒ Enabled. Username: home, Password: *****
- Installer Account:** ☐ Disabled ☒ Enabled. Username: installer, Password: *****
- Read-Only Account:** ☐ Disabled ☒ Enabled. Username: readonly, Password: *****

At the bottom left, there is a footer with 'Version 4.6.0-RC39', 'Support', and 'Community Forum'.

Onboarding cnVision Hub

In the cnVision Hub device UI, complete the following steps:

1. Navigate to **Configuration > System**.
2. Under cnMaestro section, enter cnMaestro URL.
3. Click **Save**.

The screenshot shows the 'cnVision' interface for a 'Hub_360_test_1' device. The top navigation bar includes the Cambium Networks logo, the device name 'Hub_360_test_1', and the user 'Administrator'. The main content area is titled 'cnMaestro' and contains the following settings:

- Remote Management:** ☐ Disabled ☒ Enabled
- Zero Touch:** ☐ Disabled ☒ Enabled
- cnMaestro URL:** cloud.cambiumnetworks.comom
- Cambium ID:** Cambium ID
- Onboarding Key:** *****

Below the cnMaestro section is the 'Account Management' section, which includes:

- Administrator Account:** ☐ Disabled ☒ Enabled. Username: admin, Password: *****
- Home User Account:** ☐ Disabled ☒ Enabled. Username: home, Password: *****
- Installer Account:** ☐ Disabled ☒ Enabled. Username: installer, Password: *****
- Read-Only Account:** ☐ Disabled ☒ Enabled. Username: readonly, Password: *****

At the bottom left, there is a footer with 'Version 4.6.0-RC39'.

Onboarding Enterprise AP

Onboarding through UI

In the Enterprise AP device UI, complete the following steps:

1. Navigate to **Configure > System**.
2. Scroll to **Management > cnMaestro**.
3. Enable **Remote Management**.
4. Enable **Validate Server Certificate** if required.
5. Enter **cnMaestro URL**.
6. Enter **Cambium ID** and **Onboarding Key**.
7. Navigate to **Dashboard** to view the status of the Enterprise AP device connection to cnMaestro.

Figure 53 Onboarding Enterprise AP through device UI

The screenshot shows the 'cnMaestro' configuration page. It has a title bar 'cnMaestro'. Below it, there are five settings:

- Remote Management**: A checkbox that is checked.
- Validate Server Certificate**: A checkbox that is checked.
- cnMaestro URL**: A text input field containing 'cloud.cambiumnetworks.com'.
- Cambium ID**: An empty text input field.
- Onboarding Key**: An empty text input field.

To view the status of the device connection to cnMaestro:

Figure 54 Viewing the Enterprise AP connection to cnMaestro

The screenshot shows the 'Dashboard' page of the Enterprise AP device UI. The left sidebar has a 'Dashboard' header and several menu items: Monitor, Configure, System, Radio, WLAN, Network, Services, Operations, and Troubleshoot. The main content area has a breadcrumb 'Home / Dashboard' and two summary cards: 'Clients' with a value of 0, and 'Channel' with a value of 1 at 2.4GHz and 100 at 5GHz. Below these is an 'Access Point Info' section with a table of device details:

Access Point Info	
MAC Address	[REDACTED]
Model	cnPilot E400
Software Version	3.11-r9
Location	
Hostname	E400_DDD
Uptime	0 days, 1 hours 7 minutes
Available Memory	57 %
CPU Utilization	28 %
Hardware Type	Dual Band Indoor Integrated
Regulatory	ETSI
Serial Number	[REDACTED]
cnMaestro Connection Status	Connected to cloud.cambiumnetworks.com
cnMaestro Account ID	E425__DEVICE_TEST

Onboarding ePMP 1000

Onboarding through UI

In the ePMP device UI, complete the following steps:

1. Navigate to **Configuration > System**.
2. Scroll to **cnMaestro**.
3. Select **Enable** and enter your Cambium ID and the user's Onboarding Password.
4. Navigate to **Monitor > System** to view the status of the ePMP device connection to cnMaestro.

Figure 55 Onboarding ePMP 1000 through UI

The screenshot shows the 'System' configuration page in the ePMP 1000 UI. The left sidebar has a 'System' menu item highlighted. The main content area is titled 'cnMaestro' and contains several settings:

- Traps:** Disabled (radio button selected).
- Trap Community String:** cambiumtrap
- Remote Management:** Enabled (radio button selected).
- Zero Touch:** Enabled (radio button selected).
- cnMaestro URL:** cloud.cambiumnetwork ...
- Cambium ID:** [Empty text field]
- Onboarding Key:** [Masked password field]
- Account Management:**
 - Administrator Account:** Enabled (radio button selected). Username: admin
 - Installer Account:** Enabled (radio button selected). Username: installer

To view the status of the ePMP device connection to cnMaestro:

Figure 56 Viewing the ePMP device connection to cnMaestro

The screenshot shows the 'Monitor > System' page in the ePMP 1000 UI. The left sidebar has a 'System' menu item highlighted. The main content area displays a table of system information:

Monitor > System	
Hardware Version	Force 200
Serial number (MSN)	N/A
Firmware Version	U-Boot 9342_PX 1.1.4.a (Dec 10 2014 - 14:09:23)
Software Version	2.4.5
Date and Time	08 Aug 2015, 18:24:06 GMT
System Uptime	8 days, 18 hours
Wireless MAC Address	[Masked]
Ethernet MAC Address	[Masked]
DPS Status	Not Available
Contains FCC ID(s):	Z8H89FT0015
Read-Only Users	0
Read-Write Users	1
Factory Reset Status	Enabled
Cambium Remote Management Status	UP_CONNECTED
Cambium Account ID	My_Cambium_ID

Onboarding through SNMP

The following OIDs can be configured:

- cambiumDeviceAgentEnable
- cambiumDeviceAgentCNSURL
- cambiumCNSDeviceAgentID
- cambiumCNSDeviceAgentPassword

The following OID can be used to check the status of the device's connection to cnMaestro.

- cambiumCnsServConsStat

Onboarding PMP

Onboarding through UI

To onboard PMP device connection to cnMaestro:

In the PMP device UI, complete the following steps:

1. Navigate to **Configuration > cnMaestro**.
2. Under **Configuration**, provide the following details:
 - a. Select **Enable** under **Remote Management**.
 - b. Enter the URL to connect to cnMaestro in the **cnMaestro URL** textbox.
3. Under **Credentials**, enter the **Cambium ID** and the **Onboarding Key** in the respective textboxes. The Account ID field displays the account id of the user.

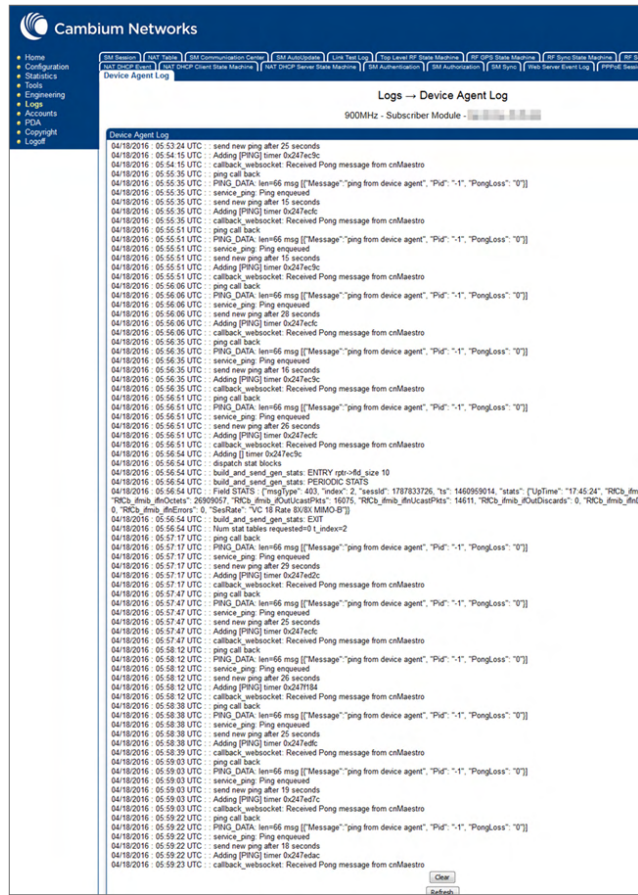
Figure 57 Onboarding PMP through UI



The screenshot shows the Cambium Networks configuration interface. The top navigation bar includes tabs for General, IP, Status, cnMaestro, Quality of Service (QoS), Security, Time, VLANs, Profiles, Protocol Filtering, Port Configuration, Tuning, and Unit Settings. The left sidebar lists various system functions like Home, Configuration, Statistics, Tools, Engineering, Logs, Accounts, Quick Start, Copyright, and Logout. The main content area is titled 'Configuration -> cnMaestro' and shows a 900MHz Access Point configuration. Below this, there are two sections: 'Configuration' and 'Credentials'. The 'Configuration' section has a 'Remote Management' toggle set to 'Enable', a 'cnMaestro URL' field with the value 'https://cloud.cambiumnetworks.com', and a 'Connection Status' field showing 'Connected to cloud.cambiumnetworks.com'. The 'Credentials' section has a 'Cambium ID' field with the value 'emp', an 'Onboarding Key' field with three asterisks, and an 'AccountID' field with the value 'KREDDUM_TESTCLOUD'. There are 'Save Changes' and 'Reboot' buttons at the top of the configuration section.

To view the logs, navigate to **Logs > Device Agent Log** page:

Figure 58 Viewing Logs



Onboarding through SNMP

The following OIDs can be configured:

- cnMaestro Enable
- cnMaestro Url
- cambium ID
- cam Onboard Key

The following OIDs can be used to check the status of the device's connection to cnMaestro.

- cam AccID
- cnMaestro Status

Onboarding PTP 650/670/700

1. Navigate to **Installation** click **Run Installation wizard** button.
2. In the **Management Configuration** window, under cnMaestro, select **Enabled**.

Management Configuration

Please enter the following configuration to manage this unit from cnMaestro.

Management configuration data entry

Attributes	Value	Units
cnMaestro	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	
cnMaestro Server	<input checked="" type="radio"/> cnMaestro Cloud <input type="radio"/> cnMaestro On-Premises	
cnMaestro Server Internet Address	cloud.cambiumnetworks.com	
cnMaestro Server Port	443	
Onboarding Method	<input type="radio"/> Serial Number <input checked="" type="radio"/> Cambium ID	
Cambium ID	<input type="text"/>	
Onboarding Key	<input type="text"/>	

Submit Management Configuration Reset Form

◀ Back Next ▶

3. Select **cnMaestro Cloud** radio button.

Management Configuration

Please enter the following configuration to manage this unit from cnMaestro.

Management configuration data entry

Attributes	Value	Units
cnMaestro	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	
cnMaestro Server	<input checked="" type="radio"/> cnMaestro Cloud <input type="radio"/> cnMaestro On-Premises	
cnMaestro Server Internet Address	cloud.cambiumnetworks.com	
cnMaestro Server Port	443	
Onboarding Method	<input checked="" type="radio"/> Serial Number <input type="radio"/> Cambium ID	

Submit Management Configuration Reset Form

◀ Back Next ▶

Onboarding Xirrus device

Perform the following steps to onboard Xirrus device through CLI.

1. Connect to the device using any SSH tool.
2. Login as admin, the default password is admin.
3. Execute the following command in ssh console:

```
#ssh admin <device IP address>
#password <admin>
#configure
#management
#cloud server cloud.cambiumnetworks.com scheme cnmaestro enable
#save
#Saving configuration...OK
#cnMaestro-onboarding id cambium_ID key onboarding_key
#save
saving configuration...OK
#show management
Cloud Management enabled Cloud Timeout 50 seconds Cloud Port 443 Cloud Retry 5
Cloud Scheme cnMaestro Cloud Server cloud.cambiumnetworks.com
Cambium ID NOTSET Cambium Key Set cnMaestro Status Not Connected
```

4. Login to Cloud account.
5. Navigate to **Home > Onboard > Devices**.
6. In the **Devices** page, the device onboarded is shown in [Figure 59](#)

Figure 59 Xirrus Device Waiting for Approval

Type	Serial Number	Name	MAC	Tier	IP Address	Source IP	Managed Account	Onboarding Mo...	Status	Onboarding Status	Duration
XD4-130		Migration-XD4-1...		Tier 3			Base Infrastructure	Using Cambium ID	Online	Waiting for Approval	3d 1h 52m
XV3-8		XV3-8-4EEEF0		Tier 3			Base Infrastructure	Using Serial Number	Offline	Waiting for Approval	1d 18h 31m
RV22 Home Mesh		RV22_800ID2		Tier 60			Base Infrastructure	Using Serial Number	Online	Waiting for Approval	2d 19h 38m
cnPilot e600		Migration_10_E6...		Tier 3			Base Infrastructure	Using Serial Number	Online	Waiting for Approval	2d 19h 38m

The Status field display **Waiting for Approval**.

It is optional to provision the device for location, software version update, and assign to an AP Group.

7. Click **Save**.
8. Click **Approve**.

For details to migrate Xirrus devices from XMS to cnMaestro X using a tool, see [XMS-Enterprise to cnMaestro X](#).



Note

- Xirrus APs are onboarded only to cnMaestro X accounts not to cnMaestro Essentials.
- Tier 3 subscription is applicable to Xirrus APs.
- Xirrus devices can only be onboarded using Cambium Id and Onboarding Key for Cloud account.

Onboarding a cnWave 5G Fixed BTS device

Claiming the cnWave 5G Fixed BTS device

To claim the cnWave 5G Fixed BTS device, you must have access to the device GUI. In the cnWave 5G Fixed BTS device UI, complete the following steps:

1. From the main home page, navigate to **System > General**.
2. In the **cnMaestro** section, enable **Remote Management**.

3. In the **Address** field, enter the cnMaestro URL or IP Address.
4. Enter your **Cambium ID** and **Onboarding Key**. **Validate Server Certificate** is an optional field.



Note

You can enter a valid **Cambium ID** and **Onboarding Key** in the cnWave 5G Fixed BTS device UI, when **Allow device to be claimed using Cambium ID** option is enabled in the **Settings** section in the cnMaestro **Onboard** page.

5. Click **Save**.

When the cnWave 5G Fixed BTS device is onboarded to the cnMaestro for the first time, the **Connection Status** field in the cnWave 5G Fixed BTS device UI displays **Device Approval Pending** as shown in [Figure 60](#).

Figure 60 Device Approval Pending status in cnWave 5G Fixed BTS

The screenshot shows the 'cnWave' configuration page in the cnMaestro UI. The 'Connection Status' field is highlighted with a red box and shows 'Device Approval Pending'. Other fields include 'System Name', 'System Location', 'System Contact', 'Geographic Location', 'Remote Management', 'Address', 'Account ID', 'Cambium ID', 'Onboarding Key', and 'Validate Server Certificate'.

6. In the cnMaestro UI, navigate to **Onboard > Devices** and click **Approve**, as shown in [Figure 61](#).

Figure 61 Approving the cnWave 5G Fixed device using the cnMaestro UI

The screenshot shows the 'Onboard' page in the cnMaestro UI. The table lists devices with columns: Type, Serial Number, Name, MAC, Tier, IP Address, Source IP, Managed Account, Onboarding Mo..., Status, Onboarding Status, and Duration. The 'Status' column shows 'Waiting for Approval' for several devices.

Type	Serial Number	Name	MAC	Tier	IP Address	Source IP	Managed Account	Onboarding Mo...	Status	Onboarding Status	Duration
XV3-8		XV3-8-EEEEFO		Tier 3			Base Infrastructure	Using Serial Number	Online	Waiting for Approval	1d 3h 3m
RV22 Home Mesh		RV22_8001D2		Tier 60			Base Infrastructure	Using Serial Number	Online	Waiting for Approval	2d 4h 10m
cnPilot e600		Migration_10_E6...		Tier 3			Base Infrastructure	Using Serial Number	Online	Waiting for Approval	2d 4h 10m
cnMatrix TX2012R-P		Migration-cnMatr...		Tier 20			Base Infrastructure	Using Serial Number	Online	Waiting for Approval	2d 4h 10m
PMP 450 SM		PMP-349834		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	3d 7h 40m
PMP 450 SM		PMP-347867		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	4d 8h 52m
PMP 450i AP		PMP-449086		Tier 2	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	4d 8h 52m
PMP 450 SM		PMP-43BE49		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	4d 9h 1m
PTP 450 BHS		PMP-439CBA		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	10d 5h 9m
PMP 450i AP		PMP-000011		Tier 2	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	11d 7h 33m

The cnWave 5G Fixed BTS device is onboarded to cnMaestro.

Figure 62 Viewing the cnWave 5G Fixed BTS device onboarded in cnMaestro

The screenshot shows the 'Onboard' page in the cnMaestro UI. The table lists devices with columns: Type, Serial Number, Name, MAC, Tier, IP Address, Source IP, Managed Account, Onboarding Mo..., Status, Onboarding Status, and Duration. The 'Status' column shows 'Onboarded' for several devices.

Type	Serial Number	Name	MAC	Tier	IP Address	Source IP	Managed Account	Onboarding Mo...	Status	Onboarding Status	Duration
cnWave 5G Fixed C10...		CPE-2		Tier 6		N/A	Base Infrastructure		Online	Onboarded	3d 2h 34m
cnWave 5G Fixed C10...		CPE-3		Tier 6		N/A	Base Infrastructure		Online	Onboarded	3d 2h 34m

The **Connection Status** field in the cnWave 5G Fixed BTS device UI displays **Connected**, on approval, as shown in [Figure 63](#).

Figure 63 *cnWave 5G Fixed BTS device Connected*

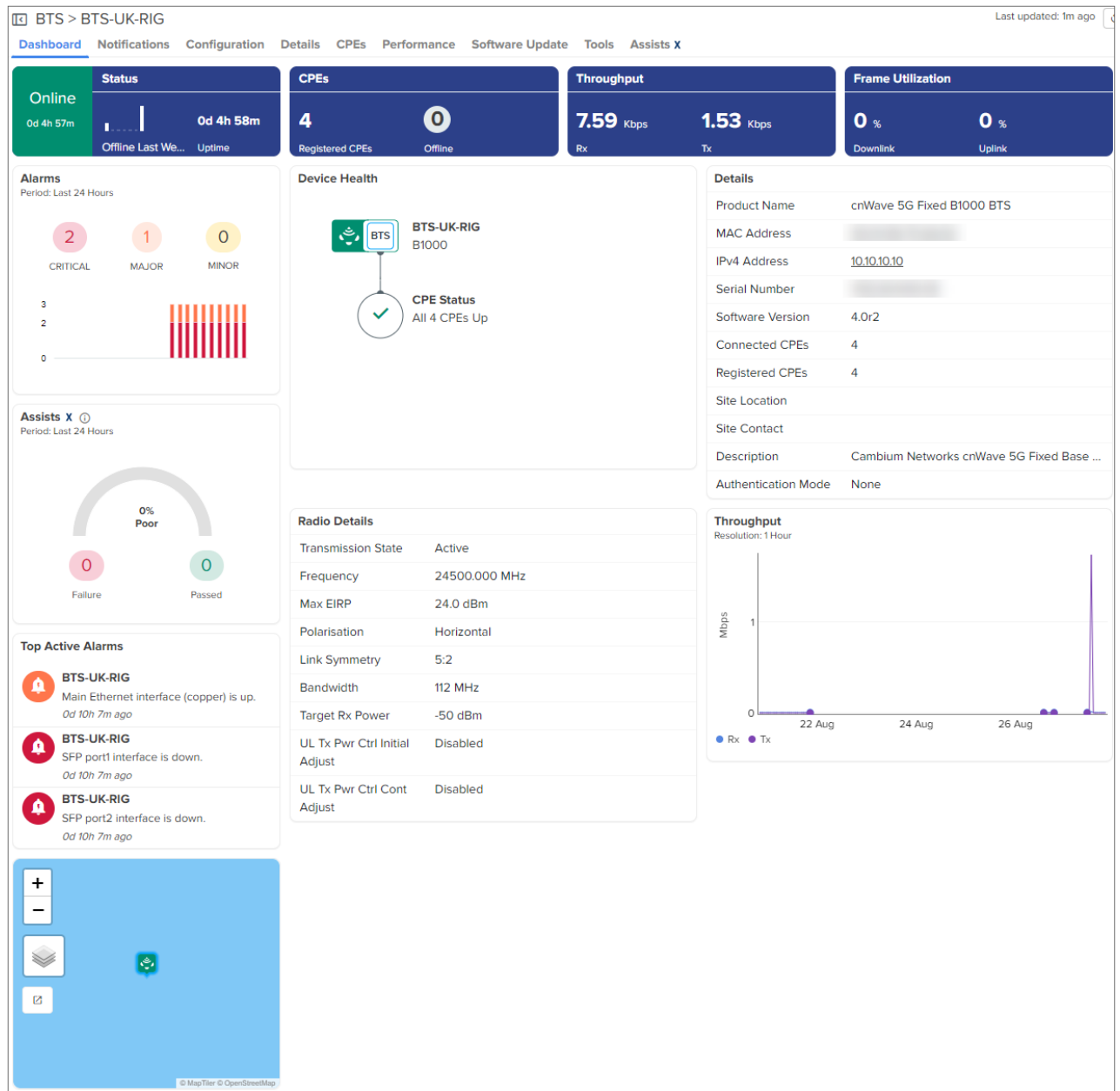
The screenshot shows the Cambium Networks cnWave 5G Fixed BTS device UI. The top bar displays 'Cambium Networks | 28 GHz cnWave™ | B1000' and user controls for 'Undo', 'Save', and 'admin'. The left sidebar contains navigation icons. The main content area is divided into two panels. The left panel, titled 'System', includes tabs for 'General', 'Management', 'Radio', 'Interfaces', 'Authentication', and 'Synchronisation'. It contains fields for 'System Name' (Cambium cnMaestro test online 12), 'System Location' (A1 Office test 12), 'System Contact' (cnMaestro team & Ram 12), and 'Geographic Location' (Latitude: 0.00000 DD, Longitude: 0.00000 DD, Altitude: 0.0 m). The right panel, titled 'cnMaestro', includes a 'Remote Management' checkbox (checked) and a 'Connection Status' field (highlighted with a red box) displaying 'Connected'. Other fields in this panel include 'Address' (cloud.cambiumnetworks.com), 'Account ID' (REGRESSION_3_1_2_CNWAVE), 'Cambium ID' (Cambium ID), 'Onboarding Key' (Onboarding Key), and a 'Validate Server Certificate' checkbox (unchecked).

To view the cnWave 5G Fixed BTS device in cnMaestro, complete the following steps:

1. From the cnMaestro UI home page, navigate to **Monitor and Manage** > default network or navigate to **Onboard** > **Devices**.
2. Click on the **Onboarded** link.

Registered cnWave 5G Fixed CPE devices are also onboarded along with cnWave 5G Fixed BTS device.

Figure 64 Viewing *cnWave 5G Fixed BTS device and registered CPE devices*



Claiming the cnWave 5G Fixed BTS device with a Serial Number

To claim and onboard the cnWave 5G Fixed BTS device, complete the following steps:

1. From the home page of cnMaestro, navigate to **Onboard > Devices** tab.

The **Onboard** page appears with details of the devices and their serial numbers, as shown in [Figure 65](#).

Figure 65 Onboard page

Type	Serial Number	Name	MAC	Tier	IP Address	Source IP	Managed Account	Onboarding M...	Status	Onboarding Status	Duration
cnWave 5G Fixed BL...		BTS-test123		Tier 7	10.10.10.10	87.82.216.58	Base Infrastructure	Using Cambium ID	Online	Waiting for Approv	
XE3-4		W8ZA09Z6R96G		Tier 3	10.110.202.210	115.110.225.242	Base Infrastructure	Using Cambium ID	Online	Waiting for Approval	< 1m
cnPilot e700		Meshbase_202...		Tier 3	10.110.202.70	115.110.225.242	Base Infrastructure	Using Cambium ID	Offline	Waiting for Device	0d 0h 2m
PMP 450 AP		PMP-903467		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	6d 4h 11m
PMP 450 AP		PMP-091227		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	6d 5h 35m
PMP 450 SM		PMP-092637		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	7d 2h 28m

- Click **Claim Device** located at the right side of the **Onboard** page, as shown in [Figure 65](#).
The **Claim Devices with Serial Number** page appears, as shown in [Figure 66](#).
- Enter the serial number of the cnWave 5G Fixed BTS device in the text box, as shown in [Figure 66](#).



Note

You can also place the cursor in the text box and use a barcode scanner to quickly claim the devices.

Figure 66 Claim Devices with Serial Number page

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](#).

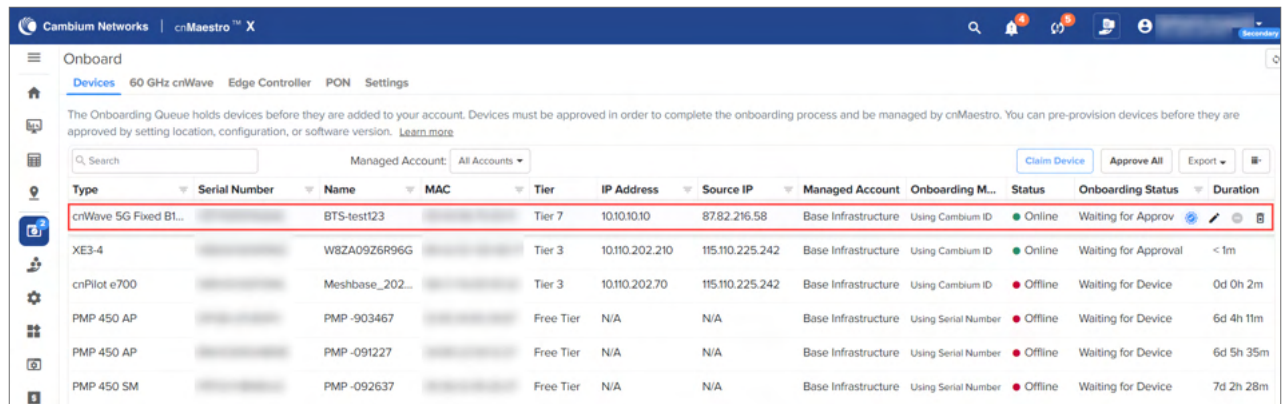
Managed Account: Base Infrastructure

Enter / Place a cursor in the box and use a barcode scanner to quickly claim devices.

Claim Devices Clear

- Click **Claim Devices**.
- To onboard the cnWave 5G Fixed BTS device, click **Approve** located at the right side of the **Onboard** page, as shown in [Figure 67](#).

Figure 67 Onboarding Queue



Type	Serial Number	Name	MAC	Tier	IP Address	Source IP	Managed Account	Onboarding M...	Status	Onboarding Status	Duration
cnWave 5G Fixed BL...		BTS-test123		Tier 7	10.10.10.10	87.82.216.58	Base Infrastructure	Using Cambium ID	Online	Waiting for Approv	
XE3-4		W8ZA09Z6R96G		Tier 3	10.110.202.210	115.110.225.242	Base Infrastructure	Using Cambium ID	Online	Waiting for Approval	< 1m
cnPilot e700		Meshbase_202...		Tier 3	10.110.202.70	115.110.225.242	Base Infrastructure	Using Cambium ID	Offline	Waiting for Device	0d 0h 2m
PMP 450 AP		PMP-903467		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	6d 4h 11m
PMP 450 AP		PMP-091227		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	6d 5h 35m
PMP 450 SM		PMP-092637		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	7d 2h 28m



Note

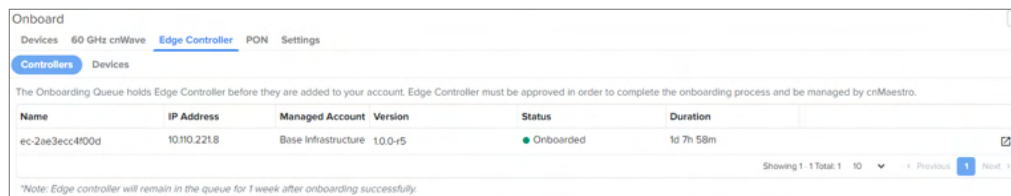
If you do not click **Approve**, the device remains in the Onboarding Queue.

Onboard Edge Controller

To onboard Edge Controller, complete the following steps:

1. Enter cnMaestro URL or IP address, Cambium ID, and Onboarding Key in CLI.
2. Navigate to **Onboard > Edge Controller > Controllers**.
3. Click **Approve**.

Figure 68 Edge Controller

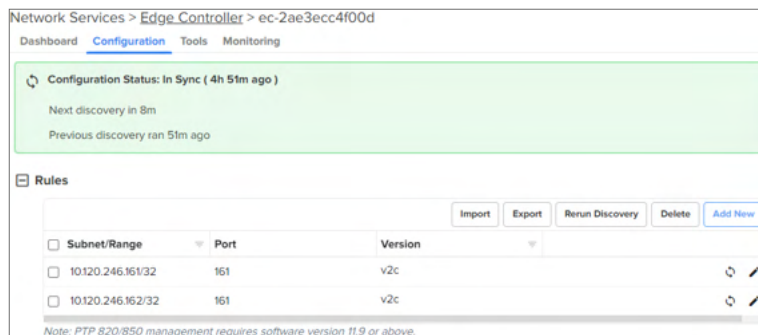


Name	IP Address	Managed Account	Version	Status	Duration
ec-2ae3ecc4f00d	10.110.221.8	Base Infrastructure	1.0.0-r5	Onboarded	1d 7h 58m

Onboard PTP 820/850 devices

To onboard PTP 820/850 devices, complete the following steps:

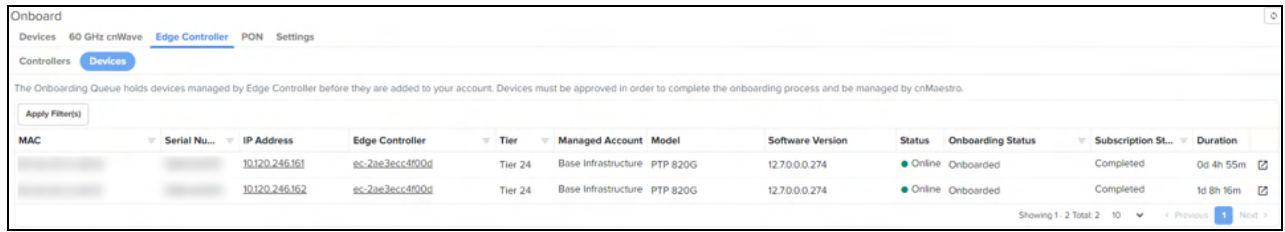
1. Ensure SNMP rules are added in Edge Controller configuration.



Subnet/Range	Port	Version
10.120.246.161/32	161	v2c
10.120.246.162/32	161	v2c

2. Navigate to **Onboard > Edge Controller > Devices**.
3. Click **Approve**.

Figure 69 PTP 820/850 devices



The Onboard interface displays a table of devices managed by the Edge Controller. The table includes columns for MAC, Serial Number, IP Address, Edge Controller, Tier, Managed Account, Model, Software Version, Status, Onboarding Status, Subscription Status, and Duration. Two devices are listed, both with IP address 10.120.246.161 and model PTP 820G. Both devices are online and onboarding is completed.

MAC	Serial Nu...	IP Address	Edge Controller	Tier	Managed Account	Model	Software Version	Status	Onboarding Status	Subscription St...	Duration
		10.120.246.161	ec-2ae3ecc4f00d	Tier 24	Base Infrastructure	PTP 820G	12.7.0.0.0.274	Online	Onboarded	Completed	0d 4h 55m
		10.120.246.162	ec-2ae3ecc4f00d	Tier 24	Base Infrastructure	PTP 820G	12.7.0.0.0.274	Online	Onboarded	Completed	1d 8h 16m

Onboarding the NSE 3000 Devices



Note

If the device needs static IP or other WAN configuration to be connected to the internet, refer to [Device UI Configuration](#).

This section describes the onboarding of NSE 3000 to the cnMaestro Cloud X account. The onboarding process requires the device Manufacturing Serial Number (MSN). The MSN of the device can be found at the bottom of the device as shown in [Figure 70](#).

Figure 70 : MSN of device



To onboard the device, complete the following steps:

1. Open a web browser and type the URL <https://cloud.cambiumnetworks.com>.
The sign in page appears.
2. Create a new cnMaestro X account or select an existing cnMaestro X account. A tier 30 subscription is required.
3. Navigate to cnMaestro **Home** > **Onboard** > click **Claim Device**.

Figure 71 Onboard page

The Onboard page displays a table of devices in the onboarding queue. The table includes columns for Type, Serial Number, Name, MAC, Tier, IP Address, Source IP, Managed Account, Onboarding Method, Status, Onboarding Status, and Duration. The devices listed are Enterprise WiFi, cnMatrix, and XE3-4, all of which are currently offline and waiting for a device.

Type	Serial Number	Name	MAC	Tier	IP Address	Source IP	Managed Account	Onboarding Mo...	Status	Onboarding Status	Duration
Enterprise WiFi	WIFI0000000000	Enterprise WiFi-6...	88:C7:7A:8E:2F:16	Tier 3	N/A	N/A	A2_Properties	Using Serial Number	Offline	Waiting for Device	4d 7h 0m
cnMatrix	WIFI0000000000	cnMatrix EX2010...	88:C7:7A:8E:2F:16	Tier 20	N/A	N/A	A2_Properties	Using Serial Number	Offline	Waiting for Device	10d 2h 13m
Enterprise WiFi	WIFI0000000000	Enterprise WiFi-6...	88:C7:7A:8E:2F:16	Tier 3	N/A	N/A	A2_Properties	Using Serial Number	Offline	Waiting for Device	10d 2h 13m
XE3-4	WIFI0000000000	XE3-4-000237-Q...	88:A2:3C:85:3D:46	Tier 3	172.16.21.13	47.180.233.48	Base Infrastructure	Using Serial Number	Online	Onboarded	0d 4h 41m
XV2-2	WIFI0000000000	XV2-2-5120IF-OS2	88:A2:3C:85:3D:46	Tier 3	172.16.21.10	47.180.233.48	Base Infrastructure	Using Serial Number	Online	Onboarded	0d 4h 45m
XV2-22H	WIFI0000000000	XV2-22H-E53DA6	88:A2:3C:85:3D:46	Tier 3	10.110.151.44	115.110.225.242	Base Infrastructure	Using Serial Number	Online	Onboarded	0d 23h 58m
XV2-2	WIFI0000000000	XV2-2-48467A	88:A2:3C:85:3D:46	Tier 3	10.110.151.43	115.110.225.242	Base Infrastructure	Using Serial Number	Online	Onboarded	1d 0h 59m
XV2-22H	WIFI0000000000	XV2-22H-E53C88	88:A2:3C:85:3D:46	Tier 3	192.168.5.100	103.181.116.62	Base Infrastructure	Using Serial Number	Offline	Onboarded	4d 3h 20m

4. **Claim Devices with Serial Number** window pops up.

Figure 72 Claim devices with Serial Number

The Claim Devices with Serial Number window prompts the user to enter the Serial Numbers (MSNs) of the devices they want to add to their account. It includes a dropdown menu for the Managed Account (Base Infrastructure) and a text box for entering the Serial Numbers. A note indicates that all devices with 12 digit strong Serial Numbers can be claimed here, and other devices can be claimed using Cambium ID.

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

Enter / Place a cursor in the box and use a barcode scanner to quickly claim devices.

[Claim Devices](#) [Clear](#)

5. Select the **Managed Account** from the dropdown.
6. Enter the Serial Number (MSN) of the device in the text box.
7. Click **Claim Devices**.

The device will be listed in the Onboarding Queue.

8. Click the **Approve Device** (🔍) icon or **Approve All** at the right side of the Onboard page, as shown in

Figure 73 Approve

The Onboard page displays a table of devices in the onboarding queue. The table includes columns for Type, Serial Number, Name, MAC, Tier, IP Address, Source IP, Managed Account, Onboarding Method, Status, Onboarding Status, and Duration. The devices listed are NSE, cnPilot R195W, cnPilot R200, and PMP 450i AP, all of which are currently offline and waiting for a device.

Type	Serial Number	Name	MAC	Tier	IP Address	Source IP	Managed Account	Onboarding M...	Status	Onboarding Status	Duration
NSE		NSE-700580		Tier 30	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	7d 22h 42m
cnPilot R195W		cnPilot-r195W-6...		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	9d 18h 8m
cnPilot R200		cnPilot-r200-08...		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	9d 18h 8m
PMP 450i AP		PMP-449086		Tier 2	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	0d 0h 42m

When device is approved appears on the Onboard page as shown below in [Figure 74](#).

Figure 74 NSE 3000 Device Onboard

Type	Serial Number	Name	MAC	Tier	IP Address	Source IP	Managed Account	Onboarding Mode	Status	Onboarding Status	Duration
NSE 3000		NSE7003EQ-165-ESS		Tier 30			Base Infrastructure	Using Serial Number	Online	Onboarded	0d 0h 17m

Onboarding Home Mesh Routers

To onboard the Home Mesh Router to cnMaestro, see [Onboarding the Home Mesh Router to cnMaestro](#).

Claiming the Home Mesh Router on the cnMaestro Cloud's **Onboard** page is not supported.

Onboarding PON devices

This section describes the onboarding of PON devices to the cnMaestro X account. The onboarding process requires the device Manufacturing Serial Number (MSN). The MSN of the device can be found at the bottom of the device as shown in [Figure 75](#).

To onboard the router, complete the following steps:

1. Navigate to cnMaestro **Home > Onboard**.

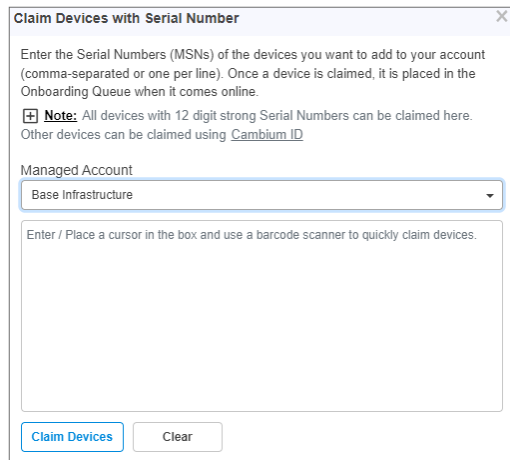
Figure 75 Onboard page for PON devices

Type	Serial Number	Name	MAC	Tier	IPv4 Add...	Managed Account	Added By	Onboarding Mode	Status	Onboarding S
TCX08 OLT		TCX08-20-02-0a		Tier 40	10.110.240.46	01_MIXED_DEVICES_MSP_SSR	Indra Reddy	Using Cambium ID	Online	Onboarded
SXX00 ONU		XGS-PON ONU Port 3		Tier 41	N/A	01_MIXED_DEVICES_MSP_SSR	-	-	Online	Onboarded
SXX00 ONU		XGS-PON ONU Port 3		Tier 41	N/A	01_MIXED_DEVICES_MSP_SSR	-	-	Online	Onboarded
SGX00 ONU		G-PON ONU Port 3		Tier 41	N/A	01_MIXED_DEVICES_MSP_SSR	-	-	Online	Onboarded
SGX00 ONU		G-PON ONU Port 3		Tier 41	N/A	01_MIXED_DEVICES_MSP_SSR	-	-	Online	Onboarded
SXX00 ONU		XGS-PON ONU Port 7		Tier 41	N/A	01_MIXED_DEVICES_MSP_SSR	-	-	Online	Onboarded
SXX00 ONU		XGS-PON ONU Port 7		Tier 41	N/A	01_MIXED_DEVICES_MSP_SSR	-	-	Online	Onboarded
TCX16 OLT		TCX16-20-04-96-qa4		Tier 40	10.110.217.4	Base Infrastructure	Kinshu Arora	Using Serial Number	Online	Onboarded
SXX00 ONU		XGS-PON ONU SN-CMBM05F68B9F		Tier 41	N/A	Base Infrastructure	-	-	Online	Onboarded
SXX00 ONU		XGS-PON ONU SN-CMBM000000DB		Tier 41	N/A	Base Infrastructure	-	-	Online	Onboarded

2. Click **Claim Device**.

The **Claim Devices with Serial Number** window is displayed.

Figure 76 Claim devices with Serial Number



3. Select the account from the **Managed Account** dropdown list .
4. Enter the Serial Number (MSN) of the device in the text box.
5. Click **Claim Devices**.

The device will be listed in the Onboarding Queue.

6. Click the **Approve Device** (🔍) icon.

Onboarding 60 GHz cnWave devices

You can onboard a 60 GHz device (V1000, V2000, V3000, or V5000) to cnMaestro with the End-to-End (E2E) Controller enabled. E2E Controller handles important management functions such as link bring-up, software upgrades, and configuration

A cnWave network is managed by a central controller called E2E Controller. Each cnWave node (V1000, V2000, V3000, or V5000) runs minion (client) that connects to the E2E Controller. The controller can run on any host with a route to the cnWave network, including a cnWave node itself.

60 GHz cnWave devices support the following E2E Controllers types:

- **External E2E Controller:** When the controller runs external to mesh, typically in a docker, it is referred as External E2E Controller. This controller type supports up to 500 nodes in a mesh.
- **Onboard E2E Controller:** When the controller runs on a cnWave node that is marked as PoP in the mesh, it is referred as Onboard E2E Controller. Currently, the Onboard E2E Controller is restricted to 31 nodes.

Based on the E2E Controller type hosted on the 60 GHz device, the onboarding process varies. Without the E2E Controller enabled, the onboarding of 60 GHz devices is not supported in cnMaestro.



Note

Before onboarding a 60 GHz cnWave device (V1000, V2000, V3000, or V5000), ensure to complete the following **prerequisite** tasks:

- Ensure that the required E2E Controller type is hosted on the 60 GHz device. For detailed information on deploying the E2E Controller for the 60 GHz device, refer to the 60 GHz cnWave E2E Controller User Guide.
- Enable the E2E Controller (after hosting) using the device UI. For detailed information on enabling the E2E Controller for the 60 GHz device, refer to the latest 60 GHz cnWave User Guide.
- Ensure that the IP address of the E2E Controller is set. The E2E Controller and cnMaestro are two

separate entities and they can be hosted on separate computers or the same computer. The E2E Controller uses IPv4 to communicate with the cnMaestro and uses IPv6 to communicate with the cnWave radios.

This topic covers the following sections:

- [Onboarding a 60 GHz device with external E2E Controller](#)
- [Onboarding a 60 GHz device with Onboard E2E Controller](#)
- [Onboarding the Onboard E2E Controller using Serial Number](#)

Onboarding a 60 GHz device with external E2E Controller

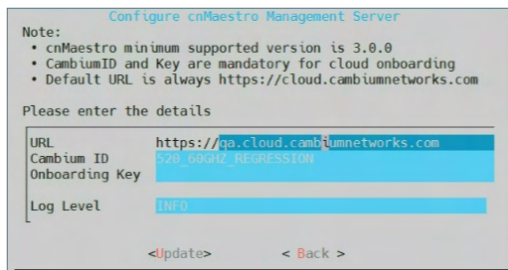
To onboard a 60 GHz device with the external E2E Controller, complete the following steps:

1. Ensure that the 60 GHz cnWave E2E Controller package (OVA file) is installed on a Linux machine or Oracle Virtualbox (which is used for device management).
2. Set the IP address of the external E2E Controller.
3. At the console, SSH into the external E2E Controller using its IP address.

The cnWave E2E Controller Terminal UI (TUI) opens.

4. Navigate to the **cnMaestro** option.

The Configure cnMaestro Management Server window opens.



```
Configure cnMaestro Management Server
Note:
• cnMaestro minimum supported version is 3.0.0
• CambiumID and Key are mandatory for cloud onboarding
• Default URL is always https://cloud.cambiumnetworks.com

Please enter the details

URL          https://qa.cloud.cambiumnetworks.com
Cambium ID   60GHz_60GHz_60GHz
Onboarding Key 60GHz_60GHz_60GHz
Log Level    INFO

<Update>    < Back >
```

5. Set appropriate values for the following parameters:

- **URL:** Enter the cnMaestro URL that is used for device management.
- **Cambium ID:** Enter the valid ID that is required for onboarding the 60 GHz cnWave device (with E2E Controller) to cnMaestro.

A Cambium ID is a string that uniquely identifies an account (which you create). It consists of letters, numbers, and underscores. Example: 60GHz_xxx_xxxxxxxxxx. It is used to onboard devices and is assigned to the devices managed by cnMaestro.

- **Onboarding Key:** Enter an appropriate onboarding key (if configured) that is mapped to an individual user account. You can set the onboarding keys for the required user accounts using the **Onboard > Settings** page in the cnMaestro UI. For more details, check [Onboarding Key configuration](#).

6. Click **Update**.

7. From the home page of cnMaestro UI, navigate to the **Monitor and Manage > Network** and select a 60 GHz cnWave network. Example: 60 GHz cnWave E2E

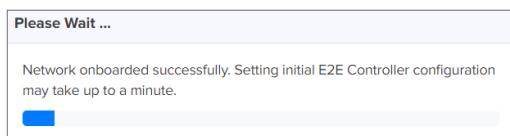


8. Click **Approve**.

The **60 GHz cnWave–Network Onboard** window appears. By default, **Auto-assign** is selected. You can select **Auto-assign** or **Manual**.

When you select **Manual**, you can update IPv6 address for the E2E Network. You must wait until the IPv6 address gets updated. If **Auto Generate IPv6 Addresses** is enabled, the E2E Controller fetches the IPv6 addresses automatically.


9. Set the required parameters and select the **Enable Layer 2 Bridge** checkbox, if required.
10. Click **Apply** and Wait until the network onboard is successful.

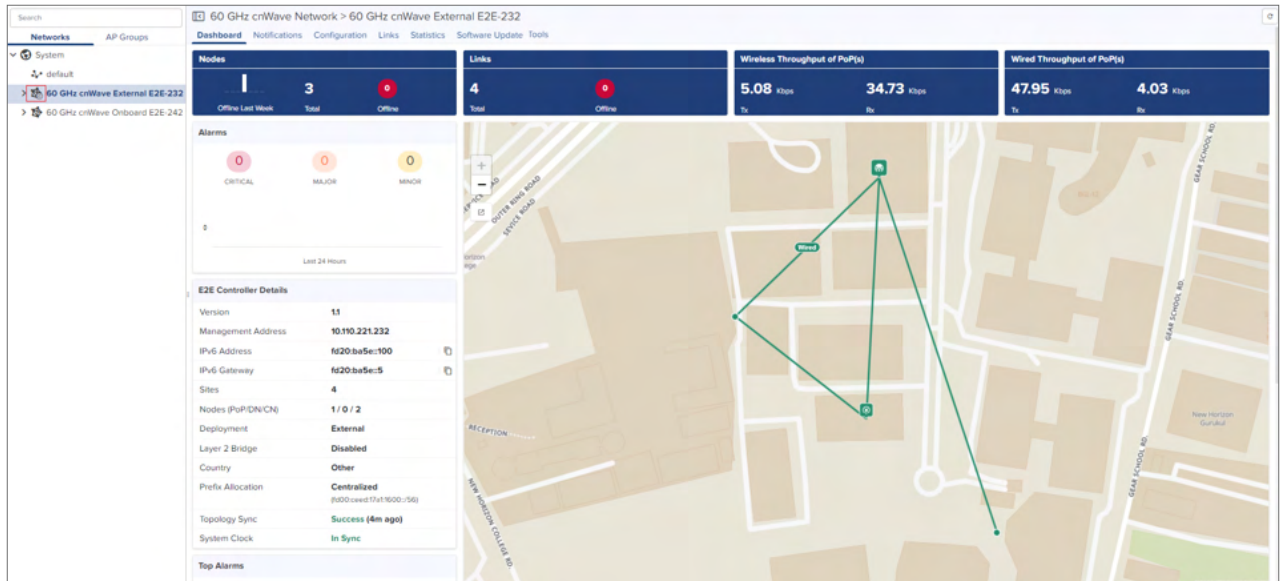


Note

The **Onboard** page in cnMaestro UI supports a separate tab for 60 GHz cnWave. Using this **60 GHz cnWave** tab, you can check the onboarding queue for E2E Controllers and cnWave devices. Users must approve the 60 GHz E2E Controller before it is added to cnMaestro as an E2E Network. The users can approve either through the Onboarding Queue or the Hierarchical Tree (where the E2E Network is placed on the Monitor and Manage page).

When the onboarding is approved, the 60 GHz cnWave E2E Network (and its devices) can be managed by cnMaestro.

When the onboard is successfully complete, the cnMaestro UI displays the External E2E Network dashboard as shown in the figure below. The  icon indicates the External E2E Controller network.



Onboarding a 60 GHz device with Onboard E2E Controller

To onboard a 60 GHz device with the internal Onboard E2E Controller (which is running on the 60 GHz cnWave device), complete the following steps:

1. Ensure that the external E2E Controller is enabled using the device UI. For details, refer to the 60 GHz cnWave User Guide.
2. Ensure that the Onboard E2E Controller is enabled using the device UI. You can set the remote management settings, including Cambium URL, Cambium ID, and onboarding key. For details, refer to the 60 GHz cnWave User Guide.
3. From the home page of cnMaestro UI, navigate to the **Monitor and Manage > Network** page and select a 60 GHz cnWave network.



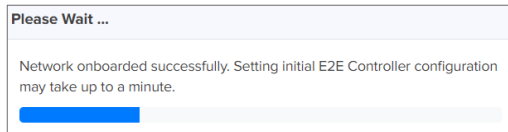
4. Click **Approve**.

The **60 GHz cnWave - Network Onboard** window appears.

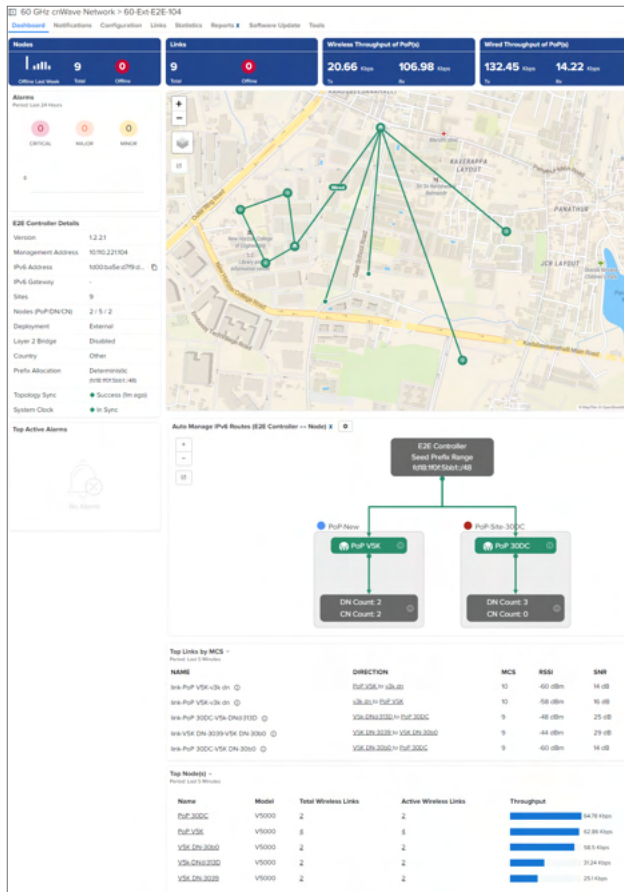
The screenshot shows the '60 GHz cnWave - Network Onboard' window. It has a title bar with a close button. Inside, there is a 'Name' label and a text input field containing '60 GHz cnWave E2E-883083'. Below the input field is a 'Save' button.


5. Edit the network name and click **Save**.

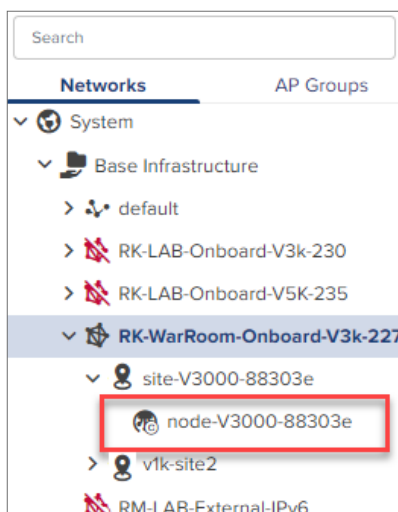
You must wait until the network onboard successful message is displayed.



When the onboard is successfully complete, the cnMaestro UI displays the Onboard E2E Network dashboard as shown in the figure below.



If a PoP node is running the Onboard E2E Controller, then the  icon indicates the PoP as shown in the figure below.



Onboarding the Onboard E2E Controller using Serial Number

To onboard the internal running 60 GHz Onboard E2E Controller using its serial number, complete the following steps:

1. From the home page of cnMaestro UI, select **Onboard** and click the **60 GHz cnWave** tab.

2. Click on the **Claim Onboard E2E** button.

The **Claim Onboard E2E Network with Serial Number** windows appears

3. Enter the serial number of the 60 GHz cnWave devices and click **Claim Devices**.

Deleting Devices in Bulk

cnMaestro allows to delete devices in bulk. You can delete devices in bulk from the following pages in cnMaestro:

- Unmanaged devices from the **Onboard > Devices** page.
- Onboarded and managed devices from the **Inventory** page—at the System-, Network-, Tower-, and Site-levels.
- From the **Manage Subscriptions > Devices** page.

Deleting the devices creates a corresponding job in the **Administration > Jobs > Actions** page. The page displays the list of all the delete jobs corresponding to the devices that were deleted. In case a deletion task is unsuccessful, it also allows you to retry deleting the devices.

The following topics are described:

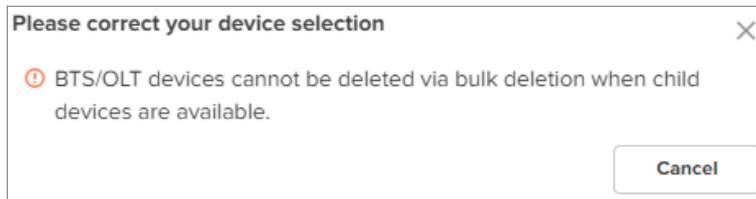
- [Device-specific restrictions](#)
- [Deleting devices in bulk](#)
- [Viewing the status of device deletion and retrying](#)

Device-specific restrictions

When deleting devices in bulk, there are a few restrictions on some devices. The following are the device-specific restrictions and the corresponding messages that appear when you try to delete these devices in bulk:

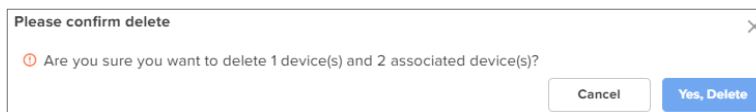
- **cnWave 5G Fixed Wireless (BTS/CPE) and PON (OLT/ONU):** You cannot delete BTS or OLT devices in bulk when they are connected to CPE or ONU devices. The following message appears:

Figure 77 *Deleting BTS/OLT devices in bulk*



However, you can delete a single BTS or OLT devices along with the associated devices (CPE or OLT) when you click the delete (🗑️) icon in the corresponding row.

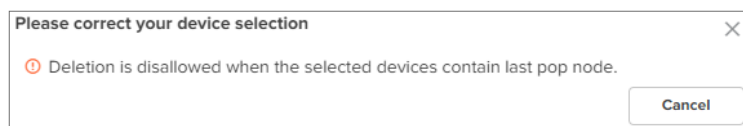
Figure 78 *Deleting single BTS/OLT device*



- **cnWave 60 GHz:** Bulk deletion works differently depending on the type of controllers you are deleting.
 - External E2E Controller: You can delete multiple devices under an External E2E controller in bulk.
 - Onboard E2E Controller: You cannot bulk delete the devices if a last pop node is also selected as one of the devices in addition to the DN and CN devices.

The following message appears:

Figure 79 *Deleting Onboard E2E Controllers with last pop node*



In this case, you must first delete the DN and CN devices, and then delete the last pop node.

- **cnVision, PMP, and ePMP:** Bulk delete of PMP and ePMP devices depend on how the SMs were onboarded.
 - SMs onboarded using the zero touch method: Bulk deleting parent APs will also delete all the associated SMs.

Figure 80 Deleting APs with SMs onboarded using zero touch method

Device	Network	Tower	CBRS Registered SMs	Zero Touched Managed	Zero 1
ePMP_2000_AP_BULKSETUP		ePMP_BulkSetup	0	52	0

- SMs onboarded without the zero touch method: Bulk deleting parent APs will delete only those APs. However, the associated SMs will be moved to the default network.

Figure 81 Deleting APs with SMs onboarded without zero touch method

- **CBRS claimed APs:** If APs that are claimed by CBRS are deleted, then the child SMs that are claimed by CBRS are deregistered and deleted from the **Management Tool** page as well.

This occurs even when CBRS-claimed SMs are not selected for bulk deletion.

Deleting devices in bulk

To delete devices in bulk, complete the following steps:

1. Navigate to one of the pages listed above, for example, **Onboard > Devices**.

Figure 82 Onboard > Devices page

2. Select the checkboxes corresponding to the devices that you want to delete and click the **Delete** () button.

Delete

Figure 83 *Select devices*

Type	Serial Number	Name	MAC	Tier	IP Address	Source IP	Managed Account	Onboarding Mode	Status	Onboarding Status	Subscription Status	Duration
<input checked="" type="checkbox"/>	PMP 450 SM	PMP-677823		N/A	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	Will attempt after appr...	1d 1h 57m
<input checked="" type="checkbox"/>	PMP 450 SM	PMP-43BE5D		N/A	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	Will attempt after appr...	2d 2h 4m
<input checked="" type="checkbox"/>	cnMatrix	cnMatrix-F5AAE0		Tier 20	N/A	N/A	Application issue test	Using Serial Number	Offline	Waiting for Device	Completed	0d 22h 41m
<input type="checkbox"/>	ePMP	ePMP Force 300...		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	Completed	5d 22h 14m
<input type="checkbox"/>	ePMP	ePMP Force 300...		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	Completed	5d 22h 14m
<input type="checkbox"/>	PMP 450 SM	PMP-894356		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	Completed	5d 22h 14m
<input type="checkbox"/>	PMP 450 AP	PMP-678954		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	Completed	5d 22h 14m
<input type="checkbox"/>	PMP 450i SM	PMP-4546A7		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	Completed	5d 22h 14m
<input type="checkbox"/>	PMP 450i High ...	PMP 450i SM-BE...		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	Completed	5d 22h 14m
<input type="checkbox"/>	PMP 450i High ...	PMP 450i SM-BE...		Free Tier	N/A	N/A	Base Infrastructure	Using Serial Number	Offline	Waiting for Device	Completed	5d 22h 14m

- Click **Yes, Delete** in the confirmation dialog box that appears.

Figure 84 *Confirmation*

Please confirm delete

Are you sure you want to delete 3 device(s)?

Cancel Yes, Delete

- The devices are removed from the page and a deletion job creation banner appears on the top of the page.

Figure 85 *Deletion job banner*



- Click the link in the banner to view the status of the deletion.

Viewing the status of device deletion and retrying

When you delete bulk devices from any of the pages listed—Onboard, Manage Subscriptions, or Inventory—cnMaestro creates job for that activity.

To view the status of the bulk deletion activity, complete the following steps:

- Navigate to **Administration > Jobs > Actions** page.

Figure 86 *Administration > Jobs > Actions* page

Type	Managed Account	Source	Occurrence	Created by	Created on	Completed on	Status
Delete	Base Infrastructure	N/A	Now	Administrator	Jun 28, 2024 12:39	Jun 28, 2024 12:39	Completed:
Delete	Base Infrastructure	N/A	Now	Administrator	Jun 28, 2024 12:30	Jun 28, 2024 12:33	Completed:
Delete	Base Infrastructure	N/A	Now	Administrator	Jun 28, 2024 12:23	Jun 28, 2024 12:24	Completed:
Delete	Base Infrastructure	N/A	Now	Administrator	Jun 28, 2024 11:52	Jun 28, 2024 11:54	Completed:
Delete	Base Infrastructure	N/A	Now	Administrator	Jun 28, 2024 10:55	Jun 28, 2024 10:56	Completed:
Delete	Base Infrastructure	N/A	Now	Administrator	Jun 28, 2024 09:37	Jun 28, 2024 09:38	Completed:
Delete	Base Infrastructure	N/A	Now	Administrator	Jun 27, 2024 22:10	Jun 27, 2024 22:10	Completed:
Delete	Base Infrastructure	N/A	Now	Administrator	Jun 27, 2024 19:36	Jun 27, 2024 19:38	Completed:
Delete	Base Infrastructure	N/A	Now	Administrator	Jun 27, 2024 17:07	Jun 27, 2024 17:07	Completed:
Delete	Base Infrastructure	N/A	Now	Administrator	Jun 27, 2024 17:07	Jun 27, 2024 17:07	Completed:

- To view the status of an ongoing bulk delete activity, click the show more (📄) icon.

The Delete Status window appears.

Figure 87 Delete Status window

Delete Status			
Created By Administrator			
Apply Filter(s)			
Device	Mode	Result	Message
ePMP_2000_AP_BULKSETUP	AP	Processing	-

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

Close

The following colors display the various statuses of the bulk delete activity:

- **Success** — Displays the number of devices deleted successfully
- **Skipped** — Displays the number of devices that were skipped from deleting.
- **Failed** — Displays the number of devices that were not deleted.

For the failed status, you can view the reason for the failure and the devices that failed to delete by clicking the show more (📄) icon.

Figure 88 Delete status for failed delete

Delete Status							
Created By Administrator							
Apply Filter(s)							
Device	Managed Account	Mode	Network	Tower/Site	Status	Result	Message
CBRS-224-AP	Base Infrastructure	AP	default	PMP_Tower	Online	Failed	Cloud synced device. Need clou
EX2010-EF6CB0	Base Infrastructure	SW	default	N/A	Online	Failed	Cloud synced device. Need clou
PTP 820G - 10.120.246.161	Base Infrastructure	PTP	PTPBXX	PTPNetwork246	Online	Failed	Cloud synced device. Need clou
XE5-8-Meeting_room	01_MIXED_DEVICES_MSP	Wi-Fi	default	01_Mixed_Devices_MSP	Online	Failed	Cloud synced device. Need clou

Showing 1 - 4 Total: 4 25 < Previous 1 Next >

Close Retry

- **Unknown** — Number of devices whose delete status is unknown.

The Unknown status appears for those devices which cnMaestro failed to delete but were retried for deletion from another location other than the **Jobs > Actions** page (Onboard, Inventory or Subscriptions pages).

- **Remaining** — Number of devices that are yet to be deleted.

All the above values are also displayed as a percentage (%).

- In the delete status window, click **Retry** to restart the bulk deletion of the failed devices.

- Once you click **Retry**, cnMaestro removes the current delete activity job and creates a new job for the retry.

- However, if you retry deleting the devices from another location (Onboard, Inventory or Subscriptions pages), the failed job status is changed to **Unknown**.

Monitoring

This section includes the following topics:

- [Network Monitoring](#)
- [Network Service Edge](#)
- [Wireless LAN Dashboard](#)
- [Fiber OLT and ONU](#)
- [Inventory](#)
- [Reports](#)



Note

Following are the retention period for various data in cnMaestro:

- Audit logs—90 days
- Wi-Fi AP performance—1 year
- Guest Access session and login events—90 days
- Wi-Fi events—7 days
- Wireless Clients—30 days

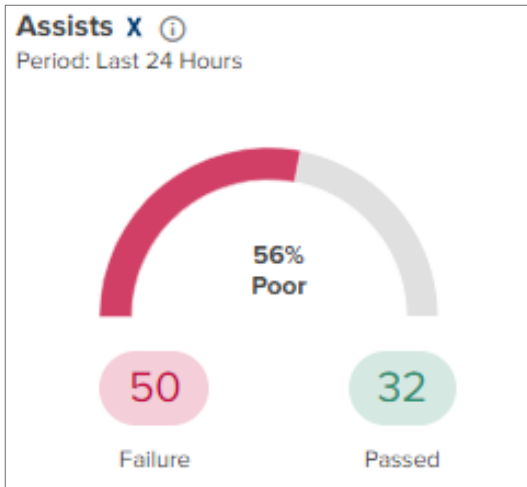
Network Monitoring

The Monitoring tab displays the monitoring pane for cnMaestro. The section includes the following:

- [Assists X](#)
- [Dashboard](#)
- [Notifications](#)
- [Configuration](#)
- [Statistics and Details](#)
- [Performance](#)
- [Map](#)
- [Tools](#)
- [Wireless Intrusion Detection System \(WIDS\)](#)
- [Wireless Intrusion Prevention System \(WIPS\)](#)

Assists X

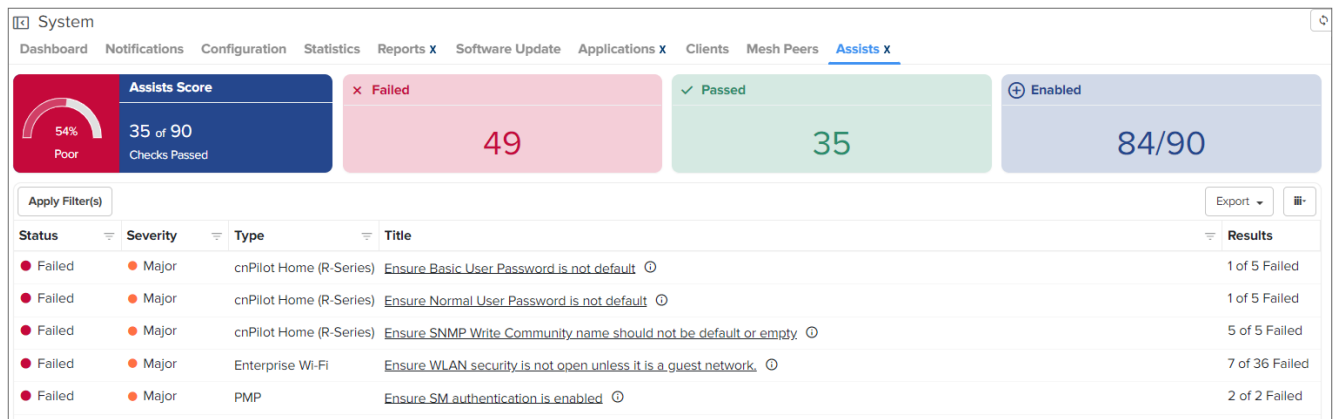
Assists X displays scanned configuration scores and results for last 24 hours.



Assists X scans the configurations and generates assists scores. It evaluates specific issues that might occur during deployment. Assists X summarizes the scores and status results at System, Network, Site, Tower, and Device levels as shown in [Figure 89](#).

This enables prioritization of management traffic.

Figure 89 Assists X home page



Note

- Assists X is a cnMaestro X feature available for cnPilot, cnMatrix, cnWave 5G Fixed, ePMP, PMP, PTP 670/700, and Enterprise Wi-Fi devices except AOS devices.
- Minimum software version for PTP 50670 and PTP 78700 is 04-10. For PTP 45700, the minimum software version is 04-02 for assist data to be generated.
- Minimum software version for cnWave 5G Fixed devices must be 3.1b5 for assist data to be generated.
- For ePMP, and cnWave 5G Fixed devices, the Assists X page generates data every 24 hours.
- For PMP devices with software version 21.1 or higher, the Assists X page generates data immediately after onboarding. For software versions lower than 21.1, this page continues to generate data on a 24-hour schedule.
- For cnPilot Home series, cnMatrix, and Enterprise Wi-Fi, PTP 670/700 devices, the Assists X page generates data immediately after onboarding.

Assists X scores are shown in percentage values. The Assists X scores guide users to isolate issues by scanning an environment and evaluating configuration and infrastructure. Assists X scores are determined as shown in [Table 16](#).

Table 16 Assist Scores

Score Value	Description
0-61%	Poor
61 % to 90%	Good
91% and above	Excellent

Table 17 Assists X parameters

Fields	Description
Status	Status of the assists are shown as follows: <ul style="list-style-type: none"> Passed Failed Disabled
Severity	Severity level of the assists are shown as follows: <ul style="list-style-type: none"> Critical: Catastrophic problem that makes the feature unusable. Major: Issue that greatly degrades the feature, but it is still usable. Minor: Limited issue that alters functionality in a targeted way. Notify: Message used primarily for information.
Type	Type of the device.
Title	Short title describing the assist.
Category	Type of category such as Security, Network, Infrastructure, and Performance.
Group	Grouped based on Position, Access, and Configuration of cnMaestro.
Results	Result of assists such as Passed, Failed, and Disabled. For more details on assists result description refer to Figure 90 .

Hovering the cursor on the **Results** column in the Assists X home page displays a preview of the assist results as shown in [Figure 90](#).

Figure 90 Assists X Results

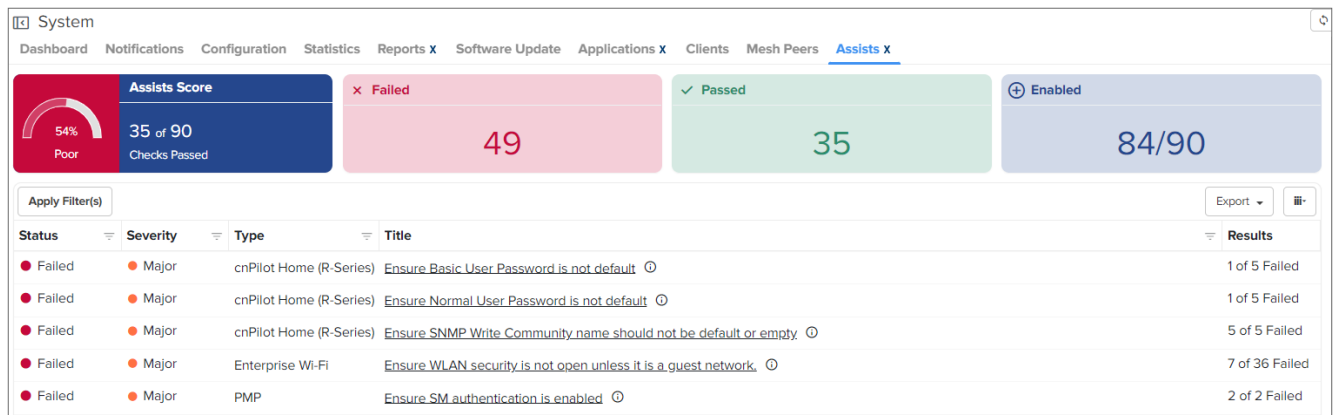


Table 18 Assist Result Status

Assist Result	Description
Passed	Assists recommendations are met.
Failed	Assists has failed.
Disabled	Assists is disabled. Note: Only Super Administrator and Administrator user roles have access to change the disabled option.

Exporting assists information

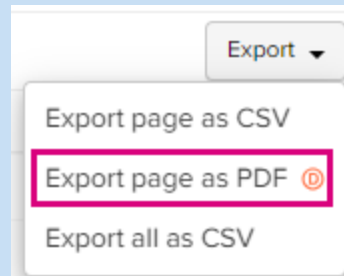
The assists table can be exported in the CSV file format. The following export options are available:

- Export page as CSV
- Export all as CSV



Note

The **Export page as PDF** option is deprecated from cnMaestro release version 5.2.0 onwards. This option will be completely removed from the UI in release version 5.3.0.



System

Dashboard Notifications Configuration Statistics Reports X Software Update Applications X Clients Mesh Peers Assurance X Assists X

Failed

62

Passed

35

Enabled

97/99

Apply Filter(s)

Status	Severity	Type	Title
Failed	Major	cnPilot Home (R-Series)	Ensure Admin User Password is not default ⓘ
Failed	Major	cnPilot Home (R-Series)	Ensure Basic User Password is not default ⓘ
Failed	Major	cnPilot Home (R-Series)	Ensure Normal User Password is not default ⓘ

Export

Export page as CSV

Export page as PDF ⓘ

Export all as CSV

1 of 11 Failed

Assists filter

To create custom filters for assists, perform the following steps:

1. In the assists table, click **Apply Filter(s)**.
2. Enter the values in the fields for applying the filters.
3. Click **Apply Filter**.

Figure 91 Assists: New Filter

The screenshot shows the 'Assists' page in the Cambium cnMaestro Cloud interface. At the top, there's a navigation bar with tabs like Dashboard, Notifications, Configuration, Statistics, Reports, Software Update, Applications, Clients, Mesh Peers, and Assists. Below this, a summary section displays the 'Assists Score' as 35 of 90 (53% Poor). To the right, there are three status boxes: 'Failed' (48), 'Passed' (35), and 'Enabled' (83/90). A 'Filters' dialog box is open, showing options to filter by Status (Failed, Passed, Disabled), Severity (Critical, Major, Minor, Notify), Type (Select or Search...), Title (Search), Category (Search), and Group (Search). The main table lists various assists, such as 'User Password is not default' and 'Write Community name should not be default or empty', with their respective counts and results.

You can manually filter or search by typing parameters in the column header of the Assists table.

4. Click **Reset** to reset the filter option in the Assists table.
5. Click **Clear Filters** to clear all the filter options.

If you do not receive expected filter details, click **Change Filter(s)** in the Assists table to apply new filters.

Assists Status

To evaluate the Assists Status, click the **Title** column with affected devices in the Assists table. A detailed Assists page appears with **Description** and **Remediation** as shown in [Figure 92](#).

To disable Assists, perform the following steps:

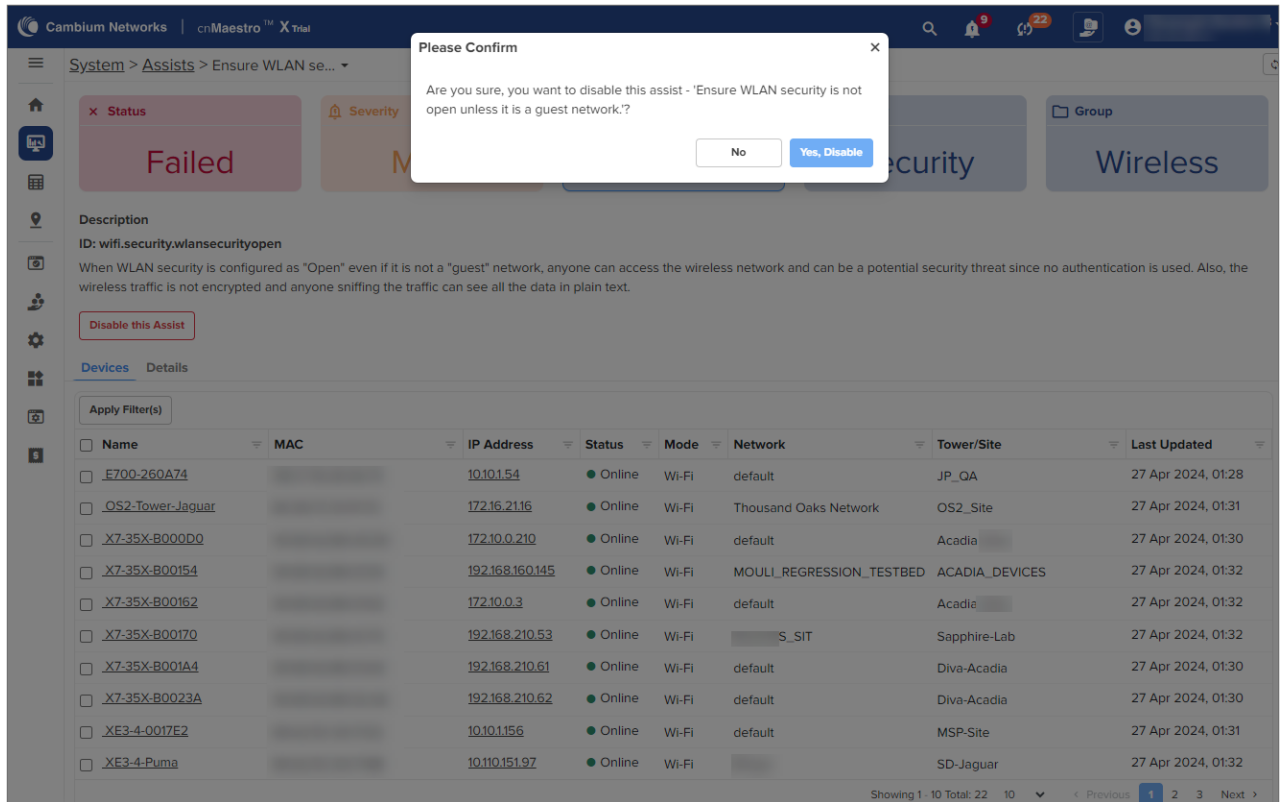
1. In the **Assist Status** page, click **Disable this Assist**.

Figure 92 Assist Status page

The screenshot shows the 'Assist Status' page in the Cambium cnMaestro Cloud interface. At the top, there's a navigation bar with tabs like System, Assists, and Ensure SNMP Write Community name should not be default or empty. Below this, a summary section displays the 'Status' as 'Failed' (Major). To the right, there are three status boxes: 'Affected Devices' (5), 'Category' (Security), and 'Group' (Management). The 'Description' section shows the ID: cnPilot.security.SNMPWriteCommunityNotEmptyandNotDefault and the message: 'SNMP Write Community name field should not be kept empty and must not be default.' A 'Disable this Assist' button is highlighted. Below, a table lists affected devices with columns for Name, MAC, IP Address, Status, Mode, Network, Tower/Site, and Last Updated.

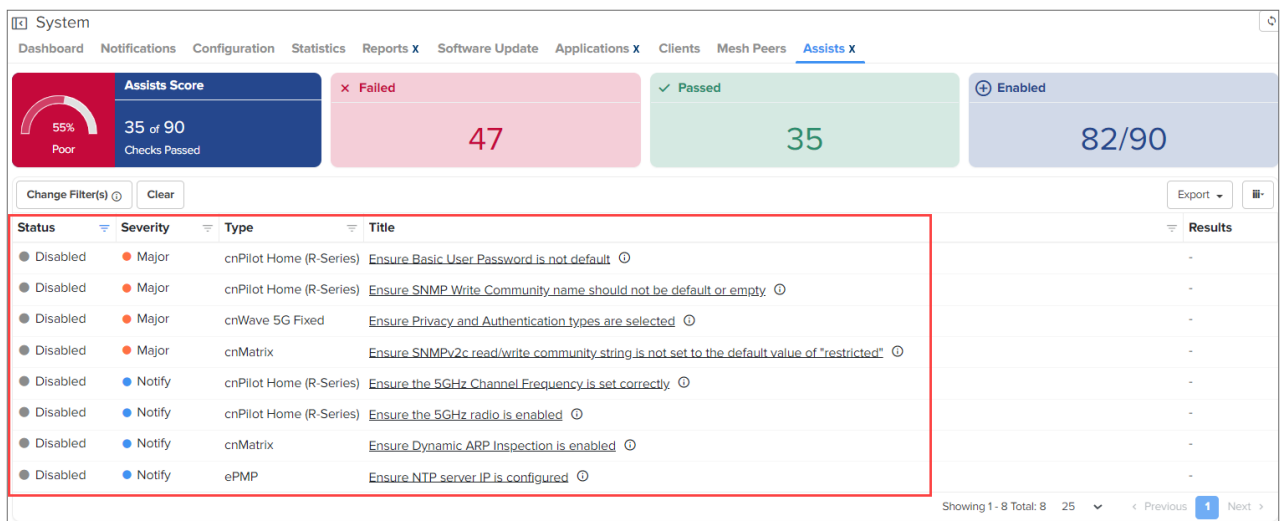
A confirmation message appears for the assist to disable.

2. Click **Yes, Disable**.



Disabled Assists are listed at the bottom of the Assists X home page. The **Results** column do not indicate the progress bar for the Assists Disabled as shown in [Figure 93](#). The total number of enabled Assists in the home page is reduced when Assists is disabled.

Figure 93 Assists Disabled



3. In the **Assists Status** page, click **Devices** tab to view the list of devices failed for the specific assist.

System > Assists > Ensure WLAN security is not open unless it is a guest network.

Status: Failed
Severity: Major
Affected Devices: 7
Category: Security
Group: Wireless

Description
ID: wifi.security.wlansecurityopen
When WLAN security is configured as "Open" even if it is not a "guest" network, anyone can access the wireless network and can be a potential security threat since no authentication is used. Also, the wireless traffic is not encrypted and anyone sniffing the traffic can see all the data in plain text.

[Disable this Assist](#)

Devices Details

Apply Filter(s)

Name	MAC	IP Address	Status	Mode	Network	Tower/Site	Last Updated
<input type="checkbox"/> E700-D090BA			Online	Wi-Fi	default	HOME-GETT-Test	17 Nov 2023, 17:12
<input type="checkbox"/> Mesh_Base			Online	Wi-Fi	Niraj	Bangalore-Home	17 Nov 2023, 17:12
<input type="checkbox"/> Meshbase_202_70_dontouch			Online	Wi-Fi	default	01_Mixed_Wi-Fi_SEKHAR	17 Nov 2023, 17:12
<input type="checkbox"/> XV2-2-5120H			Online	Wi-Fi	Aman Patwari	Aman Site	17 Nov 2023, 17:11
<input type="checkbox"/> XV2-22H-E535F			Online	Wi-Fi	Divya	Divya	17 Nov 2023, 17:11
<input type="checkbox"/> XV2-22H-E53D4C			Online	Wi-Fi	Divya	Divya	17 Nov 2023, 17:11
<input type="checkbox"/> XV2-23T-E5E9B7			Online	Wi-Fi	001_VIJAY_PRASAD_SIT_TEST	XV-XE_SERIES	17 Nov 2023, 17:12

Device filter

To create a custom device filters, perform the following steps:

1. In the Assists X page, click **Title**.
2. Navigate to Details > Device.
3. Click Apply Filters button.
4. Enter the values in the fields for applying the filters.
5. Click **Apply Filter**.

Figure 94 Assists device filter

System > Assists > Ensure WLAN security is not open unless it is a guest network.

Status: Failed
Severity: Major
Affected Devices: 7
Category: Security
Group: Wireless

Description
ID: wifi.security.wlansecurityopen
When WLAN security is configured as "Open" even if it is not a "guest" network, anyone can access the wireless network and can be a potential security threat since no authentication is used. Also, the wireless traffic is not encrypted and anyone sniffing the traffic can see all the data in plain text.

[Disable this Assist](#)

Devices Details

Apply Filter(s)

Filters

Name:

MAC:

IP Address:

Status: ☐ Online ☐ Offline

Mode:

Network:

[Apply Filter\(s\)](#) [Reset](#)

Name	MAC	IP Address	Status	Mode	Network	Tower/Site	Last Updated
<input type="checkbox"/> E700-D090BA		10.150.202.107	Online	Wi-Fi	default	HOME-GETT-Test	17 Nov 2023, 17:12
<input type="checkbox"/> Mesh_Base		192.168.88.251	Online	Wi-Fi	Niraj	Bangalore-Home	17 Nov 2023, 17:12
<input type="checkbox"/> Meshbase_202_70_dontouch		10.150.202.70	Online	Wi-Fi	default	01_Mixed_Wi-Fi_SEKHAR	17 Nov 2023, 17:12
<input type="checkbox"/> XV2-2-5120H		192.168.0.24	Online	Wi-Fi	Aman Patwari	Aman Site	17 Nov 2023, 17:11
<input type="checkbox"/> XV2-22H-E535F		10.50.0.58	Online	Wi-Fi	Divya	Divya	17 Nov 2023, 17:11
<input type="checkbox"/> XV2-22H-E53D4C		10.50.0.59	Online	Wi-Fi	Divya	Divya	17 Nov 2023, 17:11
<input type="checkbox"/> XV2-23T-E5E9B7		192.168.51.9	Online	Wi-Fi	001_VIJAY_PRASAD_SIT_TEST	XV-XE_SERIES	17 Nov 2023, 17:12

Showing 1 - 7 Total 7 10 < Previous 1 Next >

You can manually filter or search by typing parameters in the column header of the device table.

6. Click **Reset** to reset the filter option in the device table.
7. Click **Clear Filters** to clear all the filter options.

If you do not receive expected filter details, click **Change Filter(s)** in the device table to apply new filters.

Enable Assist

To enable assist, perform the following steps:

1. Click the disabled assist listed at the bottom of the Assists X home page.

Status	Severity	Type	Title	Results
Disabled	Major	cnPilot Home (R-Series)	Ensure Basic User Password is not default	-
Disabled	Major	cnPilot Home (R-Series)	Ensure SNMP Write Community name should not be default or empty	-
Disabled	Major	cnWave 5G Fixed	Ensure Privacy and Authentication types are selected	-
Disabled	Major	cnMatrix	Ensure SNMPv2c read/write community string is not set to the default value of "restricted"	-
Disabled	Notify	cnPilot Home (R-Series)	Ensure the 5GHz Channel Frequency is set correctly	-
Disabled	Notify	cnPilot Home (R-Series)	Ensure the 5GHz radio is enabled	-
Disabled	Notify	cnMatrix	Ensure Dynamic ARP Inspection is enabled	-
Disabled	Notify	ePMP	Ensure NTP server IP is configured	-

You will be directed to specific Assist page, as shown in the following figure.

2. Click **Enable this Assist**.

Assists X fix now



Note

The Assists X **Fix Now** feature is available only for ePMP and PMP devices.

Assists X **Device** page allows the user to fix the failed assists.

Perform the following steps to fix the failed assists:

1. Navigate to the Assists X **Device** page.
2. Select the devices to be fixed.

System > Assists > Ensure "SNMP Read-Write Community String" is not set to a commonly-known community string

Status **Failed**
Severity **Major**
Affected Devices **7**
Category **Security**
Group **Management**

Description

ID: `egmp.services.commonsnmpcsfsw`

The community string has been checked against a list of commonly-known community strings and found to be in that list. This could allow unauthorized access to the device using SNMP v2c. The unauthorized user will be able to read configuration and statistics from the device, change configuration and execute actions like rebooting and factory resetting the radio.

[Disable this Assist](#)

Devices Details

Apply Filter(s)

Name	MAC	IP Address	Status	Mode	Network	Tower/Site	Last Updated
<input checked="" type="checkbox"/> EPMP-Test			Online	AP	default		17 Nov 2023, 18:31
<input checked="" type="checkbox"/> F300-AP			Online	AP	default		17 Nov 2023, 18:32
<input checked="" type="checkbox"/> F400-200d16			Online	AP	AY	Kyiv F400	17 Nov 2023, 18:32
<input checked="" type="checkbox"/> PTP550-AP			Online	AP	default		17 Nov 2023, 18:31
<input checked="" type="checkbox"/> EPMP-SM			Online	SM	default		17 Nov 2023, 18:31
<input checked="" type="checkbox"/> F425-200d16			Online	SM	AY	Kyiv F400	17 Nov 2023, 18:32
<input checked="" type="checkbox"/> PTP550-SM			Online	SM	default		17 Nov 2023, 18:31

Showing 1 - 7 Total: 7 10 1 Previous 1 Next

3. Click **Fix now**.

The **Fix Now** window pops up.

Fix Now 7 Device(s)

Issue

Ensure "SNMP Read-Write Community String" is not set to a commonly-known community string

Details

This will change "SNMP Community String 1" to the value specified.
NOTE: This configuration change will not reboot the device(s).

Template

```

{
  "device_group": {
    "snmpReadWriteCommunity": "${SNMP_COMMUNITY_STRING}"
  }
}

```

SNMP_COMMUNITY_STRING

Update

☒ Now ☐ Schedule

Job Options

☐ Stop update on critical error

Within a sector, update

☒ SMs first and then AP ☐ AP first and then SMs

☐ Devices to update in parallel (1-500)

Notes

[Apply](#) [Cancel](#)

4. Select from the following options under the **Update** field, to fix the issue now or at a later date:

- **Now**—Fix the issue immediately when you click **Apply** on this page.
- **Schedule**—Fix the issue at the selected date and time. Select the required date and time from the **Start Date** and **Start Time** fields.

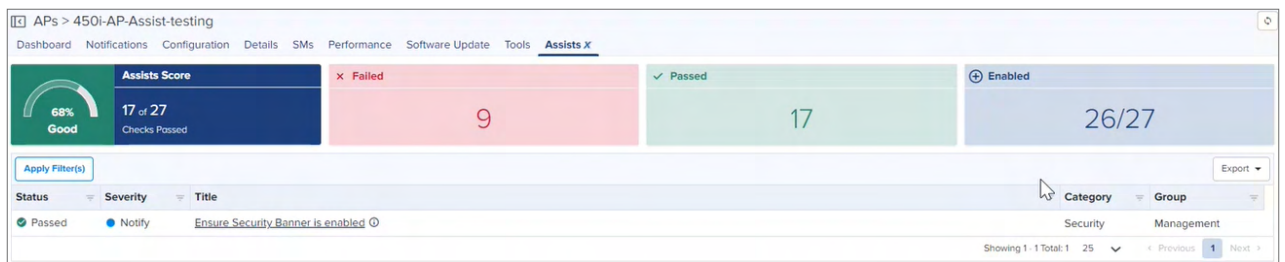
5. Click **Apply**.

Success window pops up.

ID	Details	Managed Account	Occurrence	Target	Created by	Created on	Completed on	Parallel	Stop on Error	Sector Priority	Status
14864	1 device(s)	All Accounts	Now		Auto-Sync	Nov 21, 2023 20:...	Nov 21, 2023 20:...	15	false	N/A	Completed
14863	1 device(s)	All Accounts	Now		Auto-Sync	Nov 21, 2023 20:17	Nov 21, 2023 20:...	15	false	N/A	Completed
14862	1 device(s)	All Accounts	Now		Auto-Sync	Nov 21, 2023 20:...	Nov 21, 2023 20:11	15	false	N/A	Completed
14861	1 device(s)	All Accounts	Now		Auto-Sync	Nov 21, 2023 19:59	Nov 21, 2023 20:...	15	false	N/A	Completed
14860	1 RV22 Home Mesh device...	Base Infrastructure	Now	SANJAYTEST.ME...	sanjay.jadhav	Nov 21, 2023 17:46	Nov 21, 2023 17:54	-	false	N/A	Completed
14859	3 device(s)	All Accounts	Now		Auto-Sync	Nov 21, 2023 17:38	Nov 21, 2023 17:40	15	false	N/A	Completed
14858	3 device(s)	All Accounts	Now		Auto-Sync	Nov 21, 2023 17:38	Nov 21, 2023 17:40	15	false	N/A	Completed
14857	3 device(s)	All Accounts	Now		Auto-Sync	Nov 21, 2023 17:37	Nov 21, 2023 17:38	15	false	N/A	Completed
14856	3 device(s)	All Accounts	Now		Auto-Sync	Nov 21, 2023 17:36	Nov 21, 2023 17:37	15	false	N/A	Completed
14855	3 device(s)	All Accounts	Now		Auto-Sync	Nov 21, 2023 17:36	Nov 21, 2023 17:36	15	false	N/A	Completed

When the failed assists are fixed, the status is changed to **Passed** as shown in [Figure 95](#).

Figure 95 *Passed Assists*



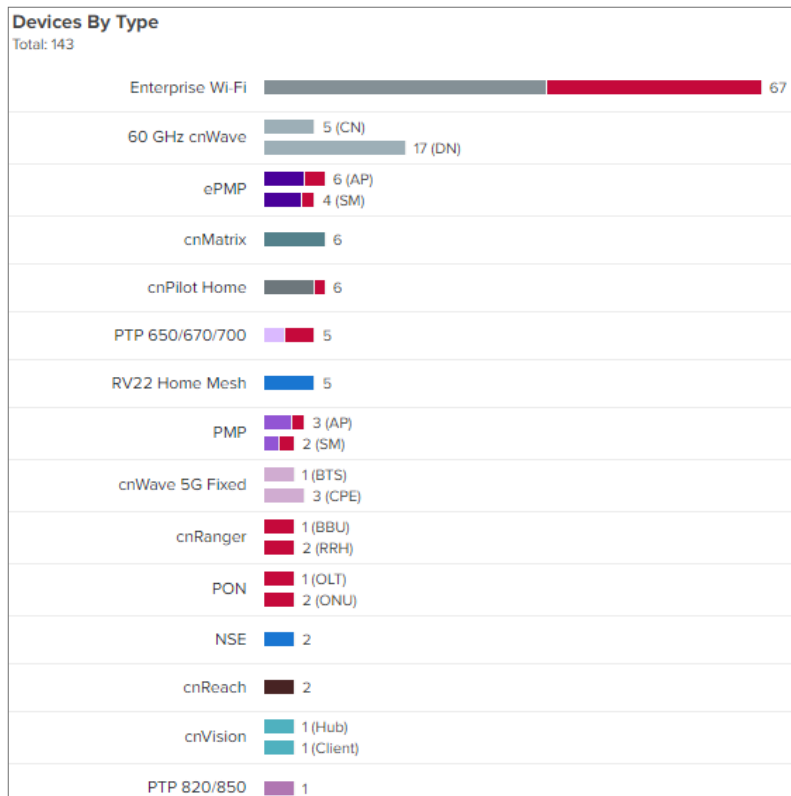
Dashboard

The **Dashboard** page in cnMaestro is customized for each device type and aggregation level (such as System, Network, Tower, and Site). Pages representing devices provide information on location, significant configuration parameters, and performance. System, Network, Tower, and Site nodes aggregate dashboard data for devices they contain.

KPI (Key Performance Indicators)

Each page has a set of KPIs tailored to the node type. These display a current value and often historical trend data over the last 24 hours.

Figure 96 *Device by Type*



Note

KPI widgets at network and Tower-level show minimum four widgets when no data is available in KPI's. Shows wireless clients KPI when at least one Wi-Fi device is available. Wireless clients KPI is moved beside Wi-Fi KPI. Machfu KPI is not supported any more.

Application History X

The Application History X widget displays top client names and their top five application usage details for last 24 hours.

Figure 97 *Application History X*

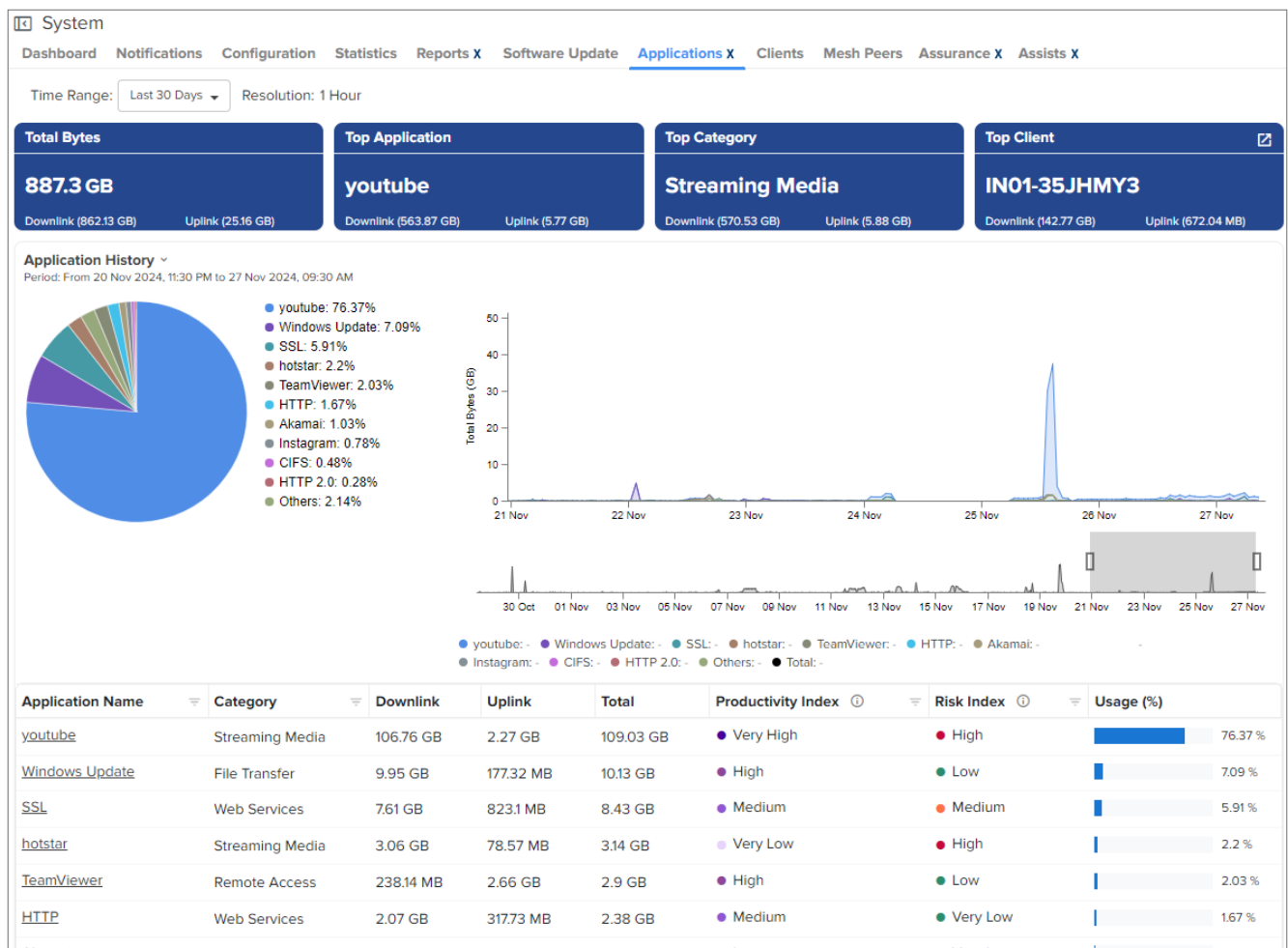


Figure 98 Category History X



The **System Dashboard** page displays detailed system level application usage in **Application History X** and **Category History X**. It displays the top five client names and their respective usage details. The parameter fields are explained in detail as shown below.

Figure 99 System > Applications X



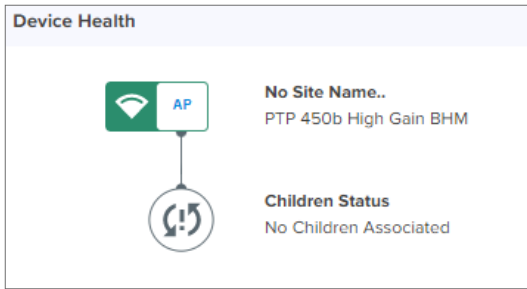
Note

- By default, the application statistics for last 24 hours is displayed.
- Application data is available for a maximum of 30 days.
- Application data is available for NSE and Enterprise Wi-Fi (XD, XE, XR, and XV) devices only.
- Application data is available only for the clients connected to NSE in Essentials accounts.

Device Health

Device Health displays the health of the network from the Tower to the edge Device.

Figure 100 *Device Health*



Connection Health

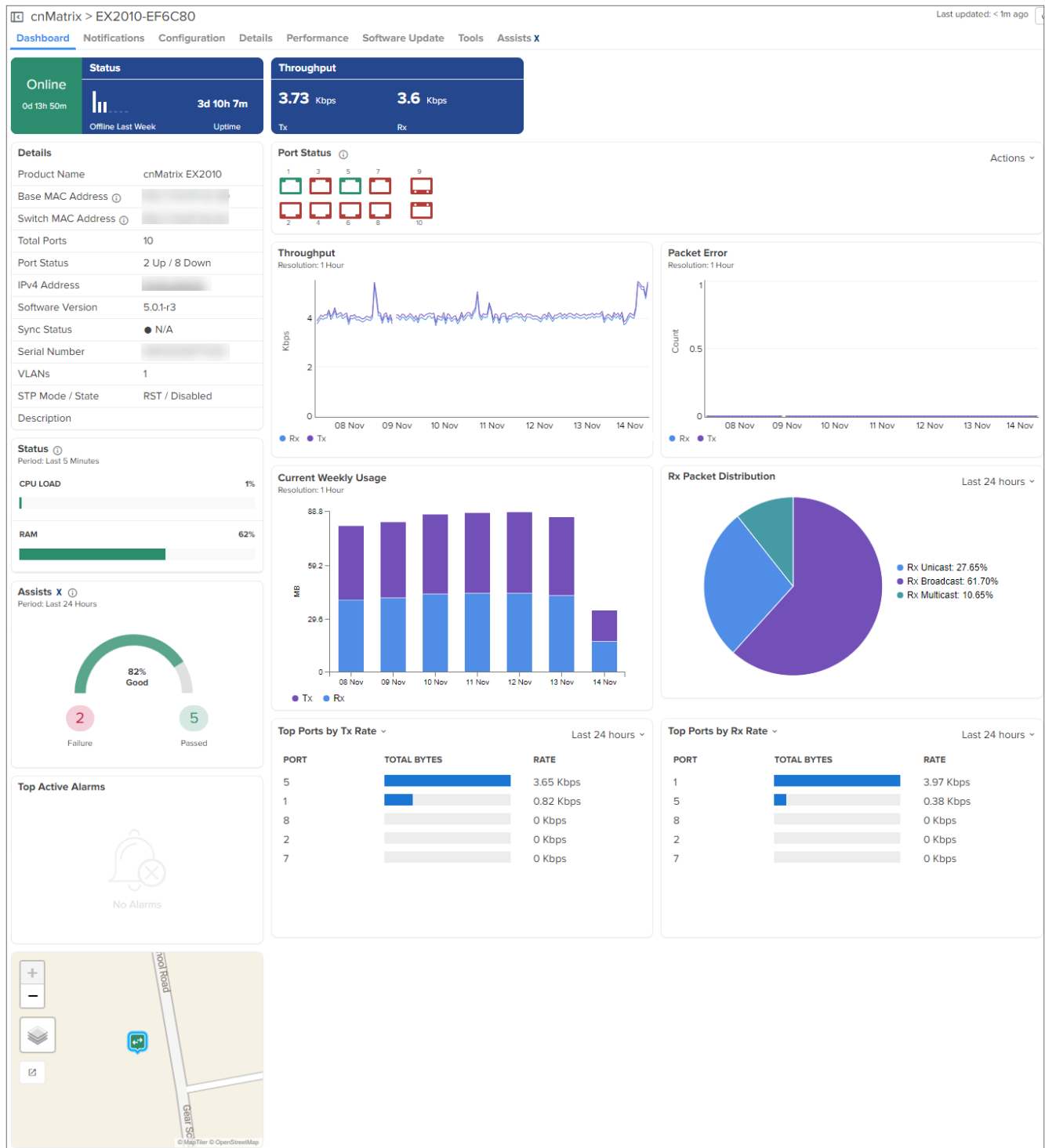
Connection Health displays the health of the devices connected to the network.



Charts and Graphs

Contextual charts and graphs provide details on important dashboard metrics.

Figure 101 *Charts and Graphs*



Notifications

The **Notifications** page displays details of alarms, alarm history, and events. These are synchronous messages that provide real-time system status.

Table 19 *Notification overview*

Type	Description
Alarms	Alarms indicate state and persist as long as the problematic activity continues; they reflect the current health of the devices in the network.
Alarms History	Expired Alarms are added to the Alarm History. The Alarm History page displays historical active alarm counts.
Events	Events are stateless, transient messages that occur in response to an input or action, such as if the CPU exceeds a threshold or a device association fails. Events are fire-and-forget; they are stored in an Event Table and provide a history of device activity.
Wi-Fi Events	Details of the Wi-Fi events are displayed.

For PTP 820/850 devices, the following two additional notifications are displayed as shown in [Figure 102](#) and [Figure 103](#):

- **Device Alarms** with the following parameters:
 - Alarm ID
 - Severity
 - Origin
 - Description
 - Probable Cause
 - Raised Time
- **Device Events** with the following parameters:
 - Raised Time
 - Sequence Number
 - Severity
 - State
 - Description
 - Origin

Figure 102 *PTP 820/850 Device Alarms*

PTP 820/850 > PTP 820G-10.120.109.111					
Dashboard Notifications Configuration Details Performance Software Update					
Alarms Alarms History Events Device Events Device Alarms					
Alarm ID	Severity	Origin	Description	Probable Cause	Raised Time
907	Critical	Slot: 1	Activation key violation	The configuration doesn't match the acti... View Details	Sat Jul 16 2022 01:16:00 UTC +0530
Showing 1 - 1 Total: 1 10 < Previous 1 Next >					

Figure 103 PTP 820/850 Device Events

Raised Time	Sequence Number	Severity	State	Description	Origin
Aug 13 2022, 01:14	551541	Warning	Event	Configuration file transfer successful	Slot: 1
Aug 13 2022, 01:14	551540	Warning	Event	Configuration file transfer in progress	Slot: 1
Aug 13 2022, 01:14	551539	Warning	Event	User issued command for transfer of configuration file	Slot: 1
Aug 13 2022, 01:14	551538	Warning	Event	Configuration file backup created	Slot: 1
Aug 13 2022, 01:14	551537	Warning	Event	Configuration file number 1 backup generation started	Slot: 1
Aug 11 2022, 23:35	551536	Warning	Event	Configuration file transfer successful	Slot: 1
Aug 11 2022, 23:35	551535	Warning	Event	Configuration file transfer in progress	Slot: 1
Aug 11 2022, 23:35	551534	Warning	Event	User issued command for transfer of configuration file	Slot: 1
Aug 11 2022, 23:35	551533	Warning	Event	Configuration file backup created	Slot: 1
Aug 11 2022, 23:35	551532	Warning	Event	Configuration file number 1 backup generation started	Slot: 1

Showing 1 - 10 Total: 840 10 < Previous 1 2 3 4 5 ... 84 Next >

Clear All

Event/Alarm Source

Identity of the source device for the event or alarm.

Aggregation

Notifications are visible at every level of the device tree. Higher levels consolidate notifications for all devices at lower levels in the hierarchy. For example, the network level displays the events and alarms for all devices within that network. This aggregation is only available for System, Networks, Towers, and Sites. When a device is selected, such as an AP, the notifications will only be for it, and not its associated SMs (even though they are lower in the tree).

Storage

Events and Alarms are stored in cnMaestro for an extended period. They will be removed when the total count across the account surpasses 1,000 multiplied by the number of devices in the account. The oldest entries are cleared first.

Events

The Event Table stores a history of the most recent events for the selected node.

Event Severity

Event Severity is mapped to the following levels:

Table 20 Event Severity

	Severity	Definition
	Critical	Catastrophic problem that makes the product/feature unusable.
	Major	Issue that greatly degrades the product/feature, but it is still usable.
	Minor	Limited issue that alters product functionality in a targeted way.
	Notify	Message used primarily for information.

Event Export

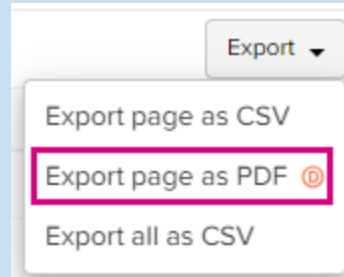
The data in the Event table is exported in a CSV file format. The following export options are available:

- Export page as CSV
- Export all as CSV



Note

The **Export page as PDF** option is deprecated from cnMaestro release version 5.2.0 onwards. This option will be completely removed from the UI in release version 5.3.0.



You can create custom filters for events. To create a custom filter, perform the following steps:

1. In the Events table, click **Apply Filter(s)**.
2. Enter the values in the fields for creating the filters.
3. Click **Apply Filter**.

Figure 104 Events: New Filter

The screenshot shows the 'Events' tab in the application. A modal dialog titled 'Apply Filter(s)' is open, allowing users to create custom filters. The dialog includes the following fields:

- Severity:** A dropdown menu.
- Category:** A dropdown menu.
- Source Type:** A text input with a placeholder 'Select or Search...'.
- Source:** A text input with a search icon and placeholder 'Search'.
- Source MAC:** A text input with a search icon and placeholder 'Search'.
- Name:** A text input with a placeholder 'Select or Search...'.

At the bottom of the dialog are 'Reset' and 'Apply Filter(s)' buttons. In the background, the 'Events' table is visible, showing a list of events with their source IDs (e.g., Cheetah-XV2-22H-B93F, Lynx-XV2-23T-E5E9B6, etc.).

You can manually filter or search by typing parameters in the column header of the Events table.

4. Click **Reset** to reset the filter option in the Events table.
5. Click **Clear Filters** to clear all the filter options.

If you do not receive expected filter details, click **Change Filter(s)** in the Events table to apply new filters.

Figure 105 Events: Source Type filter

The screenshot shows the 'Events' tab in the 'Notifications' section. A dropdown menu is open for the 'Source Type' column header. The menu lists 'Enterprise' and 'Fiber' as main categories. Under 'Enterprise', there are sub-items: 'cnMatrix', 'cnPilot Enterprise (ePM)', 'Enterprise Wi-Fi (E-Seri', 'Enterprise Wi-Fi (XE/XV', 'Enterprise Wi-Fi (Xirrus', and 'Enterprise Wi-Fi (X7-Se'. Under 'Fiber', there is a sub-item: 'Light Speed'. The background table shows columns: Severity, Category, Event Type, Source Type, and Source. The 'Source Type' column has a filter icon.

The **Source Type** column header is grouped based on the Device or System events. The **Name** column header is grouped based on the category names. The category name with corresponding subcategories and codes are shown in [Table 21](#).

Figure 106 Events: Name filter

The screenshot shows the 'Events' tab in the 'Notifications' section. A dropdown menu is open for the 'Name' column header. The menu lists 'Auto Pilot' and 'CBRS' as main categories. Under 'Auto Pilot', there is a sub-item: 'Status'. Under 'CBRS', there are sub-items: 'CBRS Account', 'CBRS Grant', 'Channel Status', 'EIRP Status', 'Payment Events', 'SAS Notifications', and 'Cloud Sum'. The background table shows columns: IPv4 Address, IPv6 Address, Name, and Raised Time. The 'Name' column has a filter icon.

You have an option to delete the event(s). To delete an event(s), select the required event(s) from the table and then click **Delete**.



Note

- You can also delete an event by hovering the cursor over the event and then clicking the delete (🗑️) icon.
- **Monitor** user cannot delete events. Only **Superadmin**, **Admin**, **Operator**, and **CPI** users can delete events.

Figure 107 Events: Delete event(s)

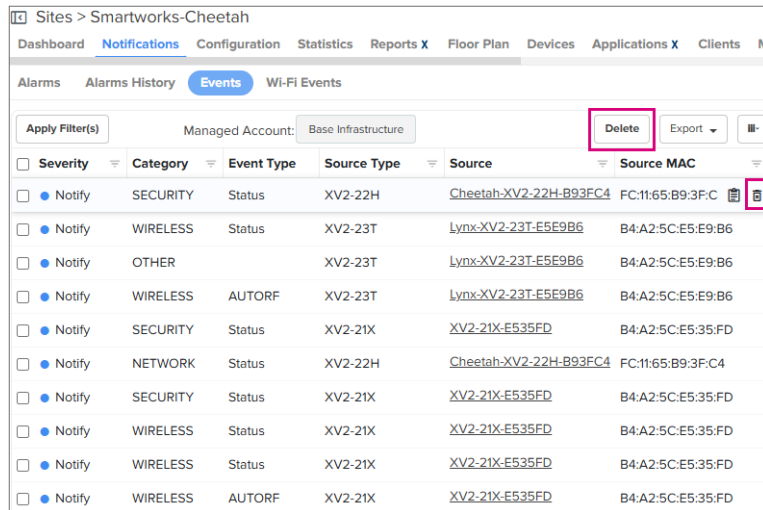


Table 21 Category Names and Codes

Category	Subcategory	Codes
Auto_pilot	Auto Pilot Status	AUTOPILOT_ADDED_AP
		AUTOPILOT_AP_CONNECTED
		AUTOPILOT_AP_DISCONNECTED
		AUTOPILOT_REMOVED_AP
CBRS	CBRS Account	CBRS_ACCOUNT
	CBRS Grant	CBRS_GRANT_TERMINATE
		CBRS_OPERATIONAL_PARAM_CHANGE
		CBRS_GRANT_SUSPEND
		CBRS_TX_ENABLE
		CBRS_TX_DISABLE
		SM_RECONNECT_FAILURE
		CBRS_ATTEMPT_CHANNEL_EXPANSION
		CBRS_START_CHANNEL_HUNT
		CHANNEL_CHANGE
		CBRS_EIRP_CHANGE
		CBRS_ALARM_PROXY_TIME_MISMATCH
	CBRS Payment	CBRS_PAYMENT
	CBRS SAS	SAS_ID_GENERATION
Cloud_Sync	Cloud Connectivity	CLOUD_SYNC

Category	Subcategory	Codes
Configuration	Config Sync	CFG_IMP
		CFG_EXP
		CONFIG_SYNC
		CFG_UPD_ST
		SYSTEM_CONFIG_APPLIED
Device	Configuration	SYSTEM_CFG_FALLBACK_REBOOT
		SYSTEM_CFG_OVERWRITE_REBOOT
		SYSTEM_CONFIG_APPLY_FAIL
		SYSTEM_CONFIG_CAP_POWER
		SYSTEM_CONFIG_DEFAULTED
	Default AUTH Key	DEF_KEY_USED_TRAP
	Device Health	SYS_REB
		SYS_UP
		SA_MODE
		STATUS_DOWN
		STATUS_UP
	Device Status	PMAC_UPD
		THRESH_CPU_UTIL
		THRESH_DEVICE_TRAFFIC
		SYSTEM_CC_NOTSET
		PBA_DYN_DATA
		SYSTEM_AP_UPLINK_STATUS
		IET8222_MPPHSDR_INFO
		IET8222_MPPHSDR_NOTICE
		IET8222_MPPHSDR_WARNING
		CISCO_POWER_SUPPLY_STATUS
		AP_REG
		SYSTEM_RADIOS_ENABLED
		SYSTEM_CRITICAL_LOW_POWER
	Link Status	REGULATORY_FAIL
	Memory	SYSTEM_LOW_MEMORY_RESTART
		SYSTEM_RESTARTING_PROCESS
	Onboarding	ONBOARDING
	SM Events	STA_REG_FAIL
	Smart Antenna Events	BSA_ST
	Watchdog	SYSTEM_WATCHDOG_RESET
		SYSTEM_WATCHDOG_UNRESP
Device_Agent	Device Agent	COLD_START
		WARM_START

Category	Subcategory	Codes
E2E	E2E Events	E2E_CTLR_IMG_UPD
GPS	GPS Status	GPS_SYNC_ST
		GPS_FW_UPD_ST
		GPS_VER
		GPS_SYNC
HA	Cluster Status	HA_STATE_CHANGE
		HA_SERVICE
Mesh	Mesh Events	WIFI_MESH_XTNDED_DEV
		WIFI_MESH_CLIENT_CONNECTED
		WIFI_MESH_CLIENT_DISCONNECTED
		WIFI_MESH_BASE_REC_TRIGGERED
Misc	Others	unknown
Mon8zn	Monetization State Update	SUBSCRIPTION_FEATURE_STATE_CHANGE
		SUBSCRIPTION_STATE_CHANGE
		SUBSCRIPTION_FEATURE_STATE_TRANSITION
	Monetization Subscription State	SUBSCRIPTION_DEFICIT
		SUBSCRIPTION_SLOT_DEFICIT
		SUBSCRIPTION_FEATURE_EXPIRY_NOTICE
Network	DHCP	DHCP_CLIENT_IP
		DHCP_SRV_IP_ASSIGNED
		DHCP_CLIENT_UPD
		DHCP_COMPLETE_EVENT
	Network - Others	NETWORK_INTERFACE_CHANGE
		MGMT_VLAN_CHANGED
		NETWORK_WWAN_DOWN
		NETWORK_WWAN_UP
		NETWORK_WWAN_BACKUP
		NETWORK_STATUS_DOWN
		NETWORK_STATUS_UP
	PPPoE Status	NETWORK_PPPOE_AUTH_FAILED
		NETWORK_PPPOE_CONNECTED
		NETWORK_PPPOE_DISCONNECTED
		NETWORK_RENEW_INTERFACE_IP
		NETWORK_TUNNEL_DOWN
		NETWORK_TUNNEL_UP
Notification	eMail Notifications	SYSTEM_EMAIL_NOTIFICATION

Category	Subcategory	Codes
NSE	Device Status	CONFIG_SYNC
		IPS_THREAT_DETECTED
		WANLB_LINK_UP
		WANLB_LINK_DOWN
		IPS_RULESET_UPDATE_FAILED
		IPS_RULESET_UPDATE
		IPS_START_FAILED
		IPS_INVALID_CONFIG
		SYSTEM_INVALID_LOGIN_ATTEMPT
		WIFI_RADIUS_SERVER_CONFIG_REQUIRED
PTP	Device Status	INCOMPATIBLE_REGULATORY_BANDS
		WIRELESS_LINK_STATUS
		NO_WIRELESS_CHANNEL_AVAILABLE
		SNTP_SYNC
		TDD_SYNC
		UNIT_OUT_OF_CALIBRATION
		CAPACITY_VARIANT_MISMATCH
		INCOMPATIBLE_MASTER_SLAVE
		INSTALL_ARM_STATE
		LICENSE_REMAINING_TRIAL_PERIOD
		LINK_MODE_OPTIMIZATION_MISMATCH
		REGULATORY_BAND
		DFS_IMPULSIVE_INTERFERENCE
		LBT_DETECTED
	Port Status	AUX_PORT_POE_OUTPUT_STATUS
		AUX_PORT_STATUS
		DATA_BRIDGING_STATUS
		MAIN_PSU_PORT_STATUS
		SFP_PORT_STATUS
		AUX_PORT_CONFIG_MISMATCH
		MAIN_PSU_PORT_CONFIG_MISMATCH
		SFP_PORT_CONFIG_MISMATCH
		SFP_ERROR
		PORT_ALLOCATION_MISMATCH

Category	Subcategory	Codes
Radio	DFS	DFS_ST
	Radar	RADAR_DETECT
	Radio Link	LINK_ST
	Radio Performance	RF_OVER_LOAD
	Radio Status	LINK_UP
		LINK_DOWN
Rate_Limit	Status	EVENT_RATELIMIT
		EVENT_BLOCKED
		EVENT_UN_BLOCKED
		METRIC_RATELIMIT
		METRIC_BLOCKED
		METRIC_UN_BLOCKED
		CLIENT_EVENT_RATELIMIT
		CLIENT_EVENT_BLOCKED
		CLIENT_EVENT_UN_BLOCKED
SM	SM Events	STA_REG
		STA_DROP
		STA_REJECT
System	Login	SYSTEM_LOGIN
	Reboot	SYSTEM_ADMIN_REBOOT
	Status	SYSTEM_CPU_UTILIZATION
		SYSTEM_MEMORY_UTILIZATION
		SYSTEM_DISK_UTILIZATION
		DISK_NOT_AVAILABLE_BACKUP
		SYSTEM_BACKUP
		SYSTEM_RESTORE
		SYSTEM_ADD_AP_FIRMWARE
		SYSTEM_PROCESS_STATUS
		AUTHENTICATION_FAILURE
		CAEM_VOLTAGE_NOTIFICATION
	System Metrics	WEAK_ADMIN_PWD
		SYSTEM_INSUFFICIENT_POWER_MITIGATING
Upgrade	Site Upgrade	SITE_SW_SYNC
	Status	SYSTEM_UPGRADE
	Upgrade Fail	SYSTEM_FW_UPGRADE_SUCCESS
	Upgrade Status	FW_UPD_ST
	Upgrade Status	MIN_FW_VER
	Upgrade Success	SYSTEM_FW_UPGRADE_FAILED
Webhook	Web Hook Status	WEBHOOK_NOTIFY

Category	Subcategory	Codes
WiFi	Client Association	WIFI_CLIENT_CONNECTED
		WIFI_CLIENT_DISCONNECTED
	RADIUS Events	WIFI_CLIENT_RADIUS_ACCT_TIMEOUT
		WIFI_CLIENT_RADIUS_AUTH_REJECT
		WIFI_CLIENT_RADIUS_AUTH_SUCCESS
		WIFI_CLIENT_RADIUS_AUTH_TIMEOUT
	Wi-Fi AP Status	THRESH_CLIENT_COUNT
		WIFI_MONITOR_HOST_DOWN
		WIFI_MONITOR_HOST_UP
		SYSTEM
		SECURITY
		SSID
	Wi-Fi Channel	WIFI_NF_CHANNEL_SWITCH
		WIFI_RADAR_DETECTED
		WIFI_ACS_CHANNEL_SWITCH
		WIFI_ACS_TRIGGERED_ON_RADIO
		WIFI_AUTO_DETECT_BACKHAUL
		WIFI_AUTORF_CHANNEL_SWITCH
		WIFI_AUTORF_TRIGGER
		WIFI_AUTORF_TXPOWER
		WIFI_CHANWIDTH_CHANGE
		WIFI_ACS_SELECTED_CHANNEL
		WIFI_ACS_TRIGGERED
	Wi-Fi Client	WIFI_CLIENT_DISCONNECT_INFO
		WIFI_CLIENT_EROAM_DISCONNECTED
		WIFI_CLIENT_GUEST_LOGIN_SUCCESS
		WIFI_CLIENT_GUEST_LOGOUT_SUCCESS
		WIFI_CLIENT_GUEST_SESSION_TIMEOUT
		WIFI_CLIENT_WPA2_INVALID_PSK
		WIFI_DISALLOW_CLIENT
		WIFI_DYN_AUTH_COA_REQ
		WIFI_DYN_AUTH_DISCONNECT_REQ
		WIFI_CLIENT_LDAP_AUTH_REJECT
		WIFI_CLIENT_LDAP_AUTH_SUCCESS
		WIFI_CLIENT_LDAP_AUTH_TIMEOUT
		WIFI_CLIENT

The following table describes the different types of system event categories and their descriptions.

Table 22 System Event Types and Definitions

System Event Category	Description
Infrastructure	Events related to infrastructure management – such as HA setup, interfacing with Message Bus or Database servers, Subscription, etc. Source: cnMaestro
Network	Events related to networking issues, such as link up/down. Source: Devices
Operations	Event related to system-level processes, such as pushing configuration, installing images, etc. Source: Devices
Other	Events related to miscellaneous categories. Source: Devices
Registration	Events related to managing/unmanaged devices. Source: Devices
Security	Events related to logging into the devices, establishing secure links, and potentially recognizing scans and security breaches in the future. Source: cnMaestro, Devices, and Clients
Services	Events related to additional services that may be added to the product in the future. There may not be any services events in the first release. Source: cnMaestro and Devices
Wireless	Events related to issues/notifications with the PTP/PMP radio connectivity, Wi-Fi Clients, etc. Source: Devices and Clients

Alarms

Alarm Life Cycle

The basic alarm life cycle has the following states:

Severity	Source Type	Source	Source MAC	IPv4 Address	IPv6 Address	Name	Message	Duration	Raised Time	Status	Acknowledge
Critical	X7-55X	X7-55X-E03846			N/A	NETWORK_TUNNEL_STATUS	Tunnel(t) went down	3d 2h 23m	14 Apr 2025, 04:54 PM	Active	Acknow
Critical	XV2-2T1	XV2-2T1-300312			N/A	NETWORK_TUNNEL_STATUS	Tunnel(t) went down	22d 18h 31m	26 Mar 2025, 12:47 AM	Active	Acknowledge

Table 23 Alarm Life Cycle

State	Description
Acknowledged	Active alarms can be acknowledged, which signifies they are known and being handled. Acknowledged alarms are not included in the total alarm count.
Active	The alarm remains active until the combination of inputs that generated it are cleared.
Inactive	Inactive alarms remain visible in the active Alarm Table for 10 minutes, before they are moved to Alarm History. An alarm becomes inactive when the inputs that generated it are no longer




Table 23 *Alarm Life Cycle*

State	Description
	present. An Inactive alarm can be pulled back to the Active/Acknowledged states if a new event reactivates the alarm.
Raised	The creation of the alarm.

Alarm Severity

Alarms have a severity that determines how they are handled.

Table 24 *Alarm Severity*

	Severity	Definition
	Critical	Catastrophic problem that makes the product/feature unusable.
	Major	Significant issue that greatly degrades the product/feature, but it is still usable.
	Minor	Limited issue that alters product functionality in a targeted way.

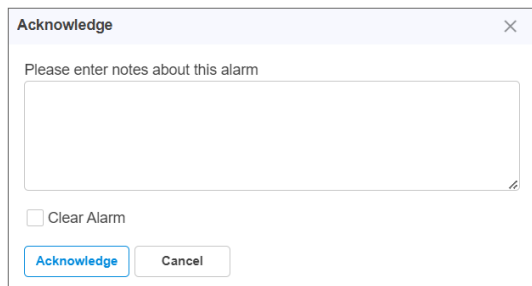
Alarm Types

Table 25 *Alarm Types*

Alarm Type	Definition
Configuration	Issues encountered during a device configuration update.
DFS State	Issues related to DFS operational status.
GPS State	Issues related to GPS synchronization.
Link State	Issues related to the status of device interfaces.
Status	Connectivity between cnMaestro and a device is lost.
Upgrade	Issues encountered during device software upgrade.

Alarm Acknowledgment

Active alarms can be acknowledged in the Alarm Table. Acknowledgment makes the alarm less visible in the table, and the administrator can further add a note describing how the alarm is being resolved. Acknowledging an alarm will also remove it from the alarm counts. You can also select the **Clear Alarm** checkbox to clear the acknowledged alarm when acknowledging the alarms.

Figure 108 *Alarm Acknowledgment*


Alarm Bulk Acknowledgment

To acknowledge multiple alarms at the same time, follow these steps:

1. Navigate to the **Monitor and Manage > Notifications > Alarms** page.

Figure 109 Alarm Bulk Acknowledgment

Severity	Source Type	Source	Source MAC	IPv4 Address	IPv6 Address	Managed Account	Name	Message
Critical	60 GHz cnWave Network	Onboard-81	V5WL00CDWP17	10.10.221.81	N/A	Base Infrastructure	NETWORK_STATUS	Network is dr

Showing 1 - 1 Total: 1 10 Previous 1 Next

2. Select the alarms from the alarms list and then click on the **Bulk Acknowledge** button on the top right corner of the list.
3. Enter **Notes** about the selected alarms.
4. (Optional) Select the **Clear Alarm** checkbox if you would like to remove those alarms from the Alarms list after you acknowledge.
5. Click **Acknowledge**

You can filter the Acknowledged and Unacknowledged devices as shown below:

Severity	Source Type	Source	Source MAC	IPv4 Address	Acknowledge	IPv6 Address	Managed Account	Name
Critical	PMP 450i AP	Scale-AP-185-178	0A...	10.10.185.178	Ack		TEST_ALARM_HIST	SM_REC
Major	60 GHz cnWave V3000 DN	DN2@31fd	00...	-	Ack	3322:2000::1	CnWave_SIT	STATUS
Major	60 GHz cnWave V1000 CN	CN@10bb	00...	-	Ack	2000:1111::1	CnWave_SIT	STATUS
Major	60 GHz cnWave V5000 DN	DN1@3935	00...	-	Acknowledge	2000:1111::1	CnWave_SIT	STATUS
Major	60 GHz cnWave V2000 DN	V2K_DN_d14c	30...	-	Acknowledge	2000:1111::1	CnWave_SIT	STATUS
Major	60 GHz cnWave V5000 DN	PoP3@388b	00...	-	Acknowledge	2000:1111::1	CnWave_SIT	STATUS
Major	60 GHz cnWave V1000 CN	CN@Q359	00...	-	Acknowledge	2000:1111::1	CnWave_SIT	STATUS
Major	60 GHz cnWave V1000 DN	V1KDN_sec1_DN1	00...	-	Acknowledge	2000:1111::1	CnWave_SIT	STATUS
Major	60 GHz cnWave V3000 DN	PoP2@346c	00...	-	Acknowledge	2000:1111::1	CnWave_SIT	STATUS
Major	60 GHz cnWave V1000 CN	CN2@Q14f	00...	-	Acknowledge	2000:1111::1	CnWave_SIT	STATUS

Showing 1 - 10 Total: 24 10 Previous 1 2 3 Next



Note

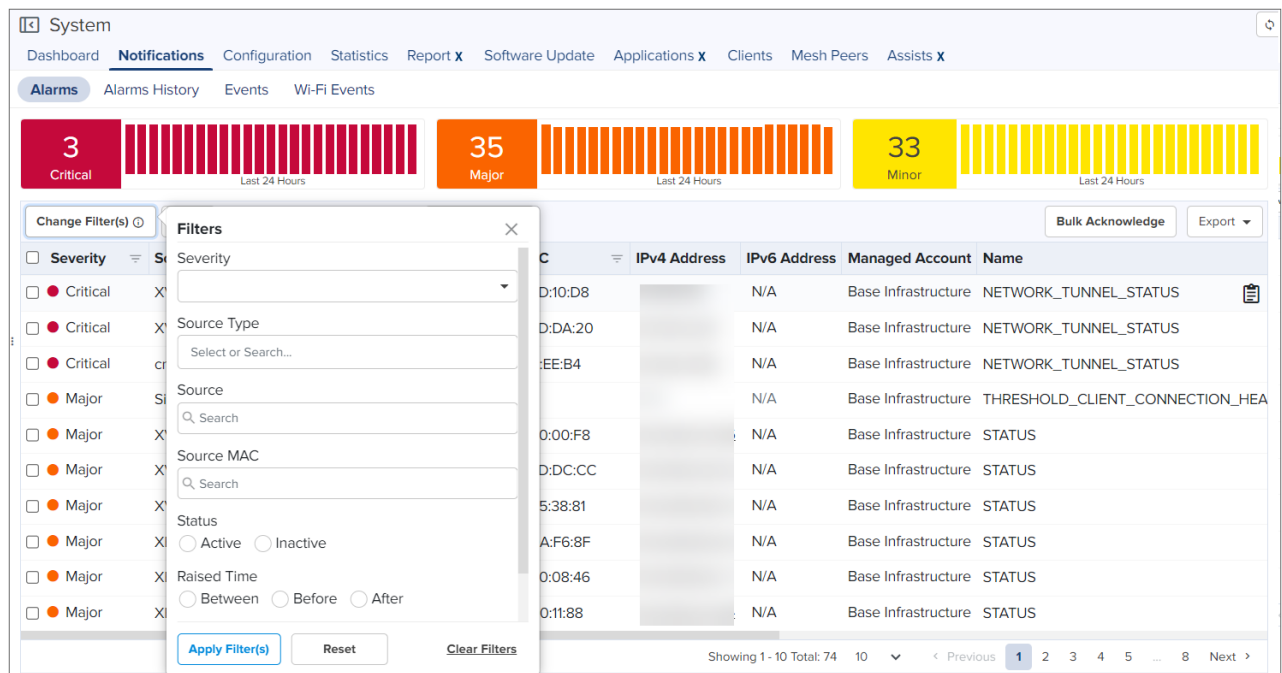
Acknowledged alarms are not shown in **Top Active Alarms**.

Alarm filters

You can create custom filters for **Alarms**. To create a custom filter, perform the following steps:

1. In the **Alarms** table, click **Apply Filter(s)**.
2. Enter the values in the fields for creating the filters.
3. Click **Apply Filter**.

Figure 110 Alarms: New Filter



You can manually filter or search by typing parameters in the column header of the Alarms table.

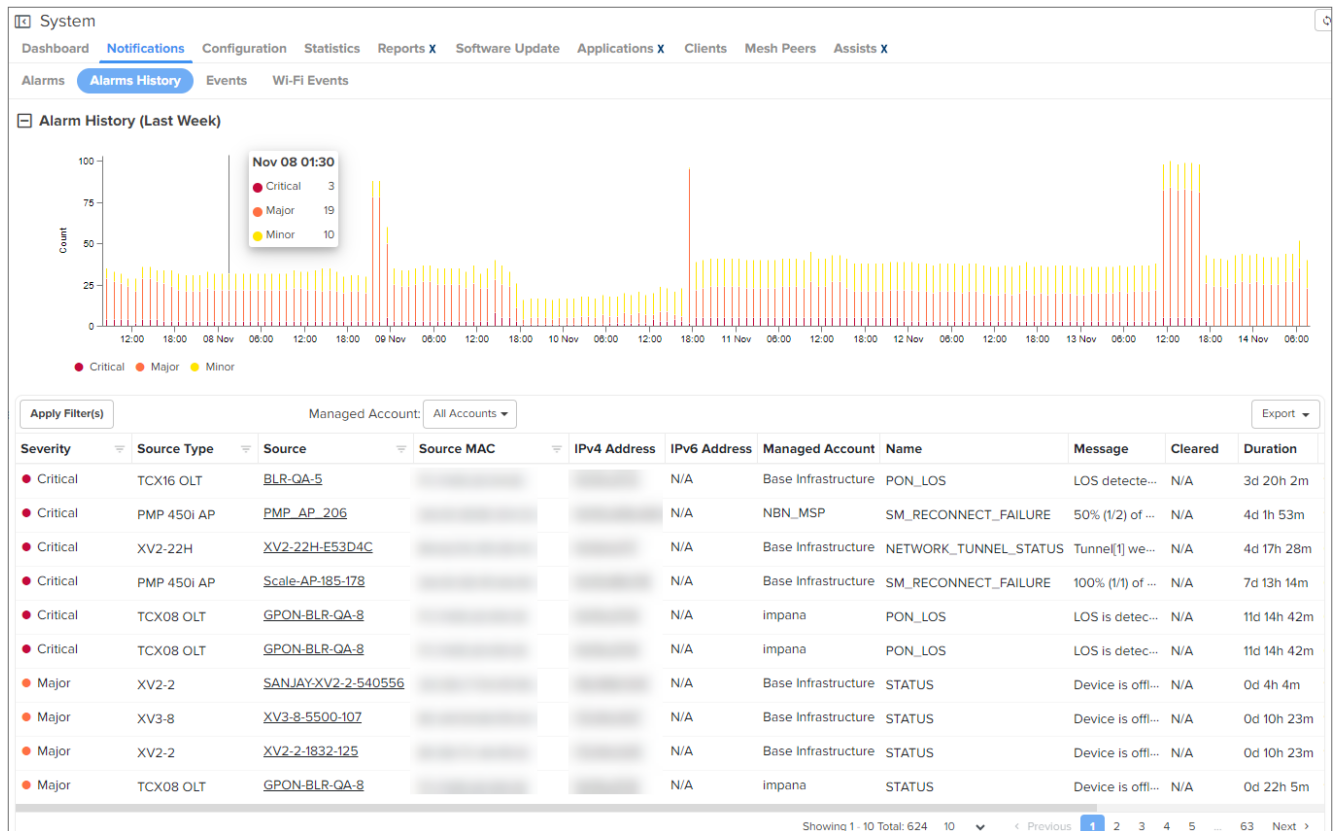
4. Click **Reset** to reset the filter option in the Alarms filter.
5. Click **Clear Filters** to clear all the filter options.

If you do not receive expected filter details, click **Change Filter(s)** in the Alarms table to apply new filters.

Alarm History

Expired Alarms are added to the Alarm History. The Alarm History displays historical active alarm counts. Clicking the bar chart filters the table data underneath, allowing you to view which alarms were active at a specific time in the past.

Figure 111 Alarm History



Alarm History filters

You can create custom filters for **Alarms History**. To create a custom filter, perform the following steps:

1. In the **Alarms History** table, click **Apply Filter(s)**.
2. Enter the values in the fields for creating the filters.
3. Click **Apply Filter**.

Figure 112 Alarm History: New Filter

The screenshot shows the 'Alarm History' page in the System interface. A filter dialog box is open, allowing users to filter alarms by Severity, Source Type, Source, Source MAC, Raised Time, and Status. The background table shows columns for MAC, IPv4 Address, IPv6 Address, Managed Account, and Name. The table is currently displaying several rows of network-related events.

You can manually filter or search by typing parameters in the column header of the Alarm History table.

4. Click **Reset** to reset the filter option in the Alarms History filter.
5. Click **Clear Filters** to clear all the filter options.

If you do not receive expected filter details, click **Change Filter(s)** in the Alarm History table to apply new filters.

Wi-Fi Events

Wi-Fi Events are listed as below:

The screenshot shows the 'Wi-Fi Events' page in the System interface. The table lists various Wi-Fi events with columns for Source, Managed Account, Source MAC, Source Name, Client Name, Client MAC, Name, and Raised Time. The events include connections and disconnections for various clients.

Source	Managed Account	Source MAC	Source Name	Client Name	Client MAC	Name	Raised Time
XV3-8-4DDADC_rajaj	Base Infrastructure	BC:56:30:4D:DA:DC	XV3-8	IN01-DK51LR2	64:5D:86:64:26:3D	WIFI_CLIENT_CONNECTED	03 Aug 2023
XV3-8-4DDADC_rajaj	Base Infrastructure	BC:56:30:4D:DA:DC	XV3-8	IN01-DK51LR2	64:5D:86:64:26:3D	WIFI_CLIENT_CONNECTED	03 Aug 2023
XV3-8-5500-107	Base Infrastructure	BC:56:30:4D:DA:DC	XV3-8	1A-9B:56:F5:07:3A	1A:9B:56:F5:07:3A	WIFI_CLIENT_CONNECTION_FAILED	03 Aug 2023
XV2_23T_Permanent_Client_DND	Base Infrastructure	BC:56:30:4D:DA:DC	XV2-23T	Galaxy-M04_Lynx_02	06:5B:56:F5:07:3A	WIFI_CLIENT_DISCONNECTED	03 Aug 2023
XV2_23T_Permanent_Client_DND	Base Infrastructure	BC:56:30:4D:DA:DC	XV2-23T	Galaxy-M04_Lynx_02	06:5B:56:F5:07:3A	WIFI_CLIENT_DISCONNECTED	03 Aug 2023
XV3-8-4DDADC_rajaj	Base Infrastructure	BC:56:30:4D:DA:DC	XV3-8	IN01-DK51LR2	64:5D:86:64:26:3D	WIFI_CLIENT_CONNECTED	03 Aug 2023
XV3-8-4DDADC_rajaj	Base Infrastructure	BC:56:30:4D:DA:DC	XV3-8	IN01-DK51LR2	64:5D:86:64:26:3D	WIFI_CLIENT_CONNECTED	03 Aug 2023
XV2_23T_Permanent_Client_DND	Base Infrastructure	BC:56:30:4D:DA:DC	XV2-23T	Lynx_01_Galaxy-M04_01	72:5B:56:F5:07:3A	WIFI_CLIENT_DISCONNECTED	03 Aug 2023
XV2_23T_Permanent_Client_DND	Base Infrastructure	BC:56:30:4D:DA:DC	XV2-23T	Lynx_01_Galaxy-M04_01	72:5B:56:F5:07:3A	WIFI_CLIENT_DISCONNECTED	03 Aug 2023
XE5_Permanent_Client_DND	Base Infrastructure	BC:56:30:4D:DA:DC	XE5-8	Sekhar_Laptop	28:5B:56:F5:07:3A	WIFI_CLIENT_CONNECTION_FAILED	03 Aug 2023

Configuration

The **Configuration** page allows you to configure the device settings.

cnWave 5G Fixed:

For the cnWave 5G Fixed products (BTS and CPE), the **Configuration** page allows you to add or modify the device details and view the existing device configuration. [Figure 113](#) is an example of the **Configuration** page for the cnWave 5G Fixed BTS product.

Figure 113 The Configuration page - BTS

The screenshot shows the 'Configuration' page for a device named 'BTS > BTS-UK-RIG'. The page has tabs for Dashboard, Notifications, Configuration (selected), Details, CPEs, Performance, Software Update, Tools, and Assists X. The 'Device Details' section includes fields for Managed Account (Base Infrastructure, Change), Name (BTS-UK-RIG), Network (default), Tower (None), Latitude, Longitude, Altitude (0.0), Azimuth (15.0), and Antenna Tilt (25.0). The 'Device Configuration' section shows a Template dropdown set to 'None' and a note about modifying settings. A table below shows 'No variables configured'. An 'Apply Configuration' button is at the bottom.

[Table 26](#) lists and describes parameters available on the **Configuration** page for the cnWave 5G Fixed products (BTS and CPE).

Table 26 List of parameters on the Configuration page

Parameter	Description
Device Details	
Managed Account	Allows you to view the device user account name. For the BTS product, you can change the managed account information. When you click on Change , the Change Managed Account box appears providing options to modify the managed account name, network, and tower details. The Change option is not available for CPE.
Name	Name of the device (BTS or CPE). This text box allows a maximum of 64 characters.
Network	Name of the network where the BTS device is available. Note: This parameter is disabled for the CPE specific settings.
Tower	Name of the antenna tower where the BTS device is located. Note: This parameter is disabled for the CPE specific settings.
Latitude	The geographic latitude of the device (BTS or CPE) in decimal degrees (DD). Note: This parameter supports values in signed degrees format (DDD.dddd).

Table 26 List of parameters on the Configuration page

Parameter	Description
	Example: 41.25 and -31.96 (Min =90 and Max=90)
Longitude	The geographic longitude of the device (BTS or CPE) in DD. Note: This parameter supports values in signed degrees format (DDD.dddd). Example: -31.96 and 115.84 (Min =180 and Max=180)
Altitude	Altitude (in metres) of the geographical location of the BTS device (Min =0 and Max=500). This parameter is available only for the BTS.
Azimuth	The direction in azimuth that the BTS is pointing towards. This parameter allows values in degrees from North (0 to 300). It is applicable only to the BTS.
Antenna Tilt	The tilt angle (in degrees) of the BTS antenna. This parameter allows values in degrees from horizon (-90 to 90). A positive value indicates that the antenna is pointing above the horizon. It is applicable only to the BTS.
Serial Number	The serial number of the device.
MAC Address	The Ethernet Media Access Control (MAC) address that is assigned to the network interface and used for the device management.
IPv4 Address	The IPv4 address that is set for the BTS or the CPE device.
Device Configuration: Allows you to view the existing device configuration.	
Template	An option to select and view the configuration templates. If you modify any parameters in the template (such as polarization, bandwidth, or link symmetry), the device automatically reboots.
Apply Configuration	An option to submit or apply the new configuration changes.

Statistics and Details

The **Statistics** page provide a tabular aggregation of data, including general information on the devices monitored, as well as wireless, network, and traffic metrics. The **Details** pages, however, provide information on a single device.

This section contains information about the following topics:

- [Statistics page](#)
- [Details page](#)

Statistics page

The following table highlights information that is displayed in the **Statistics** page at the System, MSP, Network, Tower, and Site-levels:

Table 27 Device Statistics

Device Type	Statistics Page Information
60 GHz cnWave Nodes	General <ul style="list-style-type: none"> • Device • IPv6 Address

Table 27 *Device Statistics*

Device Type	Statistics Page Information
	<ul style="list-style-type: none"> • MAC • Mode • Model • PoP Node • Serial Number • Site • Software Version • Status • Status Time • Network • Zone <p>GPS</p> <ul style="list-style-type: none"> • Fix Type • Height • Latitude • Longitude • Satellites Tracked • Sync Mode <p>Network</p> <ul style="list-style-type: none"> • Ethernet Throughput (Rx) • Ethernet Throughput (Tx) • Main Aux SFP • Radios • Sector Throughput (Rx) • Sector Throughput (Tx)
cnMatrix	<p>General</p> <ul style="list-style-type: none"> • Device Name • IPv4 Address • IPv6 Address • MAC Address • Network • Product Name • Serial Number • Status

Table 27 *Device Statistics*

Device Type	Statistics Page Information
	<ul style="list-style-type: none"> • Tower/Site Traffic <ul style="list-style-type: none"> • Throughput (DL) • Throughput (Rx)
cnPilot Home	General <ul style="list-style-type: none"> • AP Group • Device Name • IPv4 Address • IPv6 Address • MAC Address • Network • Product Name • Serial Number • Status • Tower/Site Wireless <ul style="list-style-type: none"> • Radios
cnRanger BBU	General <ul style="list-style-type: none"> • Device Name • IPv4 Address • IPv6 Address • MAC Address • Network • Registered SM Count • Serial Number • Status • Tower/Site Wireless <ul style="list-style-type: none"> • Radios
cnRanger SM	General <ul style="list-style-type: none"> • Device Name • IPv4 Address • IPv6 Address

Table 27 *Device Statistics*

Device Type	Statistics Page Information
	<ul style="list-style-type: none"> • MAC Address • Network • Serial Number • Status • Tower/Site Wireless <ul style="list-style-type: none"> • Radios
cnReach	General <ul style="list-style-type: none"> • Device • IPv4 Address • IPv6 Address • MAC • Network • Radio • Status • Tower/Site
cnReach XIO	General <ul style="list-style-type: none"> • Active S/W Version • Device • IPv4 Address • IPv6 Address • MAC • Network • Product Name • Serial Number • Status • Tower/Site
cnVision Client	General <ul style="list-style-type: none"> • Device Name • Distance • IPv4 Address • IPv6 Address • MAC Address • Network

Table 27 *Device Statistics*

Device Type	Statistics Page Information
	<ul style="list-style-type: none"> • Serial Number • Session Time • Status • Tower/Site <p>Network</p> <ul style="list-style-type: none"> • LAN Interface • LAN Interface 2 • WAN IP Address <p>Wireless</p> <ul style="list-style-type: none"> • Antenna Gain • Connected AP • Radios
cnVision Hub	<p>General</p> <ul style="list-style-type: none"> • Device Name • IPv4 Address • IPv6 Address • MAC Address • Network • Registered SM Count • Serial Number • Status • Tower/Site <p>Network</p> <ul style="list-style-type: none"> • LAN Interface • LAN Interface 2 <p>Wireless</p> <ul style="list-style-type: none"> • Antenna Gain • DL/UL Ratio • Max Range • Radios
cnWave 5G Fixed BTS	<p>Overview</p> <ul style="list-style-type: none"> • Device Name • MAC

Table 27 *Device Statistics*

Device Type	Statistics Page Information
	<ul style="list-style-type: none"> • IPv4 Address • Network • Status • Tower/Site <p>Radio Details: Radio status of the BTS device</p> <ul style="list-style-type: none"> • Bandwidth • Frequency (MHz) • Link Symmetry • Max EIRP (dBm) • Polarization • Registered CPEs • SFP1 Speed • SFP2 Speed • UL Target Rx Power (dBm) • UL Tx Pwr Ctrl Initial Adjust • UL Tx Pwr Ctrl Cont Adjust
cnWave 5G Fixed CPE	<p>Overview</p> <ul style="list-style-type: none"> • Device Name • CRNTI • IMSI • IPv4 Address • Link Uptime • MAC • Network • Registration Count • Registration State • Status • Tower/Site <p>Radio Details</p> <ul style="list-style-type: none"> • Alignment Active • Current EIRP (dBm) • DL Backoff (dB) • DL Channel Distortion (dB) • DL EVM (dB)

Table 27 *Device Statistics*

Device Type	Statistics Page Information
	<ul style="list-style-type: none"> • DL MCS • DL Rx Power (dBm) • DL Sounding State • DL Spatial Frequency • Polarization • Range (km) • UL Backoff (dB) • UL Channel Distortion (dB) • UL EVM (dB) • UL MCS • UL Rx Power (dBm) • UL Sounding State • UL Spatial Frequency
Enterprise Wi-Fi	<p>General</p> <ul style="list-style-type: none"> • AP Group • Device Name • IPv4 Address • IPv6 Address • MAC Address • Network • Product Name • Serial Number • Status • Tower/Site <p>Wireless</p> <ul style="list-style-type: none"> • Radios
ePMP AP	<p>General</p> <ul style="list-style-type: none"> • Device Name • IPv4 Address • IPv6 Address • MAC Address • Network • Registered SM Count • Serial Number

Table 27 *Device Statistics*

Device Type	Statistics Page Information
	<ul style="list-style-type: none"> • Status • Tower/Site <p>Network</p> <ul style="list-style-type: none"> • LAN Interface • LAN Interface 2 <p>Wireless</p> <ul style="list-style-type: none"> • Antenna Gain • DL/UL Ratio • Max Range • Radios
ePMP SM	<p>General</p> <ul style="list-style-type: none"> • Device Name • Distance • IPv4 Address • IPv6 Address • MAC Address • Network • Serial Number • Session Time • Status • Tower/Site <p>Network</p> <ul style="list-style-type: none"> • LAN Interface • LAN Interface 2 • WAN IP Address <p>Wireless</p> <ul style="list-style-type: none"> • Antenna Gain • Connected AP • Radios
PMP AP	<p>General</p> <ul style="list-style-type: none"> • Device Name • IPv4 Address • IPv6 Address

Table 27 *Device Statistics*

Device Type	Statistics Page Information
	<ul style="list-style-type: none"> • MAC Address • Network • Registered SM Count • Serial Number • Status • Tower/Site <p>Network</p> <ul style="list-style-type: none"> • LAN Interface <p>Traffic</p> <ul style="list-style-type: none"> • Busy Index (DL) • Busy Index (UL) <p>Wireless</p> <ul style="list-style-type: none"> • Antenna Gain • Color Code • DL/UL Ratio • Max Range • Radios
PMP SM	<p>General</p> <ul style="list-style-type: none"> • Device Name • Distance • IPv4 Address • IPv6 Address • MAC Address • Network • Serial Number • Session Time • Status • Tower/Site <p>Network</p> <ul style="list-style-type: none"> • LAN Interface • WAN IP Address <p>Wireless</p> <ul style="list-style-type: none"> • Actual Average EVM (DL)

Table 27 *Device Statistics*

Device Type	Statistics Page Information
	<ul style="list-style-type: none"> • Actual Average EVM (UL) • Antenna Gain • BER (Average) • Color Code • Connected AP • LUID • Radios
PTP 650/670/700	<p>System</p> <ul style="list-style-type: none"> • Device Name • IPv4 Address • IPv6 Address • MAC Address • Network • Product Name • Status • Tower/Site <p>Network</p> <ul style="list-style-type: none"> • Aux Interface • Main PSU Interface • SFP Interface <p>Wireless</p> <ul style="list-style-type: none"> • Antenna Gain • Errored Seconds • Licensed Country • Radios • Severely Errored Seconds • Unavailable Seconds
PTP 820/850	<p>General</p> <ul style="list-style-type: none"> • Device Name • Edge Controller • IPv4 Address • IPv6 Address • MAC Address • Model

Table 27 *Device Statistics*

Device Type	Statistics Page Information
	<ul style="list-style-type: none"> • Network • Radios • Serial Number • Status • Tower/Site
RV22 Home Mesh	<p>General</p> <ul style="list-style-type: none"> • Device Name • IPv4 Address • IPv6 Address • MAC Address • Network • Product Name • Serial Number • Status • Tower/Site <p>Wireless</p> <ul style="list-style-type: none"> • Radios

Details page

The **Details** page displays device-specific information, such as system info, radio parameters, and software versions.

The **Details** page is provided for the following devices:

- [60 GHz cnWave](#)
- [cnMatrix](#)
- [cnPilot Home](#)
- [cnRanger BBU](#)
- [cnRanger SM](#)
- [cnReach](#)
- [cnVision Client](#)
- [cnVision Hub](#)
- [cnWave 5G Fixed Details](#)
 - [cnWave 5G Fixed BTS](#)
 - [cnWave 5G Fixed CPE](#)
- [Enterprise Wi-Fi AP \(XE-, XV-, and X7-Series\)](#)
- [ePMP AP](#)

- [PMP AP](#)
- [PMP SM](#)
- [PON \(OLT\)](#)
- [PTP 650/670/700](#)
- [PTP 820/850 Details](#)
- [Home Mesh Routers](#)

60 GHz cnWave

The **Details** section displays following tabs for 60 GHz cnWave:

- Overview
- Network Info

Overview

Figure 114 60 GHz cnWave: Device > Details > Overview

60 GHz cnWave > V5K DN

Dashboard

Notifications

Configuration

Links

Details

Performance

Software Update

Tools

Overview

Network

System

Name	V5K DN
Product Name	60 GHz cnWave V5000 DN
MAC Address	
Health	Online (10d 6h 45m)
IPv6 Address	
Software Version	1.3.3
Firmware Version	10.11.0.98
Serial Number	
Onboard Date	Apr 27, 2024 07:27
Sync Mode	GPS

GPS

Latitude	
Longitude	
Height	930 m
Fix Num Sat	15
Fix Type	3D

Links

	Wireless	Wired
Total	2	0
Active	2	0

Sectors

	Sector 1	Sector 2
MAC Address		
Channel	3	3
Links	2	0
Rx Packets	4796698	0
Tx Packets	5249366	0
Security	None	None
Error Association	0	0
Channel Last State	0	0

Software Update

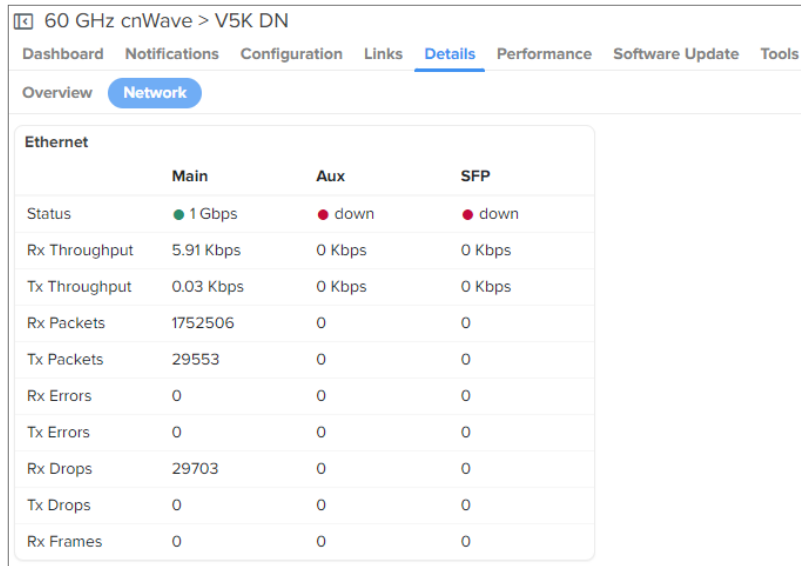
Software Version	1.3.3
------------------	-------

History

Date	Status	Version
12 Jun 2024, 06:26 PM	Success	1.3.3
06 Jun 2024, 04:07 PM	Success	1.4-beta1
14 May 2024, 12:42 PM	Success	1.4-dev25

Network Info

Figure 115 60 GHz cnWave: Device > Details > Network Info



	Main	Aux	SFP
Status	● 1 Gbps	● down	● down
Rx Throughput	5.91 Kbps	0 Kbps	0 Kbps
Tx Throughput	0.03 Kbps	0 Kbps	0 Kbps
Rx Packets	1752506	0	0
Tx Packets	29553	0	0
Rx Errors	0	0	0
Tx Errors	0	0	0
Rx Drops	29703	0	0
Tx Drops	0	0	0
Rx Frames	0	0	0

cnMatrix

The **Details** section displays following tabs for cnMatrix:

- Overview
- Topology
- Port Statistics

Overview

Figure 116 *cnMatrix: Device > Details > Overview*

cnMatrix > EX3028RP-A5D7C0

Dashboard

Notifications

Configuration

Details

Performance

Software Update

Tools

Assists X

Overview

Topology

Port Statistics

System

Name

EX3028RP-A5D7C0

Device Type

cnMatrix EX3028R-P

System Uptime

23d 6h 52m

Coordinates

[0, 0]

Description

Hardware

Ethernet switch 12 copper 1G ports (60w4PPoE), 12 copper 2.5G ports with POE+ and 4 SFP+ 10G ports, with 4PPoE and removable power supply

Hardware Version

01

DA Version

4.14

Manufacture Date

2023-07-14

Onboard Date

Jun 11 2024 20:04:26

Last Reboot

Tue Mar 26 2024 11:36 (cnMaestro initiated configuration update)

Software Update

Active Software Version

5.0.2-r4

History

Date	Status	Version
22 Jun 2024, 08:39 PM	● Skipped	5.0.2-r4

Configuration Update

History

Date	Status	Template
------	--------	----------

Configuration History Unavailable

Topology

Figure 117 *cnMatrix: Device > Details > Topology*

cnMatrix > EX3028RP-A5D7C0

Dashboard

Notifications

Configuration

Details

Performance

Software Update

Tools

Assists X

Overview

Topology

Port Statistics

Apply Filter(s)

ID	Name	Chassis ID	Description	MAC Address	IPv4 Address
GI0/1	EX3052RP-A5F480-UpLink-DND		Cambium Networks cnMatrix EX3052R-P Ethernet Switch HW:01 SW:5.0.1-r4		10.110.166.2

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

Port Statistics

Figure 118 *cnMatrix: Device > Details > Port Statistics*

cnMatrix > EX3028RP-A5D7C0

Dashboard Notifications Configuration **Details** Performance Software Update Tools Assists X

Overview Topology **Port Statistics**

Apply Filter(s)

Port	Switch	Tags	Description	Rx Unicast Pkts	Rx Multicast Pkts	Rx Broadcast Pkts	Rx Errors	Rx Total Pkts	Tx Errors	Tx Total Pkts	Link Transitions
Gi0/1	EX3028RP-A5D7C0	-	EX3052RP-A5F480-UpLink-DND	244703	73878	69494	0	388075	0	498981	1
Gi0/2	EX3028RP-A5D7C0	-		0	0	0	0	0	0	0	0
Gi0/3	EX3028RP-A5D7C0	-		0	0	0	0	0	0	0	0
Gi0/4	EX3028RP-A5D7C0	-		0	0	0	0	0	0	0	0
Gi0/5	EX3028RP-A5D7C0	-		0	0	0	0	0	0	0	0
Gi0/6	EX3028RP-A5D7C0	-		0	0	0	0	0	0	0	0
Gi0/7	EX3028RP-A5D7C0	-		0	0	0	0	0	0	0	0
Gi0/8	EX3028RP-A5D7C0	-		0	0	0	0	0	0	0	0
Gi0/9	EX3028RP-A5D7C0	-		0	0	0	0	0	0	0	0
Gi0/10	EX3028RP-A5D7C0	-		0	0	0	0	0	0	0	0

Showing 1 - 10 Total: 28 10 < Previous 1 2 3 Next >

cnPilot Home

The **Details** section displays following tabs for cnPilot Home:

- Overview
- Network Info

Overview

Figure 119 *cnPilot Home: Device > Details > Overview*

Wi-Fi > Migration_04_R195W_02

DashboardNotificationsConfigurationDetailsPerformanceSoftware UpdateToolsClientsWLANsAssists X

OverviewNetwork Info

System

Device	Migration_04_R195W_02
Product Name	cnPilot r195W
Health	● Online (9d 10h 19m)
IPv4 Address	10.10.209.224
MAC Address	
Description	
Serial Number	
Hardware	V4.3
DA Version	3.43
Last Reboot	Tue Jun 25 2024 11:28 (cnMaestro initiated configuration update)
Location	
Onboard Date	Jun 24 2024 16:30:26
Available Memory	39%
CPU Utilization	7%

Configuration Update

History

Date	Status	AP Group
25 Jun 2024, 11:28 AM	● Success	CNM_SIT_R-S...
24 Jun 2024, 09:53 PM	● Success	CNM_SIT_R-S...

Radio Details

Radio	Radio 1	Radio 2
Band	2.4 GHz	5 GHz
Channel	1	40
Channel Width	MHz	MHz
Power	6 %	6 %
Clients	0	0
UL Throughput	0 Kbps	0 Kbps
DL Throughput	0 Kbps	0 Kbps

Software Update

Active Software Version	4.8-R15
Inactive Software Version	N/A

History

Date	Status	Version
------	--------	---------

Version History Unavailable

Network Info

Figure 120 *cnPilot Home: Device > Details > Network Info*

Wi-Fi > Migration_04_R195W_02

DashboardNotificationsConfigurationDetailsPerformanceSoftware UpdateToolsClientsWLANsAssists X

OverviewNetwork Info

Ethernet Ports

Type	Tx Bytes	Rx Bytes	Tx Packets	Rx Packets	Tx Error Bytes	Rx Error Bytes
WAN	10284044	533791444	81501	2185448	0	0
LAN 1	0	0	0	0	0	0
LAN 2	0	0	0	0	0	0
LAN 3	0	0	0	0	0	0
LAN 4	0	0	0	0	0	0

FXS Ports

Type	SIP Account Status	Phone Number	Hook State
FXS 1	Disable	-	On
FXS 2	Disable	-	On

cnRanger BBU

The **Details** section displays following tabs for cnRanger BBU:

- Overview

Overview

Figure 121 *cnRanger BBU: Device > Details > Overview*

The screenshot shows the 'Overview' tab for a cnRanger BBU device. The page is titled 'BBU > Migration-cnRanger-sierra-800-02'. The navigation bar includes 'Dashboard', 'Notifications', 'Configuration', 'Details' (active), 'SMs', 'Performance', 'Software Update', and 'Tools'. The 'Overview' tab is selected. The page is divided into several sections: 'System', 'Network', 'GPS Sync', 'Software Update', and 'History'.

System	
Name	Migration-cnRanger-sierra-800-02
Device Type	Sierra 800
System Uptime	30d 10h 14m
Coordinates	[0, 0]
Description	
Hardware	Sierra 800
DA Version	2.106
Onboard Date	Jun 12 2024 11:16:35
Available Memory	68%
CPU Core Utilization	32%, 2%, 12%, 44%

Network	
LAN MAC	
IPv4 Address	10.110.209.201
Subnet Mask	255.255.255.0
Bridge Mode	Enabled

GPS Sync	
Source	Free Run
Status	Up
Software Version	AXN_5.1.1
Sync Lost Count	58

Software Update	
Active Software Version	2.1.2.0-r7
Inactive Software Version	0.0.0.9

History		
Date	Status	Version
Version History Unavailable		

cnRanger SM

The **Details** section displays following tabs for cnRanger SM:

- Overview

Overview

Figure 122 *cnRanger SM: Device > Details > Overview*

The screenshot displays the 'Overview' tab for a 'cnRanger SM' device. The page has a navigation bar with tabs: Dashboard, Notifications, Configuration, Details (active), Performance, Software Update, and Tools. Below the navigation bar is a sub-tab 'Overview'. The main content area is divided into four sections: System, Network, Software Update, and Wireless.

System	
Name	Migration-cnRanger-101-SM-02
Device Type	2GHz cnRanger 201 SM
System Uptime	1d 9h 4m
Coordinates	[0, 0]
Description	
Hardware	2GHz cnRanger 201 SM
DA Version	2.106
Onboard Date	Jul 02 2024 16:09:09
Available Memory	73%
CPU Utilization	0%

Network	
LAN MAC	[Redacted]
Ethernet Interface	Unknown
IPv4 Address	10.110.209.207
Subnet Mask	255.255.255.0
Operating Mode	NAT
Gateway	0.0.0.0
DNS Server(s)	[Redacted]

Wireless	
Operating Frequency	2620 MHz
Channel Bandwidth	20 MHz
Transmitter Output Power	-19.5 dBm
RRH MAC	[Redacted]
ECGI	[Redacted]

Software Update		
Active Software Version	2.1.2.0-r9	
Inactive Software Version	2.1.2.0-r7	

History		
Date	Status	Version
03 Jul 2024, 12:20 PM	Success	2.1.2.0-r9
03 Jul 2024, 11:01 AM	Success	2.1.2.0-r7
02 Jul 2024, 04:19 PM	Success	2.1.2.0-r9

cnRanger RRH

The **Details** section displays following tabs for cnRanger RRH:

- Overview

Overview

Figure 123 *cnRanger RRH: Device > Details > Overview*

The screenshot displays the 'Overview' tab for a 'cnRanger RRH' device. The page has a navigation bar with tabs: Dashboard, Notifications, Configuration, Details (active), and Performance. Below the navigation bar is a sub-tab 'Overview'. The main content area is divided into three sections: System, Network, and Wireless.

System	
Name	Migration-cnRanger-sierra-800-02:RRH-1
Device Type	2GHz cnRanger 220 RRH
System Uptime	23d 8h 42m
Description	
Onboard Date	Jun 12 2024 11:16:35
CPU Utilization	6.0%

Network	
LAN MAC	[Redacted]

Wireless	
Operating Frequency	2610 MHz
Channel Bandwidth	20 MHz
Transmitter Output Power	33 dBm
External Antenna Gain	17 dBi
Internal Antenna Gain	
Height	5
Azimuth	6 degree

cnReach

The **Details** section displays following tabs for cnReach:

- Overview
- Interfaces
- Neighbors
- Radio 1 (BHM) Children

Overview

Figure 124 *cnReach: Device > Details > Overview*

cnReach > cnReach_Dev_AP

Dashboard Notifications Configuration **Details** Performance Software Update Tools

Overview Interfaces Neighbors Radio 1 (BHM) Children

System

Name	cnReach_Dev_AP
Device Type	cnReach BHM
System Uptime	0d 11h 10m
Coordinates	
Description	
Hardware	EB-EBB63
DA Version	2.68.20096
Onboard Date	Jun 27 2024 15:56:06

Software Update

Active Software Version	cn-EBX.5.2.18d
Inactive Software Version	cn-EBX.5.2.18g
GPS Firmware Version	

History

Date	Status	Version
Version History Unavailable		

Configuration Update

History

Date	Status	Template
Configuration History Unavailable		

Network

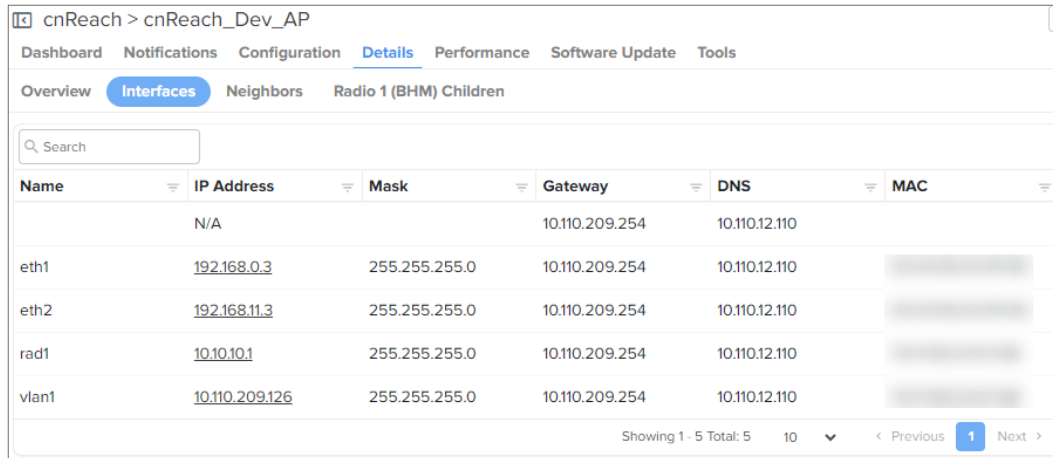
LAN MAC	
IPv4 Address	10.110.209.126
Subnet Mask	N/A
Gateway	N/A
DNS Server(s)	N/A

Radio Details

Type	Radio 1
MAC	
Mode	AP
Network Type	PTP
Network Address	100
Device ID	301
Linked With	201
Tx Power	1007 mW
Software Version	1.57.20870
RSSI	-60 dBm
Margin	50 dB
Noise	-110 dBm
Room Temperature	39 °C
Parent MAC	
Throughput (UL)	0 Kbps
Throughput (DL)	0 Kbps

Interfaces

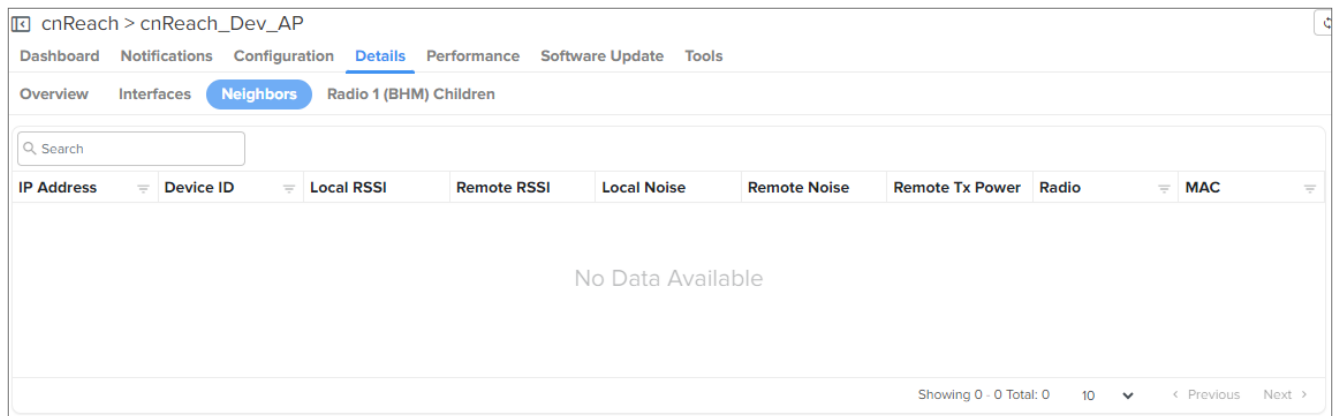
Figure 125 *cnReach: Device > Details > Interfaces*



Name	IP Address	Mask	Gateway	DNS	MAC
	N/A		10.110.209.254	10.110.12.110	
eth1	192.168.0.3	255.255.255.0	10.110.209.254	10.110.12.110	
eth2	192.168.11.3	255.255.255.0	10.110.209.254	10.110.12.110	
rad1	10.10.10.1	255.255.255.0	10.110.209.254	10.110.12.110	
vlan1	10.110.209.126	255.255.255.0	10.110.209.254	10.110.12.110	

Neighbors

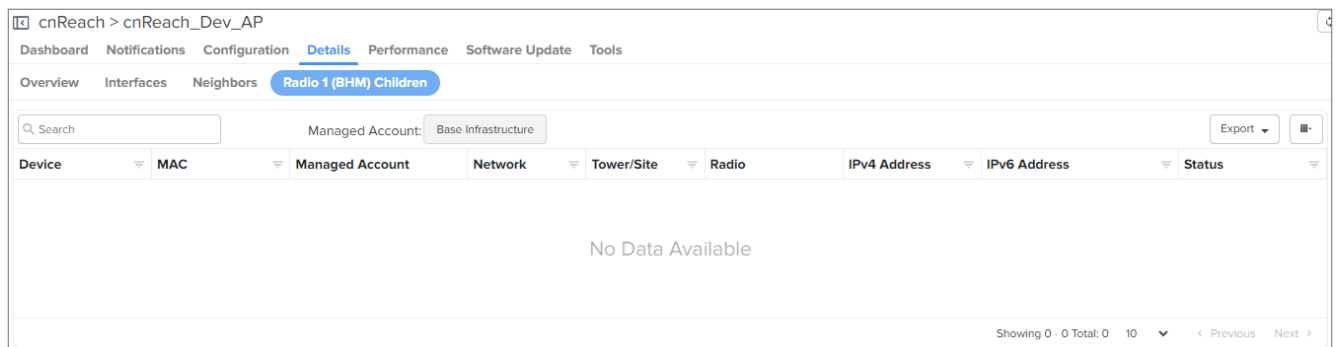
Figure 126 *cnReach: Device > Details > Neighbors*



IP Address	Device ID	Local RSSI	Remote RSSI	Local Noise	Remote Noise	Remote Tx Power	Radio	MAC
No Data Available								

Radio 1 (BHM) Children

Figure 127 *cnReach: Device > Details > Radio 1 (BHM) Children*



Device	MAC	Managed Account	Network	Tower/Site	Radio	IPv4 Address	IPv6 Address	Status
No Data Available								

cnVision Client

The **Details** section displays following tabs for cnVision Client:

- Overview
- Wi-Fi APs

Overview

Figure 128 *cnVision Client: Device > Details > Overview*

The screenshot shows the 'Overview' tab of the 'Details' page for a client named 'Migration_cnVision_Client_@2'. The page is divided into several sections:

- System:** A table with fields: Name (Migration_cnVision_Client_@2), Device Type (cnVision CLIENT MAXr), System Uptime (31d 8h 19m), Coordinates (redacted), Description, Hardware (CLIENT MAXr(ROW/ETSI)), DA Version (2.105.48), Onboard Date (Jul 05 2024 11:31:10), and Reboots (0).
- Software Update:** A table with fields: Active Software Version (4.8), Inactive Software Version (4.7.1), and GPS Firmware Version (N/A).
- History:** A table with columns: Date, Status, and Version. It contains the text 'Version History Unavailable'.
- Configuration Update:** A table with columns: Date, Status, and Template. It contains the text 'Configuration History Unavailable'.
- Network:** A table with fields: LAN MAC (redacted), Ethernet Interface (Down), IPv4 Address (10.110.209.134), Subnet Mask (255.255.255.0), Gateway (10.110.209.254), DNS Server(s) (10.110.12.110 10.110.12.111), and Management VLAN ID (Disabled).
- Wireless:** A table with fields: Operating Frequency (5820 MHz), Channel Bandwidth (40 MHz), Transmitter Output Power (4 dBm), Maximum Transmit Power (N/A), Country Code (India), External Antenna Gain (19 dBi), Internal Antenna Gain, SSID (Cambium-ePMP-MP-3000-AP-HUB3), AP MAC (redacted), Authentication (WPA2), DFS Status (N/A), Wireless MAC (redacted), Wireless Interface (Up), and Frame Utilization (DL) (N/A).

Wi-Fi APs

Figure 129 *cnVision Client: Device > Details > Wi-Fi APs*

The screenshot shows the 'Wi-Fi APs' tab of the 'Details' page for the same client. The page features a search bar, a 'Managed Account' dropdown set to 'Base Infrastructure', and an 'Export' button. Below these is a table with the following columns: Device Name, MAC Address, Managed Account, Product Name, Network, Tower/Site, Radios, IPv4 Address, IPv6 Address, Status, and AP Group. The table is currently empty, displaying 'No Data Available'. At the bottom right, it shows 'Showing 0 - 0 Total: 0' and navigation links for 'Previous' and 'Next'.

cnVision Hub

The **Details** section displays following tabs for cnVision Hub:

- Overview
- Wi-Fi APs

Overview

Figure 130 *cnVision Hub: Device > Details > Overview*

The screenshot shows the 'Overview' tab for a 'CNVISION 202 AP' device. The interface includes a top navigation bar with tabs for Dashboard, Notifications, Configuration, Details (selected), SMs, Performance, Software Update, and Tools. Below this, there are sub-tabs for Overview (selected) and Wi-Fi APs. The main content area is divided into several sections: System, Network, Software Update, History, Configuration Update, Wireless, and Limits. The System section provides details about the device name, type, uptime, coordinates, description, hardware, DA version, onboard date, and reboots. The Network section lists LAN MAC, Ethernet interface status, IPv4 address, subnet mask, gateway, DNS servers, and management VLAN ID. The Software Update section shows active and inactive software versions and GPS firmware version. The History section for both software and configuration updates is currently unavailable. The Wireless section displays operating frequency, channel bandwidth, transmitter output power, maximum transmit power, country code, antenna gains, DL/UL ratio, SSID, authentication, DFS status, wireless MAC, interface status, and frame utilization. The Limits section shows the maximum number of subscribers and the maximum range.

System	
Name	CNVISION 202 AP
Device Type	cnVision HUB 360r
System Uptime	0d 10h 45m
Coordinates	[1, 1]
Description	
Hardware	5 GHz HUB 360r Radio
DA Version	2.105.47
Onboard Date	Jul 02 2024 10:55:14
Reboots	2

Network	
LAN MAC	
Ethernet Interface	Up
IPv4 Address	10.110.208.202
Subnet Mask	255.255.255.0
Gateway	10.110.208.254
DNS Server(s)	10.110.12.110 10.110.12.111
Management VLAN ID	Disabled

Software Update	
Active Software Version	4.6.0.1
Inactive Software Version	4.6.1-RC14
GPS Firmware Version	N/A

History		
Date	Status	Version
Version History Unavailable		

Configuration Update		
Date	Status	Template
Configuration History Unavailable		

Wireless	
Operating Frequency	5800 MHz
Channel Bandwidth	20 MHz
Transmitter Output Power	15 dBm
Maximum Transmit Power	N/A
Country Code	United States
External Antenna Gain	8 dBi
Internal Antenna Gain	
DL/UL Ratio	30/70
SSID	Cambium-360r-HUB-4
Authentication	WPA2
DFS Status	N/A
Wireless MAC	
Wireless Interface	Up
Frame Utilization (DL)	4.7%

Limits	
Max Subscribers	64
Max Range	3 Miles

Wi-Fi APs

Figure 131 *cnVision Hub: Device > Details > Wi-Fi APs*

Hubs > CNVISION 202 AP										
Dashboard Notifications Configuration Details SMs Performance Software Update Tools										
Overview Wi-Fi APs										
Q Search Managed Account: Base Infrastructure Export										
Device Name	MAC Address	Managed Account	Product Name	Network	Tower/Site	Radios	IPv4 Address	IPv6 Address	Status	AP Group
No Data Available										
Showing 0 - 0 Total: 0 10 < Previous Next >										

cnWave 5G Fixed Details

cnWave 5G Fixed BTS

The **Details > Overview** section displays following tabs for cnWave 5G Fixed BTS device:

- Overview
- Interfaces
- Radios

Overview

Overview page provides the information such as Details, Boot Loader, Boot, and Shutdown.

Figure 132 *cnWave 5G Fixed: Device > Details > Overview*

BTS > BTS-...-lab		
Dashboard Notifications Configuration Details CPEs Performance Software Update Tools Assists X		
Overview Interfaces Radios		
System		
Product Name	cnWave 5G Fixed B1000 BTS	
MAC Address		
IPv4 Address	192.168.1.10	
Serial Number		
Software Version	4.0	
Connected CPEs	2	
Registered CPEs	2	
Site Location		
Site Contact		
Description	Cambium Networks cnWave 5G Fixed Base Transc...	
Boot Loader		
Git Tag	develop/6/18	
Build Name	BOOTLOADER 18/2024-03-22 (W) 11:46:53 -0500	
Hardware Version	Digits P9.2 RF 6.0	
Boot		
Startup Reason	Non-Power Cycle	
Startup Count	39	
Shutdown		
Date & Time	Reason	Detail
2024-07-02 04:08:54	Firmware Upgrade	cnMaestro upgrade
2024-07-02 02:49:49	Firmware Upgrade	cnMaestro upgrade
2024-07-02 02:19:22	Firmware Upgrade	cnMaestro upgrade
2024-06-12 07:53:18	User Action	cnMaestro-initiated-reboot
2024-06-04 06:05:18	User Action	cnMaestro-initiated-reboot
2024-06-03 06:06:01	User Action	cnMaestro-initiated-reboot
2024-05-30 06:21:28	Firmware Upgrade	cnmaestro-bts-upgrade
0000-00-00 00:00:00	Power Loss	Boot after long power cycle

Interfaces

Interface page provides the information such as Interface Configuration, GNSS, Tx/Rx Errors, and Tx/Rx Counters.

Figure 133 *cnWave 5G Fixed BTS: Device > Details > Interfaces*

BTS > BTS- -lab

Dashboard

Notifications

Configuration

Details

CPEs

Performance

Software Update

Tools

Assists X

Overview

Interfaces

Radios

Interface Configuration

SFP1 Speed

Autoneg 1000BASE-X

SFP2 Speed

Autoneg 10GBASE-R

GNSS

Tracking

3D Fix

Altitude

-

Location

Satellites In View

16

Tx/Rx Errors

Wireless

Main

SFP 1

SFP 2

In Discards

20

2

0

0

In Errors

0

0

0

0

Out Discards

20

0

0

0

Out Errors

0

0

0

0

Tx/Rx Counters

Wireless

Main

SFP 1

SFP 2

In Octets

311272890

229928...

0

0

In Unicast Packets

243618

47479

0

0

In Multicast Packets

1237313

122

0

0

In Broadcast Packets

84399

42

0

0

Out Octets

59796181

2193786...

0

0

Out Unicast Packets

266120

36263

0

0

Out Multicast Packets

368

1237156

0

0

Out Broadcast Packets

292

84500

0

0

Radios

Radios page provide the details of radios.

Figure 134 *cnWave 5G Fixed BTS: Device > Details > Radios*

BTS > BTS- -lab	
Dashboard Notifications Configuration Details CPEs Performance Software Update Tools Assists X	
Overview Interfaces Radios	
Status	
Transmission State	Active
Frequency	26875.000 MHz
Max EIRP	30.0 dBm
Polarisation	Horizontal
Link Symmetry	6:1
Bandwidth	56 MHz
Target Rx Power	-50 dBm
UL Tx Pwr Ctrl Initial Adjust	Enabled
UL Tx Pwr Ctrl Cont Adjust	Enabled

cnWave 5G Fixed CPE

The **Details** section displays following pages for cnWave 5G Fixed CPE device:

- Overview
- Interfaces
- Radios

Overview

Overview page provides the information such as Details, Radio Details, and Sessions.

Figure 135 *cnWave 5G Fixed CPE: Device > Details > Overview*

CPE > CPE-1	
Dashboard Notifications Configuration Details Performance Software Update Tools Assists X	
Overview Interfaces Radios	
System	
Product Name	cnWave 5G Fixed C100 CPE
MAC Address	
IPv4 Address	192.168.1.11
Serial Number	
Software Version	4.0
Site Location	
Site Contact	
Altitude	-
Coordinates	
Session	
Registration State	Registered
Registration Count	1
Link Uptime	2d 10h 50m
IMSI	
Radio Details	
Range	0.01 km
DL EVM (dB)	-31.9 dB
UL EVM (dB)	-25.7 dB
DL Rx Power (Data)	-43 dBm
UL Rx Power (Data)	-66 dBm
DL MCS	24
UL MCS	22

Interfaces

Interface page provides the information such as Ethernet and Wireless.

Figure 137 *cnWave 5G Fixed CPE: Device > Details > Radios*

CPE > CPE1			
Dashboard		Notifications	
Configuration		Details	
Performance		Software Update	
Tools		Assists X	
Overview		Interfaces	
		Radios	
Radio Details		Quality of Service	
Alignment Active	False	ULBR	0 Kbps
Range	0.009	ULBL	0 Kb
Current EIRP	-1 dBm	DLBR	0 Kbps
UL Backoff (dB)	5 dB	DLBL	0 Kb
DL Backoff (dB)	6 dB	LPULCIR	0 Kbps
DL Sounding State	Assessing	MPULCIR	0 Kbps
UL Sounding State	Assessing	HPULCIR	0 Kbps
DL Channel Distortion (dB)	-6 dB	UHPULCIR	0 Kbps
UL Channel Distortion (dB)	-6 dB	LPDLCIR	0 Kbps
DL EVM (dB)	-28.8	MPDLCIR	0 Kbps
UL EVM (dB)	-25.6	HPDLCIR	0 Kbps
DL MCS	23	UHPDLCIR	0 Kbps
UL MCS	23		
DL Rx Power (Data)	-47 dBm		
UL Rx Power (Data)	-52 dBm		
DL Spatial Frequency	236		
UL Spatial Frequency	45		
Polarization	Horizontal		

Enterprise Wi-Fi AP (XE-, XV-, and X7-Series)

See [Details](#).

ePMP AP

The **Details** section displays following tabs for ePMP APs:

- Overview
- Wi-Fi APs

Overview

Figure 138 ePMP AP: Device > Details > Overview

APs > F600L_112233

Dashboard Notifications Configuration **Details** SMs Performance Software Update Tools Assists X

Overview Wi-Fi APs

System		Network	
Name	F600L_112233	LAN MAC	
Device Type	ePMP Force 4625 AP	Ethernet Interface	Down
System Uptime	658d 3h 12m	IPv4 Address	192.168.0.1
Coordinates	[0, 0]	Subnet Mask	255.255.255.0
Description		Gateway	192.168.0.31
Hardware	6 GHz Force 4625 USB GPS Radio (FCC)	DNS Server(s)	172.17.48.16 1.1.1.1
DA Version	2.105.48	Management VLAN ID	Disabled
Onboard Date	Jul 06 2022 18:13:49	Wireless	
Reboots	0	Operating Frequency	6705 MHz
Software Update		Channel Bandwidth	20 MHz
Active Software Version	5.4.0.26	Transmitter Output Power	10 dBm
Inactive Software Version	5.4.0.22	Maximum Transmit Power	N/A
GPS Firmware Version	N/A	Country Code	United States
History		External Antenna Gain	25 dBi
Date	Status	Internal Antenna Gain	
Version History Unavailable			
Configuration Update		DL/UL Ratio	N/A
History		SSID	Cambium-AXYOV
Date	Status	Authentication	WPA2
Configuration History Unavailable			
		DFS Status	N/A
		Wireless MAC	
		Wireless Interface	Up
		Limits	
		Max Subscribers	1
		Max Range	20 Miles

Wi-Fi APs

Figure 139 ePMP AP: Device > Details > Wi-Fi APs

APs > F600L_112233

Dashboard Notifications Configuration **Details** SMs Performance Software Update Tools Assists X

Overview **Wi-Fi APs**

Search Managed Account: Base Infrastructure Export

Device Name	MAC Address	Managed Account	Product Name	Network	Tower/Site	Radios	IPv4 Address	IPv6 Address	Status	AP Group
No Data Available										

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

ePMP SM

The **Details** section displays following tabs for ePMP SMs:

- Overview
- Wi-Fi APs
- Installation Summary **X**

Overview

Figure 140 ePMP SM: Device > Details > Overview

SMs > F600L_aa4422

Dashboard

Notifications

Configuration

Details

Performance

Software Update

Tools

Assists **X**

Overview

Wi-Fi APs

Installation Summary **X**

System

Name

F600L_aa4422

Device Type

ePMP Force 4625 SM

System Uptime

724d 6h 33m

Coordinates

[0, 0]

Description

Hardware

6 GHz Force 4625 USB GPS Radio (FCC)

DA Version

2.105.48

Onboard Date

Jul 06 2022 18:14:21

Reboots

1

Software Update

Active Software Version

5.4.0.10

Inactive Software Version

5.4.0.6

GPS Firmware Version

N/A

History

Date

Status

Version

Version History Unavailable

Configuration Update

History

Date

Status

Template

Configuration History Unavailable

Network

LAN MAC

Ethernet Interface

Down

IPv4 Address

192.168.0.2

Subnet Mask

255.255.255.0

Gateway

192.168.0.31

DNS Server(s)

172.17.48.16 1.1.1.1

Management VLAN ID

Disabled

Wireless

Operating Frequency

6705 MHz

Channel Bandwidth

common.channelWidth.6

Transmitter Output Power

3 dBm

Maximum Transmit Power

N/A

Country Code

United States

External Antenna Gain

25 dBi

Internal Antenna Gain

SSID

Cambium-AX

AP MAC

Authentication

WPA2

DFS Status

N/A

Wireless MAC

Wireless Interface

Up

208 | Network Monitoring

Cambium cnMaestro Cloud | User Guide

Wi-Fi APs

Figure 141 ePMP SM: Device > Details > Wi-Fi APs

SMs > F600L_aa4422

Dashboard Notifications Configuration **Details** Performance Software Update Tools Assists X

Overview **Wi-Fi APs** Installation Summary X

Search Managed Account: Base Infrastructure Export

Device Name	MAC Address	Managed Account	Product Name	Network	Tower/Site	Radios	IPv4 Address	IPv6 Address	Status	AP Group
No Data Available										

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

Installation Summary X

Figure 142 ePMP SM: Device > Details > Installation Summary X

SMs > F600L_aa4422

Dashboard Notifications Configuration **Details** Performance Software Update Tools Assists X

Overview **Wi-Fi APs** **Installation Summary X**

Installations: N/A

Summary	
SM Name	-
MAC Address	-
MSN	-
Product	-
Software Version	-
RSSI	-
SSR	-
External Antenna	-
Start Timestamp	-
End Timestamp	-
Added By	-
Comment	-

Configuration	
IP Address/Setting	undefined/undefined
Subnet	-
Gateway	-
DNS	-
Management VLAN	-
Data VLAN	-
Security	-
PSK	-
Status	-
Software Update	-
Template	-
Onboarding Details	-

Photos & Location

No Data Available

Link Test Result

Time	Mode	Throughput Uplink/Downlink	Modulation Uplink/Downlink
No Data Available			

AP Scan Result

AP MAC	AP Bandwidth	AP Frequency	Registered
No Data Available			

PMP AP

The **Details** section displays following tabs for PMP APs:

- Overview
- Wi-Fi APs

Overview

Figure 143 PMP AP: Device > Details > Overview

APs > PMP 450i-BB95F3

Dashboard

Notifications

Configuration

Details

SMS

Performance

Software Update

Tools

Assists X

Overview

Wi-Fi APs

System

Name	PMP 450i-BB95F3
Device Type	PMP 450i AP
System Uptime	16d 2h 38m
Coordinates	
Description	
Hardware	021022
DA Version	22.1.5
Onboard Date	Apr 24 2024 12:44:22
Temperature	34 °C
CPU Utilization	2%

Software Update

Active Software Version	22.1 (Build SIT-12)
Inactive Software Version	N/A
GPS Firmware Version	

History

Date	Status	Version
Version History Unavailable		

Configuration Update

History

Date	Status	Template
Configuration History Unavailable		

Network

LAN MAC	
Ethernet Interface	1000Base-T Full Duplex
IPv4 Address	10.110.208.81
Subnet Mask	255.255.255.0
Gateway	10.110.208.254
DNS Server(s)	10.110.12.110, 10.110.12.111
Management VLAN ID	1

Wireless

Operating Frequency	5735 MHz
Channel Bandwidth	20 MHz
Transmitter Output Power	17 dBm
Maximum Transmit Power	N/A
Country Code	FCC
External Antenna Gain	0 dBi
Internal Antenna Gain	0 dBi
Downlink Ratio	75/25
Color Code	222
Authentication	Disabled
DFS Status	Idle
Contention Slots	3

210 | Network Monitoring

Cambium cnMaestro Cloud | User Guide

Wi-Fi APs

Figure 144 PMP AP: Device > Details > Wi-Fi APs

APs > PMP 450I-BB95F3

Dashboard Notifications Configuration **Details** SMs Performance Software Update Tools Assists X

Overview **Wi-Fi APs**

Search Managed Account: DP_MSP Export

Device Name	MAC Address	Managed Account	Product Name	Network	Tower/Site	Radios	IPv4 Address	IPv6 Address	Status	AP Group
No Data Available										

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

PMP SM

The **Details** section displays following tabs for PMP SMs:

- Overview
- Wi-Fi APs
- Installation Summary X

Overview

Figure 145 PMP SM: Device > Details > Overview

SMs > PMP 450i-BBB425

Dashboard

Notifications

Configuration

Details

Performance

Software Update

Tools

Assists X

Overview

Wi-Fi APs

Installation Summary X

System

Name	PMP 450i-BBB425
Device Type	PMP 450i SM
System Uptime	0d 1h 0m
Coordinates	
Description	
Hardware	102723
DA Version	23.0.2
Onboard Date	Jul 02 2024 13:03:10
Temperature	37 °C
CPU Utilization	2%
SW Key – Max Throughput	Unlimited

Software Update

Active Software Version	23.0
Inactive Software Version	N/A
GPS Firmware Version	N/A

History

Date	Status	Version
Version History Unavailable		

Configuration Update

History

Date	Status	Template
Configuration History Unavailable		

Network

LAN MAC	
Ethernet Interface	No Link
IPv4 Address	10.110.208.83
Subnet Mask	255.255.255.0
Gateway	10.110.208.254
DNS Server(s)	10.110.12.110, 10.110.12.111
Management VLAN ID	1

Wireless

Operating Frequency	5735 MHz
Channel Bandwidth	20 MHz
Transmitter Output Power	8 dBm
Maximum Transmit Power	N/A
Country Code	FCC
External Antenna Gain	0 dBi
Internal Antenna Gain	0 dBi
Color Code	222
AP MAC	
DFS Status	Idle
LUID	2

Wi-Fi APs

Figure 146 PMP SM: Device > Details > Wi-Fi APs

SMs > PMP 450i-BBB425

Dashboard

Notifications

Configuration

Details

Performance

Software Update

Tools

Assists X

Overview

Wi-Fi APs

Installation Summary X

Search

Managed Account: DP_MSP

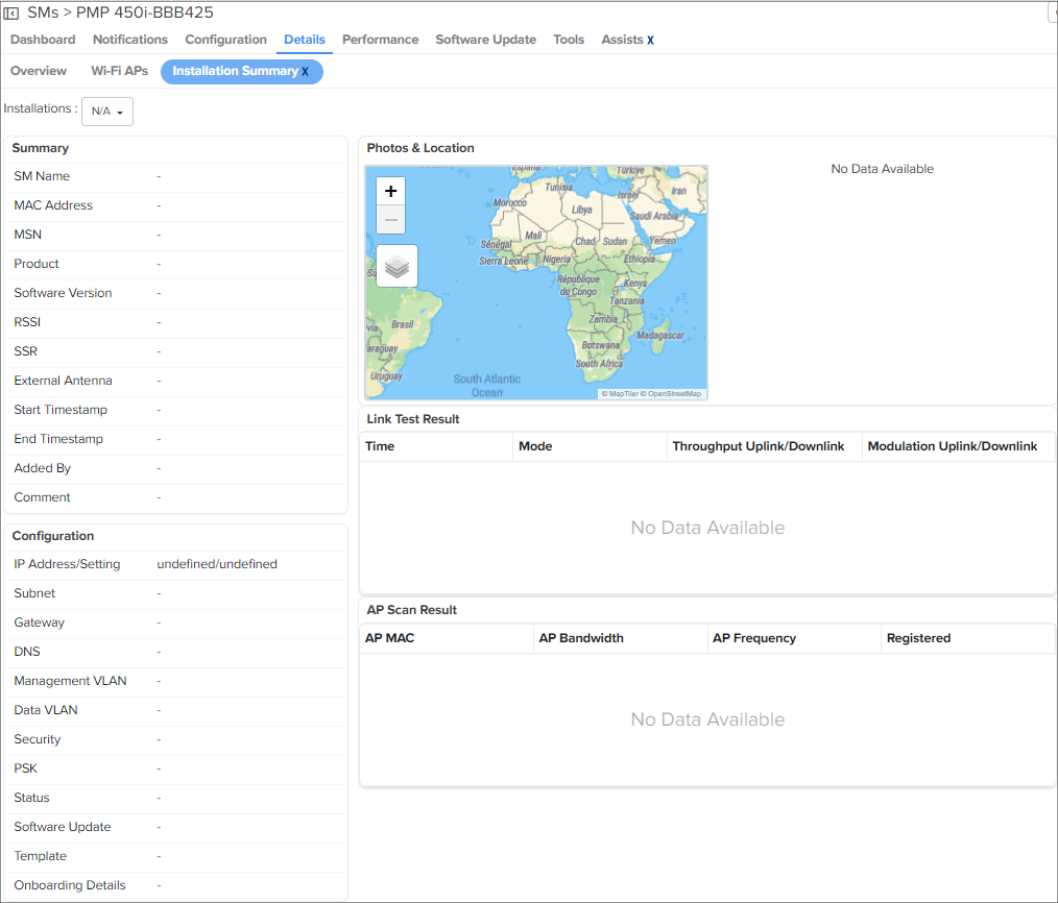
Export

Device Name	MAC Address	Managed Accou...	Product Name	Network	Tower/Site	Radios	IPv4 Address	IPv6 Address	Status	AP Group
No Data Available										

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

Installation Summary X

Figure 147 PMP SM: Device > Details > Installation Summary X



PON (OLT)

The **Details** section displays following information for PON (OLT) device. For more information, see [Details](#).

Figure 148 PON (OLT): Device > Details

OLT > TCX16-20-04-96

Dashboard

Notifications

Configuration

Details

Performance

ONUs

Ports

Software Update

System

Device Name

TCX16-20-04-96

Device Type

TCX16 OLT

System Uptime

17d 6h 42m

Session Time

16d 11h 3m

Coordinates

0,0

Software Version

1.2.0.51

DA Version

2.105.48

Onboard Date

Jun 18 2024 11:29:34

Description

Network

MAC Address

IP Address

10.110.217.4

Subnet Mask

255.255.255.0

Gateway

10.110.217.254

Primary DNS Server

10.110.12.32

Secondary DNS Server

10.110.12.33

Software Update

Active Software Version

1.2.0.51

Inactive Software Version

N/A

History

Date	Status	Version
No Data Available		

PTP 650/670/700

The **Details** section displays following tabs for PTP 650/670/700:

- Overview
- Network Info

Overview

Figure 149 PTP 650/670/700: Device > Details > Overview

PTP 650/670/700 Master > Master_58_B8_25	
Dashboard Notifications Details Slaves Configuration Performance Software Update Assists X	
Overview Network Info	
System	
Name	Master_58_B8_25
Device Type	PTP 50670
System Uptime	10d 6h 13m
Coordinates	[0, 0]
Description	
Hardware	B0P06.01-C-FPS
DA Version	2.94
Onboard Date	Jun 27 2024 15:07:28
Network	
Main PSU Interface	1000 Mbps Full Duplex
Aux Interface	Down
SFP Interface	Down
IPv4 Address	10.110.190.105
Subnet Mask	255.255.255.0
Gateway	10.110.190.254
DNS Server(s)	10.110.12.110, 10.110.12.111
Management VLAN ID	No VLAN
Management VLAN Type	No VLAN
Ethernet	
Main PSU Speed And Duplex	1000 Mbps Full Duplex
Main PSU Rx Frames Oversize	0
Main PSU Tx Bandwidth Utilization	-
Main PSU Rx Bandwidth Utilization	-
Aux Speed And Duplex	Down
Aux Rx Frames Oversize	0
Aux Tx Bandwidth Utilization	-
Aux Rx Bandwidth Utilization	-
SFP Speed And Duplex	Down
SFP Rx Frames Oversize	0
SFP Tx Bandwidth Utilization	-
SFP Rx Bandwidth Utilization	-
Wireless	
Transmit Frequency	5238 MHz
Receive Frequency	5238 MHz
Channel Bandwidth	45 MHz
Country Code	Development Key
External Antenna Gain	23 dBi
Internal Antenna Gain	
Symmetry	1 to 1
Byte Error Ratio	2.98e-9

Network Info

Figure 150 PTP 650/670/700: Device > Details > Network Info

PTP 650/670/700 Master > Master_58_B8_25									
Dashboard Notifications Details Slaves Configuration Performance Software Update Assists X									
Overview Network Info									
Ethernet Ports									
Port	Tx Octets	Rx Octets	Tx Frames	Rx Frames	Rx Frames With Error	Tx Broadcasts	Rx Broadcasts	Rx Frames Undersize	Rx Frames Oversize
Main PSU	57934476	461014067	236167	4416204	0	120	3401017	0	0
AUX	0	0	0	0	0	0	0	0	0
SFP	0	0	0	0	0	0	0	0	0
Showing 1 - 3 Total: 3 10 < Previous 1 Next >									

PTP 820/850 Details

The **Details** section displays following tabs for PTP 820/850:

- Overview
- Ethernet
- Security
- Activation Key

Overview

Overview page provides the information such as System, Radio Parameters and Software Version.

Figure 151 PTP 820/850: Device > Details > Overview

PTP 820/850 > PTP 820G - 10.120.246.162

Dashboard
Notifications
Configuration
Details
Performance
Software Update

Overview
Ethernet
Security
Activation Key

System

Name	PTP 820G - 10.120.246.162
Product Name	PTP 820
MAC Address	
Health	Online (0d 23h 44m)
IPv4 Address	10.120.246.162
Software Version	12.7.0.0.0.274
Serial Number	
Edge Controller	
Onboard Date	Jul 04 2024 14:49:59
Temperature	33 °C
Voltage (V)	54

Radio Parameters

Radio Location	Slot 1, Port 1	Slot 1, Port 2
Tx Frequency (MHz)	5989.675	37086
Rx Frequency (MHz)	6241.715	38346
Operational Tx Level (dBm)	10	0
Rx Level (dBm)	-36	-99
Modem MSE (dB)	-42.26	-99
Modem XPI (dB)	0	99
Defective Blocks	0	0
Tx Mute Status	Unmute	Mute
Tx Bit Rate (Mbps)	261.357	0
Rx Bit Rate (Mbps)	261.357	0

Software Versions

Running	12.7.0.0.0.274
Downloaded	12.7.0.0.0.274

Show Detailed Information

Package Name	Target Device	Running Version	Downloaded Version	Reset Type
gnss	cleared	12.7.0.0.0.274	12.7.0.0.0.274	main-board-cold-reset
gnss-fpga-fw-elic	eLicEth4x1GEA	N/A	1.8.7	main-board-cold-reset
gnss-fpga-fw-rmc	rmcA	N/A	2.4	main-board-cold-reset
gnss-rmc-b	rmcB	N/A	3.27.21	main-board-cold-reset
gnss-fpga-fw-tcc	tccB	6274	N/A	tcc-cold-reset
gnss-atp	tccB	12.7.0.0.0.274	N/A	no-reset
gnss-management	tccB	1.12.7.37	1.12.7.37	main-board-cold-reset
gnss-mctl	tccB	12.7.0.0.0.274	12.7.0.0.0.274	main-board-cold-reset
gnss-mrmc-scripts	rmcA	N/A	7.16	main-board-cold-reset
gnss-mrmc-b-scripts	rmcB	N/A	7.29	main-board-cold-reset
gnss-rfu	cleared	N/A	3.0.11	main-board-cold-reset
gnss_tcc-config	tccB	N/A	N/A	no-reset
gnss_tcc-kernel	tccB	2.6.34.8	N/A	no-reset
gnss-modem-fw	rmcA	N/A	3.40.2	main-board-cold-reset
gnss-pwc	pwe3-16xE1T1	N/A	6.24	main-board-cold-reset
gnss-pwc-stm1	pwe3-1xSTM1	N/A	6.25	main-board-cold-reset
gnss-vm-control	cleared	N/A	1.0.2.12	main-board-cold-reset
gnss-fpga-fw-hrzn	cleared	N/A	N/A	no-reset

Ethernet

Ethernet page provides the information RMON.

Figure 152 PTP 820/850: Device > Details > Ethernet

PTP 820/850 > PTP 820G - 10.120.246.162

Dashboard Notifications Configuration **Details** Performance Software Update

Overview **Ethernet** Security Activation Key

RMON Ethernet Radio Group Management

	Slot: 1, Port 1	Slot: 1, Port 2	Slot: 1, Port 3	Slot: 1, Port 4	Slot: 1, Port 5	Slot: 1, Port 6
Clear On Read	No	No	No	No	No	No
Tx Byte Count	183168	183168	183168	183168	183168	183168
Tx Frame Count	2862	2862	2862	2862	2862	2862
Tx Multicast Frame Count	2862	2862	2862	2862	2862	2862
Tx Broadcast Frame Count	0	0	0	0	0	0
Tx Control Frame Count	0	0	0	0	0	0
Tx Pause Frame Count	0	0	0	0	0	0
Tx FCS Error Frame Count	0	0	0	0	0	0
Tx Length Error Frame Count	0	0	0	0	0	0
Tx Oversize Frame Count	0	0	0	0	0	0
Tx Undersize Frame Count	0	0	0	0	0	0
Tx Fragment Frame Count	0	0	0	0	0	0
Tx Jabber Frame Count	0	0	0	0	0	0
Tx 64 Frame Count	2862	2862	2862	2862	2862	2862
Tx 65-127 Frame Count	0	0	0	0	0	0
Tx 128-255 Frame Count	0	0	0	0	0	0
Tx 256-511 Frame Count	0	0	0	0	0	0
Tx 512-1023 Frame Count	0	0	0	0	0	0
Tx 1024-1518 Frame Count	0	0	0	0	0	0
Tx 1519-1522 Frame Count	0	0	0	0	0	0
Rx Byte Count	0	0	0	0	0	0
Rx Frame Count	0	0	0	0	0	0
Rx Multicast Frame Count	0	0	0	0	0	0
Rx Broadcast Frame Count	0	0	0	0	0	0
Rx Control Frame Count	0	0	0	0	0	0
Rx Pause Frame Count	0	0	0	0	0	0
Rx FCS Error Frame Count	0	0	0	0	0	0
Rx Length Error Frame Count	0	0	0	0	0	0
Rx Code Error Count	0	0	0	0	0	0
Rx Oversize Frame Count	0	0	0	0	0	0
Rx Undersize Error Frame Count	0	0	0	0	0	0
Rx Fragment Frame Count	0	0	0	0	0	0
Rx Jabber Frame Count	0	0	0	0	0	0
Rx 64 Frame Count	0	0	0	0	0	0
Rx 65-127 Frame Count	0	0	0	0	0	0
Rx 128-255 Frame Count	0	0	0	0	0	0
Rx 256-511 Frame Count	0	0	0	0	0	0
Rx 512-1023 Frame Count	0	0	0	0	0	0
Rx 1024-1518 Frame Count	0	0	0	0	0	0
Rx 1519-1522 Frame Count	0	0	0	0	0	0
Rx Exceed Max With Error Frame Count	0	0	0	0	0	0
Rx Exceed Max Frame Count	0	0	0	0	0	0

Security

Security page provides the information of General Parameters, Protocols, Login and Password Management, User Account, and SNMP V3 Users.

Figure 153 PTP 820/850: Device > Details > Security

PTP 820/850 > PTP 820G - 10.120.246.162

Dashboard Notifications Configuration **Details** Performance Software Update

Overview Ethernet **Security** Activation Key

General Parameters

IPSec Pre-Shared Key	*****	Show
IPSec Mode Admin	Disable	
FIPS Mode Admin	Disable	
Import/Export security settings	Enable	
Session timeout (Minutes)	10	

Protocols

Redirect from HTTP to HTTPS	Yes	
HTTP Admin	Enable	
SNMP Admin	Enable	
SNMP Operational Status	Up	
SNMP V1V2 Blocked	No	
SNMP Read Community	*****	Show
SNMP Write Community	*****	Show
SNMP Trap Version	V1	

Login and Password Management

Password change for first login	Yes
Enforce password strength	No
Password aging (Days)	No Aging
Enforce password history	5
Failure login attempts to block user	3
Blocking period (Minutes)	5
Unused account period for blocking (Days)	No Blocking

User Accounts

Username	Profile	Blocked	Login Status	Last Logout	Expiration Date
admin	admin	No	Yes	Yes	Unlimited

SNMP V3 Users

Username	Security Mode	Authentication Algorithm	Encryption (Privacy) Mode	Access Mode
No Data Available				

Activation Key

Activation Key provides the information of Feature Name, Feature Description, Feature Usage, Feature Credit, and Violation.

Figure 154 PTP 820/850: Device > Details > Activation Key

PTP 820/850 > PTP 820C-10.120.109.102

Dashboard Notifications Configuration **Details** Performance Software Update

Overview Ethernet Security **Activation Key**

Feature Name	Feature Description	Feature Usage	Feature Credit	Violation Status
Services Mode	SL-0311-0: Smart-Pipe mode, SL-0312-0: Edge-CET-Node mode, SL-0313-0: Agg-Lvl-1-CET-Node mode, SL-0314-0: Agg-Lvl-2-CET-Node mode	Not Used	Smart Pipe	Ok
Number of Services	Number of allowed Ethernet services	2	10	Ok
H-QoS	SL-0320-0: Hierarchical QoS (Quality of Service)	Not Used	Not Allowed	Ok
Network Resiliency	SL-0327-0: Network resiliency protocols (Smart-TDM Path Protection, G.8032)	Not Used	Not Allowed	Ok
Eth. OAM-Fault Management	SL-0329-0: Enables Connectivity Fault Management (FM) per Y.1731/ 802.1ag and 802.3ah (CET mode only)	Not Used	Not Allowed	Ok
Eth. OAM-Perf. Monitoring	SL-0330-0: Ethernet OAM (Operation Administration and Maintenance) Performance Monitoring (PM) - Y.1731	Not Used	Not Allowed	Ok
LACP	SL-0405-0: Enables Link Aggregation Control Protocol (LACP)	Not Used	Not Allowed	Ok
L1 Link Bonding	SL-0445-0: L1 Link Bonding feature	Not Used	Not Allowed	Ok
Synchronous Ethernet	SL-0322-0: ITU-T G.8262 SyncE and ITU-T G.8264 ESMC (Ethernet Synchronization Message Control)	Not Used	Not Allowed	Ok
IEEE 1588v2 Transparent Clock	SL-0324-0: IEEE 1588v2 Precision Time Protocol - Transparent Clock	Not Used	Not Allowed	Ok
IEEE 1588v2 Transparent Clock BRCM	SL-0443-0: IEEE 1588v2 Precision Time Protocol - Transparent Clock BRCM	Not Used	Not Allowed	Ok
IEEE 1588v2 Ordinary Clock	SL-0325-0: IEEE 1588v2 Precision Time Protocol - Ordinary Clock	Not Used	0	Ok
IEEE 1588v2 Boundary Clock	SL-0326-0: IEEE 1588v2 Precision Time Protocol - Boundary Clock	Not Used	Not Allowed	Ok
IEEE 1588v2 Boundary Clock BRCM	SL-0442-0: IEEE 1588v2 Precision Time Protocol - Boundary Clock BRCM	Not Used	Not Allowed	Ok
Main card redundancy	SL-0328-0: Enables the use of a second TCC in a 2RU chassis for TCC redundancy	Not Used	Not Allowed	Ok
TDM Pseudowire	SL-0352-0: Enables TDM Pseudowire services on units with TDM interfaces	Not Used	Not Allowed	Ok

Home Mesh Routers

See [Viewing router system information and network traffic status.](#)

Performance

Performance pages display a synchronized view of time-series data for devices. The data can be filtered using the interval ranges in the upper left (last 1 hours to last 1 year) , or by dragging the cursor on the graph to select a specific range. The data presented varies based upon device type.



Note

cnMaestro supports 14 months of historical data for the following devices:

- cnPilot Home (R-Series)
- Enterprise devices (Enterprise Wi-Fi and cnMatrix)
- IIoT devices

cnMaestro supports 26 months of historical data for the following devices:

- Fixed Wireless

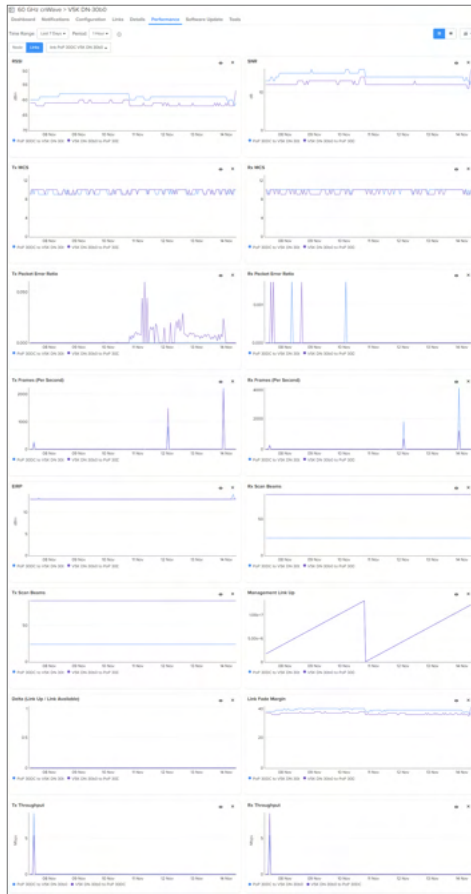
Period = 1 day is available for a Time Range of more than 24 hrs.

The following images represent the sample performance graphs for 60 GHz cnWave, cnMatrix, cnPilot Enterprise, cnPilot Home, cnRanger, cnReach, cnVision, cnWave 5G Fixed, ePMP AP, ePMP SM, PMP AP, PMP SM, PTP 650/670/700, and PTP 820/850.

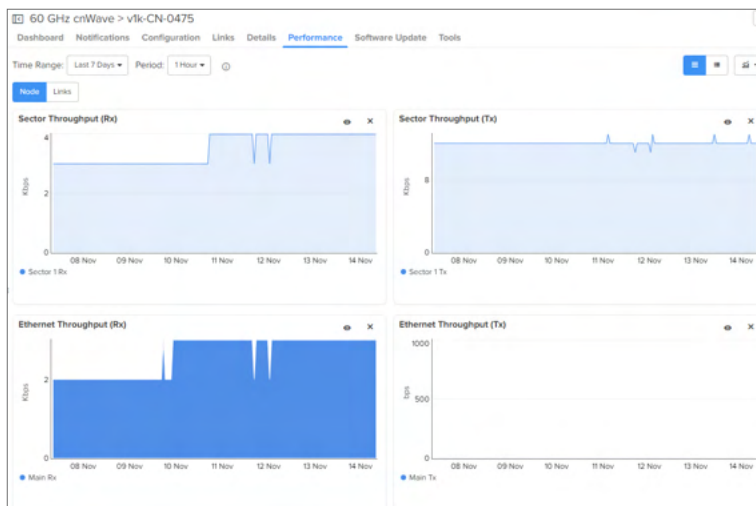
- 60 GHz cnWave (Links)

Displays the following graphs:

- Delta (Link Up/Link Available)
- EIRP
- Link Fade Margin
- Management Link Up
- RSSI
- Rx Frames (Per Second)
- Rx MCS
- Rx Packet Error Ratio
- Rx Scanbeams
- Rx Throughput
- SNR
- Tx Frames (Per Second)
- Tx MCS
- Tx Packet Error Ratio
- Tx Scanbeams
- Tx Throughput



- 60 GHz cnWave (Node)
Displays the following graphs:
 - Ethernet Throughput (Rx)
 - Ethernet Throughput (Tx)
 - Sector Throughput (Rx)
 - Sector Throughput (Tx)



- cnMatrix

Displays the following graphs:

- CPU
- Packet Error
- Rx Packets
- Throughput
- Tx Packets



- cnPilot Home

Displays the following graphs:

- CPU
- Stacked Clients by Band
- Stacked Clients by Radio
- Stacked Throughput by Band (Downlink)
- Stacked Throughput by Band (Uplink)
- Stacked Throughput by Radio (Downlink)
- Stacked Throughput by Radio (Uplink)



- cnReach

Displays the following graphs:

- Neighbors
- Noise
- RSSI
- Throughput
- Transmit Power



- cnRanger BBU

Displays the following graphs:

- Available Memory
- CPU
- Interface (eth1)
- Interface (eth2)
- SMs Registered
- Temperature
- Throughput



- cnRanger RRH

Displays the following graphs:

- Ambient Temperature
- CPU
- Die Temperature
- Frame Utilization
- SMs Registered
- Throughput



- cnRanger SM

Displays the following graphs:

- Available Memory
- CPU
- MCS
- RSRP
- RSRQ
- RSSI
- SINR
- Throughput



- cnVision Client

Displays the following graphs:

- CPU
- MCS
- Retransmission
- RSSI
- Session Drops

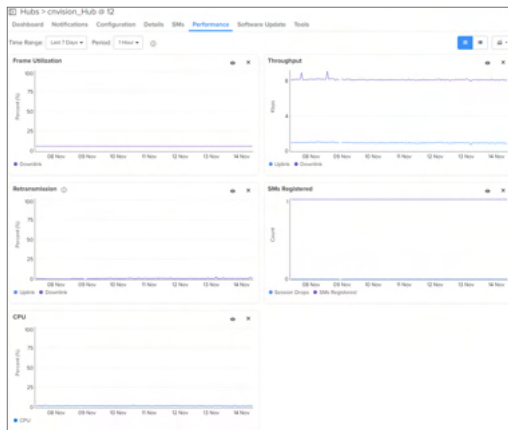
- SNR
- Throughput



- cnVision Hub

Displays the following graphs:

- CPU
- Frame Utilization
- Retransmission
- SMs Registered
- Throughput



- cnWave 5G Fixed BTS

Displays the following graphs:

- CPE Count
- Downlink MU-MIMO Grouping
- Downlink MU-MIMO Grouping Size Distribution
- Throughput
- Uplink MU-MIMO Grouping
- Uplink MU-MIMO Grouping Size Distribution



- cnWave 5G Fixed CPE

Displays the following graphs:

- EVM
- MCS
- Registration Count
- Rx Power
- Throughput

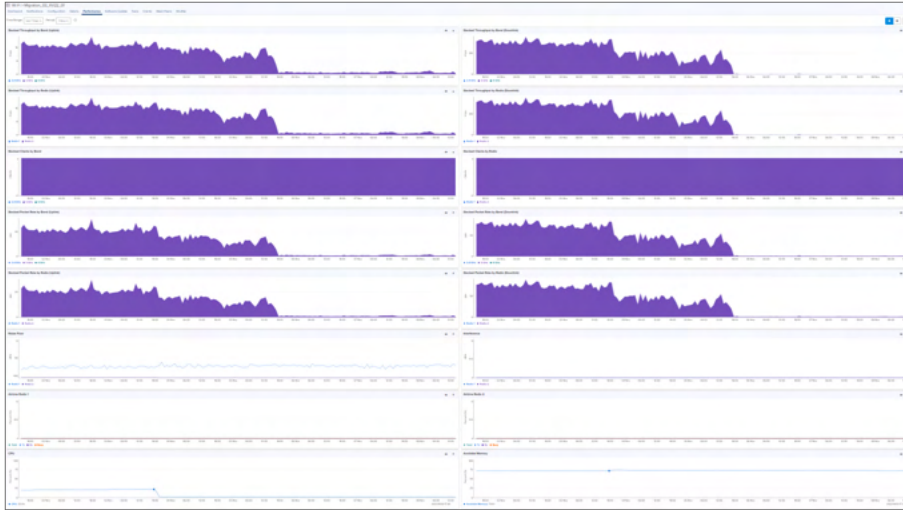


- Enterprise Wi-Fi

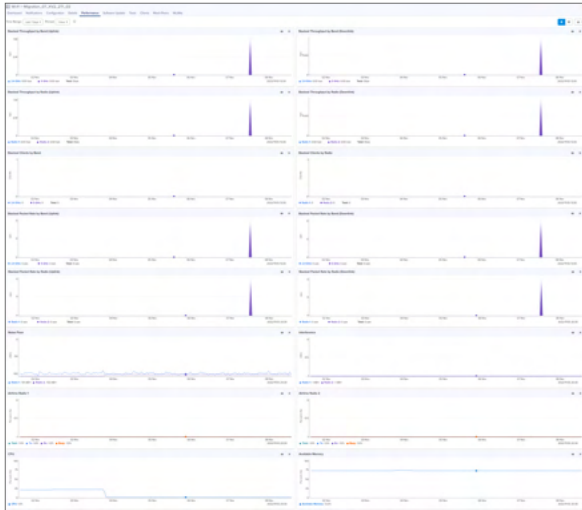
Displays the following graphs:

- Airtime Radio 1
- Airtime Radio 2
- Available Memory
- Clients by Band
- Clients by Radio
- CPU
- Interference
- Noise Floor
- Stacked Clients by Band
- Stacked Clients by Radio
- Stacked Packet Rate by Band (Downlink)

- Stacked Packet Rate by Band (Uplink)
- Stacked Packet Rate by Radio (Downlink)
- Stacked Packet Rate by Radio (Uplink)
- Stacked Throughput by Band (Downlink)
- Stacked Throughput by Band (Uplink))
- Stacked Throughput by Radio (Downlink)
- Stacked Throughput by Radio (Uplink)



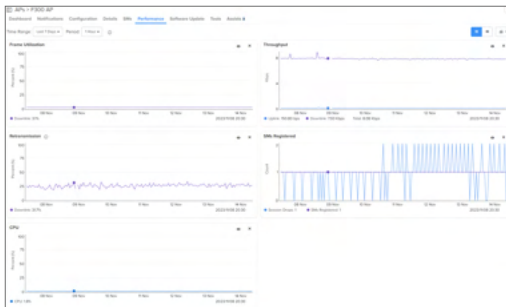
- Enterprise Wi-Fi (Xirrus-Series)
 - Displays the following graphs:
 - Available Memory
 - Clients by Band
 - Clients by Radio
 - CPU
 - Stacked Packet Rate by Band (Downlink)
 - Stacked Packet Rate by Band (Uplink)
 - Stacked Packet Rate by Radio (Downlink)
 - Stacked Packet Rate by Radio (Uplink)
 - Stacked Throughput by Band (Downlink)
 - Stacked Throughput by Band (Uplink)
 - Stacked Throughput by Radio (Downlink)
 - Stacked Throughput by Radio (Uplink)



- ePMP AP

Displays the following graphs:

- CPU
- Frame Utilization
- Retransmission
- SMs Registered
- Throughput



- ePMP SM

Displays the following graphs:

- CPU
- MCS
- Retransmission
- RSSI
- Session Drops
- SNR
- Throughput



- NSE 3000

Displays the following graphs:

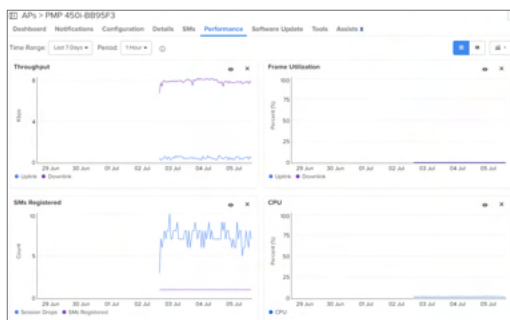
- Available Memory
- CPU



- PMP AP

Displays the following graphs:

- CPU
- Frame Utilization
- SMs Registered
- Throughput



- PMP SM

Displays the following graphs:

- BER
- CPU
- DL RSSI Imbalance
- EVM
- LQI (Link Quality Indicator)
- Modulation
- RSSI
- Session Drops
- SNR (Horizontal)
- SNR (Vertical)
- Throughput



Note

BER with zero values are not plotted on the logarithmic scale graphs.

• PON

Displays the following graphs:

- CPU
- Memory

- ONUs
- Temperature



- PTP and HCMP Masters

Displays the following graphs:

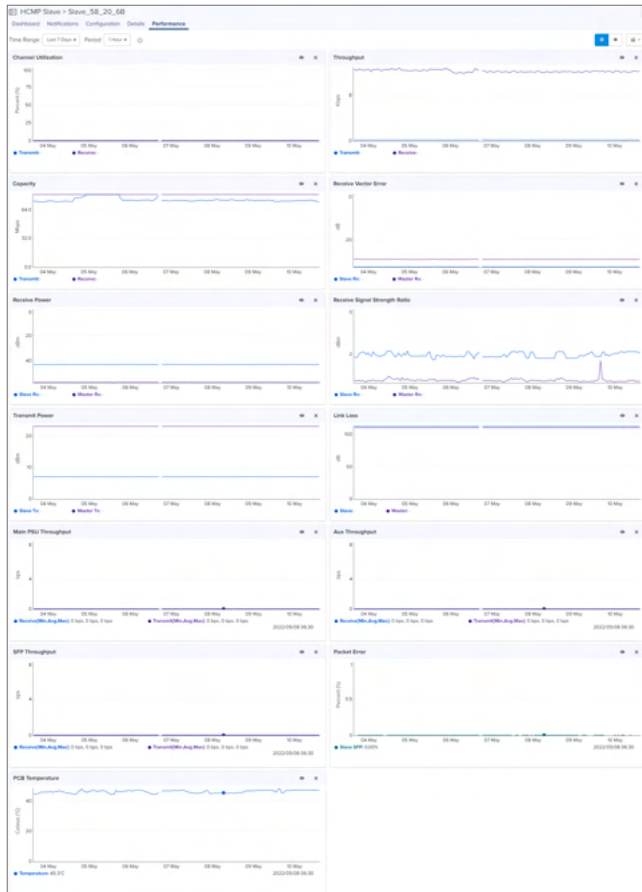
- Aux Throughput
- Capacity
- Channel Utilization
- Link Loss
- Main PSU Throughput
- Packet Error
- PCB Temperature
- Receive Power
- Receive Signal Strength Ratio
- Receive Vector Error
- SFP Throughput
- Throughput
- Transmit Power



- PTP and HCMP Slaves

Displays the following graphs:

- Aux Throughput
- Capacity
- Channel Utilization
- Link Loss
- Main PSU Throughput
- Packet Error
- PCB Temperature
- Receive Power
- Receive Signal Strength Ratio
- Receive Vector Error
- SFP Throughput
- Throughput
- Transmit Power



- PTP 820/850
 - Displays the following graphs:
 - Modem MSE
 - Modem XPI
 - MRMC Profile
 - Peak Throughput By Groups
 - Peak Throughput By Radios
 - Signal Level - RSL
 - Signal Level - TSL
 - Throughput By Groups
 - Throughput By Radios



- RV22 Home Mesh

Displays the following graphs:

- Airtime 2.4 GHz
- Airtime 5 GHz
- Available Memory
- CPU
- Data Rate
- Interference
- Noise Floor
- RSSI
- SNR
- Stacked Throughput by Band (Downlink)
- Stacked Throughput by Band (Uplink)
- Stacked Clients by Band



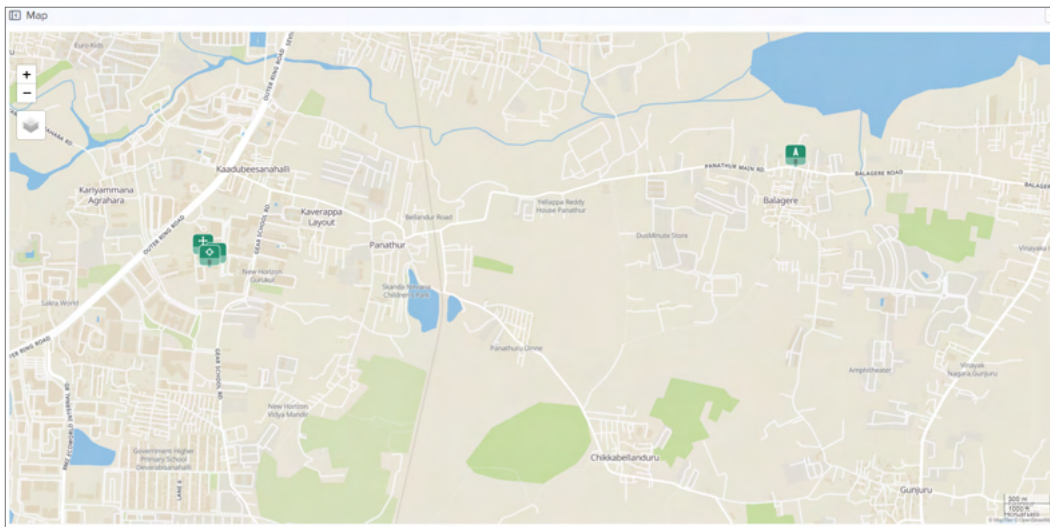
Map

Maps provide visualization for Towers, Sites, and Devices. They display proximity to other devices, connectivity between devices, device health, and selectable status parameters. An example Map is presented below.

Three views are supported in System Maps and Network/Tower Dashboard Maps:

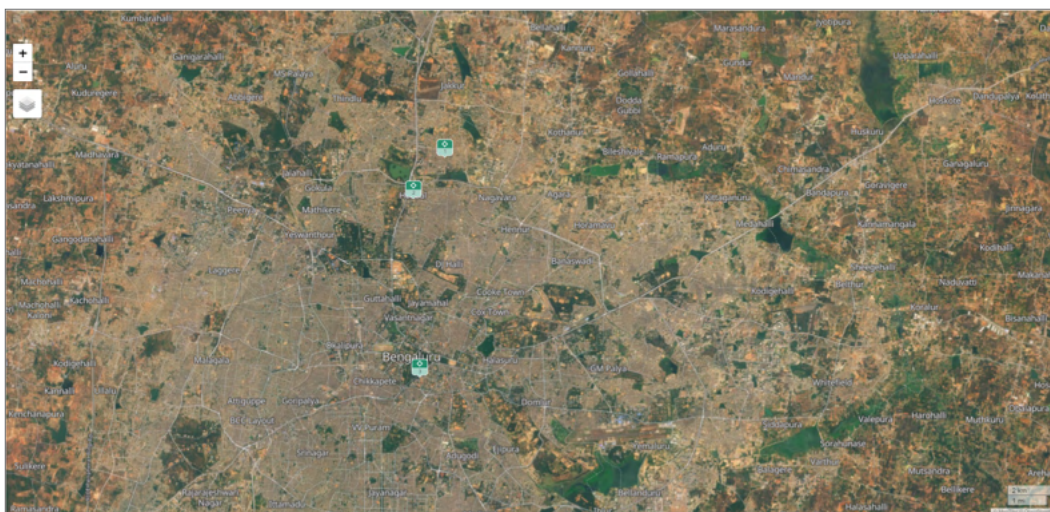
- Street View
- Satellite View
- Terrain View

Figure 155 Map Street View



The Satellite View is supported in limited US and EU regions.

Figure 156 Map Satellite View



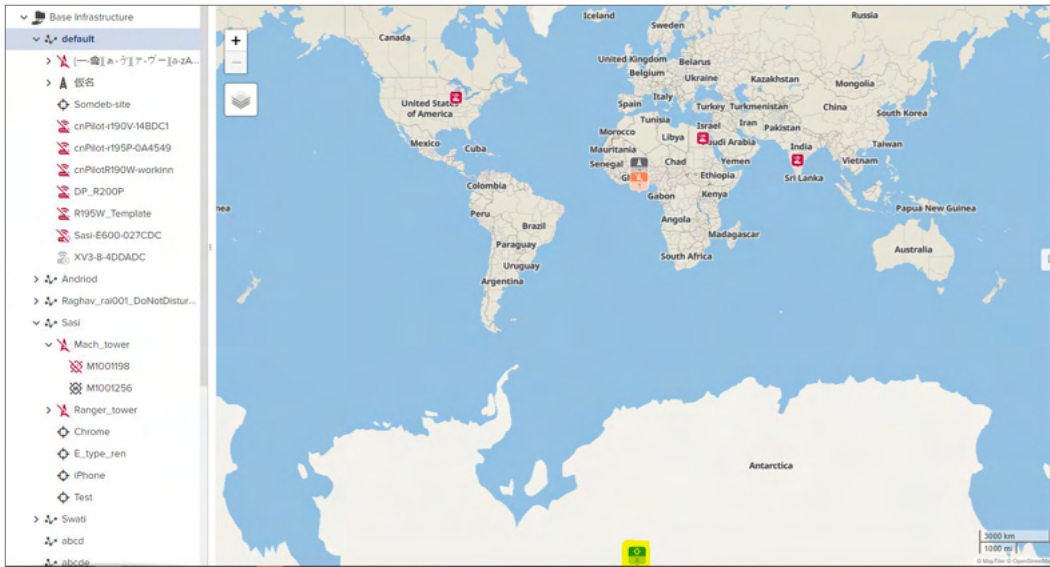
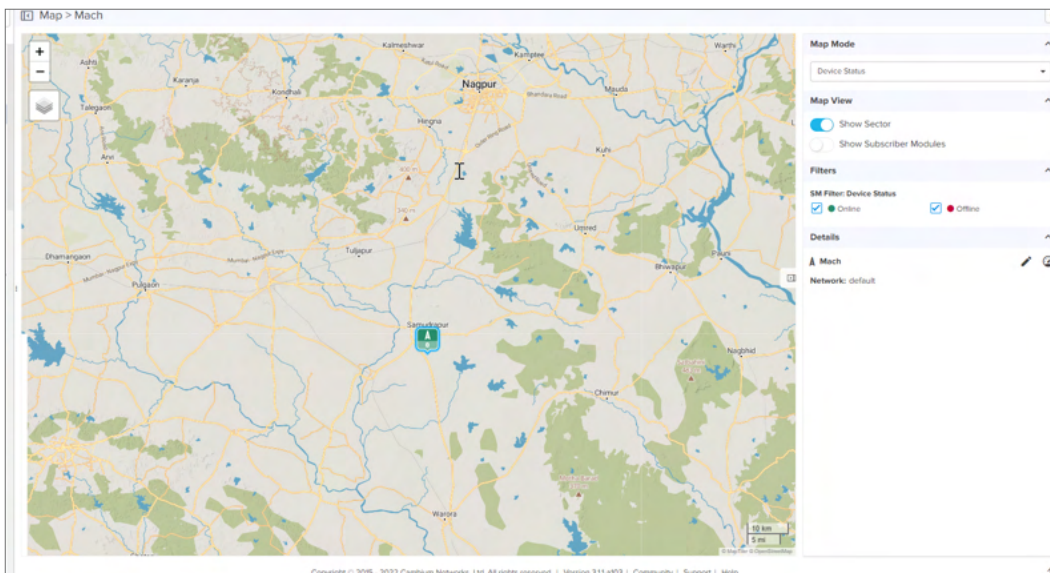


Figure 157 Map Terrain View



If latitude or longitudinal of Site or Tower or Device is (-90°, 90°, -180°, 180°) or (0,0) then they will not display in the map.



Note

- (0,0) is the default value for devices that do not have a location set cnMaestro does not plot devices with this location.
- (x, 180°) and (x, -180°) require the user to zoom out in order to see the markers.
- (90°, y) and (-90°, y) also displays incorrectly.

Map Navigation

There are a various ways to navigate the map display.

Action	Description
Click	Click the following items on the Map to auto-select the same item in the Tree.

Action	Description
	<ul style="list-style-type: none"> ePMP SM Tower
Double-click	Double-click on the following items on the Map to auto-navigate to the Dashboard of that item. <ul style="list-style-type: none"> ePMP SM Site Tower
Hover	Hovering over a tower or device displays a tool tip that provides basic status information. Hovering over an RF link displays status on the link.
Standard Components	In the upper-left corner are generic map navigation components that allow one to zoom in and out. Use the mouse to drag and reposition the view. as well as turn on the satellite display.

Mode

The map can be placed in a number of different modes, which define how the device status is presented.

Table 28 *Mode*

Mode	Details
Alarm Status	Highlights devices based upon alarm count (Critical, Major, Minor).
Average MCS	Displays the Uplink or Downlink average MCS per device.
Device Status	Displays whether a device is Up (Green) or Down (Red).
Frequency	Displays the device sector frequency.
Link Quality Indicator (PMP)	Displays the Uplink or Downlink status.
Packet Loss	Displays the Uplink or Downlink packet loss per device.
Reregistration Count	Displays the nodes based upon the number of re-registrations in the last 24 hours. The more re-registrations, the larger the node is display.
Retransmission Percentage (ePMP and cnVision)	Displays the Uplink or Downlink percentage status.

Embedded Maps

Maps are embedded into some additional UI views (most notably, the Dashboard). These embedded maps do not provide the full feature set of the map view.

Sector Visualization

cnMaestro presents a basic sector View for ePMP and PMP fixed wireless devices. This requires configuration of Height, Azimuth, Elevation, and Beamwidth under cnRanger ePMP/PMP AP configuration. This configured data is used to generate the Sector View. The presentation is not based upon link planning or geographic topology.

Figure 158 AP Configuration

Device Details

Managed Account: [Base Infrastructure](#) [Change](#)

Name:

Network:

Tower:

Description:

Height:

Azimuth:

Elevation:

Beam Width:

[View Tower location on map](#)

Device Configuration [View Device Configuration](#)

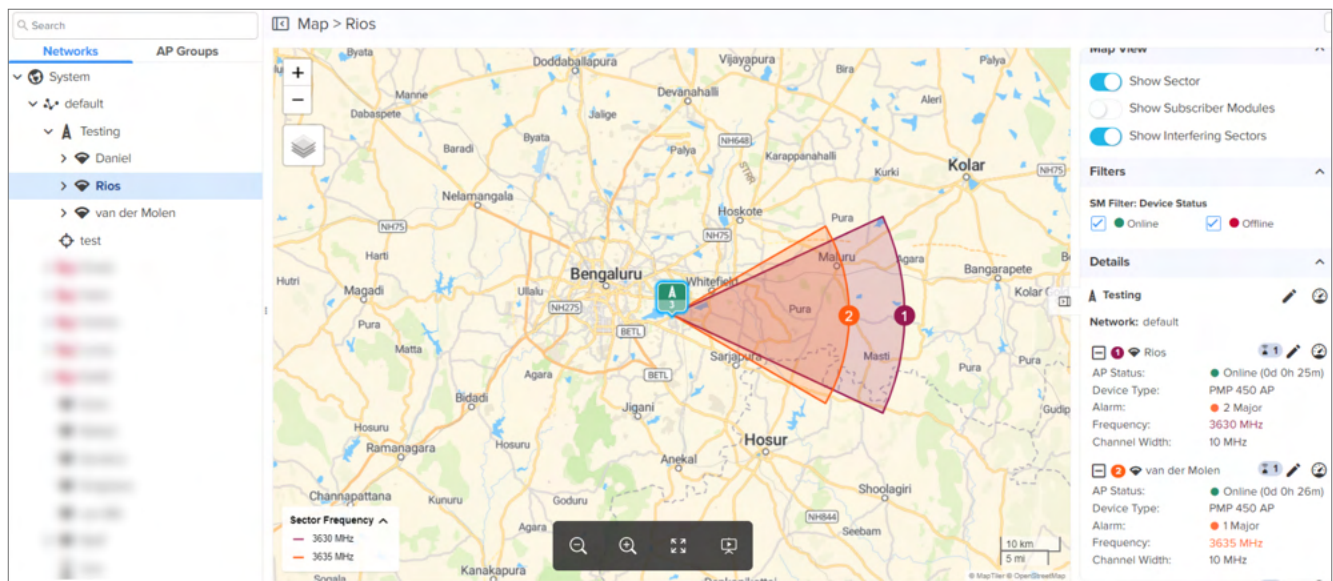
Template: [View Template](#)

Name	Value	Default
No variables configured		

[Apply Configuration](#)

Sector Visualization is available in **Map View**. By selecting the **Show Sector** option, the following map is displayed:

Figure 159 Sector Visualization



Show Subscriber Modules option is available at System, Network, Tower, and AP levels. User can also choose to set the color of SMs based upon frequency or Online or Offline Status.



Note

- By default **Show Subscriber Modules** is disabled.

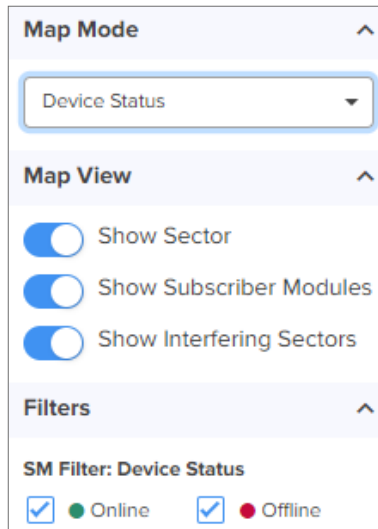
- Map view is supported for PMP, ePMP, cnRanger, cnPilot Home, PTP, 60 GHz cnWave, cnVision, cnMatrix, Enterprise Wi-Fi Series, and RV22 Home Mesh at site- and device-levels.

The **Show Interfering sector** option compares the frequency and bandwidth with all other devices in the network. The map displays the devices that have overlapping frequencies.



Note

Show Interfering Sectors is applicable only for PMP devices and is enabled only if the **Show Sector** button is **ON**.



Maps are available for the Site and Device levels. The right pane displays the device details in the map. To view the map device details, do one of the following:

- Click the (+) plus sign, next to Site or Device in the right pane of the Map page, to view the device and site details as shown in [Figure 160](#).
- Click the Dashboard(📊) icon next to the Site or Device name, to view the site or device dashboard details.

Figure 160 Map: Enterprise Site level

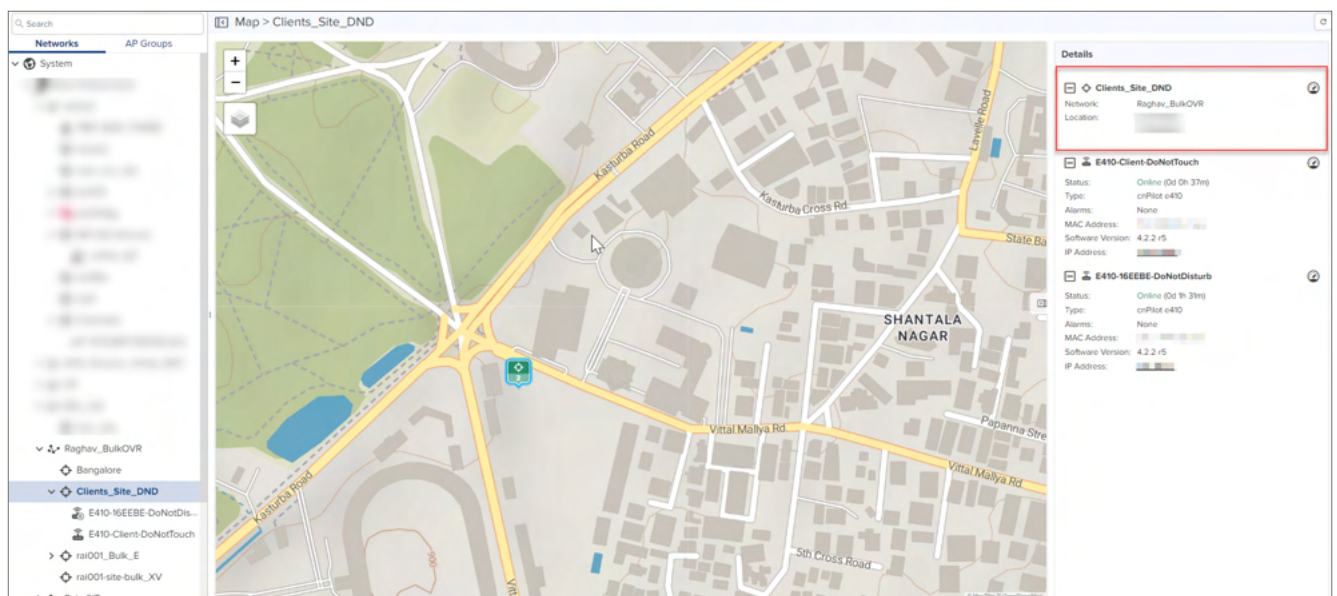


Figure 161 Map: Home Site level

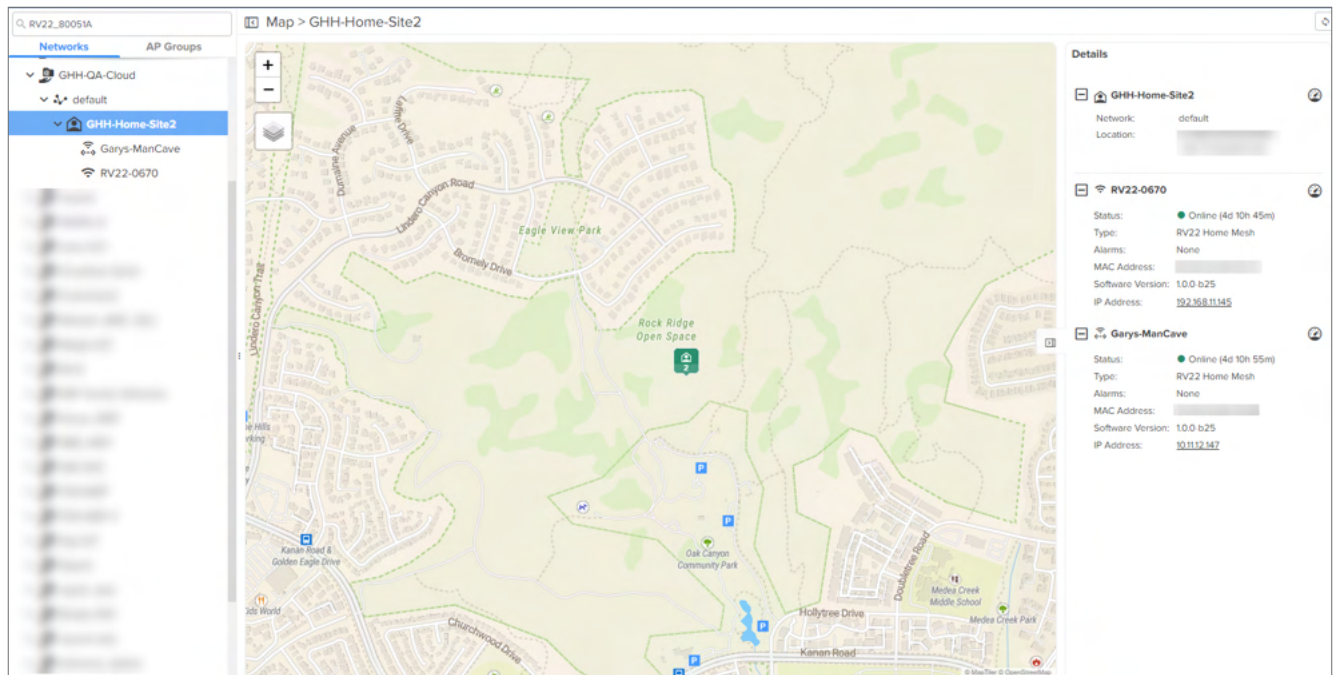


Figure 162 Map: Device level

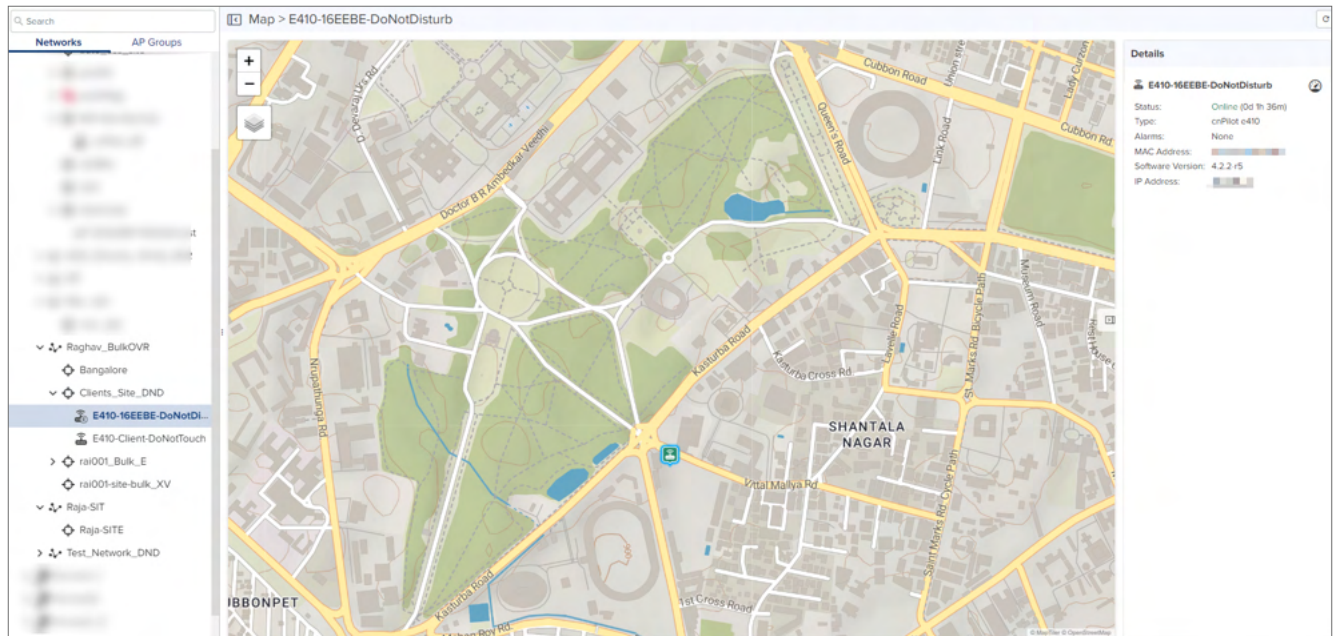


Figure 163 Map view: *cnMatrix*

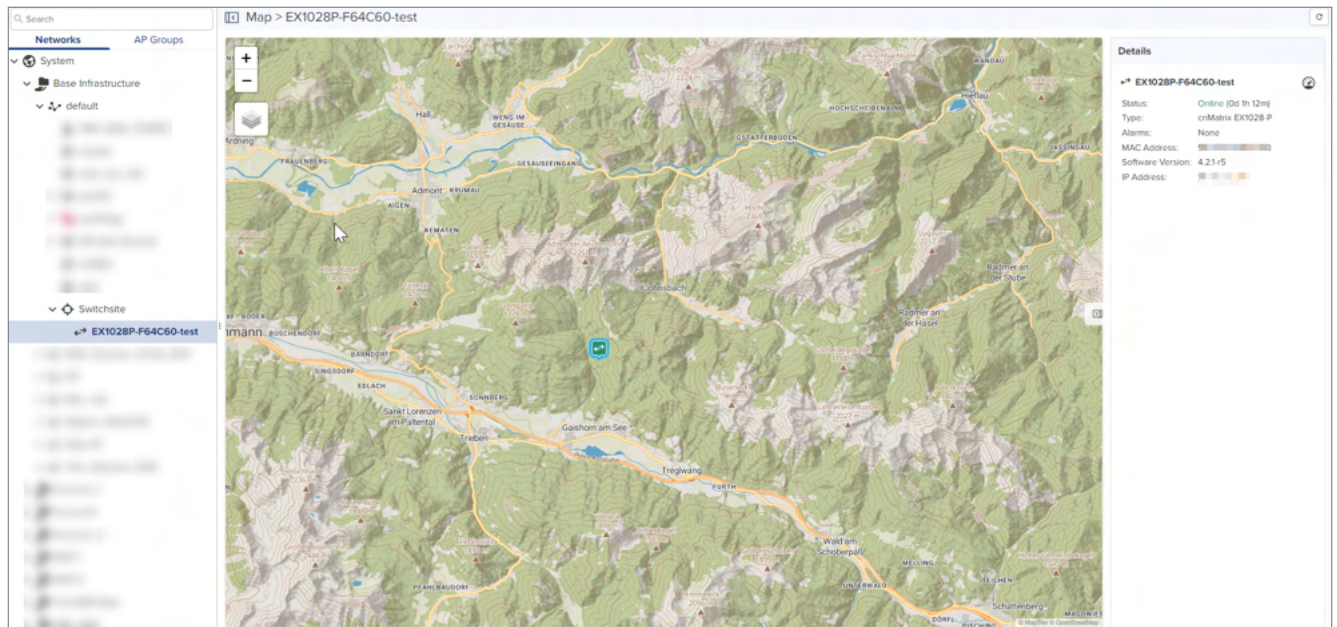


Figure 164 Map view: *Enterprise Wi-Fi (Xirus-Series)*

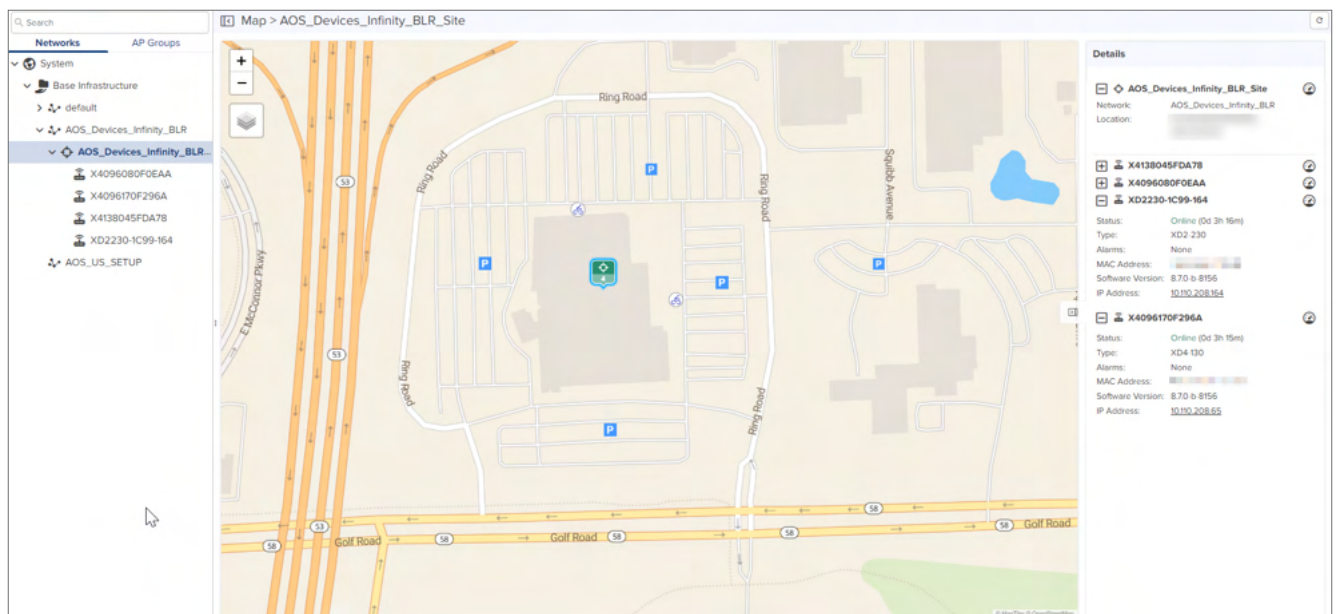
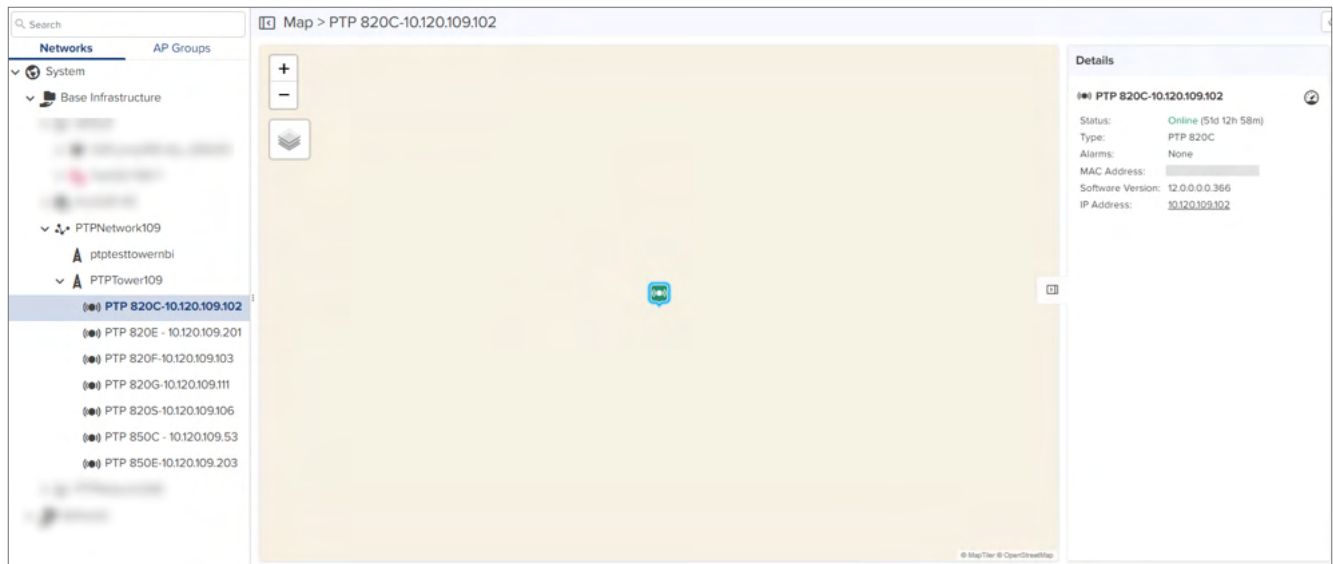


Figure 165 Map View: PTP 820/850



Tools

This section provides the following details:

- [60 GHz cnWave Tools](#)
- [cnMatrix Tools](#)
- [cnPilot Home Tools](#)
- [cnRanger Tools](#)
- [cnReach Tools](#)
- [cnVision Tools](#)
- [Edge Controller Tools](#)
- [Enterprise Wi-Fi Tools](#)
- [ePMP Tools](#)
- [PMP Tools](#)
- [cnWave 5G Fixed Tools](#)
- [RV22 Home Mesh Tools](#)

60 GHz cnWave Tools

In E2E Network **Tools** tab you can view Operations, Diagnostics, Debug, Remote Command, Services, and Settings. Refer to [E2E Network Tools](#).

In Nodes **Tools** tab you can view the Status, Debug, and Remote Command of the device. Refer to [Node Tools](#).

cnMatrix Tools

In **Status** tab you can view the status of the device (either Online or Offline). It allows one to reboot the device.

Table 29 *cnMatrix Tools*

Field	Description
Network Connectivity	Executes Ping, DNS, or Traceroute tests.
Remote CLI	Enter CLI command in the command text box to execute on device. <ul style="list-style-type: none">• Only Show command is allowed for Operator users.• All CLI commands are supported by Super Admin and Admin users.
Status	Displays the Status and Port Status.

The **Status** tab displays the status of the device (either Online or Offline). It also allows one to reboot the device.

cnMatrix > TX2020RP-B0D980

Dashboard Notifications Configuration Details Performance Software Update **Tools** Assists X

Status Remote CLI Network Connectivity

cnMatrix TX2020R-P

Online

Port Status - Port 1

Warning: Port operation can be reverted to the Switch Port configuration during next config sync. Auto-sync should be disabled in the Switch Group to avoid this from happening.

Cable Diagnostic X Port Enable Port Disable PoE Enable PoE Disable PoE Toggle

Output Complete

```
Device->config terminal; cable-diagnostics test inter gi 0/1 force
Warning: Deprecated command, use "test cable-diagnostics" from exec mode
% Cable diagnostics test has started for interface Gi0/1
Device->show cable-diagnostics inter gi 0/1;
Cable Diagnostics Port Status
-----
Port    Pair  Status      Distance Date of
        Pair  to Fault  Last Valid Test
-----
Gi0/1   Pair 1  OK          0 m     Wed May 17 05:54:16 2023
        Pair 2  OK          0 m
        Pair 3  OK          0 m
        Pair 4  OK          0 m
Cable Diagnostics Port Status
-----
Port    Pair  Status      Distance Date of
        Pair  to Fault  Last Valid Test
```

Port Status, presents the following data for the **PoE Switches**:

- Cable Diagnostic
- Port Enable
- Port Disable
- PoE Enable
- PoE Disable
- PoE Toggle

Cable Diagnostic

Navigate to **Tools > Status > Port Status**, select the Port and click **Cable Diagnostic**, the following output is displayed:

cnMatrix > TX2020RP-B0D980

Dashboard Notifications Configuration Details Performance Software Update **Tools** Assists X

Status Remote CLI Network Connectivity

cnMatrix TX2020R-P

Online

Port Status - Port 1

Warning: Port operation can be reverted to the Switch Port configuration during next config sync. Auto-sync should be disabled in the Switch Group to avoid this from happening.

Cable Diagnostic X Port Enable Port Disable PoE Enable PoE Disable PoE Toggle

Output

Complete

```
Device->config terminal; cable-diagnostics test inter gi 0/1 force
Warning: Deprecated command, use "test cable-diagnostics" from exec mode
% Cable diagnostics test has started for interface Gi0/1
Device->show cable-diagnostics inter gi 0/1;
Cable Diagnostics Port Status
-----
Port   Pair  Status      Distance  Date of
      to Fault Last Valid Test
-----
Gi0/1  Pair 1 OK          0 m      Wed May 17 05:54:16 2023
      Pair 2 OK          0 m
      Pair 3 OK          0 m
      Pair 4 OK          0 m
Cable Diagnostics Port Status
-----
Port   Pair  Status      Distance  Date of
      to Fault Last Valid Test
```

- Download the generated output by clicking the download (📄) icon.
- Clear the generated output by clicking the delete (✕) icon.

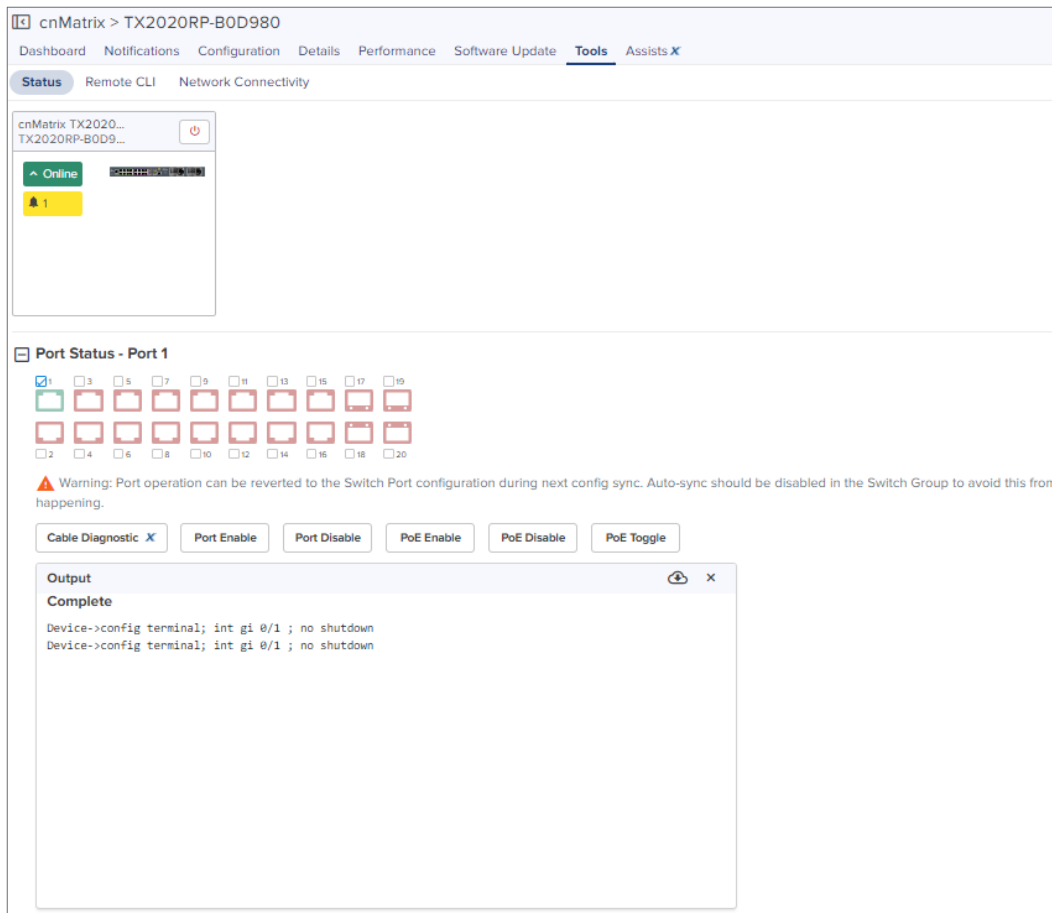


Note

Cable Diagnostic is a cnMaestro X feature.

Port Enable or Port Disable

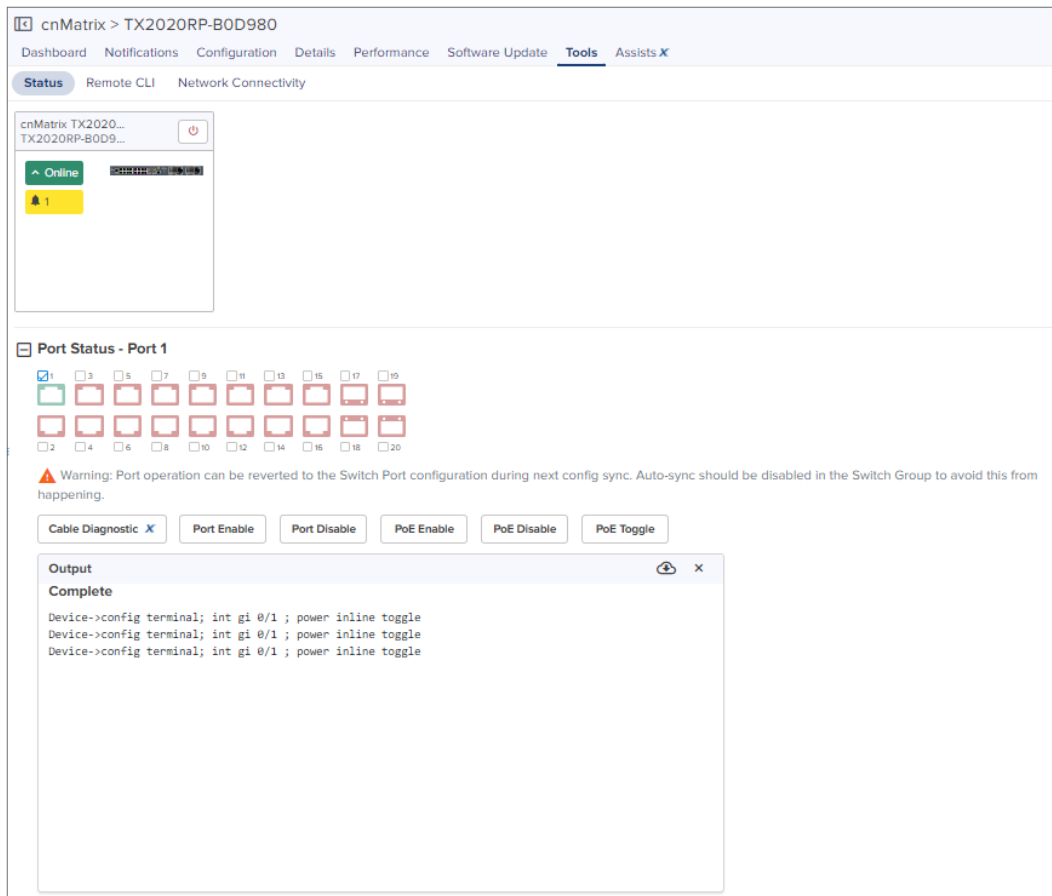
Navigate to **Tools > Status > Port Status**, select the Port and click **Port Disable** or **Port Enable**, the following output is displayed:



- Download the generated output by clicking the download (📄) icon.
- Clear the generated output by clicking the delete (✖) icon.

PoE Toggle

Navigate to **Tools > Status > Port Status**, select the Port and click **PoE Toggle**, the following output is displayed:



- Download the generated output by clicking the download (📄) icon.
- Clear the generated output by clicking the delete (✕) icon.

PoE Enable or PoE Disable

Navigate to **Tools > Status > Port Status**, select the Port and click **PoE Enable** or **PoE Disable**, the following output is displayed:

cnMatrix > TX2020RP-B0D980
Dashboard
Notifications
Configuration
Details
Performance
Software Update
Tools
Assists

Status
Remote CLI
Network Connectivity

cnMatrix TX2020...
TX2020RP-B0D9...

Online

Port Status - Port 1

☒ 1
☐ 3
☐ 5
☐ 7
☐ 9
☐ 11
☐ 13
☐ 15
☐ 17
☐ 19

☐ 2
☐ 4
☐ 6
☐ 8
☐ 10
☐ 12
☐ 14
☐ 16
☐ 18
☐ 20

Warning: Port operation can be reverted to the Switch Port configuration during next config sync. Auto-sync should be disabled in the Switch Group to avoid this from happening.

Cable Diagnostic
Port Enable
Port Disable
PoE Enable
PoE Disable
PoE Toggle

Output

Complete

Device->config terminal; int gi 0/1 ; power inline auto
Device->config terminal; int gi 0/1 ; power inline auto
Device->config terminal; int gi 0/1 ; power inline auto


Port Status, presents the following port status for the **non-PoE Switches**:

- Cable Diagnostic
- Port Enable
- Port Disable

cnMatrix >
Dashboard
Notifications
Configuration
Details
Performance
Software Update
Tools


Status
Remote CLI
Network Connectivity

Online
0



Port Status - Port 5

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28



Cable Diagnostic
Port Enable
Port Disable

Output
Complete
Device->config terminal; cable-diagnostics test inter gi 0/5 force
%Cable diagnostics test has started for interface Gi0/5
Device->show cable-diagnostics inter gi 0/5;
Cable Diagnostics Port Status

Port	Pair	Status	Distance to Fault	Date of Last Valid Test
Gi0/5	Pair 1	Test in Progress	0 m	Tue Nov 9 08:31:55 2021
	Pair 2	Test in Progress	0 m	
	Pair 3	Test in Progress	0 m	
	Pair 4	Test in Progress	0 m	

Remote CLI

Navigate to **Tools > Remote CLI**, when you select a command type and click **Run**, the following output is displayed:

cnMatrix > EX1028P-F61240
Dashboard
Notifications
Configuration
Details
Performance
Software Update
Tools

Status
Remote CLI
Network Connectivity

Command
Type CLI command ⓘ

Run

Output

cnMatrix > cnMatrix-EX2010

Dashboard
Notifications
Configuration
Details
Performance
Software Update
Tools

Status
Remote CLI
Network Connectivity

Command

Type CLI command

Run

Output

```

Policy-1 match rule Rule-1 set action Action-1
poa policy Policy-1 precedence 100 enable
vlan 2
ip arp inspection
!
vlan 3
ip arp inspection
!
vlan 4
ip arp inspection
!
vlan 5
ip arp inspection
!
vlan 6
ip arp inspection
!
cnmaestro url "10.110.209.84"
end

```

- Download the generated output by clicking the download (📄) icon.
- Clear the generated output by clicking the delete (✕) icon.

cnMatrix > TX2012RP-AD7700

Dashboard
Notifications
Configuration
Details
Performance
Software Update
Tools
Assists X

Status
Remote CLI
Network Connectivity

Test Type

Ping

Network ping to a hostname or IP address.

IP Address or Hostname

www.google.com

Number of Packets (-c)

3

Min = 1, Max = 10

Buffer Size (-s)

56

Min = 1, Max = 65507

Start Ping

Ping Result

Complete

Hostname www.google.com

PING www.google.com (142.250.193.132): 56 data bytes
64 bytes from 142.250.193.132: seq=0 ttl=59 time=10.478 ms
64 bytes from 142.250.193.132: seq=1 ttl=59 time=10.453 ms
64 bytes from 142.250.193.132: seq=2 ttl=59 time=10.320 ms

--- www.google.com ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 10.320/10.417/10.478 ms

cnPilot Home Tools

The Tools page for cnPilot Home devices consolidates a number of operations into a single troubleshooting interface. The operations of cnPilot Home are listed in the table below:

Table 30 *cnPilot Home*

Tools	Description
Debug	Displays the log details.
Network Connectivity	Executes Ping, DNS, or Traceroute tests.
Packet Capture	Lists packet capture details.
Status	Displays the Status of device.
Wi-Fi Analyzer	Displays radio traffic and signal.
Wi-Fi Performance	Wi-Fi performance measures the backhaul speed across devices with respect to cnMaestro.

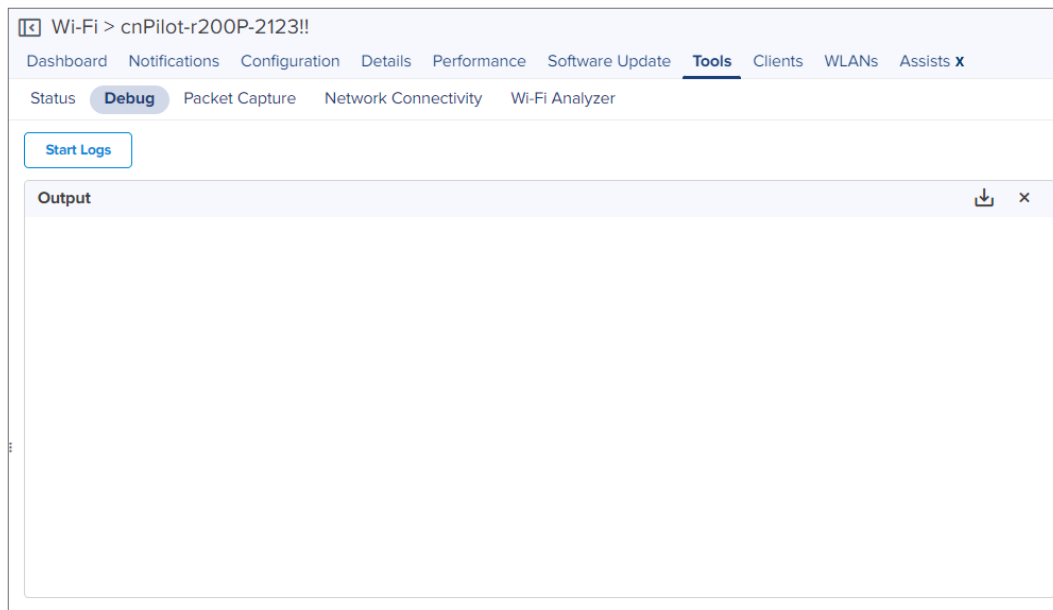
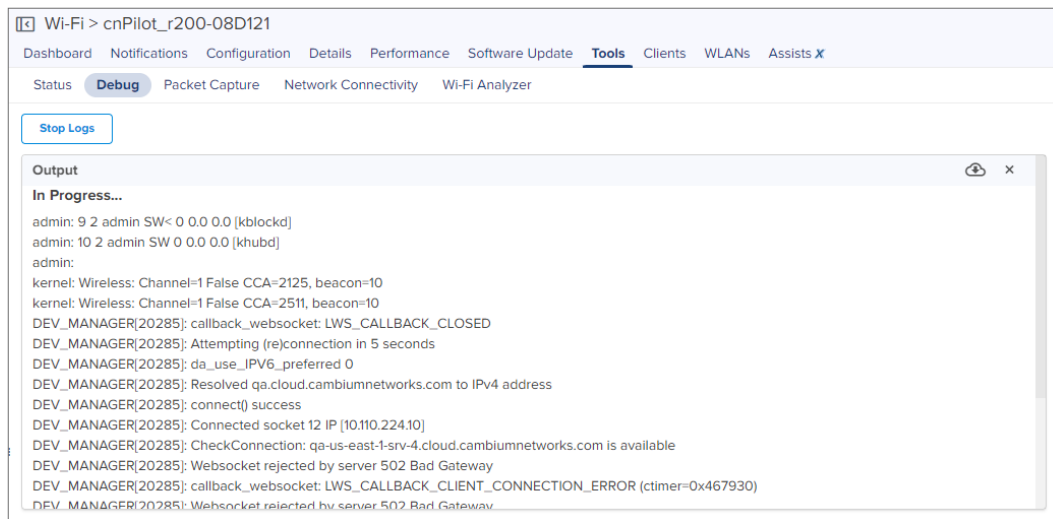
Figure 166 *cnPilot Tools***Figure 167** *cnPilot Debug Tools*

Figure 168 *cnPilot Tools Status*

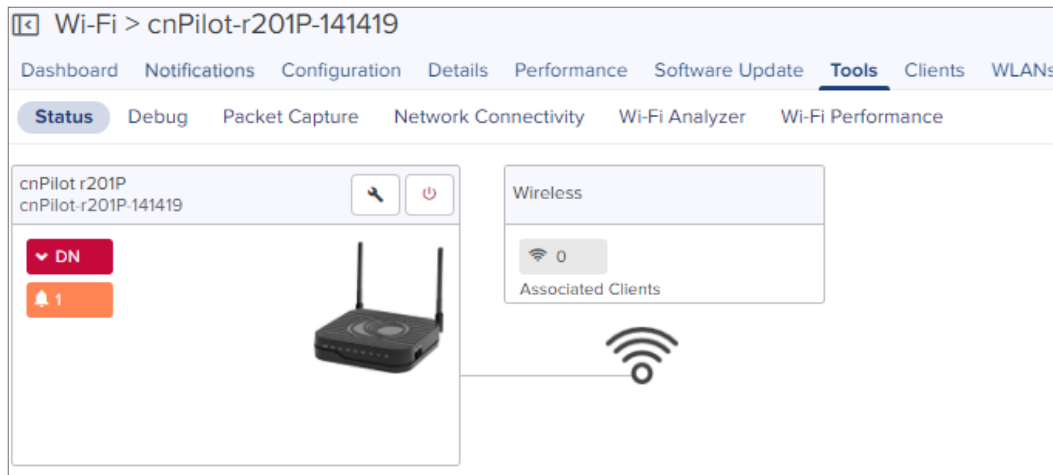


Figure 169 *cnPilot Tools > Packet Capture*

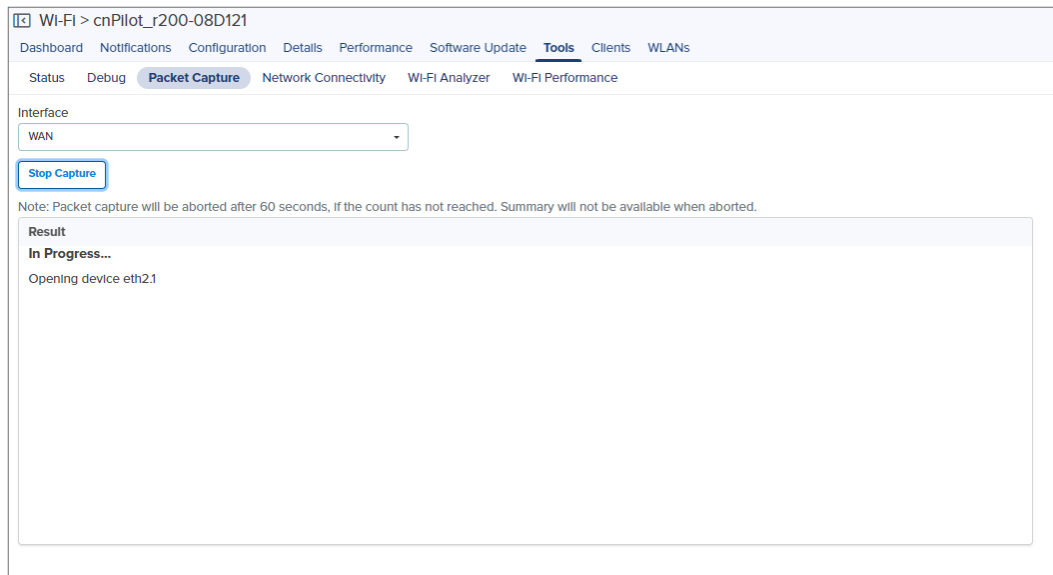


Figure 170 *cnPilot Tools > Network Connectivity*

Wi-Fi > cnPilot_r200-08D121

Dashboard Notifications Configuration Details Performance Software Update **Tools** Clients WLANs

Status Debug Packet Capture **Network Connectivity** Wi-Fi Analyzer Wi-Fi Performance

Test Type
Ping Network ping to a hostname or IP address.

IP Address or Hostname
Enter a valid < IP Address / Hostname >

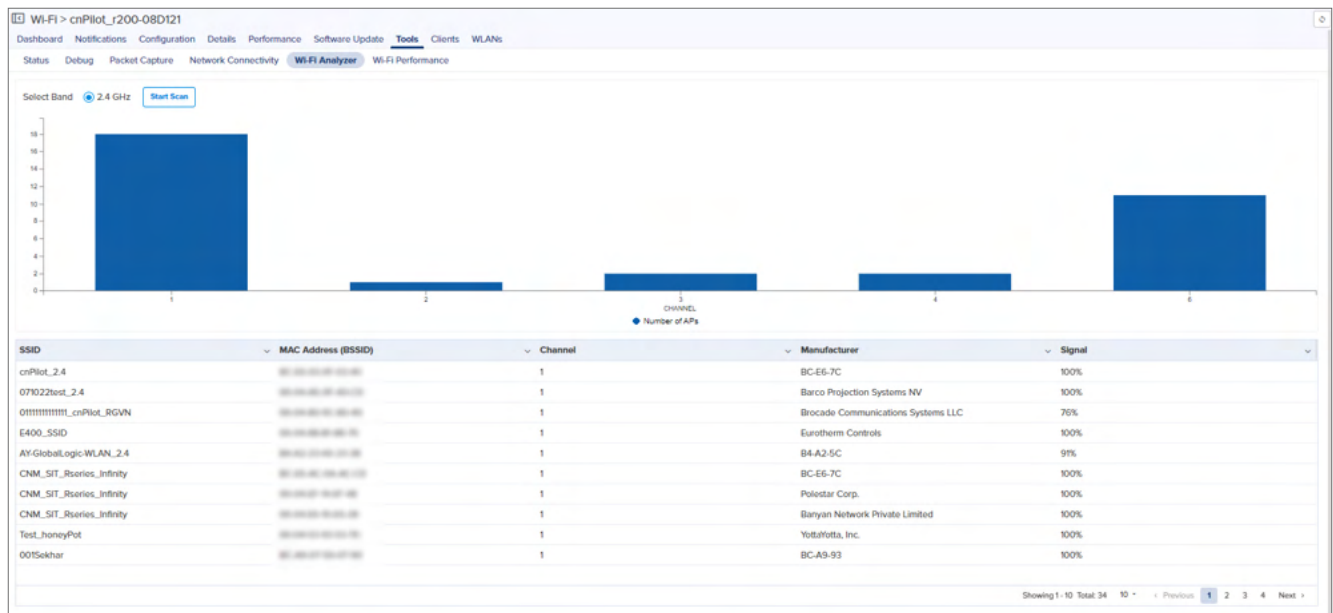
Number of Packets (-c)
3 Min = 1, Max = 10

Buffer Size (-s)
56 Min = 1, Max = 65507

Start Ping

Ping Result

Figure 171 *cnPilot Tools > Network Connectivity*



cnRanger Tools

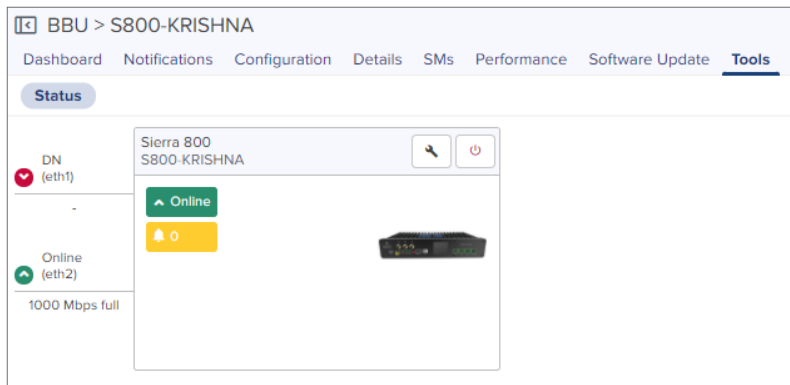


Note

cnMaestro supports the tools page of cnRanger from device version 2.1.0.0-r3.

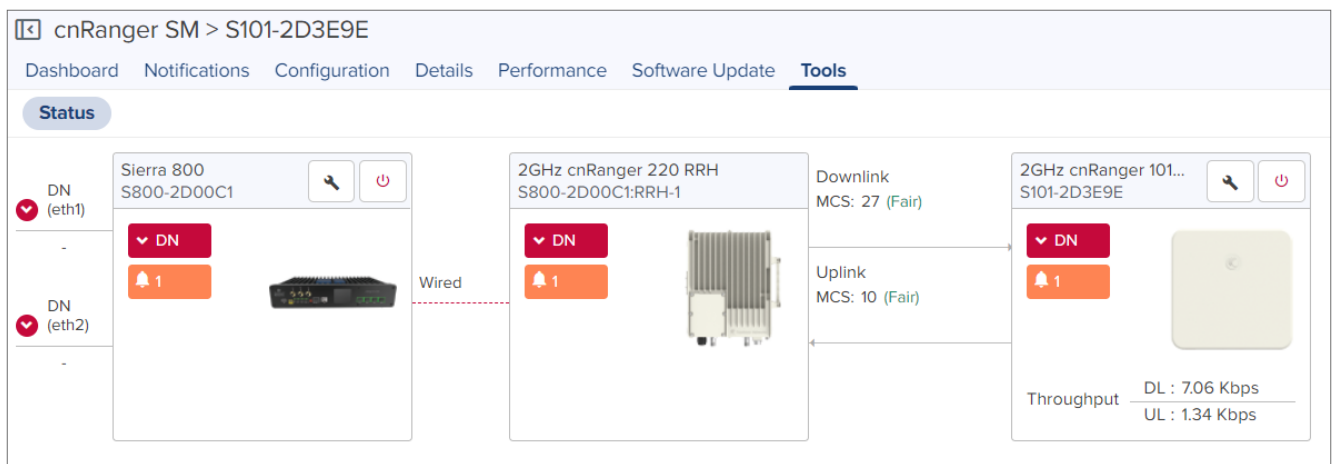
cnRanger BBU

In **Status** tab, user can view the status of the device either Online or Offline. It also supports downloading Tech Support File and rebooting the device.



cnRanger SM

In **Status** tab, user can view the status of the device (either Online or Offline), It also supports downloading the Tech Support File, displaying the wired connectivity status, and rebooting the device.



cnReach Tools

The Tools page for cnReach devices consolidates a number of operations into a single troubleshooting interface. The operations are listed below:

Table 31 *cnReach Tools*

Tools	Description
Ping	Network ping to a hostname or IP address.
RF Ping	RF reachability test between local radios that provides details on signal quality.
RF Throughput	RF throughput test between local radios that provides details on throughput.

Figure 172 *cnReach Tools*

cnReach > Bridge_Mode_AP_Edit_11

Dashboard Notifications Configuration Details Performance Software Update **Tools**

Radio 1 **Network Connectivity**

Test Type
Ping Network ping to a hostname or IP address.

IP Address or Hostname
www.cambiumnetworks.com

Number of Packets (-c)
5 Min = 1, Max = 10

Buffer Size (-s)
32 Min = 1, Max = 65507

Start Ping

Ping Result
Complete
Hostname www.cambiumnetworks.com

PING www.cambiumnetworks.com (18.190.92.212): 32 data bytes
 40 bytes from 18.190.92.212: seq=0 ttl=226 time=243.345 ms
 40 bytes from 18.190.92.212: seq=1 ttl=226 time=245.100 ms
 40 bytes from 18.190.92.212: seq=2 ttl=226 time=242.973 ms
 40 bytes from 18.190.92.212: seq=3 ttl=226 time=244.276 ms
 40 bytes from 18.190.92.212: seq=4 ttl=226 time=243.404 ms

--- www.cambiumnetworks.com ping statistics ---
 5 packets transmitted, 5 packets received, 0% packet loss
 round-trip min/avg/max = 242.973/243.819/245.100 ms

cnVision Tools

The Tools page for cnVision devices consolidates a number of operations into a single troubleshooting interface. The operations are listed below:

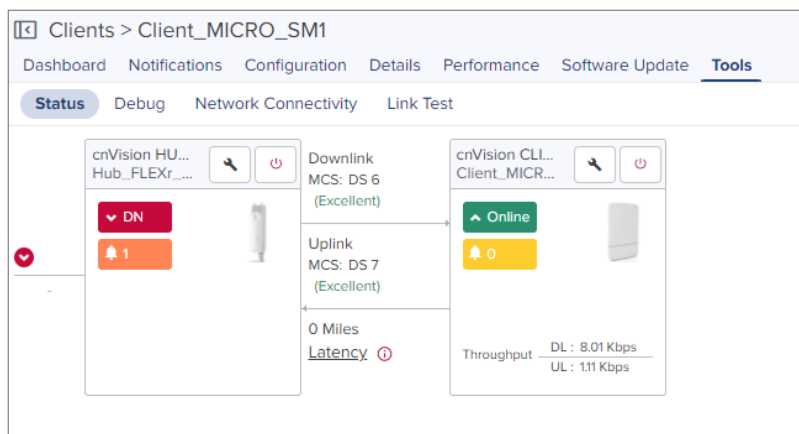
Table 32 *cnVision Tools*

Field	Description
Debug	Displays the log details.
Network Connectivity	Executes Ping, DNS, or Traceroute tests.
Status	Displays the Status.
Subscriber Modules	Displays the SM linked to the Hub and supports reboot and download the Tech Support File.
Link Test	<p>The Link Capacity Test measures the throughput of the RF link between two cnVision modules. cnVision Link Test only utilizes the spare sector capacity for this test; therefore, sector traffic will not be disrupted. For the most accurate wireless link test results, it is best to run this test when there is minimal customer data traffic.</p> <p>Displays the link related test result for Throughput. Link Test can be performed on the cnVision Hub and its SM link. To run this operation, select the device and then the Tools tab.</p>

Table 32 *cnVision Tools*

Field	Description
	<ul style="list-style-type: none"> If cnVision Hub is selected you can choose the SM from the list and start the test. <div data-bbox="406 245 1079 594" data-label="Image"> </div> Displays the following fields: <ul style="list-style-type: none"> Packet Size: Choose the Packet Size to use for the throughput test. Duration: Choose the time duration in seconds to use for the throughput test. If a cnVision Client is selected, click Start Test to run the Link Test. <div data-bbox="406 816 1079 1165" data-label="Image"> </div> Displays the following fields: <ul style="list-style-type: none"> Packet Size: Choose the packet size to use for the throughput test. Duration: Choose the time duration in seconds to use for the throughput test.

Figure 173 *cnVision Tools*



Edge Controller Tools

For details on Tools section, refer to Edge Controller User Guide.

Enterprise Wi-Fi Tools

The Tools page for Enterprise Wi-Fi devices consolidates a number of operations into a single troubleshooting interface.



Note

Both IPv4 and IPv6 addresses are supported for all the troubleshooting operations.

The operations of Enterprise Wi-Fi are listed below:

Table 33 Enterprise Wi-Fi Tools

Tools	Description
Debug	Displays the log details.
Flash LEDs (only Enterprise Wi-Fi devices)	Flash LED indicates that a device is ready to receive the signal.
Network Connectivity	Executes Ping, DNS, or Traceroute tests.
Packet Capture	Lists packet capture details. <div> <p>Note When AP packet capture is configured at the radio or wireless LAN interface, the AP records data only from the nearby APs. It does not capture its own transmissions like beacon frames or SSID broadcasts.</p> </div>
Remote CLI	Enter CLI command in the command text box to execute on device. <ul style="list-style-type: none"> Only Show command is allowed for Operator users. All CLI commands are supported by Super Admin and Admin users.
Status	Displays the Status of device.
Wi-Fi Analyzer	Displays radio traffic and signal.
Wi-Fi Performance	Wi-Fi performance measures the backhaul speed across devices with respect to cnMaestro.

Figure 174 Enterprise Wi-Fi Tools

The screenshot shows the 'Wi-Fi > E500-BB15702' interface. The 'Tools' tab is selected, and the 'Debug' sub-tab is active. A 'Stop Logs' button is visible. The 'Output' window displays the following log entries:

```

2021-05-25 07:05:27 749 device-agent.c:667-PING_DATA: len=28 msg [{"Pid": "749", "Ploss": "0"}]
May 25 07:05:27: wifid : notify msg type CMB_NOTIFY_MSG_TYPE_NEIGH_AP_DATA[21] received (cache.c:2871)
May 25 07:05:30: wifid : notify msg type CMB_NOTIFY_MSG_TYPE_NEIGH_AP_DATA[21] received (cache.c:2871)
May 25 07:05:33: scmd : prev_tx 150983395 curr_tx 0 (stats.c:1052)
May 25 07:05:33: scmd : prev_rx 1034060344 curr_rx 0 eth index 0 (stats.c:1053)
May 25 07:05:34: wifid : notify msg type CMB_NOTIFY_MSG_TYPE_NEIGH_AP_DATA[21] received (cache.c:2871)
May 25 07:05:40: wifid : notify msg type CMB_NOTIFY_MSG_TYPE_NEIGH_AP_DATA[21] received (cache.c:2871)
May 25 07:05:43: wifid : lldp frame:dmac 01-80-C2-00-00-0E smac B0-B9-8A-6E-F1-03 type 88cc (lldp.c:89)
May 25 07:05:46: scmd : stats timer at 1621926346 (stats.c:196)
2021-05-25 07:05:52 749 device-agent.c:667-PING_DATA: len=28 msg [{"Pid": "749", "Ploss": "0"}]
2021-05-25 07:11:09 749 log.c:207:start_cns_logging: Send log history (10 lines)
May 25 07:05:54: scmd : Device IP 10.110.208.137 (stats.c:346)
2021-05-25 07:05:54 749 wifid:948:Stats read successfully cleanup g_scm_fd
  
```

Figure 175 Enterprise Wi-Fi Packet Capture

Interface	Packets	Duration	Size	Filter	Start Time	Expires In	Status
Tunnel (bcp0)	241	2m/2m	28.3 KB/10 MB	-	07 Oct 2021 21:47	0d 0h 0m	Uploaded
Radio1	28565	1m 45s/2m	10.0 MB/10 MB	-	07 Oct 2021 21:47	0d 0h 0m	Uploaded
Vlan 1	5296	1m 59s/2m	4.3 MB/10 MB	-	07 Oct 2021 21:47	0d 0h 0m	Uploaded
Eth1	5475	2m/2m	4.3 MB/10 MB	-	07 Oct 2021 21:47	0d 0h 0m	Uploaded
Radio3 (Channel: 2)	874	4s/2m	348.1 KB/10 MB	(type mgt subtype beacon)	07 Oct 2021 21:42	0d 0h 0m	Uploaded
Radio1	0	2m	10 MB	-	07 Oct 2021 21:40	-	Failed
SSID (diva_pact)	986	1m 59s/2m	83.2 KB/10 MB	-	07 Oct 2021 21:38	0d 0h 0m	Uploaded
Vlan 50	29	2m/2m	2.4 KB/10 MB	-	07 Oct 2021 21:35	0d 0h 0m	Uploaded
Vlan 215	0	2m	10 MB	-	11 Oct 2021 13:17	-	Failed
Vlan 115	6	51s/2m	2.1 KB/10 MB	-	07 Oct 2021 21:34	0d 0h 0m	Uploaded

Showing 1 - 10 Total: 23 10 < Previous 1 2 3 Next >

Figure 176 Enterprise Wi-Fi Remote CLI Tools

Command

Type CLI command

Run

Output

In Progress...

Device >

Device > show config

```
!
management user admin password $crypt$1$bC50U7LVxFK9C5sE5ZpFOgYI7ssnfRYm
no management radius-auth
management cambium-remote
management cambium-remote url 10.10.209.84
management cambium-remote validate-server-cert
no management telnet
management ssh
management ssh idle-timeout 300
management http
management http port 80
management https
management https port 443
```

Figure 177 Flash LEDs

Duration

10

Flash LED (1-120) seconds

Flash LEDs

Packet Capture

Packet Capture allows the user to capture all packets on a specified interface. The user can trigger packet capture on an interface (or multiple interfaces simultaneously).



Note

Enhanced packet capture is available for version 6.4 or higher in Enterprise devices.

Wi-Fi > E400-922372

Dashboard Notifications Configuration Details Performance Software Update **Tools** Clients Mesh Peers WLANs WIDS X

Status Debug Remote CLI **Packet Capture** Network Connectivity Wi-Fi Analyzer Wi-Fi Performance Flash LEDs

Interface
 Ethernet 1 Min = 1, Max = 2

Source IP/Destination IP
 Source IP Destination IP

Source MAC/Destination MAC
 Source MAC Destination MAC

Direction
 Both

Count
 E.g.: 100

Filter
 E.g.: icmp[icmpype] == 8

Start Capture

Note: Packet capture will be aborted after 60 seconds, if the count has not reached. Summary will not be available when aborted.

Result

To view Packet Capture, navigate to **Network** or **Site > Wi-Fi AP > Tools > Packet Capture**.

Wi-Fi > XV2-22H-E0477

Dashboard Notifications Configuration Details Performance Software Update **Tools** Clients Mesh Peers WLANs Assists X

Status Debug Remote CLI **Packet Capture** Network Connectivity Wi-Fi Analyzer Flash LEDs

Delete Start New Packet Capture

Interface	Packets	Duration	Size	Filter	Start Time	Expires In	Status
No Data Available							

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

Table 34 *Packet Capture fields*

Field	Description
Duration	Represents packet capture running duration in seconds versus maximum duration configured.
Expires In	Expiry time of packet capture. The default is 24 hours.
Filter	Type of filter.
Interface	The following interfaces are supported: <ul style="list-style-type: none"> BRIDGE Ethernet PPPoE

Table 34 *Packet Capture fields*

Field	Description
	<ul style="list-style-type: none">• Radio• SSID• TUNNEL• VLAN• Wireless LAN
Packets	Represents number of packets captured versus maximum limit of packet count configured.
Size	Current packet capture size versus maximum packet capture size configured.
Start Time	Start time of the capture.
Status	Status of packet captured is as follows: <ul style="list-style-type: none">• Aborted• Failed• Queued• Skipped

Configuring a new packet capture

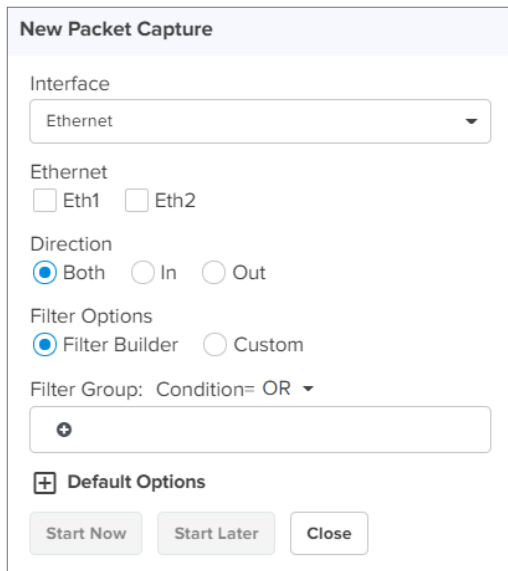
Perform the following steps to start a new packet capture:



Note

- Filter options vary for different interfaces (Radio, Wireless LAN, VLAN, SSID, TUNNEL, BRIDGE, and PPPoE. Radio, SSID has wireless 802.11 filters, other interfaces has wired 802.3 filters).
- User can also add custom filters if needed.
- Packet Capture on **Radio** interface is available only for online Enterprise Wi-Fi XV-Series and XE-Series.

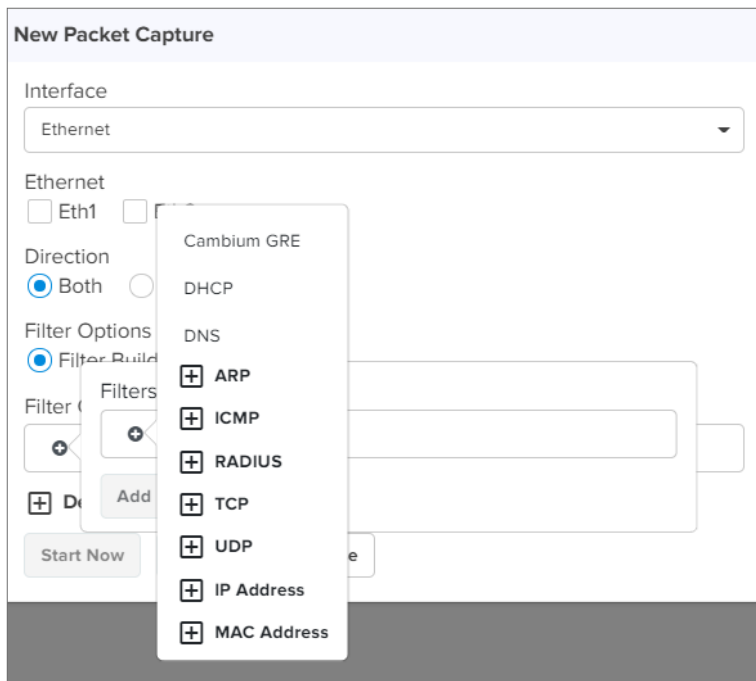
1. Click **New Packet Capture** to start packet capture.



The 'New Packet Capture' dialog box is shown. It has a title bar 'New Packet Capture'. Below it, there is a section 'Interface' with a dropdown menu showing 'Ethernet'. Under 'Ethernet', there are two checkboxes: 'Eth1' and 'Eth2'. Below that is a 'Direction' section with three radio buttons: 'Both' (selected), 'In', and 'Out'. Then is a 'Filter Options' section with two radio buttons: 'Filter Builder' (selected) and 'Custom'. Below that is a 'Filter Group' section with a label 'Condition= OR' and a dropdown arrow. There is a text input field with a plus icon. At the bottom left is a button '+ Default Options'. At the bottom right are three buttons: 'Start Now', 'Start Later', and 'Close'.

2. Select the **Interface** type from the dropdown.
3. Select **Ethernet** as **Eth1** or **Eth2**.
4. Choose the **Direction** as **Both**, **In**, or **Out**.
5. Select **Filter options** as **Filter Builder** or **Custom**.

You can filter the packets captured by specifying Cambium GRE, DHCP, DNS, ARP, ICMP, Radius, TCP, UDP, IP Address, and MAC Address.



The 'New Packet Capture' dialog box is shown with a menu open over the 'Filter Options' section. The menu lists the following filter options: Cambium GRE, DHCP, DNS, ARP, ICMP, RADIUS, TCP, UDP, IP Address, and MAC Address. Each option has a plus icon next to it. The background of the dialog box is slightly dimmed.

6. Click **Default Options** to configure **Packets**, **Duration**, **Packet Length**, and **File Size**.

New Packet Capture

Interface
 Ethernet

Ethernet
☐ Eth1 ☐ Eth2

Direction
☒ Both ☐ In ☐ Out

Filter Options
☒ Filter Builder ☐ Custom

Filter Group: Condition= OR

+

Default Options

Packets
 0
 0 to 65535 (default 0 indicates unlimited)

Duration
 120
 1 to 600 (default 120) seconds

Packet Length
 0
 0 to 1500 (default 0 indicates full packet length)

File Size
 10
 1 to 50 (default is 10 MB on 11ax APs)

Start Now Start Later Close

- Click **Start Now** to capture the packets immediately, or start the capture later by selecting **Start Later** option. The progress of packets captured can be seen in the **Status** field.
- Click the download (↓) icon to download the capture in **PCAP** file format.



Note

For cnMaestro X, a maximum of four packet capture sessions are supported, whereas for cnMaestro Essentials a maximum of two packet capture sessions are supported.

The user can **Edit**, **Clone**, and **Delete** the packets capture entry. Packet Capture entries can be cloned depending on the type of interface selected for the capture.

Search

Networks AP Groups

System

- Base Infrastructure
 - default
 - D_Zone
 - #123
 - _site
 - E41C
 - WBV**
 - XV2
 - XV3
 - dev
 - mSp@123

Wi-Fi > W8VK0CQ523F1

Dashboard Notifications Configuration Details Performance Software Update **Tools** Clients Mesh Peers X WLANs

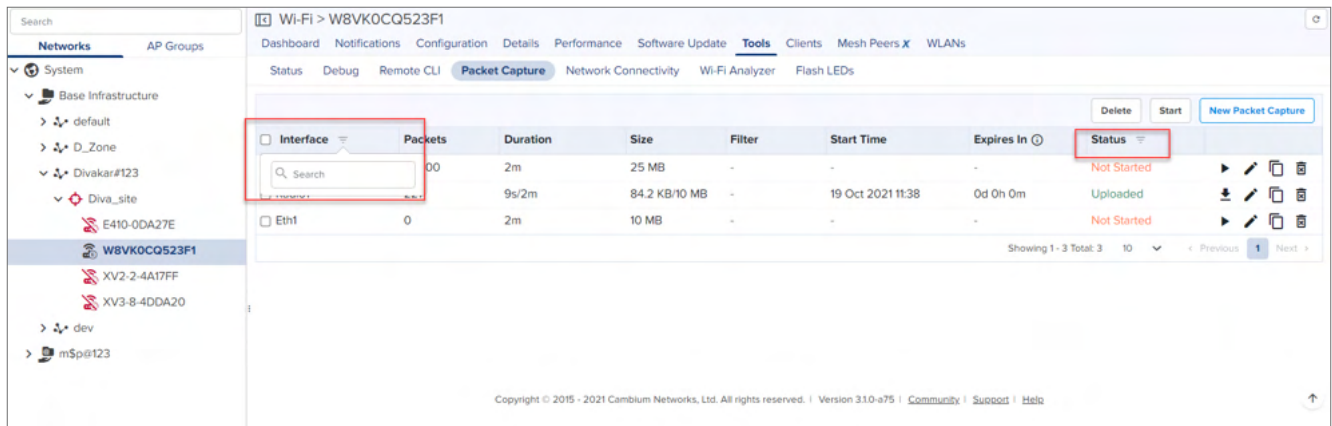
Status Debug Remote CLI **Packet Capture** Network Connectivity Wi-Fi Analyzer Flash LEDs

Delete Start New Packet Capture

Interface	Packets	Duration	Size	Filter	Start Time	Expires In	Status	
<input type="checkbox"/> Radio1	227	9s/2m	84.2 KB/10 MB	-	19 Oct 2021 11:38	0d 15h 51m	Uploaded	↓ ✎ 📄 🗑
<input type="checkbox"/> Eth1	0	2m	10 MB	-	-	-	Not Started	▶ ✎ 📄 🗑

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

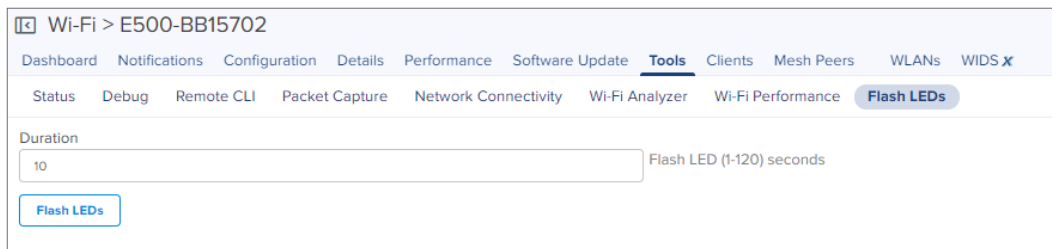
The user can search the packet capture by **Interface** type and **Status**.



Note

- User can start packet capture by clicking the **Play** button. This also works if the packet capture is stopped at **Not Started/Failed/ Expired**.
- **Bulk Start** and **Bulk Delete** are performed by selecting multiple packet capture.
- Expired packet capture is deleted from cnMaestro after 7 days.
- Packet capture is removed immediately, when device (AP) is deleted from cnMaestro.
- Packet captures cannot be started on same interface simultaneously.
- Only **Show** command works for the Operator user.

Figure 178 *Flash LEDs*



eMP Tools

The Tools page for eMP devices consolidates a number of operations into a single troubleshooting interface. The operations are listed below:

Table 35 *eMP Tools*

Field	Description
Debug	Displays the log details.
Link Test	<p>The Link Capacity Test measures the throughput of the RF link between two eMP modules. eMP Link Test only utilizes the spare sector capacity for this test, therefore, sector traffic will not be disrupted. For the most accurate wireless link test results, it is best to run this test when there is minimal customer data traffic.</p> <p>Displays the link related test result with respect to Throughput. Link Test can be performed on the eMP AP and its SM link. In order to run this operation, select the device and then the Tools tab.</p> <ul style="list-style-type: none"> • If an eMP AP is selected, choose the SM from the list and start the test.

Table 35 *ePMP Tools*

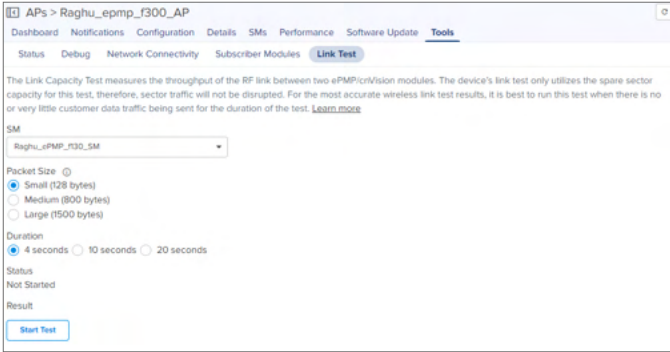
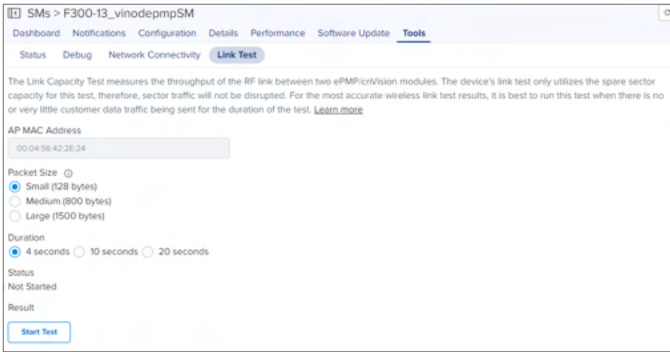
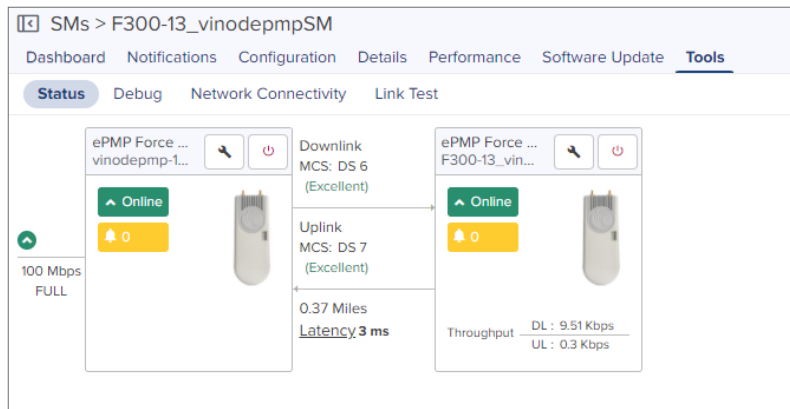
Field	Description
	 <p>Displays the following fields:</p> <ul style="list-style-type: none"> ◦ Packet Size: Choose the Packet Size to use for the throughput test. ◦ Duration: Choose the time duration in seconds to use for the throughput test. • If an ePMP SM is selected, click Start Test to run the link test.  <p>Displays the following fields:</p> <ul style="list-style-type: none"> ◦ Packet Size: Choose the Packet Size to use for the throughput test. ◦ Duration: Choose the time duration in seconds to use for the throughput test.
Network Connectivity	Executes Ping, DNS, or Traceroute tests.
Status	Displays the status.
Subscriber Modules	Displays the Subscriber Modules details.

Figure 179 ePMP Tools



PMP Tools

The Tools page for PMP devices consolidates a number of operations into a single troubleshooting interface. The operations are listed below:

Table 36 PMP Tools

Field	Description
Debug	Displays the log details.
Link Test	<p>The Link Capacity Test measures the throughput and efficiency of the RF link between two PMP modules. Many factors, including packet length, affect throughput. Packets are added to one or more queues in the AP to fill the frame. Throughput and efficiency are then calculated during the test.</p> <p>The Link Capacity Test tool has the following modes:</p> <ul style="list-style-type: none"> Flood Link Test: Tests the link's performance by flooding it with heavy traffic and assesses link's behavior under extreme network loads. An addition Multiple LUIDs option is available in the Current SM dropdown list. The Multiple LUIDs feature allows users to specify LUIDs, including single numbers (for example, 23, 32), or to conduct the flood test with ranges (for example, 2-22) as shown in Figure 180. <p>Figure 180 Flood Link Test: PMP 450m AP</p> <p>Note</p> <p>Flood Link Test is applicable only for 450m APs.</p> <ul style="list-style-type: none"> Link Test without Bridging: Tests radio-to-radio communication, but does not bridge traffic. Link Test with Bridging: Bridges traffic to “simulated” Ethernet ports, providing a status of the

Table 36 *PMP Tools*

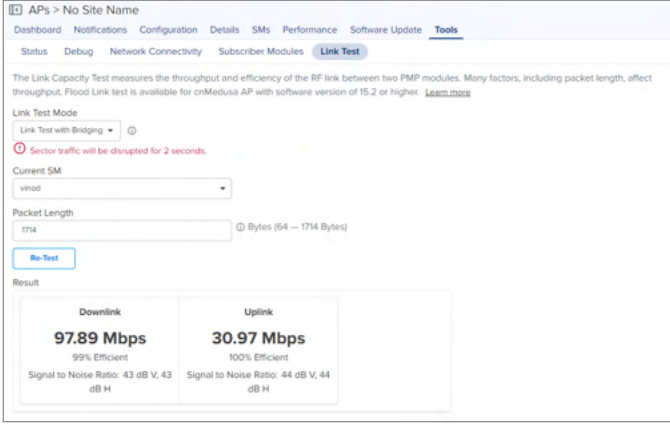
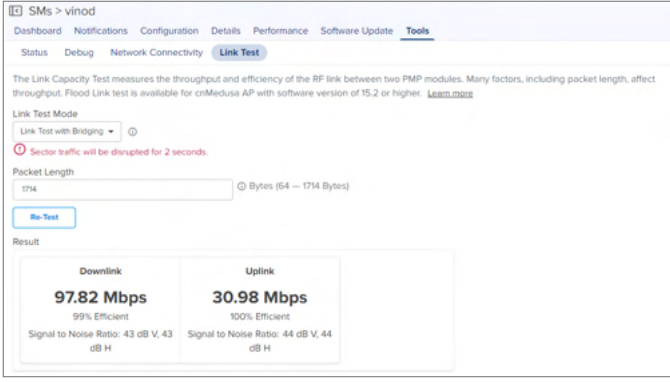
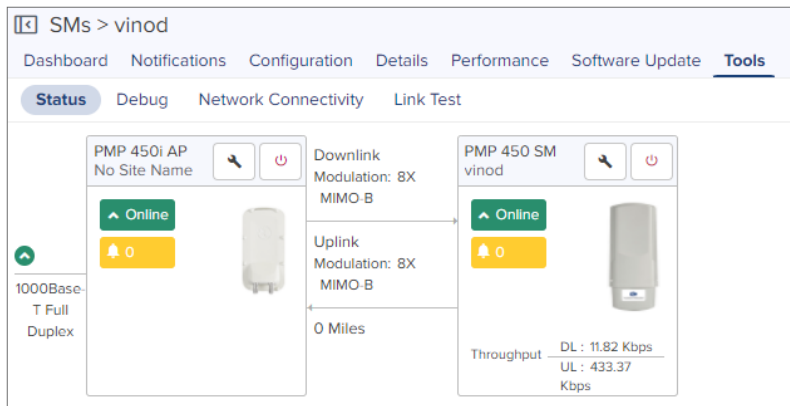
Field	Description
	<p>bridged link.</p> <ul style="list-style-type: none"> • Link Test with Bridging and MIR: Bridges the traffic during test and also adheres to any MIR (Maximum Information Rate) settings for the link. • Extrapolated Link Test: Estimates the link capacity by sending few packets and measuring link quality. <p>Displays the link related test result with respect to Throughput and Interference. Link Test can be performed on the PMP AP and its SM link. To run this operation, select the device and then the Tools tab.</p> <ul style="list-style-type: none"> • If a PMP AP is selected you can choose the SM from the list and start the test.  <ul style="list-style-type: none"> • If a PMP SM is selected, click Start Test to run the Link Test. 
Network Connectivity	Executes Ping, DNS, or Traceroute tests.
Status	Displays the status.
Subscriber Modules	Lists all the SMs connected to the selected AP. This is available for PMP APs only.

Figure 181 *PMP Tools*

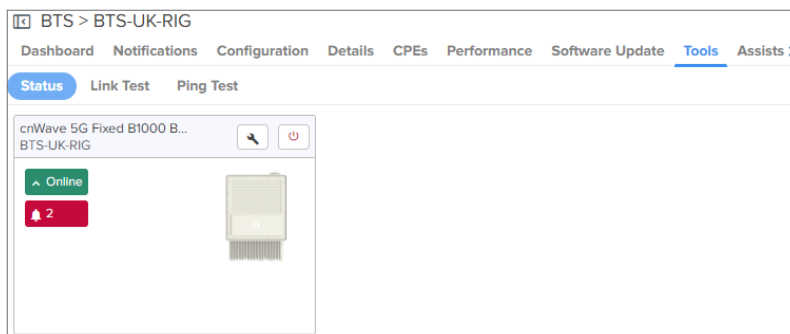


cnWave 5G Fixed Tools

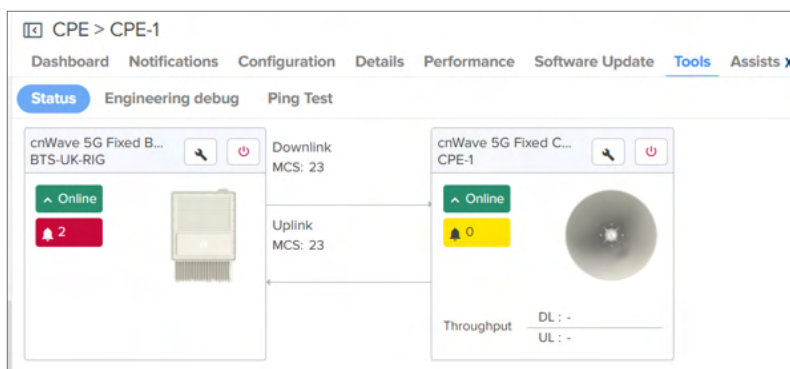
For cnWave 5G Fixed products (BTS and CPE), the **Tools** page in cnMaestro contains the following tabs:

Status

The Status page displays device connection state (online or offline) for the BTS and a CPE. To access the Status page, go to **Monitor and Manage > BTS > Tools**. The following figure is an example of the **Tools > Status** page for the BTS:



To view the status of the link between the BTS and CPE modules, select a CPE under **Monitor and Manage > BTS** and go to the **Tools > Status** page. The following figure is an example of the **Tools > Status** page for a CPE.



Link Test

The **Link Test** tool is applicable only to the BTS device. The **Link Test** Page allows you to test the links (uplink, downlink, or both) and analyze the link performance for a CPE (s). The test output helps in managing the traffic and troubleshooting the links for the selected CPE (s).



Note

The **Link Test** tool is supported only on cnWave 5G Fixed devices running Release

version 3.1 or later.

The **Link Test** tool measures the throughput and utilization of RF link between the BTS and its CPE modules. To conduct a link test between a BTS and its CPE (s), complete the following steps:

1. Go to **Monitor and Manage > BTS > Tools > Link Test**.

The screenshot shows the 'Link Test' configuration page for a specific BTS (BTS-UK-RIG). The page has tabs for 'Status', 'Link Test', and 'Ping Test', with 'Link Test' being the active tab. A descriptive text block explains that the Link Capacity Test measures RF link throughput and utilizes spare sector capacity. Below this, there are input fields for 'CPE' (a dropdown menu), 'Duration (-4)' (a text input with a hint to enter duration in seconds from 5 to 3600), and 'Interval' (a dropdown menu currently set to 5). There are radio buttons for 'Direction' with options: Downlink (selected), Uplink, and Bidirectional. A 'Start Test' button is located below the direction options. At the bottom, a 'Detailed Test Statistics' table is partially visible with columns for 'Device Name', 'MAC', 'DL Throughput (Mbps)', and 'UL Throughput (Mbps)'.

2. Set the parameters, as described in the table below:

Table 37 Parameters on the Link Test page

Parameter	Description
CPE	Name of the CPE device (s) for which you want to conduct the link capacity test. From the CPE dropdown list, select a CPE name or the required multiple CPE names. You can also search for the required CPE name or select all using this dropdown list.
Duration	Duration (in seconds) of the transmission of the traffic that you want to test. This parameter supports the value from 5 - 3600 seconds.
Interval	Time interval (in seconds) at which the test output is updated. This is a read-only parameter. Default value: 5 seconds Note: If you set a value between 5 and 60 seconds in the Duration field, the output is updated every 5 seconds. Similarly, if you set a value between 61 and 3600 seconds, the output is updated every 60 seconds.
Direction	Direction of the transmission of the traffic that you want to test. This parameter supports the following options: <ul style="list-style-type: none">• Downlink• Uplink• Bidirectional Select the required traffic direction.

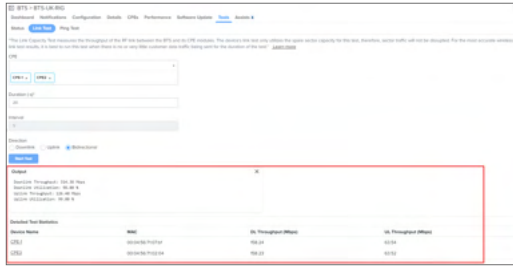
3. Click **Start Test**.

When the test is complete for the set duration, the **Output** section displays the result. You can also click **Stop Test** after running the test for the required period.



Note

If you switch to another tab or page while the link test is running, the test continues without stopping.



The **Detailed Test Statistics** section displays the test result for the selected CPE (s). This section displays CPE name, MAC address, UL throughput and DL throughput (in Mbps). When you click on a CPE name in this section, the respective CPE dashboard page opens. In addition, you can sort and view the statistics in this section.

Ping Test

The **Ping Test** tool helps you to test the connectivity and accessibility of a BTS or CPE to the radio network. This page allows you to verify whether the BTS or CPE is properly connected to your network. For example, BTS connectivity with cnMaestro or a RADIUS server and CPE connectivity with the BTS. This tool is useful for troubleshooting network connection issues.

To run the Ping Test tool, complete the following steps:

1. From the home page, navigate to **Monitor and Manage > BTS network > Tools > Ping Test**.

The **Ping Test** page appears, as shown below.

BTS > BTS-UK-RIG1

Dashboard Notifications Configuration Details CPEs Performance Software Update **Tools** Assists X

Status Engineering debug Link Test **Ping Test**

IP Address or Hostname*

Enter a valid < IP Address / Hostname >

Number of Packets (-c)*

3 Min = 1, Max = 10

Buffer Size (-s)*

56 Min = 1, Max = 65507

Start Ping

Output

2. Set the parameters, as described in the table below.

Table 38 Parameters on the Ping Test page

Parameter	Description
IP Address or Hostname	The valid IP address or a DNS name of the required network or destination. Type an appropriate value in the text box. This is a mandatory parameter.
Number of Packets (-c)	Number of ping packets that has to be sent to the network. Default value: 3 This parameter supports minimum one packet and maximum 10 packets. This is a mandatory parameter.
Buffer Size (-s)	Number of data bytes that have to be sent to the network.

Table 38 Parameters on the Ping Test page

Parameter	Description
	Default value: 56 data bytes, which are translated into 64 ICMP data bytes when combined with the 8 bytes of ICMP header data. This parameter supports a minimum of one data byte and maximum of 65507 data bytes. This is a mandatory parameter.

3. Click **Start Ping**.

The **Output** section displays the test result, as shown below. You can click **Stop Ping** to stop the test.



Note

Similarly, you can run the ping test tool for CPE in the **Monitor and Manage > BTS network > CPE name > Tools > Ping Test** page.

4. Use the download icon in the Output section to download the test result.

RV22 Home Mesh Tools

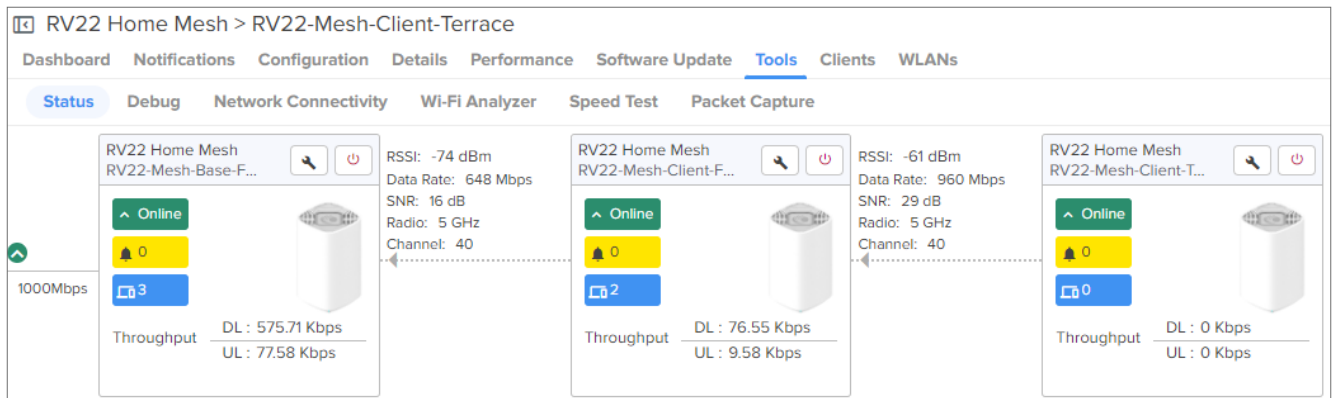
cnMaestro provides the following tools to troubleshoot and debug RV22 Home Mesh routers:

- [Status](#)
- [Debug](#)
- [Network Connectivity](#)
- [Wi-Fi Analyzer](#)
- [Speed Test](#)
- [Packet Capture](#)


To access these tools, navigate to **Monitor and Manage > <RV22-router-name> > Tools**.

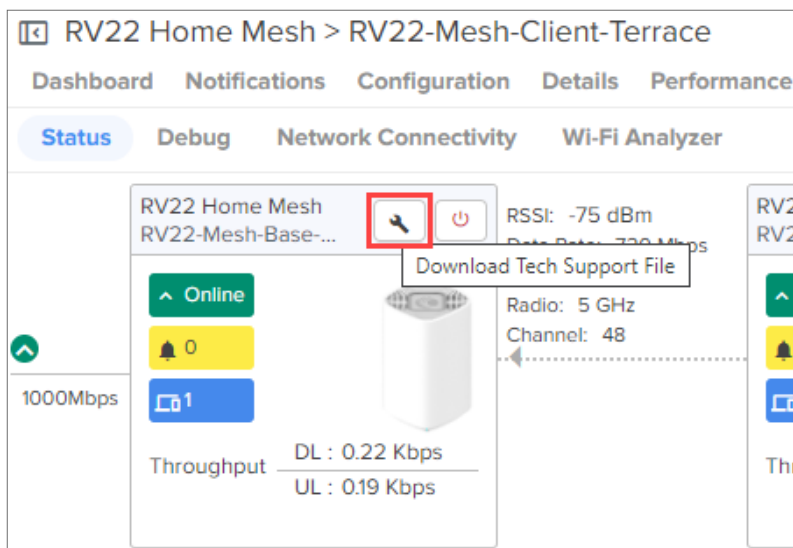
Status

To view the status of the link between the RV22 Home Mesh base and client routers, access the **Status** page under **Monitor and Manage > <RV22-router-name> > Tools**.



Downloading tech support file

To download the tech support file, on the **Status** page, click the **Download Tech Support File** () icon.

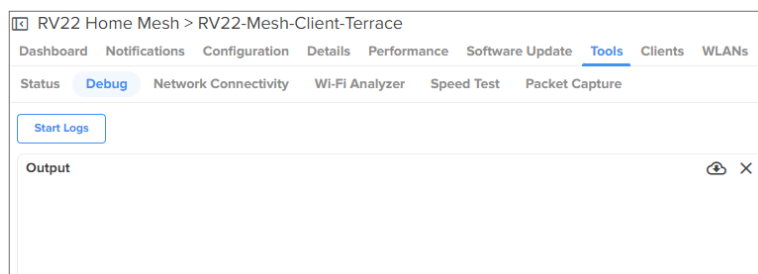


Debug

Displays log information of the RV22 Home Mesh router. To view the debug information:

1. Navigate to **Monitor and Manage** > <RV22-router-name> > **Tools** > **Debug**.
2. Click **Start Logs**.

The log information is displayed in the **Output** window.



Network Connectivity

Provides network connectivity information of the RV22 Home Mesh routers.

The following connectivity tests are available:

- Ping
- DNS Lookup
- Traceroute

To test network connectivity of the router:

1. Navigate to **Monitor and Manage** > <RV22-router-name> > **Tools** > **Network Connectivity**.
2. Select the test type and provide the corresponding parameters required for the test.
3. Click **Start Test**.

cnMaestro initiates the test and displays the result in the <**Test Type**> **Result** window as shown below.

RV22 Home Mesh > RV22-Mesh-Client-Terrace

Dashboard Notifications Configuration Details Performance Software Update **Tools** Clients WLANs

Status Debug **Network Connectivity** Wi-Fi Analyzer Speed Test Packet Capture

Test Type
Ping Network ping to a hostname or IP address.

IP Address or Hostname*
www.cambiumnetworks.com

Number of Packets (-c)
3 Min = 1, Max = 10

Buffer Size (-s)
56 Min = 1, Max = 65507

Start Ping

Ping Result

Complete

Hostname www.cambiumnetworks.com

```
common_ping: hostname www.cambiumnetworks.com
PING www.cambiumnetworks.com (141.193.213.10): 56 data bytes
64 bytes from 141.193.213.10: seq=0 ttl=57 time=26.367 ms
64 bytes from 141.193.213.10: seq=1 ttl=57 time=24.968 ms
64 bytes from 141.193.213.10: seq=2 ttl=57 time=25.795 ms

--- www.cambiumnetworks.com ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 24.968/25.710/26.367 ms
```

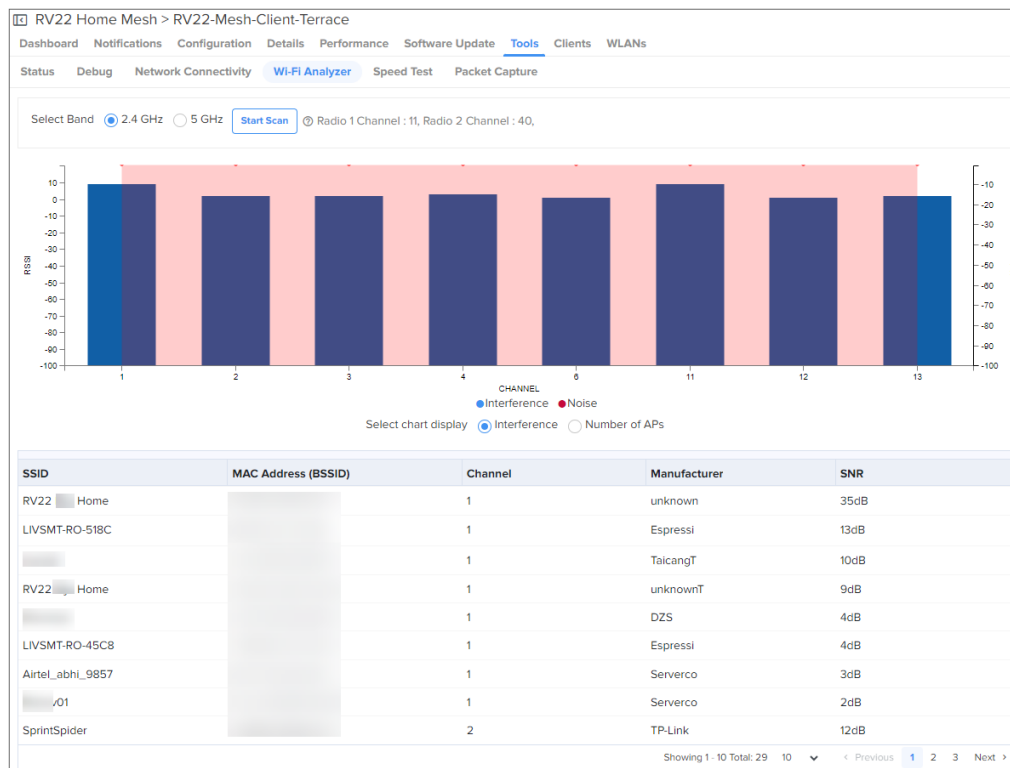
Wi-Fi Analyzer

Displays radio traffic and signal information for the selected band. It displays the interference and noise measured for the selected band.

To view the Wi-Fi Analyzer details:

1. Navigate to **Monitor and Manage** > <RV22-router-name> > **Tools** > **Wi-Fi Analyzer**.
2. Select the required band (2.4 or 5 GHz).
3. Click **Start Scan**.

cnMaestro analyzes the band and displays the result in table as shown below.



Speed Test

Displays the internet speed provided by the RV22 Home Mesh router.

To know the speed of the router:

1. Navigate to **Monitor and Manage** > <RV22-router-name> > **Tools** > **Speed Test**.
2. Provide the details in the fields provided.
3. Click **Start Speed Test**.

cnMaestro checks the speed and displays both download and upload speeds in megabytes per second (MBps).

The screenshot shows the 'Speed Test' configuration interface in the cnMaestro 'Tools' section. The interface has tabs for 'Status', 'Debug', 'Network Connectivity', 'Wi-Fi Analyzer', 'Speed Test' (selected), and 'Packet Capture'. Below the tabs, there are four input fields for configuring the speed test:

- Duration (Seconds):** A text input field with the value '15'. To its right, it says 'Test duration for each download and upload test - Min = 1, Max = 60'.
- Parallel Streams:** A text input field with the value '3'. To its right, it says 'Number of parallel streams to run the test - Min = 1, Max = 10'.
- Download Size (MB):** A text input field with the value '20'. To its right, it says 'Min = 1, Max = 1000'.
- Upload Size (MB):** A text input field with the value '20'. To its right, it says 'Min = 1, Max = 1000'.

At the bottom of the form, there is a blue button labeled 'Start Speed Test'.


Packet Capture

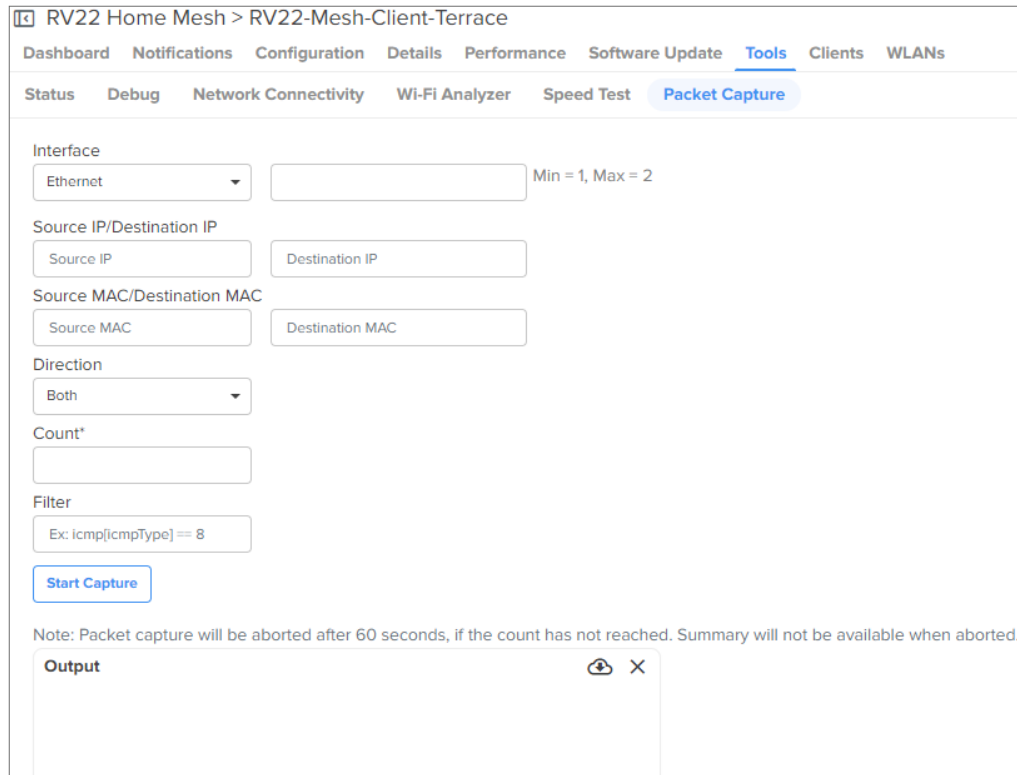
Packet Capture allows the user to capture all packets on a specified interface.

To capture packet data:

1. Navigate to **Monitor and Manage** > <RV22-router-name> > **Tools** > **Packet Capture**.
2. Select the required interface and provide the source and destination IP address or MAC address.
3. Provide the number of packets to be captured.
4. Click **Start Capture**.

cnMaestro displays the information in the **Output** window.

5. To download the PCAP file, click the download () icon.



RV22 Home Mesh > RV22-Mesh-Client-Terrace

Dashboard Notifications Configuration Details Performance Software Update **Tools** Clients WLANs

Status Debug Network Connectivity Wi-Fi Analyzer Speed Test **Packet Capture**

Interface
Ethernet Min = 1, Max = 2

Source IP/Destination IP
Source IP Destination IP

Source MAC/Destination MAC
Source MAC Destination MAC



Direction
Both

Count*

Filter
Ex: icmp[icmpType] == 8

Start Capture

Note: Packet capture will be aborted after 60 seconds, if the count has not reached. Summary will not be available when aborted.

Output  

Wireless Intrusion Detection System (WIDS)



Note

This is a beta feature.

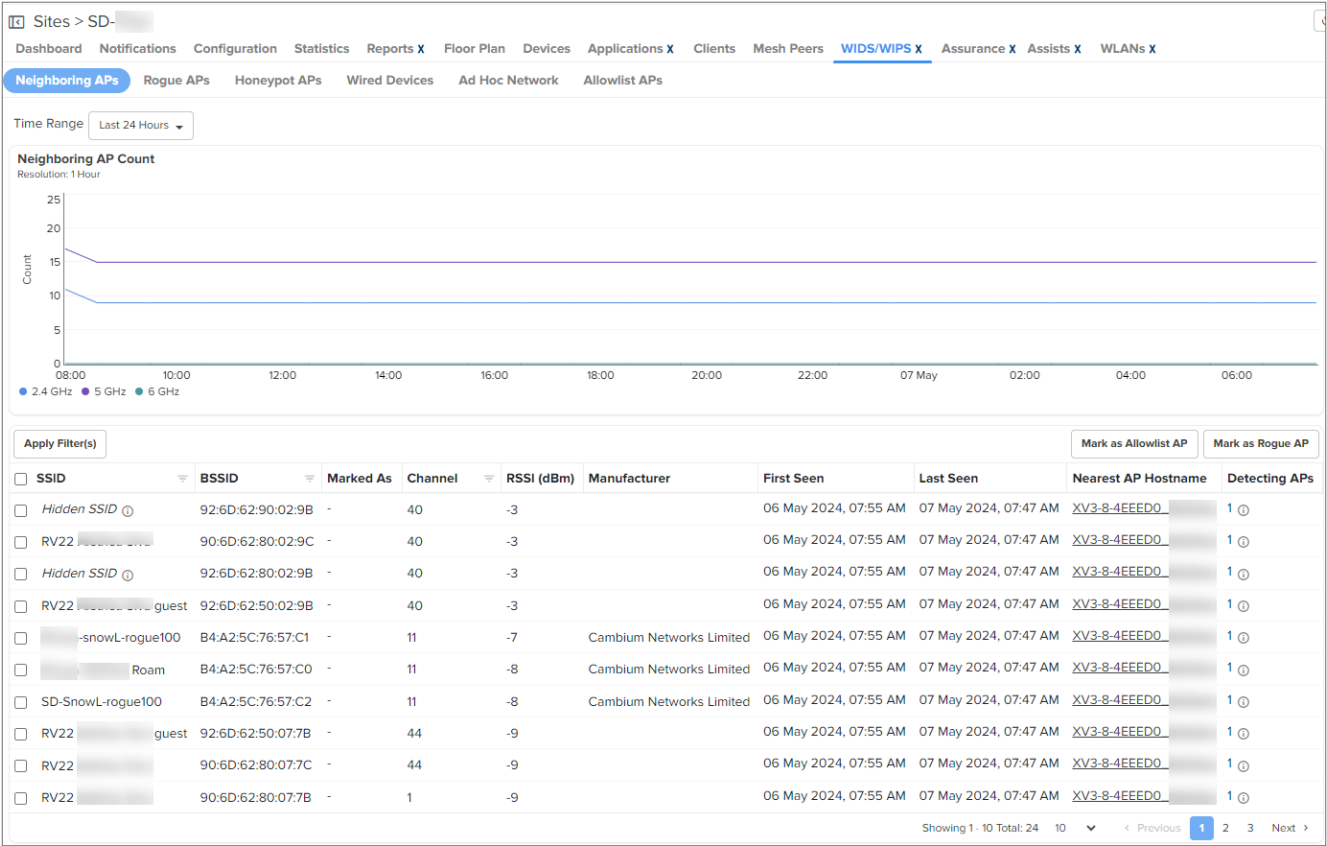
WIDS is a powerful feature within cnMaestro that helps administrators monitor and protect their wireless networks from unauthorized access and potential security threats. WIDS works by continuously scanning the wireless spectrum to detect and mitigate potential intrusions, ensuring the integrity and security of your network infrastructure.

This section provides detailed monitoring of various aspects including:

- Neighboring APs
- Rogue APs
- Honeypot APs
- Wired Devices

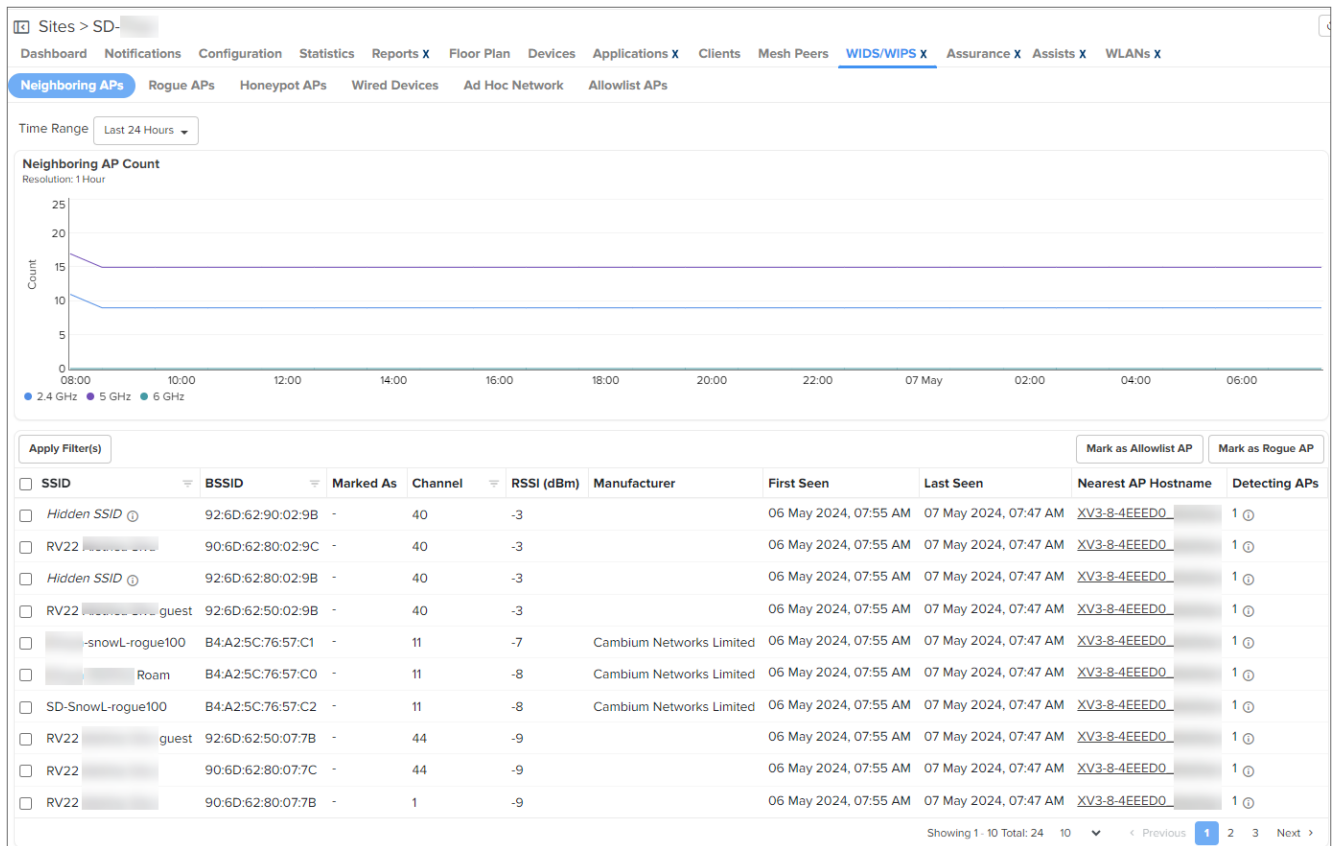
- Ad Hoc Network
- Allowlist APs

To view the WIDS page, navigate to **Network > Site > WIDS/WIPS** page.



Neighboring APs

This feature allows user to monitor and manage neighboring APs effectively to ensure optimal network performance and security.



User can selectively mark neighboring APs as **Allowlist APs** or **Rogue APs** directly from the Neighboring AP page. This functionality enables administrators to categorize neighboring APs based on their legitimacy and take appropriate actions to manage them.

The neighboring APs that are marked as allowlist or rogue APs are moved to the **Allowlist APs** and **Rogue APs** tabs respectively.

The Neighboring AP page offers flexibility in analyzing data by providing options to select the **Time Range**. User can choose between **Last 24 hours** and **Last 7 days** to view neighboring AP data within the specified time frame.

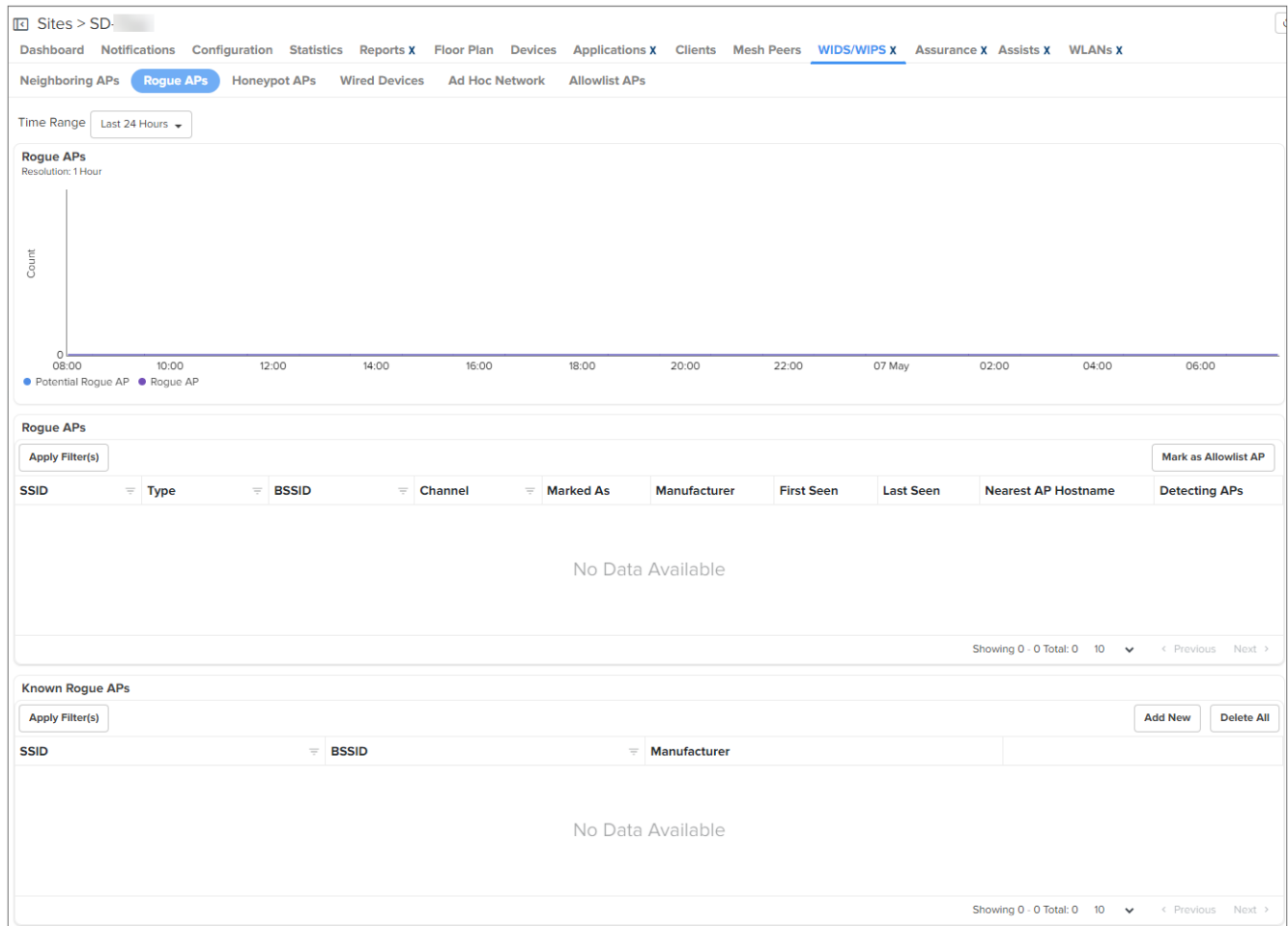
The following Neighboring APs parameters are displayed:

Table 39 *Neighboring APs parameters*

Field	Description
SSID	Name of the wireless network.
BSSID	MAC address of the AP.
Marked As	Indicates whether the neighboring AP is marked as an allowlist AP or a rogue AP.
Channel	Radio frequency channel on which the neighboring AP operates.
RSSI (dBm)	Received signal strength indication, measured in decibels relative to one milliwatt (dBm).
Manufacturer	Manufacturer name of the neighboring AP (For example, TP-Link, NETGEAR).
First Seen	Date and time when the neighboring AP was first detected.
Last Seen	Date and time when the neighboring AP was last detected.
Nearest AP Host name	Hostname of the nearest AP to the neighboring AP.
Detecting APs	Number of APs that have detected the neighboring AP.

Rogue APs

A Rogue AP is an unauthorized AP that is 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.



The following Rogue AP parameters are displayed:

Table 40 *Rogue APs parameters*

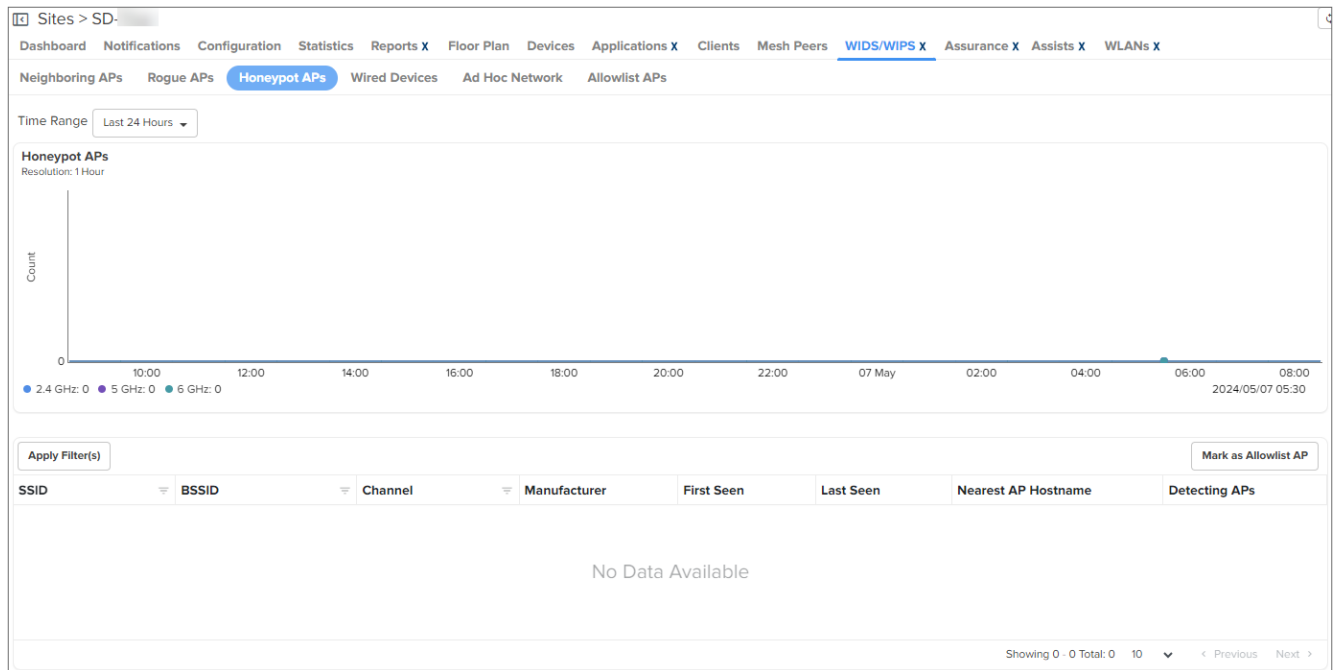
Field	Description
SSID	SSID of the rogue AP.
Type	Indicates the type of the rogue AP. Following are the supported values: <ul style="list-style-type: none"> Rogue AP Potential Rogue AP
BSSID	AP MAC address.
Channel	Channel in which the rogue AP operates.
Marked As	Indicates whether the rogue AP has been marked as an allowlist AP or a rogue AP.
Manufacturer	Manufacturer name of the neighboring AP (For example, TP-Link, NETGEAR).
First Seen	Time at which the rogue AP is detected for the first time.
Last Seen	Time at which the rogue AP was last detected.

Table 40 *Rogue APs parameters*

Field	Description
Nearest AP Hostname	Hostname of the nearest AP to the rogue AP.
Detecting APs	Number of APs that have detected the rogue AP.

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.



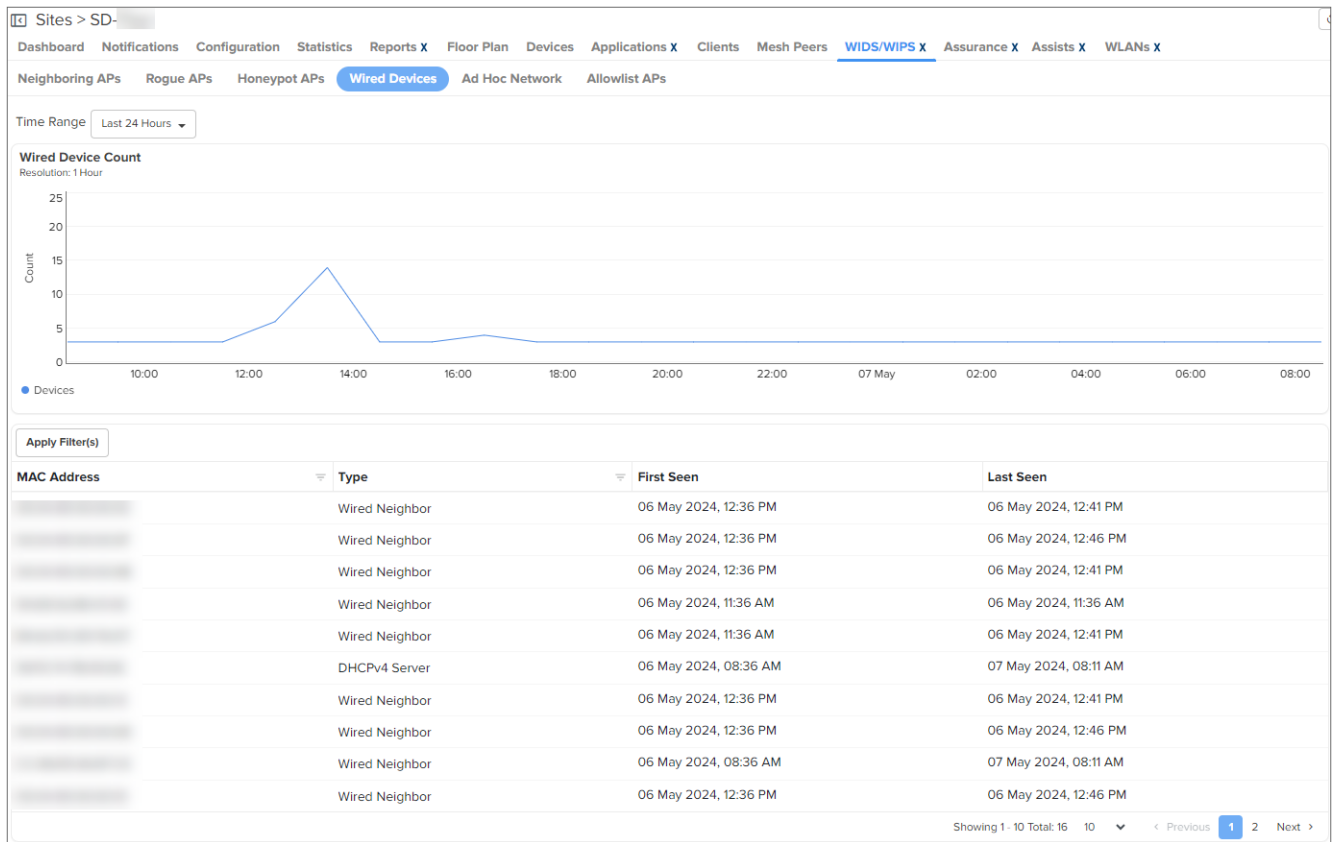
The following parameters related to Honeypot APs are displayed:

Table 41 *Honeypot APs parameters*

Field	Description
SSID	Name of the honeypot wireless network.
BSSID	AP MAC address.
Channel	Radio frequency channel on which the honeypot AP operates.
Manufacturer	Manufacturer name of the honeypot AP.
First Seen	Date and time when the honeypot AP was first detected.
Last Seen	Date and time when the honeypot AP was last detected.
Nearest AP Hostname	Hostname of the nearest AP to the honeypot AP.
Detecting APs	Number of APs that have detected the honeypot AP.

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.



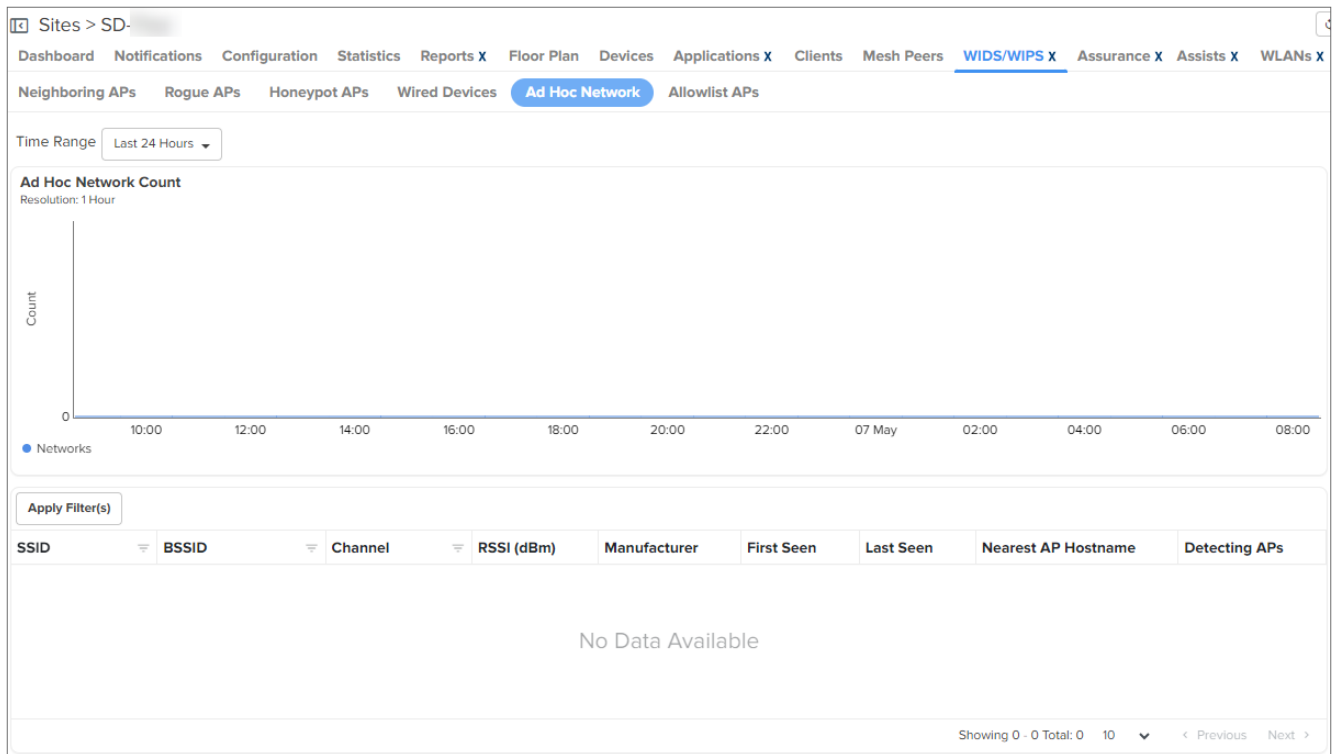
The following parameters related to Wired Devices are displayed:

Table 42 *Wired Devices parameters*

Field	Description
MAC Address	The MAC address of the wired device.
Type	The type or category of the wired device.
First Seen	The date and time when the wired device was first detected.
Last Seen	The date and time when the wired device was last detected.

Ad Hoc Networks

Ad hoc networks are temporary networks formed spontaneously by wireless devices for direct communication without the need for a central AP.



The following parameters related to Ad Hoc Networks are displayed:

Table 43 *Ad Hoc Networks parameters*

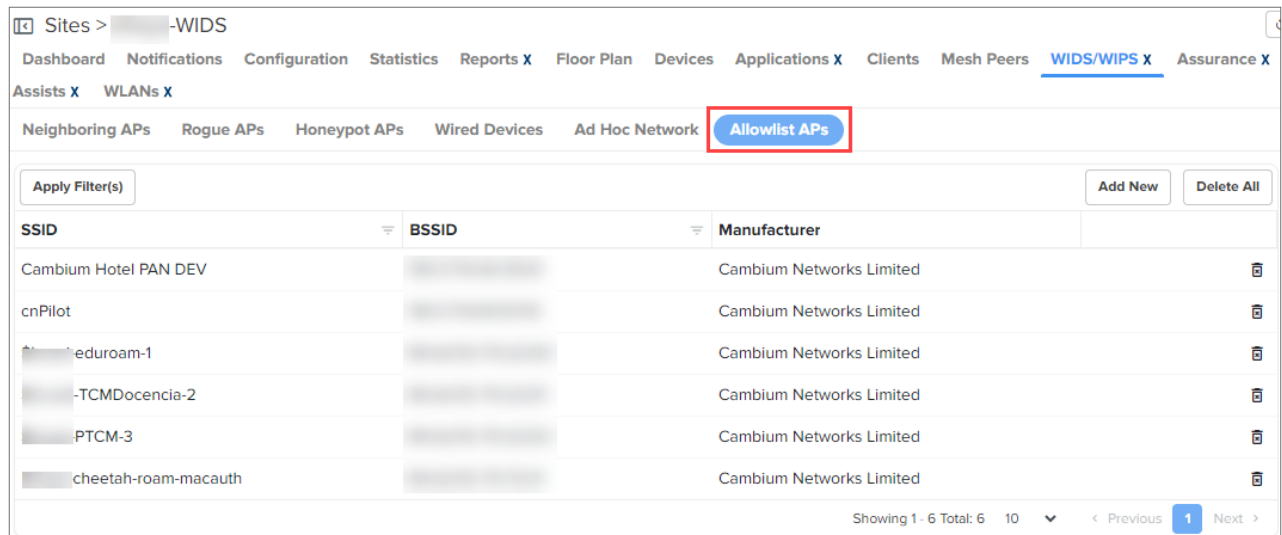
Field	Description
SSID	The name of the ad hoc wireless network.
BSSID	The MAC address of the ad hoc network.
Channel	The radio frequency channel on which the ad hoc network operates.
RSSI (dBm)	The received signal strength indication, measured in decibels relative to one milliwatt (dBm), of the ad hoc network.
Manufacturer	The manufacturer name of the device creating the ad hoc network.
First Seen	The date and time when the ad hoc network was first detected.
Last Seen	The date and time when the ad hoc network was last detected.
Nearest AP Hostname	The hostname of the nearest AP to the ad hoc network.
Detecting APs	The number of APs that have detected the ad hoc network.

Allowlist APs

Allowlist APs allow administrators to configure the SSID and MAC addresses of authorized access points, providing control over permitted devices in the network infrastructure.

To add Allowlist APs, follow these steps:

1. Navigate to **WIDS > Allowlist APs**.



2. Click **Add New**. The **Add New Allowlist AP** windows appears.

Add New Allowlist AP

BSSID/MAC*

Entries can have either '.', '*' or '*' to specify required pattern matching
(e.g. AF* will allowlist all MACs starting with AF).

SSID

Save

3. Enter the **BSSID/MAC** address.
4. Enter **SSID**.
5. Click **Save**.

The following parameters related to Whiteilist APs are displayed:

Table 44 Allowlist APs parameters

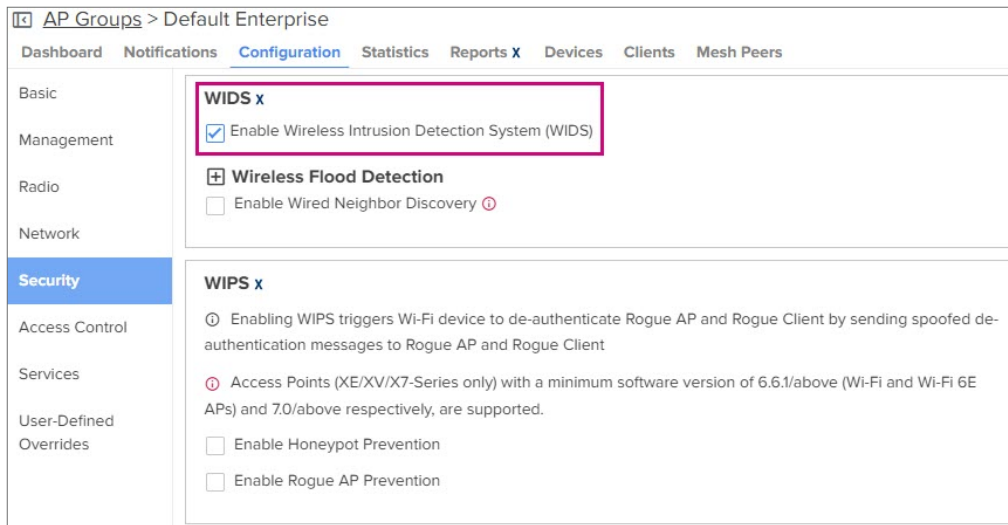
Field	Description
SSID	The name of the wireless network.
BSSID	The MAC address of the AP.
Manufacturer	The manufacturer of the AP.
Delete All	Allows to delete all Allowlist APs in the list.

Configuring WIDS

To enable WIDS feature perform the following steps:

1. Navigate to **Configuration > Wi-Fi Profiles > AP Groups** tab.
2. Select the **AP Group** and navigate to **Security** page.

3. Select the **Enable Wireless Intrusion Detection System (WIDS)** checkbox.



AP Groups > Default Enterprise

Dashboard Notifications **Configuration** Statistics Reports x Devices Clients Mesh Peers

Basic

Management

Radio

Network

Security

Access Control

Services

User-Defined Overrides

WIDS x

☒ Enable Wireless Intrusion Detection System (WIDS)

Wireless Flood Detection

☐ Enable Wired Neighbor Discovery ⓘ

WIPS x

ⓘ Enabling WIPS triggers Wi-Fi device to de-authenticate Rogue AP and Rogue Client by sending spoofed de-authentication messages to Rogue AP and Rogue Client

ⓘ Access Points (XE/XV/X7-Series only) with a minimum software version of 6.6.1/above (Wi-Fi and Wi-Fi 6E APs) and 7.0/above respectively, are supported.

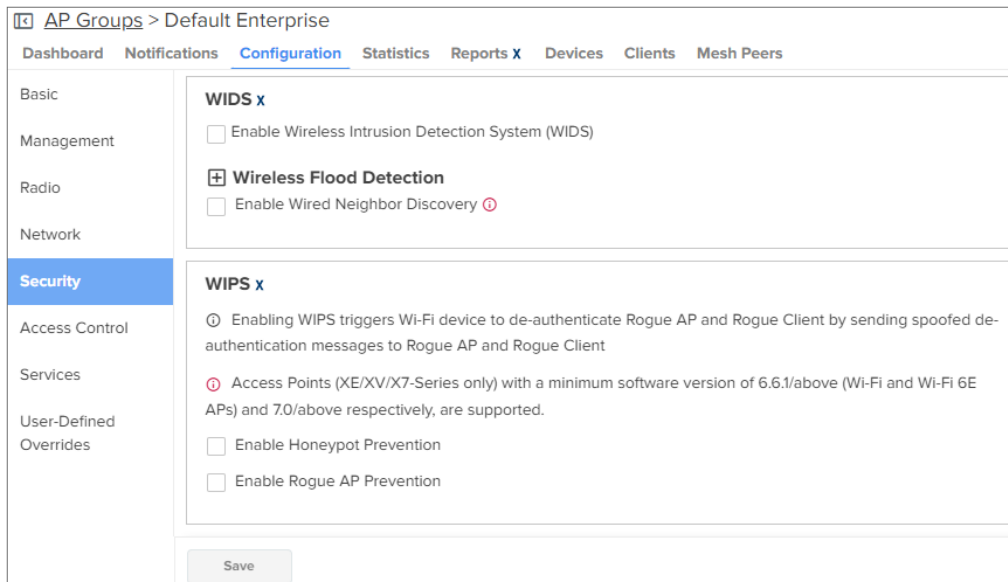
☐ Enable Honeypot Prevention

☐ Enable Rogue AP Prevention

Configuring Wired Neighbor Discovery

To enable wired neighbor discovery, perform the following steps:

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 Wired Neighbor Discovery** checkbox.



AP Groups > Default Enterprise

Dashboard Notifications **Configuration** Statistics Reports x Devices Clients Mesh Peers

Basic

Management

Radio

Network

Security

Access Control

Services

User-Defined Overrides

WIDS x

☐ Enable Wireless Intrusion Detection System (WIDS)

Wireless Flood Detection

☐ Enable Wired Neighbor Discovery ⓘ

WIPS x

ⓘ Enabling WIPS triggers Wi-Fi device to de-authenticate Rogue AP and Rogue Client by sending spoofed de-authentication messages to Rogue AP and Rogue Client

ⓘ Access Points (XE/XV/X7-Series only) with a minimum software version of 6.6.1/above (Wi-Fi and Wi-Fi 6E APs) and 7.0/above respectively, are supported.

☐ Enable Honeypot Prevention

☐ Enable Rogue AP Prevention

Save

Wireless Flood Detection

Wireless Flood Detection in cnMaestro is crucial for identifying and mitigating flood attacks in wireless networks. This feature provides administrators with the ability to monitor various parameters to detect potential flood attacks and take appropriate actions.



Note

You need to enable the WIDS to configure the Wireless Flood Detection and Rouge AP detection.

Wireless Flood Detection is used to detect the flood attacks of Association, Authentication, Deauthentication, Disassociation, and EAP.

AP Groups > Default Enterprise

Dashboard Notifications **Configuration** Statistics Reports X Devices Clients Mesh Peers

Basic

Management

Radio

Network

Security

Access Control

Services

User-Defined Overrides

WIDS x

☒ Enable Wireless Intrusion Detection System (WIDS)

☒ **Wireless Flood Detection**

Packets: 500 Per Minutes: 2 Default is 500 packets per 2 minutes

☐ 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

☐ Enable Wired Neighbor Discovery ⓘ

WIPS x

ⓘ Enabling WIPS triggers Wi-Fi device to de-authenticate Rogue AP and Rogue Client by sending spoofed de-authentication messages to Rogue AP and Rogue Client

ⓘ Access Points (XE/XV/X7-Series only) with a minimum software version of 6.6.1/above (Wi-Fi and Wi-Fi 6E APs) and 7.0/above respectively, are supported.

☐ Enable Honeypot Prevention

☐ Enable Rogue AP Prevention

Wireless Flood Detection displays the following parameters:

Table 45 *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)



Note

This is a beta feature.

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.

AP Groups > Default Enterprise

Dashboard Notifications **Configuration** Statistics Reports X Devices Clients Mesh Peers

Basic

Management

Radio

Network

Security

Access Control

Services

User-Defined Overrides

WIDS x

☒ Enable Wireless Intrusion Detection System (WIDS)

Wireless Flood Detection

☐ Enable Wired Neighbor Discovery ⓘ

WIPS x

ⓘ Enabling WIPS triggers Wi-Fi device to de-authenticate Rogue AP and Rogue Client by sending spoofed de-authentication messages to Rogue AP and Rogue Client

ⓘ Access Points (XE/XV/X7-Series only) with a minimum software version of 6.6.1/above (Wi-Fi and Wi-Fi 6E APs) and 7.0/above respectively, are supported.

☐ Enable Honeypot Prevention

☐ Enable Rogue AP Prevention

Off Channel Scan (OCS)



Note

- OCS (on 2.4 GHz, 5 GHz and 6 GHz) and Rogue AP detection should be enabled for WIDS option to work at the site-level in cnMaestro.
- It will take about 20 minutes after the AP restarts or turns on to detect the Rogue APs.

To enable Off Channel Scan (OCS), perform the following steps:

1. Navigate to **Configuration > Wi-Fi Profiles > AP Groups > Radio** (Available on all radios—2.4 GHz, 5 GHz, and 6 GHz) page.
2. Expand the **Channel Scan** section and select the **Off Channel Scan** checkbox.

AP Groups > Default Enterprise

Dashboard Notifications **Configuration** Statistics Reports X Devices Clients Mesh Peers

Basic

Management

Radio

Network

Security

Access Control

Services

User-Defined Overrides

Channel Scan

☐ Off Channel Scan

OCS periodically goes away from current operating channel (home channel) to other channels and collects data about neighboring clients, AP and RF characteristics. Applicable to APs running 4.x Firmware (Wi-Fi5)

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

Save

3. Click **Save**.

Network Service Edge (NSE 3000)

The Network Service Edge (NSE 3000) delivers advanced security, routing and SD-WAN policies for small and medium enterprises. NSE 3000 model has two Gigabit WAN ports and four Gigabit LAN ports. It offers WAN throughputs of up to 1 Gbps. NSE 3000 is managed using the cloud-hosted cnMaestro (a management solution from Cambium Networks).

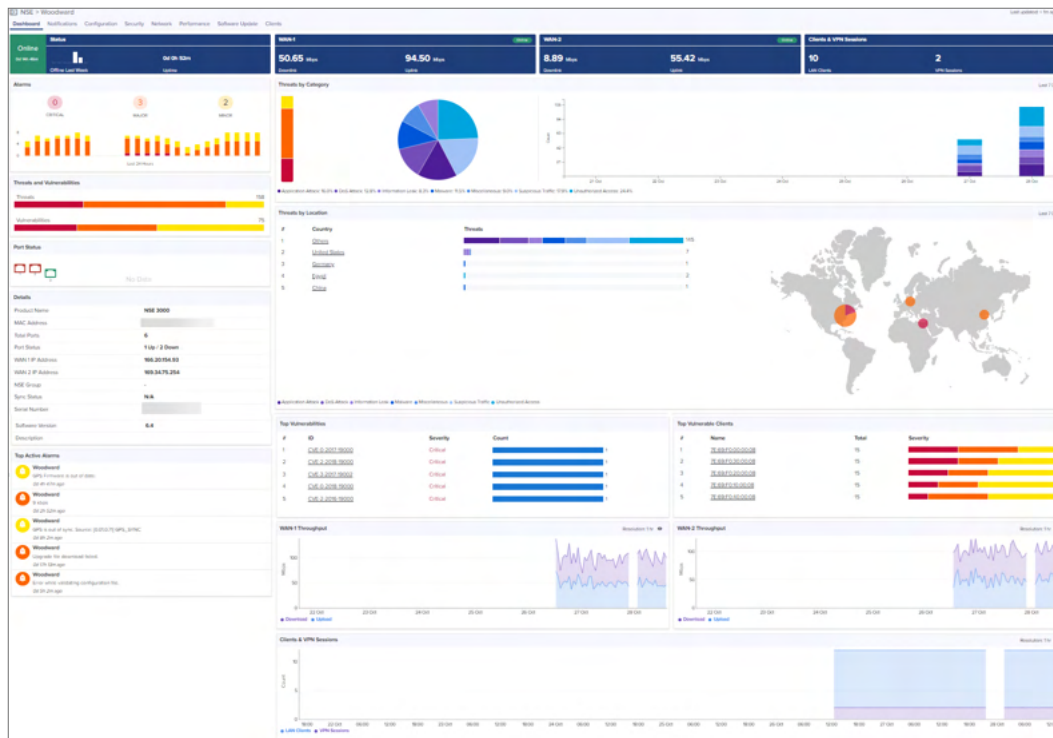
This section describes the following tabs available in cnMaestro for NSE 3000 model:

- [Dashboard](#)
- [Notifications](#)
- [Configuration](#)
- [Security](#)
- [Network](#)
- [Tools](#)
- [Clients](#)
- [Certificate](#)

Dashboard

Dashboard widgets provides you a comprehensive overview of NSE device and network health. The dashboard displays **Details** of NSE device, status of **WAN-1** and **WAN-2** usage, number of **LAN Clients & VPN Sessions**, **Alarms**, **Threats by Category**, **Threats by Location**, **Threats and Vulnerabilities** categorized as **Critical**, **Major** and **Minor**, **Port Status**, **Top Vulnerabilities**, **Top Vulnerable Clients**, **Top Active Alarms**, **WAN-1 and WAN-2 Throughput**, and **Clients and VPN Sessions**.

Figure 182 The NSE dashboard page



Notifications

Notifications consist of Alarms, Alarms History, and Events. They are synchronous messages that provide real-time system status.

Figure 183 *The Notifications page*

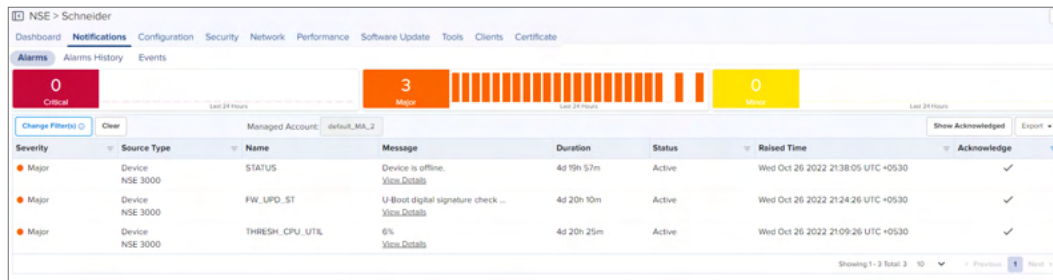


Table 46 *Notification overview*

Type	Description
Alarms	Alarms have a state and persist as long as the problematic activity continues; they reflect the current health of the devices in the network. The inactive alarms are removed from the alarms page after 10 minutes.
Alarms History	Expired Alarms are added to the Alarm History. The Alarm History displays historical active alarm counts. The history contains both the outstanding (active) and inactive alarms.
Events	Events are stateless, transient messages that occur in response to an input or action, such as if the CPU exceeds a threshold or a device association fails. Events are fire-and-forget; they are stored in an Event Table and provide a history of device activity.

Configuration

The Configuration page allows you to configure the following for a device:

- [Advanced Settings](#)
- [Factory Reset](#)
- [User-Defined Overrides](#)
- [Configuration Lock](#)

To apply the Configuration Method, perform the following:

1. Navigate to the **Configuration** page.
2. In the **Device Configuration** section, select an NSE group from the **NSE Group** dropdown list.

Device Configuration [View Device Configuration](#)

NSE Group
 Rashin_NSE_SCALE_171 [Edit](#) [Create](#)

☒ Advanced Settings

Management
WAN
VPN and Radius Server

Override	Field Name	Value	Default Value
<input type="checkbox"/>	Time Zone	<div></div>	
<input type="checkbox"/>	NTP Server 1	time.google.com	time.google.com
<input type="checkbox"/>	NTP Server 2	<div></div>	

To view the jobs, click **View Configuration Jobs** or navigate to **Administration > Jobs > Configuration Update**.

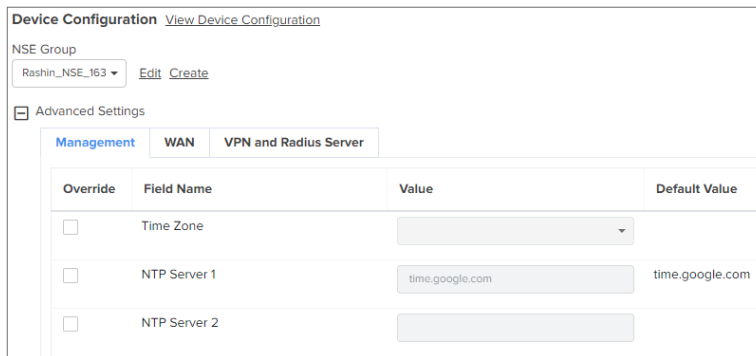
Advanced Settings

In the **Advanced Settings** you can configure the following tabs:

- [Management](#)
- [WAN](#)
- [VPN and Radius Server](#)

Management

1. In the **Management** tab, select the **Field Name** to override the settings.



The screenshot shows the 'Device Configuration' page with the 'View Device Configuration' link. Under 'NSE Group', 'Rashin_NSE_163' is selected with 'Edit' and 'Create' buttons. The 'Advanced Settings' section is expanded, showing three tabs: 'Management' (selected), 'WAN', and 'VPN and Radius Server'. The 'Management' tab contains a table with columns 'Override', 'Field Name', 'Value', and 'Default Value'.

Override	Field Name	Value	Default Value
<input type="checkbox"/>	Time Zone	<input type="text"/>	
<input type="checkbox"/>	NTP Server 1	<input type="text" value="time.google.com"/>	time.google.com
<input type="checkbox"/>	NTP Server 2	<input type="text"/>	

2. Click **Apply Configuration**.

WAN

In the **WAN**, you can override settings for **WAN 1** and **WAN 2**.

WAN 1

1. Select **Enable WAN Overrides** option.

The screenshot shows the 'Advanced Settings' window with the 'WAN' tab selected. Under the 'WAN 1' sub-tab, the 'Enable WAN Overrides' checkbox is checked. The 'IP Address Assignment' dropdown is set to 'Static'. The 'IP Address*' field contains '10.110.185.165', 'Subnet Mask*' is '255.255.255.0', 'Default Gateway' is '10.110.185.254', 'Primary DNS*' is '10.110.12.110', and 'Secondary DNS' is '10.110.12.111'. The 'VLAN Id' field is empty. The 'Enable Source NAT' checkbox is checked. The 'Load Balancing Mode' dropdown is set to 'Shared', and the 'Traffic Share Percentage' is '50'.

2. Select the fields to override.
3. Click **Apply Configuration**.

WAN 2

1. Select **Enable WAN Overrides** option.

The screenshot shows the 'Advanced Settings' window with the 'WAN' tab selected. Under the 'WAN 2' sub-tab, the 'Enable WAN Overrides' checkbox is checked. The 'IP Address Assignment' dropdown is set to 'Dynamic'. The 'VLAN Id' field is empty. The 'Enable Source NAT' checkbox is checked. The 'Load Balancing Mode' dropdown is set to 'Shared', and the 'Traffic Share Percentage' is '50'.

2. Select the fields to override.
3. Click **Apply Configuration**.

VPN and Radius Server

In the **VPN and Radius Server** tab you can override the Two Factor Authentication and RADIUS User settings.

1. To enable two factor authentication, first select the **Two Factor Authentication** checkbox.

Advanced Settings

Management WAN **VPN and Radius Server**

Override	Field Name	Value	Default Value
<input checked="" type="checkbox"/>	Two Factor Authentication	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Disable

☒ Enable Radius User Overrides

Email ID
No Data Available

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

2. Select the **Enable** or **Disable** option.
3. To add RADIUS users, select the **Enable Radius User Overrides** checkbox.
4. To add a new RADIUS user, click **Add New**.

The Add Radius user window is displayed.

Add Radius User

Email ID*

Password*

☐ Enable 2FA

5. Add the **Email ID** and **Password** for the RADIUS user.
6. To enable two factor authentication for the this RADIUS user, select the **Enable 2FA** checkbox.
7. Click **Add**.
8. Click **Apply Configuration**.

Factory Reset

To erase all the configuration on the device and bring the device back to the default factory configuration, follow these steps:

1. Navigate to the **NSE > Configuration** page and click Factory Reset.

NSE > NSE-702750

Dashboard Notifications **Configuration** Security Network Performance Software Update Tools Clients Certificate

Device Details

Managed Account: Alamo Downs

Name: NSE-702750 ⓘ

Serial Number: [Redacted]

MAC Address: [Redacted]

Network: [Redacted] LAN

IPv4 Address: 192.168.60.131

Site: [Redacted] Remote Site 1

Sync Status: In Sync

Showing all sites without NSE devices

Description: [Redacted]

Latitude: [Redacted] ⓘ

Longitude: [Redacted] ⓘ

[+ Set the device location using a map](#)

Device Configuration [View Device Configuration](#)

NSE Group: [Redacted] NSE Group [Edit](#) [Create](#)

Auto VPN Group: [Redacted] [Auto VPN Group](#)

[+ Advanced Settings ⓘ](#)

[+ Factory Reset](#)

Warning: Before you get started, know that a factory reset will erase all the data on the device. You should first back up all your configuration data. The device may no longer be able to connect to the network (unless DHCP is set up correctly).

Factory Reset

[Apply Configuration](#) [View Configuration Jobs](#)

2. In the confirmation window that appears, Click **Yes, Factory Reset**.

Please confirm factory reset [X]

Are you sure you want to factory reset NSE7003E0-165-ESS ([Redacted])?

No Yes, Factory reset

User-Defined Overrides

User-Defined Overrides are appended to the NSE groups before the configuration is applied to the device. This allows setting configuration parameters which are not supported by GUI.

To configure overrides based on your customized requirements by using variables and macros, follow these steps:

1. Navigate to **NSE Profiles > NSE Groups > <NSE-group-name> page > User-Defined Overrides** section.
2. Define your overrides in the text box.

Figure 184 *The User-Defined Overrides page*

The screenshot shows the 'User-Defined Overrides' page for an NSE Group. The breadcrumb trail at the top is 'NSE Groups > [Group Name]'. The left sidebar contains a navigation menu with options: Basic, Management, Network, Groups, WAN, Firewall, DNS, Threat Protection, VPN, and User-Defined Overrides (which is highlighted). The main content area is titled 'User-Defined Overrides' and contains the following text: 'Advanced configuration settings entered below will be applied on top of the NSE 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 titled 'Variables and Macros' with a checkbox. It explains that configuration variables are supported in the format: `$(VARIABLE_NAME)` or `$(VARIABLE_NAME=default value)`, and that `VARIABLE_NAME` should not contain dollar (\$), period (.), or spaces and should be no more than 64 characters long. It also states that macros are supported to automatically insert values taken from the device in the format: `%(ESN)` for the MAC address, `%(esn)` for MAC address in lowercase, `%(ESN-)` for MAC address in separated by '-', `%(esn-)` for MAC address in lowercase separated by '-', `%(ESN6)` for the last 6 non-separator characters of the MAC address, `%(esn6)` for the last 6 non-separator characters of the MAC address in lowercase, and `%(MSN)` for the serial number. A note at the bottom of this section says: 'For more information please see the "Help" link at the bottom of this page.' Below the text is a warning icon and a 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 NSE Group is valid and safe to use.' At the bottom of the page is a text area containing the following configuration snippet:

```
!
interface eth 1
management-access all
!
!
interface eth 2
management-access all
!
```

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

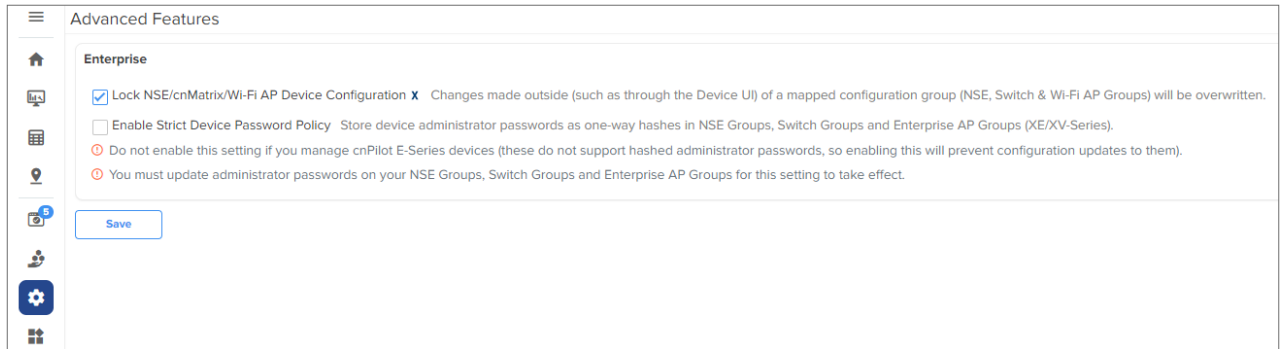
3. Click **Save**.

Configuration Lock

Configuration Lock forces the configuration on NSE and cnMaestro to be in sync always. If there is any configuration change done directly on the device, then cnMaestro tracks that device and triggers a configuration sync job to bring back the device to same configuration which is applied from the NSE Group.

To enable the configuration lock, follow these steps:

1. Navigate to the **Configuration > Advanced Features**.
2. Select the **Lock NSE/cnMatrix/Wi-Fi AP Device Configuration** checkbox.



3. Click **Save**.

Security

The **Security** page allows you to report the vulnerability and threats detected by the device.

Threats

1. Navigate to **NSE > Security > Threats**.
2. Select **Time Range** from the dropdown.
 - Last 24 hours
 - Last 7 Days
 - Last 30 Days

The threat page displays **Threats by Location**, **Total Threats**, and threat categories based on **Critical**, **Major**, **Minor**, and origin of the threat (country of origin). The bar graph on the left hand side displays the count based upon the **Threats by Category**. The pie chart displays the percentage of threats with respect to other threats. The per day bar chart displays the threat count aggregated on per day basis.

Figure 185 *The Threats page*

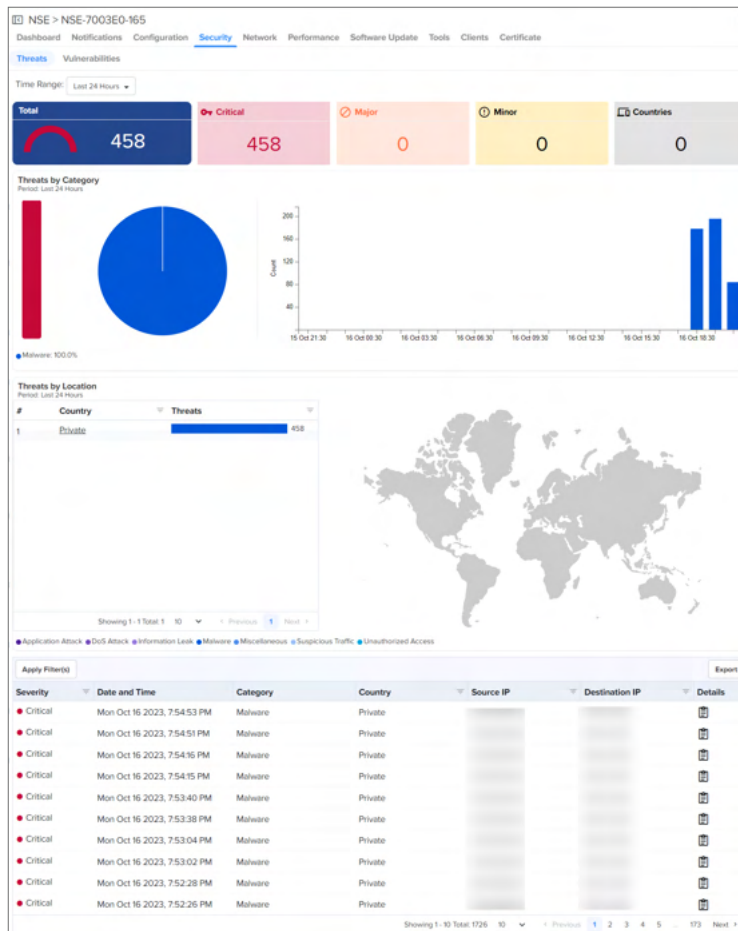


Table 47 *Parameters on the Threats page*


Parameter	Description
Severity	The severity of threat such as Critical, Major, and Minor.
Date and Time	The date and time of the threat occurrence.
Category	Displays any of the following categories of threat: <ul style="list-style-type: none"> • Application Attack • DoS Attack • Information Leak • Malware • Miscellaneous • Suspicious Traffic • Unauthorized Access
Country	The source country of the threat is displayed for threats that originate from WAN to LAN.
Source IP	Source IP address of the flow which is resulted in the threat.
Destination IP	Destination IP address of the flow which is resulted in the threat.
Details	Displays the above details in a single window in addition to a description of the threat. When you click the  icon, the Threat Details window appears, as shown in Figure 186 .

Figure 186 *The Threat Details window*

Threat Details	
Severity	Critical
Date and Time	Wed Oct 25 2023, 5:41:04 PM
Category	Malware
Country	Private
Source IP	10.110.185.165
Destination IP	10.110.203.8
Description	Intrusion attempt from [10.110.185.165:59866] to [10.110.203.8:8080] [1:26264:6] [MALWARE-CNC Dapato banking Trojan variant outbound connection] Classification [trojan-activity] Priority [1] Protocol [TCP]

Vulnerabilities

The Vulnerabilities page displays **Total Vulnerabilities**, **Unique Critical**, **Unique Major**, **Unique Minor**, and **Vulnerable Clients**.

Figure 187 *The Vulnerabilities page*

NSE > NSE7003E0-165-ESS

Dashboard

Notifications

Configuration

Security

Network

Performance

Software Update

Tools

Clients

Certificate

Threats

Vulnerabilities

Total Vulnerabilities

3

Unique Critical

0

Unique Major

3

Unique Minor

0

Vulnerable Clients

1

Vulnerable Clients

Apply Filter(s)

Export

Hostname	IP Address	MAC Address	Type	OS	Last Scan	Vulnerabilities Count	Severity
Raspberry-Wireless-165			RASPBERRY	Android	16 Feb 2024, 01:14 PM	3	

Showing 1 - 1 Total: 1

Previous

1

Next

All Active Vulnerabilities

Apply Filter(s)

Export

Severity	Identifier	Known Exploit	Exploitation Probability	Product	Product Version	Clients Impacted	
Major	CVE-2022-30522	No	42%	Apache httpd	2.4.7	1	
Major	CVE-2022-30556	No	< 1%	Apache httpd	2.4.7	1	
Major	CVE-2017-15715	No	96%	Apache httpd	2.4.7	1	

Showing 1 - 3 Total: 3

Previous

1

Next

All Ignored Vulnerabilities

Apply Filter(s)

Export

Severity	Identifier	Known Exploit	Exploitation Probability	Product	Product Version	Clients Ignored	
Major	CVE-2016-5387	No	21%	Apache httpd	2.4.7	1	
Major	CVE-2022-22721	No	< 1%	Apache httpd	2.4.7	1	
Major	CVE-2019-17567	No	< 1%	Apache httpd	2.4.7	1	
Major	CVE-2013-5704	No	47%	Apache httpd	2.4.7	1	
Major	CVE-2015-0228	No	4%	Apache httpd	2.4.7	1	
Major	CVE-2016-8743	No	< 1%	Apache httpd	2.4.7	1	
Major	CVE-2022-28614	No	< 1%	Apache httpd	2.4.7	1	
Critical	CVE-2021-44790	No	9%	Apache httpd	2.4.7	1	
Major	CVE-2017-9798	No	97%	Apache httpd	2.4.7	1	
Major	CVE-2022-29404	No	5%	Apache httpd	2.4.7	1	

Showing 1 - 10 Total: 47

Previous

12345

Next

Table 48 *Parameters on the Vulnerabilities page*

Parameter	Description
Vulnerable Clients	
Hostname	Hostname of the client. When you click the hostname, you can view the vulnerabilities discovered by the NSE for the

Table 48 *Parameters on the Vulnerabilities page*


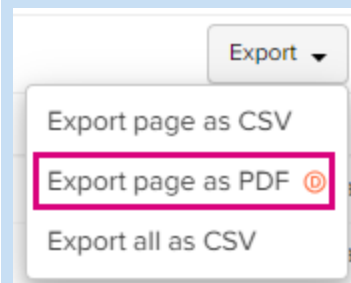
Parameter	Description
	client, as shown in Figure 203 .
IP Address	Source IPv4 address of the vulnerable client.
MAC Address	MAC address of the client.
Type	Type of client. For example, Computer, or Switch.
OS	Operating system running on the client. For example, Windows, or macOS.
Last Scan	Date and time of the last security scan performed on the client.
Vulnerabilities Count	Number of vulnerabilities found on the client during the security scan.
Severity	Level of severity assigned to each vulnerability, such as Critical, Major, or Minor.
Export	<p>Exports a list of vulnerable clients.</p> <p>The following options are supported:</p> <ul style="list-style-type: none"> • Export page as CSV • Export all as CSV <div>  <div> <p>Note</p> <p>The Export page as PDF option is deprecated from cnMaestro release version 5.2.0 onwards. This option will be completely removed from the UI in release version 5.3.0.</p>  </div> </div>
All Active Vulnerabilities	
Severity	<p>The severity level of the vulnerability:</p> <ul style="list-style-type: none"> • Critical • Major • Minor
Identifier	CVE ID number for the discovered vulnerability.
Service	Service of the vulnerability.
Port	Port number of the service.
Known Exploit	<p>Indicates whether the vulnerability is exploited in the wild and is present in the Known Exploited Vulnerabilities (KEV) catalog.</p> <p>For information on KEV catalog, see Known Exploited Vulnerabilities Catalog.</p>
Exploitation Probability	<p>The probability (in percentage) that a vulnerability will be exploited in the next 30 days. A higher value indicates a higher probability of the vulnerability being exploited.</p> <p>For information on Exploit Prediction Scoring System (EPSS), see Exploit Prediction Scoring</p>

Table 48 *Parameters on the Vulnerabilities page*






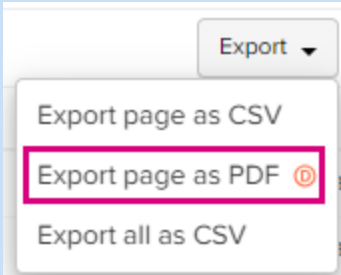
Parameter	Description
	System .
Product	Name of the product.
Product Version	Version of the product.
Clients Impacted	<p>Number of clients impacted by the vulnerability.</p> <p>When you click the number in the Clients Impacted column, a window appears as shown in Figure 188.</p>
Details 	<p>Displays the above details in a single window in addition to a short description of the vulnerability.</p> <p>A short description typically includes essential information, such as details on how an attacker can potentially exploit the vulnerability and which product versions are affected by it.</p> <p>When you click the Details  icon, the Vulnerability Details window appears, as shown in Figure 189.</p> <p>When you click the CVE Identifier link, you can access detailed information about a specific vulnerability in the National Vulnerability Database (NVD) page, as shown in Figure 190.</p>
Ignore 	<p>An option to ignore vulnerability(s).</p> <p>When you click the ignore  icon, a window appears, as shown in Figure 192.</p> <p>To ignore vulnerability(s), select the required vulnerability(s), provide your reason in the Reason field, and then click Ignore button.</p> <p>The ignored vulnerability(s) are included in All Ignored Vulnerabilities section.</p>
Export	<p>Exports a list of all active vulnerabilities.</p> <p>The following options are supported:</p> <ul style="list-style-type: none"> • Export page as CSV • Export all as CSV <div>  <div> <p>Note</p> <p>The Export page as PDF option is deprecated from cnMaestro release version 5.2.0 onwards. This option will be completely removed from the UI in release version 5.3.0.</p> </div>  </div>
All Ignored Vulnerabilities	
Severity	<p>The severity level of the vulnerability:</p> <ul style="list-style-type: none"> • Critical

Table 48 *Parameters on the Vulnerabilities page*






Parameter	Description
	<ul style="list-style-type: none"> • Major • Minor
Identifier	CVE ID number for the discovered vulnerability.
Service	Service of the vulnerability.
Port	Port number of the service.
Known Exploit	<p>Indicates whether the vulnerability is exploited in the wild and is present in the Known Exploited Vulnerabilities (KEV) catalog.</p> <p>For information on KEV catalog, see Known Exploited Vulnerabilities Catalog.</p>
Exploitation Probability	<p>The probability (in percentage) that a vulnerability will be exploited in the next 30 days. A higher value indicates a higher probability of the vulnerability being exploited.</p> <p>For information on Exploit Prediction Scoring System (EPSS), see Exploit Prediction Scoring System.</p>
Product	Name of the product.
Product Version	Version of the product.
Clients Ignored	<p>Number of clients ignored.</p> <p>When you click the number in the Clients Ignored column, a window appears as shown in Figure 193.</p>
Details 	<p>Displays the above details in a single window in addition to a short description of the vulnerability.</p> <p>A short description typically includes essential information, such as details on how an attacker can potentially exploit the vulnerability and which product versions are affected by it.</p> <p>When you click the Details () icon, the Vulnerability Details window appears, as shown in Figure 189.</p> <p>When you click the CVE Identifier link, you can access detailed information about the specific vulnerability in the National Vulnerability Database (NVD) page, as shown in Figure 190.</p>
Re-activate 	<p>An option to reactivate the ignored vulnerability(s).</p> <p>When you click the Reactivate () icon, a window appears, as shown in Figure 194.</p> <p>To reactivate an ignored vulnerability(s), select the vulnerability(s) and then click Re-activate button.</p> <p>The reactivated vulnerability(s) are included in All Active Vulnerabilities section.</p>
Export	<p>Exports a list of all ignored vulnerabilities.</p> <p>The following options are supported:</p> <ul style="list-style-type: none"> • Export page as CSV • Export all as CSV <div>  <div> <p>Note</p> <p>The Export page as PDF option is deprecated from cnMaestro release version 5.2.0 onwards. This option will be completely removed from the UI in release</p> </div> </div>

Table 48 Parameters on the Vulnerabilities page

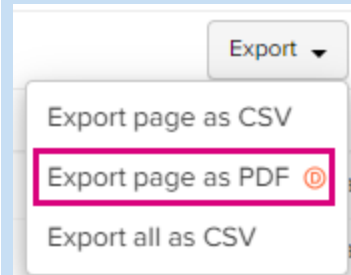
Parameter	Description
	<p>version 5.3.0.</p> 

Figure 188 A window with impacted clients

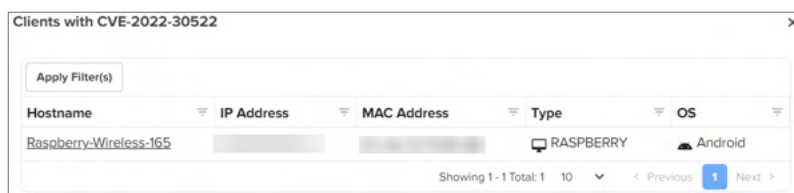


Figure 189 The Vulnerability Details window

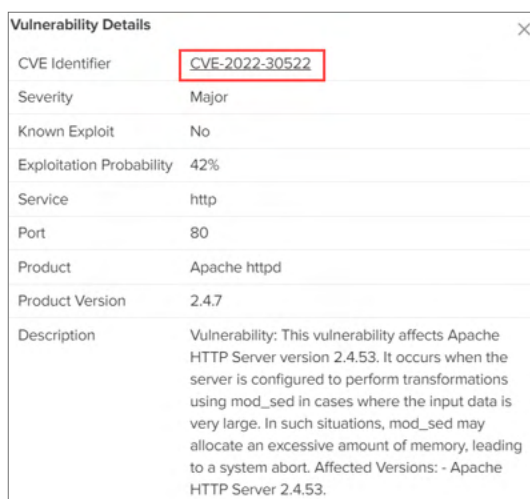


Figure 190 The NVD page

The screenshot shows the NIST National Vulnerability Database (NVD) page for CVE-2022-30522. The page has a dark blue header with the NIST logo and a 'NVD MENU' button. Below the header, there's a blue banner with 'Information Technology Laboratory' and 'NATIONAL VULNERABILITY DATABASE'. A green 'VULNERABILITIES' button is on the left. A yellow 'NOTICE' box contains text about NIST's current work. The main content area is titled 'CVE-2022-30522 Detail'. It includes a 'MODIFIED' section stating the vulnerability has been modified since last analyzed. A 'Description' section explains that if Apache HTTP Server 2.4.53 is configured to do transformations with mod_sed in contexts where the input to mod_sed may be very large, mod_sed may make excessively large memory allocations and trigger an abort. A 'Severity' section shows 'CVSS Version 3.x' selected, with a 'Base Score' of 7.5 HIGH and a 'Vector' of CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H. A 'QUICK INFO' sidebar on the right lists the CVE Dictionary Entry, NVD Published Date (06/09/2022), NVD Last Modified (11/06/2023), and Source (Apache Software Foundation).

NIST Information Technology Laboratory
NATIONAL VULNERABILITY DATABASE

VULNERABILITIES

NOTICE

NIST is currently working to establish a consortium to address challenges in the NVD program and develop improved tools and methods. You will temporarily see delays in analysis efforts during this transition. We apologize for the inconvenience and ask for your patience as we work to improve the NVD program.

CVE-2022-30522 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Description

If Apache HTTP Server 2.4.53 is configured to do transformations with mod_sed in contexts where the input to mod_sed may be very large, mod_sed may make excessively large memory allocations and trigger an abort.

Severity CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 7.5 HIGH **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

QUICK INFO

CVE Dictionary Entry:
CVE-2022-30522

NVD Published Date:
06/09/2022

NVD Last Modified:
11/06/2023

Source:
Apache Software Foundation

You can refine your search results using **Apply Filter(s)** option as shown in [Figure 191](#).

Figure 191 *Apply Filter(s) option*

Vulnerable Clients

Hostname	IP Address	MAC Address	Type	OS
Raspberry-Wireless-165	192.168.200.53		RASPBERRY	Android

All Active Vulnerabilities

Severity	Identifier	Known Exploit	Product	Product Version	Exploitation Probability	Product
Major					42%	Apache httpd
Major					< 1%	Apache httpd
Major					96%	Apache httpd

Filters

Severity:

Identifier:

Known Exploit: ☐ Yes ☐ No

Product:

Product Version:

Figure 192 *A window with an option to ignore the client(s)*

Clients with CVE-2022-30522

Hostname	IP Address	MAC Address	Type	OS
<input type="checkbox"/> Raspberry-Wireless-165	192.168.200.53		Notebook	ChromeOS

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

Reason*

Ignore

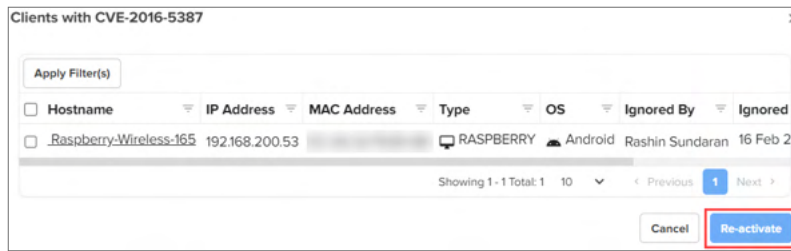
Figure 193 *A window with ignored clients*

Clients with CVE-2016-5387

Hostname	IP Address	MAC Address	Type	OS	Ignored By	Ignored Time
Raspberry-Wireless-165	192.168.200.53		Notebook	ChromeOS		16 Feb 2024

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

Figure 194 A window with an option to reactivate



Network

Network page displays information about onboard DHCP servers, Route table, and WAN statistics.

LAN

LAN page displays **Subnet** and **DHCP Leases**. You can **Apply Filters** for the table header to search for a specific parameter in the table.

Figure 195 The LAN page

NSE > NSE-7003B8

Dashboard

Notifications

Configuration

Security

Network

Performance

Software Update

Clients

LAN

Routes

WAN

Subnet

Apply Filter(s)

VLAN	IP Address	DHCP Mode	Relay Server	Start Address	End Address	Leases Used
1010	192.168.10.1	Server	N/A	192.168.10.10	192.168.10.200	2/191
1020	192.168.20.1	Server	N/A	192.168.20.10	192.168.20.15	5/6
1030	192.168.30.1	Server	N/A	192.168.30.1	192.168.30.100	0/100
1040	192.168.40.254	Server	N/A	192.168.40.10	192.168.40.200	0/191
2000	192.168.200.1	Server	N/A	192.168.200.50	192.168.200.150	0/101

Showing 1 - 5 Total: 510< Previous1Next >

DHCP Leases

Apply Filter(s)

MAC Address	IP Address	Host Name	Expires On	VLAN
	192.168.10.12	-	Sep 20 2022, 22:17	1010
	192.168.10.10	LAPTOP-025DVPT	Sep 20 2022, 22:24	1010
	192.168.20.12	Solutions-Air-	Sep 20 2022, 21:37	1020
	192.168.20.13	solution	Sep 20 2022, 21:38	1020
	192.168.20.15	Galaxy-A21s-So	Sep 20 2022, 21:41	1020
	192.168.20.10	sitindia	Sep 20 2022, 21:38	1020
	192.168.20.11	IN01-5J5S0G2	Sep 20 2022, 21:37	1020

Showing 1 - 7 Total: 710< Previous1Next >

Table 49 Parameters displayed in LAN

Parameter	Description
Subnet	
VLAN	VLAN ID.
IP Address	Static IP address of the VLAN interface.
DHCP Mode	Status of the DHCP server mode enabled or disabled.
Relay Server	Status of the relay server mode enabled or disabled.
Start Address	DHCP pool start IP address.
End Address	DHCP pool end IP address.

Table 49 Parameters displayed in LAN

Parameter	Description
Lease Used	Active IP address issued by the DHCP server.
DHCP Leases	
MAC Address	MAC address of the client.
IP Address	The leased IP address to the client.
Host Name	The hostname of the client.
Expires On	The duration for the leased IP.
VLAN	The VLAN ID assigned to the client.

Routes

Routes page displays layer 3 routing table of the device. You can **Apply Filters** for the table header to search for a specific parameter in the table.

Figure 196 The Routes page

NSE > NSE-7003B8

Dashboard

Notifications

Configuration

Security

Network

Performance

Software Update

Clients

LAN

Routes

WAN

Routes

Apply Filter(s)

Destination	Mask	Gateway	Flags	Metric	Interface
0.0.0.0	0.0.0.0	10.110.200.1	UG	1	ETH1
0.0.0.0	0.0.0.0	10.110.200.65	UG	2	ETH2
10.110.200.0	255.255.255.192	0.0.0.0	U	0	ETH1
10.110.200.64	255.255.255.224	0.0.0.0	U	0	ETH2
192.168.10.0	255.255.255.0	0.0.0.0	U	0	VLAN1010
192.168.20.0	255.255.255.0	0.0.0.0	U	0	VLAN1020
192.168.30.0	255.255.255.0	0.0.0.0	U	0	VLAN1030
192.168.40.0	255.255.255.0	0.0.0.0	U	0	VLAN1040
192.168.200.0	255.255.255.0	0.0.0.0	U	0	VLAN2000

U - Up, G - Gateway, H - Host

Showing 1 - 9 Total: 9

10

< Previous

1

Next >

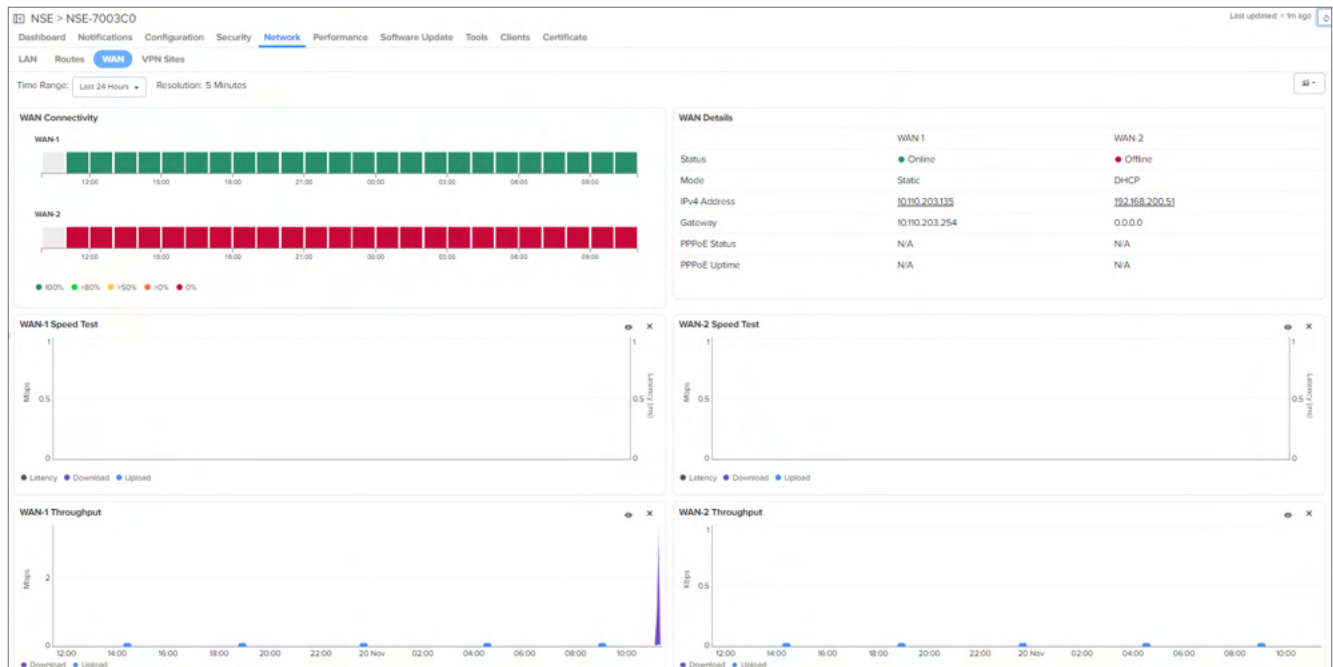
Table 50 Parameters on the Routes page

Parameter	Description
Routes	
Destination	Destination address of the routes.
Mask	Subnet mask of the specific route.
Gateway	Default gateway of the routes.
Flags	Flags of the routes.
Metric	Metric of the routes.
Interface	Interface of the routes.

WAN

WAN page displays **WAN Connectivity**, **WAN Details**, graphical representation of **Speed Test**, **Throughput** in **WAN-1** and **WAN-2** in selected **Time Range** (Last 24 hours or Last 7 Days).

Figure 197 *The WAN page*



- **WAN connectivity:** Provides the status of the periodic health check of WAN links.
- **WAN speed test:** Provides the status of the MAX uplink and downlink bandwidth of the WAN link.
- **WAN throughput:** Provides the usage of WAN uplink and downlink over a period of time.

WAN Details

Table 51 *Parameters displayed on the WAN Details section*

Parameter	Description
WAN Details	
Status	Status (online or offline) based upon the periodic WAN link health check.
Refresh time	Last update of date and time.
IP mode	Mode as DHCP or Static.
IPv4 Address	IPv4 Address of the WAN.
Gateway	Default gateway of the WAN interface.

VPN Sites

The VPN Sites page displays the network traffic and connection details as shown in [Figure 198](#).

Figure 198 *The VPN Sites page*

The screenshot displays the VPN Sites page for NSE-7003C0. It includes a top navigation bar with tabs for Dashboard, Notifications, Configuration, Security, Network (selected), Performance, Software Update, Tools, Clients, and Certificate. Below the navigation bar, there are tabs for LAN, Routes, WAN, and VPN Sites (selected). The page shows a time range of 'Last 24 Hours' and a resolution of '5 Minutes'.

VPN Sites Table:

Name	IKE State	IPSec State	Remote Host	Remote Port	Duration	Rx Bytes	Tx Bytes	Remote Subnets
site2	Established	Installed	10.110.32.70	4500	0d 0h 10m	0	0	192.168.80.0/24

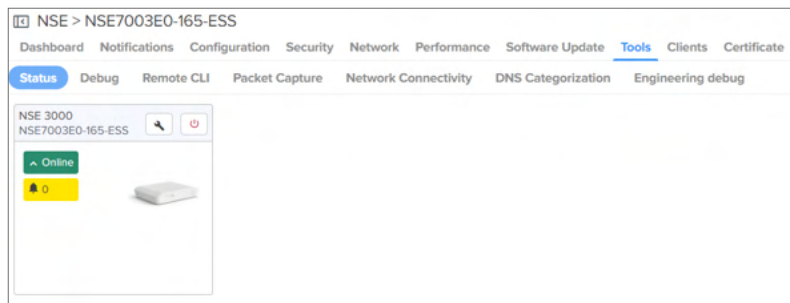
Table 52 Parameters displayed on the VPN Sites page

Parameter	Description
VPN Sites	
Name	Name of the VPN site.
IKE State	Current state of IKE protocol.
IPSec State	Current state of IPSec protocol.
Remote Host	IP address of the remote VPN endpoint.
Remote Port	Port number of the remote VPN endpoint.
Duration	Duration of the VPN connection.
Rx Bytes	Number of bytes received by the local VPN endpoint from the remote VPN endpoint.
Tx Bytes	Number of bytes transmitted by the local VPN endpoint to the remote VPN endpoint.
Remote Subnets	IP address ranges assigned to the remote VPN endpoint's network.

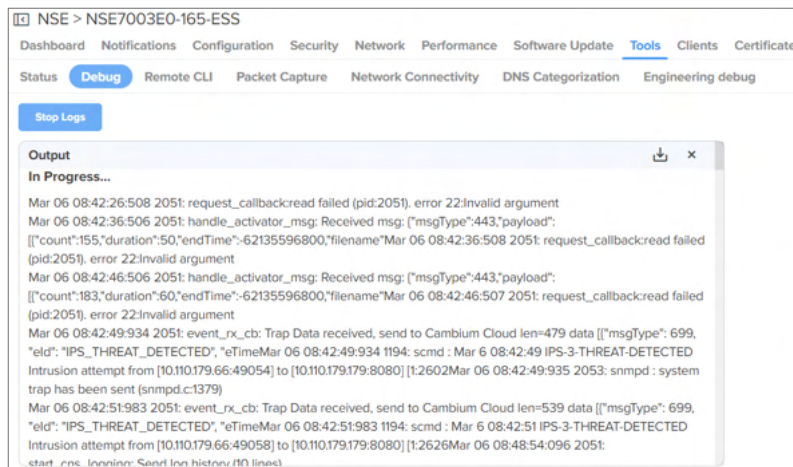
Debug Tools

You can capture logs, run remote CLI commands to see stats in real time, run traceroute, ping to check the reachability, and run live packet capture on the NSE devices on the selected interface.

To display the NSE device status, navigate to **NSE > Tools > Status** page.



To access the logs, navigate to **NSE > Tools > Debug** tab and click **Start Logs**:



To run CLI commands, navigate to **NSE > Tools > Remote CLI** page, enter the **Command** and then click **Run**:

NSE > NSE7003E0-165-ESS

Dashboard
Notifications
Configuration
Security
Network
Performance
Software Update
Tools
Clients
Certificate

Status
Debug
Remote CLI
Packet Capture
Network Connectivity
DNS Categorization
Engineering debug

Command

Type CLI command

Run

Output

Complete

Device > show connected-clients

MAC ADDRESS	IP ADDRESS	HOSTNAME	TYPE	TYPE NAME	BRAND	OS	OS VER	LAST SEEN
	192.168.200.52	E430-6EA393	Enterprise WiFi	Cambium Networks	Cambium Networks	Cambium OS		2024-03-06 08:11:47
	192.168.200.56	kali-raspberry-p	RASPBERRY	Raspberry Pi	Raspberry Pi	Raspbian		2024-03-06 08:10:41
	192.168.200.51	Rashin-AP-7003E0	Enterprise WiFi	Cambium Networks	Cambium Networks	Cambium OS		2024-03-06 07:54:34
	192.168.200.50	none	Enterprise Switc	Cambium Networks	Cambium Networks	Cambium OS		2024-03-06 07:22:31
	192.168.200.53	Raspberry-Wirele	RASPBERRY	Raspberry Pi	Raspberry Pi	Android	APT-HTTP	2024-03-06 07:26:32

Device > show lldp neighbors

LLDP neighbors:

Interface: ETH1, via: LLDP, RID: 12, Time: 17 days, 19:47:39

Chassis:

ChassisID: mac 08:36:c9:2f:4c:ae

SysDescr: 8-Port Gigabit Smart Managed Pro Switch with PoE+ and 2 SFP Ports

MgmtIP: 10.110.185.68

MgmtIface: 19

Capability: Bridge, on

Capability: Router, off

To run packet capture on the NSE device, navigate to **NSE > Tools > Packet Capture** page and follow these steps:

1. Click **New Packet Capture** and complete the details.

NSE > NSE7003E0-165-ESS

Dashboard
Notifications
Configuration
Security
Network
Performance
Software Update
Tools
Clients
Certificate

Status
Debug
Remote CLI
Packet Capture
Network Connectivity
DNS Categorization
Engineering debug

New Packet Capture

Start

Delete

Interface	Packets	Duration	Size	Filter	Start Time	Expires In	Status
WAN-1	397	2m 2s/2m	5 MB	-	06 Mar 2024 14:11	0d 23h 59m	Uploaded

Showing 1 - 1 Total: 1

The New Packet Capture window is displayed.

New Packet Capture ✕

Interface
 Ethernet ▼

Ethernet
☒ WAN-1 ☐ WAN-2 ☐ Port-3 ☐ Port-4 ☐ Port-5 ☐ Port-6

Filter Options
☒ Filter Builder ☐ Custom

Filter Group: Condition = OR ▼

+

Default Options

Packets

 0 to 65535 (default 0 indicates unlimited)

Duration

 1 to 600 (default 120) seconds

Packet Length

 0 to 1500 (default 0 indicates full packet length)

File Size

 1 to 10 (default is 5 MB)

Cancel Start Later Start Now

2. Click either **Start Now** or **Start Later** and then click **Close**.
3. If you had clicked **Start Later**, you can start the packet capture by clicking the right pointed triangle in the right most column of the interface details list.

To check the network connectivity, navigate to **NSE > Tools > Network Connectivity** page, complete the details, and then click **Start Ping**:

NSE > NSE7003E0-165-ESS

Dashboard Notifications Configuration Security Network Performance Software Update **Tools** Clients Certificate

Status Debug Remote CLI Packet Capture **Network Connectivity** DNS Categorization Engineering debug

Test Type
 Ping ▼ Network ping to a hostname or IP address.

IP Address or Hostname

Number of Packets (-c)
 Min = 1, Max = 10

Buffer Size (-s)
 Min = 1, Max = 65507

Start Ping

Ping Result

To access DNS categorization, navigate to **NSE > Tools > DNS Categorization**.

The DNS categorization tool is used to determine the category of the domain under which the queried domain falls. It is employed in scenarios where the administrator knows the specific domain and wants to ascertain which category to select while configuring the DNS filter. Additionally, it indicates whether the queried domain is permitted or denied for the specified group configured on the box.

NSE > NSE7003E0-165-ESS

Dashboard Notifications Configuration Security Network Performance Software Update **Tools** Clients Certificate

Status Debug Remote CLI Packet Capture Network Connectivity **DNS Categorization** Engineering debug

Domain name*

www.google.com

Run

Output

Category

1. Search Engines

Denied Groups

1. group1

Allowed Groups

1. group2

Clients

The Clients page displays information depending on the system, network, or the device level from where you are accessing the page.

- [Device-level information](#)
- [Network- and Site-level information](#)
- [Client Dashboard](#)

Device-level information

Clients page at the device-level displays the Local and Remote clients (VPN clients) connected to the NSE device.



Note

You can connect up to 1000 clients on the LAN side of NSE 3000. The clients can be either wired clients or wireless clients.

Local

The Local page displays the total client count which are connected to the NSE on the LAN side. Using device fingerprinting NSE provides **Device Type**, **Device OS**, and **OS Version**.

NSE > NSE-700880-UK

Dashboard Notifications Configuration Security Network Performance Software Update Tools **Clients** Certificate

Local Remote

Apply Filter(s) Export

Host Name	IPv4 Address	MAC	Manufacturer	Type	Model	OS	OS Version
Unknown	192.168.201.53		VMware	VIRTUAL_MACHINE		Windows	-
Unknown	192.168.201.50		VMware	VIRTUAL_MACHINE		Windows	-
none	192.168.201.60		Apple	MOBILE		iOS	-
Unknown	192.168.201.54		Dell	COMPUTER		Windows	-
Unknown	192.168.201.51		Cambium Networks	Enterprise Switch		Cambium OS	-
IN01-G24BJM2	192.168.201.57		Dell	COMPUTER		Windows	-
Unknown	192.168.201.59		Cambium Networks	Enterprise WiFi Access Point		Cambium OS	-
Unknown	192.168.201.55		Cambium Networks	Enterprise WiFi Access Point		Cambium OS	-
none	192.168.201.52		Raspberry Pi	RASPBERRY		Raspbian	-
Unknown	192.168.201.56		Raspberry Pi	RASPBERRY		Raspbian	-

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

Click **Host Name**. It navigates to detailed Client Dashboard as shown in [Figure 202](#).

Remote

The **Remote** page displays client count (vpn client) connected on the WAN side.

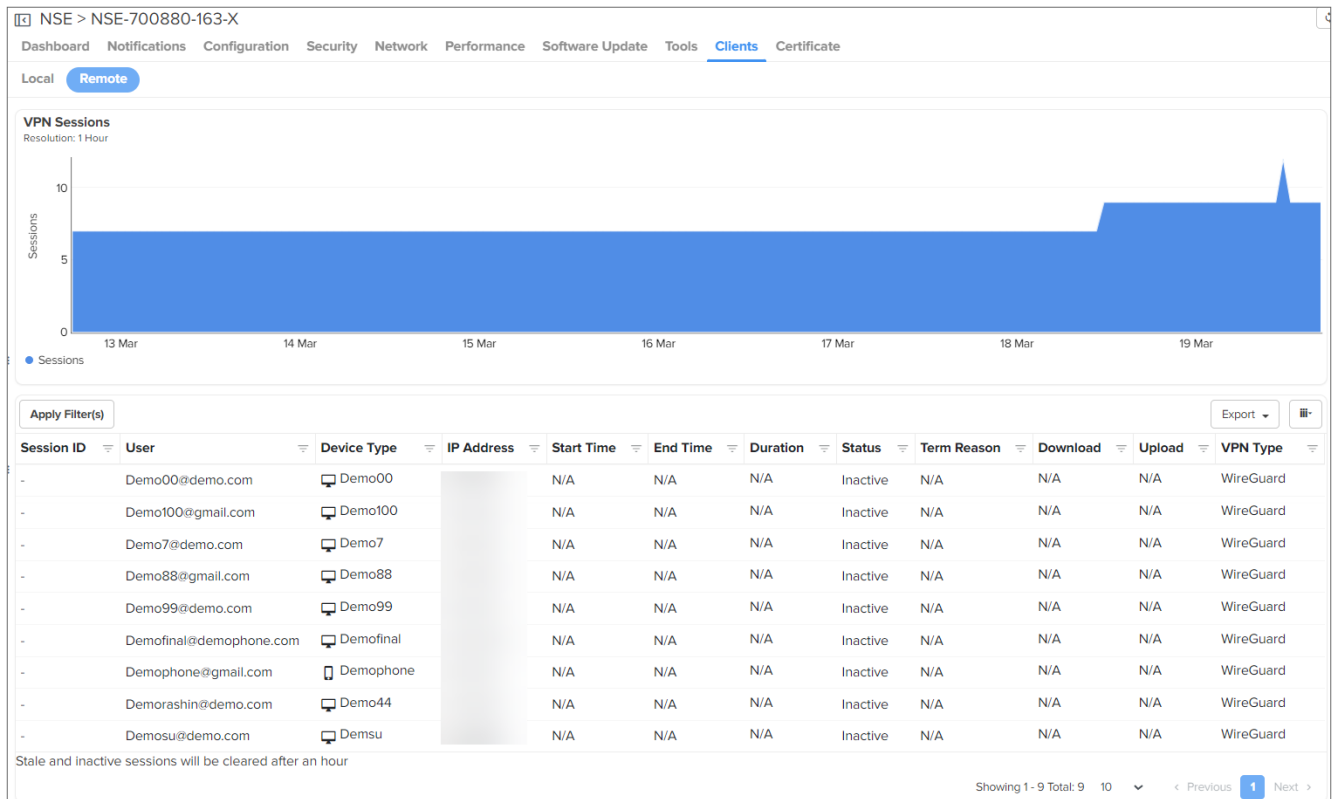


Table 53 Parameters displayed in VPN sessions

Parameter	Description
VPN Sessions	
Session ID	ID of the session. Note: The session ID is displayed only for IPSec IKEV2 and L2TP over IPSec VPN types.
User	VPN user name.
Device Type	Type of device.

Table 53 *Parameters displayed in VPN sessions*

Parameter	Description
IP Address	IP Address assigned to the VPN client.
Start Time	VPN session start time.
End Time	VPN session end time.
Duration	Total session duration.
Status	Session status as active or inactive.
Term Reason	Terminated reason of the session disconnected or timeout.
Download	Total download by the VPN user.
Upload	Total upload by the VPN user.
VPN Type	Type of VPN. The following options are supported: <ul style="list-style-type: none">• WireGuard• IPSec IKEV2• L2TP over IPSec

Network- and Site-level information

The Clients page at the Network- and Site-level displays the details of all the connected wireless and wired clients, and all unconnected clients.

- [Wireless Clients](#)
- [Wired Clients](#)
- [Unconnected Clients](#)

Wireless Clients

The **Clients > Wireless Clients** page at the Network- and Site-level displays the following details:

- **General**
 - Device
 - Device MAC
 - Host Name
 - Last Duration
 - Last Seen
 - Manufacturer
 - OS
 - Status
 - User
- **Guest Access**
 - Auth Status
 - Authentication Type

- Client Type
- Download Quota
- Download Quota Balance
- Guest Access Type
- Session Expiry
- Total Quota
- Total Quota Balance
- Upload Quota
- Upload Quota Balance
- **Network**
 - IPv4 Address
 - IPv6 Address
 - MAC
 - VLAN-ID
- **Wireless**
 - Band
 - Capability
 - Download
 - Radio ID
 - Radio Mode
 - RSSI
 - SNR
 - SSID
 - Upload

Figure 199 *Site > Clients > Wireless Clients*

Host Name	Status	User	MAC	IPv4 Address	VLAN-ID	SSID	Last Duration	RSSI	Band	Capability	Device	Radio ID	Radio Mode	SNR
No Data Available														

Wired Clients

The **Clients > Wired Clients** page at the Network- and Site-level displays the following details:

- **General**
 - Address Type
 - Device

- Device MAC
- Download
- Expires
- Host Name
- Last Duration
- Manufacturer
- Model
- OS
- OS Version
- Type
- Upload
- **Guest Access**
 - Auth Status
 - Authentication Type
 - Client Type
 - Download Quota
 - Download Quota Balance
 - Guest Access Type
 - Portal Mode
 - Session Expiry
 - Total Quota
 - Total Quota Balance
 - Upload Quota
 - Upload Quota Balance
- **Network**
 - Interface
 - IPv4 Address
 - MAC
 - VLAN-ID

Figure 200 *Site > Clients > Wired Clients*

Host Name	Device	IPv4 Address	MAC	Manufacturer	Type	Model	OS	OS Version	VLAN-ID	Interface	Address Type	Auth Status	Exp
	NSE-700880-UK	192.168.201.53		VMware	VIRTUAL_MACHINE		Windows					false	-
	NSE-700880-UK	192.168.201.50		VMware	VIRTUAL_MACHINE		Windows					false	-
	NSE-700880-UK	192.168.201.54		Dell	COMPUTER		Windows					false	-
	NSE-700880-UK	192.168.201.51		Cambium Networks	Enterprise Switch		Cambium OS					false	-
	NSE-700880-UK	192.168.201.59		Cambium Networks	Enterprise WIFI Access Point		Cambium OS					false	-
	NSE-700880-UK	192.168.201.55		Cambium Networks	Enterprise WIFI Access Point		Cambium OS					false	-
	NSE-700880-UK	192.168.201.56		Raspberry Pi	RASPBERRY		Raspbian					false	-
IN01G248IM2	NSE-700880-UK	192.168.201.57		Dell	COMPUTER		Windows					false	-
000E	NSE-700880-UK	192.168.201.52		Raspberry Pi	RASPBERRY		Raspbian					false	-

Unconnected Clients

The **Clients > Unconnected Clients** page at the Network- and Site-level displays the following details:

- Host Name
- Device
- Last Seen
- MAC (address)
- SSID
- Manufacturer

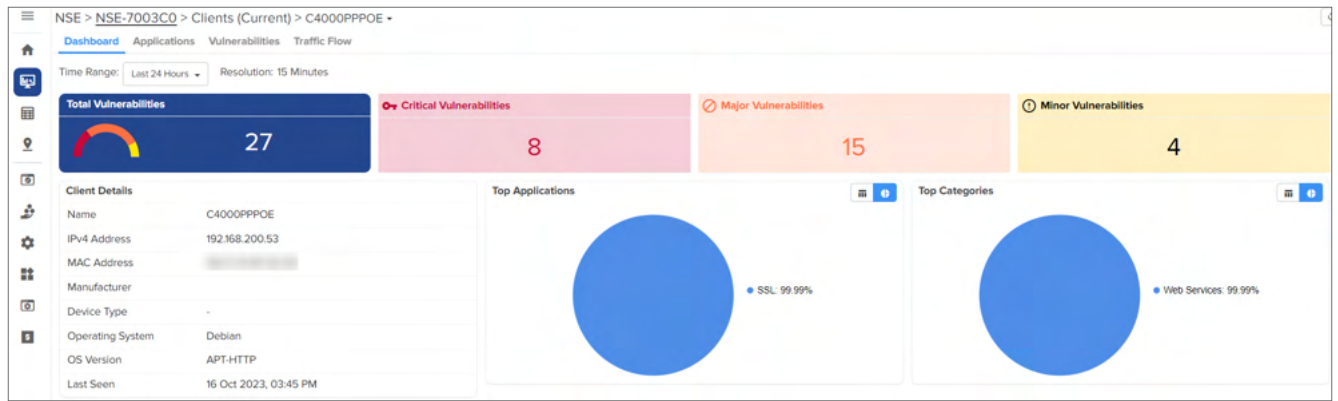
Figure 201 *Site > Clients > Unconnected Clients*

Host Name	Device	MAC	Manufacturer	SSID	Last Seen
No Unconnected Clients					

Client Dashboard

Dashboard provides overview of the wired and wireless clients usage. Click the pie chart to view specific application usage.

Figure 202 *Client Dashboard*

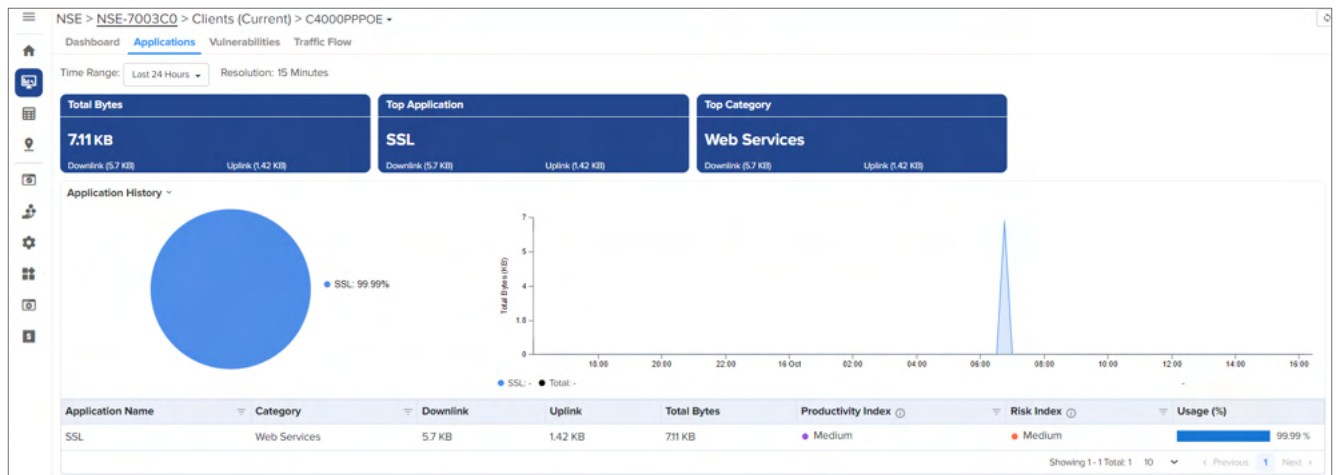


The following parameters are displayed for NSE Clients:

- Total Vulnerabilities
- Critical Vulnerabilities
- Major Vulnerabilities
- Minor Vulnerabilities
- Client Details
- Top Applications
- Top Categories

Applications

The Applications tab displays **Application History**, **Top Application**, **Top Category**, and **Total Bytes**.



The Application data can be presented most for 24 hours, 7 days, or 30 days.



Note

The NSE 3000 device supports up to 256000 concurrent connections.

- **Top Application:** Represent the most used application by the client.
- **Total Bytes:** Represents the sum of Uplink and Downlink traffic across all applications used by the client.
- **Top Category:** Category of the top application used by the client.

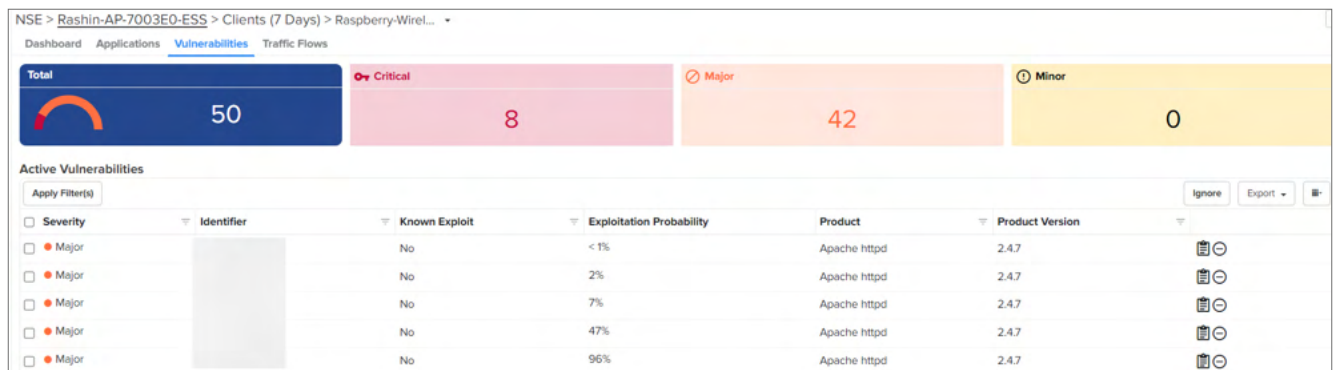
Table 54 Parameters on the Applications page

Field	Description
Application Name	Name of the application.
Category	Category of the application.
Downlink	Total number of downlink bytes during the period selected.
Uplink	Total number of uplink bytes during the period selected.
Total Bytes	Total amount of application data (uplink plus downlink).
Productivity Index	The estimate of the typical productivity of the application. A higher value means better productivity.
Risk Index	The estimate of the typical security risk of the application. A higher value means greater risk.
Usage	The percentage of usage by this application in comparison to all applications.

Vulnerabilities

The **Vulnerabilities** page displays the vulnerabilities discovered for the client by the NSE. Vulnerabilities are categorized as Minor, Major, and Critical.

Figure 203 Vulnerabilities dashboard



Traffic Flows

Traffic flows can be referred to as a current snapshot of existing flows. The flow direction can be either LAN to WAN or WAN to LAN.



Note

The NSE 3000 device supports up to 256000 concurrent connections.

The **Traffic Flows** page displays the active connections or flows of a client, as shown in [Figure 204](#).

Figure 204 The Traffic Flows page

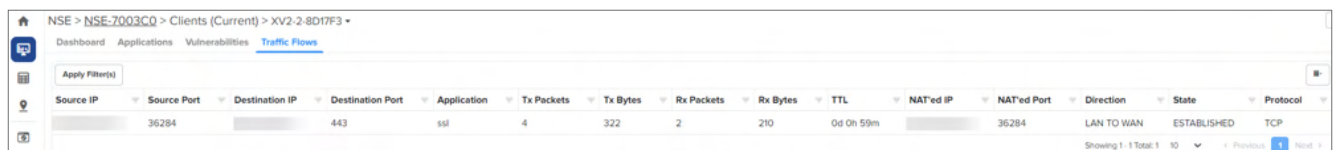


Table 55 Parameters on the Traffic Flows page

Parameter	Description
Source IP	Source IP address of the device or endpoint, based on the flow direction. If the flow direction is from LAN to WAN, the source IP address is the source IP address of the

Table 55 *Parameters on the Traffic Flows page*

Parameter	Description
	device. If the flow direction is from WAN to LAN, the source IP address is the source IP address of the endpoint to which the device has connection to.
Source Port	Source port number.
Destination IP	Destination IP address of the device or endpoint, based on the flow direction. If the flow direction is from LAN to WAN, the destination IP address is the destination IP address of the endpoint. If the flow direction is from WAN to LAN, the destination IP address is the destination IP address of the device.
Destination Port	Destination port number.
Application	Name of the application.
Tx Packets	Transmitted packets.
Tx Bytes	Transmitted bytes.
Rx Packets	Received packets.
Rx Bytes	Received bytes.
TTL	Time to live. Time period during which a session or connection is active.
NAT'ed IP	IP address after the Network Address Translation (NAT) process.
NAT'ed Port	Port number after the NAT process.
Direction	Direction of the communication, indication whether it is incoming or outgoing. Outgoing: LAN to WAN Incoming: WAN to LAN
State	Current state of a connection. The following connection states are valid only if the protocol is TCP. <ul style="list-style-type: none"> • SYN_SENT • SYN_RECV • ESTABLISHED • FIN_WAIT • CLOSE_WAIT • LAST_ACK • TIME_WAIT • CLOSE
Protocol	Name of the protocol, such as TCP, UDP, ICMP, or any.

Certificate

To secure the communication between an NSE device and the VPN clients, you can encrypt the communication. To apply the encryption certificate, navigate to **NSE > Certificate**, upload the certificate and the key files, and then click **Apply Certificate**.



Note

Only certificates with **.der** and **.pem** file extensions are accepted.

Figure 205 *The Certificate page*

The screenshot shows the 'Certificate' page for a device named 'NSE > NSE-700290'. The page has a navigation bar with tabs: Dashboard, Notifications, Configuration, Security, Network, Performance, Software Update, Tools, Clients, and Certificate (which is currently selected). Below the navigation bar, there is a text instruction: 'Download device certificate and private key on the device to encrypt the communication between device & VPN clients connecting using IPSec.' The main content area contains three sections: 'Status' with a text box showing 'Not Uploaded'; 'Certificate' with a text box and a 'Select File' button; and 'Private Key' with a text box and a 'Select File' button. At the bottom left of the form, there is a blue button labeled 'Apply Certificate'.

Wireless LAN Dashboards

This section describes the following topics:

- [Wi-Fi Monitoring](#)
- [Site Dashboard](#)
- [WLANs Dashboard](#)

Wi-Fi Monitoring

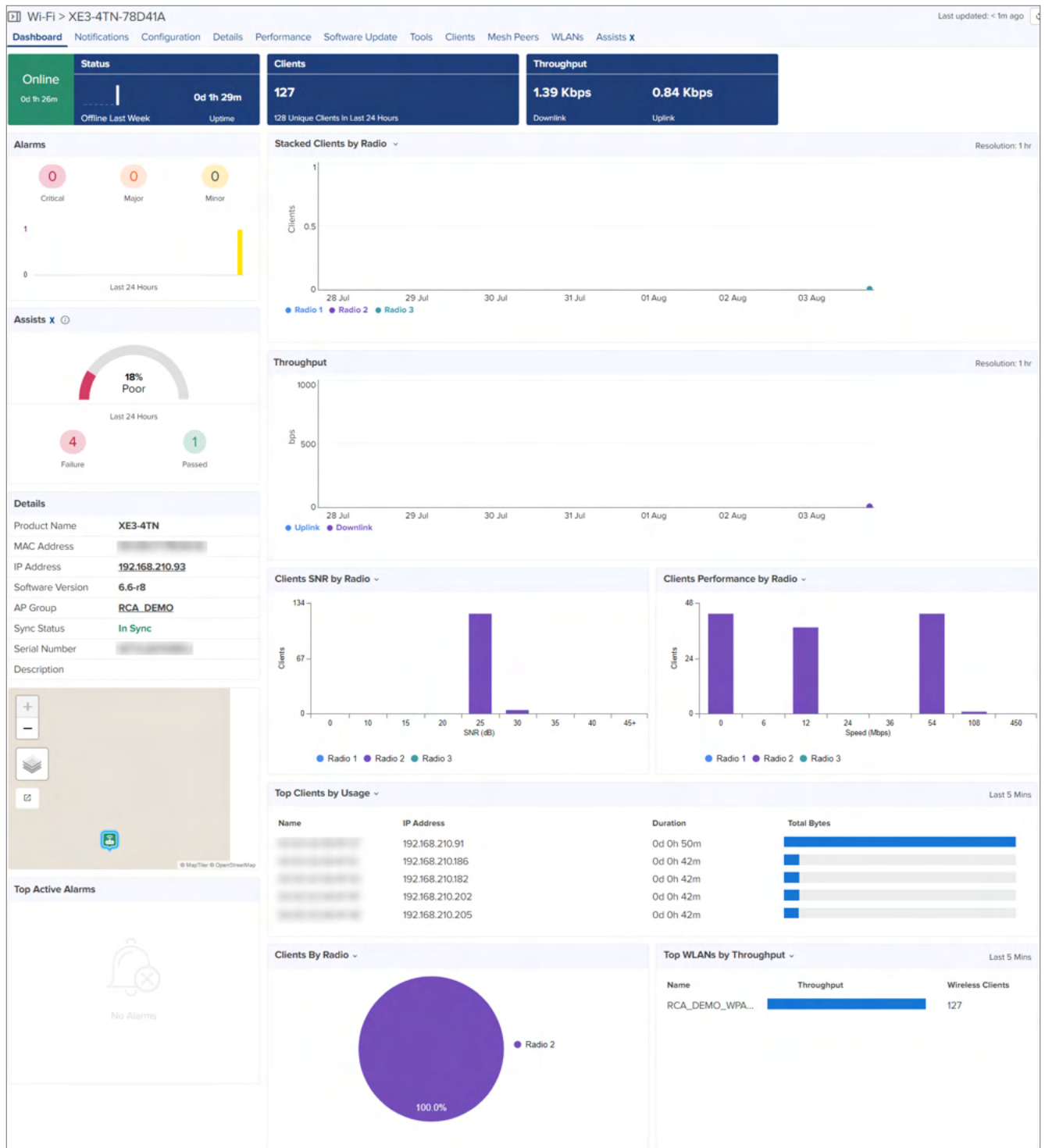
The Wi-Fi Monitoring pages include the following:

- [Dashboard](#)
- [Clients](#)
- [Details](#)
- [Mesh Peers](#)

Dashboard

The cnPilot Dashboard displays **Stacked Clients by Radio, Stacked Clients by Band, Clients by Radio, Clients by Band, Details, Status, Throughput, Top Active Alarms, Top Clients by Usage, Top Clients by Session, Top WLANs by Clients, and Top WLANs by Throughput.**

Figure 206 Device > Dashboard



Clients

The Clients tab displays the details of all the wireless, wired, and unconnected clients.



Note

Clients' historical data is available for 24 Hours and 7 Days for cnMaestro X users.

The following parameters are displayed for wireless clients connected to cnPilot Home (R-Series) APs:

- Actions
 - Edit client name
- Band
- Download
- Host Name
- IPv4 Address
- MAC
- Manufacturer
- RSSI
- SSID
- Upload

Figure 207 *cnPilot Home: Device > Clients > Wireless Clients*

Host Name	IP Address	MAC	Manufacturer	SSID	Band	Radio ID	RSSI	Download	Upload	Actions
Sekhar_Client	192.168.1.39	AA-BB-CC-73-5A-BF	[Local MAC]	76L5-Indra-Test...	5 GHz	2	-55 dBm	48.3 GB	1.6 GB	

The following parameters are displayed for wired clients connected to cnPilot Home (R-Series) APs:

- Actions
 - Edit client name
- Address Type
- Expires
- Interface
- IPv4 Address
- MAC
- Name
- Status

Figure 208 *cnPilot Home (R-Series): Device > Wired Clients*

Name	IP Address	MAC	Address Type	Expires	Interface	Status
IN01H35G152	192.168.1.207		DHCP	65740s	LAN3	Active

The following parameters are displayed for wireless clients connected to Enterprise Wi-Fi APs (E-, XE-, XV-, and X7-Series):

- Actions
 - Edit client name
 - Block client
- Device (Displayed only at the site-level)
- Device MAC (Displayed only at the site-level)
- Auth Status
- Authentication Type
- Band
- Capability
- Client Type
- Download
- Download Quota
- Download Quota Balance
- Guest Access Type
- Host Name
- IPv4 Address
- IPv6 Address
- Last Duration
- Last seen
- MAC
- Manufacturer
- OS
- Radio ID
- Radio Mode
- RSSI
- Session Expiry
- SNR
- SSID
- Status
- Streams
- Total Quota
- Total Quota Balance
- Upload
- Upload Quota
- Upload Quota Balance
- User

- VLAN-ID

Figure 209 *Enterprise Wi-Fi: Device Dashboard > Wireless Clients*

Wi-Fi > XE5-8-E01E51													
Dashboard Notifications Configuration Details Performance Software Update Tools Clients Mesh Peers WLANs Assists X													
Wireless Clients Wired Clients Unconnected Clients													
<input type="text"/> Apply Filter(s) Managed Account: Base Infrastructure Disconnect Disconnect All Export													
<input type="checkbox"/>	Host Name	User	MAC	IPv4 Address	VLAN-ID	SSID	Last Duration	RSSI	Band	Capability	Streams	Radio ID	Radio Mode
<input type="checkbox"/>	DESKTOP-K9P7CAE		E4:60:17:64:E9:D4	192.168.20.104	1	rfc_lion	1d 2h 3m	-43 dBm	5 GHz	6E	2	5	axa

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

The following parameters are displayed for wired clients connected to Enterprise Wi-Fi APs (E-, XE-, XV-, and X7-Series):

- Address Type
- Auth Status
- Authentication Type
- Client Type
- Device (Displayed only at the site-level)
- Device MAC (Displayed only at the site-level)
- Download
- Download Quota
- Download Quota Balance
- Expires
- Guest Access Type
- Host Name
- Interface
- IPv4 address
- Last Duration
- MAC
- Manufacturer
- Model
- OS
- OS Version
- Portal Mode
- Session Expiry
- Total Quota
- Total Quota Balance
- Type
- Upload
- Upload Quota

- Upload Quota Balance
- VLAN-ID



Note

The historical clients data is available for 24 Hours and 7 Days for cnMaestro X users in System-/ Network-/Site- and the device-levels.

Figure 210 Enterprise Wi-Fi: Device Wired Clients

Figure 211 Enterprise Wi-Fi (Xirrus-Series) Wireless Clients



Note

Wired clients are not supported on Xirrus-Series APs.

The following parameters are displayed for unconnected clients for Enterprise Wi-Fi APs (E-, XE-, XV-, and X7-Series):



Note

Following are some of the typical failure reasons for unconnected clients:

- Denied access by a MAC Association ACL
- Failed authentication to a RADIUS server due to invalid credentials
- Failed the protocol handshake of WPA2-Pre-shared keys

- Host Name
- MAC
- Manufacturer
- SSID
- Last Seen

Figure 212 Enterprise Wi-Fi: Device Dashboard > Unconnected Clients

Host Name	MAC	Manufacturer	SSID	Last Seen
No Unconnected Clients				

Client Dashboard

The user can view the applications used by client when the **Application Visibility** option is enabled as shown below.

The Client Dashboard displays the details of the clients connected to the Wi-Fi device.



Note

- Enable the **Application Visibility** feature to view **Application** page. It is supported only for XE, XV, X7 series devices.
- **Dashboard** is supported for all cnPilot devices.
- The historical clients data is available for 24 hours, 7 days, and to a maximum of 30 days for cnMaestro X users.

Figure 213 XE, XV, and X7 Series: Device Dashboard Wireless Clients

Wi-Fi > XE3-4TN-78D41A

Dashboard

Notifications

Configuration

Details

Performance

Software Update

Tools

Clients

Mesh Peers

WLANs

Assists

X

Wireless Clients

Wired Clients

Unconnected Clients

Apply Filter(s)

Managed Account: Megha

Clients: Current

Disconnect

Disconnect All

Export

<input type="checkbox"/>	Host Name	Managed Account	User	AP	IP Address	MAC	VLAN-ID	Manufacturer	OS	Capability	SSID	
<input type="checkbox"/>	00:00:00			XE	11A	19:00:00:00:00:49	0C:00:00:00:00:01	1	Marconi plc	Linux	an	RCA_DEMO_WPA2PSK_1
<input type="checkbox"/>	00:00:01			XE	11A	19:00:00:00:00:23	0C:00:00:00:00:01	1	Marconi plc	Linux	an	RCA_DEMO_WPA2PSK_1
<input type="checkbox"/>	00:00:02			XE	11A	19:00:00:00:00:37	0C:00:00:00:00:02	1	Marconi plc	Linux	an	RCA_DEMO_WPA2PSK_1
<input type="checkbox"/>	00:00:03			XE	11A	19:00:00:00:00:16	0C:00:00:00:00:03	1	Marconi plc	Linux	an	RCA_DEMO_WPA2PSK_1
<input type="checkbox"/>	00:00:04			XE	11A	19:00:00:00:00:38	0C:00:00:00:00:04	1	Marconi plc	Linux	an	RCA_DEMO_WPA2PSK_1
<input type="checkbox"/>	00:00:05			XE	11A	19:00:00:00:00:36	0C:00:00:00:00:05	1	Marconi plc	Linux	an	RCA_DEMO_WPA2PSK_1
<input type="checkbox"/>	00:00:06			XE	11A	19:00:00:00:00:42	0C:00:00:00:00:06	1	Marconi plc	Linux	an	RCA_DEMO_WPA2PSK_1
<input type="checkbox"/>	00:00:07			XE	11A	19:00:00:00:00:50	0C:00:00:00:00:07	1	Marconi plc	Linux	an	RCA_DEMO_WPA2PSK_1
<input type="checkbox"/>	00:00:08			XE	11A	19:00:00:00:00:20	0C:00:00:00:00:08	1	Marconi plc	Linux	an	RCA_DEMO_WPA2PSK_1
<input type="checkbox"/>	00:00:09			XE	11A	19:00:00:00:00:26	0C:00:00:00:00:09	1	Marconi plc	Linux	an	RCA_DEMO_WPA2PSK_1

0 - Clients Selected

Showing 1 - 10 Total: 12710< Previous12345...13Next>

To view the **Dashboard**, navigate to **Clients > Wireless Clients** and click a value in the **Host Name** column.

A detailed **Client Dashboard** page is displayed. For more details, refer to

Renaming Client Host-names

You can assign friendly host-names for the clients. To edit the host-name of connected wired or wireless client, follow these steps:

1. Navigate to **Clients > Wireless Clients** or **Wired Clients** tab.

System

Dashboard Notifications Configuration Statistics Report X Software Update Applications X **Clients** Mesh Peers Assists X

Wireless Clients Wired Clients

Search Managed Account: All Accounts Clients: Current Export

SNR	Client Type	Upload	Download	Managed Account	Status	Last Duration	Last Seen	Actions
31 dB	Client	6.0 KB	94.5 KB	Base Infrastructure	Connected	0d 0h 57m	28 Mar 2023, 12:03:48 PM	
42 dB	Client	141.8 MB	8.3 GB	Sekhar_Operator	Connected	0d 19h 3m	28 Mar 2023, 12:03:49 PM	
41 dB	Client	14.8 MB	0	Sekhar_Operator	Connected	7d 21h 50m	28 Mar 2023, 12:03:49 PM	
58 dB	Client	404.4 KB	207.5 KB	Base Infrastructure	Connected	0d 1h 11m	28 Mar 2023, 12:03:49 PM	
45 dB	Client	6.7 MB	353.3 MB	Sekhar_Operator	Connected	0d 19h 4m	28 Mar 2023, 12:03:49 PM	

Showing 1 - 5 Total: 5 10 < Previous 1 Next >

2. Scroll to the right most side of the clients list and click on the **Edit** icon under the **Actions** column.
3. In the **Edit Client Name** pop-up window, enter a friendly name for the client.

Edit Client Name

Host Name*

Hostname_new

Save Cancel

4. Click **Save**.

The new host-name is displayed in all the places such as the Client Dashboards, Audit logs, and Reports.

Details

Details page displays the Overview, Network Info, and Neighbors List.

Wi-Fi > X7-35X-B0007A

Dashboard

Notifications

Configuration

Details

Performance

Software Update

Tools

Clients

Mesh Peers

WLANs

Assists X

Overview

Network Info

Neighbors List

System

Device

X7-35X-B0007A

Product Name

X7-35X

Health

● Online (7d 7h 51m)

IPv4 Address

10.110.202.171

MAC Address

Description

Serial Number

Hardware

Tri Radio Tri Band Wi-Fi 7 2x2 Indoor Access Point

DA Version

4.131

Last Reboot

Thu Apr 18 2024 18:16 (cnMaestro initiated software update)

Location

Onboard Date

Apr 03 2024 12:02:22

Available Memory

77%

CPU Utilization

3%

RF Statistics (%)

Radio

Radio 1

Radio 2

Radio 3

Band

2.4 GHz

5 GHz

6 GHz

Noise Floor

-85

-100

-110

Interference

14634

18

1661

Airtime (total/tx/rx/busy)

14635/1/0/0

19/1/0/0

1661/0/0/0

Channel Utilization

14635

19

1661

Packet Error Rate

0

0

0

Network Allocation Vector

-

-

-

Configuration Update

History

Date

Status

AP Group

24 Apr 2024, 12:15 PM

● Success

_voucher_testing

23 Apr 2024, 02:32 PM

● Success

_voucher_testing

22 Apr 2024, 01:21 PM

● Success

_voucher_testing

Radio Details

Radio

Radio 1

Radio 2

Radio 3

Band

2.4 GHz

5 GHz

6 GHz

State

ON

ON

ON

Channel

6

157

149

Channel Width

20 MHz

40 MHz

20 MHz

Power ⓘ

24 dBm

25 dBm

12 dBm

Antenna Gain

5 dBi

6 dBi

6 dBi

EIRP

29 dBm

31 dBm

18 dBm

MAC Address

RF Quality

🟢 Excellent

🟢 Excellent

🟢 Excellent

WLANs

1

1

1

Mesh

OFF

OFF

OFF

Clients

0

0

0

UL Throughput

0 Kbps

0 Kbps

0 Kbps

DL Throughput

0 Kbps

0 Kbps

0 Kbps

Software Update

Active Software Version

7.0-b10

Inactive Software Version

7.0-b2

History

Date

Status

Version

18 Apr 2024, 06:19 PM

● Success

7.0-b10

18 Apr 2024, 12:47 PM

● Skipped

6.6.0.3-r8

Overview

The **Details > Overview** page displays information, such as System, RF Statistics (%), Configuration Update, Radio Details, Software Update, and History.

Network Info

The **Details > Network Info** page displays the following parameters for cnPilot Home (R-Series) router:

- Ethernet Ports
 - Rx Bytes
 - Rx Error Bytes
 - Rx Packets
 - Tx Bytes
 - Tx Error Bytes
 - Tx Packets
 - Type
- FXS Ports

- Hook State
- Phone Number
- SIP Account Status
- Type

Figure 214 *cnPilot Home: Device > Details > Network Info*

Wi-Fi > cnPilot-r201P-D0N0TDIsTuRB						
Dashboard Notifications Configuration Details Performance Software Update Tools Clients WLANs						
Overview Network Info						
Ethernet Ports						
Type	Tx Bytes	Rx Bytes	Tx Packets	Rx Packets	Tx Error Bytes	Rx Error Bytes
WAN	4518147	18211803	28696	54061	0	0
LAN 1	0	0	0	0	0	0
LAN 2	0	0	0	0	0	0
LAN 3	0	0	0	0	0	0
LAN 4	0	0	0	0	0	0
FXS Ports						
Type	SIP Account Status	Phone Number	Hook State			
FXS 1	Unregistered	-	On			
FXS 2	Unregistered	-	On			

- Ethernet Ports
- PPPoE
- Routes
- Tunnels
- VLAN Pool

Figure 215 *Enterprise Wi-Fi: Device >Details > Network Info*

Wi-Fi > E700-DD9052

Dashboard

Notifications

Configuration

Details

Performance

Software Update

Tools

Clients

Mesh Ports

WLANs

Overview

Network Info

Neighbors List

VLAN

Interface Name	IPv4 Address	IPv6 Address	Source	Tx Bytes	Rx Bytes	Tx Avg	Tx Max	Tx Min	Bx Avg	Bx Max	Bx Min	Tx Drops	Rx Drops
PORT CHANNEL1	0.0.0.0	N/A		0	0	0	0	0	0	0	0	0	0
VLAN1	10.10.202.76	9-B0:5a:c1:7a:f0:ad:90:52:64	255.255.255.0	259895	28201884							0	0
ETH-0	0.0.0.0	N/A		312835	3481763	0	0	0	16	20	16	0	562
ETH-0	0.0.0.0	N/A		0	0	0	0	0	0	0	0	0	0

IPv4 Routes

Destination	Mask	Gateway	Flags	Metric	Interface
0.0.0.0	0.0.0.0	10.10.202.254	UG	0	VLAN0
10.10.202.0	255.255.255.0	0.0.0.0	U	0	VLAN0
169.254.0.0	255.255.0.0	0.0.0.0	U	0	VLAN0

IPv6 Routes

Destination	Gateway	Flags	Metric	Route	Use	Interface
No Routes Configured						

DNS Server(s)

IP Address	Interface
10.10.0.10	VLAN0
10.10.0.11	VLAN0

Domain Name

Domain Name

CAMWORK.COM

Ethernet Ports

Type	Status	Mode	Access VLAN	Native VLAN	Native Tag	Allowed VLAN	Port Speed	Duplex	MAC
ETH-0	N/A	Access	1	1	Native		1000M		
ETH-0	N/A	Access	1	1	Native				

IPv6 Routes

IPv6 Routes						
Destination	Gateway	Flags	Metric	Refs	Use	Interface
2006:cafe::15::/64	::	UAe	256	0	0	VLAN1
::/0	fe80::529a:4c:ffe2:b0ee10	UGDAe	1024	1	0	VLAN1

DNS Servers

DNS Server(s)	
IP Address	Interface
10.110.12.110	VLAN1
10.110.12.111	VLAN1

The following parameter details are displayed in E-Series:

- Port
- Rx Broadcasts
- Rx Frames
- Rx Frames Oversize
- Rx Frames Undersize
- Rx Frames with Error
- Rx Octets
- Tx Broadcasts
- Tx Frames
- Tx Octets

Figure 216 Enterprise Wi-Fi (Xirrus-Series): Device > Dashboard > Network Info

Wi-Fi > X4096170F296A																
Dashboard Notifications Configuration Details Performance Software Update Tools Clients WLANs																
Overview Network Info																
VLAN																
Interface Name	Status	Link	Duplex	Speed	Rx Bytes	Tx Bytes	Rx Packets	Tx Packets	Rx Errors	Tx Errors	Rx Drops	Tx Drops	Rx Compressed	Tx Compressed	Rx Multicast	
gig1	up	up	full	1000	222854845	17340307	687537	39288	0	0	8	0	0	0	417162	
gig2	up	down	half	10	0	0	0	0	0	0	0	0	0	0	0	

Figure 217 PTP 650/670/700: Device > Details > Network Info

Ethernet Ports									
Type	Status	Mode	Access VLAN	Native VLAN	Native Tag	Allowed VLAN	Port Speed	Duplex	MAC
ETH1	N/A	access	1	1	false		1000M		
ETH2	N/A	access	1	1	false		-		

Neighbors List

The **Neighbors List** displays the BSSID, SSID, Channel, and SNR details of neighboring 2.4 GHz and 5 GHz radios.

Figure 218 *Neighbors List*

Wi-Fi > XE5-8-E001CB

Dashboard Notifications Configuration **Details** Performance Software Update Tools Clients Mesh Peers WLANs

Overview Network Info **Neighbors List**

2.4 GHz 5 GHz

BSSID Search

BSSID	SSID	Channel	SNR
	jp_sage_1	6	13
	cm_sit_tiger1_clone	6	45
	epsk1	6	7
	Cambium	6	7
	cm_sit_tiger1_ours	6	30
	cm_sit_tiger1_our	6	48
	cm_sit_tiger1_clone	6	8
	Ragh_EPSKTest	6	13
	HA-WLAN-Raja	6	16
	cm_sit_tiger1_our505	6	25

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

Mesh Peers

The Mesh Peers tab displays information related to mesh such as SNR, RSSI, and Band. This provides insight to the performance between the Mesh Client and Mesh Base.

Figure 219 *Device > Mesh Peers*

System

Dashboard Notifications Configuration Statistics Reports x Software Update Applications x Clients **Mesh Peers** Assists x

Band Search Managed Account: All Accounts Export

Base AP	MAC	Mesh Base	Mesh Client	SSID	End Hosts	Host Name	Managed Account	IP Address	Band	VLAN	WLAN	Uptime	SNR	RSSI	Auth
XV2-22H-E537CF				_Mesh_B...	View End Hosts		Base Infrastructure	0.0.0.0	5 GHz	1	2	0d 0h 28m	42	-53	Yes
XV2-23T-E53F39				_Mesh_B...	View End Hosts		Base Infrastructure	0.0.0.0	5 GHz	1	1	0d 0h 33m	40	-55	Yes

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

Roaming History for Mesh Peers

To view the **Information** and **Roaming History**, perform the following:

In the **Mesh Peers** tab, click the **Host Name**.

A detailed Information and Roaming History window pops up.

Figure 220 *Mesh Peers > Host Name > Information*



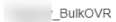
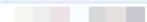
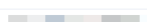
Information		Roaming History
Base		
Client		
IP Address	192.168.1.4	
IPv6 Address		
Name	E410-Client-DoNotTouch	
SSID	mesh-link	
VLAN	1	
Age	N/A	
Band	5 GHz	
SNR	40 dBm	
RSSI	-55 dBm	
Average SNR	dBm	
Average RSSI	dBm	
Association Time	N/A	
Tx Packets	2142	
Rx Packets	3836	
Tx Bytes	518537 Bytes	
Rx Bytes	678387 Bytes	
Average Tx	Kbps	
Average Rx	Kbps	
Max Tx	Kbps	
Max Rx	Kbps	
Min Tx	Kbps	
Min Rx	Kbps	
Data Rate	173	
Status	UP	
Autorized	Yes	
Profile	base	
End Hosts		
Network	 _BulkOVR	
Tower/Site	Clients_Site_DND	
Managed Account	Base Infrastructure	

Figure 221 *Mesh Peers > Host Name > Roaming History*

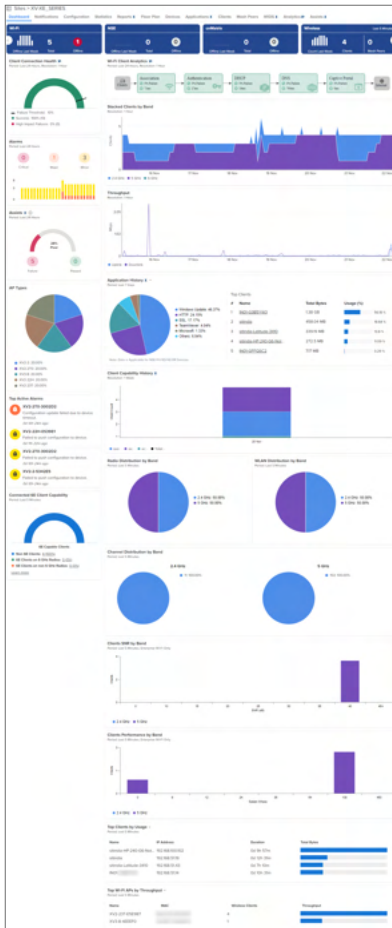
Information **Roaming History**

Connected AP	AP MAC Address	Connected	Last Duration	Tx + Rx
N/A		Tue May 17 2022 09:42:55 UTC +0...	0d 0h 9m	1.3 KB
N/A		Mon May 16 2022 15:55:14 UTC +0...	0d 2h 35m	2.1 KB

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

Site Dashboard

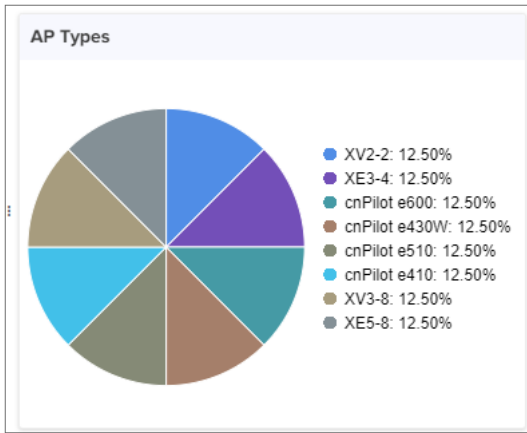
The Site Dashboard provides the overview of site-related parameters and devices.



The Site Dashboard displays the following graphics:

- [AP Types](#)
- [Stacked Clients by Band](#)
- [Channel Distribution by Band](#)
- [Clients Performance by Band \(Enterprise Wi-Fi\)](#)
- [Clients SNR by Band \(Enterprise Wi-Fi\)](#)
- [Connected 6E Client Capability](#)
- [Client Capability History](#)
- [Radio Distribution by Band](#)
- [WLAN Distribution by Band](#)
- [RF Quality](#)
- [Wireless LAN Dashboards](#)
- [Wireless LAN Dashboards](#)
- [Floor Plan](#)
- [Wireless LAN Dashboards](#)
- [Wireless LAN Dashboards](#)

AP Types

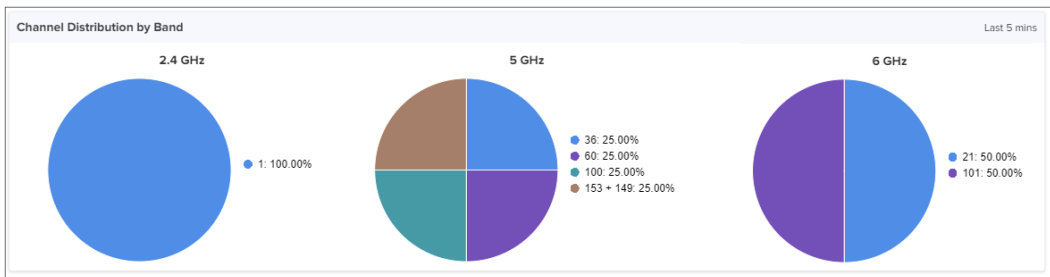


Stacked Clients by Band



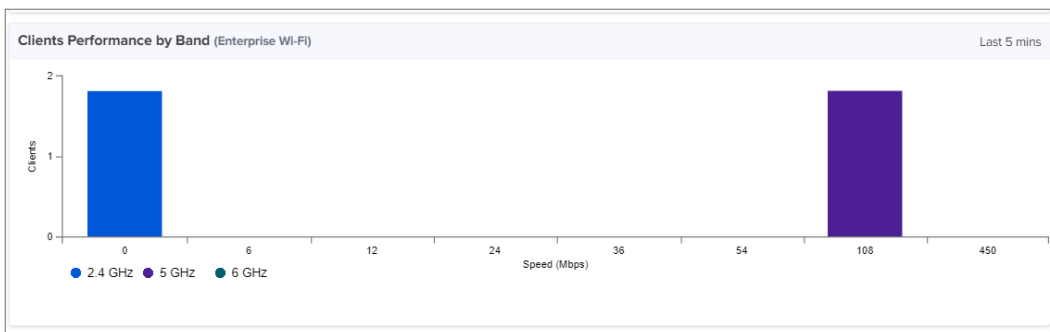
Channel Distribution by Band

Channel distribution displays usage of channels in 2.4 GHz, 5 GHz and 6 GHz. This helps in planning and implementing WLANs within a high-density environment. It displays the usage details for last 5 minutes.

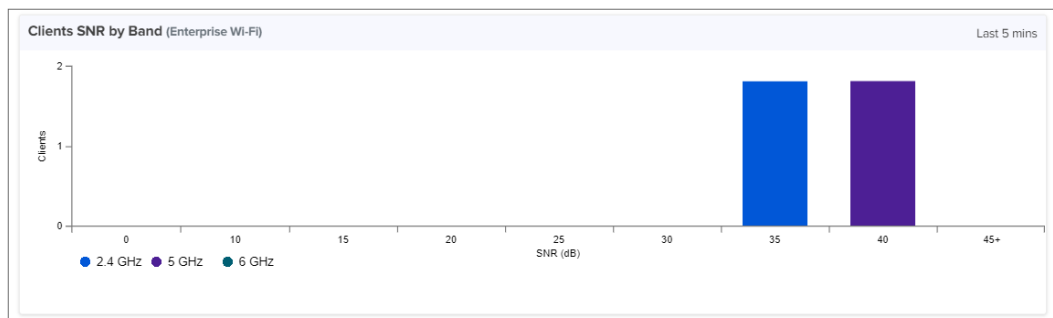


Clients Performance by Band (Enterprise Wi-Fi)

Clients performance details is displayed for last 5 minutes.



Clients SNR by Band (Enterprise Wi-Fi)



Connected 6E Client Capability

The Connected 6E Client Capability widget presents a point-in-time view of Wi-Fi 6E Clients associating to non-6E radios. These Clients may experience better service if SDR radios are upgraded from 5 GHz to 6 GHz. A high percentage of 6E Capable Clients connecting to non-6E radios is a signal to upgrade radios to 6 GHz. The Connected 6E Client Capability widget is represented using different colors and corresponding percentage values as described below:

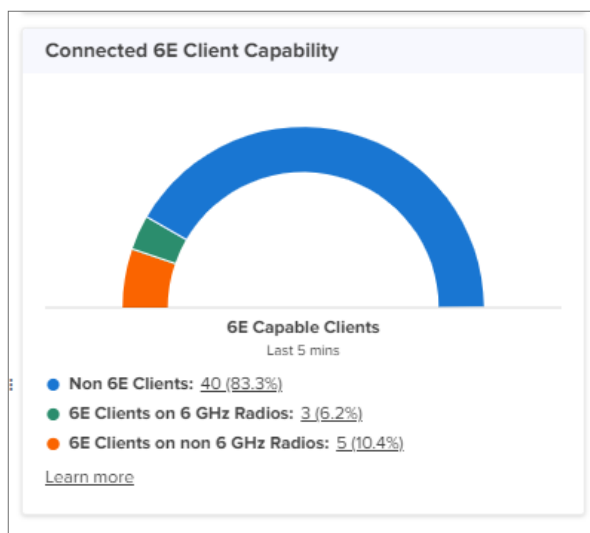
- Non 6E Clients: represents non 6E clients connected across the devices at the Site level.
- 6E Clients on 6 GHz Radios: represents 6E clients connected across the devices at the Site level.
- 6E Clients on non 6 GHz Radios: represents 6E clients connected across the devices on non 6 GHz radios at the Site level.



Note

For best results, deploy a few radios in 6G mode in high traffic areas.

Figure 222 *Connected 6E Client Capability*



Clicking next to clients number navigates to **Wireless Clients** page.

Client Capability History

The Client Capability History graphic displays the highest detected Wi-Fi protocol for Clients active at a Site on weekly basis. Wi-Fi 6E devices are grouped into a single 6E category. A large number of 6E Capable Clients are a signal to expand infrastructure to include 6 GHz radios. If the period of evaluation extends more than a few weeks, the bar chart converts to a line chart.

Figure 223 Clients History in line chart

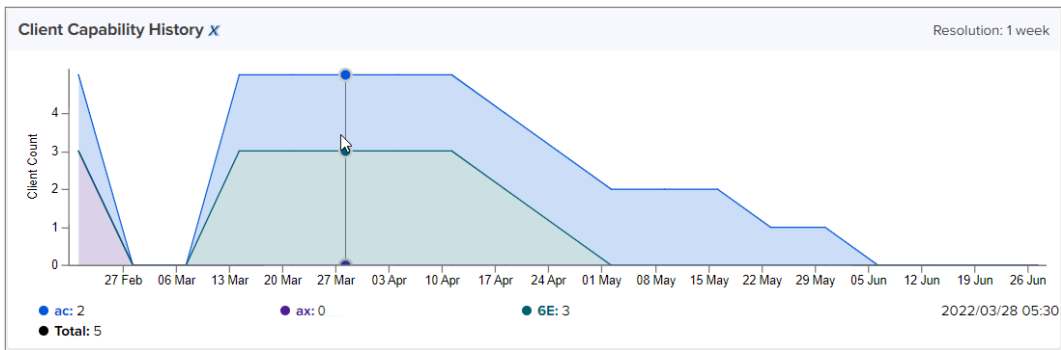
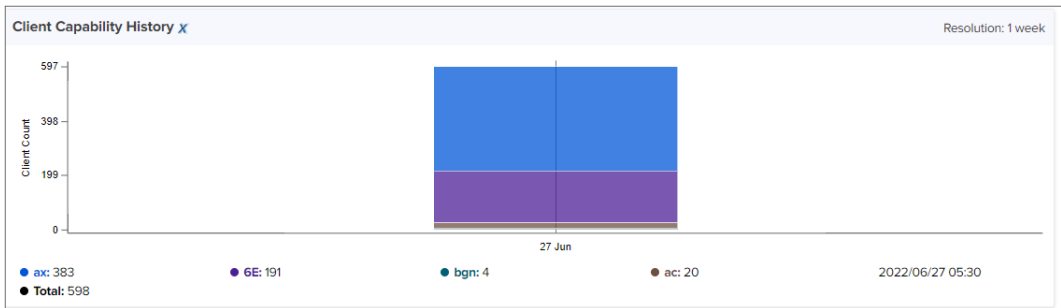
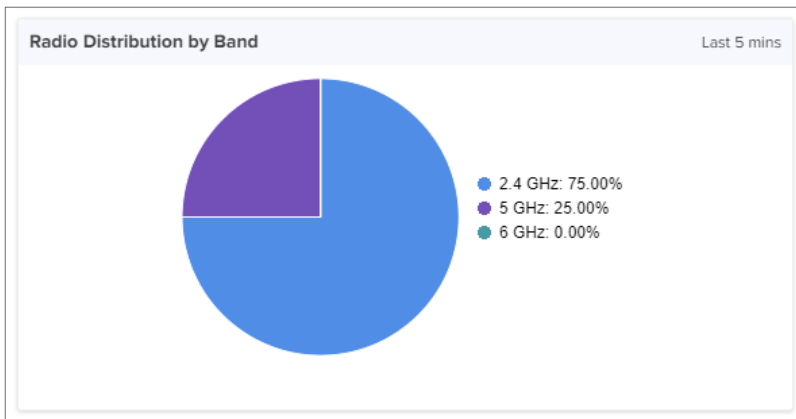


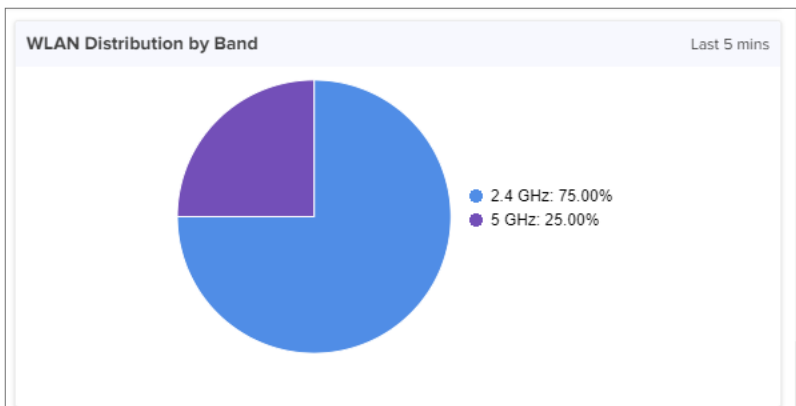
Figure 224 Clients History in bar chart



Radio Distribution by Band



WLAN Distribution by Band



RF Quality

Provides an indication of the current RF Quality across the Site.

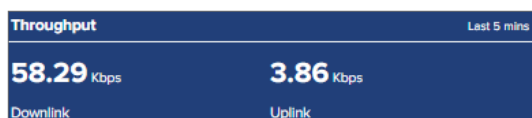


Radio RF Quality Index is an indication of wireless clients and or MESH clients' RF link as seen by the access point radio (AP). It is the average of all the wireless clients and or mesh clients SNR.

- If aggregated SNR is more than 45: RF Quality Index is marked as Excellent
- If aggregated SNR is more than or equal to 35 and below 45: RF Quality Index is marked as Good
- If aggregated SNR is more than or equal to 25 and below 35: RF Quality Index is marked as Average
- If aggregated SNR is less than 25: RF Quality Index is marked as poor

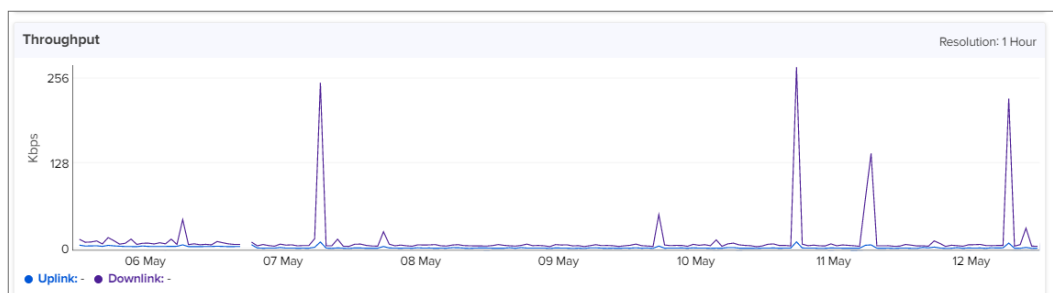
Throughput

Displays aggregated throughput for all the clients.



Throughput Graph

Throughput graph displays client traffic for the last week.



Top Wi-Fi APs by Throughput

Top Wi-Fi APs by Throughput			Last 5 mins
Name	Clients	Throughput	
E600-0C1864	3	<div></div>	
MB-XV3-8-4DDB84	1	<div></div>	
E510-C18B5F	2	<div></div>	
E600-027AA6	1	<div></div>	
E410-E1508C	4	<div></div>	

Wi-Fi Devices Availability (Total and Offline)

Displays total number of Access Points in the Site and the devices that are Offline.



Top Clients by Session

Displays the top clients by session and the respective details.

Top Clients by Session ▾				Last 5 mins
Name	IP Address	Duration	Total Bytes	
	192.168.210.58	0d 6h 6m		
sitindia-Vostro-15-3568	192.168.210.146	0d 6h 6m		
sitindia-Latitude-3410	192.168.210.55	0d 6h 6m		
	192.168.210.151	0d 6h 6m		
sitindia-Latitude-3410	192.168.210.120	0d 6h 6m		

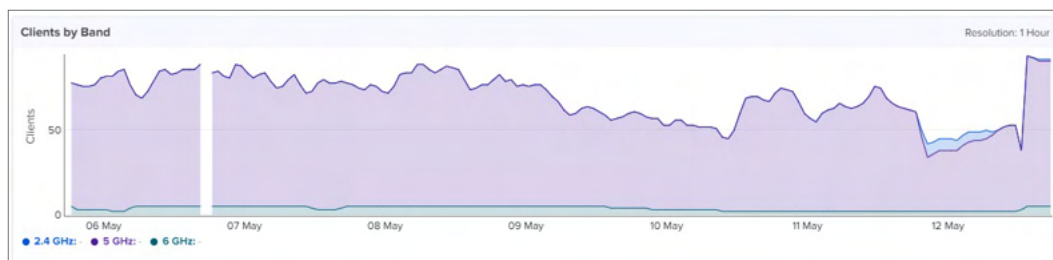
Top Clients by Usage

Displays the top clients by usage and the respective details.

Top Clients by Usage ▾				Last 5 mins
Name	IP Address	Duration	Total Bytes	
	192.168.210.131	0d 6h 3m		
sitindia-Latitude-3410	192.168.210.54	0d 6h 3m		
	192.168.210.117	0d 6h 3m		
	192.168.210.95	0d 4h 3m		
sitindia-Latitude-3410	192.168.210.120	0d 6h 3m		

Wireless Clients Graph

Wireless clients graph displays clients that are connected in Radio 1 (2.4 GHz), Radio 2 (5 GHz), and Radio 3 (6 GHz).



Floor Plan

A Floor Plan is used to view APs, device status, connected clients, and transmit power. This is done by creating the floor plan and adding devices. You can upload a floor plan for each floor based on the selected environment type.

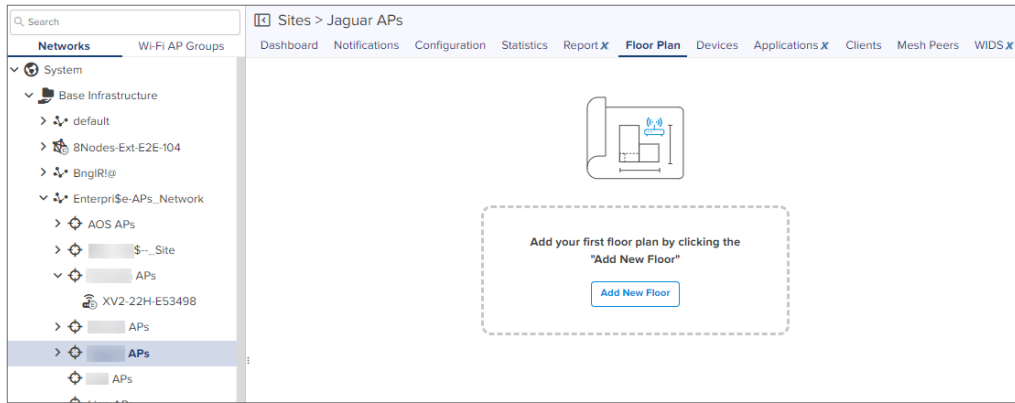
To create a floor plan, perform the following steps:

1. Navigate to **System > Network > Enterprise Site > Floor Plan**.

Floor Plan can be uploaded when a **Site** is created.

2. Click **Add New Floor**.

The **Add New Floor** window appears.



3. Enter the parameters for a new floor plan.

Add New Floor

Name

Level

0

Environment Type

Office (Cubicle)

Adjustment (dB)

0

AP Height

Meters

Floor Plan

Select File

Minimum recommended size 1024 px X 800 px. Maximum size of 5MB.

Allowed file formats are JPEG,JPG,PNG or GIF.

Width

Length

Meters

Add

Cancel

Table 56 *Fields in Floor Plan*

Field	Description
Name	Name of the floor.
Level	Level of the floor.
Environment Type	Floor type such as the following: <ul style="list-style-type: none"> • Apartment • Hospital • Hotel • Office (Cubicle) • Office (Walled) • Outdoors

Table 56 *Fields in Floor Plan*

Field	Description
	<ul style="list-style-type: none"> School University Warehouse
Adjustment	Device adjustment in dB.
Height	Height of the ceiling in meters or feet.
Width	Width of the floor in meters or feet.
Length	Length of the floor in meters or feet.



Note

Environment Type, Adjustment, and Height are currently unused by cnMaestro. They will become important when RF Heat Maps are added in a later release.

- Click **Select File** and browse the required floor plan for uploading.

A preview of the uploaded floor plan is shown below:

Preview of Floor Plan

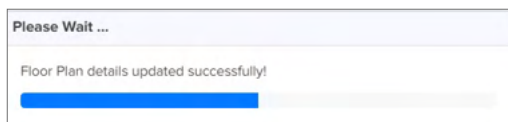


Note

- The minimum size of a floor plan is 1024 X 800 pixels.
- The maximum supported file size is 5 MB.
- The supported file formats are JPEG, JPG, PNG, and GIF.

- Click **Add**.

A successful message is displayed, as shown below:



The **Zoom** control allows you to zoom in and out of the floor plan.



Note

- Only cnMaestro X users can upload more than one floor plan.
- You cannot duplicate the floor level for other floor plans.
- If the devices are in a default location and upgraded to 3.1.1, the devices are moved to the **Unmapped Devices** option.

The right pane of the Floor Plan window provides details of uploaded floor plans, such as Floor View, Map Opacity, Radio Details, Filters, and the devices in the floor plan.

Figure 225 *Configure Floor Plan*

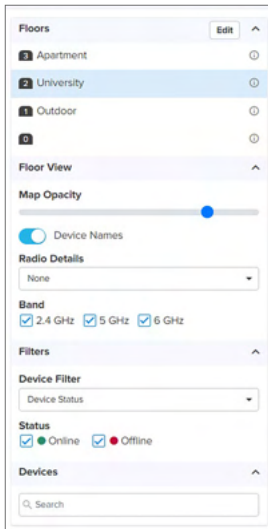


Table 57 *Fields to configure floor plan page*

Field	Description
Floors	<p>Indicates the floor level. The following actions are available:</p> <ul style="list-style-type: none">• Click Add to add new floor level.• Drag and drop the selected devices from the right pane to the required floor level. If multiple floor levels are available, then select required floor level from the dropdown.• Select the floor level and click Edit (✎) icon to edit the uploaded floor level.• Click the Delete (✖) icon to delete a uploaded floor level.• Click on the info icon, next to floor level uploaded, to view the floor details. <div></div> <ul style="list-style-type: none">• In the Devices on this floor dropdown, you can view the following options:<ul style="list-style-type: none">◦ Unmapped Devices: Devices not mapped to the floor plan.

Table 57 Fields to configure floor plan page


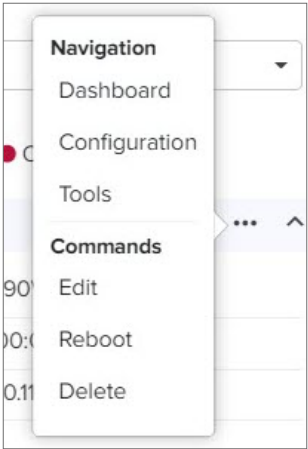
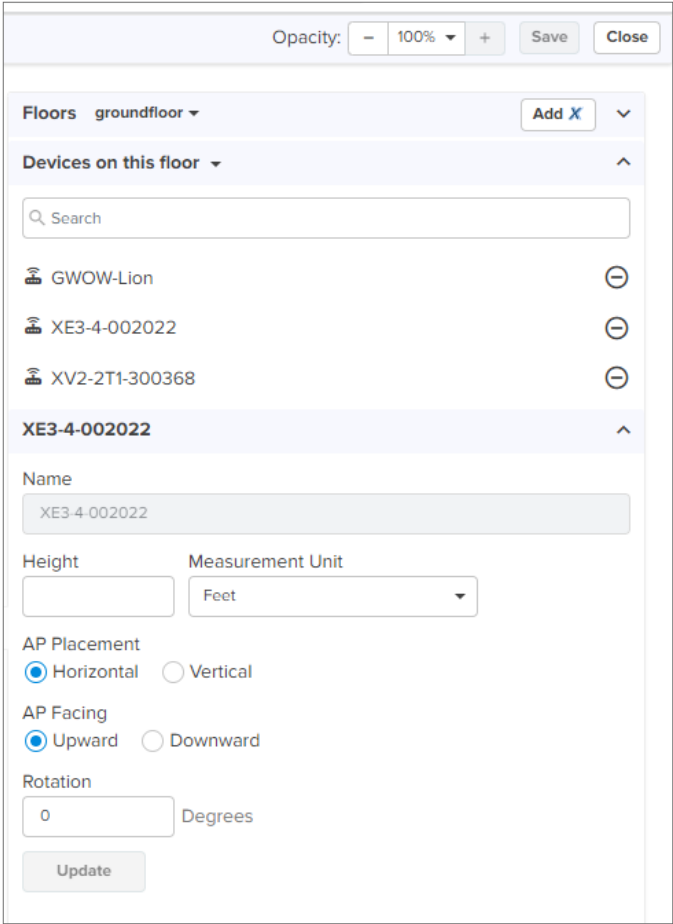
Field	Description
	<ul style="list-style-type: none"> ◦ Devices on this floor: Devices available on the floor plan. ◦ Devices on other floors: Displays devices on the other floors. • Click Remove (⊖) icon to remove device from the floor level.
Floor View	<p>Configure device presentation. The following options are available:</p> <ul style="list-style-type: none"> • Map Opacity: Increase or decrease the opacity for the better visibility of uploaded floor plan. • Device Names: Toggle to view device names on the floor plan. • Radio Details: View the radio details such as Client Count, Channel, and Power. • Band: Select the desired band 2.4 GHz, 5 GHz, and 6 GHz (radio frequency).
Filter	Filter devices by Device Status, Channel, and Power.
Devices	<p>View and edit the device details. The following actions are available:</p> <ul style="list-style-type: none"> • Select the device on the floor plan or type the device name in the search field. • Click the eye icon (👁) to Show or Hide the device on the floor plan. • Click on the device name to view device details, as shown below:  <ul style="list-style-type: none"> • Click ellipsis (...) icon next to the device name, to navigate to the device homepage.  <ul style="list-style-type: none"> • Click Edit on the top right corner and select the device in the current floor.

Table 57 Fields to configure floor plan page

Field	Description
	 <p>Edit the AP Placement, AP Facing and Rotation options.</p> <ul style="list-style-type: none"> • Click Update and Save. • Click Remove (⊖) icon to remove device from the floor plan. • Click Save.

WLANs Dashboard

The **WLANs** dashboard displays details of all WLANs that are applied on devices at a given site. It also displays the number of APs on which the WLAN is applied, the SSID that is configured, and the number of clients that are currently connected to those SSIDs. It also displays the uplink and downlink throughput for that WLAN.

WLAN aggregation is performed only at the site-level. If no clients are connected to the APs, no WLAN data is aggregated.

- To view the WLANs dashboard, navigate to **Monitor and Manage** > **<Site-Name>** > **WLANs^X** tab.

Figure 226 *WLANs Dashboard*

WLAN	SSID	AP	Clients	Downlink Usage	Uplink Usage
diva_wpa2_ent_rca	diva_wpa2_ent_rca	2	2	158.9 KB	247.9 KB
diva_open_rca	diva_open_rca	2	1	822 B	241 KB
diva_wpa3_rca	diva_wpa3_rca	2	1	754 B	22.8 KB
diva_psk_rca	diva_psk_rca	2	0	0	0
diva_mac_auth_rca	diva_mac_auth_rca	2	0	0	0
diva_sae_owe_rca	diva_sae_owe_rca	2	0	0	0
diva_ga_rca	diva_ga_rca	2	0	0	0

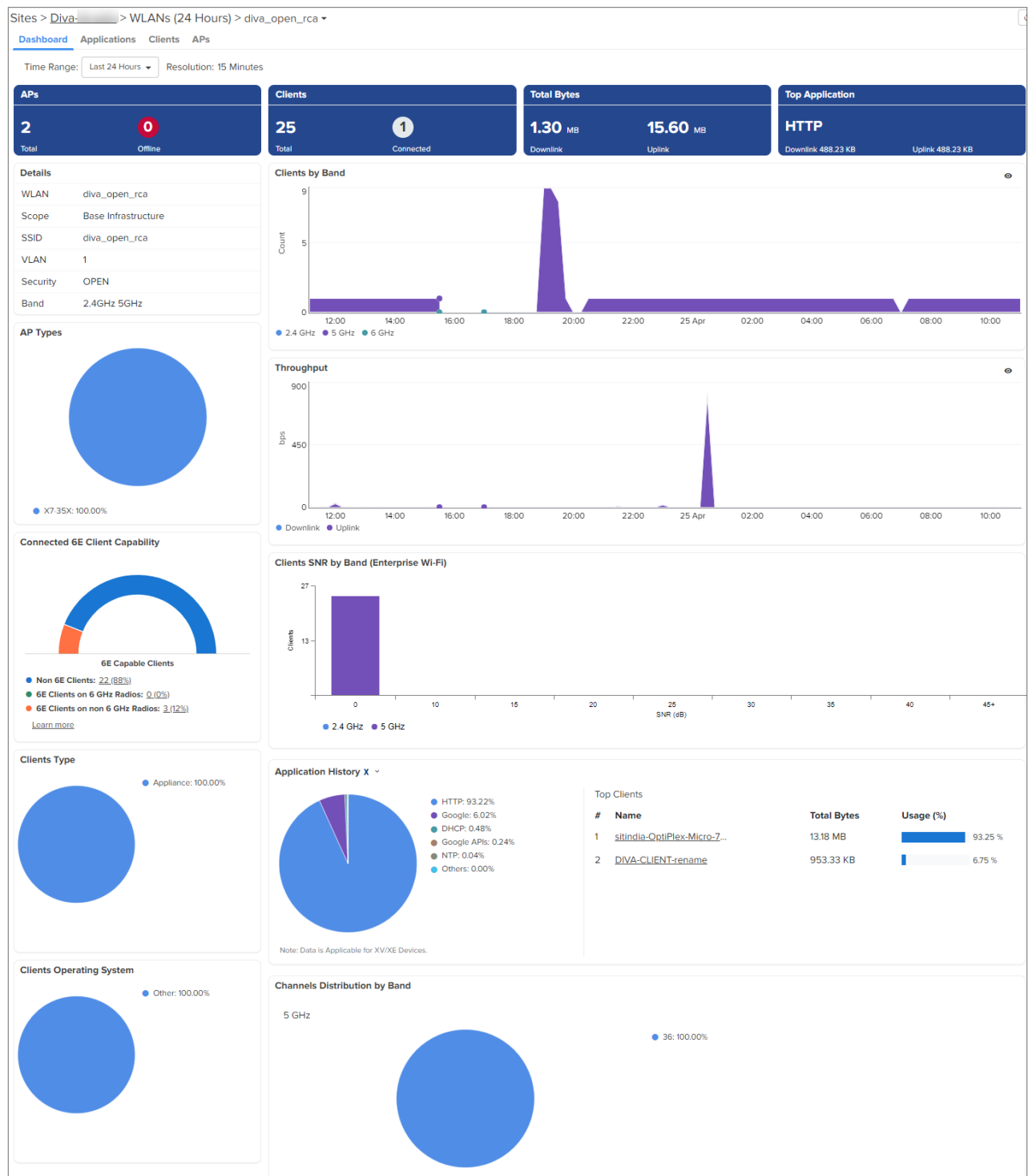
The WLANs data is available for the following durations:

- **Last 5 minutes**—Includes the most recent WLANs data (active clients and data traffic) for the last five minutes.
- **24 hours**—Includes WLAN data aggregated every 15 minutes for the last 24 hours. This may include details of any active clients that are still connected to the APs.
- **7 days**—Includes WLAN data that is aggregated every 1 hour for the last seven days.
- Click a WLAN in the WLANs page to view the WLAN-specific dashboard.

You can view the data for last 24 hours or seven days by selecting the option from the **Time Range** dropdown list.

- The dashboard displays the following data:
 - Details
 - AP Types
 - Connected 6E Client Capability
 - Client Type
 - Client Operating System
 - Clients By Band
 - Throughput
 - Clients SNR By Band (Enterprise (Wi-Fi))
 - Application History^X
 - Channels Distribution By Band

Figure 227 WLAN-specific Dashboard



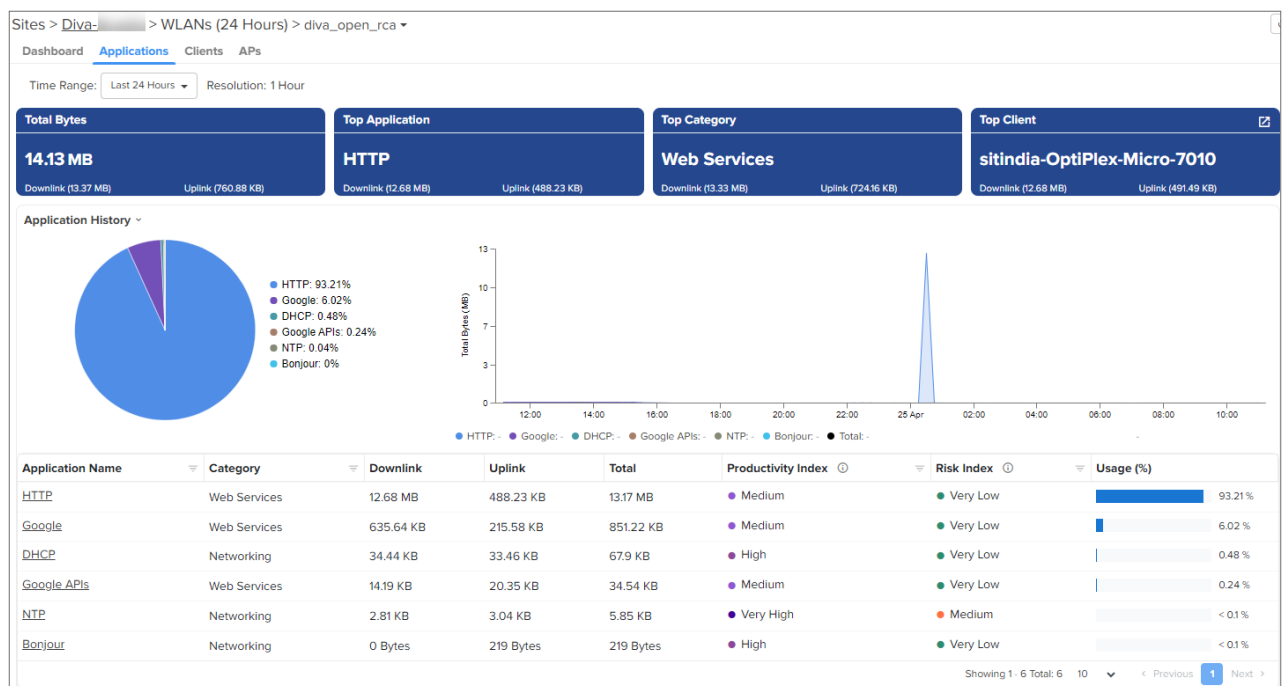
- To view the details of the applications accessed through this WLAN, click the **Monitor and Manage** > **<Site-Name>** > **WLANs^X** > **<WLAN-Name>** > **Applications** tab.

The **Applications** dashboard displays both a graphical data and details in a table with the following fields:

Table 58 *Application fields*

Field	Description
Application Name	Name of the application.
Category	Category of the application.
Downlink	Total number of downlink bytes during the period selected.
Uplink	Total number of uplink bytes during the period selected.
Total	Total amount of application data (uplink plus downlink).
Productivity Index	<p>Estimate of the typical productivity of the application.</p> <p>Following are the supported values:</p> <ul style="list-style-type: none"> • Very Low • Low • Medium • High • Very High
Risk Index	<p>Estimate of the typical security risk of the application.</p> <p>Following are the supported values:</p> <ul style="list-style-type: none"> • Very Low • Low • Medium • High • Very High
Usage (%)	Percentage of usage by this application in comparison to all applications.

Figure 228 *WLAN-specific Application Dashboard*



- To view information about clients connected to the selected WLAN in the site, click the **Monitor and Manage** > **<Site-Name>** > **WLANs^X** > **<WLAN-Name>** > **Clients** tab.

The **Clients** dashboard displays information, such as the hostname of the client, AP to which client was connected, operating system, and radio capabilities.

Figure 229 WLAN-specific Clients Dashboard

Host Name	User	AP	IPv4 Address	IPv6 Address	MAC Address	VLAN-ID	Manufacturer	OS	Capabilities	Band	Status
DivA-CLIENT-rename		X7-35X-B0023A	10.50.25.52	N/A		215	CLOUD NETWORK TE...	Other	axa	5 GHz	Disconnected
		X7-35X-B0023A	0.0.0.0	N/A		215	Intel Corporate		ac	5 GHz	Disconnected
	sitindia	X7-35X-B0023A	0.0.0.0	N/A		215	Intel Corporate		ac	5 GHz	Disconnected
		X7-35X-B0023A	0.0.0.0	N/A		315	Intel Corporate		ac	5 GHz	Disconnected
	sitindia	X7-35X-B0023A	0.0.0.0	N/A		415	Intel Corporate		ac	5 GHz	Disconnected
		X7-35X-B0023A	0.0.0.0	N/A		315	Intel Corporate		ac	5 GHz	Disconnected
		X7-35X-B0023A	0.0.0.0	N/A		315	Intel Corporate		ac	5 GHz	Disconnected
sitindia-OptiPlex-Micro-7010		X7-35X-B0023A	0.0.0.0	N/A		315	Intel Corporate	Other	6E	5 GHz	Disconnected
sitindia-OptiPlex-Micro-7010		X7-35X-B0023A	192.168.210.30	N/A		1	Intel Corporate	Other	6E	5 GHz	Connected
sitindia-OptiPlex-Micro-7010		X7-35X-B0023A	0.0.0.0	N/A		315	Intel Corporate	Other	6E	5 GHz	Disconnected

- To view information about the APs that are associated with the selected WLAN, click the **Monitor and Manage** > **<Site-Name>** > **WLANs^X** > **<WLAN-Name>** > **APs** tab.

The **APs** dashboard displays APs information, such as the device name, MAC address, the AP model, and the data usage..

Figure 230 WLAN-specific APs Dashboard

Device	MAC Address	Type	IPv4 Address	IPv6 Address	Status	Serial Number	Downlink Usage	Uplink Usage
X7-35X-B001A4		X7-35X	192.168.210.61	N/A	Online		0	0
X7-35X-B0023A		X7-35X	192.168.210.62	N/A	Online		1.3 MB	15.6 MB

Fiber OLT and ONU

The Fiber Optical Line Terminal (OLT) from Cambium Networks is a Passive Optical Network (PON) device that connects to a core switch using either an Ethernet cable or a fiber cable. It supports Gigabit Passive Optical Network (GPON), 10 Gigabit Symmetrical PON (XGS-PON), and combo-PON (GPON co-existing with XGS-PON) Optical Defined Networking (ODN) access. The Fiber OLT is available in 8 and 16 ports, including All-in-One (AIO) PON interfaces, allowing simultaneous support for multiple PON technologies. It is used for network development with GPON and User Network Interface (UNI) ports. The high-performance access design of the Fiber OLT focuses on Software-Defined Networking (SDN) deployments, providing open interfaces to all control management functions for seamless integration with SDN environments.

cnMaestro provides management, configuration, and monitoring services for Fiber OLT. It includes the following pages for Fiber OLT and ONU, providing comprehensive tools for efficient management and optimization:

- [Dashboard](#)
- [Notifications](#)

- [Configuration](#)
- [Details](#)
- [Performance](#)
- [ONU](#)
- [Ports](#)
- [Software Update](#)

Dashboard

Displays the monitoring information of the OLT.

Figure 231 Fiber OLT dashboard



Dashboard has the following elements:

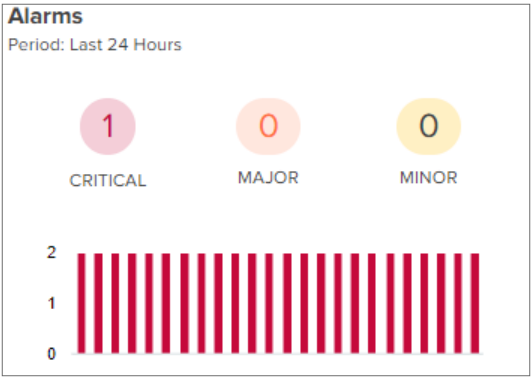
- [Alarms](#)
- [Port Status](#)
- [ONU by Signal Level](#)
- [ONU by Signal Level per Port](#)
- [ONUs](#)
- [PON Downlink Utilization](#)
- [PON Downlink throughput](#)

- [PON Uplink throughput](#)
- [Ethernet Downlink throughput](#)
- [Ethernet Uplink throughput](#)

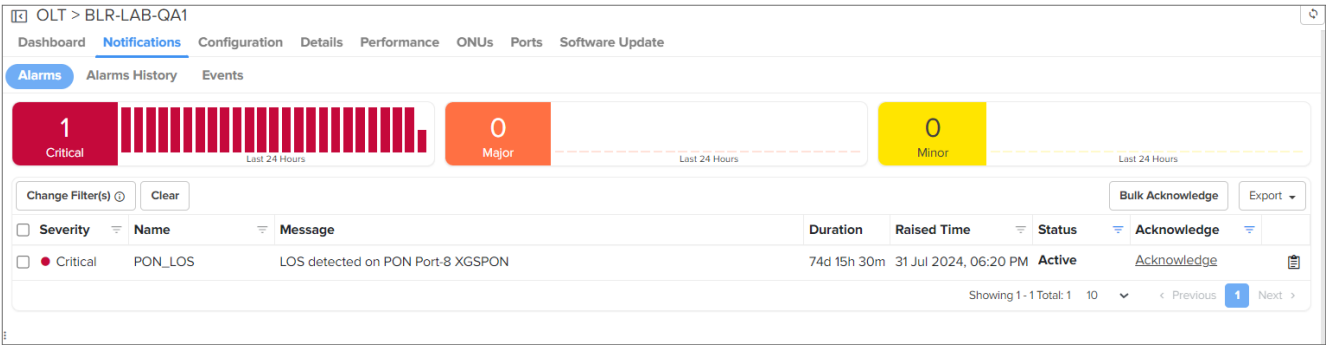
Alarms

Displays the critical, major, and minor alarms. [Figure 232](#) shows the status of the alarms.

Figure 232 Alarms



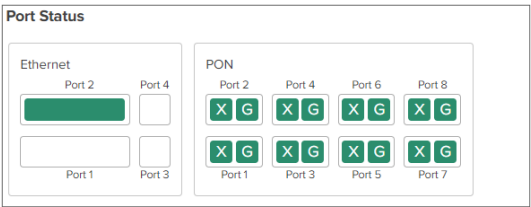
To view the detailed information, click on the respective alarm count.



Port Status

Displays the connection status for Network-to-Network Interface (NNI) or Ethernet (uplink) ports and PON ports (downlink). Small Form-Factor Pluggable (SFP) devices are connected to the Ethernet ports, and ONUs are connected to the PON ports. The uplink NNI has four ports. Port 1 and port 2 support 100 Gbps speed. Port 3 and port 4 support 10 Gbps speed. There are 16 downlink PON ports, with each port supporting both GPON and XGSPON.

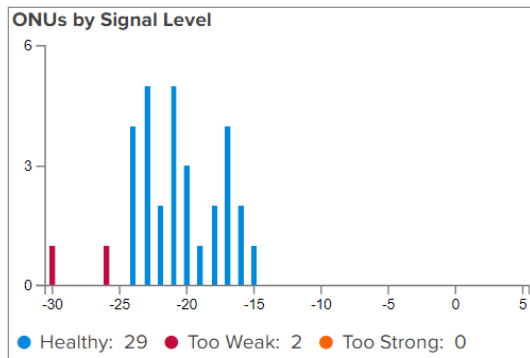
Figure 233 Port status



ONU by Signal Level

Displays the signal level received by the ONU.

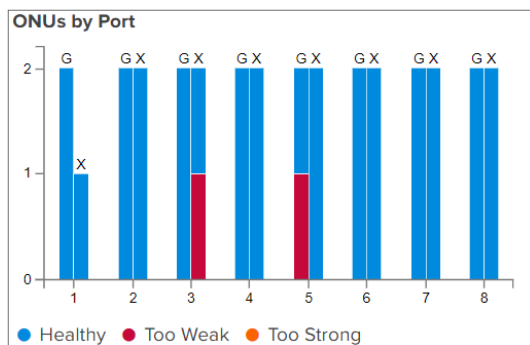
Figure 234 ONU by signal level graph



ONU by Signal Level per Port

Displays the number of ONU connected and their corresponding power levels.

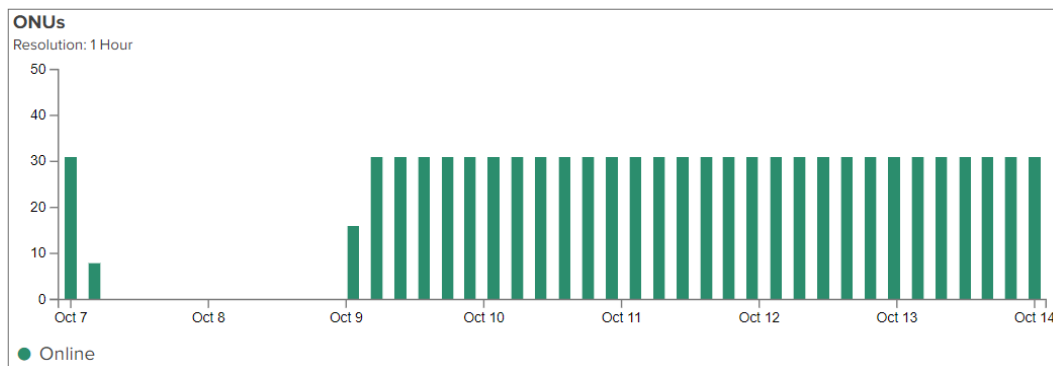
Figure 235 ONU by signal level per port



ONUs

Displays the number of ONUs connected to the OLT.

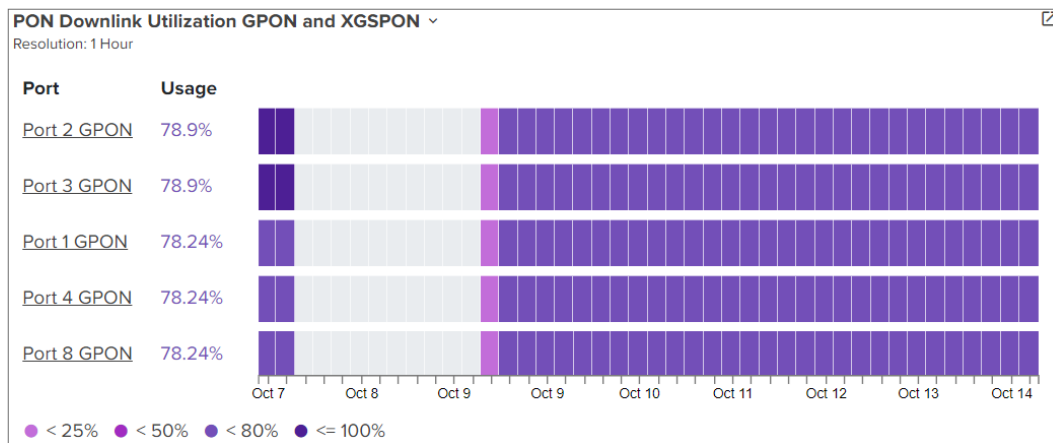
Figure 236 ONU



PON Downlink Utilization

Displays the utilization of GPON and XGS-PON.

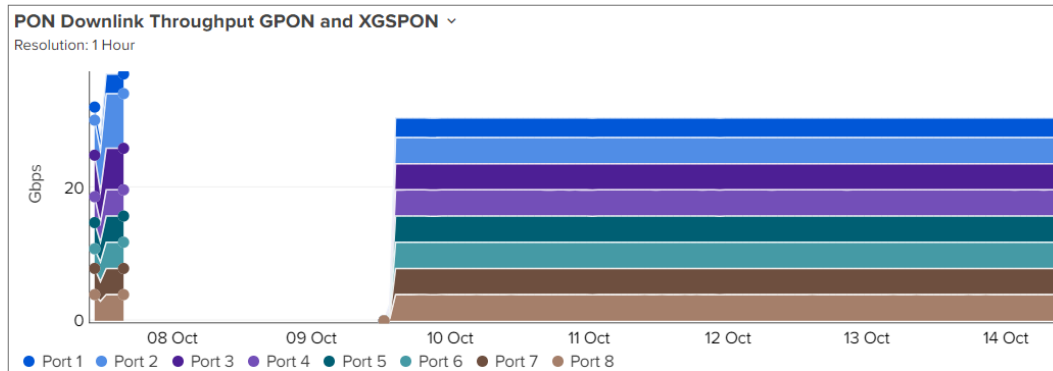
Figure 237 PON Downlink Utilization



PON Downlink Throughput

PON Downlink throughput displays the downlink throughput information of GPON and XGS-PON.

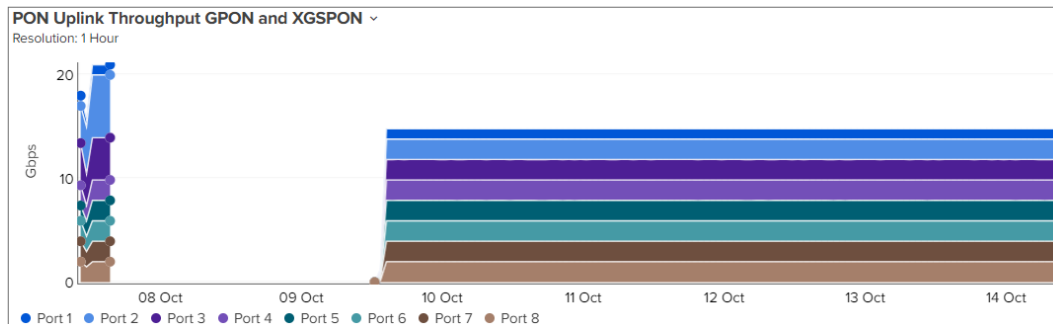
Figure 238 PON Downlink Throughput



PON Uplink Throughput

Displays the uplink throughput information of GPON and XGS-PON.

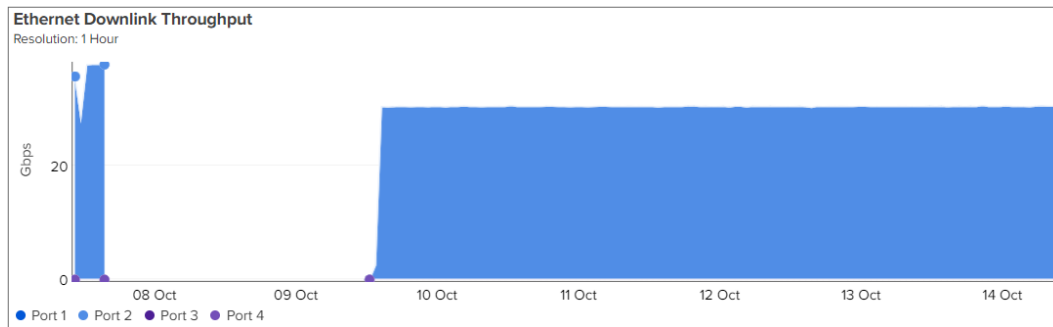
Figure 239 PON Uplink Throughput



Ethernet Downlink Throughput

Displays the Ethernet Downlink information of GPON and XGS-PON.

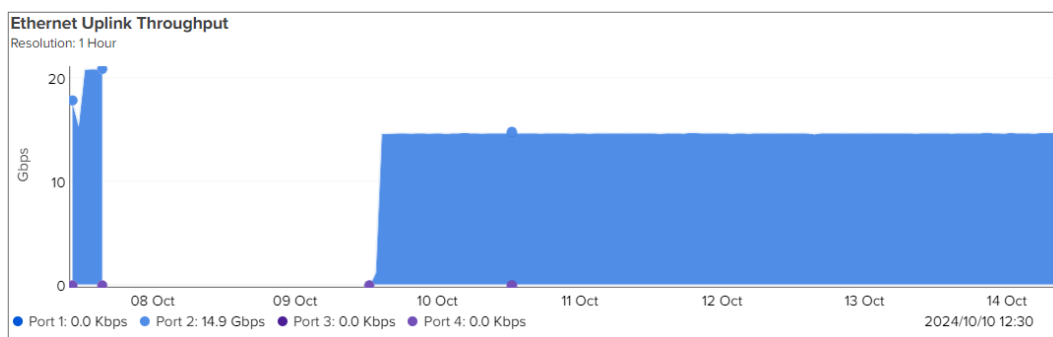
Figure 240 Ethernet Downlink throughput



Ethernet Uplink Throughput

Displays the Ethernet Uplink information of GPON and XGS-PON.

Figure 241 Ethernet Uplink Throughput



Notifications

Displays the alarm information of the OLT.

Figure 242 Notifications

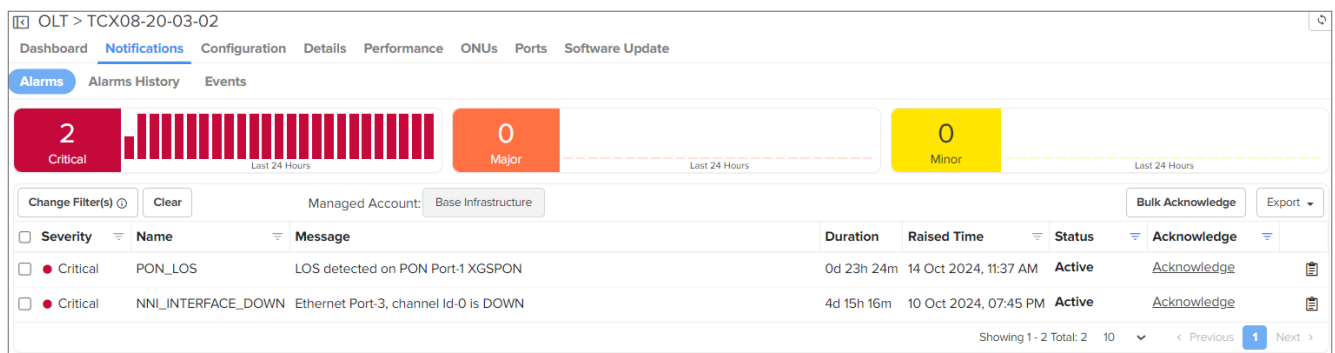


Table 59 Parameters on the Notifications page

Parameter	Description
Severity	Severity level of the alarm. This parameter supports the following severity levels: <ul style="list-style-type: none"> Critical Major Minor

Parameter	Description
Source	Name of the OLT.
Mode	Type of the device. The following device types are supported: <ul style="list-style-type: none"> • OLT • ONU
Source MAC	MAC address of the OLT.
IPv4 address	IPv4 address of the OLT.
Name	Name of the ONU.
Message	A brief description of the alarm message.
Duration	Duration of the alarm.
Status	Status of the alarm. The following status values are supported: <ul style="list-style-type: none"> • Active • Inactive
Raised Time	Time when the alarm was raised.

Configuration

Users can configure the OLT using the Configuration tab. To sync the configuration with the E2E network, from the tree menu, click the **Actions** (⚙️) icon corresponding to the OLT device and select **Sync Topology**

Figure 243 Configuration

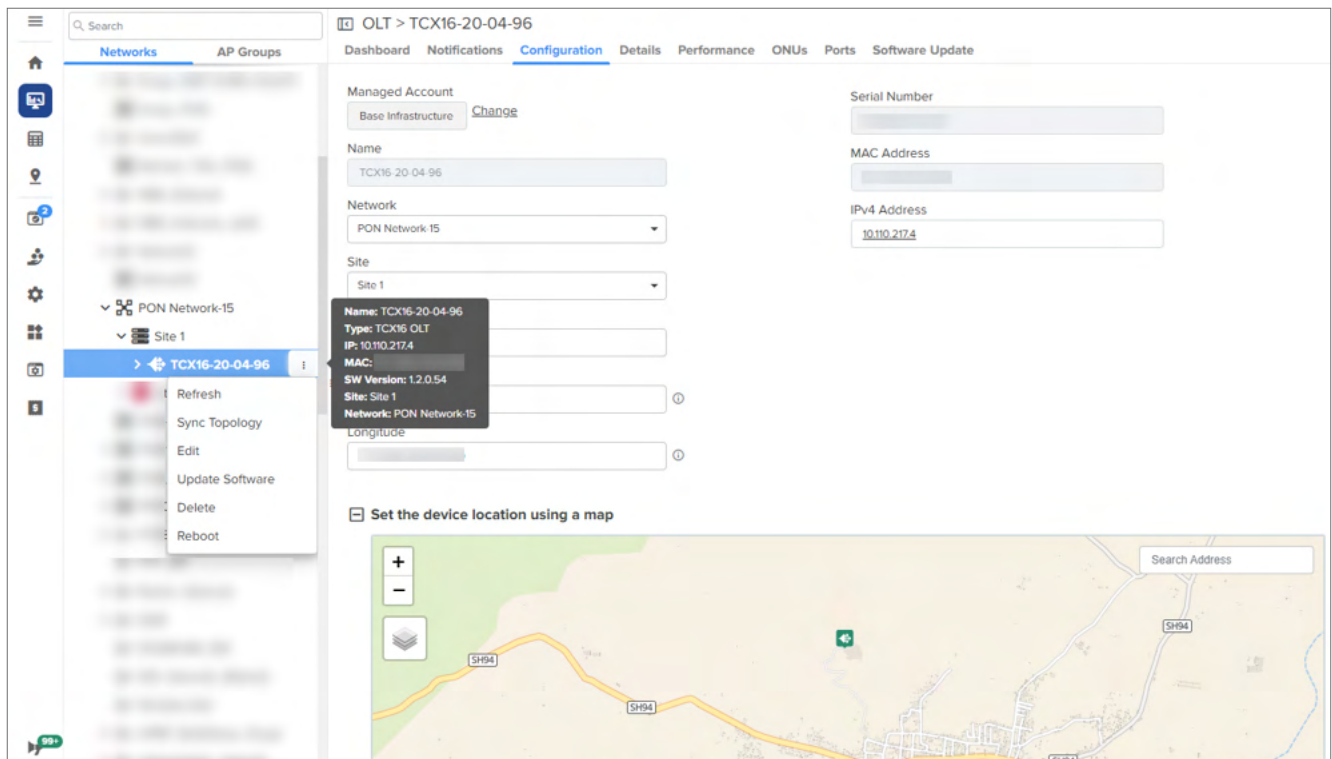


Table 60 Parameters on the Configuration page

Parameter	Description
Managed Account	Name of the site where OLT is configured.
Name	Name of the OLT.
Network	Name of the network where OLT is configured.
Site	Name of the site.
Description	A brief description of the OLT.
Latitude	Latitude of the OLT.
Longitude	Longitude of the OLT.
Serial Number	Serial Number (MSN) of the OLT.
MAC Address	MAC Address of the OLT.
IPv4 Address	IPv4 Address of the OLT.

Details

The Details page displays general configuration and runtime information of the OLT.

Figure 244 Details

Search

NetworksAP Groups

System

- default
- BLR-QA
 - TCX08-20-01-31
 - TCX08-20-09-94

OLT > TCX08-20-09-94

DashboardNotificationsConfigurationDetailsPerformanceONUsPortsSoftware Update

System

Device NameTCX08-20-09-94

Device TypeTCX08 OLT

System Uptime0d 13h 34m

Session Time0d 13h 30m

Coordinates0,0

Software Version11.0-RC21

DA Version2.105.48

Onboard DateNov 08 2023 12:25:32

Description

Software Update

Active Software Version11.0-RC21

Inactive Software VersionN/A

History

DateStatusVersion

09 Nov 2023, 08:06 PMSuccess11.0-RC20

Network

MAC Address

IP Address10.110.217.7

Subnet Mask255.255.255.0

Gateway10.110.217.254

Primary DNS Server10.110.12.110

Secondary DNS Server10.110.12.111

Table 61 Parameters on the Details page

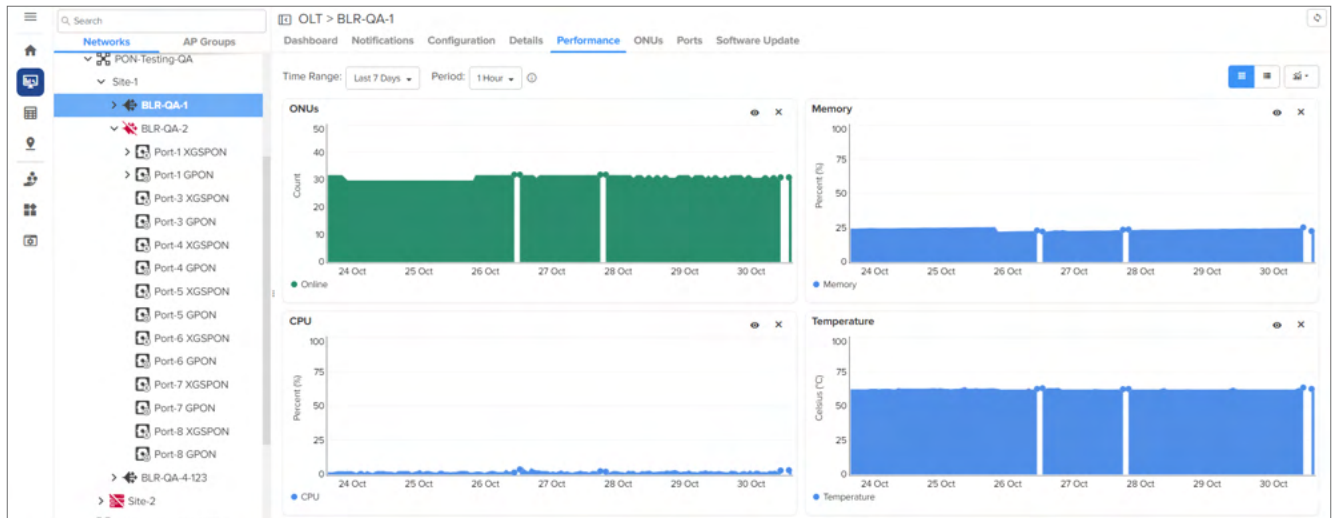
Parameter	Description
System	
Device Name	Name of the device.
Device Type	Type of the device. This parameter supports the following device types: <ul style="list-style-type: none"> OLT ONU
System Uptime	Date and time configured for the device.

Parameter	Description
Session Time	Duration of the session.
Coordinates	Latitude and longitude.
Software Version	The current software version used.
DA Version	Version of the device agent (DA).
Onboard Date	Onboard date of the device.
Description	A brief user-defined description of the onboarded device.
Software Update	
Active Software Version	Version of the active software.
Inactive Software Version	Version of the inactive software.
History	History of software version updates.
Network	
MAC Address	MAC Address of the device.
IP Address	IP Address of the device.
Subnet Mask	Subnet Mask of the device.
Gateway	Gateway address of the device.
Primary DNS Server	IP address of the primary DNS server.
Secondary DNS Server	IP address of the secondary DNS server.

Performance

Displays the performance graphs for ONU, CPU, memory, and temperature of the OLT and ONU.

Figure 245 Performance



ONU

Displays the number of ONUs connected to the OLT and their information.

Figure 246 ONU

Name	MAC Address	Status	Connection Time	ONU ID	OLT Rx Power
XGS-PON ONU Port 7	00:13:25:00:00:01	Online	8d 15h 0m	1	-23 dBm
XGS-PON ONU Port 7	B8:FF:B3:12:30:31	Online	8d 15h 0m	2	-22.4 dBm

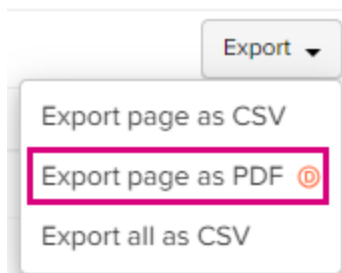
Table 62 Parameters on the ONU page

Parameter	Description
Name	Name of the OLT. Click the Name to view the ONU-specific Dashboard page as shown in Figure 249 .
MAC Address	MAC address of the OLT.
Status	Status of the OLT.
OLT Port	Port number of the OLT to which ONU is connected.
Connection Time	Time during which ONU is connected to OLT.
ONU ID	ID of the ONU.
OLT Rx Power	Receive power of the OLT.

Export ONUs

Perform the following steps to export the ONUs table:

1. Click **Export**. A dialogue box appears.

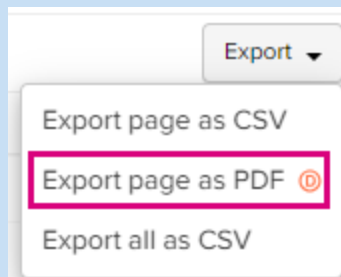


2. Select **Export page as CSV/all as CSV** and export the file.



Note

The **Export page as PDF** option is deprecated from cnMaestro release version 5.2.0 onwards. This option will be completely removed from the UI in release version 5.3.0.



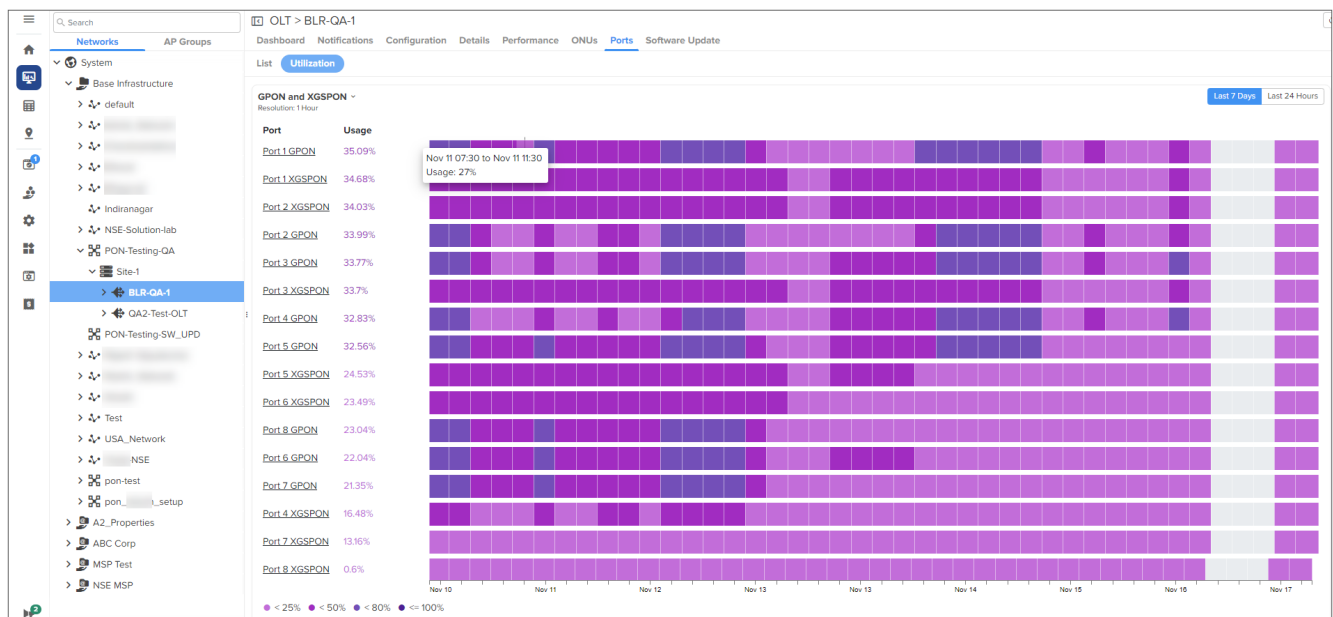
Ports

Displays the port details. Fiber OLT has 8 ports and 16 ports.

Figure 247 Ports

OLT > BLR-LAB-QA1							
Dashboard Notifications Configuration Details Performance ONUs Ports Software Update							
List Utilization							
Apply Filter(s)							
Port	Type	Status	Online ONUs	Temperature	Rx Power	PON Downlink Utilization	
1	XGSPON	Up	1	52.9 °C	-18.6 dBm	<div></div>	9 %
1	GPON	Up	2	52.9 °C	-23.2 dBm	<div></div>	79 %
2	XGSPON	Up	2	54.7 °C	-19.3 dBm	<div></div>	19 %
2	GPON	Up	2	54.7 °C	-20.7 dBm	<div></div>	79 %
3	XGSPON	Up	2	54.4 °C	-25.8 dBm	<div></div>	19 %
3	GPON	Up	2	54.5 °C	-22.4 dBm	<div></div>	79 %
4	XGSPON	Up	2	55.8 °C	-15.1 dBm	<div></div>	19 %
4	GPON	Up	2	55.8 °C	-21.3 dBm	<div></div>	79 %
5	XGSPON	Up	2	51.8 °C	-16.4 dBm	<div></div>	19 %
5	GPON	Up	2	51.8 °C	-21 dBm	<div></div>	79 %
Showing 1 - 10 Total: 16 10 < Previous 1 2 Next >							

Figure 248 Ports utilization



To filter selected ports, perform the following steps:

1. Click **Apply Filter(s)**, type the port name.
2. Select the type of the OLT.
3. Select the status of the OLT and click **Apply Filter(s)**.

Filters [X]

Port

Type
☐ XGSPON ☐ GPON

Status
☐ Down ☐ Up

Apply Filter(s) **Reset**

Table 63 *Parameters on the Ports page*

Parameter	Description
Port	Port number of the OLT.
Type	Type of the PON.
Status	Status of the ONU.
Online ONU	Number of ONUs online.
Temperature	Temperature of the ONU.
Rx Power	Receive power of the ONU.
PON Downlink Utilization	Utilization percentage of the PON Downlink.

Software Update

Users can upgrade the OLT and ONU firmware using the **Software Update** page.

OLT Software Update

To upgrade the software, perform the following steps:

1. Download the latest firmware from [Cambium Networks Support Site](#).
2. Navigate the **Monitor and Manage** > <Site-Name> > **OLT** > **Software Update** tab.
The Software Update page appears.
3. Select **OLT**.
4. Select the **Versions** from the dropdown list.
5. Select **Update Now** to apply immediately or **Schedule** to upgrade later.
6. Click **Add Software Job** to upload the latest firmware file.
7. Once the firmware file is uploaded, the software update job is added to the list of update jobs.

OLT > TCX08-20-03-02

Dashboard Notifications Configuration Details Performance ONUs Ports **Software Update**

OLT **ONU**

Versions
111 (Recommended)

Update
☒ Now ☐ Schedule

Job Options

Notes

Add Software Job **View Update Jobs**

Name

Type

Status
Online

Active
12.0-RC13

Inactive

Click **View Update Jobs** to view the history of the software updates. This provides a record of all previous software update jobs.

ONU Software Update



Note

The ONU software update is applicable only when the OLT software is upgraded to version 1.2.0 or higher.

To upgrade the software for ONU, perform the following steps:

1. Download the latest firmware from [Cambium Networks Support Site](#).
2. Navigate the **Monitor and Manage** > <Site-Name> > **OLT** > **Software Update** tab.
The Software Update page appears.
3. Select **ONU**.
4. Select the **Versions** from the dropdown list.
5. Select the **Hardware Type**.
6. Select the **Devices** from the list.
7. Select **Update Now** to apply immediately or **Schedule** to upgrade later.
8. Click **Add Software Job** to upload the latest firmware file.
9. Once the firmware file is uploaded, the software update job is added to the list of update jobs.

The screenshot shows the 'Software Update' page for an ONU. At the top, there's a breadcrumb trail: OLT > TCX08-20-03-02 > Dashboard > Notifications > Configuration > Details > Performance > ONUs > Ports > Software Update. Below this, there's a tab bar with 'OLT' and 'ONU' (selected). The 'Versions' dropdown is set to '1.1 (Recommended)'. The 'Hardware Type' section has 'XGSPON' selected and 'GPON' unselected. A search bar and 'Managed Account: Base Infrastructure' are visible. Below this is a table with columns: Devices, OLT Port, Status, and Running Version. The table shows two devices, both with 'Port 1' as the OLT Port, 'Online' status, and '1.2.0-RC13' as the Running Version. At the bottom, there's an 'Update' section with 'Now' selected and 'Schedule' unselected. Below that is a 'Job Options' section with a 'Notes' text area. At the very bottom, there's a blue button 'Add Software Job to 0 device(s)' and a link 'View Update Jobs'.

Click **View Update Jobs** to view the history of the software updates. This provides a record of all previous software update jobs.

ONU Dashboard



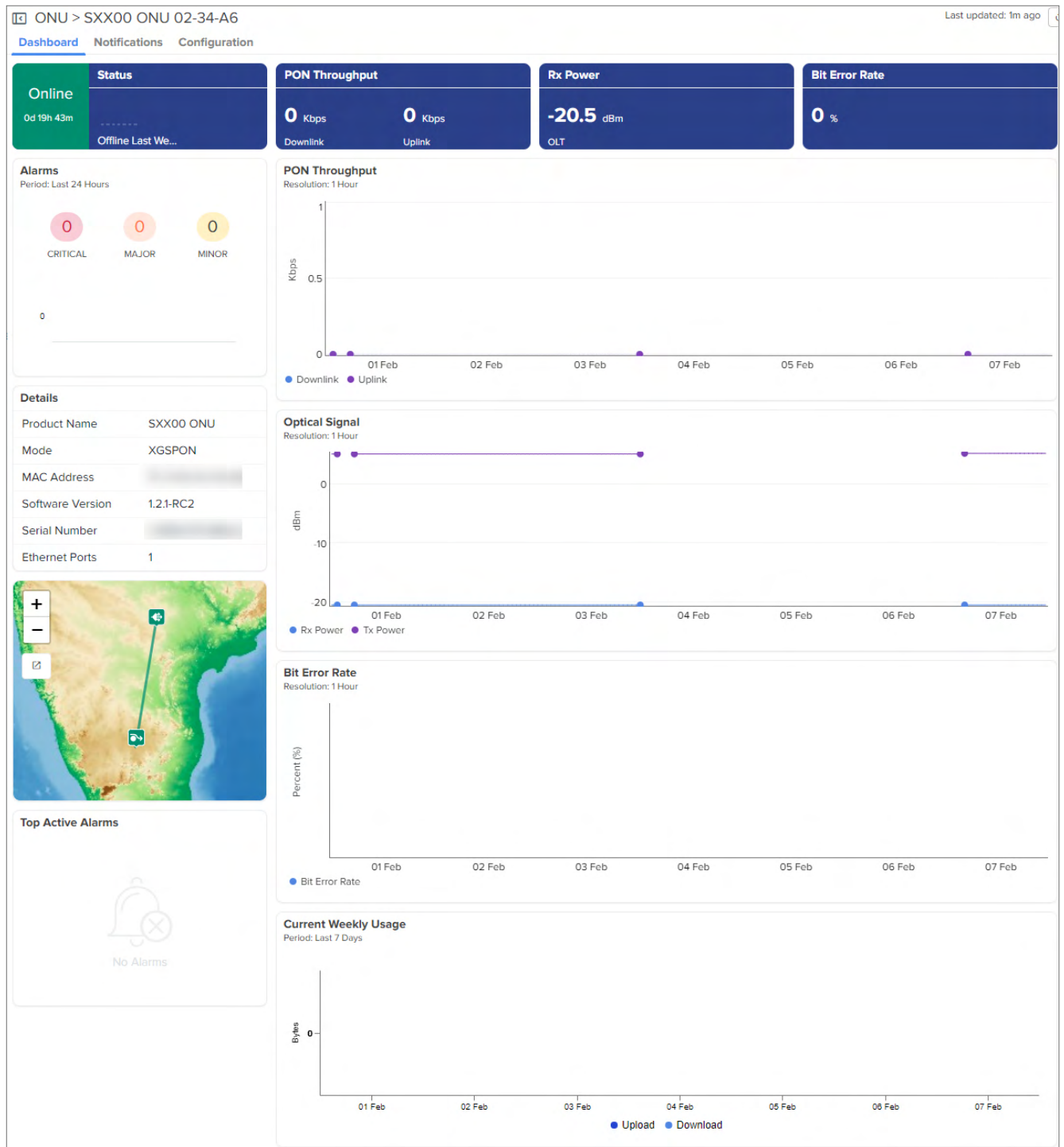
Note

The ONU dashboard displays map data only when latitude and longitude are configured.

The dashboard displays the following data:

- Alarms
- Bit Error Rate
- Current Weekly Usage
- Details
- Optical Signal
- PON Throughput
- Rx Power
- Status
- Top Active Alarms

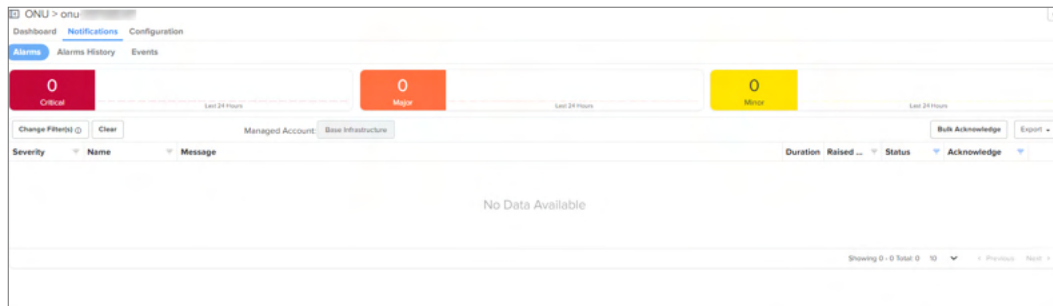
Figure 249 ONU Dashboard



To view information about notifications connected to the selected ONU in the site, click the **Monitor and Manage** > **<Site-Name> > OLT > PON Port > ONU > <ONU-Name> > Notifications** tab..

The Notification tab displays ONUs information, such as the Alarms, Alarms History, and Events.

Figure 250 ONU Notifications



To view and configure the information about the selected ONU in the site, click the **Monitor and Manage** > **<Site-Name>** > **OLT** > **PON Port** > **ONU** > **<ONU-Name>** > **Configuration** tab.

To configure the ONU, perform the following steps:

1. Enter **Description**.
2. Enter **Latitude**.
3. Enter **Longitude**.
4. Click **Apply Configuration**.

Figure 251 ONU Configuration

Table 64 Parameters on the Configuration page

Parameter	Description
Name	Displays the name of the ONU.
Description	A brief description of the ONU.
Latitude	Latitude of the ONU.
Longitude	Longitude of the OLT.
Serial Number	Serial Number (MSN) of the ONU.
MAC Address	MAC Address of the ONU.

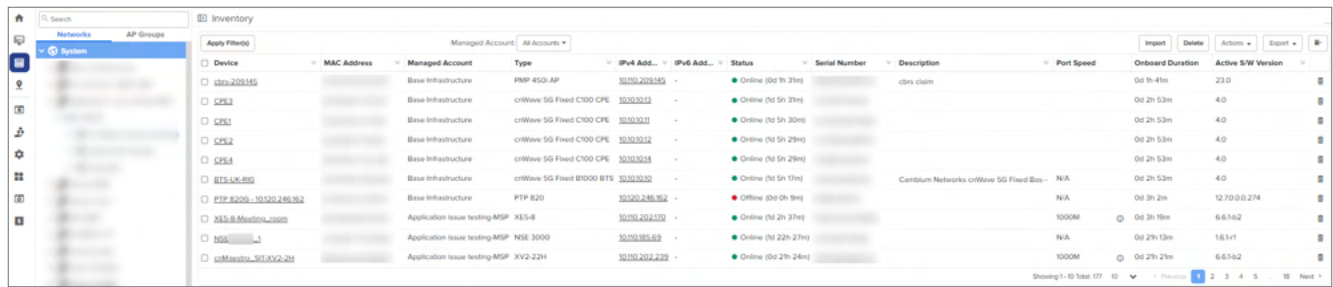
Inventory

The Inventory page displays a list of devices under the selected Node. It presents health and maintenance information in a tabular view that allows for sorting and filtering. When selected for a single device, it presents a

detailed customized page of that device.

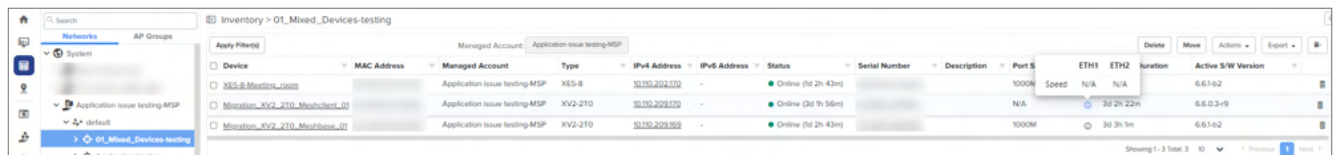
Navigate to the **Inventory** tab on the left pane.

Figure 252 Inventory page at the System-level



Device	MAC Address	Managed Account	Type	IPv4 Address	IPv6 Address	Status	Serial Number	Description	Port Speed	Onboard Duration	Active S/W Version
ctm-209145		Base Infrastructure	PMF 450 AP	10.10.209.145	-	Online (0d 1h 31m)		ctm claim		0d 1h 41m	23.0
CP51		Base Infrastructure	cnWave 5G Fixed C100 CPE	10.10.30.1	-	Online (1d 5h 31m)				0d 2h 53m	4.0
CP51		Base Infrastructure	cnWave 5G Fixed C100 CPE	10.10.30.1	-	Online (1d 5h 30m)				0d 2h 53m	4.0
CP52		Base Infrastructure	cnWave 5G Fixed C100 CPE	10.10.30.2	-	Online (1d 5h 29m)				0d 2h 53m	4.0
CP52		Base Infrastructure	cnWave 5G Fixed C100 CPE	10.10.30.2	-	Online (1d 5h 29m)				0d 2h 53m	4.0
RTS-LK-850		Base Infrastructure	cnWave 5G Fixed B1000 BTS	10.10.30.30	-	Online (1d 5h 13m)		Cambium Networks cnWave 5G Fixed Bas...	N/A	0d 2h 53m	4.0
PTP 8200 - 10.120.246.902		Base Infrastructure	PTP 820	10.120.246.902	-	Offline (0d 0h 1m)			N/A	0d 3h 2m	12.70.0.0.274
XIS-8-Mission-test		Application issue testing-MSP	XIS-8	10.10.202.229	-	Online (1d 2h 37m)			1000M	0d 3h 19m	6.6.1-62
NSE		Application issue testing-MSP	NSE 3000	10.10.195.63	-	Online (1d 22h 27m)			N/A	0d 2h 13m	16.1-1
cnMaestro_SIT_XV2-201		Application issue testing-MSP	XV2-22H	10.10.202.229	-	Online (0d 27h 24m)			1000M	0d 27h 2m	6.6.1-62

Figure 253 Inventory page at the Site-level



Device	MAC Address	Managed Account	Type	IPv4 Address	IPv6 Address	Status	Serial Number	Description	Port S	ETH1	ETH2	Duration	Active S/W Version
XIS-8-Mission-test		Application issue testing-MSP	XIS-8	10.10.202.229	-	Online (1d 2h 43m)			1000M	Speed	N/A	N/A	6.6.1-62
Mission_XV2-270_MuchMore-01		Application issue testing-MSP	XV2-270	10.10.209.170	-	Online (3d 1h 56m)			N/A			3d 2h 22m	6.6.0.3-r9
Mission_XV2-270_MuchMore-01		Application issue testing-MSP	XV2-270	10.10.209.160	-	Online (1d 2h 43m)			1000M			3d 3h 1m	6.6.1-62



Note

The **Port Speed** column displays the port speed (in Mbps) for the Enterprise Wi-Fi devices only.

- At the System-level, you can enable the **Port Speed** column by selecting the **Port Speed** checkbox from the Column selector (🔍).
- At the Site-level, the **Port Speed** column is displayed by default.

Inventory Export



Note

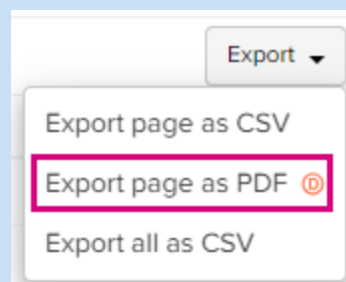
Inventory export is supported for PON devices starting from version 5.2.1.

The inventory table can be exported in the CSV format. The values exported will match those in the selected table columns. You can customize the health and maintenance views to add or delete columns.



Note

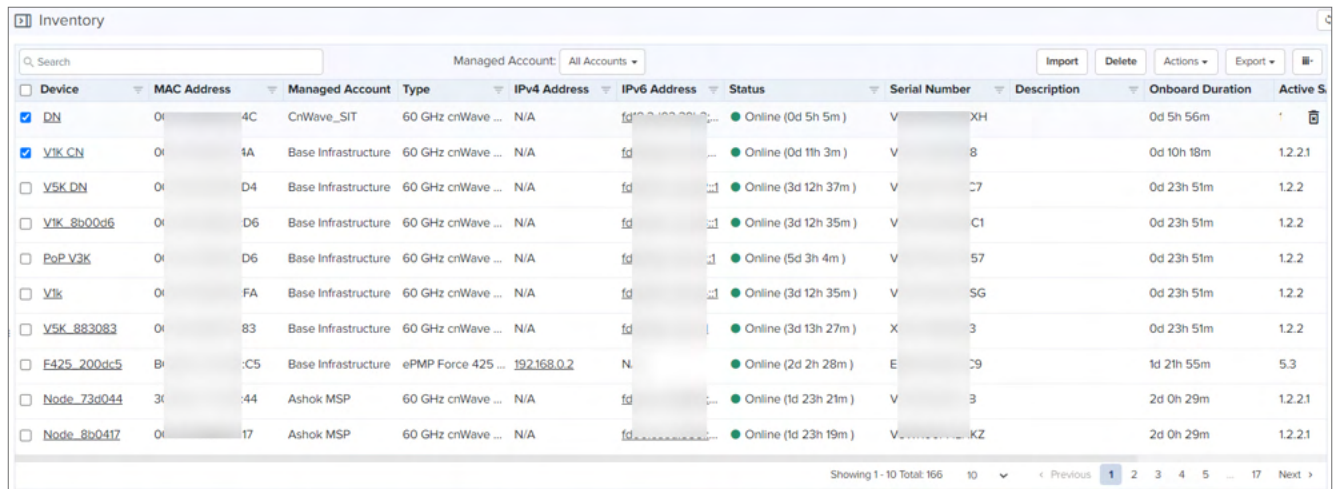
The **Export page as PDF** option is deprecated from cnMaestro release version 5.2.0 onwards. This option will be completely removed from the UI in release version 5.3.0.



Bulk Delete

The **Bulk Delete** option is available in the inventory page of System/MSP/Tower/Network/Site.

Figure 254 Bulk Delete



Device	MAC Address	Managed Account	Type	IPv4 Address	IPv6 Address	Status	Serial Number	Description	Onboard Duration	Active S
<input checked="" type="checkbox"/> DN	01:00:00:00:00:00	4C	CnWave_SIT	60 GHz cnWave ...	N/A	Online (0d 5h 5m)	V5...	XH	0d 5h 56m	1.2.2.1
<input checked="" type="checkbox"/> VIK_CN	01:00:00:00:00:00	4A	Base Infrastructure	60 GHz cnWave ...	N/A	Online (0d 11h 3m)	V5...	8	0d 10h 18m	1.2.2.1
<input type="checkbox"/> V5K_DN	01:00:00:00:00:00	D4	Base Infrastructure	60 GHz cnWave ...	N/A	Online (3d 12h 37m)	V5...	C7	0d 23h 51m	1.2.2
<input type="checkbox"/> VIK_8b00d6	01:00:00:00:00:00	D6	Base Infrastructure	60 GHz cnWave ...	N/A	Online (3d 12h 35m)	V5...	C1	0d 23h 51m	1.2.2
<input type="checkbox"/> PoP_V3K	01:00:00:00:00:00	D6	Base Infrastructure	60 GHz cnWave ...	N/A	Online (5d 3h 4m)	V5...	57	0d 23h 51m	1.2.2
<input type="checkbox"/> VIK	01:00:00:00:00:00	FA	Base Infrastructure	60 GHz cnWave ...	N/A	Online (3d 12h 35m)	V5...	SG	0d 23h 51m	1.2.2
<input type="checkbox"/> V5K_883083	01:00:00:00:00:00	83	Base Infrastructure	60 GHz cnWave ...	N/A	Online (3d 13h 27m)	X1C...	3	0d 23h 51m	1.2.2
<input type="checkbox"/> F425_200dc5	B1:00:00:00:00:00	C5	Base Infrastructure	ePMP Force 425 ...	192.168.0.2	Online (2d 2h 28m)	E8...	C9	1d 21h 55m	5.3
<input type="checkbox"/> Node_73d044	31:00:00:00:00:00	44	Ashok MSP	60 GHz cnWave ...	N/A	Online (1d 23h 21m)	V5...	B	2d 0h 29m	1.2.2.1
<input type="checkbox"/> Node_8b0417	01:00:00:00:00:00	17	Ashok MSP	60 GHz cnWave ...	N/A	Online (1d 23h 19m)	V5...	KZ	2d 0h 29m	1.2.2.1

To delete devices using bulk delete, perform the following steps:

1. Navigate to the **Inventory** page of System/MSP/Network/Tower/Site.
2. Select one or multiple devices by selecting the corresponding checkboxes.
3. Click the **Delete** button.

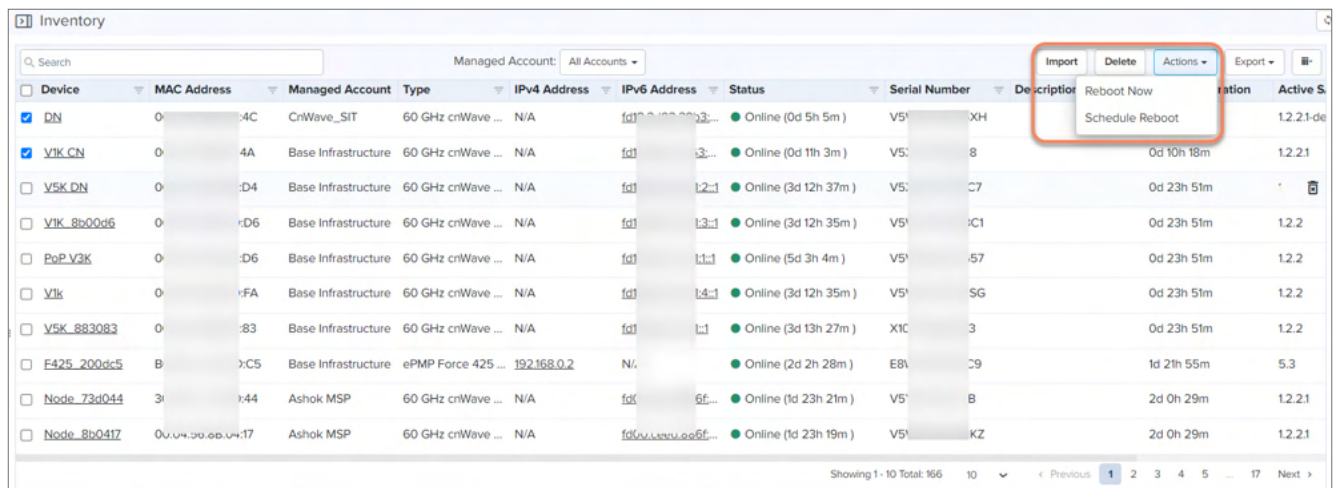
After deleting devices in bulk, you can view the status in the **Administration > Jobs > Actions** page.

For more information about deleting devices in bulk, see [Deleting Devices in Bulk](#).

Bulk Reboot

The **Bulk Reboot** option is available on the inventory page of Tower/Network/Site. When the devices are rebooted using Bulk Reboot, all the Network/Tower/Site Dashboards, Graphs, Clients, Reports, and Mesh Peers will be updated accordingly.

Figure 255 Bulk Reboot



Device	MAC Address	Managed Account	Type	IPv4 Address	IPv6 Address	Status	Serial Number	Description	Onboard Duration	Active S
<input checked="" type="checkbox"/> DN	01:00:00:00:00:00	4C	CnWave_SIT	60 GHz cnWave ...	N/A	Online (0d 5h 5m)	V5...	XH	0d 5h 56m	1.2.2.1
<input checked="" type="checkbox"/> VIK_CN	01:00:00:00:00:00	4A	Base Infrastructure	60 GHz cnWave ...	N/A	Online (0d 11h 3m)	V5...	8	0d 10h 18m	1.2.2.1
<input type="checkbox"/> V5K_DN	01:00:00:00:00:00	D4	Base Infrastructure	60 GHz cnWave ...	N/A	Online (3d 12h 37m)	V5...	C7	0d 23h 51m	1.2.2
<input type="checkbox"/> VIK_8b00d6	01:00:00:00:00:00	D6	Base Infrastructure	60 GHz cnWave ...	N/A	Online (3d 12h 35m)	V5...	C1	0d 23h 51m	1.2.2
<input type="checkbox"/> PoP_V3K	01:00:00:00:00:00	D6	Base Infrastructure	60 GHz cnWave ...	N/A	Online (5d 3h 4m)	V5...	57	0d 23h 51m	1.2.2
<input type="checkbox"/> VIK	01:00:00:00:00:00	FA	Base Infrastructure	60 GHz cnWave ...	N/A	Online (3d 12h 35m)	V5...	SG	0d 23h 51m	1.2.2
<input type="checkbox"/> V5K_883083	01:00:00:00:00:00	83	Base Infrastructure	60 GHz cnWave ...	N/A	Online (3d 13h 27m)	X1C...	3	0d 23h 51m	1.2.2
<input type="checkbox"/> F425_200dc5	B1:00:00:00:00:00	C5	Base Infrastructure	ePMP Force 425 ...	192.168.0.2	Online (2d 2h 28m)	E8...	C9	1d 21h 55m	5.3
<input type="checkbox"/> Node_73d044	31:00:00:00:00:00	44	Ashok MSP	60 GHz cnWave ...	N/A	Online (1d 23h 21m)	V5...	B	2d 0h 29m	1.2.2.1
<input type="checkbox"/> Node_8b0417	01:00:00:00:00:00	17	Ashok MSP	60 GHz cnWave ...	N/A	Online (1d 23h 19m)	V5...	KZ	2d 0h 29m	1.2.2.1

To reboot devices using bulk reboot, perform the following steps:

1. Navigate to **Inventory** page of Network/Tower/Site.
2. Select one or multiple devices.

- Click **Actions** and choose **Reboot Now**.

Schedule Reboot

Schedule a reboot of the device(s) by selecting **Schedule Reboot** from **Actions** dropdown.

To reboot devices using schedule reboot, perform the following steps:

- Navigate to **Inventory** page of Network/Tower/Site.
- Select one or multiple devices.
- Click **Actions** and choose **Schedule Reboot**.
- Enter **Date** and **Time**.
- Click **Schedule**.

After creating a scheduled reboot job, you can view the status in the **Administration > Jobs > Actions** 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		
86	Reboot	Base Infrastructure	Sasi	Schedule	Raghavendra Atmakuri	May 10, 2021 12:14	May 10, 2021 19:01	Completed:	<div></div>	
85	Reboot	All Accounts	System	Schedule	Raghavendra Atmakuri	May 10, 2021 12:07	May 10, 2021 19:31	Completed:	<div></div>	
84	Reboot	All Accounts	System	Now	Sai Mahesh	Mar 18, 2021 15:13	Mar 18, 2021 15:13	Completed:	<div></div>	
83	Reboot	Base Infrastructure	AutoUpdate	Schedule	Durga Prasad	Feb 12, 2021 19:57	Feb 13, 2021 10:10	Completed:	<div></div>	
82	Reboot	Base Infrastructure	Sasi	Schedule	Sasikumar R	Feb 12, 2021 19:52	Feb 13, 2021 09:31	Completed:	<div></div>	
81	Reboot	All Accounts	System	Schedule	jishma asmi	Feb 12, 2021 19:47	Feb 12, 2021 23:53	Completed:	<div></div>	
80	Reboot	Base Infrastructure	site2	Schedule	jishma asmi	Feb 12, 2021 19:47	Feb 12, 2021 19:52	Completed:	<div></div>	
79	Reboot	All Accounts	System	Now	jishma asmi	Feb 09, 2021 22:37	Feb 09, 2021 22:37	Completed:	<div></div>	
78	Reboot	All Accounts	System	Now	Raghavendra Atmakuri	Jan 06, 2021 16:40	Jan 06, 2021 16:40	Completed:	<div></div>	
77	Reboot	All Accounts	System	Schedule	Raghavendra Atmakuri	Jan 06, 2021 16:40	Jan 06, 2021 16:45	Completed:	<div></div>	

Import Device Configuration

Import device(s) configuration is available from the inventory page at System/Network/Managed Account/ePMP or PMP AP device levels.



Note

The Import Device configuration is supported only for the Access and Backhaul account and is applicable only on ePMP/PMP AP and SM devices.

The following parameters are supported for ePMP/PMP AP in the CSV file:

- Azhimuth
- Beamwidth
- Elevation
- Height

- Latitude
- Longitude

The following parameters are supported for ePMP/PMP SM is in the CSV file:

- Latitude
- Longitude

Figure 256 Import Device Configuration

Device	Managed Account	Type	IP Address	Health	Serial Number	Description	Onboarded	Active S/W Version	Height
E600-VSM	Base Infrastructure	cnPilot e600	192.168.0.5	Offline 0d 2h 29m			9d 12h 38m	4.1-r3	N/A

Sample Configuration File

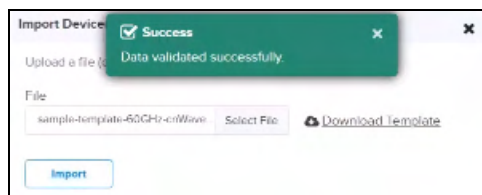
MAC	LATITUDE	LONGITUDE	AZIMUTH	ELEVATION	BEAM WIDTH	HEIGHT	HEIGHT UN
Supports formats with ':', '-', 'no space', upper and lower case.	Signed degrees format (DDD.ddd).	Signed degrees format (DDD.ddd).	Degrees from North (0 to 360)	Degrees from horizon (-90 to 90)	Degrees from 1 to 360	Min=0, Max=5 Meters/Feet	
	16	19	17	17	130	1500	Feet
	-90	119.0123	190	64	120	1000	feet
	79.0123	11	111	74	112	110	Meters
	-44	-12.78	124	67	177	190	meters

Sample Configuration File (60 GHz cnWave)

Figure 257 Sample Configuration file: 60 GHz cnWave

A	B	C	D	E	F	G	H	I	J	K	L	M
1	MAC	Serial Number	Device Name	Model	Device MAC	PoP Node	Site	Latitude	Longitude	Azimuth	Elevation	Description
2	Supports f	Serial Number	Name of t	V5000/V3000/DN/CN	Yes/No	Name of f	Signed de	Signed de	Degrees fr	Degrees from horizon (-90 to 90)		
3			POP-Node	V5000	DN	Yes	East-Pole	44.68233	12.1452	17	17	
4			DN-Node	V5000	DN	No	West-Pole	-12.5425	119.0123		190	64
5			CN-Node	V3000	CN	No	North-Pole	44.2311	35.622	111	74	
6			CN-Node	V1000	CN	No	South-Pole	22.6533	-12.78	124	67	
7												

While importing the file, it automatically validates the data as shown below:



If any invalid fields are found, an error message pops up:

Import Device(s) Configuration

Upload a file (csv) as per the format specified in the template.

File: sample-template-60GHz-cnWave-devices (8).csv [Select File](#) [Download Template](#)

MAC Address	Name	Model	Mode	Site	Latitude	Longitude	Azimuth	Elevation
00:04:56:11:11:11	POP-Node	V5000		East Pole-POP	44.68233	12.1452	17	17
00:04:56:33:33:33	CN-Node-V3K			North-Pole-CN	44.2311	35.622	111	74

[Validate](#) [Validation Summary](#) Invalid: 2 Total: 4

[Import](#) [Download Modified Data](#)

Uploading a Configuration File

To upload a configuration file (CSV) using the format specified in the sample template, perform the following steps:

1. Click **Download Sample Template** or prepare a sheet in CSV file format with necessary column details.
2. Upload a configuration file (CSV) using the format specified in the sample template.



Note

You must know the MAC address of the device to push the configuration.

3. Click **Import**.

Figure 258 Uploading Configuration file

Import Device(s) Configuration

Upload a configuration file (csv) as per the format specified in the sample template. The configuration file supports ePMP and PMP devices.

Configuration file

[Select File](#)

[Import](#) [Download Sample Template](#)

4. A configuration job will be created.

Import Summary

Configuration job was successfully created for 1/2 device(s). However, the following device(s) were excluded as they had invalid values. Please check the formatting or validity of the values.

Info: 1 Device(s) accepted without latitude/longitude values.

[OK](#)

- You can view the completed status of the configuration import in the configuration update page.

Administration > Jobs

Configuration Update Software Update Reports Actions

All Managed Account: All Accounts

ID	Details	Managed Account	Occurrence	Target	Created by	Created on	Completed on	Parallel	Stop on Error	Sector Priority	Status	
4357	1 onMatrix EX2010 device(s)	Base Infrastructure	Now	onMatrix-Syslog.co...	Durga Prasad	May 15, 2021 12:47	May 15, 2021 12:47	-	false	N/A	Completed: <div></div>	
4356	1 device(s)	Base Infrastructure	Now		Auto-Sync	May 15, 2021 12:47	May 15, 2021 12:47	15	false	N/A	Completed: <div></div>	
4355	1 device(s)	Base Infrastructure	Now		Auto-Sync	May 15, 2021 12:46	May 15, 2021 12:46	15	false	N/A	Completed: <div></div>	
4354	1 onMatrix EX2010 device(s)	Base Infrastructure	Now	Default-Syslog	Durga Prasad	May 15, 2021 12:46	May 15, 2021 12:46	-	false	N/A	Completed: <div></div>	
4353	1 device(s)	Base Infrastructure	Now		Auto-Sync	May 14, 2021 16:10	May 14, 2021 16:11	15	false	N/A	Completed: <div></div>	
4352	1 device(s)	Base Infrastructure	Now		Auto-Sync	May 14, 2021 15:52	May 14, 2021 15:52	15	false	N/A	Completed: <div></div>	
4351	1 device(s)	Base Infrastructure	Now		Auto-Sync	May 14, 2021 15:51	May 14, 2021 15:51	15	false	N/A	Completed: <div></div>	
4350	1 device(s)	Base Infrastructure	Now		Auto-Sync	May 14, 2021 15:50	May 14, 2021 15:51	15	false	N/A	Completed: <div></div>	
4349	1 device(s)	Base Infrastructure	Now		Auto-Sync	May 14, 2021 15:47	May 14, 2021 15:47	15	false	N/A	Completed: <div></div>	
4348	1 onPilot e510 device(s)	Base Infrastructure	Now	Sysloghouse	Raja Muriyandy	May 13, 2021 13:11	May 13, 2021 13:12	-	false	N/A	Completed: <div></div>	

Showing 1-10 Total: 4,236 10 < Previous 1 2 3 4 5 ... 424 Next >

The following table provides details on different errors that might occur while importing a CSV file:

Table 65 *Importing Error*

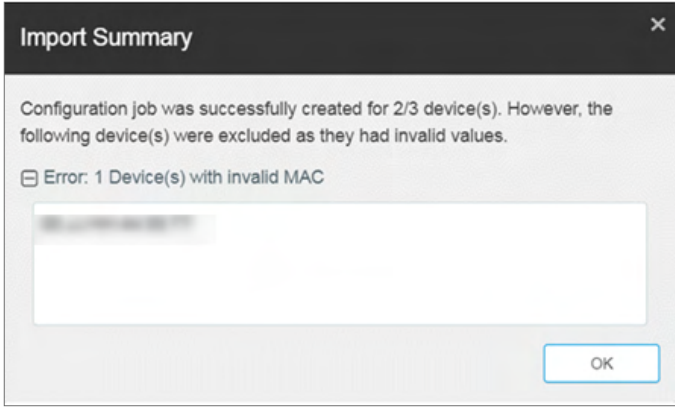
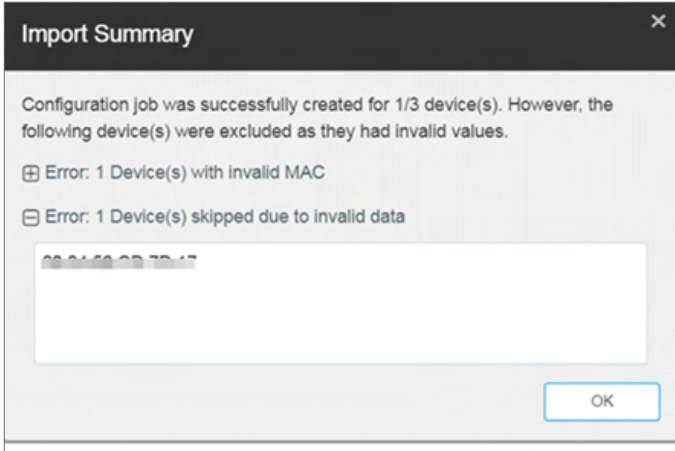
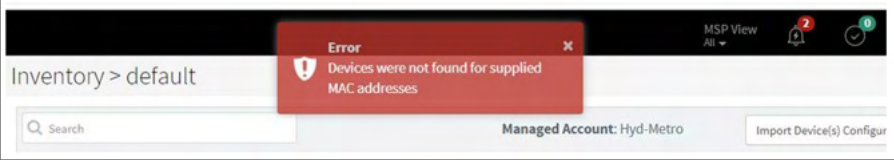
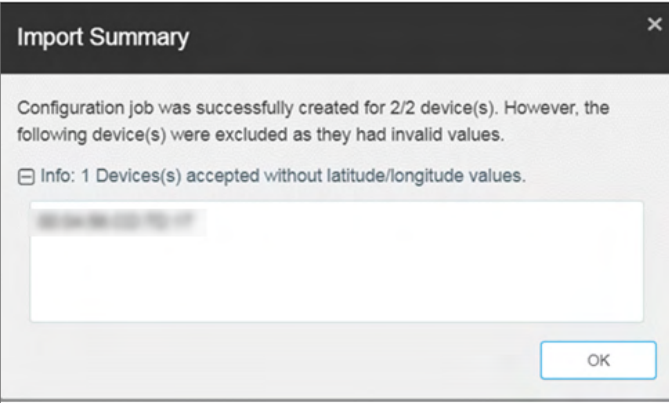
Error	Description
{Count of Devices} Device(s) with invalid MAC	<p>This error is displayed if the uploaded CSV file contains an invalid MAC Address.</p> 
{Count of Devices} Device(s) skipped due to invalid data	<p>This error is displayed if the uploaded CSV file contains invalid Data or data not relevant for Latitude, Longitude, Azimuth, Height, and Elevation.</p> 
Devices were not found for	<p>This error message is displayed if the devices were not found with correct MAC address in the CSV file.</p>

Table 65 *Importing Error*

Error	Description
supplied MAC Address	
Info: 1 Device(s) accepted without latitude/longit ude values	<p>This error is displayed when the latitude and longitude values are tried to push on to ePMP AP or PMP AP which are under a Tower.</p> 

Reports

There are two types of reports: Data Reports and Graphical Reports. Data Reports generate a CSV file and are meant to be read by Excel, Power BI, or a custom application. Graphical Reports generate a PDF file meant for human consumption.

The **Scheduled** tab displays reports that have not run. This includes reports executed periodically and those meant to run a single time. The **Completed** tab lists all reports that have finished and are available for download.

Scheduled Reports include the Scheduled, Terminated, and Timeout status in the Status column. **Completed Reports** include the Completed and Failed status in the Status column. Data reports are displayed only in a tabular format while graphical reports include charts and graphs.



Note

You can schedule and view reports (data and graphical) at the following levels in cnMaestro:

- System
- Network—Only data reports are available
- Site
- MSP

To view all scheduled data and graphical reports, navigate to **Monitor and Manage > System/<Network-name>/<Site-name>/<MSP-name> > Reports X > Scheduled**.

System										
Dashboard Notifications Configuration Statistics Reports X Software Update Applications X Clients Mesh Peers Assurance X Assists X										
Scheduled Completed										
Displays the list of Scheduled/Terminated/Timeout reports created under the tree node selected. Learn More										
<div> Add New Graphical Report Add New Data Report Delete </div>										
ID	Name	Report	Type	Schedule	Managed Account	Created by	Created on	Starts At	Status	Next Scheduled Time
479	lastmonth	Graphical	-	Monthly (30 ...	All Accounts		16 Apr 2025, 03:44 PM	16 Apr 2025, 07:45 P...	Scheduled	16 May 2025, 07:45 PM
477	lastweek	Graphical	-	Weekly	All Accounts		16 Apr 2025, 03:43 PM	16 Apr 2025, 08:00 ...	Scheduled	30 Apr 2025, 08:00 PM
469	MSP1	Graphical	-	Monthly (30 ...	Megha_MSP		16 Apr 2025, 03:38 PM	16 Apr 2025, 05:30 ...	Scheduled	16 May 2025, 05:30 PM
435	PON-Devices-Perf...	Data	Perform...	Daily	Base Infrastru...		16 Apr 2025, 12:18 PM	16 Apr 2025, 12:23 PM	Scheduled	30 Apr 2025, 12:23 PM
417	Audit_Weekly	Data	Audit Lo...	Weekly	All Accounts		16 Apr 2025, 10:06 AM	16 Apr 2025, 10:12 AM	Scheduled	07 May 2025, 10:12 AM
415	GR-16-4-25-Weekly	Graphical	-	Weekly	All Accounts		16 Apr 2025, 10:05 AM	16 Apr 2025, 10:10 AM	Scheduled	07 May 2025, 10:10 AM
414	GR-16-4-25-Daily	Graphical	-	Daily	All Accounts		16 Apr 2025, 10:04 AM	16 Apr 2025, 10:09 AM	Scheduled	01 May 2025, 10:09 AM
365	PON-DP2-P	Data	Perform...	Daily	Base Infrastru...		15 Apr 2025, 12:31 PM	15 Apr 2025, 09:16 PM	Scheduled	30 Apr 2025, 09:16 PM
364	PON-DP1	Data	Devices	Daily	Base Infrastru...		15 Apr 2025, 12:29 PM	15 Apr 2025, 09:15 PM	Scheduled	30 Apr 2025, 09:15 PM
352	60Ghz perf nodes ...	Data	Perform...	Daily	All Accounts		15 Apr 2025, 10:43 AM	15 Apr 2025, 10:49 AM	Scheduled	01 May 2025, 10:49 AM
Showing 1 - 10 Total: 36 10 < Previous 1 2 3 4 Next >										

To download completed reports, navigate to **System > Monitor and Manage > Reports X > Completed**.

System										
Dashboard Notifications Configuration Statistics Reports X Software Update Applications X Clients Mesh Peers Assurance X Assists X										
Scheduled Completed										
Displays the list of Completed/Failed reports created under the tree node selected. Learn More										
<div> Delete </div>										
ID	Name	Report	Type	Sched...	Managed Account	Created by	Status	Generated on		
50	events_daily	Data	Events	Daily	Base Infrastru...		Completed	30 Apr 2025, 10:54 AM	Download	Delete
352	60Ghz perf nodes ...	Data	Perform...	Daily	All Accounts		Completed	30 Apr 2025, 10:49 AM	Download	Delete
351	60GHz daily devic...	Data	Devices	Daily	All Accounts		Completed	30 Apr 2025, 10:48 AM	Download	Delete
415	GR-16-4-25-Weekly	Graphical	-	Weekly	All Accounts		Completed	30 Apr 2025, 10:14 AM	Download	Delete
417	Audit_Weekly	Data	Audit Lo...	Weekly	All Accounts		Completed	30 Apr 2025, 10:13 AM	Download	Delete
414	GR-16-4-25-Daily	Graphical	-	Daily	All Accounts		Completed	30 Apr 2025, 10:11 AM	Download	Delete
365	PON-DP2-P	Data	Perform...	Daily	Base Infrastru...		Completed	29 Apr 2025, 09:16 PM	Download	Delete
364	PON-DP1	Data	Devices	Daily	Base Infrastru...		Completed	29 Apr 2025, 09:15 PM	Download	Delete
176	KK	Data	Devices	Daily	All Accounts		Completed	29 Apr 2025, 05:15 PM	Download	Delete
242	Lastday_MSP	Graphical	-	Daily	Megha_MSP		Completed	29 Apr 2025, 05:01 PM	Download	Delete
Showing 1 - 10 Total: 1016 10 < Previous 1 2 3 4 5 ... 102 Next >										



Note

- You can have 50 reports in the **Scheduled** tab and any number in the **Completed** tab. Only 50 reports can be generated in parallel in a cnMaestro account.
- The completed reports are available for download for 30 days in the Cloud and for seven days in On-Premises.
- While generating Alarm History, Events, Performance, Clients, and Guest Access reports, there is a delay of up to 20-30 minutes for the recent entries to be available in the report.

Data Reports

Data Reports generate a CSV document that can be viewed in Excel, Power BI or other data analysis tools.

This section details how to schedule and generate different types of data reports in cnMaestro.

- [Devices Report](#)
- [Audit Logs Report](#)
- [Performance Report](#)
- [Active Alarms Report](#)
- [Alarm History Report](#)
- [Events Report](#)
- [Wireless Clients Report](#)
- [Wi-Fi Events Report](#)
- [Guest Access Login Events](#)



Note

cnMaestro supports 14 months of historical data for the following devices:

- cnPilot Home (R-Series)
- Enterprise devices (Enterprise Wi-Fi and cnMatrix)
- IIoT devices

cnMaestro supports 26 months of historical data for the following devices:

- Fixed Wireless

Devices Report

Devices Reports are generated as CSV files and include all devices under the selected tree node.

To generate Devices Reports, perform the following steps:

1. Navigate to **Reports X> Scheduled** tab within System, MSP, Site, Network, or Tower nodes in the hierarchical tree.
2. Click **Add New Data Report**. The following window is displayed.

Reports > Add Report

Generate report for device parameters as a comma-separated value (CSV) file. All devices under the tree node selected will be included in the export. Select all parameters that should be included. [Learn More](#)

Name*

Description

Recipients
 Enter valid email and press enter (max 5 recipients)

Type*

Device Type

Select data to include in report

☒ **Basic**

<input checked="" type="checkbox"/> Country	<input checked="" type="checkbox"/> Description	<input checked="" type="checkbox"/> Device Location	<input checked="" type="checkbox"/> Device Name
<input checked="" type="checkbox"/> Device Type	<input checked="" type="checkbox"/> Hardware	<input checked="" type="checkbox"/> IPv4 Address	<input checked="" type="checkbox"/> IPv6 Address
<input checked="" type="checkbox"/> Last Update Message	<input checked="" type="checkbox"/> Last Update Status	<input checked="" type="checkbox"/> MAC Address	<input checked="" type="checkbox"/> Network
<input checked="" type="checkbox"/> Onboard Date	<input checked="" type="checkbox"/> Onboarding Status	<input checked="" type="checkbox"/> Product Name	<input checked="" type="checkbox"/> Serial Number
<input checked="" type="checkbox"/> Software Version	<input checked="" type="checkbox"/> Status	<input checked="" type="checkbox"/> Status Time	<input checked="" type="checkbox"/> Tower/Site

☒ **Location**

☒ GPS Coordinates

Schedule
☒ Now ☐ Daily ☐ Weekly ☐ Monthly (30 days)

Report generation may take several minutes, depending upon quantity of data.

3. Enter a **Name** and **Description** for the report.
4. Enter email addresses (maximum of 5) in the **Recipients** field to send reports.
5. Select the **Report Type** as **Devices**.
6. Select the type of device from the **Device Type** dropdown list.
7. Select the data parameters to include in the report.
8. Select the **Schedule** such as Now, Daily, Weekly, or Monthly.
9. Click **Add**. The report is added to the **Scheduled Reports** page.

If **Device Type** is **All**, then **Basic** data export parameters are available, rather than parameters specific to a device type.

The device data parameters exported for the following devices are listed below:

- [60 GHz cnWave](#)
- [cnMatrix](#)
- [cnPilot Home \(R-Series\)](#)
- [cnRanger](#)
- [cnReach](#)
- [cnReach XIO](#)
- [cnVision](#)
- [cnWave 5G Fixed](#)
- [Enterprise Wi-Fi](#)

- [ePMP](#)
- [PMP](#)
- [PON](#)
- [PTP 650/670/700](#)
- [PTP 820/850](#)
- [RV22 Home Mesh](#)

If 60 GHz cnWave device is selected as **Device Type**, then the following parameter sections are available:

- Mode (CN or DN)
- Basic
- Ethernet
- GPS
- Radio

Figure 259 *Device Report: 60 GHz cnWave*

Mode
☒ CN ☒ DN

Select data to include in report

☒ **Basic**

<input checked="" type="checkbox"/> Description	<input checked="" type="checkbox"/> Device Name	<input checked="" type="checkbox"/> Device Type	<input checked="" type="checkbox"/> IPv6 Address
<input checked="" type="checkbox"/> MAC	<input checked="" type="checkbox"/> Mode	<input checked="" type="checkbox"/> Model	<input checked="" type="checkbox"/> Network
<input checked="" type="checkbox"/> Onboard Status	<input checked="" type="checkbox"/> PoP Node	<input checked="" type="checkbox"/> Product Name	<input checked="" type="checkbox"/> Serial Number
<input checked="" type="checkbox"/> Site	<input checked="" type="checkbox"/> Software Version	<input checked="" type="checkbox"/> Status	<input checked="" type="checkbox"/> Status Time

☒ **Radio**

<input checked="" type="checkbox"/> MAC	<input checked="" type="checkbox"/> Packets	<input checked="" type="checkbox"/> Radio Channel	<input checked="" type="checkbox"/> Radio Polarity
<input checked="" type="checkbox"/> Throughput			

☒ **GPS**

<input checked="" type="checkbox"/> Fix Type	<input checked="" type="checkbox"/> GPS Coordinates	<input checked="" type="checkbox"/> GPS Satellites Tracked	<input checked="" type="checkbox"/> Height
<input checked="" type="checkbox"/> Sync Mode			

☒ **Ethernet**

<input checked="" type="checkbox"/> Errors	<input checked="" type="checkbox"/> Packet Drops	<input checked="" type="checkbox"/> Packets	<input checked="" type="checkbox"/> Status
<input checked="" type="checkbox"/> Throughput			

If cnMatrix is selected as the **Device Type**, then **Basic** data export parameters will be exported.

Figure 260 *Device Report: cnMatrix*

Select data to include in report

☒ **Basic**

<input checked="" type="checkbox"/> Description	<input checked="" type="checkbox"/> Device Location	<input checked="" type="checkbox"/> Device Name	<input checked="" type="checkbox"/> Device Type
<input checked="" type="checkbox"/> Hardware	<input checked="" type="checkbox"/> IP Address	<input checked="" type="checkbox"/> Last Update Message	<input checked="" type="checkbox"/> Last Update Status
<input checked="" type="checkbox"/> MAC	<input checked="" type="checkbox"/> Network	<input checked="" type="checkbox"/> Onboard Date	<input checked="" type="checkbox"/> Onboard Status
<input checked="" type="checkbox"/> Product Name	<input checked="" type="checkbox"/> Serial Number	<input checked="" type="checkbox"/> Site	<input checked="" type="checkbox"/> Software Version
<input checked="" type="checkbox"/> Status	<input checked="" type="checkbox"/> Status Time	<input checked="" type="checkbox"/> Tower	

If cnPilot Home (R-Series) is selected as the **Device Type**, then the following parameter sections are available:

- Basic
- Location

- Network
- Radio

Figure 261 *Device Report: cnPilot Home (R-Series)*

Select data to include in report

☒ **Basic**

☒ Description
☒ Device Location
☒ Device Mode
☒ Device Name
☐ Device Type
☒ Hardware
☐ IP Address
☐ IPv6 Address
☒ Last Update Message
☒ Last Update Status
☒ Last Updated Time
☐ MAC
☒ Network
☒ Onboard Date
☐ Onboard Status
☒ Product Name
☒ Serial Number
☒ Site
☐ Software Version
☐ Status
☐ Status Time
☒ Sync Status

☒ **Network**

☒ Default Gateway
☒ Ethernet
☒ WAN IP Address

☒ **Radio**

☒ End Hosts
☒ Radios Band
☒ Radios Channel
☒ Radios Client Count
☒ Radios MAC
☒ Radios Power
☒ Radios State
☒ Radios Throughput
☒ Radios WLANs

☒ **Location**

☒ GPS Coordinates

If cnRanger is selected as the **Device Type**, then the following parameter sections are available:

- Basic
- CBRS
- Location
- Network
- Radio

Figure 262 *Device Report: cnRanger*

Mode
☒ BBU
☒ RRH
☒ SM

Select data to include in report

☒ **Basic**

☒ Antenna Gain (dBi)
☒ Channel Width (MHz)
☒ Connected BBU MAC
☒ Connected RRH MAC
☒ Description
☒ Device Location
☒ Device Mode
☐ Device Name
☒ Firmware Version
☒ Hardware Model
☐ IP Address
☒ Last Update Message
☒ Last Update Status
☒ Last Updated Time
☐ MAC
☒ Network
☒ Onboard Date
☒ Onboard Status
☒ Product Name
☒ Serial Number
☐ Software Version
☐ Status
☐ Status Time
☒ TDD Ratio
☒ Temperature (°C)
☒ Tower

☒ **Network**

☒ DNS
☒ Default Gateway
☒ LAN Status
☒ LAN Status
☒ Netmask
☒ Physical Cell Id
☒ Secondary DNS
☒ Special Subframe

☒ **Radio**

☒ RF Frequency (MHz)
☒ RSRP (dBm)
☒ RSRQ (dBm)
☒ Radio TX Power (dBm)

☒ **Location**

☒ GPS Coordinates

☒ **CBRS**

☒ CBRS Heartbeat Timestamp
☒ CBRS Location
☒ CBRS State
☒ CBRS Status
☒ Grant EIRP
☒ Request EIRP

If cnReach is selected as the **Device Type**, then the following sections are available:

- Basic
- Network
- Radio

Figure 263 *Device Report: cnReach*

Select data to include in report

☒
Basic

☒ DA Version
☒ Device Name
☒ IP Address
☒ Last Update Message

☒ Last Update Status
☒ MAC
☒ Product Name
☒ Software Version

☒
Network

☒ DNS
☒ Default Gateway
☒ Netmask

☒
Radio

☒ MAC
☒ Neighbors
☒ RSSI
☒ Radio Temperature

☒ Role
☒ SNR
☒ Throughput
☒ TxPower

If cnReach XIO is selected as the **Device Type**, then the following sections are available:

- Basic
- Network

Figure 264 *Device Report: cnReach XIO*

Select data to include in report

☒
Basic

☒ DA Version
☒ Device Name
☒ IP Address
☒ Last Update Message

☒ Last Update Status
☒ MAC
☒ Product Name
☒ Software Version

☒
Network

☒ DNS
☒ Default Gateway
☒ Netmask

If cnVision is selected as the **Device Type**, then the following sections are available:

- Mode (Client or Hub)
- Basic
- Location
- Mode
- Network
- Radio

Figure 265 *Device Report: cnVision*

Mode

☒ Client
☒ Hub

Select data to include in report

☒ **Basic**

☒ Antenna Gain (dBi)
☒ Authentication Type
☒ Client Distance
☒ Configuration Version
☒ Connected AP MAC
☒ Connected Clients
☒ Country
☒ Description
☒ Device Location
☒ Device Mode
☒ Device Name
☒ GPS Sync State
☒ Hardware
☒ IPv4 Address
☒ IPv6 Address
☒ Last Update Message
☒ Last Update Status
☒ Last Updated Time
☒ MAC Address
☒ Max Range
☒ Network
☒ Onboard Date
☒ Onboarding Status
☒ Product Name
☒ Reboot Count
☒ Serial Number
☒ Session Time
☒ Software Version
☒ SSID
☒ Status
☒ TDD Ratio
☒ Tower
☒ Up Time

☒ **Network**

☒ Default Gateway
☒ DNS
☒ LAN Mode Status
☒ LAN Speed Status (Mbps)
☒ LAN Status
☒ LAN Status
☒ Netmask
☒ Network LAN MTU (Bytes)
☒ WAN IP Address
☒ Wireless MAC
☒ WLAN Status

☒ **Radio**

☒ Channel Width
☒ Client TX Capacity
☒ Client TX Quality
☒ DFS Status
☒ DL Frame Utilization
☒ MCS
☒ PacketCount
☒ Radio Mode
☒ Radio TX Power
☒ Retransmission
☒ Retransmission Percentage
☒ RF Frequency
☒ RSSI
☒ SNR

☒ **Location**

☒ Antenna Tilt
☒ Azimuth
☒ BeamWidth
☒ Device Coordinates
☒ Height

If cnWave 5G Fixed device is selected as **Device Type**, choose the type of **Mode** (BTS or CPE) then the following sections are available:

- Mode (BTS or CPE)
- Basic
- Location
- Radio

Figure 266 *Device Report: cnWave 5G Fixed*

Mode

☒ BTS
☒ CPE

Select data to include in report

☒ **Basic**

☒ CRNTI
☒ Description
☒ Device Mode
☒ Device Name
☒ Downlink MCS
☒ IMSI
☒ IP Address
☒ MAC
☒ Product Name
☒ Registered CPEs
☒ Registration Count
☒ Registration State
☒ Serial Number
☒ Software Version
☒ Status
☒ Uplink MCS

☒ **Radio**

☒ Alignment Active
☒ Bandwidth
☒ Current EIRP (dBm)
☒ DL Backoff (dB)
☒ DL Channel Distortion (dB)
☒ DL Codeword Rate
☒ DL EVM (dB)
☒ DL Rx Power (dBm)
☒ DL Sounding State
☒ DL Spatial Frequency
☒ Link Symmetry
☒ Max EIRP (dBm)
☒ Polarisation
☒ Range (km)
☒ RF Frequency (MHz)
☒ SFP1 Speed
☒ SFP2 Speed
☒ UL Channel Distortion (dB)
☒ UL EVM (dB)
☒ UL Rx Power (dBm)
☒ UL Sounding State
☒ UL Spatial Frequency
☒ UL Target Rx Power (dBm)
☒ UL Tx Pwr Ctrl Cont Adjust
☒ UL Tx Pwr Ctrl Initial Adjust

☒ **Location**

☒ GPS Coordinates
☒ Site Contact
☒ Site Location

If Enterprise Wi-Fi is selected as the **Device Type**, then the following sections are available:

- AFC
- Basic

- GPS
- Location
- Network
- Radio

Figure 267 *Device Report: Enterprise(Wi-Fi)*

Select data to include in report

<input checked="" type="checkbox"/> Basic			
<input checked="" type="checkbox"/> Description	<input checked="" type="checkbox"/> Device Location	<input checked="" type="checkbox"/> Device Mode	<input checked="" type="checkbox"/> Device Name
<input checked="" type="checkbox"/> Device Type	<input checked="" type="checkbox"/> Hardware	<input checked="" type="checkbox"/> IPv4 Address	<input checked="" type="checkbox"/> IPv6 Address
<input checked="" type="checkbox"/> Last Update Message	<input checked="" type="checkbox"/> Last Update Status	<input checked="" type="checkbox"/> Last Updated Time	<input checked="" type="checkbox"/> MAC Address
<input checked="" type="checkbox"/> Network	<input checked="" type="checkbox"/> Onboard Date	<input checked="" type="checkbox"/> Onboarding Status	<input checked="" type="checkbox"/> Product Name
<input checked="" type="checkbox"/> Serial Number	<input checked="" type="checkbox"/> Site	<input checked="" type="checkbox"/> Software Version	<input checked="" type="checkbox"/> Status
<input checked="" type="checkbox"/> Status Time	<input checked="" type="checkbox"/> Sync Status		
<input type="checkbox"/> Network			
<input checked="" type="checkbox"/> Default Gateway	<input checked="" type="checkbox"/> Ethernet	<input checked="" type="checkbox"/> WAN IP Address	<input checked="" type="checkbox"/> WLAN(1-4) VLAN
<input type="checkbox"/> WLAN(13-16) VLAN	<input type="checkbox"/> WLAN(5-8) VLAN	<input type="checkbox"/> WLAN(9-12) VLAN	
<input checked="" type="checkbox"/> Radio			
<input checked="" type="checkbox"/> End Hosts	<input checked="" type="checkbox"/> Mesh Peers	<input checked="" type="checkbox"/> Radios Band	<input checked="" type="checkbox"/> Radios Channel
<input checked="" type="checkbox"/> Radios Client Count	<input checked="" type="checkbox"/> Radios MAC	<input checked="" type="checkbox"/> Radios Power	<input checked="" type="checkbox"/> Radios RF Quality
<input checked="" type="checkbox"/> Radios RF Utilization	<input checked="" type="checkbox"/> Radios State	<input checked="" type="checkbox"/> Radios Throughput	<input checked="" type="checkbox"/> Radios WLANs
<input checked="" type="checkbox"/> GPS			
<input checked="" type="checkbox"/> GPS Altitude	<input checked="" type="checkbox"/> GPS Altitude Type	<input checked="" type="checkbox"/> GPS Axis	<input checked="" type="checkbox"/> GPS Fix Type
<input checked="" type="checkbox"/> GPS GNSS	<input checked="" type="checkbox"/> GPS Satellites	<input checked="" type="checkbox"/> GPS Timestamp	<input checked="" type="checkbox"/> GPS Vertical Uncertainty
<input checked="" type="checkbox"/> Location			
<input checked="" type="checkbox"/> Device Coordinates			
<input checked="" type="checkbox"/> AFC			
<input checked="" type="checkbox"/> AFC Channels	<input checked="" type="checkbox"/> AFC Description	<input checked="" type="checkbox"/> AFC EIRP	<input checked="" type="checkbox"/> AFC Last Updated
<input checked="" type="checkbox"/> AFC Location	<input checked="" type="checkbox"/> AFC Status	<input checked="" type="checkbox"/> AFC Token	<input checked="" type="checkbox"/> AFC Token Expiry
<input checked="" type="checkbox"/> AFC Version			

If eMPM is selected as the **Device Type** then the following sections are available:

- Mode (AP or SM)
- Basic
- Location
- Network
- Radio

Figure 268 Device Report: ePMP

Mode
☒ SM ☒ AP

Select data to include in report

☒ **Basic**

<input checked="" type="checkbox"/> Antenna Gain (dBi)	<input checked="" type="checkbox"/> Authentication Type	<input checked="" type="checkbox"/> Configuration Version	<input checked="" type="checkbox"/> Connected AP MAC
<input checked="" type="checkbox"/> Connected SMs	<input checked="" type="checkbox"/> Country	<input checked="" type="checkbox"/> Description	<input checked="" type="checkbox"/> Device Location
<input checked="" type="checkbox"/> Device Mode	<input checked="" type="checkbox"/> Device Name	<input checked="" type="checkbox"/> GPS Sync State	<input checked="" type="checkbox"/> Hardware
<input checked="" type="checkbox"/> IP Address	<input checked="" type="checkbox"/> IPv6 Address	<input checked="" type="checkbox"/> Last Update Message	<input checked="" type="checkbox"/> Last Update Status
<input checked="" type="checkbox"/> Last Updated Time	<input checked="" type="checkbox"/> MAC	<input checked="" type="checkbox"/> Max Range	<input checked="" type="checkbox"/> Network
<input checked="" type="checkbox"/> Onboard Date	<input checked="" type="checkbox"/> Onboard Status	<input checked="" type="checkbox"/> Product Name	<input checked="" type="checkbox"/> Reboot Count
<input checked="" type="checkbox"/> SM Distance	<input checked="" type="checkbox"/> SSID	<input checked="" type="checkbox"/> Serial Number	<input checked="" type="checkbox"/> Session Drops
<input checked="" type="checkbox"/> Session Time	<input checked="" type="checkbox"/> Software Version	<input checked="" type="checkbox"/> Status	<input checked="" type="checkbox"/> Status Time
<input checked="" type="checkbox"/> TDD Ratio	<input checked="" type="checkbox"/> Tower		

☒ **Network**

<input checked="" type="checkbox"/> DNS	<input checked="" type="checkbox"/> Default Gateway	<input checked="" type="checkbox"/> LAN Mode Status	<input checked="" type="checkbox"/> LAN Speed Status (Mbps)
<input checked="" type="checkbox"/> LAN Status	<input checked="" type="checkbox"/> LAN Status	<input checked="" type="checkbox"/> Netmask	<input checked="" type="checkbox"/> Network LAN MTU (Bytes)
<input checked="" type="checkbox"/> WAN IP Address	<input checked="" type="checkbox"/> WLAN Status	<input checked="" type="checkbox"/> Wireless MAC	

☒ **Radio**

<input checked="" type="checkbox"/> Channel Width	<input checked="" type="checkbox"/> DFS Status	<input checked="" type="checkbox"/> DL Frame Utilization	<input checked="" type="checkbox"/> MCS
<input checked="" type="checkbox"/> PacketCount	<input checked="" type="checkbox"/> RF Frequency	<input checked="" type="checkbox"/> RSSI	<input checked="" type="checkbox"/> Radio Mode
<input checked="" type="checkbox"/> Radio TX Power	<input checked="" type="checkbox"/> Retransmission	<input checked="" type="checkbox"/> Retransmission Percentage	<input checked="" type="checkbox"/> SM TX Capacity
<input checked="" type="checkbox"/> SM TX Quality	<input checked="" type="checkbox"/> SNR		

☒ **Location**

<input checked="" type="checkbox"/> Azimuth	<input checked="" type="checkbox"/> BeamWidth	<input checked="" type="checkbox"/> Elevation	<input checked="" type="checkbox"/> GPS Coordinates
<input checked="" type="checkbox"/> Height			

If PMP is selected as the **Device Type**, then the following sections are available:

- Mode (AP or SM)
- AFC
- Basic
- CBRS
- Location
- Network
- Radio

Figure 269 *Device Report: PMP*

Mode
☒ AP ☒ SM

Select data to include in report

☒ **Basic**

☒ Antenna Gain (dBi) ☒ AP Color Codes ☒ Authentication Type ☒ Configuration Version
☒ Connected AP MAC ☒ Connected SMs ☒ Country ☒ Description
☒ Device Location ☒ Device Mode ☒ Device Name ☒ Hardware Model
☒ Internal Antenna Gain (dBi) ☒ IPv4 Address ☒ Last Update Message ☒ Last Update Status
☒ Last Updated Time ☒ MAC Address ☒ Max Range ☒ Network
☒ Onboard Date ☒ Onboarding Status ☒ PMP SNR ☒ Product Name
☒ RSSI Imbalance ☒ Serial Number ☒ Session Drops ☒ Session Time
☒ SM Color Codes ☒ SM Distance ☒ Software Version ☒ SSR(Signal Strength Ratio)
☒ Status ☒ Status Time ☒ SW Key - Max Throughput ☒ TDD Ratio
☒ Temperature (°C) ☒ Tower ☒ VLAN

☒ **Network**

☒ Default Gateway ☒ DNS ☒ LAN Status ☒ Netmask
☒ Secondary DNS

☒ **Radio**

☒ BER (Average) ☒ Channel Width ☒ Contention Slots ☒ DFS Status
☒ DL Actual Average EVM (db) ☒ EIRP ☒ Frame Period ☒ LUID
☒ PacketCount ☒ Radio TX Power ☒ RF Frequency ☒ RSSI
☒ Sync Source ☒ Sync State ☒ UL Actual Average EVM (db)

☒ **Location**

☒ Antenna Tilt ☒ Azimuth ☒ BeamWidth ☒ Device Coordinates
☒ Height ☒ Site Contact ☒ Site Location

☒ **CBRS**

☒ CBRS Center Frequency ☒ CBRS Channel Bandwidth ☒ CBRS Heartbeat Timestamp ☒ CBRS Location
☒ CBRS State ☒ CBRS Status ☒ Grant EIRP ☒ Request EIRP

☒ **AFC**

☒ AFC Description ☒ AFC EIRP ☒ AFC High Frequency ☒ AFC Last Updated
☒ AFC Location ☒ AFC Low Frequency ☒ AFC Status ☒ AFC Token
☒ AFC Token Expiry ☒ AFC Version

If PON is selected as the **Device Type**, then the following sections are available:

- Basic
- Location

Figure 270 *Device Report: PON*

Mode
☒ OLT ☒ ONU

Select data to include in report

☒ **Basic**

☒ Connected OLT MAC ☒ ConnectionTime ☒ Device Name ☒ Device Type
☒ Hardware ☒ IPv4 Address ☒ MAC Address ☒ Network
☒ OLT Port ☒ OLT RxPower ☒ Onboard Date ☒ Onboarding Status
☒ ONU ID ☒ Serial Number ☒ Software Version ☒ Status
☒ Tower/Site ☒ Up Time

☒ **Location**

☒ Device Coordinates

If PTP 650/670/700 is selected as the **Device Type**, then the following sections are available:

- Basic
- Location

- Network
- Radio

Figure 271 Device Report: PTP 650/670/700

Select data to include in report

☒ **Basic**

<input checked="" type="checkbox"/> Antenna Gain (dBi)	<input checked="" type="checkbox"/> Color Code	<input checked="" type="checkbox"/> DA Version	<input checked="" type="checkbox"/> Description
<input checked="" type="checkbox"/> Device Mode	<input checked="" type="checkbox"/> Hardware	<input checked="" type="checkbox"/> IPv4 Address	<input checked="" type="checkbox"/> IPv6 Address
<input checked="" type="checkbox"/> License Country	<input checked="" type="checkbox"/> Link Name	<input checked="" type="checkbox"/> MAC Address	<input checked="" type="checkbox"/> Max Range
<input checked="" type="checkbox"/> Maximum Number Of Slaves	<input checked="" type="checkbox"/> Network	<input checked="" type="checkbox"/> Product Name	<input checked="" type="checkbox"/> Receive Frequency
<input checked="" type="checkbox"/> Remote MAC Address	<input checked="" type="checkbox"/> Remote Unit Name	<input checked="" type="checkbox"/> Software Version	<input checked="" type="checkbox"/> Status Time
<input checked="" type="checkbox"/> Throughput	<input checked="" type="checkbox"/> Topology	<input checked="" type="checkbox"/> Tower	<input checked="" type="checkbox"/> Transmit Frequency
<input checked="" type="checkbox"/> Unit MSN	<input checked="" type="checkbox"/> Unit Name		

☒ **Network**

<input checked="" type="checkbox"/> Default Gateway	<input checked="" type="checkbox"/> IP Version
---	--

☒ **Radio**

<input checked="" type="checkbox"/> Antenna Type	<input checked="" type="checkbox"/> Cable Loss	<input checked="" type="checkbox"/> Channel Width	<input checked="" type="checkbox"/> Data Bridging Availability
<input checked="" type="checkbox"/> Dual Payload	<input checked="" type="checkbox"/> Highest Mod Mode	<input checked="" type="checkbox"/> Link Capacity (Mbps)	<input checked="" type="checkbox"/> Link Capacity Variant
<input checked="" type="checkbox"/> Link Optimization (IP / TDM)	<input checked="" type="checkbox"/> Link Status	<input checked="" type="checkbox"/> Link Symmetry	<input checked="" type="checkbox"/> Link UpTime
<input checked="" type="checkbox"/> Lower Centre Frequency (MHz)	<input checked="" type="checkbox"/> Lowest Ethernet Modulation Mode	<input checked="" type="checkbox"/> Maximum Transmit Power (dBm)	<input checked="" type="checkbox"/> QoS Data Priority Scheme
<input checked="" type="checkbox"/> Receive DataRate (Mbps)	<input checked="" type="checkbox"/> Signal Strength Ratio (dB)	<input checked="" type="checkbox"/> Spectrum Management Control	<input checked="" type="checkbox"/> TDD Sync Device
<input checked="" type="checkbox"/> TDD Synchronization Mode	<input checked="" type="checkbox"/> Transmit DataRate (Mbps)	<input checked="" type="checkbox"/> Wireless Link Availability	<input checked="" type="checkbox"/> Wireless Link Encryption

☒ **Location**

<input checked="" type="checkbox"/> GPS Coordinates

If PTP 820/850 is selected as the **Device Type**, then the following sections are available:

- Basic
- Radio

Figure 272 Device Report: PTP 820/850

Select data to include in report

☒ **Basic**

<input checked="" type="checkbox"/> Description	<input checked="" type="checkbox"/> Device Name	<input checked="" type="checkbox"/> Device Type	<input checked="" type="checkbox"/> Edge Controller
<input checked="" type="checkbox"/> IP Address	<input checked="" type="checkbox"/> MAC	<input checked="" type="checkbox"/> Model	<input checked="" type="checkbox"/> Network
<input checked="" type="checkbox"/> Product Name	<input checked="" type="checkbox"/> Serial Number	<input checked="" type="checkbox"/> Software Version	<input checked="" type="checkbox"/> Status
<input checked="" type="checkbox"/> Status Time	<input checked="" type="checkbox"/> Tower		

☒ **Radio**

<input checked="" type="checkbox"/> Bit Rate	<input checked="" type="checkbox"/> Defective Blocks	<input checked="" type="checkbox"/> Frequency	<input checked="" type="checkbox"/> Modem MSE
<input checked="" type="checkbox"/> Modem XPI	<input checked="" type="checkbox"/> Remote IPv4	<input checked="" type="checkbox"/> Remote Radio Location	<input checked="" type="checkbox"/> RFU Serial Number
<input checked="" type="checkbox"/> Signal Level	<input checked="" type="checkbox"/> Tx Mute		

The following sections are available for RV22 Home Mesh routers:

- Basic
- Location
- Network
- Radio

Figure 273 Device Report: RV22 Home Mesh

Select data to include in report

<input checked="" type="checkbox"/> Basic			
<input checked="" type="checkbox"/> Description	<input checked="" type="checkbox"/> Device Location	<input checked="" type="checkbox"/> Device Mode	<input checked="" type="checkbox"/> Device Name
<input checked="" type="checkbox"/> Device Type	<input checked="" type="checkbox"/> Hardware	<input checked="" type="checkbox"/> IPv4 Address	<input checked="" type="checkbox"/> IPv6 Address
<input checked="" type="checkbox"/> Last Update Message	<input checked="" type="checkbox"/> Last Update Status	<input checked="" type="checkbox"/> Last Updated Time	<input checked="" type="checkbox"/> MAC Address
<input checked="" type="checkbox"/> Network	<input checked="" type="checkbox"/> Onboard Date	<input checked="" type="checkbox"/> Onboarding Status	<input checked="" type="checkbox"/> Product Name
<input checked="" type="checkbox"/> Serial Number	<input checked="" type="checkbox"/> Site	<input checked="" type="checkbox"/> Software Version	<input checked="" type="checkbox"/> Status
<input checked="" type="checkbox"/> Status Time	<input checked="" type="checkbox"/> Sync Status		
<input checked="" type="checkbox"/> Network			
<input checked="" type="checkbox"/> Default Gateway	<input checked="" type="checkbox"/> Ethernet	<input checked="" type="checkbox"/> WAN IP Address	
<input checked="" type="checkbox"/> Radio			
<input checked="" type="checkbox"/> Radios Band	<input checked="" type="checkbox"/> Radios Channel	<input checked="" type="checkbox"/> Radios Client Count	<input checked="" type="checkbox"/> Radios MAC
<input checked="" type="checkbox"/> Radios Power	<input checked="" type="checkbox"/> Radios State	<input checked="" type="checkbox"/> Radios Throughput	<input checked="" type="checkbox"/> Radios WLANs
<input checked="" type="checkbox"/> Location			
<input checked="" type="checkbox"/> GPS Coordinates			



Note

Reports are available for each of the following hierarchical nodes in the tree:

- System
- Managed Account
- Network
- Tower
- Site
- AP Group

Audit Logs Report



Note

Audit log data is available for a maximum of 90 days.

The Audit logs report generates, in the CSV format, the cnMaestro audit log data that is available on the **Administration > Audit Logs X** page.

To generate the Audit Logs report, perform the following steps:

1. Navigate to **Reports X > Scheduled** tab.
2. Click **Add New Data Report**.
The Add Report page appears.
3. Enter a **Name** and **Description** for the report.
4. Enter email addresses (maximum of 5) in the **Recipients** field to send reports.
5. Select the **Report Type** as Audit Logs.
6. Select data parameters to include in the report.
Select the required checkboxes.
7. Select the following options:

- Schedule type (Now, Daily, Weekly, or Monthly (30 days))
- Time Range (Last Day, Last Week, Last Month, or Custom Time Range (up to a maximum of 90 days))

8. Click **Add**. The report is saved and listed in the **Scheduled Reports** page.

Figure 274 Audit Logs Report

Reports > Add Report

Generate report for Audit logs [Learn More](#)

Name*

Description

Recipients
Type and press Enter Enter valid email and press enter (Max 5 recipients)

Type*
Audit Logs

☒ Basic

☒ Action ☒ Description ☒ IP Address ☒ Module

☒ Result ☒ Source ☒ Time ☒ Type

Schedule
☒ Now ☐ Daily ☐ Weekly ☐ Monthly (30 days)

Time Range
☒ Last Day ☐ Last Week ☐ Last Month ☐ Custom Time Range

Report generation may take several minutes, depending upon quantity of data.

Add **Cancel**

Performance Report

The Performance Report generates device time-series performance data as a comma-separated value (CSV) file. All devices of selected type under the tree node will be included in the export.



Note

- You must select the parameters.
- This feature may generate a large file if many devices are selected.

To generate Performance reports, perform the following steps:

1. Navigate to **Report X > Scheduled** tab.
2. Click **Add New Data Report**.
3. Enter a **Name** and **Description** for the report.
4. Enter email addresses (maximum of 5) in the **Recipients** field to send reports.
5. Select **Type** as **Performance**.
6. Select the **Device Type**.

Reports > Add Report

Generate report for the "device time-based performance data" as a comma-separated value (CSV) file. All devices of selected type under the tree node will be included in the export. Select all parameters that should be included.
 Note: This feature may generate a large file if many devices are selected. [Learn More](#)

Name*

Description

Recipients
 Enter valid email and press enter (max 5 recipients)

Type*
 Performance

Device Type
 60 GHz cnWave

Type
☐ Links ☒ Nodes

Mode
☒ CN ☒ DN

Select data to include in report

☒ **Basic**

<input checked="" type="checkbox"/> Device Mode	<input checked="" type="checkbox"/> Device Name	<input checked="" type="checkbox"/> Device Type	<input checked="" type="checkbox"/> MAC
<input checked="" type="checkbox"/> Network	<input checked="" type="checkbox"/> Timestamp	<input checked="" type="checkbox"/> Site	

☒ **Network**

<input checked="" type="checkbox"/> Ethernet Throughput	<input checked="" type="checkbox"/> Sector Throughput
---	---

Schedule
☒ Now ☐ Daily ☐ Weekly ☐ Monthly (30 days)

Time Range
☒ Last Day ☐ Last Week ☐ Last Month ☐ Custom Time Range

Period ☐
☒ 5 Minutes ☐ 1 Hour ☐ 1 Day

Report generation may take several minutes, depending upon quantity of data.

7. Select the data parameters to include in the report.
8. Select the following options:
 - Schedule type (Now, Daily, Weekly, or Monthly)
 - Time Range (Last Day, Last Week, Last Month, Custom Time Range)
 - Period (5 Minutes, 1 Hour, or 1 Day)
9. Click **Add**. The report is added to the Scheduled Reports page.

60 GHz cnWave Performance Report

Figure 275 Performance Report: 60 GHz cnWave (Links Type)

Type
☒ Links ☐ Nodes

Select data to include in report

☒ **Basic**

<input checked="" type="checkbox"/> Timestamp	<input checked="" type="checkbox"/> Link Name	<input checked="" type="checkbox"/> A-Node Sector MAC	<input checked="" type="checkbox"/> Z-Node Sector MAC
<input checked="" type="checkbox"/> RSSI	<input checked="" type="checkbox"/> SNR	<input checked="" type="checkbox"/> MCS	<input checked="" type="checkbox"/> EIRP
<input checked="" type="checkbox"/> Frame Rate	<input checked="" type="checkbox"/> PER	<input checked="" type="checkbox"/> Scan Beams	<input checked="" type="checkbox"/> Delta (Link Up / Link Available)
<input checked="" type="checkbox"/> Management Link Up	<input checked="" type="checkbox"/> Link Fade Margin		

Figure 276 Performance Report: 60 GHz cnWave (Node Type)

Type
☐ Links ☒ Nodes

Mode
☒ CN ☒ DN

Select data to include in report

☒ **Basic**

<input checked="" type="checkbox"/> Device Mode	<input checked="" type="checkbox"/> Device Name	<input checked="" type="checkbox"/> Device Type	<input checked="" type="checkbox"/> MAC
<input checked="" type="checkbox"/> Network	<input checked="" type="checkbox"/> Timestamp	<input checked="" type="checkbox"/> Site	

☒ **Network**

<input checked="" type="checkbox"/> Ethernet Throughput	<input checked="" type="checkbox"/> Sector Throughput
---	---

cnMatrix Performance Report

Figure 277 Performance Report: cnMatrix

Select data to include in report

☒ **Basic**

<input checked="" type="checkbox"/> CPUs	<input checked="" type="checkbox"/> Device Name	<input checked="" type="checkbox"/> Device Type	<input checked="" type="checkbox"/> MAC
<input checked="" type="checkbox"/> Packet Error	<input checked="" type="checkbox"/> Packets Count (Rx)	<input checked="" type="checkbox"/> Throughput	<input checked="" type="checkbox"/> Timestamp
<input checked="" type="checkbox"/> Packets Count (Tx)			

cnPilot Home (R-Series) Performance Report

Figure 278 Performance Report: cnPilot Home (R-Series)

Select data to include in report

☒ **Basic**

<input checked="" type="checkbox"/> Avg No. Of Mesh Peers	<input checked="" type="checkbox"/> Avg Receive Rate	<input checked="" type="checkbox"/> Avg Send Rate	<input checked="" type="checkbox"/> Avg Usage
<input checked="" type="checkbox"/> Device Mode	<input checked="" type="checkbox"/> Device Name	<input checked="" type="checkbox"/> Device Type	<input checked="" type="checkbox"/> MAC
<input checked="" type="checkbox"/> Max Receive Rate	<input checked="" type="checkbox"/> Max Send Rate	<input checked="" type="checkbox"/> Max Usage	<input checked="" type="checkbox"/> Min Receive Rate
<input checked="" type="checkbox"/> Min Send Rate	<input checked="" type="checkbox"/> Min Usage	<input checked="" type="checkbox"/> Network	<input checked="" type="checkbox"/> No. of Clients
<input checked="" type="checkbox"/> Received Bytes (2.4 GHz)	<input checked="" type="checkbox"/> Received Bytes (5 GHz)	<input checked="" type="checkbox"/> Sent Bytes (2.4 GHz)	<input checked="" type="checkbox"/> Sent Bytes (5 GHz)
<input checked="" type="checkbox"/> Site	<input checked="" type="checkbox"/> Timestamp	<input checked="" type="checkbox"/> Total Received Bytes	<input checked="" type="checkbox"/> Total Sent Bytes

cnRanger Performance Report

Figure 279 Performance Report: cnRanger

Mode
☒ BBU ☒ RRH ☒ SM

Select data to include in report

☒ **Basic**

<input checked="" type="checkbox"/> CPU	<input checked="" type="checkbox"/> Device Mode	<input checked="" type="checkbox"/> Device Name	<input checked="" type="checkbox"/> Device Type
<input checked="" type="checkbox"/> MAC	<input checked="" type="checkbox"/> MCS	<input checked="" type="checkbox"/> Network	<input checked="" type="checkbox"/> RSRP
<input checked="" type="checkbox"/> RSRQ	<input checked="" type="checkbox"/> RSSI	<input checked="" type="checkbox"/> Session Drops	<input checked="" type="checkbox"/> SINR
<input checked="" type="checkbox"/> SM Count	<input checked="" type="checkbox"/> Throughput	<input checked="" type="checkbox"/> Timestamp	<input checked="" type="checkbox"/> Tower

cnReach Performance Report

Figure 280 *Performance Report: cnReach*

Select data to include in report

☒ **Basic**

☒ Device Name ☒ Device Type ☒ MAC ☒ Neighbors

☒ Noise ☒ RSSI ☒ Throughput ☒ Timestamp

cnVision Performance Report

Figure 281 *Performance Report: cnVision*

Mode

☒ Client ☒ Hub

Select data to include in report

☒ **Basic**

☒ Connected AP MAC ☒ CPUs ☒ Device Mode ☒ Device Name

☒ Device Type ☒ DL Frame Utilization ☒ MAC ☒ MCS

☒ Network ☒ Usage (Packet Count) ☒ Retransmission ☒ RSSI

☒ Session Drops ☒ SM Count ☒ SNR ☒ Throughput

☒ Timestamp ☒ Tower

cnWave 5G Fixed Performance Report

Figure 282 *Performance Report: cnWave 5G Fixed*

Mode

☒ BTS ☒ CPE

Select data to include in report

☒ **Basic**

☒ Connected CPEs ☒ Device Mode ☒ Device Name ☒ Device Type

☒ EVM ☒ MAC ☒ MCS ☒ Network

☒ Timestamp ☒ Registered CPEs ☒ Rx Power ☒ Throughput

☒ Tower

Enterprise Wi-Fi

Figure 283 Performance Report: Enterprise Wi-Fi

Select data to include in report

☒ **Basic**

<input checked="" type="checkbox"/> Avg Receive Rate	<input checked="" type="checkbox"/> Avg Send Rate	<input checked="" type="checkbox"/> Avg Usage	<input checked="" type="checkbox"/> Device Mode
<input checked="" type="checkbox"/> Device Name	<input checked="" type="checkbox"/> Device Type	<input checked="" type="checkbox"/> MAC	<input checked="" type="checkbox"/> Max Receive Rate
<input checked="" type="checkbox"/> Max Send Rate	<input checked="" type="checkbox"/> Max Usage	<input checked="" type="checkbox"/> Min Receive Rate	<input checked="" type="checkbox"/> Min Send Rate
<input checked="" type="checkbox"/> Min Usage	<input checked="" type="checkbox"/> Network	<input checked="" type="checkbox"/> No. of Clients	<input checked="" type="checkbox"/> Site
<input checked="" type="checkbox"/> Timestamp	<input checked="" type="checkbox"/> Total Received Bytes	<input checked="" type="checkbox"/> Total Sent Bytes	

☒ **Radio 1**

<input checked="" type="checkbox"/> Airtime	<input checked="" type="checkbox"/> Band	<input checked="" type="checkbox"/> Interference	<input checked="" type="checkbox"/> Noise Floor
<input checked="" type="checkbox"/> Received Bytes	<input checked="" type="checkbox"/> Sent Bytes		

☒ **Radio 2**

☒ **Radio 3**

☒ **Radio 4**

☒ **Radio 5**

☒ **Radio 6**

☒ **Radio 7**

☒ **Radio 8**

ePMP Performance Report

Figure 284 Performance Report: ePMP

Mode
☒ AP ☒ SM

Select data to include in report

☒ **Basic**

<input checked="" type="checkbox"/> Channel Width	<input checked="" type="checkbox"/> Connected AP MAC	<input checked="" type="checkbox"/> CPUs	<input checked="" type="checkbox"/> Device Mode
<input checked="" type="checkbox"/> Device Name	<input checked="" type="checkbox"/> Device Type	<input checked="" type="checkbox"/> DL Frame Utilization	<input checked="" type="checkbox"/> MAC
<input checked="" type="checkbox"/> MCS	<input checked="" type="checkbox"/> Network	<input checked="" type="checkbox"/> Usage (Packet Count)	<input checked="" type="checkbox"/> Retransmission
<input checked="" type="checkbox"/> RF Frequency	<input checked="" type="checkbox"/> RSSI	<input checked="" type="checkbox"/> Session Drops	<input checked="" type="checkbox"/> SM Count
<input checked="" type="checkbox"/> SNR	<input checked="" type="checkbox"/> Throughput	<input checked="" type="checkbox"/> Timestamp	<input checked="" type="checkbox"/> Tower

PMP Performance Report

Figure 285 Performance Report: PMP

Mode
☒ AP ☒ SM

Select data to include in report

☒ **Basic**

<input checked="" type="checkbox"/> BER (Average)	<input checked="" type="checkbox"/> Channel Width	<input checked="" type="checkbox"/> Connected AP MAC	<input checked="" type="checkbox"/> CPU
<input checked="" type="checkbox"/> Device Mode	<input checked="" type="checkbox"/> Device Name	<input checked="" type="checkbox"/> Device Type	<input checked="" type="checkbox"/> EVM
<input checked="" type="checkbox"/> Frame Utilization	<input checked="" type="checkbox"/> LQI	<input checked="" type="checkbox"/> MAC	<input checked="" type="checkbox"/> Modulation
<input checked="" type="checkbox"/> Multiplex Gain	<input checked="" type="checkbox"/> Network	<input checked="" type="checkbox"/> RF Frequency	<input checked="" type="checkbox"/> RSSI
<input checked="" type="checkbox"/> RSSI Imbalance	<input checked="" type="checkbox"/> Session Drops	<input checked="" type="checkbox"/> SM Count	<input checked="" type="checkbox"/> SNR
<input checked="" type="checkbox"/> Temperature	<input checked="" type="checkbox"/> Throughput	<input checked="" type="checkbox"/> Timestamp	<input checked="" type="checkbox"/> Tower

PON Performance Report

Figure 286 *Performance Report: PON*

Mode
☒ OLT ☒ ONU

Select data to include in report
☒ **Basic**

☒ BER (Average)

☒ CPU

☒ Device Name

☒ Device Type

☒ Downlink Throughput

☒ MAC

☒ Memory

☒ Connected OLT MAC

☒ Timestamp

☒ Receive Power

☒ Temperature

☒ Uplink Throughput

The modulation mappings for the PMP device are as follows:

Figure 287 *Mapping PMP*

Value	Description
-1	N/A
0	1X MIMO-A
1	2X MIMO-A
2	3X MIMO-A
3	4X MIMO-A
4	2X MIMO-B
5	3X MIMO-B
6	4X MIMO-B
7	5X MIMO-B
8	6X MIMO-B
9	7X MIMO-B
10	8X MIMO-B

Figure 288 *PMP 450m*

Value	Description
0	N/A
1	1X MIMO-A
2	2X MIMO-A
3	3X MIMO-A
4	4X MIMO-A

Figure 289 *PMP 450m*

Value	Description
0	N/A
2	2X MIMO-B
3	3X MIMO-B
4	4X MIMO-B
5	5X MIMO-B

Value	Description
6	6X MIMO-B
7	7X MIMO-B
8	8X MIMO-B

Figure 290 PMP 430

Value	Description
-1	N/A
0	1X SISO
1	2X SISO
2	3X SISO

Figure 291 PMP 450v

Value	Description
0	N/A
2	2X MIMO-B
3	3X MIMO-B
4	4X MIMO-B
5	5X MIMO-B
6	6X MIMO-B
7	7X MIMO-B
8	8X MIMO-B

PTP 650/670/700 Performance Report

Figure 292 Performance Report: PTP 650/670/700

Select data to include in report

☒ **Basic**

☒ Capacity
☒ Device Name
☒ Device Type
☒ Link Loss

☒ MAC
☒ Power
☒ Receive SSI
☒ Throughput

☒ Timestamp
☒ Vector Error

PTP 820/850 Performance Report

Figure 293 Performance Report: PTP 820/850

Select data to include in report

☒ **Basic**

☒ Device Name ☒ Device Type ☒ MAC ☒ Network
☒ Timestamp ☒ Tower

☒ **Radio Slot 1**

☒ Modem MSE ☒ Modem XPI ☒ MRMC Profile ☒ Peak Throughput
☒ Signal Level ☒ Throughput

☒ **Radio Slot 2**

☒ Modem MSE ☒ Modem XPI ☒ MRMC Profile ☒ Peak Throughput
☒ Signal Level ☒ Throughput

☒ **Radio Groups**

☒ Peak Throughput ☒ Throughput

RV22 Home Mesh Performance Report

Figure 294 Performance Report: RV22 Home Mesh

Select data to include in report

☒ **Basic**

☒ Avg Receive Rate ☒ Avg Send Rate ☒ Avg Usage ☒ Device Mode
☒ Device Name ☒ Device Type ☒ MAC ☒ Max Receive Rate
☒ Max Send Rate ☒ Max Usage ☒ Min Receive Rate ☒ Min Send Rate
☒ Min Usage ☒ Network ☒ No. of Clients ☒ Site
☒ Timestamp ☒ Total Received Bytes ☒ Total Sent Bytes

Active Alarms Report

The Active Alarms Report will export the data for the active alarms at the report generation time. Active alarms for all devices under the tree node will be included in the export.

To generate the Active Alarms reports, perform the following steps:

1. Navigate to **Reports X > Scheduled** tab.
2. Enter a **Name** and **Description** for the report.
3. Enter email addresses (maximum of 5) in the **Recipients** field to send reports.
4. Select the **Report Type** as *Active Alarms*.
5. Select data parameters to include in the report.
6. Select the following options:
 - Schedule type (Now, Daily, Weekly, or Monthly)

- Click **Add**. The report gets added to the Scheduled Reports page.

Reports > Add Report

Generate report for active alarms as a comma-separated value (CSV) file. Active alarms for all devices under the tree node will be included in the export. [Learn More](#)

Name*

Description

Recipients

Type*

Schedule

Report generation may take several minutes, depending upon quantity of data.

Add Cancel

Alarm History Report

The Alarm History Report will generate data for all alarms that were active at any time within the time period. Alarms for all devices under the tree node selected will be included.

To generate the Alarms History reports, perform the following steps:

- Navigate to **Reports X > Scheduled** tab.
- Enter a **Name** and **Description** for the report.
- Enter email addresses (maximum of 5) in the **Recipients** field to send reports.
- Select the **Report Type** as Alarms History.
- Select data parameters to include in the report.
- Select the following options:
 - Schedule type (Now, Daily, Weekly, or Monthly)
 - Time Range (Last Day, Last Week, Last Month, Custom Time Range)
- Click **Add**. The report gets added to the **Scheduled Reports** page.

8. Click **View Jobs** to view the reports.

Reports > Add Report

Generate report for all alarms that were active at any time within the time period selected. Alarms for all devices under the tree node selected will be included in the export. [Learn More](#)

Name*

Description

Recipients
 Enter valid email and press enter (max 5 recipients)

Type*

☒ **Basic**

<input checked="" type="checkbox"/> Acknowledged By	<input checked="" type="checkbox"/> Clear Time	<input checked="" type="checkbox"/> Duration	<input checked="" type="checkbox"/> IP Address
<input checked="" type="checkbox"/> IPv6 Address	<input checked="" type="checkbox"/> MAC	<input checked="" type="checkbox"/> Message	<input checked="" type="checkbox"/> Name
<input checked="" type="checkbox"/> Raised Time	<input checked="" type="checkbox"/> Severity	<input checked="" type="checkbox"/> Source	<input checked="" type="checkbox"/> Source Type
<input checked="" type="checkbox"/> Status			

Schedule
☒ Now ☐ Daily ☐ Weekly ☐ Monthly (30 days)

Time Range
☒ Last Day ☐ Last Week ☐ Last Month ☐ Custom Time Range

Report generation may take several minutes, depending upon quantity of data.

Events Report

The Events Report is generated for the events raised during the time period. Events for devices under the tree node will be included in the export.

To generate the Events reports, perform the following steps:

1. Navigate to **Reports X > Scheduled** tab.
2. Enter a **Name** and **Description** for the report.
3. Enter email addresses (maximum of 5) in the **Recipients** field to send reports.
4. Select the **Report Type** as Events.
5. Select data parameters to include in the report.
6. Select the following options:
 - Schedule type (Now, Daily, Weekly, or Monthly)
 - Time Range (Last Day, Last Week, Last Month, Custom Time Range)

- Click **Add**. The report gets added to the **Scheduled Reports** page.

Reports > Add Report

Generate report for all events raised during the time period selected. Events for devices under the tree node will be included in the export. [Learn More](#)

Name*

Description

Recipients
 Enter valid email and press enter (max 5 recipients)

Type*

☒ Basic

<input checked="" type="checkbox"/> Category	<input checked="" type="checkbox"/> IP Address	<input checked="" type="checkbox"/> IPv6 Address	<input checked="" type="checkbox"/> MAC
<input checked="" type="checkbox"/> Message	<input checked="" type="checkbox"/> Name	<input checked="" type="checkbox"/> Raised Time	<input checked="" type="checkbox"/> Severity
<input checked="" type="checkbox"/> Source	<input checked="" type="checkbox"/> Source Type	<input checked="" type="checkbox"/> Event Type	

Schedule
☒ Now ☐ Daily ☐ Weekly ☐ Monthly (30 days)

Time Range
☒ Last Day ☐ Last Week ☐ Last Month ☐ Custom Time Range

ⓘ Report generation may take several minutes, depending upon quantity of data.

Wireless Clients Report

The Wireless Clients report generates data for Wi-Fi clients.



Note

Client Data is available for the last day, last 24 hours, last week, and a maximum of 30 days.

To generate the Wireless Clients reports, perform the following steps:

- Navigate to **Reports X > Scheduled** tab.
- Click **Add New Data Report**.
The Add Report page appears.
- Enter a **Name** and **Description** for the report.
- Enter email addresses (maximum of 5) in the **Recipients** field to send reports.
- Select the **Report Type** as Wireless Clients.
- Select data parameters to include in the report.
- Select the following options:
 - Schedule type (Now, Daily, Weekly, or Monthly (30 days))
 - Time Range (Last Day, Last Week, Last Month, or Custom Time Range (up to a maximum of 30 days))
- Click **Add**. The report is saved and listed in the **Scheduled Reports** page.

Figure 295 *Wireless Clients Report*

Reports > Add Report

Generate report for clients data [Learn More](#)

Name*

Description

Recipients

Type*

Wireless Clients

☒ **Basic**

<input checked="" type="checkbox"/> AP	<input checked="" type="checkbox"/> Average Signal	<input checked="" type="checkbox"/> Average Signal Quality	<input checked="" type="checkbox"/> Average Usage
<input checked="" type="checkbox"/> Avg Receive Rate (Kbps)	<input checked="" type="checkbox"/> Avg Transmit Rate (Kbps)	<input checked="" type="checkbox"/> Band	<input checked="" type="checkbox"/> Capability
<input checked="" type="checkbox"/> Client Class	<input checked="" type="checkbox"/> Client MAC	<input checked="" type="checkbox"/> Client OS	<input checked="" type="checkbox"/> Client Type
<input checked="" type="checkbox"/> Duration	<input checked="" type="checkbox"/> Hostname	<input checked="" type="checkbox"/> IP Address	<input checked="" type="checkbox"/> IPv6 Address
<input checked="" type="checkbox"/> Last Seen	<input checked="" type="checkbox"/> Max Receive Rate (Kbps)	<input checked="" type="checkbox"/> Max Transmit Rate (Kbps)	<input checked="" type="checkbox"/> Max Usage (Kbps)
<input checked="" type="checkbox"/> Manufacturer	<input checked="" type="checkbox"/> Min Receive Rate (Kbps)	<input checked="" type="checkbox"/> Min Transmit Rate (Kbps)	<input checked="" type="checkbox"/> Min Usage (Kbps)
<input checked="" type="checkbox"/> Radio Mode	<input checked="" type="checkbox"/> Radio ID	<input checked="" type="checkbox"/> Rate	<input checked="" type="checkbox"/> RSSI
<input checked="" type="checkbox"/> Rx Rate	<input checked="" type="checkbox"/> SNR	<input checked="" type="checkbox"/> SSID	<input checked="" type="checkbox"/> Total Receive Traffic
<input checked="" type="checkbox"/> Total Traffic	<input checked="" type="checkbox"/> Total Transmit Traffic	<input checked="" type="checkbox"/> Tx Rate	<input checked="" type="checkbox"/> User
<input checked="" type="checkbox"/> VLAN-ID			

☒ **Last Known**

<input checked="" type="checkbox"/> Association Time	<input checked="" type="checkbox"/> Device Name	<input checked="" type="checkbox"/> Dissociation Time	<input checked="" type="checkbox"/> Network
<input checked="" type="checkbox"/> Site Name			

Schedule

☒ Now ☐ Daily ☐ Weekly ☐ Monthly (30 days)

Time Range

☒ Last Day ☐ Last Week ☐ Last Month ☐ Custom Time Range

Report generation may take several minutes, depending upon quantity of data.

Wi-Fi Events Report



Note

Wi-Fi events data is available for a maximum of seven days.

The Wi-Fi Events report generates the Wi-Fi events data that is available on the **Notifications > Wi-Fi Events** page.

To generate the Wi-Fi Events reports, perform the following steps:

1. Navigate to **Reports X > Scheduled** tab.
2. Click **Add New Data Report**.
The Add Report page appears.
3. Enter a **Name** and **Description** for the report.
4. Enter email addresses (maximum of 5) in the **Recipients** field to send reports.
5. Select the **Report Type** as Wi-Fi Events.
6. Select data parameters to include in the report.

Select the required checkboxes.

7. Select the following options:

- Schedule type (Now, Daily, or Weekly)
- Time Range (Last Day, Last Week, or Custom Range (up to a maximum of seven days))

8. Click **Add**. The report is saved and listed in the **Scheduled Reports** page.

Figure 296 *Wi-Fi Events Report*

[Reports](#) > Add Report

Generate report for Wi-Fi events raised during the time period selected. Events for devices under the tree node will be included in the export. [Learn More](#)

Name*

Description

Recipients
 Enter valid email and press enter (Max 5 recipients)

Type*

☒ **Basic**

☒ Client MAC ☒ Client Name ☒ Name ☒ Raised Time
☒ Source ☒ Source MAC ☒ Source Type

Schedule
☒ Now ☐ Daily ☐ Weekly

Time Range
☒ Last Day ☐ Last Week ☐ Custom Time Range

Report generation may take several minutes, depending upon quantity of data.

Guest Access Login Events

The Guest Access Login Events represent Wi-Fi guest access logins.

Note

- Guest access report can be generated only at the system level.
- Guest access login data is available for a maximum of 90 days.

To generate the Guest Access Login Events report, perform the following steps:

1. Navigate to **Report X > Scheduled** tab.
2. Enter a **Name** and **Description** for the report.
3. Enter email addresses (maximum of 5) in the **Recipients** field to send reports.
4. Select the **Report Type** as Guest Access Login Events.
5. Select the **Managed Account**, if applicable.
6. Select the **Guest Access Portal**, if applicable.
7. Select data parameters to include in the report.
8. Select the following options:

- Schedule type (Now, Daily, Weekly, or Monthly (30 days))
- Time Range (Last Day, Last Week, Last Month, or Custom Time Range (up to a maximum of 90 days))

9. Click **Add**. The report gets added to the **Scheduled Reports** page.

[Reports](#) > Add Report

Generate Report for Guest Access Login Events [Learn More](#)

Name*

Description

Recipients
 Enter valid email and press enter (Max 5 recipients)

Type*

Guest Access Login Events

Managed Account

All Accounts

Guest Access Portal

All Guest Access Portals

Select data to include in report

☒ **Basic**

☒ Access Type
 ☒ Access Point
 ☒ Client MAC
 ☒ Email

☒ Guest Access Portal
 ☒ ID
 ☒ Login Time
 ☒ Mobile Number

☒ Name
 ☒ SSID
 ☒ User Info
 ☒ Voucher Code

Schedule

☒ Now
 ☐ Daily
 ☐ Weekly
 ☐ Monthly (30 days)

Time Range

☒ Last Day
 ☐ Last Week
 ☐ Last Month
 ☐ Custom Time Range

ⓘ Report generation may take several minutes, depending upon quantity of data.

Add

Cancel

Report Jobs

The report jobs displays the list of scheduled jobs created by different users. To view jobs, navigate to **Administration > Jobs > Reports**.

Figure 297 *Report Jobs*

Administration > Jobs											
Configuration Update Software Update Reports X Actions											
Displays the list of scheduled reports created by different users. Learn more											
Managed Account: All Accounts Delete											
<input type="checkbox"/>	ID	Type	Managed Account	Source	Schedule	Starts At	Ends After	Created by	Created on	Status	Last Report
<input type="checkbox"/>	1858	Alarm History	TEST_ALARM_HIS1	System	Monthly	03 Aug 2023, 04:...	23 Feb 2025, 04:...	N...	03 Aug 2023, 04:...	Scheduled (02 Sep 2023, 04:...	03 Aug 2023,...
<input type="checkbox"/>	1857	Alarm History	TEST_ALARM_HIS1	System	Weekly	03 Aug 2023, 04:...	14 Dec 2023, 04:...	N...	03 Aug 2023, 04:...	Scheduled (10 Aug 2023, 04:...	03 Aug 2023,...
<input type="checkbox"/>	1856	Alarm History	TEST_ALARM_HIS1	System	Daily	03 Aug 2023, 04:...	22 Aug 2023, 04:...	N...	03 Aug 2023, 04:...	Scheduled (04 Aug 2023, 04:...	03 Aug 2023,...
<input type="checkbox"/>	1855	Graphical Re...	All Accounts	System	Daily	03 Aug 2023, 01:...	04 Aug 2023, 04:...	Le...	03 Aug 2023, 04:...	Scheduled (04 Aug 2023, 01:...	03 Au...
<input type="checkbox"/>	1854	Graphical Re...	All Accounts	System	Daily	03 Aug 2023, 02:...	04 Aug 2023, 04:...	Se...	03 Aug 2023, 04:...	Scheduled (04 Aug 2023, 02:...	03 Aug 2023,...
<input type="checkbox"/>	1853	Graphical Re...	All Accounts	System	Now	03 Aug 2023, 04:...	03 Aug 2023, 04:...	Se...	03 Aug 2023, 04:...	Completed	03 Aug 2023,...
<input type="checkbox"/>	1852	Alarm History	Imanaged	System	Monthly	03 Aug 2023, 04:...	29 Apr 2024, 04:...	N...	03 Aug 2023, 04:...	Scheduled (02 Sep 2023, 04:...	03 Aug 2023,...
<input type="checkbox"/>	1851	Alarm History	Imanaged	System	Daily	03 Aug 2023, 04:...	12 Aug 2023, 04:...	N...	03 Aug 2023, 03:...	Scheduled (04 Aug 2023, 04:...	03 Aug 2023,...
<input type="checkbox"/>	1850	Alarm History	NBN_MSP	System	Monthly	03 Aug 2023, 04:...	29 Apr 2024, 04:...	N...	03 Aug 2023, 03:...	Scheduled (02 Sep 2023, 04:...	03 Aug 2023,...
<input type="checkbox"/>	1849	Active Alarms	Reports	System	Weekly	03 Aug 2023, 03:...	05 Oct 2023, 03:...	N...	03 Aug 2023, 03:...	Scheduled (10 Aug 2023, 03:...	03 Aug 2023,...
Showing 1 - 10 Total: 1,588 10 < Previous 1 2 3 4 5 ... 159 Next >											

A scheduled report job displays the following **Action** buttons:

- **Edit:** Visible only for **Active Jobs** which have not yet run. You can reschedule a job with this option.
- **Terminate:** Stop the **Active Jobs**.
- **Show History:** Display the detailed status of the generated reports and the file transfer status.
- **Delete:** Delete **Active** and **Completed Jobs**.
- **Instant Download:** Download the latest report without checking the **Show History**.

Graphical Reports

The data reports contain a lot of data that need to be represented graphically so that you can quickly summarize and get a better visualization. In such cases, you can use the Graphical Reports. Graphical Reports can be created by first building a template of the report you want to view, optionally with your own branding such as your logo and brand name. Then, apply the template at a level in the hierarchical tree in cnMaestro such managed service, system, or site. Each graphical report can consist of multiple pages called widgets. The following widgets are available with applicable type of graphs and charts based on context. Each widget has both a graphical and tabular representation of the data. The output is a PDF file.

[Figure 298](#) lists the Graphical Reports widgets available in cnMaestro and the version they were introduced in.

Figure 298 List of Graphical Reports widgets available

Name of Widget	Version Introduced
Assurance	
Assurance: Top Access Points Reporting Client Disconnections—Top APs reporting client disconnections	4.1.0
Assurance: Top Client Connection Failures—Top client connection failure types by number of failures	4.1.0
Assurance: Top Affected Client OS by Failure Count	5.2.0
Assurance: Top Affected Client Types by Failure Count	5.2.0
Access Points	
Top Access Points by Traffic Usage—Top APs by traffic usage	5.1.0
Clients	
6E Clients by Radio—Comparison between 6E Clients on 6 GHz radios and other radios	4.1.0
Client Capability Trend—Count of clients based on their Wi-Fi capabilities over time	4.1.0
Client Count by Band—Client count by band	4.1.0
Client Count by Manufacturers—Top manufacturers by number of clients	4.1.0
Client Count over Time—Connected clients by band over time	4.1.0
Client Traffic over Time—Client uplink and downlink speeds over time	4.1.0
Peak and Unique Clients—Total unique clients and peak time number of unique clients	4.1.0
Top Applications by Usage—Top applications by data usage	4.1.0
Top Access Points by Unique Clients—Top APs by unique clients	4.1.0
Top Category by Usage—Top applications category by data usage	4.1.0
Client Count by OS—Top client types by number of clients	5.1.0
Top Application Category by Client Count—Top application category by number of unique clients	5.1.0

Name of Widget	Version Introduced
Top Applications by Client Count—Top applications by number of clients	5.1.0
Top Client Types by Traffic Usage—Top client types by traffic usage	5.1.0
Top Sites by Client Count—Top sites by number of clients	5.1.0
Top Sites by Traffic Usage—Top sites by traffic usage	5.1.0
Top SSIDs by Client Count—Top SSIDs by number of clients	5.1.0
Top SSIDs by Traffic Usage—Top SSIDs by traffic usage	5.1.0
Top Clients by Traffic Usage—Top clients by traffic usage	5.1.0
Top Managed Accounts by Traffic Usage—Top managed accounts by traffic usage	5.1.0

The standard process for graphical report generation includes the following:

1. Create a template using the widgets listed above.
2. Select a level of the hierarchy on which to apply the template.
3. Schedule the report to either execute one-time or periodically.



Note

- Graphical reports are only supported for Wi-Fi APs and clients, and they can only be applied at the Managed Service, System, and Site levels.
- If there is no data for the specific period, then a blank page is displayed in the PDF.
- The title page of the PDF displays the date and time zone of the user who scheduled the report.
- Data is available for a maximum of 30 days.

The **Scheduled** tab presents reports pending execution, and the **Completed** tab provides access to reports that have finished running. The already generated reports are listed as **Completed Reports** (includes Success and Failed status in the status column) and those that are not yet generated but scheduled for a future time are listed as **Scheduled reports** (includes and Future and Terminated status in the status column).

System											
Dashboard Notifications Configuration Statistics Reports X Software Update Applications X Clients Mesh Peers Assurance X Assists X											
Scheduled Completed											
Displays the list of Scheduled/Terminated/Timeout reports created under the tree node selected. Learn More											
<div> Add New Graphical Report Add New Data Report Delete </div>											
ID	Name	Report	Type	Schedule	Managed Account	Created by	Created on	Starts At	Status	Next Scheduled Time	
479	lastmonth	Graphical	-	Monthly (30 ...	All Accounts		16 Apr 2025, 03:44 PM	16 Apr 2025, 07:45 P...	Scheduled	16 May 2025, 07:45 PM	✓ ⌵ ⌶ ⌵
477	lastweek	Graphical	-	Weekly	All Accounts		16 Apr 2025, 03:43 PM	16 Apr 2025, 08:00 ...	Scheduled	30 Apr 2025, 08:00 PM	✓ ⌵ ⌶ ⌵
469	MSP1	Graphical	-	Monthly (30 ...	Megha_MSP		16 Apr 2025, 03:38 PM	16 Apr 2025, 05:30 ...	Scheduled	16 May 2025, 05:30 PM	✓ ⌵ ⌶ ⌵
435	PON-Devices-Perf...	Data	Perform...	Daily	Base Infrastru...		16 Apr 2025, 12:18 PM	16 Apr 2025, 12:23 PM	Scheduled	30 Apr 2025, 12:23 PM	✓ ⌵ ⌶ ⌵
417	Audit_Weekly	Data	Audit Lo...	Weekly	All Accounts		16 Apr 2025, 10:06 AM	16 Apr 2025, 10:12 AM	Scheduled	07 May 2025, 10:12 AM	✓ ⌵ ⌶ ⌵
415	GR-16-4-25-Weekly	Graphical	-	Weekly	All Accounts		16 Apr 2025, 10:05 AM	16 Apr 2025, 10:10 AM	Scheduled	07 May 2025, 10:10 AM	✓ ⌵ ⌶ ⌵
414	GR-16-4-25-Daily	Graphical	-	Daily	All Accounts		16 Apr 2025, 10:04 AM	16 Apr 2025, 10:09 AM	Scheduled	01 May 2025, 10:09 AM	✓ ⌵ ⌶ ⌵
365	PON-DP2-P	⊕ Data	Perform...	Daily	Base Infrastru...		15 Apr 2025, 12:31 PM	15 Apr 2025, 09:16 PM	Scheduled	30 Apr 2025, 09:16 PM	✓ ⌵ ⌶ ⌵
364	PON-DP1	⊕ Data	Devices	Daily	Base Infrastru...		15 Apr 2025, 12:29 PM	15 Apr 2025, 09:15 PM	Scheduled	30 Apr 2025, 09:15 PM	✓ ⌵ ⌶ ⌵
352	60Ghz perf nodes ...	Data	Perform...	Daily	All Accounts		15 Apr 2025, 10:43 AM	15 Apr 2025, 10:49 AM	Scheduled	01 May 2025, 10:49 AM	✓ ⌵ ⌶ ⌵
Showing 1 - 10 Total: 36 10 < Previous 1 2 3 4 Next >											

System										
Dashboard Notifications Configuration Statistics Reports X Software Update Applications X Clients Mesh Peers Assurance X Assists X										
Scheduled Completed										
Displays the list of Completed/Failed reports created under the tree node selected. Learn More										
Delete										
<input type="checkbox"/>	ID	Name	Report	Type	Sched...	Managed Account	Created by	Status	Generated on	
<input type="checkbox"/>	50	events_daily	Data	Events	Daily	Base Infrastru...		Completed	30 Apr 2025, 10:54 AM	Download Delete
<input type="checkbox"/>	352	60Ghz perf nodes ...	Data	Perform...	Daily	All Accounts		Completed	30 Apr 2025, 10:49 AM	Download Delete
<input type="checkbox"/>	351	60GHz daily devic...	Data	Devices	Daily	All Accounts		Completed	30 Apr 2025, 10:48 AM	Download Delete
<input type="checkbox"/>	415	GR-16-4-25-Weekly	Graphical	-	Weekly	All Accounts		Completed	30 Apr 2025, 10:14 AM	Download Delete
<input type="checkbox"/>	417	Audit_Weekly	Data	Audit Lo...	Weekly	All Accounts		Completed	30 Apr 2025, 10:13 AM	Download Delete
<input type="checkbox"/>	414	GR-16-4-25-Daily	Graphical	-	Daily	All Accounts		Completed	30 Apr 2025, 10:11 AM	Download Delete
<input type="checkbox"/>	365	PON-DP2-P	Data	Perform...	Daily	Base Infrastru...		Completed	29 Apr 2025, 09:16 PM	Download Delete
<input type="checkbox"/>	364	PON-DP1	Data	Devices	Daily	Base Infrastru...		Completed	29 Apr 2025, 09:15 PM	Download Delete
<input type="checkbox"/>	176	KK	Data	Devices	Daily	All Accounts		Completed	29 Apr 2025, 05:15 PM	Download Delete
<input type="checkbox"/>	242	Lastday_MSP	Graphical	-	Daily	Megha_MSP		Completed	29 Apr 2025, 05:01 PM	Download Delete
Showing 1 - 10 Total: 1016 10 < Previous 1 2 3 4 5 ... 102 Next >										

Refer to the following topics to create templates and schedule reports:

- [Create Graphical Report Templates](#)
- [Generate Reports Based on Templates](#)

Create Graphical Report Templates

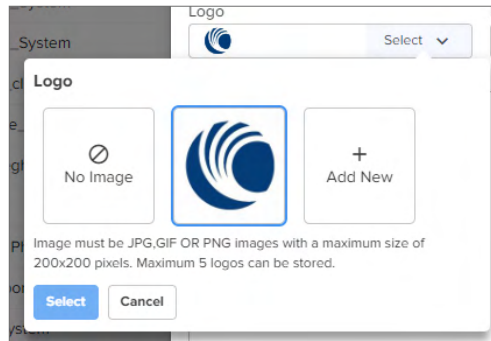
To create a graphical report template, complete the following steps:

1. Navigate to **Configuration > Graphical Report Template X** page.

Configuration > Graphical Report Template x						
Displays the list of Graphical Report templates. Learn More						
Apply Filter(s) Add New Delete						
<input type="checkbox"/>	Name	Title	Description	Scope	Created by	
<input type="checkbox"/>	SITE	SITE		Site		Copy Edit Delete
<input type="checkbox"/>	SYSTEM	SYSTEM		System		Copy Edit Delete
<input type="checkbox"/>	_MSP_SYSTEM	_MSP		System		Copy Edit Delete
Showing 1 - 3 Total: 3 10 < Previous 1 Next >						

2. Click **Add New** and complete the following details:
 - **Name**—Enter a meaningful name for the template.
 - **Scope**—Select the scope of the report such as **System** or **Site** from the dropdown list.
Depending on the scope selected, different widgets are available under the **Add New** window.
 - **Title**—Enter the title that you want to see in the Title page of the generated PDF document.
 - **Description**—Optionally, describe the report in details.
3. Optionally, brand the report as per your requirement.

- **Logo**—To select an existing logo, click the down arrow and then click **Select**. You can also add a new logo by clicking **Add New**.



- **Brand Image**—To select an existing brand image, click the down arrow, and then click **Select**. You can also add a new brand image by clicking **Add New**.
- **Themes**—Select a theme for the title page of the report as either **Vertical Lines**, **Brand Box**, or **Plain**.



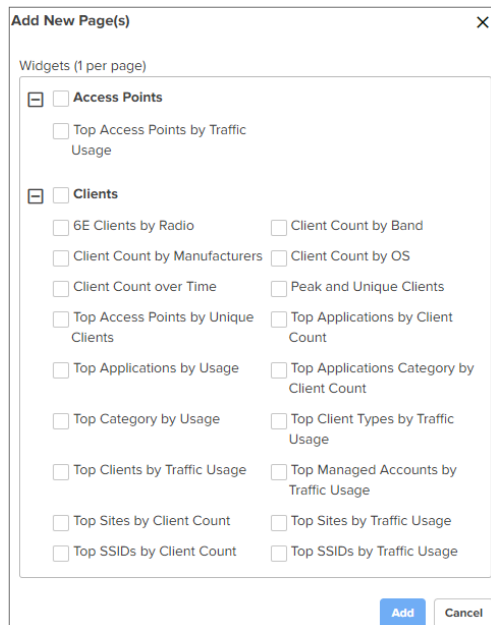
- **Theme Color**—Select the Theme Color by clicking the desired colored square.

4. Click **Add**.

The report template design page is displayed. You can add one or more widgets to the report, one per page.

5. Click **Add New** in the left pane. The following widgets are available:

- For the **System** scope:



- For the **Site** scope:

Add New Page(s)
X

Widgets (1 per page)

☐ Assurance

☐ Assurance: Top Access Points Reporting Client Disconnections
☐ Assurance: Top Affected Client OS by Failure Count
☐ Assurance: Top Affected Client Types by Failure Count
☐ Assurance: Top Client Connection Failures

☐ Access Points

☐ Top Access Points by Traffic Usage

☐ Clients

☐ 6E Clients by Radio
☐ Client Capability Trend
☐ Client Count by Band
☐ Client Count by Manufacturers
☐ Client Count by OS
☐ Client Count over Time
☐ Client Traffic over Time
☐ Peak and Unique Clients
☐ Top Access Points by Unique Clients
☐ Top Applications by Client Count
☐ Top Applications by Usage
☐ Top Applications Category by Client Count
☐ Top Category by Usage
☐ Top Client Types by Traffic Usage
☐ Top Clients by Traffic Usage
☐ Top SSIDs by Client Count
☐ Top SSIDs by Traffic Usage

Cancel
Add

6. Select the checkbox for one or more **Widgets** and click **Add**. Each page can have only one widget. Drag and drop the pages in the left pane to rearrange the widgets.



7. For each page, select the page properties in the right pane. They differ based on widget and options that you have chosen.

The **Duration** parameter supports the following options—**Last Day**, **Last 7 days**, and **Last 30 days**.

Page Property

Description

Duration

Last 7 days

Delete Page

Chart

Data Limit*

Top 5

Graph Style*

Horizontal Bar

8. You can also select the Table columns for each page.

Table

Data Limit*

Top 5

Sort By*

Total Usage

Columns(Max 4 Columns Can Be Selected)

Application Name

Category

Usage (%)

Total Usage

Downlink

Uplink

The following options are available based on the page type:

- **Title**—Title for the report.
- **Description**—Detailed information about the report criteria.
- **Duration**— Time interval. For example, **Last Day** or **Last 7 Days**.
- **Chart/Graph Style**— Type of graph. For example, **Horizontal Bar** or **Pie Chart**
- **Data Limit**—Volume of data to be filtered. For example, **Top 5** or **Top 10**.
- **Sort By**—Column name in the tabular format. For example, **Count**, or **Total Usage**.

9. Click **Save**.

Generate Reports Based on Templates

To add a new report, follow the steps below:

1. Navigate to **Monitor and Manage > System** or **Site > Reports X > Scheduled** tab.

System

Dashboard

Notifications

Configuration

Statistics

Reports X

Software Update

Applications X

Clients

Mesh Peers

Assurance X

Assists X

Scheduled

Completed

Displays the list of Scheduled/Terminated/Timeout reports created under the tree node selected. [Learn More](#)

Add New Graphical Report

Add New Data Report

Delete

ID	Name	Report	Type	Schedule	Managed Account	Created by	Created on	Starts At	Status	Next Scheduled Time				
479	lastmonth	Graphical	-	Monthly (30 ...	All Accounts		16 Apr 2025, 03:44 PM	16 Apr 2025, 07:45 P...	Scheduled	16 May 2025, 07:45 PM	✓	🔄	🗑️	📄
477	lastweek	Graphical	-	Weekly	All Accounts		16 Apr 2025, 03:43 PM	16 Apr 2025, 08:00 ...	Scheduled	30 Apr 2025, 08:00 PM	✓	🔄	🗑️	📄
469	MSP1	Graphical	-	Monthly (30 ...	Megha_MSP		16 Apr 2025, 03:38 PM	16 Apr 2025, 05:30 ...	Scheduled	16 May 2025, 05:30 PM	✓	🔄	🗑️	📄
435	PON-Devices-Perf...	Data	Perform...	Daily	Base Infrastru...		16 Apr 2025, 12:18 PM	16 Apr 2025, 12:23 PM	Scheduled	30 Apr 2025, 12:23 PM	✓	🔄	🗑️	📄
417	Audit_Weekly	Data	Audit Lo...	Weekly	All Accounts		16 Apr 2025, 10:06 AM	16 Apr 2025, 10:12 AM	Scheduled	07 May 2025, 10:12 AM	✓	🔄	🗑️	📄
415	GR-16-4-25-Weekly	Graphical	-	Weekly	All Accounts		16 Apr 2025, 10:05 AM	16 Apr 2025, 10:10 AM	Scheduled	07 May 2025, 10:10 AM	✓	🔄	🗑️	📄
414	GR-16-4-25-Daily	Graphical	-	Daily	All Accounts		16 Apr 2025, 10:04 AM	16 Apr 2025, 10:09 AM	Scheduled	01 May 2025, 10:09 AM	✓	🔄	🗑️	📄
365	PON-DP2-P	Data	Perform...	Daily	Base Infrastru...		15 Apr 2025, 12:31 PM	15 Apr 2025, 09:16 PM	Scheduled	30 Apr 2025, 09:16 PM	✓	🔄	🗑️	📄
364	PON-DP1	Data	Devices	Daily	Base Infrastru...		15 Apr 2025, 12:29 PM	15 Apr 2025, 09:15 PM	Scheduled	30 Apr 2025, 09:15 PM	✓	🔄	🗑️	📄
352	60Ghz perf nodes ...	Data	Perform...	Daily	All Accounts		15 Apr 2025, 10:43 AM	15 Apr 2025, 10:49 AM	Scheduled	01 May 2025, 10:49 AM	✓	🔄	🗑️	📄

Showing 1 - 10 Total: 36 10 < Previous 1 2 3 4 Next >

2. Click **Add New Graphical Report**.

Reports > Add Report

Generate Graphical report using user defined template as PDF file. Data for devices under the tree node selected will be included in the report. [Learn More](#)

Name*

Description

Template*
 [Add New](#)

Recipients
 Enter valid email and press enter (Max 5 recipients)

Schedule
☐ Now ☒ Daily ☐ Weekly ☐ Monthly (30 days)

Start Date **Start Time**

End
 Occurrences (1-100)

ⓘ Report generation may take several minutes, depending upon quantity of data.

3. Complete the following details:

- **Name**—Enter a name for the report.
- **Description**—Enter a detailed description for the report.
- **Template**—Select the PDF template from the dropdown list. If there is no template listed, click **Add New** to create a new PDF template.
- **Recipients**—Add email addresses of the recipients to whom the report is applicable.
- **Schedule**—Select a schedule to generate the report from the following options:
 - **Now**—Generate the report immediately after you click **Add**.
 - **Daily**—Generate the report at the following interval:
 - **Start Date**—Select the date.
 - **Start Time**—Select the time.
 - **End**—Stop generating this report:
 - **After**—Enter the number of instances. The maximum is 100 instances.
 - **By**—Select the date when the report generations should be completely stopped.
 - **Weekly**—Generates the report at the following interval.
 - **Monthly**—Generates the report at the following interval.

4. Click **Schedule**. Adds the report to the list of Scheduled Reports.

Provisioning

The Provisioning chapter includes both Device Software Update and Configuration. It includes the following topics:

- [Software Update](#)
- [Fixed Wireless Configuration](#)
- [Wireless LAN Configuration](#)
- [Switch Groups Configuration](#)
- [60 GHz cnWave Configuration](#)
- [NSE 3000 Configuration](#)
- [Configuring Advanced Features](#)

Software Update

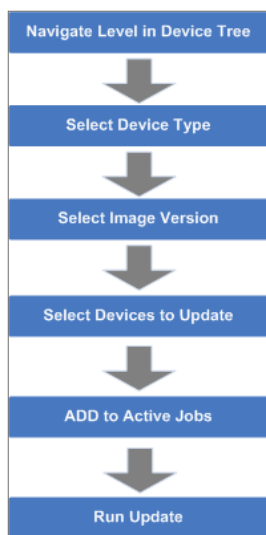
The **Software Update** tab displays the device update details. This section includes the following:

- [Software Update Overview](#)
- [Create Software Update Job](#)
- [Software Update Jobs and Parameters](#)
- [Viewing Running Jobs in header](#)

Software Update Overview

The Software Update feature allows users to deploy the latest software images to devices. Software updates can be started at any level in the Device Tree. Updates are created as Jobs and placed into the Jobs Queue. When the update is ready to run, it can be started. The process flow of Software Update is shown below:

Figure 299 *Software Update Overview*



When a Job completes, it is placed in the completed Jobs table. Jobs are available for one week before they are deleted.

Create Software Update Job

Device Selection

Navigate the device tree to an appropriate level for the devices to be updated. For example, selecting a Fixed Wireless AP will filter the devices to include the AP and its children.

Device Type

Software Updates are executed on one type of device at a time.

Software Update Dashboard

Once the device type is chosen, the UI displays the most recent software release version for that device type. It also displays a breakdown of the different software versions currently installed on the devices.



Note

Enterprise Wi-Fi shown below contains device types on the **Software Update** page:

- Enterprise Wi-Fi (E-Series)
- Enterprise Wi-Fi (XE/XV/X7-Series)
- Enterprise Wi-Fi (Xirrus-Series)

Figure 300 Software Update: Enterprise Wi-Fi

System

Dashboard
Notifications
Statistics
Reports X
Software Update
Applications X
Clients
Mesh Peers
Assurance X
Assists X

Device Type
Enterprise Wi-Fi (XE/XV/X7-Series)

Versions
6.6.0.3-r9

Search
Managed Account: All Accounts

Devices	Managed Account	Status	Client Count	Active	Inactive
<input type="checkbox"/> AP_Unit_2000		Offline (16d 8h 47m)	N/A	6.6.0.3-r9	6.6.0.2-r5
<input type="checkbox"/> AP_Unit_2001		Online (1d 18h 16m)	0	6.6.1-a11	6.6.1-a7
<input type="checkbox"/> Kimiko-unit01	Base Infrastructure	Online (11d 17h 12m)	0	7.1-a5	7.0-r5
<input type="checkbox"/> Petals-unit01	-MSP	Online (5d 2h 28m)	0	6.6.1-a11	6.6.1-a10
<input type="checkbox"/> Petals-unit02	-MSP	Online (5d 2h 26m)	0	6.6.1-a11	6.6.1-a5
<input type="checkbox"/> Petals-unit03	-MSP	Online (5d 2h 27m)	0	6.6.1-a11	6.6.1-a9
<input type="checkbox"/> Petals-unit04	-MSP	Online (5d 2h 25m)	0	6.6.1-a11	6.6.1-a5
<input type="checkbox"/> Petals-unit05	Base Infrastructure	Online (5d 2h 29m)	0	6.6.1-a11	6.6.1-a9
<input type="checkbox"/> Petals-unit06	Base Infrastructure	Online (5d 2h 28m)	0	6.6.1-a11	6.6.1-a9
<input type="checkbox"/> Petals-unit07	-MSP	Online (4d 21h 50m)	0	6.6.1-a11	6.6.0.3-r9

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



Note

- **Update both partitions** option is available at System/Network/Site/Device levels. It is only available for the devices that support it.
- **Perform sequential updates within a site** option is available at System/Network/Site level except the Device level.

If the **Update both partitions** option is enabled/ disabled, the device level of the Software Update will be displayed as follows:

- **Enable:** Tp
- Selected target image will be upgraded in only active portion of the device.

Figure 301 *Software Update: Device level*

Wi-Fi > AP_Unit_2001

Dashboard Notifications Configuration Details Performance **Software Update** Tools Clients Mesh Peers WLANs Assists X

Versions
6.6.0.3-r9

Name
AP_Unit_2001

Status
Online

Active
6.6.1-a11

Inactive
6.6.1-a7

Update
☒ Now ☐ Schedule

Job Options

☒ Retry skipped/offline device(s) on reconnect ⓘ

☐ Update both partitions

Notes

[Add Software Job](#) [View Update Jobs](#)

If **Perform sequential updates within a site** is enabled, the image upgrade will happen only on one device at a time.

Figure 302 *Software Update: cnMatrix*

System

Dashboard Notifications Statistics Reports **Software Update** Applications X Clients Mesh Peers Assurance X Assists X

Device Type
cnMatrix

Versions
4.4-r3 (Recommended)

Search Managed Account: All Accounts

Devices	Managed Account	Status	Active	Inactive
<input type="checkbox"/> EX1010P-F5E040	Base Infrastructure	Online (1d 19h 26m)	5.0.2-r4	N/A

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

Update
☒ Now ☐ Schedule

Job Options

☐ Stop update on critical error

☐ Disable Auto Reboot

☒ Retry skipped/offline device(s) on reconnect ⓘ

10 Devices to update in parallel (1-500)

Notes

[Add Software Job to 0 device\(s\)](#) [View Update Jobs](#)

Disable Auto Reboot option disables reboot after applying the new software image. The user must manually reboot the device to complete the software update.

Figure 303 *Software Update: cnRanger*

System

Dashboard
Notifications
Configuration
Statistics
Reports X
Software Update
Applications X
Clients
Mesh Peers
Assurance X
Assists X

Device Type

cnRanger

Versions

2.1.0-r1

[Release Notes](#)

Q Search

Managed Account: All Accounts

Devices	Selected SMs	Managed Account	Status	Active	Inactive
<input type="checkbox"/> Migration-cnRanger-sierra-800-02		Base Infrastructure	Online (29d 3h 7m)	2.1.2.0-r7	0.0.0.9
<input type="checkbox"/> S800-123	<input type="checkbox"/> Select SMs	Base Infrastructure	Online (0d 2h 14m)	2.1.2.0-r9	0.0.0.9

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

Update

☒ Now
☐ Schedule

Job Options

☐ Stop update on critical error
☒ Retry skipped/offline device(s) on reconnect ⓘ

Within a sector, update

☐ SMs first and then BBU
☒ BBU first and then SMs

10
Devices to update in parallel (1-500)

Notes

Add Software Job to 0 device(s)

[View Update Jobs](#)

Figure 304 Software Update: 60 GHz cnWave

System
Dashboard
Notifications
Configuration
Statistics
Reports X
Software Update
Applications X
Clients
Mesh Peers
Assurance X
Assists X

Device Type
60 GHz cnWave
Versions
E2E Controller
Ext E2E-101
Versions
1.3.3 (Recommended)
Release Notes

Search

Devices	Managed Account	Model	Mode	PoP Node	Status	Active
<input type="checkbox"/> Node_8b00fa	Base Infrastructure	V1000	CN	No	Online (20d 15h...	1.3.3
<input type="checkbox"/> PoP_V3K	Base Infrastructure	V3000	DN	Yes	Online (20d 15h...	1.3.3
<input type="checkbox"/> V1K_8b00d6	Base Infrastructure	V1000	DN	No	Online (8d 23h ...	1.3.3
<input type="checkbox"/> V5K_DN	Base Infrastructure	V5000	DN	No	Online (8d 23h ...	1.3.3
<input type="checkbox"/> V5K_883083	Base Infrastructure	V5000	DN	No	Online (20d 15h...	1.3.3

Showing 1 - 5 Total: 5
10
Previous
1
Next

Update
Now
Schedule
Job Options
Batch Size
Unlimited
No Size Limit
Limited
Upgrade Timeout
900
The per-batch timeout for the upgrade operation (in seconds)
Download Retry Limit
1
The maximum retry attempts for each node
Download Timeout
600
The timeout for downloading the image (in seconds)
Download Protocol
HTTPS
Torrent
Skip Failures
Skip PoP Failures
Notes
Add Software Job to 0 device(s)
View Update Jobs

Figure 305 *Software Update: PTP 670/700*

PTP 650/670/700 Master > Migration_PTP_700_Master_02

Dashboard Notifications Details Slaves Configuration Performance **Software Update**

Note: The PTP 45700 software upgrade from cnMaestro is compatible starting from version 04-02.

Versions

04-03

Search

Managed Account: Base Infrastructure

Devices	Selected Slaves	Managed Account	Status	Active	Inactive
Migration_PTP_700_Master_02	Select Slaves	Base Infrastructure	Online	04-03	N/A

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

Update

☒ Now ☐ Schedule

Job Options

☐ Stop update on critical error

☒ Retry skipped/offline device(s) on reconnect

10 Devices to update in parallel (1-500)

Notes

Add Software Job to 0 device(s) View Update Jobs



Note

- Ensure that PTP 45700 devices are running the software version 04-02 or later before proceeding with the upgrade.
- Software update is supported on PTP devices from the following cnMaestro versions:
 - from cnMaestro 5.1.0 and later—PTP 78700 and PTP 50670 devices running software version 04-10 and later.
 - from cnMaestro 5.1.1 and later—PTP 48670 devices running software version 04-10 and later.

Software Update

The software version on the devices can be automatically updated to the preferred version when the device first contacts cnMaestro.

Enable the automatic update of device software as follows:

1. Navigate to **Administration > Jobs > Software Update** page.
2. Select the **Manual** or **Auto** page for updating the device software feature.
3. Choose the software version depending on the device type.
4. Click **Start**.

Figure 306 Manual update

Administration > Jobs

Configuration Update **Software Update** Reports Actions

Manual Auto

All Managed Account: All Accounts

ID	Details	Managed Account	Image Type	Occurrence	Target	Created by	Created on	Completed on	Status	
3235	2 eFMP Device(s)	Base Infrastructure	Device	Now	4.6.1-RC26	Luis	May 20, 2021 20:55	May 20, 2021 20:59	Completed:	
3234	2 eFMP Device(s)	Base Infrastructure	Device	Now	4.6.1-RC26	Luis	May 20, 2021 20:54	May 20, 2021 21:00	Completed:	
3233	1 cnMatrix Device(s)	Base Infrastructure	Device	Now	3.2.3+3	Durga Prasad	May 20, 2021 17:14	May 20, 2021 17:18	Completed:	
3232	1 eFMP Device(s)	Base Infrastructure	Device	Now	4.6.1-RC26	krishnareddy	May 19, 2021 15:41	May 19, 2021 15:48	Completed:	
3231	1 eFMP Device(s)	Base Infrastructure	Device	Now	4.6.1-RC26	krishnareddy	May 19, 2021 15:38	May 19, 2021 15:42	Completed:	
3230	2 eFMP Device(s)	Base Infrastructure	Device	Now	4.6.1-RC26	krishnareddy	May 19, 2021 15:24	May 19, 2021 15:29	Completed:	
3229	1 cnMatrix Device(s)	All Accounts	Device	Now	3.2.3+3	Durga Prasad	May 15, 2021 12:37	May 15, 2021 12:41	Completed:	
3228	1 cnMatrix Device(s)	All Accounts	Device	Now	3.2.3+3	Durga Prasad	May 15, 2021 12:34	May 15, 2021 12:34	Completed:	
3227	1 cnMatrix Device(s)	Base Infrastructure	Device	Now	3.2.2+3	Durga Prasad	May 15, 2021 12:29	May 15, 2021 12:33	Completed:	
3226	1 cnMatrix Device(s)	Base Infrastructure	Device	Now	3.2.3+3	Durga Prasad	May 15, 2021 12:24	May 15, 2021 12:28	Completed:	

Showing 1 - 10 Total 3191 10 < Previous 1 2 3 4 5 ... 320 Next >



Note

A Manual Update can be aborted at any point of time by clicking the Abort.

Figure 307 Auto update

Administration > Jobs

Configuration Update **Software Update** Reports Actions

Manual Auto

Once job is paused, it will automatically disable auto software update setting for managed devices at [Software Images](#) page. Similarly when job is resumed, it will automatically enable auto software update setting 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.

ID	Details	Target	Created on	Status	
13	cnPilot Home (R-Series) Device(s)	4.7.5-B4	Oct 14, 2020 10:49	Aborted:	
12	Enterprise Wi-Fi (E-Series) Device(s)	4.0+14	Oct 14, 2020 10:49	Aborted:	
11	cnPilot Home (R-Series) Device(s)	4.6-R16	Oct 13, 2020 12:39	Aborted:	
10	Enterprise Wi-Fi (E-Series) Device(s)	4.1+1	Oct 13, 2020 12:38	Aborted:	
9	Enterprise Wi-Fi (E-Series) Device(s)	3.11.4+9	Aug 25, 2020 14:...	Aborted:	
8	Enterprise Wi-Fi (E-Series) Device(s)	4.0+17	Mar 06, 2020 19:...	Aborted:	
7	Enterprise Wi-Fi (E-Series) Device(s)	3.9+3	Mar 06, 2020 19:...	Aborted:	
6	Enterprise Wi-Fi (E-Series) Device(s)	4.0+17	Jan 14, 2020 12:57	Aborted:	
5	cnPilot Home (R-Series) Device(s)	4.5-R7	Dec 09, 2019 13:26	Aborted:	
4	Enterprise Wi-Fi (E-Series) Device(s)	4.0+8	Dec 09, 2019 13:26	Aborted:	

Showing 1 - 10 Total 13 10 < Previous 1 2 Next >



Note

Auto update can't be manually aborted.

You need to download the new image version released from the Support Site. For more details refer to Managing Device Software Images.

Device Table

Select the devices to upgrade in the Devices Table.



Note

- You can upgrade a device only when status is Up. If you try to upgrade a device when it is Down, you will receive a message the selected device is down.
- If the device is under the Auto Software Upgrade, the manual software update is not possible.

The following parameters are visible (though some are only available for certain device types).

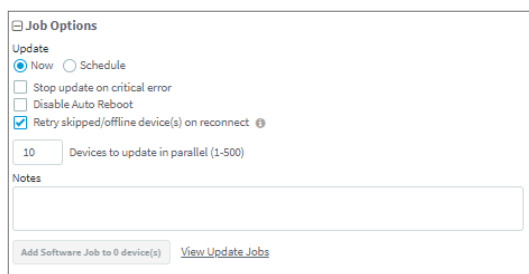
Table 66 *Parameters in Device Table*

Parameter	Description
Current Version	The version of the active software image running on the device.
Devices	The names of available devices in a system. The list is pre-filtered based upon the node selected in the Device Tree.
Selected SMs	If the AP is selected, the corresponding SMs will also be selected.
Status	The status of a particular device in a system. Devices that are not connected cannot be updated.

Retry Software Update

The **Retry skipped/offline device(s) on reconnect** option is available in every **Software Update** tab (System-, Network-, Site-, and device-levels) and enabled, by default.

Figure 308 *Retry Software Update*



If the software update job was skipped for a device because it was offline, the retry (↺) icon appears next to the Active Software version of the device. It indicates that the software update for the device will be retried with the target device version mentioned in the job, whenever the device reconnects to cnMaestro.

If the software update job was skipped while upgrading with the same version as the device active version, the icon will not be displayed, and the device will not update when it reconnects.



Note

A new job is not created when the software update is retried on a device when it reconnects.

Options

Stop update on critical error

If one of the updates fail, do not start any additional updates and instead pause the update job. However, all existing, concurrent updates will be allowed to proceed until completion. The administrator will be able to continue the update where it left off if desired.

Sector upgrade order

The recommended update order for devices within a sector will be pre-configured according to the recommendations for the device. It can be changed if desired.



Note

Device update occurs sector-by-sector. One sector needs to complete before a second sector is started.

Parallel upgrades

Specify how many device upgrades to perform in parallel to complete the upgrade faster. However if the job is configured to halt on an error, all concurrent sessions will still be allowed to complete.

Upgrade steps

To update the software version of devices, perform the following steps:

1. Navigate to **Monitor and Manage > Software Update**.

You can also navigate to the System-, Network-, Tower-, or Site-level and then

To update a single device, Navigate to System/Network/Tower/Device level and select the device.

2. Select the device type from the **Device Type** dropdown list:

The following options are supported:

- a. 60 GHz cnWave
- b. cnMatrix
- c. cnPilot Enterprise (ePMP Hotspot)
- d. cnPilot Home (R-Series)
- e. cnRanger
- f. cnVision
- g. cnWave 5G Fixed
- h. Enterprise Wi-Fi (E-Series)
- i. Enterprise Wi-Fi (XE/XV/X7-Series)
- j. Enterprise Wi-Fi (Xirrus-Series)
- k. ePMP (Sectors)
- l. NSE
- m. PMP (Sectors)
- n. PON
- o. PTP 670/700
- p. PTP 820/850
- q. RV22 Home Mesh

3. Select the software image to update from the **Versions** dropdown list.
4. Select checkbox for the devices to update.
5. Expand the **Job Options** section and configure the required parameters.
The job options available vary for different devices.
6. Click **Add Software Job to** <Number of devices> **device(s)**.

Software Update Jobs and Parameters

The Software Update Jobs table lists all currently running, queued, and completed jobs. The jobs can be triggered immediately, or they can be run later.

(**Administration > Jobs > Software Update** tab.)

The following table displays the list of parameters in the **Software Update Jobs** tab:

Table 67 *Parameters in Software Update Jobs*

Parameter	Description
Action	Use the Start or Delete button to manage the upgrade process. After the upgrade has started, the Pause button will stop new upgrades from the beginning. If the upgrade process fails or the upgrade has been paused, you can restart the process by clicking the Resume button.
Created By	The user who has created this job.
Created On	Date and time the job is created.
Details	Count of devices and date and time the upgrade process is initiated.
ID	Identification number of the active job.
Image Type	Displays Device for Device Firmware Upgrade.
Occurrence	Displays Now and Scheduled depending upon the job options selected during Software Update Job.
Parallel	Number of devices to start in parallel.
Sector Priority	For cnVision, ePMP/PMP, the priority of AP/SM to start.
Status	Status of update.
Stop on Error	Stop the job on an error in any device update.
Target	Target software version to upgrade.
By selecting the Show More icon, you can view the following parameters:	
Device	Device for which the upgrade is initiated.
Message	The message that is displayed after the update.
Original Version	The current software image version of the device.
Result	The upgrade status of the device.
Status	Status of the device.

The user can filter the jobs based on the running status. The user can also filter the devices in a particular job based on the parameters mentioned in the above table.

Abort Software Job

Abort operation will skip devices that are waiting for an update to begin. Devices already being updated may continue, but cnMaestro will stop tracking their progress. Aborting a Software Job puts the device into a "Completed" state that cannot be manually restarted by the user. The "pending" devices will not begin their updates.

Figure 309 Abort Software Job

Administration > Jobs

Configuration Update **Software Update** Reports Actions

Manual Auto

Once job is paused, it will automatically disable auto software update setting for managed devices at [Software Images](#) page. Similarly when job is resumed, it will automatically enable auto software update setting 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.

ID	Details	Target	Created on	Status	
13	cnPilot Home (R-Series) Device(s)	4.73-R4	Oct 14, 2020 10:49	Aborted: <div><div></div></div>	
12	Enterprise Wi-Fi (E-Series) Device(s)	4.0-r14	Oct 14, 2020 10:49	Aborted: <div><div></div></div>	
11	cnPilot Home (R-Series) Device(s)	4.6-R16	Oct 13, 2020 12:39	Aborted: <div><div></div></div>	
10	Enterprise Wi-Fi (E-Series) Device(s)	4.1-r1	Oct 13, 2020 12:38	Aborted: <div><div></div></div>	
9	Enterprise Wi-Fi (E-Series) Device(s)	3.11.4-r9	Aug 25, 2020 14:...	Aborted: <div><div></div></div>	
8	Enterprise Wi-Fi (E-Series) Device(s)	4.0-r17	Mar 06, 2020 19:...	Aborted: <div><div></div></div>	
7	Enterprise Wi-Fi (E-Series) Device(s)	3.9-r3	Mar 06, 2020 19:...	Aborted: <div><div></div></div>	
6	Enterprise Wi-Fi (E-Series) Device(s)	4.0-r17	Jan 14, 2020 12:57	Aborted	
5	cnPilot Home (R-Series) Device(s)	4.5-R7	Dec 09, 2019 13:26	Aborted: <div><div></div></div>	
4	Enterprise Wi-Fi (E-Series) Device(s)	4.0-r8	Dec 09, 2019 13:26	Aborted	

Showing 1 - 10 Total 13 10 < Previous 1 2 Next >



Note

1. Devices which are already updated display as **Completed** with a message **Update Complete** along with the status as Completed.
2. Devices that are ongoing display as **Aborted** with a message **Manually Aborted** with the status as Aborted.
3. Devices that have not yet started display as **Skipped** with a message **Job was aborted** with the status as **Skipped**.
4. Software update jobs can be scheduled in parallel irrespective of other running jobs in cnMaestro X accounts.
5. Only **Configuration** or **Software Update Job** operation can be performed on the device, as the job locks the device.

Viewing Running Jobs in header

Click the icon in the top right corner of the UI. This navigates to the **Software Update** tab > **Jobs** page of the Software Update section. For more information, see [Software Update](#)

Fixed Wireless Configuration

This chapter provides the following information:

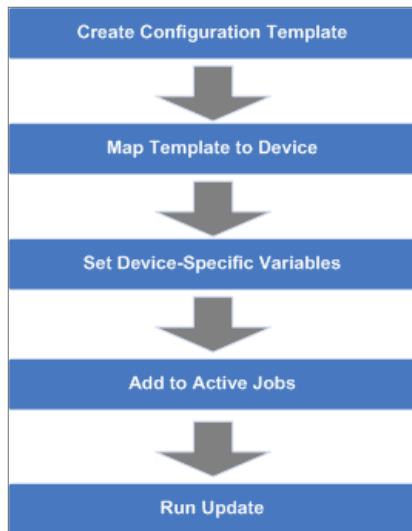
- [Overview](#)
- [Configuration Templates](#)
- [Configuration Variables](#)
- [Configuration Update at Onboarding](#)

Overview

Template configuration is supported for ePMP, PMP, cnWave 5G Fixed devices. Templates are textual representations of device settings that contain a full or partial configuration. When a template is applied to a device, the only parameters changed are those in the template.

The process flow of the basic template configuration is shown below:

Figure 310 Basic Template Configuration Flow



Configuration Templates

Templates can be pushed to a device manually through a configuration job. This is accomplished in the configuration management page. Templates can also be applied prior to onboarding, in which they would be provisioned in the Onboarding Queue.

Some sample templates are listed below. The ellipses (...) represents additional content that has been excised from the example to limit the size of the text. Each device type has its own template syntax, which can be examined by viewing the device configuration.

Sample ePMP Template

The ePMP template uses the exported ePMP configuration format, which is JSON-encoded.

Figure 311 Sample ePMP Template

```
{
  "device_props": {
    "accEnable": "0",
    "accScanMinDwellTime": "200",
    "accScanMaxDwellTime": "300",
    "accControl": "0",
    "bcPriority": "0",
    "cambiumInternetConnectionServerIP": "",
    "centerFrequency": "5670",
    "dataLANEnable": "0",
    "dataLANVID": "",
    ...,
    "snmpTrapTable": [
      {
        "snmpTrapEntryIP": "10.120.143.176",
        "snmpTrapEntryPort": "162"
      }
    ],
    ...
  }
}
```

Configuration Variables

Administrators can embed variables into templates that will be replaced when the template is applied to a device. This allows one to leverage a shared, generic template, but to tailor it to individual devices when it is pushed. Template variables are added to a configuration file by replacing an existing parameter with a customer-defined string of the format `${VARIABLE}`. An example configuration line with a single variable replacement is shown below:

`"networkLanIPAddr": ${IP ADDRESS}`

The above variable is named `IP_ADDRESS`. When the template is pushed to a device, this variable will be replaced with a value specific to the device. This value needs to be set for the device prior to the template application, else the configuration will not be pushed. Default values can also be specified for variables, as shown below:

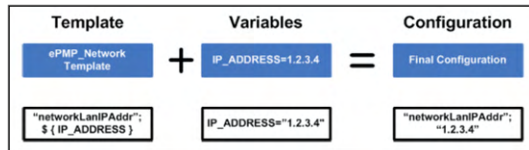
`"networkLanIPAddr": ${IP ADDRESS="10.1.1.254"}},`

The default value is "10.1.1.254". In this case, if the variable is not set for a device, the default value is used.

Variable Usage

The Templates and Variables are merged to create the final configuration that is pushed to the device. The figure below explains the usage of variables for configuration:

Figure 312 Variable Usage



Macros

Macros can be used in templates similar to variables except that they automatically embed values provided by the device itself.

- %[ESN] will be replaced with the MAC address of the device
- %[MSN] will be replaced with the Serial Number of the device

Variable Caching

Variables set for a particular device will be cached, so they can be reused later. This means the next time a template is applied that leverages a variable with the same name as used previously that value will be pre-populated with the previous value. It is therefore beneficial to define a uniform variable naming and usage scheme for variables across different templates.

Device Type-Specific Configurations

The format and values of a configuration template are unique to the different device types. Templates that work with device type do not work with others, and all templates need to be mapped to a specific device type upon creation.

Device Mode restrictions

Some devices, such as ePMP execute in AP and SM modes. The ePMP templates can be configured to only apply to devices that support a selected mode.

Variable validation

All variables for a selected template must be mapped to a value in order to create a configuration job. If any variables are not mapped, an error will be generated. Variables with default settings do not cause an error if they are unset.

Sample Templates

A number of sample templates are provided for each device type. These are not meant to be applied directly, but rather serve as an example of the configuration data format accepted by the device. Refer to the device documentation for complete information.

Template file creation

The typical process for creating your own configuration templates is below:

1. On a test device configure the parameters to the devices. This can be done directly on the device UI .
2. Export the device configuration using cnMaestro.
 - Navigate to **Configuration > Templates**, select the device in the left-hand tree and click the **View Device Configuration** link. This can also be done via the device GUI, typically in the Administration or Operations section where there will be an **Export** for configuration.
3. View the configuration file in a text editor like Notepad++ and search for the values entered in step 1. You can also search for the parameter name to find the correct lines.
4. Copy and paste the relevant lines into a new file.
5. Optionally replace values with replacement variable text. This will allow you to set the value per device.
6. Once you have this partial template, it can be copied into the template creation text field and saved.

Template

To create a configuration template:

1. Navigate to **Configuration > Templates** in the main menu.

Shared Settings > Templates

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.

Search Clear Scope: All Accounts Add Template

Template Name	Device Type	Template Type	Scope	Description	Variable	Last Updated	Created By	
snmp_v2_space	PTP 820/850	Custom	Shared	snmp_v2	-	Thu Jul 14 2022 11:16:45 UTC +0530	Administrator	
snmp_v3	PTP 820/850	Custom	Shared	-	-	Wed Jul 27 2022 10:38:17 UTC +0530	Administrator	
snmp_v2	PTP 820/850	Custom	Shared	-	-	Thu Jul 14 2022 12:01:59 UTC +0530	Administrator	
snmp_v3_multi	PTP 820/850	Custom	Shared	-	-	Tue Aug 02 2022 17:16:58 UTC +0530	Administrator	
NTP	PTP 820/850	Custom	Shared	-	-	Sun Jul 17 2022 09:36:34 UTC +0530	Administrator	
All_config_PTP820_850	PTP 820/850	Custom	Shared	-	-	Tue Sep 20 2022 13:54:28 UTC +0530	Administrator	

Showing 1-6 Total: 6 10 1 Previous Next

The following template is for BTS:

Shared Settings > Templates > cnWave 5G Fixed

Scope: Base Infrastructure

Name: BTS

Description: N/A

Device Mode: ☒ BTS ☐ CPE

Configuration Text

```
{
  "aaa": {
    "cfg": {
      "mode": "RADIUS AAA",
      "cPEIPAddressSource": "RADIUS",
      "radius": {
        "accounting": "True",
        "auth0": {
          "role": "Primary",
          "addrType": "ipv4",

```

The following template is for CPE:

Shared Settings > [Templates](#) > cnWave 5G Fixed

Scope
Base Infrastructure

Name*
CPE

Description
N/A

Device Mode
☐ BTS ☒ CPE

Configuration Text
 [Select File](#)

```

{
  "accounts": {
    "options": {
      "preferences": {
        "Highlight Changes": false,
        "Login Page Background Image": true
      }
    },
    "user": {}
  }
}
  
```

[Save](#)

2. Click **Add Template** button.

Shared Settings > [Templates](#) > cnPilot Home (R-Series)

Scope
Shared

Name

Description

Configuration Text
 [Select File](#)

[Save](#)

3. Choose a **Device Type**, **Name**, and **Description** for the template. For ePMP, PMP, cnWave 5G Fixed, cnReach, and cnMatrix templates, you should select a **Device Type** as well.
4. Either upload your template into the UI or paste the template text into the text area.



Note

No default templates available for R-series. User needs to create a new template.

5. After clicking **Save**, the template will be available in the selection menu on the configuration and onboarding pages, as long as the device type and model match the device selected.
6. By selecting the Custom option under the Template type filter All Default templates will be hidden.



Note

When you navigate to the Template page default template type filter will be custom. User needs to select **All** or **Default** to view other templates.

BTS and CPE Configuration

To configure BTS, navigate to **Monitor and Manage > BTS > Configuration**.

The screenshot shows the 'BTS > BTS-...-lab' configuration page. The 'Configuration' tab is active, with sub-tabs for Details, CPEs, Performance, Software Update, Tools, and Assists. The 'Device Details' section includes fields for Managed Account (Base Infrastructure), Name (BTS Bangalore lab), Network (default), Tower (None), Latitude, Longitude, Height (936.1), Azimuth (0.0), and Antenna Tilt (0.0). The 'Device Configuration' section has a 'Restore from Backup' checkbox, a 'Template' dropdown (None), and a warning message. Below this is a table for configuration variables, currently showing 'No variables configured'. The 'Configuration Backup' section includes a 'Backup Now' button and the last backup timestamp: 'Tue Jul 02 2024 08:12'. An 'Apply Configuration' button is at the bottom.

Device Details

Managed Account: Base Infrastructure [Change](#)

Name: BTS Bangalore lab

Network: default

Tower: None

Latitude:

Longitude:

Height: 936.1

Azimuth: 0.0

Antenna Tilt: 0.0

Device Configuration [View Device Configuration](#)

☐ Restore from Backup

Template: None [View Template](#)

ⓘ Please note that modifying the polarization, bandwidth, or link symmetry settings will trigger an automatic reboot of the device.

Name	Value	Default
No variables configured		

☒ **Configuration Backup**

Configuration Backup pulls and stores and restores configuration from Fixed Wireless (PMP, ePMP, cnVision and cnWave 5G Fixed) and cnReach devices

[Backup Now](#) Last Backup: Tue Jul 02 2024 08:12 [View](#)

[Apply Configuration](#)

To configure CPE, navigate to **Monitor and Manage > BTS > CPE > Configuration**.

CPE > CPE-2

Dashboard Notifications **Configuration** Details Performance Software Update Tools Assists X

Device Details

Managed Account: Base Infrastructure

Name: CPE-2

Network: default

Tower: None

Latitude:

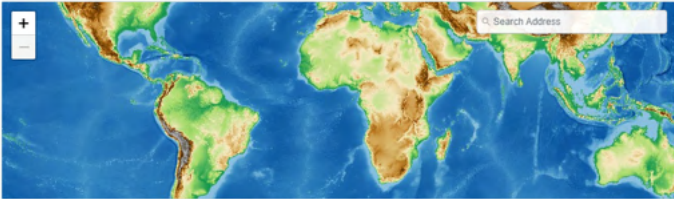
Longitude:

Serial Number:

MAC Address:

IPv4 Address: 192.168.1.12

☐ Set the device location using a map



Device Configuration

[View Device Configuration](#)

☐ Restore from Backup

Template: None [View Template](#)

Name	Value	Default
No variables configured		

Configuration Backup

Configuration Backup pulls and stores and restores configuration from Fixed Wireless (PMP, ePMP, cnVision and cnWave 5G Fixed) and cnReach devices

[Backup Now](#) Last Backup: N/A

[Apply Configuration](#)

Configuration Template for PTP 820/850

To create a configuration template of PTP 820/850 device, perform the following steps:

1. Navigate to **Configuration > Templates** in the main menu.

Configuration > Templates

Search: Device Type: All Scope: All Accounts Template Type: Custom [Add Template](#)

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.

Template Name	Mode	Scope	Description	Variable	Last Updated	Created By	
Machfu_Template	GW	Shared	N/A		Wed Oct 28 2020 13:33	Sesikumar R	
PMP_Template_Ver	AP, SM	Shared	N/A	lat==12.80, long==77.90	Tue Oct 27 2020 14:55	RAGHAVENDRA	
SvoLoo_Template_Basics	Wi-Fi	Shared	N/A		Wed Oct 28 2020 19:37	RAGHAVENDRA	
Test_SNMP	AP, SM	Shared	N/A		Tue Oct 27 2020 14:56	RAGHAVENDRA	
PMP450AP_SanJose	AP	SanJose, tenant	N/A	COLOR_CODE=222, FREQ_CA...	Tue Nov 24 2020 22:16	Azil demo setup	
PMP450SM_SanJose	SM	SanJose, tenant	N/A	COLOR_CODE=1-222	Tue Nov 24 2020 22:16	Azil demo setup	

Showing 1 - 6 Total: 6 [Previous](#) [Next](#)

2. In the **Add Template** dropdown, select PTP 820/850.

Shared Settings > Templates

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.

Q Search Clear Scope All Accounts Add Template

Template N...	Device Type	Scope	Descri...	Variable	Last Updated	Created By	
BTS	cnWave 5G Fixed	Shared		-	31 May 2024, 05:34 PM	Administrator	
BTS_latest	cnWave 5G Fixed	Base Infrastructure	N/A	-	28 Jun 2024, 10:12 AM	Administrator	
CPE	cnWave 5G Fixed	Shared		Contact=abc, Name=CPE4, Location=...	31 May 2024, 05:35 PM	Administrator	
CPE_latest	cnWave 5G Fixed	Base Infrastructure	N/A	-	28 Jun 2024, 10:13 AM	Administrator	
PTP8xx	PTP 820/850	Shared		-	31 May 2024, 05:34 PM	Administrator	
cnMatrix-DNS	cnMatrix	Shared		dns=10.110.12.113	03 Jun 2024, 08:36 AM	Administrator	
cnreach_admin	cnReach	Shared		-	03 Jun 2024, 02:41 PM	Administrator	
cnvision	cnVision	Shared		Latitude=, Longitude=+, Site Con...	03 Jun 2024, 11:07 AM	Administrator	
epmp	ePMP	Shared		Latitude=, Longitude=+, Site Con...	03 Jun 2024, 11:07 AM	Administrator	
pmp	ePMP	Shared		Latitude=, Longitude=+, Site Con...	03 Jun 2024, 11:07 AM	Administrator	

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

The **Basic** template page appears.

3. In the **Basic** page, enter **Name** and **Description** and click **Save**.

By default, **NTP Configuration**, **Time Services**, **SNMP**, and **Security** pages are disabled. Click slider icon next to the fields to enable the pages and configure the template.

Shared Settings > Templates > PTP 820/850

Basic

Scope: Shared

Name:

Description:

Save

NTP Configuration ☐

Time Services ☐

SNMP ☐

Security ☐

NTP Configuration

1. In the **NTP Configuration**, click **Add New**.

Shared Settings > Templates > PTP 820/850

Basic

NTP Configuration ☒

Time Services ☐

SNMP ☐

Security ☐

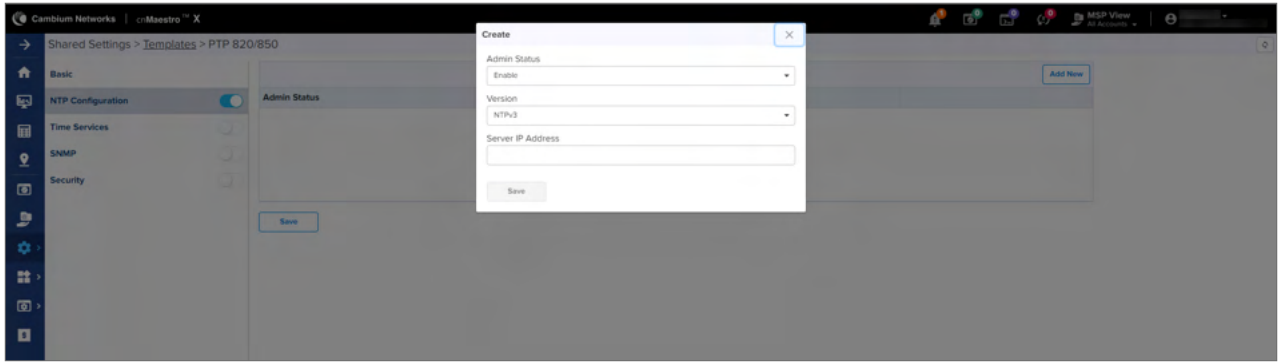
Admin Status Version Server IP Address

No Data Available

Save

Add New

Create window appears.



2. Select **Admin Status** from dropdown.
3. Select **Version** from dropdown.
4. Enter **Server IP Address**.
5. Click **Save**.

NTP configuration is added to the table. You can perform the following actions for configurations added in the table.

1. Click edit icon to edit the configuration
2. Click delete icon to delete the configuration.

Time Services

1. Enter the values for the following fields:
 - Offset from GMT
 - Daylight Saving Start Time
 - Daylight Saving End Time

Shared Settings > [Templates](#) > PTP 820/850

Basic

NTP Configuration ☒

Time Services ☒

SNMP ☐

Security ☐

Offset from GMT

UTC Offset Hours

UTC Offset Minutes

Daylight Saving Start Time

Month

Day

Daylight Saving End Time

Month

Day

DST offset (Hours)

Save

2. Click **Save**.

SNMP

1. Enter the details for **V2 Users**, add **V3 Users** and **Trap Managers**, and select **Trap Version**.

Shared Settings > Templates > PTP 820/850

Basic

NTP Configuration ☒

Time Services ☒

SNMP ☒

Security ☐

V2 Users

Read Community

Write Community

v1 v2 Blocked
☐ Yes ☒ No

V3 Users [Add New](#)

Username	Authentication Algorithm	Encryption (Privacy) mode	Security mode	Access mode
No Data Available				

Note: It requires a manual update in discovery rule to use the above configured v3 user.

Trap Managers [Add New](#)

Admin Status	IPv4 Address	Description	Port	Heartbeat	CLI	V3 User Name	
No Data Available							

Trap Version
v1

[Save](#)

2. Click **Save**.

Security

1. Select the values for **General Access Control**.
2. Select **Protocol Control**.

Shared Settings > Templates > PTP 820/850

Basic

NTP Configuration ☐

Time Services ☐

SNMP ☐

Security ☒

General Access Control

Failure login attempts to block user (Minutes)
1

Blocking Period (Minutes)
10

Unused Account Blocking Period (Days)
No Blocking

Protocol Control

Session timeout (Minutes)
10

[Save](#)

3. Click **Save**.

Configuration Update

Device Selection

Navigate to the **Configuration Update** tab, and then navigate the Device Tree to the appropriate level for device selection. For example, selecting a Fixed Wireless AP will enable selection of the AP and all its SMs.

Device Type

Configuration jobs are created for a single device type. The type includes the specific hardware (ePMP, PMP) as well as the mode of the device (cnVision, PMP or PTP mode for ePMP for example).

Device Table

Select the devices to upgrade in the Devices Table. The following parameters are visible in the table:

Table 68 *Device Table parameters*

Parameter	Description
Devices	The names of available devices in a system. The list is pre-filtered based upon the node selected in the Device Tree.
Network/Tower	The network and the tower on which the device is located.
Status	The status of a particular device in a system. Devices that are “Down” can not have images pushed to them.



Note

- You can only push configuration to a device when its status is **Up**.
- The user should validate the configuration before pushing it to the device from cnMaestro.

Options

Stop all Configuration on a Critical Error

If one of the configuration updates fails, then do not start any additional updates and instead pause the update job. All existing, concurrent updates will be allowed to proceed until completion. The administrator will be able to continue the update where it left off.

Parallel Upgrades

Define how many configuration updates to perform in parallel.

Update Ordering

Allows you to specify update ordering within a Fixed Wireless sector. Options are SMs first and then AP or AP first and then SMs.

Abort Configuration

Abort operation will skip devices that are waiting for update to begin. Devices already being updated may continue but cnMaestro will stop tracking their progress. Aborting a Configuration Job puts the device into a complete state that cannot be manually restarted by the user. The pending devices will not begin their updates.

Figure 313 *Abort Configuration*

Administration > Jobs												
Configuration Update Software Update Reports Actions												
Aborted Managed Account: All Accounts												
ID	Details	Managed Account	Occurrence	Target	Created by	Created on	Completed on	Parallel	Stop on Error	Sector Priority	Status	
52	1 cnPilot Home (R-Series) de...	Base Infrastructure	Schedule	BSeries	jishma asmi	May 31, 2021 17:43	May 31, 2021 19:30	10	false	N/A	Aborted:	
53	1 cnPilot Home (R-Series) de...	Base Infrastructure	Schedule	zyxlog	jishma asmi	May 31, 2021 17:43	May 31, 2021 19:30	10	false	N/A	Aborted:	
32	2 Machfu device(s)	All Accounts	Schedule	Machfu_template...	Sasikumar R	May 31, 2021 12:33	May 31, 2021 17:49	1	false	N/A	Aborted:	
33	2 ePMP device(s)	All Accounts	Schedule	Example SNMP Cr...	Sasikumar R	May 31, 2021 12:35	May 31, 2021 17:49	10	false	SM First	Aborted:	
34	2 Enterprise Wi-Fi (E-Series, ...	All Accounts	Schedule	DATA_AP_US	Sasikumar R	May 31, 2021 12:36	May 31, 2021 17:48	1	false	N/A	Aborted:	
35	2 Enterprise Wi-Fi (E-Series, ...	All Accounts	Schedule	THOR_AP	Sasikumar R	May 31, 2021 12:36	May 31, 2021 17:48	2	false	N/A	Aborted:	
36	2 cnPilot Enterprise (ePMP H...	All Accounts	Schedule	HOT_SPOT_AP	Sasikumar R	May 31, 2021 12:56	May 31, 2021 17:48	10	false	N/A	Aborted:	
15	1 cnPilot e500 device(s)	Base Infrastructure	Now	DATA_AP_US	Sasikumar R	May 19, 2021 19:08	May 19, 2021 19:09	-	false	N/A	Aborted:	
14	1 cnPilot e500 device(s)	Base Infrastructure	Now	DATA_AP_US	Sasikumar R	May 19, 2021 19:07	May 19, 2021 19:09	-	false	N/A	Aborted:	
Showing 1 - 9 Total 9												



Note

1. Devices which are already updated display as **Completed** with a message Update Complete along with the status as **Completed**.
2. Devices which are ongoing display as **Aborted** with a message Manually Aborted with the status as **Aborted**.
3. Devices which have not yet started display as **Skipped** with a message Job was Aborted with the status as **Skipped**.

Configuration Update Steps

To update the configuration of an ePMP (Sectors) device, perform the following steps:

1. Navigate to **Manage > Configuration > Device Details** in the Main Menu.
2. Navigate to **System > Network** in the Device Tree. From the list of available networks, select a network in which the device belongs to.
3. Select ePMP (Sectors) from the **Device Type** dropdown.
4. Select the configuration template to upgrade from the **Template** dropdown.
5. Select the device(s) to upgrade.
6. Click the gear icon to view or edit variables that are required for selected devices.
7. Click **Apply Configuration**.



Note

- The Configuration Upgrade cannot proceed until all required variables (those without default parameters) are entered. If you attempt to create a configuration job without setting required variables, the gear icon will turn red for any devices not meeting this requirement.
- To save and download the existing Device Configuration as Template, click **View Device Configuration** link.

Configuration Jobs

Navigate to **Administration > Jobs > Configuration Update** tab.

Jobs are presented with various Status values: Running, Queued, Skipped, and Completed. They can be triggered to execute immediately or run later. The list of parameters in the Jobs tab is shown below:

Configuration Update													
Managed Account: All Accounts													
ID	Details	Managed Account	Occurrence	Target	Created by	Created on	Completed on	Parallel	Stop on Error	Sector Priority	Status		
4357	1 cnMatrix EX2010 device(s)	Base Infrastructure	Now	cnMatrix_Syslog...	Durga Prasad	May 15, 2021 12:47	May 15, 2021 12:47	-	false	N/A	Completed:	<div></div>	
4356	1 device(s)	Base Infrastructure	Now		Auto-Sync	May 15, 2021 12:47	May 15, 2021 12:47	15	false	N/A	Completed:	<div></div>	
4355	1 device(s)	Base Infrastructure	Now		Auto-Sync	May 15, 2021 12:46	May 15, 2021 12:46	15	false	N/A	Completed:	<div></div>	
4354	1 cnMatrix EX2010 device(s)	Base Infrastructure	Now	Default Switch	Durga Prasad	May 15, 2021 12:46	May 15, 2021 12:46	-	false	N/A	Completed:	<div></div>	
4353	1 device(s)	Base Infrastructure	Now		Auto-Sync	May 14, 2021 16:10	May 14, 2021 16:11	15	false	N/A	Completed:	<div></div>	
4352	1 device(s)	Base Infrastructure	Now		Auto-Sync	May 14, 2021 15:52	May 14, 2021 15:52	15	false	N/A	Completed:	<div></div>	
4351	1 device(s)	Base Infrastructure	Now		Auto-Sync	May 14, 2021 15:51	May 14, 2021 15:51	15	false	N/A	Completed:	<div></div>	
4350	1 device(s)	Base Infrastructure	Now		Auto-Sync	May 14, 2021 15:50	May 14, 2021 15:51	15	false	N/A	Completed:	<div></div>	
4349	1 device(s)	Base Infrastructure	Now		Auto-Sync	May 14, 2021 15:47	May 14, 2021 15:47	15	false	N/A	Completed:	<div></div>	
4348	1 cnPlot e510 device(s)	Base Infrastructure	Now	Session Issue	Raja Muniyandy	May 13, 2021 13:11	May 13, 2021 13:12	-	false	N/A	Completed:	<div></div>	

Showing 1 - 10 Total: 4,236 10 < Previous 1 2 3 4 5 ... 424 Next >

**Note**

cnMaestro X account user can run any number of **Jobs** in parallel.

The following table displays the list of parameters in the **Jobs** tab:

Table 69 *Configuration Update parameters*

Parameter	Description
Action	Use the Start or Delete button to manage the upgrade process. After the upgrade has started, the Pause button will stop new upgrades from the beginning. If the upgrade process fails or the upgrade has been paused, you can restart the process by clicking the Resume button.
Created By	The user who has created this job.
Created On	Date and time on which the job is created.
Details	Count of devices and date and time the upgrade process is initiated.
ID	Identification number of the active job.
Parallel	Number of devices to start in parallel.
Sector Priority	For ePMP/PMP, cnRanger, cnVision Hub/Client, the priority of AP/BBU/SM to start.
Status	Status of update.
Stop on Error	Stop the job, if any device in middle finds any error.
Target	Target software version to upgrade.
By selecting the Show More icon, you can view the following parameters:	
Device	Device for which the upgrade is initiated.
Message	The message displayed after the update.
Result	The upgrade status of the device.
Status	Status of the device.
Mode	SM or AP mode selected.
Network	Type of Network.
Tower	Name of the Tower.

Configuration Update at Onboarding

Administrators can apply the configuration to devices during the onboarding process: Prior to approving the device in the Onboarding Queue, the configuration template and variables can be specified. These will then be pushed to the device during onboarding. For more details on onboarding, see [Device Onboarding](#).

Wi-Fi Configuration

Wi-Fi configuration is handled through AP Groups or Templates, which Fixed Wireless devices, such as ePMP and PMP, exclusively use Templates. This section will focus exclusively on AP Groups.

This chapter provides details on the following sections:

- [Enterprise Wi-Fi AP](#)
- [Factory Reset](#)
- [Association ACL](#)

- [Access Control Policies](#)
- [Custom Applications](#)

Enterprise Wi-Fi AP

Following are the various types of Wi-Fi hardware available:

- Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)
- cnPilot Enterprise APs
- cnPilot Home (cnPilot R-series devices)
- Enterprise Wi-Fi (Xirrus-Series)
- RV22 Home Mesh Routers

These four hardware types map to the following AP group types:

- Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)
- Enterprise Wi-Fi (Xirrus-Series)
- cnPilot Home (R-Series)
- RV22 Home Mesh

Multiple AP Group types are needed, because the features available across the groups are different.



Note

Wi-Fi devices can alternately be configured using a template mechanism, in which a subset of configuration is pushed to the device manually through a user-defined template of parameters. See the section on Templates for more information. Template configuration and AP Group configuration cannot be used simultaneously.

Configuring Enterprise Wi-Fi APs using Wi-Fi Profiles

Wi-Fi devices are configured by creating an AP Group, mapping it to shared WLANs, and assigning it to devices through the Configuration tab. Once assigned, the configuration is pushed manually or automatically (if **Auto Sync** is enabled).



Note

Xirrus devices embed WLAN configuration directly into the AP Group Full Configuration tab and do not support separate WLAN profiles.

Auto Synchronization

AP Groups can automatically synchronize device configuration whenever the AP Group or associated WLANs are updated. This is done by enabling **Auto Sync** in the AP Group **Configuration** page.

Manual Synchronization

When a device is mapped to an AP Group without **Auto Sync** turned on, the device is placed in an **Unsynchronized** state until it is manually synchronized. Manual synchronization can be done as follows:

- Navigate to device **Configuration** page > **Sync Now** or
- Navigate to **Administration** > **Sync Configuration** > **Sync Configuration**. page.

Create an AP Group



Note

- This example demonstrates how to create an Enterprise Wi-Fi (E-Series, XE/XV/X7-Series) AP Group. A similar process can be followed for the cnPilot Home (R-Series) AP Group.
- The Enterprise Wi-Fi (Xirrus-Series) AP Group is different than the others. It embeds a full configuration template of CLI commands that needs to be updated manually. The Xirrus AP Group will support Auto Synchronization when the embedded template is changed, which makes it different than applying the configuration through the standalone Template mechanism.

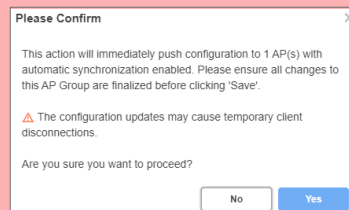


Warning

After creating an AP group, any modifications to the parameters may cause client disconnections. A warning message is displayed when saving the AP group depending on if there are any devices in the group and if the Auto Sync function is enabled or disabled:

- Auto Sync is enabled and if devices are present in the AP Group:

Figure 314 *Warning when modifying WLAN*

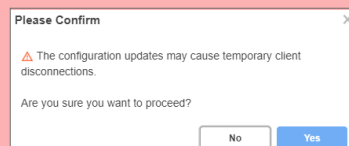


- Auto Sync is enabled and if no devices are present in the AP Group:

OR

Auto Sync is disabled and regardless of devices present or not in the AP Group:

Figure 315 *Warning when modifying WLAN*



To create an AP Group, perform 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** dropdown list.



Note

- Certain special characters can be used when creating the AP Group and WLAN passwords, such as a-zA-Z_-*&%#@!<>(). []^~\$1234567890.
- By default, the password is not configured. User must configure the password for AP Groups.
You can also rename the password after creating one.

Basic

In the **Basic** page, configure the following details such as:

1. Select **Type** from one of the following:
 - cnPilot Home (R-Series)
 - Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)
 - Enterprise Wi-Fi (Xirrus-Series)
2. Enter the mandatory fields based on device type.
 - Name
 - Country
 - Description
 - WLAN
3. Click **Add WLAN** and select **WLAN** from the list.
4. Click **Save**.

Figure 316 Basic: cnPilot Home (R-Series)

AP Groups > Add New

Basic

Management

Radio

Network

User-Defined Overrides

Basic Information

Type
cnPilot Home (R-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

WLAN

Add WLAN Create WLAN

Order	WLAN
No WLAN Selected	

Save Close

Figure 317 Basic: Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)

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

Figure 318 Basic: Enterprise Wi-Fi (Xirrus-Series)

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

The Xirrus AP Group embeds a Full Configuration of CLI commands.

Figure 319 Full Configuration: Enterprise Wi-Fi (Xirrus-Series)

AP Groups > APGroup-165_import&Export

Dashboard Notifications Configuration Statistics Report X APs Clients Mesh Peers

Basic

Full Configuration

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 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.

```
!
configure
!
description
hostname X11873574581C
location "BLR-INFINITY"
exit
!
contact info
name ""
phone ""
email ""
exit
```

Save Import Export

Management

The **Management** page allows to configure the **Administrator Access**, **Time Settings**, **Event Logging** and **SNMP**.



Note

The AP uses the AES-128 algorithm for encryption and SNMPv3 password configuration parameter is used for encryption and authentication.

Figure 320 Management: Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)

AP Groups > APG_CNM_SIT_ESeries_Infinity

Dashboard Notifications **Configuration** Statistics Report X Devices Clients Mesh Peers

Basic

Management

Radio

Network

Security

Access Control

Services

User-Defined Overrides

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 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 RADIUS server shared secret

Time Settings

Time Zone Configure Time Zone

NTP Server 1 Name or IP Address of Network Time Protocol Server

NTP Server 2

☒ Event Logging

☒ SNMP

Save

Radio

The **Radio** page allows the user to enable or disable the Software Defined Radio operations. It allows to configure **Software Defined Radios, Basic, Enhanced Roaming, Off Channel Scan, Auto-RF, and External Antennas.**

Figure 321 Radio: Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)

AP Groups > tests

Dashboard Notifications **Configuration** Statistics Reports X Devices Clients Mesh Peers

Basic

Management

Radio

Network

Security

Access Control

Services

User-Defined Overrides

Software Defined Radios

Model	Radio 1	Radio 2	Radio 3	Radio 4	Radio 5
XV3-8	2.4 GHz	5 GHz (8x8)	N/A	N/A	N/A
XE3-4/XE3-4TN	2.4 GHz	5 GHz	6 GHz	N/A	N/A
XE5-8	2.4 GHz	5 GHz	6 GHz	5 GHz (Split 4x4)	5 GHz

2.4 GHz Band 5 GHz Band 6 GHz Band

☒ Basic

☒ Enhanced Roaming

☒ Channel Scan

☒ Auto-RF

External Antennas

Model	Radio 1	Radio 2	Radio 3
XE3-4TN	Omnidirectional...	Omnidirectional...	Omnidirectional...

Save

**Note**

The software defined radio creation and channel listing are populated based on the country-specific restrictions, device type, and release version.

Software Defined Radios

The Software Defined Radios (SDR) allows you to configure radio parameters for XV3-8, XE3-4, and XE5-8 device models. By default these device models are configured for radio bands as shown in [Figure 321](#). The other radio bands for which the devices can be configured are as shown in [Table 70](#).

Table 70 Supported Radio bands for Enterprise Wi-Fi Series (E-Series, XV-Series and XE-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	<ul style="list-style-type: none">100 to 165 in Split 4x4 dual radio36 to 165 in 8x8 - single 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 71 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

* 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 (Supported only on XV3-8 and XE5-8 APs) splits 8x8 5 GHz radio into two 4x4 5 GHz radios.
- 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 71 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 & 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 `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 the device, the predefined default channel list can be overridden.

To configure `no channels-distribution` using the AP groups in cnMaestro UI, complete the following steps:

1. Navigate to **Configuration > Wi-Fi Profiles > AP Groups** page.
2. Select the AP group that you want to update with the `no channels-distribution` CLI.
3. Click **User-Defined Overrides** tab.
4. Enter the following command in the box:

```
!
no channels-distribution
!
```

5. Click **Save**.

1. In the **Radio** tab, you can configure **Software Defined Radios** for the required **Model** as shown in [Table 70](#). Enterprise Wi-Fi (E-Series, XE/XV/X7-Series) devices can be configured with radio features for 2.4 GHz, 5 GHz, and 6 GHz radio bands.
2. Expand the **Basic** section, select either **Enable** or **Disable** option to enable or disable the radio.
3. Select **Auto** in the **Channel** dropdown.
4. In the **Candidates Channel** select **All**.
5. Select the parameter values from the dropdown for the following fields:
 - Channel Width
 - Transmit Power
 - Beacon Interval
 - Minimum Unicast Rate
 - Multicast Data Rate
 - Mode

Figure 322 *Radio page - Basic section*

AP Groups > Add New

Basic
Management
Radio
Network
Security
Access Control
Services
User-Defined Overrides

2.4 GHz Band 5 GHz Band 6 GHz Band

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) ⓘ

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 Clients to connect in 802.11 b/g/n mode

☐ 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

6. Expand the **Enhanced Roaming** section and select the **Enable** checkbox to enable enhanced roaming. Configure the threshold value (in dB) in the **Roam SNR Threshold** field.

AP Groups > Add New

Basic	<div> <div>Software Defined Radios</div> <div> <div>2.4 GHz Band</div> <div>5 GHz Band</div> <div>6 GHz Band</div> </div> <div> <div>Basic</div> <div>Enhanced Roaming</div> </div> </div> <div> <div>Please enable enhanced roaming only in networks with sufficient signal strength throughout the coverage area, otherwise clients could face connectivity issues</div> <div> <input type="checkbox"/> Enable Enable active disconnection of clients with weak signal </div> <div> <div>Roam SNR Threshold</div> <div>15</div> <div>SNR below which clients will be forced to roam (1-100 dB)</div> </div> </div>
Management	
Radio	
Network	
Security	
Access Control	
Services	



Note

Enable **Enhanced Roaming** only in networks with sufficient signal strength throughout the coverage area, otherwise clients could face connectivity issues.

- Expand the **Channel Scan** section and select the **Off Channel Scan** checkbox:

☐ **Channel Scan**

☐ Off Channel Scan

OCS periodically goes away from current operating channel (home channel) to other channels and collects data about neighboring clients, AP and RF characteristics.
Applicable to APs running 4.x Firmware (Wi-Fi5)

- Expand the **Auto-RF** section and configure any of the following modes:

- **Dynamic Channel**

AP Groups > Add New

Basic	<div> <div>Enhanced Roaming</div> <div>Channel Scan</div> <div>Auto-RF</div> </div> <div> <div>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.</div> <div>Mode Selection</div> <div> <div>Dynamic Channel</div> <div>Dynamic Power</div> </div> <div> <div> <input checked="" type="checkbox"/> Enable Enable Auto-RF to adjust dynamic channel selection based on RF conditions </div> <div> <input type="checkbox"/> Packet Error Rate Enable channel change using unsuccessful packet transmissions by the AP </div> <div> <input type="checkbox"/> Channel Utilization Enable channel change using the channel efficiency </div> <div> <input type="checkbox"/> Noise Enable channel change with higher noise </div> <div> <div>Samples</div> <div>3</div> <div>Configure the minimum number of samples required to run the channel selection (1-20)</div> </div> <div> <input type="checkbox"/> Enable time range for Auto-RF. <div>Configure time range (24 hour format) at which Auto-RF needs to run everyday.</div> </div> <div> <div>Channel Hold Time</div> <div>1440</div> <div>Channel 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'.</div> </div> <div> <div>Deprecated (Version 3.11.4 and 4.0)</div> <div> <div>Channel Selection Mode</div> <div>Interference</div> <div>Channel selection done based on interference</div> </div> <div> <div>Channel Utilization Threshold</div> <div>25</div> <div>Configure channel utilization threshold in %(20-40)</div> </div> </div> </div></div>
Management	
Radio	
Network	
Security	
Access Control	
Services	
User-Defined Overrides	



Note

The **Channel Hold Time** parameter specifies the time (in minutes) for which the AP will hold the channel.

The supported values vary as per the AP firmware version installed:

- 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.

Default value: 1440 minutes

• Dynamic Power

AP Groups > Add New

Basic
Management
Radio
Network
Security
Access Control
Services
User-Defined Overrides

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

Minimum Transmit Power
8
Minimum transmit power that the AP can assign to a radio when adjusting automatic cell sizes. (5-20) dBm

Minimum Neighbour Threshold
2
The Minimum number of neighbors to consider for power reduction by autotcell logic. (1-10)

Cellsize Overlap Threshold
50
Cell overlap that will be allowed when the AP is determining automatic cell sizes (0-100) %

9. Click **Save**.

External Antennas

This feature allows users to customize the antenna models for each of the three radios in the XE3-4TN AP as shown in [Figure 323](#). This customization helps in achieving optimal wireless network performance customized for specific deployment scenarios.

Figure 323 External Antennas for XE3-4TN APs

Model	Radio 1	Radio 2	Radio 3
XE3-4TN	Omnidirectional...	Omnidirectional...	Omnidirectional...

Save

Network

The **Network** page allows to configure **Ethernet Ports**, **VLANs**, **Routes** for IPv4 and IPv6, **DHCP Pool**, **Tunnels**, **PPPoE**, **VLAN Pool**, and **WWAN**.

Figure 324 Network: Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)

The screenshot shows the 'Configuration' page for 'Enterprise' in the 'Network' section. The 'Ethernet Ports' tab is active, displaying settings for 'Ethernet Port 1'. Under the 'Port Control' section, the '802.1X Authentication' checkbox is checked, and 'Single Host' is selected for 'Host Mode'. Below this is a 'VLANs' table with one entry: VLAN 1, dhcp, disabled, enabled, Allow from Wired and Wireless, Disabled. Further down is a 'Routes' section with fields for Default Gateway, Domain Name, DNS Server 1, and DNS Server 2.

Configuring 802.1X port-based authentication

802.1X authentication on Ethernet ports enhance the network security of the AP.

The AP supports 802.1X port-based authentication with the following authentication modes:

- Single-host authentication—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.
- Multi-host authentication—Authentication is enforced on all clients connecting to the wired port. After the first client authenticates, the port VLAN is assigned based on RADIUS assigned VLAN. Any further client connections to the port will be part of the initial Radius VLAN that was assigned.



Note

- By default, the 802.1X port-based authentication feature is enabled in the single-host authentication mode.
- 802.1X port-based authentication does not support CoA messages.

802.1X port-based authentication also requires a RADIUS AAA server for authentication and accounting.

To configure 802.1X, complete the following steps:

1. Navigate to **Configuration > Network > Ethernet Ports**.
2. Expand the **Port Control** section and select the **802.1x Authentication** checkbox.

The **Host Mode** field is enabled.

3. Select from the following authentication modes in the **Host Mode** dropdown list.
 - Single Host
 - Multi Host
4. Expand the **RADIUS Server** section and configure the following RADIUS server parameters for 802.1X authentication.

Table 72 *RADIUS Server parameters*

Parameters	Description	Range	Default
Authentication Server	<p>Specifies the authentication server details, such as:</p> <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 <p>A maximum of three RADIUS authentication servers can be configured.</p>	-	Disabled
Accounting Server	<p>Specifies the accounting server details, such as:</p> <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 accounting server. Default—1813 <p>A maximum of three RADIUS accounting servers can be configured.</p>	-	Disabled
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	Users can configure multiple Authorization and Accounting servers. Based on a number of wireless stations, the user can	-	Failover

Parameters	Description	Range	Default
	choose Failover mode. <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. 		
Interim update interval	Time (in seconds) to wait for sending RADIUS interim accounting update packets. Note: This interval is applicable only when you select the Start-Interim-Stop option in the Accounting Mode parameter.	10–65535	1800
Dynamic Authorization	This option is required, where there is CoA request from AAA/RADIUS server.	-	Enabled

IPv6 Support

IPv6 enables the next generation of large-scale IP networks by supporting addresses that are 128 bits long.



Note

- In the current release, IPv6 functionality is supported only for cnPilot Enterprise devices.
- IPv6 functionality is supported on cnPilot from System Release 4.0.

Configuring IPv6

To configure IPv6, perform the following:

1. Navigate to **Configuration Wi-Fi Profiles > AP Groups** tab.
2. Select **Network** tab and click **Edit VLAN**.

3. Click the (+) plus sign next to **IPv6** option.

IPv6

Mode
Static

IPv6 Address

Prefix Length

☒ Request Option All
Use IPv6 Gateway, DNS, DHCPv6 options received on this interface

General

Update

4. Select **Mode** from dropdown list. By default, the IPv6 Mode is **Disabled**. The different IPv6 modes are **Static**, **Stateless DHCPv6**, **Stateful DHCPv6**, and **Auto Configuration**.

IPv6

Mode
Static

Disabled

Static

Stateless DHCPv6

Stateful DHCPv6

Auto Configuration

Use IPv6 Gateway, DNS, DHCPv6 options received on this interface

General

Update

If **Static** is selected, provide the following details:

- **IPv6 Address:** Enter IPv6 address.
- **Prefix Length:** Enter IPv6 prefix. For example: 2001:1111:2222:3333::/64.

5. Enable **Request Option All** to use the IPv6 Gateway, DNS, DHCPv6 options received on this interface.
By default the priority of **IPv6 Gateway Source Precedence** is **Static** and then **Auto-config/DHCPv6**.

IPv6 Gateway Source Precedence

1	Static
2	Auto-config/DHCPv6

To create a new static Route,

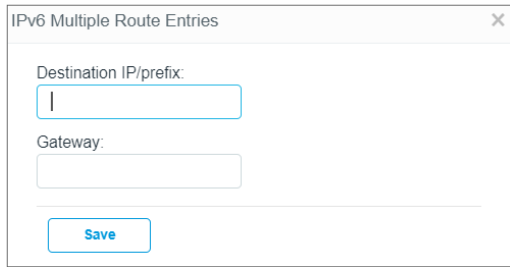
1. Navigate to **IPv6 Multiple Route Entries** section.
2. Click **Add New**.

IPv6 Multiple Route Entries

Destination IP	Gateway	Edit	Delete
No Multiple Routes available			

Add New

3. Enter **Destination IP/Prefix** and **Gateway**.



IPv6 Multiple Route Entries

Destination IP/prefix:

Gateway:

Save

4. Click **Save**.

To set the preference of IPv4 and IPv6:

1. Navigate to **Routes** tab.
2. Select the **IPv6 Preference** checkbox.



Routes

☒ IPv4 Routing & DNS

☒ IPv6 Routing & DNS

Default Gateway IP address of default gateway

Domain Name

DNS Server 1 Primary domain name server

DNS Server 2 Secondary domain name server

☐ IPv6 Preference Prefer IPv6 address over IPv4 for addresses resolved via DNS

Security

The **Security** page allows to configure **DoS Protection** and **Rogue AP**.

Map WLANs to AP Groups

WLANs are added in the AP Group configuration. Ensure the WLANs are ordered correctly if Mesh mode is used. When a WLAN uses Mesh Client mode it must always be the first WLAN in the AP Group, and only one Mesh Client WLAN is allowed per AP Group.

The ordering when using Mesh mode is as follows:

1. Client (maximum of one Mesh Client is selected)
2. Base (maximum of two Mesh Base is selected)
3. Recovery (maximum of one Mesh Recovery is selected)
4. WLANs with Mesh Mode Off (total WLAN limit including Mesh WLANs)



Note

Maximum of 16 WLAN policies are supported for E-Series and XV-Series devices. Only one WLAN is available for cnPilot Home devices.

Lock device Configuration

Locking automatically restores the configuration of devices if it is changed outside of cnMaestro. When this feature is enabled, external configuration changes are automatically reverted by reapplying the AP Group configuration. The configuration is pushed only if the device is in Sync status.

AP Groups > Add New

Basic

Management

Radio

Network

User Defined Overrides

Basic Information

Type: cnPilot Home (R-Series)

Name: ewe

Scope: Shared

☐ Auto Sync: Automatically push configuration changes to devices sharing this AP Group

Country: NONE For appropriate regulatory configuration

Description:

WLAN

Order	WLAN	Delete
No WLAN selected		

[Add WLAN](#) [Create WLAN](#)

[Save](#) [Close](#)

The default password **admin** of cnPilot R-Series should be changed before upgrading to the build 4.6-RX.

AP Groups > Add New

Basic

Management

Radio

Network

User Defined Overrides

Administrator Access

User Type: Admin User Choose the user type from admin user and normal user and basic user

New User Name: admin

New Password: Show Configure password for authentication of GUI and CLI sessions (max 25 characters)

After upgrading to 4.6-RX, the default password **admin** is invalid and needs to be reset through the WAN.



Note

Default User Name: **admin** can be used after the upgrade.

Apply AP Group to Device

A Configuration Job can be created as follows:

1. Navigate to **Monitor and Manage > System > Configuration**.

Figure 325 System Configuration (Enterprise Wi-Fi E-Series, XE,/XV/X7-Series)

System

Dashboard Notifications **Configuration** Statistics Reports X Software Update Applications X Clients Mesh Peers Assurance X Assists X

Device Type: Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)

Managed Account: All Accounts

Search

[Sync Configuration](#) [Configuration Jobs](#) [Configure](#)

Device	Managed Account	Configuration Group	Status	Sync Status	Network	Tower/Site
cnPilot-test	Base Infrastructure	APG_000_Test	Offline	Not In Sync	default	01_Enterprise Site
E500-8766E6-V3K-301a	Base Infrastructure	AA_CNM_Sit_Meeting_room	Online	In Sync	default	01WLAN-Test
Migration_04_XV22_02	Base Infrastructure	APG_000_Test	Online	Not In Sync	default	01WLAN-Test
Migration_06_XV2_2T1_02	eMSP	APG_000_Test	Online	Not In Sync	default	
-AP-7003E0-ESS	Base Infrastructure	_Wifi_7003E0	Online	In Sync	Durga-R	Rashin
-AP-700880-X	Base Infrastructure	N/A	Online	N/A	Rashin_Network	Rashin_Site
X7-35X-B0007A	Application issue testing-MSF	_voucher_testing	Online	In Sync	default	Application testing
X7-35X-B00254	Base Infrastructure	Default Enterprise	Online	In Sync	Kunal-BLR	Kunal-BLR
XE3-4TN-780144	Base Infrastructure	Sanity-Migration	Online	In Sync	test-raja	test
XE5-8-E00399	Base Infrastructure	AA_CNM_Sit_Meeting_room	Online	In Sync	default	01_Mixed_Devices-new-ijji

Showing 1 - 10 Total: 13 10 < Previous 1 2 Next >

2. Select from one of the following options in the **Device Type** dropdown list:

- cnPilot Home (R-Series)
- cnPilot Enterprise (ePMP Hotspot)

- Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)
 - Enterprise Wi-Fi (Xirrus-Series)
 - The list of enterprise Wi-Fi devices are listed.
3. Select the devices to which you want to apply the AP group.
 4. Click **Configure**.

The **System > Configuration** page is displayed.

Figure 326 Configuration page: Enterprise Wi-Fi (E-Series, XE,/XV/X7-Series)

Figure 327 Configuration page: cnPilot Home (R-Series)

Figure 328 Configuration page: Enterprise Wi-Fi (Xirrus-Series)

5. Select the AP group from the **AP Group** dropdown list.
6. Click **Apply Configuration**.

AP Group and WLAN Import/Export

The AP groups and WLANs are created for cnPilot Home and Enterprise Wi-Fi devices. The configurations that are created for each WLAN and AP group in a server can be exported and imported to a different server.



Note

From release 5.1.0, **Built-In** profiles will not be created for MSP accounts and you can create your own profile.

AP Groups												
WLANs Association ACL Access Control Policies Custom Applications X												
<div>Change Filter(s) Clear</div> <div>Device Type: All Scope: All Accounts</div> <div>Add Import Sync</div>												
Name	Scope	Type	AP Status	Clients Now	Clients 24 HR	Throughput (DL/UL)	AP Group	Guest Access	Last Updated	Last Updated By	Origin	
cm_sit_radius	Shared	Enterprise Wi-Fi	0 of 2 offline	1	1	0.37 Kbps / 0.64 Kbps	cm_sit_radius_2	Internal Access Point	24 Apr 2024, 12:47 AM		Custom	
JP-W7-11.2	Shared	Enterprise Wi-Fi	1 of 1 offline	0	1	0 Kbps / 0 Kbps	JP-S-DHCP-Pools-overlapping-J1	N/A	24 Apr 2024, 12:37 AM		Custom	
JP-W7-11.4	Shared	Enterprise Wi-Fi	0 of 0 offline	0	0	0 Kbps / 0 Kbps	JP-S-DHCP-Pools-NAT-DHCP	N/A	24 Apr 2024, 12:33 AM		Custom	
JP-W7-15	Shared	Enterprise Wi-Fi	0 of 0 offline	0	0	0 Kbps / 0 Kbps	JP-S-DHCP-Pools-NAT-DHCP	N/A	23 Apr 2024, 07:50 PM		Custom	
JP-W7-14	Shared	Enterprise Wi-Fi	0 of 0 offline	0	0	0 Kbps / 0 Kbps	JP-S-DHCP-Pools-NAT-DHCP	N/A	23 Apr 2024, 07:09 PM		Custom	
JP-W7-13	Shared	Enterprise Wi-Fi	0 of 0 offline	0	0	0 Kbps / 0 Kbps	JP-S-DHCP-Pools-NAT-DHCP	N/A	23 Apr 2024, 07:09 PM		Custom	
JP-W7-12	Shared	Enterprise Wi-Fi	0 of 0 offline	0	0	0 Kbps / 0 Kbps	JP-S-DHCP-Pools-NAT-DHCP	N/A	23 Apr 2024, 07:09 PM		Custom	
JP-W7-11	Shared	Enterprise Wi-Fi	0 of 0 offline	0	0	0 Kbps / 0 Kbps	JP-S-DHCP-Pools-NAT-DHCP	N/A	23 Apr 2024, 07:08 PM		Custom	
Vlax60_Acadia	Shared	Enterprise Wi-Fi	0 of 1 offline	0	3	0 Kbps / 0 Kbps	Vlax_Acadia_7_dot_0_Baseinf	N/A	23 Apr 2024, 06:18 PM		Custom	
JP-W7-17	Shared	Enterprise Wi-Fi	0 of 0 offline	0	0	0 Kbps / 0 Kbps	JP-S-DHCP-Pools-NAT-DHCP	N/A	23 Apr 2024, 05:26 PM		Custom	
Showing 1 - 10 Total: 520 10 < Previous 1 2 3 4 5 ... 52 Next >												

AP Groups												
WLANs Association ACL Access Control Policies Custom Applications X												
<div>Search Clear</div> <div>Device Type: All Scope: All Accounts WLAN: All</div> <div>Add New Import Sync</div>												
Name	Type	AP Status	Scope	Clients Now	Clients 24 HR	Throughput (DL/UL)	WLANs	Auto Sync	Last Updated	Last Updated By	Origin	
diva_RCA	Enterprise Wi-Fi (E-Series, XE...	1 of 5 offline	Base Infrastructure	6	6	125.36 Kbps / 4.39 K...	diva_ra_rca_diva_w...	ON	04 Apr 2024, 12:18 PM		Custom	
MOULI MONITOR_HOST	Enterprise Wi-Fi (E-Series, XE...	0 of 0 offline	Shared	0	0	0 Kbps / 0 Kbps	MOULI_MH_WLAN1...	ON	04 Apr 2024, 12:09 PM		Custom	
DhayaWIDS	Enterprise Wi-Fi (E-Series, XE...	0 of 1 offline	Shared	5	5	0.29 Kbps / 0.28 Kbps	Dhaya-max-wids-rog...	ON	04 Apr 2024, 12:08 PM		Custom	
Vlax_Acadia_7_dot_0_B...	Enterprise Wi-Fi (E-Series, XE...	0 of 1 offline	Shared	6	6	23.48 Kbps / 7.86 Kb...	Default_Acadia_Vlax...	OFF	04 Apr 2024, 11:51 AM		Custom	
Acadia_APGP	Enterprise Wi-Fi (E-Series, XE...	0 of 1 offline	Shared	3	3	9.3 Kbps / 186.07 Kbps	Acadia_WLAN_Acad...	ON	04 Apr 2024, 11:02 AM		Custom	
sachin-ra-ra-ra-srv-4	Enterprise Wi-Fi (E-Series, XE...	0 of 1 offline	Sachin	0	0	0 Kbps / 0 Kbps	Sachin-wlan-ra-ra-s...	ON	03 Apr 2024, 06:57 PM		Custom	
Tiger_OS2_Osnoburck	Enterprise Wi-Fi (E-Series, XE...	0 of 1 offline	Base Infrastructure	38	58	123.49 Mbps / 73.7 M...	OS2-WPA2-EAP_Osn...	OFF	03 Apr 2024, 05:09 PM		Custom	
Jaquar_OS2_Osnoburck	Enterprise Wi-Fi (E-Series, XE...	0 of 1 offline	Base Infrastructure	18	37	64.16 Mbps / 30.55 M...	OS2-WPA2-EAP_Osn...	OFF	03 Apr 2024, 05:08 PM		Custom	
JP-W7-Mar11	Enterprise Wi-Fi (E-Series, XE...	0 of 1 offline	Shared	3	3	0.64 Kbps / 0.55 Kbps	JP-W7-Mar11	ON	03 Apr 2024, 12:59 PM		Custom	
Dhaya-Alethea	Enterprise Wi-Fi (E-Series, XE...	0 of 0 offline	Base Infrastructure	0	0	0 Kbps / 0 Kbps	Dhaya-Alethea room...	ON	02 Apr 2024, 07:00 PM		Custom	
Showing 1 - 10 Total: 231 10 < Previous 1 2 3 4 5 ... 24 Next >												

Export AP Groups and WLANs

To export AP Group or WLANs, perform the following steps:

1. Navigate to **Configuration > Wi-Fi Profiles** page.
2. Select **AP Group** or **WLAN** tab.
3. Click **Export** icon in the row of the AP Group or WLANs to export.



Note

- The AP Groups and WLANs should be exported separately as the associated WLANs are not included while exporting an AP Group.
- The AP Groups and WLANs will be exported with proper name and timestamp.

Import AP Groups and WLANs

To import AP Group and WLANs, perform the following steps:

1. Navigate to **Configuration > Wi-Fi Profiles** page.
2. Select **AP Group** or **WLAN** tab.
3. Click **Import**.

Import AP Group window appears.

1. Enter the **Name**.
2. Select the **Scope** from dropdown.
3. Select the **Configuration file** in JSON format.
4. Click **Import**.



Note

- To import an AP Group, ensure all associated WLANs in the AP Group are already imported. If the WLAN associated with the AP Group is unavailable, an error message will be displayed during import.
- If the name is not provided for WLAN or AP Group while importing, it will take the name of the imported file.
- If the name provided for the AP Group/WLAN is already in use, an error message **The specified policy name already exists** will be displayed.

Creating a WLAN

To create a WLAN, perform the following steps:

1. Navigate to **Configuration > Wi-Fi Profiles > WLAN** tab, or WLAN page in the Wireless LAN View.
2. In **WLAN** tab select **New**.

As with AP Groups, WLANs are separated into cnPilot Home and Enterprise Wi-Fi. You can configure WLAN, RADIUS, Guest Access, Usage Limits, Scheduled Access, and Access parameters with Enterprise Wi-Fi WLANs. With the cnPilot Home WLANs, you can configure SSID, Scheduled Access, and Access parameters.



Note

- Special characters can be used to create AP Group and WLAN names (Eg: a-zA-Z_-*%#@!<>.[^~\$1234567890). The user can also rename the AP group and WLAN names, if required.
- The MAC authentication fallback feature works only when Guest Access is configured with RADIUS authentication under **WLANs > Guest Access > Access Policy > RADIUS**.

To create a WLAN, perform the following steps:

1. Navigate to **Configuration > Wi-Fi Profiles**.
2. Select **WLANs** tab and then click **Add**.
3. Enter **Type**, **Name**, and WLAN parameters.
4. Ensure **WPA2 PSK** is enabled in **Security** dropdown.



Note


- WPA3 security standard is not supported on Enterprise Wi-Fi 5 APs (version 4.x.)
- To support ePSK with WPA3, you must select either the **WPA2/WPA3 Pre-shared Keys** or **WPA3 Pre-shared Keys** option in the **Security** dropdown list, and configure ePSK passphrase.
- ePSK support with WPA3 requires a cnMaestro X subscription.
- When the **Security** parameter is configured with the **WPA2 Pre-Shared Keys** option, 6 GHz clients connect to the AP using the secure Simultaneous Authentication of Equals (SAE) method.


For information on client (WPA2 and WPA3-compliant) registration with ePSK passphrase, see [ePSK registration for WPA3 clients](#).



The following table lists the description of the basic and advanced parameters available in the WLAN tab:

Table 73 WLAN > Basic Settings parameters

Parameters	Description	Range	Default
WLAN > Basic Settings parameters			
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	This parameter is required when a WDS connection is established with Enterprise Wi-Fi devices. This parameter supports the following options: <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.	-	Off (Access Profile Mode)

Parameters	Description	Range	Default
	<ul style="list-style-type: none"> • 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. 		
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 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. • Osen 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. • OWE (Enhanced Open) This method ensures the communication between each pair of endpoints is protected from other endpoints. • WPA2 Pre-Shared Keys 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. <div style="display: flex; align-items: center;">  <div style="margin-left: 10px;"> <p>Note</p> <p>6 GHz clients connect to the AP using the secure Simultaneous Authentication of Equals (SAE) method.</p> </div> </div> <ul style="list-style-type: none"> • WPA2 Enterprise This security type uses 802.1x authentication to associate wireless stations. This is a centralized system of authentication methods. • WPA2/WPA3 Pre-shared Keys 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 SAE method. • WPA3 Pre-shared Keys 	-	Open

Parameters	Description	Range	Default
	<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> <p>Note</p> <p>When you select WPA2/WPA3 Pre-shared Keys or WPA3 Pre-shared Keys, you can enable registration flow for WPA3 clients.</p> <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> </div> </div> <ul style="list-style-type: none"> • WPA3 Enterprise <p>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.</p> <ul style="list-style-type: none"> • WPA3 Enterprise CNSA <p>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.</p> <ul style="list-style-type: none"> • User Pre-shared keys <p>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.</p>		
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
Passphrase	The string that is a key value to generate keys based on the security method configured.	-	12345678

Parameters	Description	Range	Default
Client Isolation	<p>Enable this feature when there is a need for restriction of wireless station-to-station communication across the network or on an AP.</p> <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. that is, 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 <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> 		








Parameters	Description	Range	Default
	 <p>Note 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>		
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>  <p>Note Following priority takes precedence for the session timeout:</p> <ol style="list-style-type: none"> Configured from the RADIUS server Configured from the AP 	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>  <p>Note Following priority takes precedence for the inactivity timeout:</p> <ol style="list-style-type: none"> Configured from the RADIUS server Configured from the AP 	60-28800	1800

Table 74 WLAN > 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:	–	Disabled

Parameters	Description	Range	Default																														
	<ul style="list-style-type: none">Disabled This feature is disabled for this WLAN.Radius Based 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.Static 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/IPv6 address from the VLAN selected by the Enterprise Wi-Fi AP device.																																
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 for more details.	1-512 (Refer)	256																														
UAPSD	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. <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																														
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																														

Parameters	Description	Range	Default
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
Insert DHCP Option 82	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: <ul style="list-style-type: none"> • Hostname • AP MAC • BSSID • SSID • VLAN ID • SITEID • Custom • All 	–	Disabled

Parameters	Description	Range	Default
	 <p>Note</p> <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 		
Tunnel Mode	This option is enabled when user traffic is tunneled to the DMZ network either using L2TP or L2GRE.	–	Disabled
Fast-Roaming Protocol	<p>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.</p> <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>	–	Disabled
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 • Support for WPA2 authentication method 	–	Disabled
802.11v	Provision to enable 802.11v BSS Transition Management.	–	Disabled
PMF	802.11w also termed as Protected Management Frames (PMF) Service, defines	–	Option

Parameters	Description	Range	Default
(802.11w)	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.		al
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

5. Click **Save**.



Note

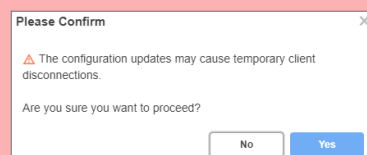
In 6 GHz Band, **Open** option is not supported in **Security**.



Warning

After creating a WLAN, any modifications to the WLAN parameters may cause client disconnections. The following warning message is displayed when saving the WLAN:

Figure 329 *Warning when modifying WLAN*



ePSK registration for WPA3 clients



Note

ePSK support for WPA3 clients requires a cnMaestro X subscription.

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. Here 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](#)
- [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.

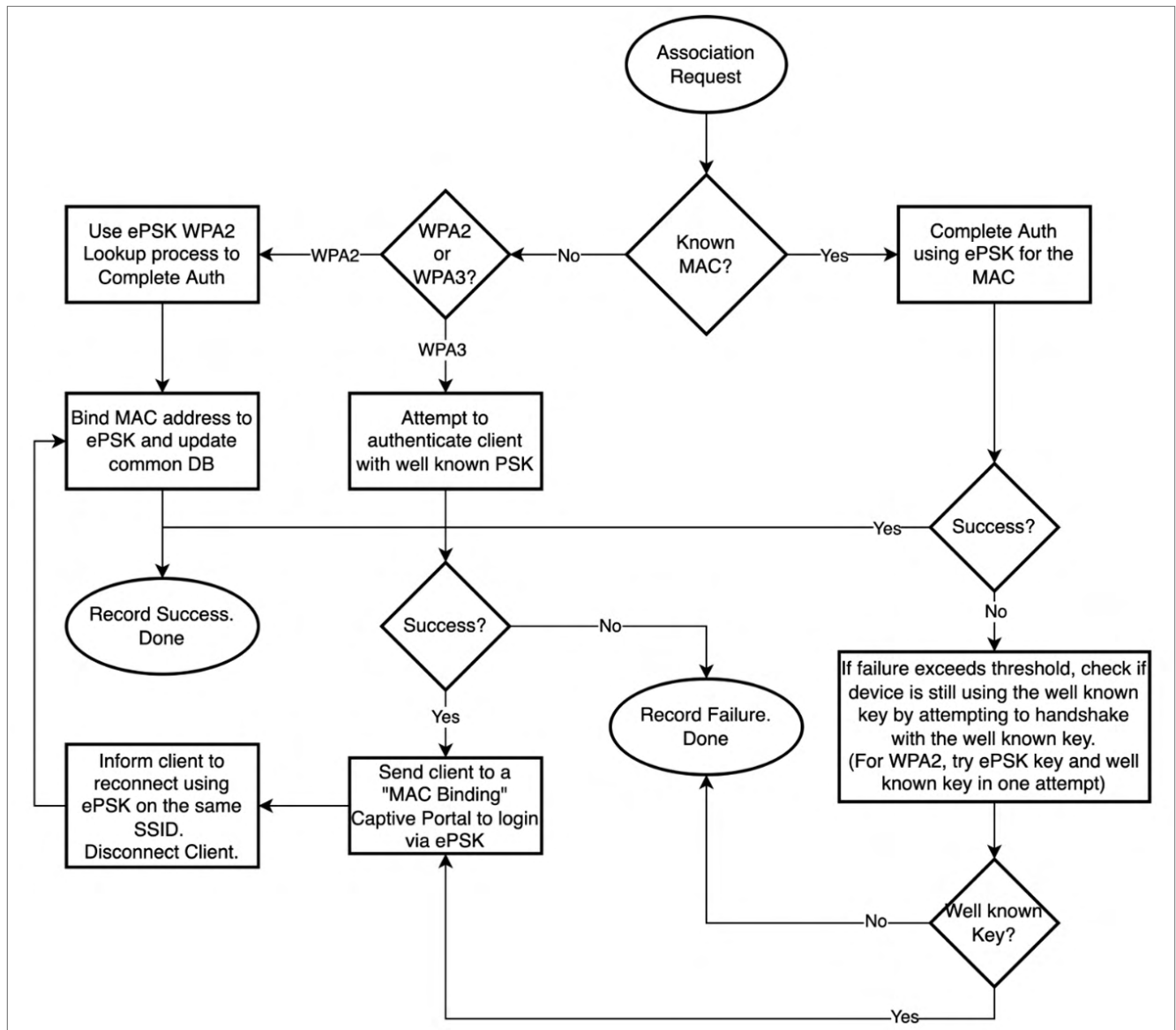
Scenarios while registering clients

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 330 Client registration flow for WPA3 clients



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** dropdown 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** dropdown 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 331 Message on the ePSK page when no ePSK entries are added

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.

Passphrase Strength
☐ Easy ☒ Strong ☐ Number This allows Alphanumeric and Special Characters (up to 16 Characters)

☐ This WLAN uses WPA3 security. Client registration flow is required and will be enabled when ePSK entries are added. Client registration flow is supported only on cnMaestro X. 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](#) [Export QR Code](#) [Delete](#)

<input type="checkbox"/>	User Name	MAC Address	Passphrase	Creation Date	Expiration Da...	Status	VLAN
No Data Available							

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

- 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** dropdown list, the following messages appear respectively

Figure 332 When **WPA3 Pre-shared Keys** option is selected

SSID

☒ Enable

SSID*

ePSK-WPA3 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

WPA3 Pre-Shared Keys Set authentication and encryption type

☐ 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.

Passphrase*

wlanpassword Hide WPA3 Pre-shared security passphrase or key (must contain 8 to 63 ASCII or 64 Hexadecimal digits)

Figure 333 When **WPA2/WPA3 Pre-shared Keys** option is selected

SSID

☒ Enable

SSID*

ePSK-WPA3 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/WPA3 Pre-Shared Keys Set authentication and encryption type

☐ Registration flow for ePSK is enabled for WPA3 clients. [Learn more](#) on how to enable WPA3 with ePSK.

Passphrase*

wlanpassword Hide WPA2/WPA3 Pre-shared security passphrase or key (must contain 8 to 63 ASCII or 64 Hexadecimal digits)

- Click the **ePSK** tab and add the passphrase.

After the ePSK passphrase is added, the following message is displayed explaining the registration flow.

Figure 334 Message on the ePSK page when ePSK entries are added

Passphrase Strength
☐ Easy ☒ Strong ☐ Number This allows Alphanumeric and Special Characters (up to 16 Characters)

ⓘ This WLAN uses WPA3 security. Client registration flow is active and is supported only on cnMaestro X. 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](#) [Export QR Code](#) [Delete](#)

<input type="checkbox"/>	User Name	MAC Address	Passphrase	Creation Date	Expiration Date	Status	VLAN	
<input type="checkbox"/>	ePSK	N/A	epskpassword@1234	May 01 2025 13:01:21	May 01 2026 13:01:43	Active	N/A	Edit Delete

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

- To download the QR code for the WLAN and the ePSK passphrase, click **Export QR Code**.

The QR code is downloaded in a PDF file as shown below.

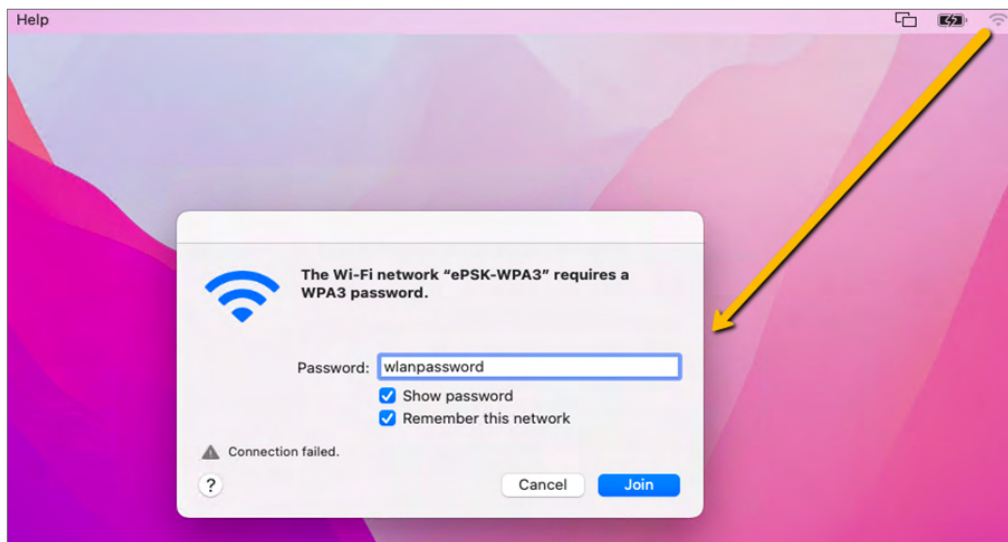


Registration flow screenshots

To register the clients to the network using the ePSK passphrase, users must complete the following steps:

- Connect the client to the network using the WLAN passphrase.

Figure 335 Using WLAN passphrase for connecting to network



- 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 336 Using ePSK passphrase for connecting

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

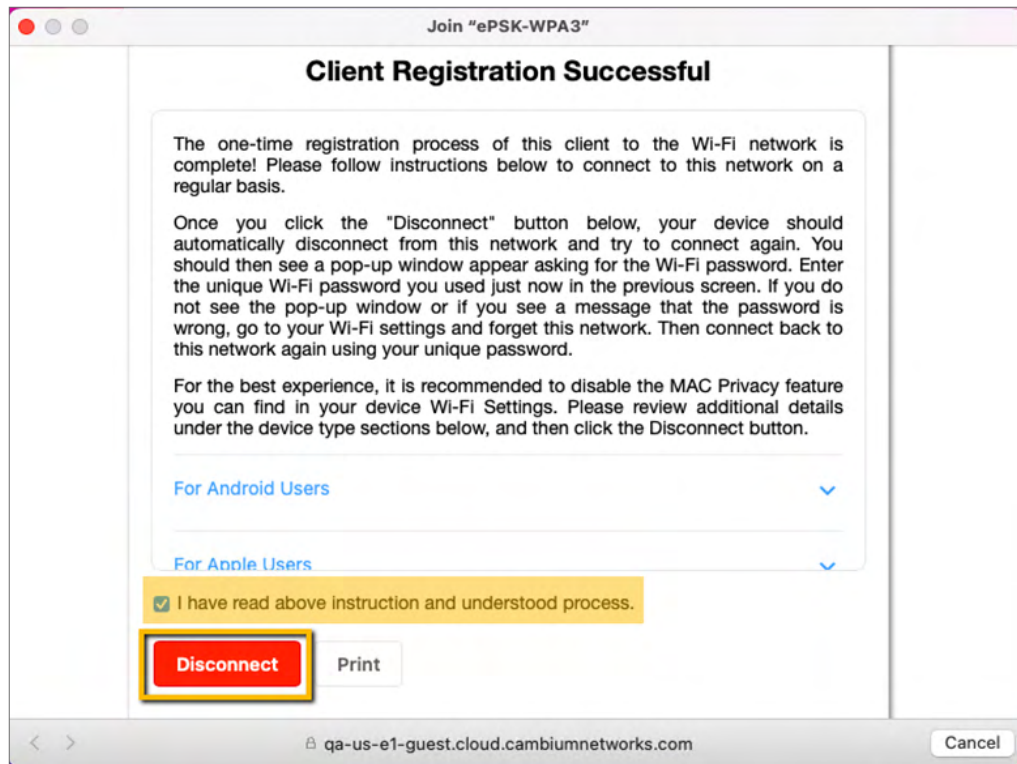
The registration success page is displayed along with a set of instructions.

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.

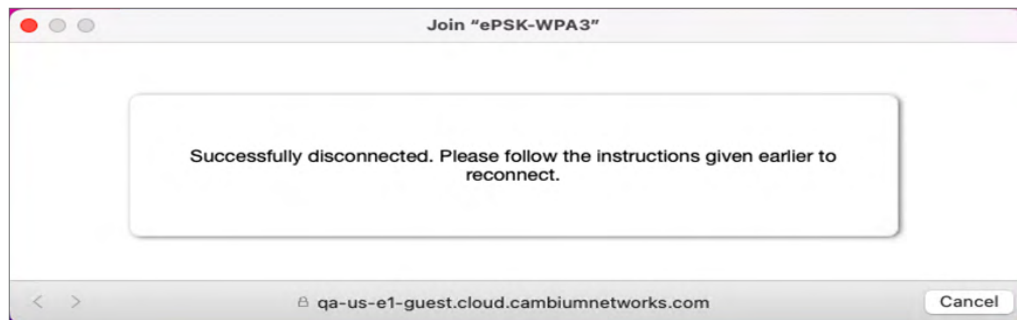
Figure 337 *Registration success page with instructions*



5. Click **Disconnect**.

The client is disconnected and a disconnect success message is displayed.

Figure 338 *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 339 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 an ePSK WLAN

To create an ePSK WLAN, perform the following steps:

1. Navigate to **Configuration > Wi-Fi Profiles** or WLAN page in the Wireless LAN View.
2. Select **WLANs** tab and click **Add**.

As with AP Groups, WLANs are separated into cnPilot Home (R-Series), Enterprise Wi-Fi, and RV22 Home Mesh types. You can configure WLAN, RADIUS, Guest Access, Usage Limits, Scheduled Access, and Access parameters with Enterprise Wi-Fi WLANs. With the cnPilot Home WLANs, you can configure SSID, Scheduled Access, and Access parameters.



Note

- The special characters can be used to create AP Group and WLAN names (Eg: a-zA-Z_-*&%#@!<>().[]^~\$1234567890). The user can also rename them if required.
- By default, password will not be configured. User has to configure the password for WLAN.

To create WLAN policy, perform 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** dropdown 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** dropdown list.

WLANs > Add New

WLAN
AAA Servers
Guest Access
Access Control
Passpoint
ePSK

Basic Information

Type*
Enterprise Wi-Fi
Name*
Scope*
Description

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
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 Hexadecimal digits)
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

5. Click **Save**.
6. In the **ePSK** page select the type of passphrase strength in the **Passphrase Strength** field (Available options: **Easy**, **Strong**, or **Number**).

WLANs > cambium-wlan

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
Export QR Code
Delete

<input type="checkbox"/>	User Name	MAC Address	Passphrase	Creation Date	Expiration Date	Status	VLAN
No Data Available							

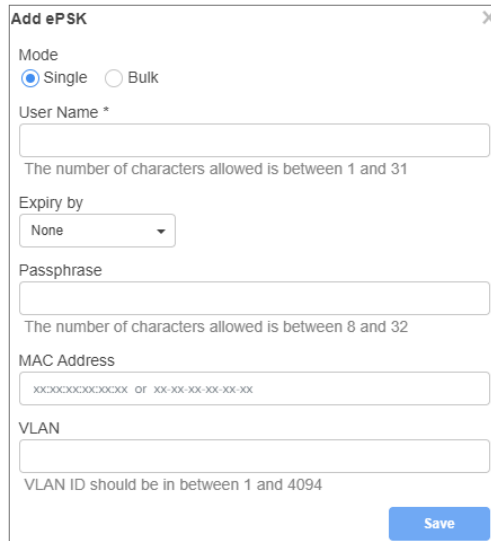
Showing 0 - 0 Total: 0 25 < Previous Next >

7. Click **Add New**.

The **Add ePSK** window is displayed.

8. Select the **Mode** parameter as one of the following:

- **Single:** In the single mode, only one entry is created. Only the **User Name** parameter is mandatory and the others are optional.



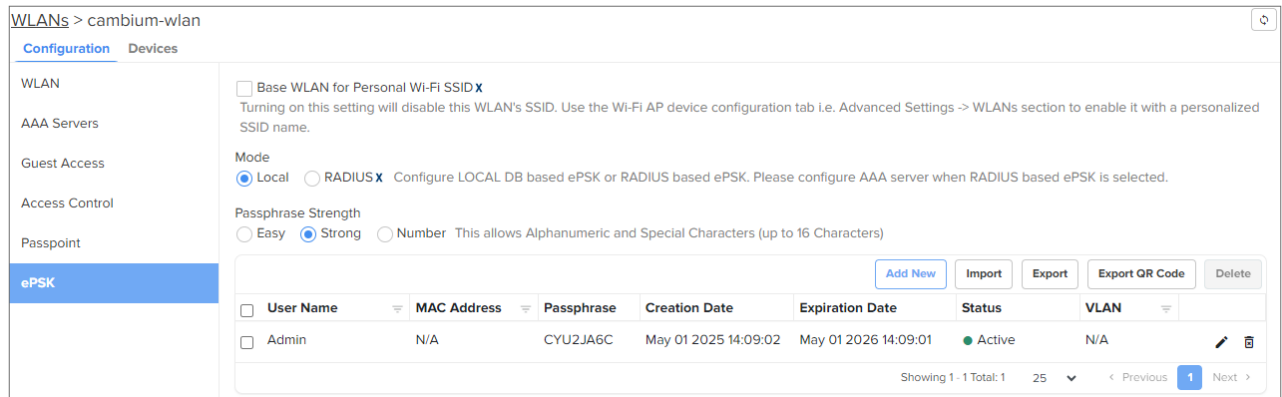
The 'Add ePSK' form contains the following fields and options:

- Mode:** Radio buttons for **Single** (selected) and **Bulk**.
- User Name ***: A text input field with a note: "The number of characters allowed is between 1 and 31".
- Expiry by**: A dropdown menu with **None** selected.
- Passphrase**: A text input field with a note: "The number of characters allowed is between 8 and 32".
- MAC Address**: A text input field with a placeholder: "XX:XX:XX:XX:XX:XX or XX-XX-XX-XX-XX-XX".
- VLAN**: A text input field with a note: "VLAN ID should be in between 1 and 4094".
- Save**: A blue button at the bottom right.



Note

Passphrase is optional and unless manually configured, it will be automatically generated based on the selected **Passphrase Strength**.



The configuration page for WLANs > cambium-wlan shows the following settings:

- Base WLAN for Personal Wi-Fi SSID**: ☐ (disabled)
- Mode**: **Local** (selected), **RADIUS** (disabled). Note: "Configure LOCAL DB based ePSK or RADIUS based ePSK. Please configure AAA server when RADIUS based ePSK is selected."
- Passphrase Strength**: **Easy** (disabled), **Strong** (selected), **Number** (disabled). Note: "This allows Alphanumeric and Special Characters (up to 16 Characters)".
- Buttons**: Add New, Import, Export, Export QR Code, Delete.
- Table**: A table with columns: User Name, MAC Address, Passphrase, Creation Date, Expiration Date, Status, and VLAN. It contains one entry: Admin, N/A, CYU2JA6C, May 01 2025 14:09:02, May 01 2026 14:09:01, Active, N/A.
- Footer**: Showing 1 - 1 Total: 1, 25, < Previous, 1, Next >

- In the **Bulk** mode, the **Count** and **User Name Prefix** are mandatory. There are multiple entries in this mode.

The bulk mode supports a minimum of two and a maximum of 2000 passphrases.

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 "a-b".

Save

WLANs > cambium-wlan

Configuration

Devices

WLAN

AAA Servers

Guest Access

Access Control

Passpoint

ePSK

☐ Base WLAN for Personal Wi-Fi SSID

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

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

Export QR Code

Delete

<input type="checkbox"/>	User Name	MAC Address	Passphrase	Creation Date	Expiration Date	Status	VLAN	
<input type="checkbox"/>	Admin-1	N/A	1QHxDseP	May 01 2025 14:03:47	May 01 2026 14:03:47	Active	N/A	
<input type="checkbox"/>	Admin-10	N/A	kBfNV6Pv	May 01 2025 14:03:47	May 01 2026 14:03:47	Active	N/A	
<input type="checkbox"/>	Admin-11	N/A	knzeH9z4	May 01 2025 14:03:47	May 01 2026 14:03:47	Active	N/A	
<input type="checkbox"/>	Admin-12	N/A	UgvYtbQx	May 01 2025 14:03:47	May 01 2026 14:03:47	Active	N/A	
<input type="checkbox"/>	Admin-13	N/A	NZXr16A4	May 01 2025 14:03:47	May 01 2026 14:03:47	Active	N/A	
<input type="checkbox"/>	Admin-14	N/A	3tKpvhfg	May 01 2025 14:03:47	May 01 2026 14:03:47	Active	N/A	
<input type="checkbox"/>	Admin-15	N/A	7AYyRPbB	May 01 2025 14:03:47	May 01 2026 14:03:47	Active	N/A	
<input type="checkbox"/>	Admin-16	N/A	e9XpUeCz	May 01 2025 14:03:47	May 01 2026 14:03:47	Active	N/A	
<input type="checkbox"/>	Admin-17	N/A	qHSxqWaN	May 01 2025 14:03:47	May 01 2026 14:03:47	Active	N/A	
<input type="checkbox"/>	Admin-18	N/A	BsBx3ta4	May 01 2025 14:03:47	May 01 2026 14:03:47	Active	N/A	

Showing 1 - 10 Total: 20 10 < Previous 1 2 Next >

9. To automatically expire ePSK details after a specific duration. The following options are available:

- **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.
- **Duration**— ePSK expires after the specified (in hours, days, months, or years) in the **Expiry by** dropdown. Supported minimum duration is one hour and the maximum is five years. No decimal values are supported, for example, 1.5 hours.



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.

10. Click **Save**.

11. To download the QR code for the WLAN and the ePSK passphrase, click **Export QR Code**.



Note

- The **Export QR Code** button is enabled only after the ePSK passphrases are created and the WLAN is saved.
- Nine QR codes are supported per page in the PDF.

The QR code is downloaded in a PDF file as shown below.

Figure 340 Sample PDF with exported QR codes



Creating a Personal Wi-Fi ePSK X

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. For example, a user can connect multiple devices to a single personal Wi-Fi.

To configure personal Wi-Fi on the AP, complete the following steps:

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.

Import ePSK

1. Click **Import**.

The screenshot shows the 'WLANs > cm_sit_Property' configuration page. The 'ePSK' tab is selected in the left sidebar. In the main content area, the 'Base Personal SSID' checkbox is checked. Below it, the 'Mode' is set to 'Local'. The 'Passphrase Strength' is set to 'Strong'. At the bottom right, there are buttons for 'Add New', 'Import' (highlighted with a red box), 'Export', and 'Delete'. Below these buttons is a table header with columns: 'User Name', 'MAC Address', 'Passphrase', 'Creation Date', 'Expiration Date', 'Status', and 'VLAN'. The table body is empty, displaying 'No Data Available'.

2. Select **Import.csv** file.

The screenshot shows the 'Add PSK' dialog box. It has a text input field for 'CSV File' with 'Import.csv' entered. Below the input field are three buttons: 'Import', 'Cancel', and 'Download Sample File'.

Alternatively, one can import a CSV file containing a list of ePSK entries. A sample file format is available from the Import dialog.

3. Click **Download Sample File**, to view sample ePSK Excel sheet.

	A	B	C	D	E
1	username	mac	passphrase	vlan	expiration_time
					Expiration time should be either none or Jun 22 2024 09:07:28 format only
2	Unique name of this entry	MAC address of the client, if any (optional)	The Passphrase (Pre Shared Key) to be used in the WPA2 handshake	The VLAN to which the client traffic should be mapped (optional)	
3	Lounge-1	11:11:11:11:11:11	646jny5ab;~B(!;		9 Jun 22 2024 08:34:28
4	Lounge-2	22:22:22:22:22:22	9jef!;a!*8GUS3%		10 Aug 22 2024 05:07:28
5	Lounge-3		*[!nQgUdeM2ErR		1 Jul 27 2024 19:07:28
6	Lounge-4]j!tam6F1)x!Zgg%		2 May 22 2024 12:07:28

Export ePSK

1. Click **Export**.
2. Select **export.csv** file.

WLANs > cm_sit_Property

Configuration Devices

WLAN

AAA Servers

Guest Access

Access Control

Passpoint

ePSK

☐ Base Personal SSID **X**
Enabling Personal SSID will disable WLAN SSID. WLAN SSID needs to be enabled from the device configuration tab i.e. Advanced Settings -> WLANs section.

Mode **X**
☒ Local ☐ RADIUS
 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"/>	test1	N/A	BS>"z7UyZv9t...	Wed, Jul 19, 2023	-	Active	N/A	...

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

	A	B	C	D	E	F	G	H	I
1	username	mac	passphrase	vlan					
2	Unique name	MAC address	The Passphrase	The VLAN to which the client traffic should be mapped (optional)					
3	Room-1		WVghr85mY_a;Q(e						
4	Room-2		a[n5&HepkU~nQt%						
5	Room-3		6q@Qk#WU8JzC.Br)						
6	Room-4		eX~gInIj tZw(j						
7	Room-5		y5cqdS(IYAww5gl;p						
8	Room-6		;Ag EBKk8KNRS*c						
9	Room-7		8H(SF)u;m9C4_MQ=						
10	Room-8		_(hgH7;dzb Ys~9w						
11	Room-9		7%(C5bqDMpt^(j2]						
12	Room-10		3mq=xY~zg&fni/mN%						

Editing ePSK

To edit an ePSK, select the required ePSK and click the edit () icon in the row.

You can edit only the passphrase and the expiry duration information.

Deleting ePSK

To delete an ePSK, select the required ePSK and click **Delete**. You can also click the delete () icon in the row.

To delete multiple ePSK entries, select the checkboxes corresponding to the ePSK entries and click **Delete**.



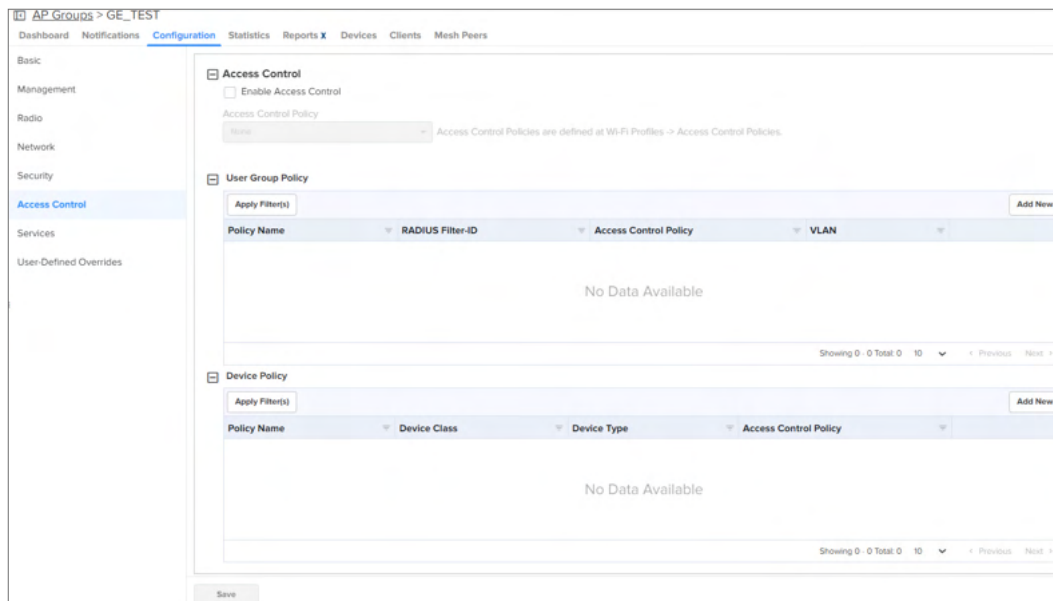
Note

ePSK feature is supported on cnPilot from Release version 3.11.1.

Access Control

The Access Control page allows user to enable or assign access control policies and configure **User Group Policy** and **Device Policy**. It offers visibility into the configured rules, ensuring efficient and secure network management.

Figure 341 Access Control page



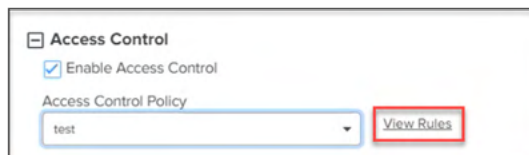
Note

If an Access Control Policy is assigned at the AP group level, it does not appear under User Group or Device Group policies.

Enable Access Control Policy

Users have the provision to enable or disable access control policies under **Access Control** tab as shown in [Figure 342](#).

Figure 342 Enabling Access Control Policy



Note

User can select the available access control policies listed in Wi-Fi profiles in **Access Control Policy** dropdown list. User can review the configured rules associated with these policies by clicking **View Rule** icon as shown in [Figure 342](#). This provides a comprehensive view of the policies and rules within the network.

User Group Policy

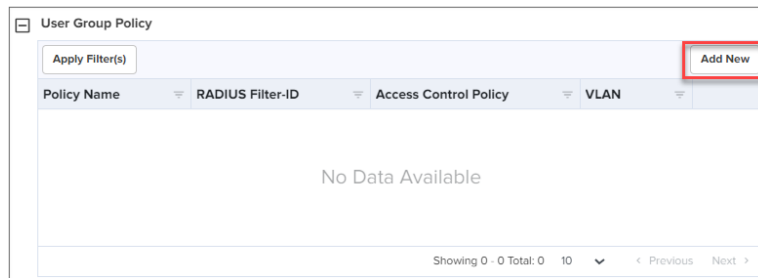
User Group Policy enables users to categorize into specific roles with customized access permissions and restrictions, facilitating fine-tuned control over network access.

Adding a new User Group Policy

To add a new User Group Policy, perform the following steps:

1. Navigate to **Configuration > Access Control** page.
2. Click **Add New** in the top right corner of the User Group Policy as shown in [Figure 343](#).

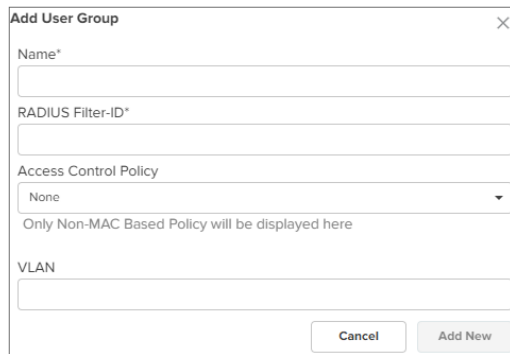
Figure 343 User Group Policy



The screenshot shows a table titled "User Group Policy". At the top right, there is a red-bordered button labeled "Add New". The table has columns: "Policy Name", "RADIUS Filter-ID", "Access Control Policy", and "VLAN". The table body is empty, displaying "No Data Available". At the bottom, it shows "Showing 0 - 0 Total: 0 10" and navigation links for "Previous" and "Next".

3. Complete the details in the **Add User Group** pop-up window as shown in [Figure 344](#).

Figure 344 Add User Group



The screenshot shows the "Add User Group" pop-up window. It contains the following fields and controls:

- Name***: A text input field.
- RADIUS Filter-ID***: A text input field.
- Access Control Policy**: A dropdown menu currently showing "None". Below it, a note states: "Only Non-MAC Based Policy will be displayed here".
- VLAN**: A text input field.
- At the bottom right, there are two buttons: "Cancel" and "Add New".



Note

- The user needs to assign an Access Control Policy or VLAN to create a User Group.
- Users can add a maximum of 64 User Groups and Device Policies each.
- Users can only select Access Control Policies (ACPs) with NON-MAC filters from the **Access Control Policy** dropdown menu.
- Mapping an Access Control Policy (ACP) to a User Group Policy (UGP) enables its use for the AP group, and vice versa. However, the same ACP cannot be shared between UGP and AP group; you can apply it to only either UGP or AP group.

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.

Adding a new Device Policy

To add a new Device Policy, perform the following steps:

1. Navigate to **Configuration > Access Control** page.
2. Click **Add New** in the top right corner of the Device Policy as shown in [Figure 345](#).

Figure 345 *Device Policy*

3. Complete the details in the **Add Device Policy** pop-up window as shown in [Figure 346](#).

Figure 346 *Add Device Policy*

Services

The **Services** tab allows to configure the **LDAP**, **NAT Logging**, **DHCP Option 82**, **Speed Test**, **Bonjour**, **Application Visibility**, and **RTLS (Real-Time Location System)** such as **Wi-Fi API**, **Bluetooth API**, and **Stanley-AeroScout**.



Note

Stanley - AeroScout and **Application Visibility** are cnMaestro X features.

Stanley-AeroScout X

Stanley-AeroScout delivers an accurate and reliable location data for assets and customers with the STANLEY Healthcare Wi-Fi tags. It is an integral component of STANLEY Healthcare's Stanley-AeroScout RTLS solutions. The Stanley-AeroScout determines a location using signal strength measurements (RSSI) which are collected by Cambium Wi-Fi APs. These Wi-Fi APs can simultaneously serve location sensors and provide network access. Stanley-AeroScout utilizes a location engine to determine the position of Wi-Fi tags.

Stanley - AeroScout X

☐ Enable Wi-Fi ⓘ

☐ Enable Bluetooth ⓘ

Host:

Port:

Pre-Defined Overrides

Some device configuration is specific to an individual device and not easily shared through an AP Group. This includes IP Address, Radio Channel settings, and WLAN details such as Enabling/Disabling SSID and Passphrase. These items can be configured in the Device Configuration page, which can be selected by choosing **Manage > Configuration** in the menu, and then selecting the device in the tree to update.

You can then choose/change different values from AP Group to be overridden. The icon to the left of a field must be selected first to override that parameter. After specifying override parameters, select **Apply Configuration** on the bottom right to save your changes to the server and create a job to push the new values to the device. This option is also applicable for Onboarding process queue.

Advanced Settings

By default, Enterprise Wi-Fi devices have **Auto-set from device** enabled. This option reads several network related configuration fields from the device and uses those as override values to prevent overwriting values that would disconnect the device.

Modify the **Advanced Settings** section on the Access Point level configuration page as below:

- Add option to override Dual 5 GHz Radio setting for XV3-8 APs below the Placement field.
- If the Dual 5 GHz Radio feature is **Enabled**, then show the settings to override/configure the 3rd 5 GHz radio.
- If the Dual 5 GHz Radio option is enabled, then allow channel range ≥ 100 for Radio 2 and 36 – 64 for Radio 3.

Wi-Fi > XV2-2-Config

Dashboard Notifications **Configuration** Details Performance Software Update Tools Clients Mesh Peers WLANs

Device Details

Managed Account

Base Infrastructure [Change](#)

Name: XV2-2-Config

Network: default

Site: None

Description:

Latitude: 0.0

Longitude: 0.0

[Set the device location using a map](#)

Serial Number:

MAC Address:

IP Address: 10.10.0.88

Sync Status: N/A

Device Configuration

[View Device Configuration](#)

AP Group: 00:04:58:85:AF:62-Alpha [Edit](#) [Create](#)

WLAN used by AP Group: MI_2-TheFallen [Cap_America](#)

Advanced Settings

[Radio and Location](#) cnMaestro VLAN (VLAN 1) Other VLANs WLANs

Override	Field Name	Value	Default Value
<input type="checkbox"/>	Location	Bengaluru	Bengaluru
<input type="checkbox"/>	Placement	<input checked="" type="radio"/> Indoor <input type="radio"/> Outdoor	Indoor

Radio 1

Override	Field Name	Value	Default Value
<input type="checkbox"/>	State	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	Enabled
<input type="checkbox"/>	Band	2.4 GHz	2.4 GHz
<input type="checkbox"/>	Channel	auto	auto
<input type="checkbox"/>	Channel Width	20	20
<input type="checkbox"/>	Transmit Power	auto	auto

Radio 2

Override	Field Name	Value	Default Value
<input type="checkbox"/>	State	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	Enabled
<input type="checkbox"/>	Band	5 GHz	5 GHz
<input type="checkbox"/>	Channel	auto	auto
<input type="checkbox"/>	Channel Width	80	80
<input type="checkbox"/>	Transmit Power	auto	auto

[Configuration Variables \(Advanced\)](#)

[Factory Reset](#)

[Apply Configuration](#) [View Configuration Jobs](#)



Note

XE3-4TN features a radio antenna override option.

Advanced Settings

[Radio and Location](#) cnMaestro VLAN (VLAN 1) Other VLANs **WLANs**

MI_2-TheFallen

Override	Field Name	Value	Default Value
<input type="checkbox"/>	SSID	MI_2-TheFallen	MI_2-TheFallen
<input type="checkbox"/>	Enable SSID	<input checked="" type="checkbox"/>	true
<input type="checkbox"/>	Passphrase	***** Show	12345678

Cap_America

Override	Field Name	Value	Default Value
<input type="checkbox"/>	SSID	Cap_America	Cap_America
<input type="checkbox"/>	Enable SSID	<input checked="" type="checkbox"/>	true
<input type="checkbox"/>	Passphrase	***** Show	12345678

[Configuration Variables \(Advanced\)](#)

[Factory Reset](#)

[Apply Configuration](#) [View Configuration Jobs](#)

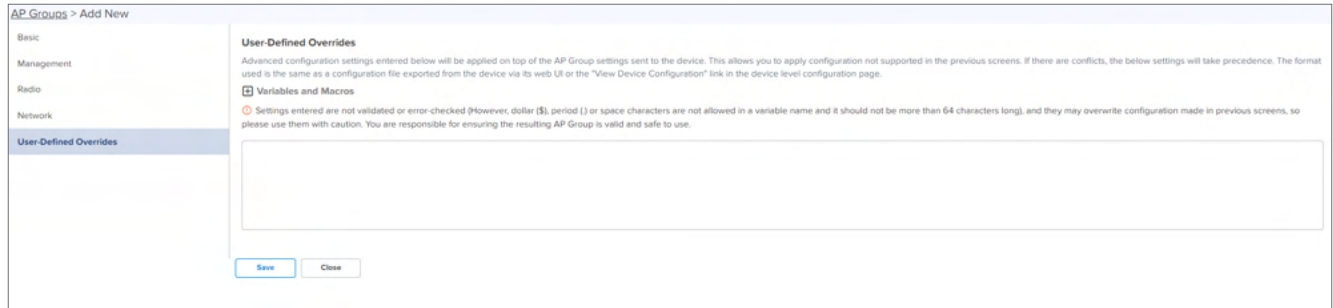
User-Defined Overrides

User-Defined Overrides can be entered into the end of an AP Group configuration. They will be appended to the AP Groups before the configuration is applied to the device. This allows setting configuration parameters which are not supported by GUI; this is an advanced operation that should rarely be used. The format of the commands is same as with the device CLI.

For example, if a new version of the software had a feature unsupported in cnMaestro, it could be pushed to the device using CLI commands through the User-Defined Override mechanism.

This can be explained with the following example, in which country-code and hostname are appended to the end of the configuration and will override any settings in the UI.

```
country-code IN
hostname Wi-Fi_Device
```



User-Defined Variables

Override configuration also supports a programmatic concept called User-Defined Variables (which are also used with templates). User-Defined Variables can be embedded into the User-Defined Override text area. They require a value to be set for each device mapped to the AP Group before the configuration can be applied. This is either through a default value, or an explicit setting in the device configuration.

The syntax for User-Defined Variables is shown in the following example: the VariableName maps to an identifier set by each Device. If the value is not set, the optional DefaultValue will be used.

```
Parametername ${VariableName=DefaultValue}
```



Note

You can also configure User-Defined Variables in the Onboarding process queue page. They are mapped individually to each device.

Other Examples

Enterprise Wi-Fi (E-Series and XV-Series) and cnPilot Enterprise (ePMP hotspot)

```
country-code ${countryname=US} // country name with US as default value
hostname ${hostname=ePMP_1000_Hostpot}
```

cnPilot Home R-Series

```
Parametername ${variableName=someDefaultValue}
```

Example

```
CountryCode=${countryName=IE}
RTDEV_CountryCode=${5GHz_CountryName=IE}
wan_ipaddr=${wan_ip=10.110.68.10}
```

Macros can be used in advanced configuration similar to User-Defined Overrides, except that they automatically obtain values provided by the device itself.

The following macros are supported:

- `%{ESN}` will be replaced with the MAC address of device.
- `%{esn}` will be replaced with the MAC address of the device in lowercase.
- `%{ESN-}` will be replaced with the MAC address of the device separated by a hyphen (-).
- `%{esn-}` will be replaced with the MAC address of the device in lowercase separated by a hyphen (-).
- `%{ESN6}` will be replaced with the last six non-separator characters of the device MAC address.
- `%{esn6}` will be replaced with the last six non-separator characters of the device MAC address in lowercase.
- `%{MSN}` will be replaced with the serial number of the device.

Bulk Overrides

Bulk Overrides allow the user to edit the multiple configurations shared through an AP Group for one or more devices.



Note

Bulk Edit option under **Configuration > Devices Overrides** is supported only for cnMaestro X.

The user can override for the following configurations in cnPilot (R-Series):

- [Management](#)
- [Radios](#)
- [Wi-Fi Configuration](#)

Figure 347 Bulk Override: cnPilot (R-Series)

The user can override for the following configurations in Enterprise Wi-Fi (E-Series, XV-Series):

- [Location](#)
- [Management VLAN](#)
- [Radios](#)

- [WLANs](#)
- [User-Defined Variables](#)

Figure 348 Bulk Override: Enterprise Wi-Fi (E-Series, XE-Series, XV-Series)



Note

Configuration tab will be available from other container levels like Network/Site and also from AP group level.

To configure Bulk Overrides for the devices, perform the following steps:

1. Navigate to **Manage > System > Configuration**.
2. Select the **Device Type** from the dropdown.
3. Select **Device** from the list and click **Configure**.

Device	Managed Account	AP Group	Status	Sync Status	Network	Tower/Site
<input checked="" type="checkbox"/> E410-5FFFC3	Base Infrastructure	BULK_APGROUP_MULTIWLAN	Online	In Sync	Bulk-Nw-WiFi	Bulk_Site
<input checked="" type="checkbox"/> E500MeshBase-B8C4DE-DONOTTOUCH	Base Infrastructure	N/A	Online	N/A	rai001	Mesh-Site-DoNotTouch
<input checked="" type="checkbox"/> E500MeshClient-B86A58-DONOTTOUCH	Base Infrastructure	N/A	Online	N/A	rai001	Mesh-Site-DoNotTouch
<input checked="" type="checkbox"/> E600-9661A2	Base Infrastructure	BULK_APGROUP_MULTIWLAN	Online	Not In Sync	rai001	Tom-JerrySite
<input checked="" type="checkbox"/> E700-1D0AE0	Base Infrastructure	BULK_APGROUP_MULTIWLAN	Online	In Sync	rai001	Tom-JerrySite
<input checked="" type="checkbox"/> XV3-8-EBF900	Base Infrastructure	THOR_APGROUP_APPVISI	Online	Not In Sync	rai001	Tom-JerrySite

4. Click the plus (+) next to **Device Override(s)**, to override the list of devices.
5. In the Device Override table, reconfigure tabs and perform the following actions:
 - Bulk Edit
 - Export
 - Import

System > Configuration

Device Type: cnPilot Home (R-Series)

Managed Account: All Accounts

Configuration Method: ☒ AP Group ☐ Template

AP Group: tl_r_series_clientdashboard_WFTK115CL20Q

WLANs: tl_r_clientdashboard_WFTK115CL20Q

Device Overrides

Device Name	Admin Mode Password
190V_Test	

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

Buttons: Apply Configuration, Schedule Configuration, Cancel

6. Select the device(s) from the Device Override table to configure.

7. Click **Bulk Edit**.

A pop-up window appears for the fields to reconfigure.

8. Click **Save**.

You can export, as described:

- Export page as CSV
- Export all as CSV

After modifying the field values, the CSV file can be imported.

System > Configuration

Device Type: Enterprise Wi-Fi (E-Series, XV-Series)

Managed Account: All Accounts

AP Group: 6-X-EPSK-PARTIAL-CONFIG

WLANs: 6-X-EPSK-PARTIAL-CONFIG, EPSK-SECOND-WLAN-PARTIAL-CFG

Device Override(s)

Buttons: Apply Configuration, Schedule Configuration, Cancel

9. Click **Import**, to import the file.

10. Select the file to import in CSV file format.

11. Click **Apply**.

Location

1. In the **Location** tab, select the devices from the list.

2. Click **Bulk Edit**.

System > Configuration

Device Type
Enterprise Wi-Fi (E-Series, XV-Series)

Managed Account
All Accounts

AP Group
-6-X-EPK-PARTIAL-CONFIG AP Groups listing only for device type - Enterprise Wi-Fi (E-Series, XV-Series)

WLANs
-6-X-EPK-PARTIAL-CONFIG, EPK-SECOND-WLAN-PARTIAL-CFG

Device Override(s)

Location Management VLAN Radios WLANs User-Defined Variables

Search

Bulk Edit (6) X

Device Name	Location	Placement
<input checked="" type="checkbox"/> E500MeshClient-B86A58-DONOTTOUCH		Indoor
<input checked="" type="checkbox"/> E500MeshBase-B8C4DE-DONOTTOUCH		Indoor
<input checked="" type="checkbox"/> E410-5FFFC3	BULK-SITE19	Indoor
<input checked="" type="checkbox"/> E600-9661A2		Indoor
<input checked="" type="checkbox"/> E700-1DOAE0		Indoor
<input checked="" type="checkbox"/> XV3-8-EBF900		Indoor

Showing 1 - 6 Total: 6 10 < Previous 1 Next >

Apply Configuration Schedule Configuration Cancel

3. **Override Location** window appears, edit the configuration details and click **Save**.

Override Location

☒ Location Prefix/Suffix Increment By

Suffix 1

☒ Placement

Outdoor

Close Save

Management VLAN

4. In the **Management VLAN** tab, select the **VLAN** of the device from the list.

System > Configuration

Device Type
Enterprise Wi-Fi (E-Series, XV-Series)

Managed Account
All Accounts

AP Group
Kunal-6-X-EPK-PARTIAL-CONFIG AP Groups listing only for device type - Enterprise Wi-Fi (E-Series, XV-Series)

WLANs
Kunal-6-X-EPK-PARTIAL-CONFIG, EPK-SECOND-WLAN-PARTIAL-CFG

Device Override(s)

Location **Management VLAN** Radios WLANs User-Defined Variables

Search

Bulk Edit X

Device Name	cnMaestro VLAN	IP Type	IP Address	Gateway	Domain Name Serv...
<input type="checkbox"/> E500MeshClient-B86A58-DONOTTOUCH	<input checked="" type="checkbox"/> Auto set from device	IPv4	Static IP 10.10.208.201 255.255.255.0	10.10.208.254	10.10.12.10 10.10.12.11
<input type="checkbox"/> E500MeshBase-B8C4DE-DONOTTOUCH	<input checked="" type="checkbox"/> Auto set from device	IPv4	Static IP 10.10.208.200 255.255.255.0	10.10.208.254	10.10.12.10 10.10.12.11
<input type="checkbox"/> E410-5FFFC3	<input checked="" type="checkbox"/> Auto set from device	IPv4	DHCP	N/A	10.10.12.10 10.10.12.11
<input type="checkbox"/> E600-9661A2	<input checked="" type="checkbox"/> Auto set from device	IPv4	DHCP	N/A	10.10.12.10 10.10.12.11
<input type="checkbox"/> E700-1DOAE0	<input checked="" type="checkbox"/> Auto set from device	IPv4	Static IP 10.10.212.213 255.255.255.0	10.10.212.254	10.10.12.10 10.10.12.11
<input type="checkbox"/> XV3-8-EBF900	<input checked="" type="checkbox"/> Auto set from device	IPv4	DHCP	N/A	10.10.12.10 10.10.12.11

Showing 1 - 6 Total: 6 10 < Previous 1 Next >

Apply Configuration Schedule Configuration Cancel

5. Click **Bulk Edit**.

System > Configuration

Device Type
Enterprise Wi-Fi (E-Series, XV-Series)

Managed Account
All Accounts

AP Group
Kunal-6-X-EPSK-PARTIAL-CONFIG AP Groups listing only for device type - Enterprise Wi-Fi (E-Series, XV-Series)

WLANs
Kunal-6-X-EPSK-PARTIAL-CONFIG, EPSK-SECOND-WLAN-PARTIAL-CFG

☒ Device Override(s)

Location Management VLAN Radios WLANs User-Defined Variables

Search

Device Name	cnMaestro VLAN	IP Type	IP Address	Gateway	Domain Name Serv...
<input checked="" type="checkbox"/> E500MeshClient-B86A58-DONOTTOUCH	<input checked="" type="checkbox"/> Auto set from device	IPv4	Static IP 10.10.208.201 255.255.255.0	10.10.208.254	10.10.12.10 100.0.0.0, 100.0.0.0
<input checked="" type="checkbox"/> E500MeshBase-B8C4DE-DONOTTOUCH	<input checked="" type="checkbox"/> Auto set from device	IPv4	Static IP 10.10.208.200 255.255.255.0	10.10.208.254	10.10.12.10 10.10.12.11
<input checked="" type="checkbox"/> E410-5FFFC3	<input checked="" type="checkbox"/> Auto set from device	IPv4	DHCP	N/A	100.0.0.0, 100.0.0.0 100.0.0.0, 100.0.0.0
<input checked="" type="checkbox"/> E600-9661A2	<input checked="" type="checkbox"/> Auto set from device	IPv4	DHCP	N/A	100.0.0.0, 100.0.0.0 100.0.0.0, 100.0.0.0
<input checked="" type="checkbox"/> E700-1D0AE0	<input checked="" type="checkbox"/> Auto set from device	IPv4	Static IP 10.10.212.213 255.255.255.0	10.10.212.254	10.10.12.10 10.120.134.201
<input checked="" type="checkbox"/> XV3-8-EBF900	<input checked="" type="checkbox"/> Auto set from device	IPv4	DHCP	N/A	100.0.0.0, 100.0.0.0 100.0.0.0, 100.0.0.0

Showing 1 - 6 Total 6 10 < Previous 1 Next >

Apply Configuration Schedule Configuration Cancel

Bulk Edit (6) X

6. **Override Management VLAN** window appears, edit the changes and click **Save**.

Override Management VLAN

☐ Auto set from device

☐ Type
IPv4

☐ IP Mode
DHCP

☐ DNS1
100.0.0.0, 100.0.0.0

☐ DNS2
100.0.0.0, 100.0.0.0

Close Save

Radios

In the **Radio** tab, select the radios from the device list, to perform **Import** and **Export** actions.

System > Configuration

Device Type
Enterprise Wi-Fi (E-Series, XV-Series)

Managed Account
Basic Infrastructure

AP Group
00-04-56-91-78-1E-APGroup AP Groups listing only for device type - Enterprise Wi-Fi (E-Series, XV-Series)

WLANs
202_Rgm_Client_connectivity

☒ Device Overrides

Location Management VLAN Radios WLANs User-Defined Variables

Search

Device Name	Radio	Band	Status	Channel	Transmit Power	Channel Width
AP-1-E500-B82238	Radio 1	2.4 GHz	Enabled	Auto	Auto	20MHz
AP-1-E500-B82238	Radio 2	5 GHz	Enabled	Auto	Auto	80MHz
2-MC-E510-C8443D	Radio 1	2.4 GHz	Enabled	Auto	Auto	20MHz
2-MC-E510-C8443D	Radio 2	5 GHz	Enabled	Auto	Auto	80MHz

Showing 1 - 4 Total 4 10 < Previous 1 Next >

Apply Configuration Schedule Configuration Cancel

Import X Export X



Note

Bulk Edit tab is removed from Radio configuration from 3.1.1 release.

7. Export the report to edit the radio parameters. You can export the radio parameter details as described:

- Export page as CSV
- Export all as CSV

After modifying the field values, the CSV file is imported.

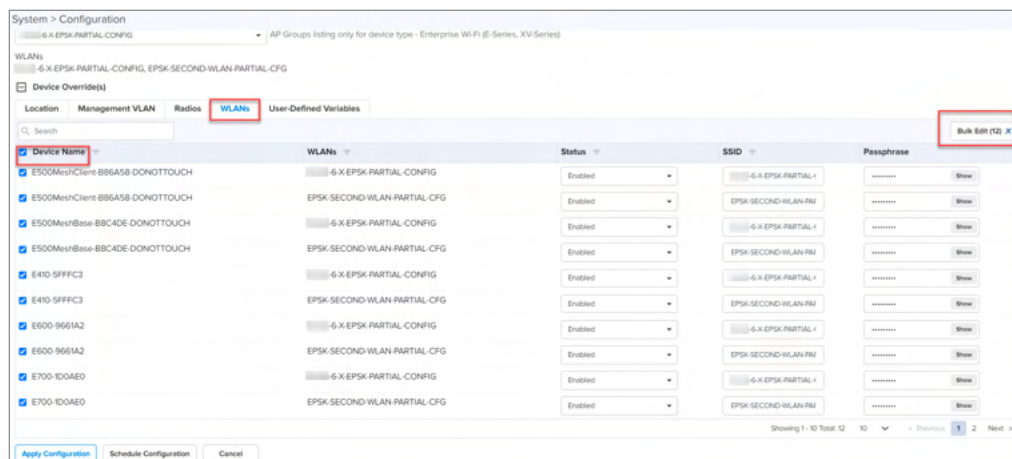
8. Click **Import**, to import the file.

9. Select the file to import in CSV file format.

10. Click **Apply Configuration** to start immediately, or click **Schedule Configuration** to schedule later.

WLANs

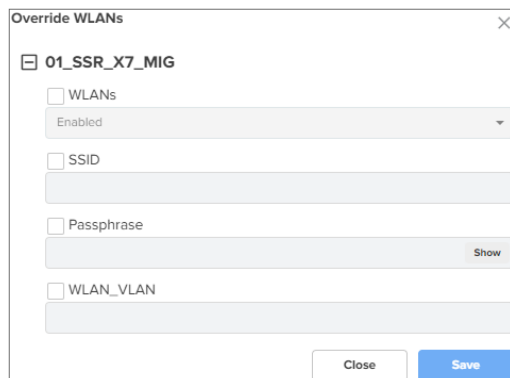
11. In the **WLANs** tab, select the WLAN of the devices from the list.



Device Name	WLANs	Status	SSID	Passphrase
E500MeshClient-B86A58-DONOTTOUCH	6-X-EPSK-PARTIAL-CONF	Enabled	6-X-EPSK-PARTIAL	Show
E500MeshClient-B86A58-DONOTTOUCH	EP5K-SECOND-WLAN-PARTIAL-CFG	Enabled	EP5K-SECOND-WLAN-PN	Show
E500MeshBase-B8C4DE-DONOTTOUCH	6-X-EPSK-PARTIAL-CONF	Enabled	6-X-EPSK-PARTIAL	Show
E500MeshBase-B8C4DE-DONOTTOUCH	EP5K-SECOND-WLAN-PARTIAL-CFG	Enabled	EP5K-SECOND-WLAN-PN	Show
E410-5FFFC3	6-X-EPSK-PARTIAL-CONF	Enabled	6-X-EPSK-PARTIAL	Show
E410-5FFFC3	EP5K-SECOND-WLAN-PARTIAL-CFG	Enabled	EP5K-SECOND-WLAN-PN	Show
E600-9661A2	6-X-EPSK-PARTIAL-CONF	Enabled	6-X-EPSK-PARTIAL	Show
E600-9661A2	EP5K-SECOND-WLAN-PARTIAL-CFG	Enabled	EP5K-SECOND-WLAN-PN	Show
E700-100AED	6-X-EPSK-PARTIAL-CONF	Enabled	6-X-EPSK-PARTIAL	Show
E700-100AED	EP5K-SECOND-WLAN-PARTIAL-CFG	Enabled	EP5K-SECOND-WLAN-PN	Show

12. Click **Bulk Edit**.

13. **Override WLANs** window appears, edit the configuration details and click **Save**.



Override WLANs

☒ 01_SSR_X7_MIG

☐ WLANs
Enabled

☐ SSID
[Input Field]

☐ Passphrase
[Input Field] Show

☐ WLAN_VLAN
[Input Field]

Close Save

User-Defined Variables

14. In the **User-Defined Variables** tab, select the devices from the list.

System > Configuration

Device Type: Enterprise Wi-Fi (E-Series, XV-Series)

Managed Account: Base Infrastructure

AP Group: BULK_APGROUP (AP Groups listing only for device type - Enterprise Wi-Fi (E-Series, XV-Series))

WLANs: BULK_SSD_WITH_OVR, BULK_WLAN

Device Override(s)

Location Management VLAN Radios WLANs **User-Defined Variables**

Search

<input checked="" type="checkbox"/> Device Name	logging_level	syslog_host_ip
<input checked="" type="checkbox"/> KV3-8-ESP900	2	1111
<input checked="" type="checkbox"/> E500MeshClient-B86A58-DONOTTOUCH	2	1111
<input checked="" type="checkbox"/> E500MeshBase-B8C4DE-DONOTTOUCH	2	1111
<input checked="" type="checkbox"/> E410-5FFFC3	5	5790
<input checked="" type="checkbox"/> E600-9661A2	2	1111
<input checked="" type="checkbox"/> E700-1D0AED	2	1111

Showing 1-6 Total 6

Apply Configuration Schedule Configuration Cancel

15. Click **Bulk Edit**.

The **Override User-Defined Variables** window appears.

Edit User Defined Variables

☐ logging_level

☐ syslog_host_ip

Save Close

16. Edit the configuration details and click **Save**.



Note

For Bulk overrides to be enabled in **User-Defined Overrides** tab, you must define the overrides in the **User-Defined Overrides** section of AP groups. For more details, see [User-Defined Overrides](#)

17. Click **Apply Configuration** to start immediately, or click **Schedule Configuration** to schedule later.

The user can override for the following configurations in Enterprises Wi-Fi (Xirrus-Series):

- User-Defined Variables

Figure 349 Bulk Override: Enterprises Wi-Fi (Xirrus-Series)

System > Configuration

Enterprise Wi-Fi (Xirrus-Series)

Managed Account: All Accounts

AP Group: test@hvac (AP Groups listing only for device type - Enterprise Wi-Fi (Xirrus-Series))

Device Overrides

User-Defined Variables

Search

<input type="checkbox"/> Device Name	name	location
<input type="checkbox"/> X4096080F0EAA		
<input type="checkbox"/> X4096170F296A		from_cnmaestro

Showing 1-2 Total 2

Apply Configuration Schedule Configuration Cancel

Bulk Edit X Import X Export X

18. In the **User-Defined Variables** tab, select the devices from the list.



19. Click **Bulk Edit**. The **Override User-Defined Variables** window appears , edit the configuration details and click **Save**.
20. Click **Apply Configuration** to start immediately, or click **Schedule Configuration** to schedule later.

Synchronize (Sync) Configuration

AP Groups can be configured to synchronize automatically or manually when they are updated. The setting is available in the AP Group configuration page.

1. **Enterprise Wi-Fi AP Groups** by default synchronize automatically (so any change of AP Group or WLAN, followed by a **Save**, will immediately push configuration to the devices without manual intervention).
2. **cnPilot Home AP Groups** by default synchronize manually. Updates to them (or the WLANs to which they map) need manual synchronization to push configuration to the devices.

Manual Synchronization

Manual configuration synchronization allows the user to synchronize any devices with a single action rather than updating each device separately.

Navigate to **Administration > Sync Configuration**.

Sync Configuration only displays devices currently **Out-of-Sync** with a mapped AP Group.

Sync Configuration has the following fields:

- AP Group (AP Group to which device is mapped)
- Device (Hostname)
- Device Type
- Network (Network in which device is present)
- Status (Up/Down)
- Site (Site under which device is present)
- Sync Status (Sync status will tell whether job is completed or failed)

Steps to Sync Configuration:

1. Click the **Sync Configuration** in the top right of the **Configuration > WLAN and AP Groups** or **Manage > Configuration > Device Details** or **Jobs** tab.
2. Select devices to synchronize.

Administration > Sync Configuration

AP Groups can be configured to synchronize automatically or manually when they are updated. [Learn more](#)

Search Device Type: All Managed Account: All Accounts

Device	Type	Status	Managed Account	Network	Site	Configuration Group	Sync Status
<input type="checkbox"/> Migration_04_XE34_01	XE3-4	Offline	A_Sekhar_Reddy_Monitor	default	MSP_Mixed_Devices_Monitor	APG_CNM_SIT_ESeries_Migration	Device out of sync : Configuration failed: country_codeCountry not supported on this sku
<input type="checkbox"/> Migration_08_R190V_02	cnPilot r190V	Offline	A_Sekhar_Reddy_Administrator	default	MSP_Mixed_Devices_Admin	R-SERIES_AP_GRP	Device out of sync : Configuration failed: Device timed out while waiting for update
<input type="checkbox"/> Migration_02_R195P_02	cnPilot r195P	Online	Base Infrastructure	default	01_Mixed_Devices	R-SERIES_AP_GRP	Device out of sync : Device's configuration changed outside of cnMaestro
<input type="checkbox"/> Migration_04_R195W_02	cnPilot r195W	Online	Base Infrastructure	default	01_Mixed_Devices	R-SERIES_AP_GRP	Device out of sync : Device's configuration changed outside of cnMaestro
<input type="checkbox"/> Migration_05_R200P_01	cnPilot r200P	Online	Base Infrastructure	default	01_Mixed_Devices	R-SERIES_AP_GRP	Device out of sync : Device's configuration changed outside of cnMaestro
<input type="checkbox"/> Migration_06_R190V_01	cnPilot r190V	Online	Base Infrastructure	default	01_Mixed_Devices	R-SERIES_AP_GRP	Device out of sync : Device's configuration changed outside of cnMaestro
<input type="checkbox"/> Migration_07_R190W_01	cnPilot r190W	Online	Base Infrastructure	default	01_Mixed_Devices	R-SERIES_AP_GRP	Device out of sync : Device's configuration changed outside of cnMaestro
<input type="checkbox"/> Migration_11_R200P_02	cnPilot r200P	Online	Base Infrastructure	default	01_Mixed_Devices	R-SERIES_AP_GRP	Device out of sync : Device's configuration changed outside of cnMaestro

Showing 1 - 8 Total 10 Previous Next

10 Devices selected

Job Options

☐ Stop update on critical error

Devices to update in parallel (1-500)

Notes

3. Click **Sync Now**.



Note

- Sync Configuration can only be used if an AP Group is already mapped to the device.
- Software Update Jobs can be scheduled in parallel irrespective of other running Jobs in cnMaestro X. Configuration and Software Update jobs execute sequentially if mapped to the same device.

Configuration Job Status

After applying the configuration, the Configuration Job status is viewed at:

- Navigate to **Monitor and Manage > Configuration > View Update Jobs** (for Access and Backhaul devices) or
- **Administration > Jobs** (for Wireless LAN devices).

When the configuration is pushed from the Sync Configuration page, a Configuration job will be created in the background.

Administration > Jobs

Configuration Update Software Update Reports Actions

All Managed Account: All Accounts Delete

ID	Details	Managed Account	Occurrence	Target	Created by	Created on	Completed on	Parallel	Stop on Error	Sector Priority	Status
<input type="checkbox"/> 4357	1 cnMatrix EX2010 device(s)	Base Infrastructure	Now	cnMatrix-Sylogis.co...	Durga Prasad	May 15, 2021 12:47	May 15, 2021 12:47	-	false	N/A	Completed: <div><div></div></div>
<input type="checkbox"/> 4356	1 device(s)	Base Infrastructure	Now		Auto-Sync	May 15, 2021 12:47	May 15, 2021 12:47	15	false	N/A	Completed: <div><div></div></div>
<input type="checkbox"/> 4355	1 device(s)	Base Infrastructure	Now		Auto-Sync	May 15, 2021 12:46	May 15, 2021 12:46	15	false	N/A	Completed: <div><div></div></div>
<input type="checkbox"/> 4354	1 cnMatrix EX2010 device(s)	Base Infrastructure	Now	Default Switch	Durga Prasad	May 15, 2021 12:46	May 15, 2021 12:46	-	false	N/A	Completed: <div><div></div></div>
<input type="checkbox"/> 4353	1 device(s)	Base Infrastructure	Now		Auto-Sync	May 14, 2021 16:10	May 14, 2021 16:11	15	false	N/A	Completed: <div><div></div></div>
<input type="checkbox"/> 4352	1 device(s)	Base Infrastructure	Now		Auto-Sync	May 14, 2021 15:52	May 14, 2021 15:52	15	false	N/A	Completed: <div><div></div></div>
<input type="checkbox"/> 4351	1 device(s)	Base Infrastructure	Now		Auto-Sync	May 14, 2021 15:51	May 14, 2021 15:51	15	false	N/A	Completed: <div><div></div></div>
<input type="checkbox"/> 4350	1 device(s)	Base Infrastructure	Now		Auto-Sync	May 14, 2021 15:50	May 14, 2021 15:51	15	false	N/A	Completed: <div><div></div></div>
<input type="checkbox"/> 4349	1 device(s)	Base Infrastructure	Now		Auto-Sync	May 14, 2021 15:47	May 14, 2021 15:47	15	false	N/A	Completed: <div><div></div></div>
<input type="checkbox"/> 4348	1 cnPilot e10 device(s)	Base Infrastructure	Now	Sessionbase	Raja Muniyandy	May 13, 2021 13:11	May 13, 2021 13:12	-	false	N/A	Completed: <div><div></div></div>

Showing 1-10 Total 4,236 Previous 1 2 3 4 5 424 Next



Note

- Configuration jobs skip offline devices. With manual synchronization, they need to be synchronized by the administrator.
- For more information on Wi-Fi AP configuration, refer to the following URLs:
 - [Unique per-Device values in Profiles Using User-Defined Overrides](#)
 - [AP Groups and Overrides for Wi-Fi Devices.](#)

- [Migrating from Templates to Profiles](#)

- cnMaestro X can run any number of Jobs in parallel.

Factory Reset

A factory reset erases all the data on the device. Factory reset is supported for two device models: Enterprise Wi-Fi higher than 3.10-R6 version and cnMatrix higher than 4.0 version.

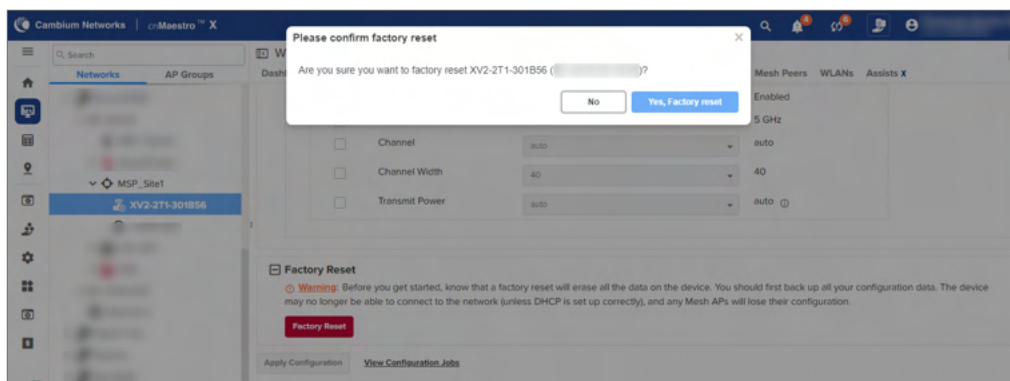
To factory reset the device perform as follows:

1. Navigate to the **Configuration** page of the device.
2. Select **Factory Reset**.

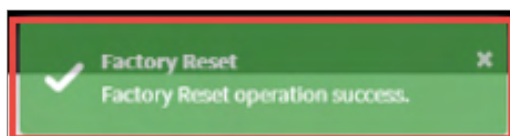
The screenshot shows the 'Configuration' page for a device. The 'Device Details' section includes fields for Name, Network, Site, Description, Latitude, and Longitude. The 'Device Configuration' section shows the AP Group set to 'None'. The 'Factory Reset' section contains a warning: 'Warning: Before you get started, know that a factory reset will erase all the data on the device. You should first back up all your configuration data. The device may no longer be able to connect to the network (unless DHCP is set up correctly), and any Mesh APs will lose their configuration.' A red 'Factory Reset' button is visible below the warning.

3. Click **Factory Reset**.

It displays **Please confirm factory reset** message as shown below:



4. Click **Yes, Factory reset** option.



If the Factory Reset is successful, the following message is displayed on the **Notifications** tab.

Severity	Device Type	Device	Managed Account	IP Address	Category	Message	Raised Time
Major	cnPilot e500	IPv6-E500-srdhar	Base Infrastructure		Status	Device is offline View Details	Wed Jul 31 2019 15:19:18 GMT+0530
Notice	cnPilot e500	IPv6-E500-srdhar	Base Infrastructure		Default System Configuration Applied	System configuration was reset to default View Details	Wed Jul 31 2019 15:19:17 GMT+0530

When Factory Reset is performed, cnMaestro deletes the existing device cookie and displays message to **Approve** in the homepage. When the device connects back you have to re-approve the device as shown below:

This On-Premises instance is not onboarded to cnMaestro Cloud. You can manage this from [Administration > Settings > Cloud Connectivity](#)

Please verify device details along with source IP and re-approve. [Learn more](#) [Approve](#)

Wi-Fi > Sasi-E500-B8B484

Dashboard Notifications **Configuration** Details Performance Software Update Tools Clients Mesh Peers WLANs

Device Details

Managed Account
Base Infrastructure [Change](#)

Name
Sasi E500 B8B484

Network
default

Site
AOS Site

Description

Latitude
12.9715987

Longitude
77.5945627

Serial Number

MAC Address

IP Address
10.110.208.10

Sync Status
N/A

[Set the device location using a map](#)

Device Configuration [View Device Configuration](#)

AP Group
None [Edit](#) [Create](#)

Factory Reset

[Apply Configuration](#) [View Configuration Jobs](#)

When Factory Reset is applied to an offline device, it displays an error as shown below:

Wi-Fi > Migration_04_XE34_01

Dashboard Notifications **Configuration** Details Performance S WLANs Assists X

Factory Reset
Device is unreachable. This operation cannot be done.

Device Details

Managed Account
A... Monitor [Change](#)

Name
Migration_04_XE34_01

Network
default

Site
MSP_Mixed_Devices_Monitor

Description

Latitude

Longitude

[Set the device location using a map](#)

Device Configuration [View Device Configuration](#)

AP Group
APG_CNM_SIT_ESeries_Migration [Edit](#) [Create](#)

WLAN used by AP Group
CNM_SIT_ESeries_Migration

Advanced Settings

Factory Reset

Warning: Before you get started, know that a factory reset will erase all the data on the device. You should first back up all your configuration data. The device may no longer be able to connect to the ne and any Mesh APs will lose their configuration.

[Factory Reset](#)

[Apply Configuration](#) [View Configuration Jobs](#)

Sync Status
Not In Sync [Sync Configuration](#)
Configuration failed: country_code:Country not supported on this sku

Association ACL

This section describes how cnMaestro replies to AP's request to allow or disallow client associations. This feature allows you to configure a MAC Association list that is used to allow/deny client associations.

Overview

When a client tries to connect to an AP, the following occurs:

1. The AP sends MAC authentication request along with the MAC Address of client and the Customer ID (CID) to the Controller. This is optional and occurs only if MAC ACL is configured for the WLAN on the AP and the policy for the MAC ACL is cnMaestro.
2. Controller checks and responds with an action to Allow or Deny the request.
3. AP allows or denies the client's request based on the response of the Controller.

Configuring Association ACL

To configure the Access Control List (ACL) in cnMaestro:

1. Navigate to **Configuration > Wi-Fi Profiles > Association ACL** tab.
2. Click **Add**.

Configuration > Association ACL

The Association ACL is shared among all Enterprise WLANs, but it must be explicitly mapped to each Enterprise Wireless LAN that uses it (at Access Control > MAC Authentication). Enter the MAC addresses of wireless clients or mesh peers to allow/deny their association with an access point. [Learn more](#)

Managed Account: Base Infrastructure

Default Access: ☒ Allow ☐ Deny Apply default access, if MAC entry for a wireless client or mesh peer does not exist in below table.

Import: Import CSV

MAC	Description	Access
		Deny
		Deny
		Deny
		Deny
		Deny
		Deny
		Deny
		Deny
		Deny
		Deny
		Allow

Showing 1 - 10 Total 364 10 < Previous 1 2 3 4 5 Next >

Save

3. Select **Allow**.
4. Enter the **MAC** and **Description**.
5. Click **Save**.

Add Association ACL

☒ Allow

MAC: XX-XX-XX-XX-XX-XX

Description:

Save Close

It displays the **Success** message.





















1. Navigate to **Configuration > Wi-Fi Profiles > Access Control Policies** tab.

Configuration > Wi-Fi Profiles

AP Groups WLANs Association ACL **Access Control Policies**

① Policies are sets of conditions, constraints, and settings that allow you to decide who can connect to the network, and how or when they are allowed to connect.

Apply Filter(s) Add WLAN Policy Add AP Group Policy

Name	Type	Managed Account	Air Cleaner En...	MAC Filtering R...	IP Filtering R...	Application Filtering R...	
uhuh	AP Group	Base Infrastructure	No	0	0	0	 
hello	AP Group	Base Infrastructure	No	1	0	1	 
sssss	AP Group	Base Infrastructure	No	0	1	1	 
test-CN	AP Group	Base Infrastructure	No	1	0	0	 
safasfa	WLAN	Shared	N/A	1	0	1	 
SSR-Test	WLAN	Base Infrastructure	N/A	1	1	0	 
shared	AP Group	Shared	Yes	13	0	0	 
only_air	AP Group	Base Infrastructure	Yes	13	0	0	 
sai_apgrp_policy	AP Group	Base Infrastructure	No	1	1	0	 
test12345	AP Group	Base Infrastructure	No	2	2	0	 

Showing 1 - 10 Total: 35 10 < Previous 1 2 3 4 Next >

2. Click **Add WLAN Policy** or **Add AP Group Policy**.

Access Control Policies > Add WLAN Access Control Policy

Name*

Scope

Base Infrastructure

① WLAN Access Control policies have less priority than AP Group Access Control policies. After creating, link this policy at WLAN -> Access Control tab.
Rules are processed in this priority: MAC Filters followed by IP and Application Filters. Maximum 50 rules are allowed in each policy.

MAC Filtering Rules

Apply Filter(s) Delete Add New

<input type="checkbox"/>	Precedence	N...	Status	Action	Direction	Source ...	Source Mask	Destination ...	Destination Mask	Protocol	Source Port	D
--------------------------	------------	------	--------	--------	-----------	------------	-------------	-----------------	------------------	----------	-------------	---

No Data Available

IP and Application Filtering Rules

Apply Filter(s) Delete Add New

<input type="checkbox"/>	Precedence	N...	Status	Action	Type	Application / Category	Protocol	Sour...	Source IP Mask	Destinati...	Destination IP Ma
--------------------------	------------	------	--------	--------	------	------------------------	----------	---------	----------------	--------------	-------------------

No Data Available

3. Enter a **Name** for the policy.
4. Select the **Scope** from the dropdown list.
5. For AP Groups, **Enable Air Cleaner**.
6. Click **Add New** in the top right corner of the **MAC Filtering Rules** list and complete the details in the **Add MAC Filtering Rule** pop-up window.

- Click **Add New** in the top right corner of the **IP and Applications Filtering Rules** list and complete the details in the **Add IP and Application Filtering Rule** pop-up window.



Note

The **Layer 7 (Application Filtering)** option is a cnMaestro X feature.

- After adding all the required rules, click **Add**.
- Navigate to **WLAN > Access Control** or **AP Group > Access Control** tab and link this policy.



Note

- AP Group Access Control Policies are applied at the device level.
- WLAN Access Control policies have less priority than AP Group Access Control policies.

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** checkbox 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**.

Application Name	Managed Account	Enabled	Category	Productivity Index	Risk Index	FQDN/IP Address
test	Base Infrastructure	Disabled	Remote Access	Medium	High	5.6.7.8
hhjksdckjldkj	Base Infrastructure	Enabled	Streaming Media	Medium	High	3.3.3.3
test_test	Base Infrastructure	Enabled	Custom	Low	Low	1.1.1.1

2. Click **Add New** on the **Custom Applications X** page.

The **Add Custom Application(s)** window is displayed.

Configure the following parameters:

Table 75 *Custom Application Parameters*

Parameter	Description
Name	Specifies the name for the custom application. Supports a maximum of 20 characters.
Scope	Specifies the availability of the custom application across managed accounts. The following values are supported: <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

Table 75 *Custom Application Parameters*

Parameter	Description
	account. Note: Once the scope has been configured on a custom application, it cannot be modified.
Category	Specifies the category to which the application must belong. Select the appropriate category from the dropdown list.
FQDN/IP Address	Specifies the IPv4 address or the domain name of the custom application.
Productivity Index	Indicates how appropriate an application is useful for business purposes. The higher the rating number, the more business-oriented an application is.
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 checkbox to enable this custom application.

3. Click **Add**.
4. To apply this configuration on the AP, click **Save and Apply**.

cnMatrix Switches

cnMatrix switches simplifies the network deployment and operation. cnMaestro provides management, configuration and control, and security services for cnMatrix with deployment options such as Policy-Based Automation (PBA) to simplify core operations and improve network security. Central to cnMaestro's orchestration of cnMatrix devices is the concept of Switch Groups.

This chapter contains the following topics:

- [Switch Group Configuration](#)
- [Synchronize \(Sync\) Configuration](#)
- [Policy Based Automation \(PBA\)](#)
- [Switches](#)
- [Switch Ports](#)
- [Device Details](#)

Switch Group Configuration

A Switch Group represents a virtual stack of switches, independent of their locations or networks. The Switch Group functionality enables users to manage multiple switches with the same configuration.

Configuration is common to all switches belonging to a Switch Group:

- Configuration changes are synchronized and applied for all the switches in a Switch Group.
- A subset of configuration attributes can be overruled for an individual switch.
- Switch Ports across all physical switches are associated with a Switch Group and can be simultaneously bulk edited.

From the **Switch Groups** tab, the administrator can navigate to the Switches and the Switch Ports tabs for configuration. The Dashboard tab is used to monitor the health condition of the virtual stack.

The process for creating a new switch group configuration is as follows:

1. Navigate to **Configuration > Switch Groups**.
2. Click **New Switch Group**.

Configuration > Switch Groups

[Learn more](#) about Switch Groups.

Search: Scope: All Accounts

New Import Sync

Name	Offline Switches	Scope	Ports Up	VLANs	Active PoE Ports	Auto Sync	Last Edited	
8-12-20202	0 of 0	Base Infrastructure	0 of 0	1	0	On	Dec 09 2020 16:24:47	
Complete_Configured	1 of 1	Base Infrastructure	1 of 16	14066	0	On	Dec 08 2020 13:22:34	
10.10.10.10	0 of 0	Shared	0 of 0	1	0	Off	Dec 08 2020 12:38:13	
10.10.10.10	0 of 0	Base Infrastructure	0 of 0	1	0	Off	Dec 08 2020 11:29:29	
8-12-2020@10.10.10.10	0 of 0	Base Infrastructure	0 of 0	1	0	On	Dec 08 2020 11:22:04	
Default Switch	0 of 0	ma_test_nbi_apl_d579d	0 of 0	1	0	On	Dec 07 2020 19:47:18	
Default Switch	0 of 0	1MSP-25Ndv	0 of 0	1	0	On	Dec 07 2020 19:47:07	
Default Switch	0 of 1	Base Infrastructure	1 of 28	1	0	On	Dec 07 2020 19:46:39	

Showing 1 - 8 Total: 8 < Previous Next >



Note

To edit the Configuration of an existing switch group, click the edit icon, navigates to Switch Group Configuration page.

3. Configure the following tab parameters to create a Switch groups:
4.
 - Basic
 - Management
 - Network
 - Security
 - User-Defined Overrides

Switch Groups > Add New

Basic

Management

Network

Security

User-Defined Overrides

Show Advanced ☐

Basic Information

Name*

Scope: Shared Shared Scope means the Switch Group is accessible to all Managed Accounts

☒ Auto Sync Automatically push configuration changes to devices sharing this Switch Group. Note: Lock Wi-Fi AP/cnMatrix/NSE device Configuration checkbox should be enabled at Configuration -> Advanced Features section.

Contact: Contact information for the device (max 64 characters)

Description:

WISP Configuration (For TX Models)

☒ PoE Auto-Detect - cnMedusa Automatically sets PoE mode to Hybrid

☒ PoE Auto-Detect - cnWave Automatically sets PoE mode to Hybrid

☐ High Temperature Mode Lower PoE budget for switch to operate in high temperature mode (TX2K only)

Input DC Voltage (For TX1012-P-DC)

☒ 9-60V ☐ 30-60V Sets PoE budget 120W (9-60V), 170W (30-60V)

Cambium Sync

☒ Antenna Administration Status Enable internal Antenna for GPS Sync

☒ cnPulse Administration Status Enable cnPulse for GPS Sync

☐ cnPulse Power Enable PoE to power cnPulse

Save



Note

- Toggle the **Show Advanced** button to view the advanced options of the Switch Groups.
- Click **Save** on individual tab parameters or click once after configuring parameters across all the tabs.

Basic

The Basic tab provides options to the user to configure the device name as well as other standard values used to identify a switch.

1. Navigate to **Configuration > Switch Groups > Basic**.
2. On the Basic page enter device identification data such as:
 - Name
 - Contact
 - Description
 - Scope
 - WISP Configuration
 - Input DC Voltage
 - Cambium Sync



Note

- The special characters should be used to create Switch Groups names (Eg: a-zA-Z_~*%#@!<>.) []^~\$1234567890). The user can also rename them if required.
- By default, the password is not configured. User has to configure the password for Switch Group.
- By default, the **Auto Sync** option for automatically applying the configuration is enabled.

3. Click **Save**.

Management

The **Management** page allows you to configure Administrator Access, Time Settings, DNS, and Event Logging.

1. Navigate to **Switch Groups > Management** page.
2. Enable the **Daylight Saving Time** and enter the details.



Note

cnMatrix Switches supports SNMP configuration from release 3.0.4.

Switch Groups > may2121

Dashboard Notifications **Configuration** Statistics Switches Switch Ports

Basic

Management

Network

Security

User-Defined Overrides

Show Advanced ☐

Administrator Access

☐ Telnet

☒ HTTP

☒ SSH

Username	Password	Privilege	
admin	*****	Root	
guest	*****	Guest	

[Add New](#) Showing 1 - 2 Total: 2 10 < Previous 1 Next >

☒ **Time Settings**

SNTP Server Address Name or IP Address of Network Time Protocol Server

Time Zone

Time Zone Name Set Time Zone Name (3-6) capital letters E.g. EST, PST, AST, IST etc. Default value set is UTC.

Daylight Saving Time ☒ Disabled ☐ Enabled

DNS

DNS Server 1

DNS Server 2

☒ **Event Logging**

Minimum Syslog Level

Server Address Port

[Save](#)

- Click **Add New** to add **Administrator Access**, enter the details and click **Add**.

Administrator Access

Username*

Password* Hover info icon for password rules [Show](#)

Confirm Password* [Show](#)

Privilege

[Add](#)

- Password should match the special characters as shown below:

Administrator Access

Username*

Password* Hover info icon for password rules

Confirm Password*

Privilege
Guest

Add

Password length should be in the range of 8 - 20 characters
 Password should contain at least 1 lowercase characters
 Password should contain at least 1 uppercase characters
 Password should contain at least 1 numerical characters
 Password should contain at least 1 special characters
 New Password should contain at least 4 characters different from old password

5. **Time Settings:** Enable the **Daylight Saving Time** and enter the corresponding details.
6. **DNS:** Enter DNS server details.
7. **SNMP:** Enter SNMP details.
8. **Event Logging:** Select **Minimum Syslog Level** from dropdown and enter server details.
9. Click **Save**.

Network

The Network page allows the user to configure VLANs, PBA, IP Route, and Spanning Tree details.



Note

From release 3.0.4 cnMatrix Switches supports MSTP Mode and Path Cost Method in Spanning Tree.

1. Navigate to **Switch Groups > Network**, enter the details of **VLANs**, **Policy Based Automation**, **MAC List File Server Settings**, **IP route**, and **Spanning Tree**.

Switch Groups > Test123_clone12

Dashboard Notifications Configuration Statistics Switches Switch Ports

Basic Management **Network** Security User-Defined Overrides

Show Advanced ☒

VLANs

VLAN Name	VLAN ID	IGMP Snooping	DHCP Snooping	ARP Inspection	Voice VLAN	Voice Data VLAN
vlan1	1	Disabled	Disabled	Disabled	Disabled	Disabled

[Add New](#) Showing 1-1 Total: 1 10 < Previous 1 Next >

Policy Based Automation [Learn more](#)

☒ Auto Attach Controls the Policy Based Automation status on the switch

☒ Auto VLAN

☒ Use Site Name for localization **X**

MAC List File Server Settings **X**

Policies Rules Actions **MAC Lists** **X**

Name	Rule	Action	Precedence	Enabled
No Data Available				

[Add New](#) Showing 0-0 Total: 0 10 < Previous Next >

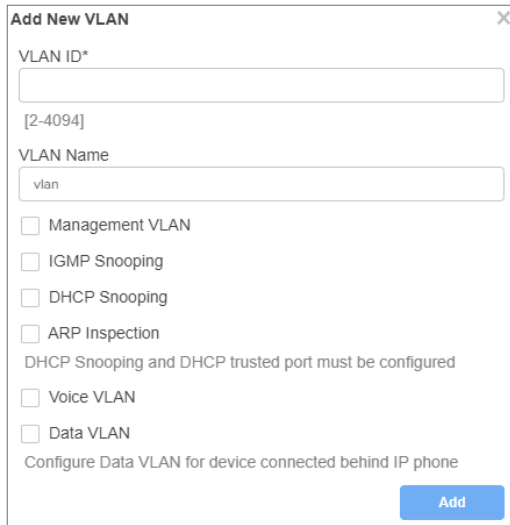
Save



Note

Use Site Name for localization, MAC List File Server Settings, and MAC Lists are cnMaestro X features.

2. To Add a new VLANs click **Add New**.
3. Enter the **VLAN ID**.
4. Enter the **VLAN Name**.



Add New VLAN [X]

VLAN ID*
[2-4094]

VLAN Name
vlan

☐ Management VLAN

☐ IGMP Snooping

☐ DHCP Snooping

☐ ARP Inspection
DHCP Snooping and DHCP trusted port must be configured

☐ Voice VLAN

☐ Data VLAN
Configure Data VLAN for device connected behind IP phone

Add

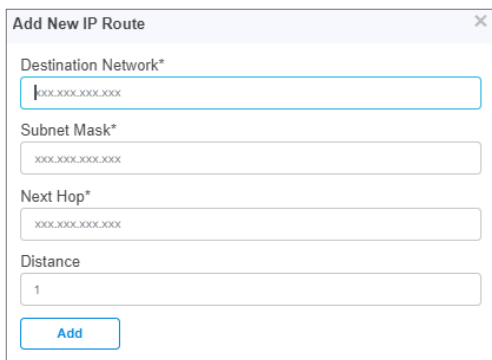
5. Enable or disable the following options:

- Management VLAN
- IGMP Snooping
- DHCP Snooping
- ARP Inspection
- Voice VLAN
- Data VLAN

6. Click **Add**.

7. To Add a new IP Route click **Add New**.

- a. Enter the **Destination Network**.
- b. Enter the **Subnet Mask**.



Add New IP Route [X]

Destination Network*
xxx.xxx.xxx.xxx

Subnet Mask*
xxx.xxx.xxx.xxx

Next Hop*
xxx.xxx.xxx.xxx

Distance
1

Add

- c. Enable the **Next Hop**.
- d. Enable the **Distance**.
- e. Click **Add**.

8. Enable **Spanning Tree**.

- a. Select the Mode **RSTP** from the dropdown.
 - Select Path Cost Method **Long** or **Short**.
 - Select **Priority**.

Spanning Tree

☒ Enable

Mode
RSTP

Path Cost Method
☒ Long ☐ Short

Priority
32768

Save

- b. Select the Mode **PVRST** from the dropdown.
 - Select Path Cost Method **Long** or **Short**.
 - Select **Priority**.

Spanning Tree

☒ Enable

Mode
PVRST

Path Cost Method
☒ Long ☐ Short

Bulk Edit

VLAN ID	Priority
1	32768

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

Save

- c. Select the Mode **MSTP** from the dropdown.
 - Select Path Cost Method **Long** or **Short**.
 - Enter the **Region Name** and **Revision**.

Spanning Tree









☒ Enable

Mode
MSTP

Path Cost Method
☒ Long ☐ Short


Region Name

Revision
0

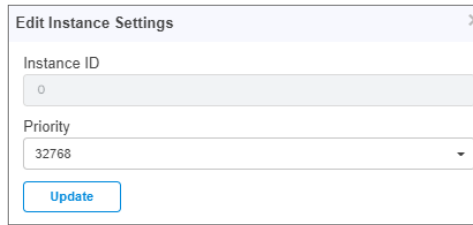
Instance ID	VLAN List	Priority	
0		32768	
1		32768	
2		32768	
3		32768	
4		32768	
5		32768	
6		32768	
7		32768	

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

Save

- User can edit **Priority** by clicking the edit () icon.

- Select the Priority and click **Update**.



Dialog box titled "Edit Instance Settings" with a close button (X). It contains two input fields: "Instance ID" with the value "0" and "Priority" with a dropdown menu showing "32768". At the bottom is a blue "Update" button.

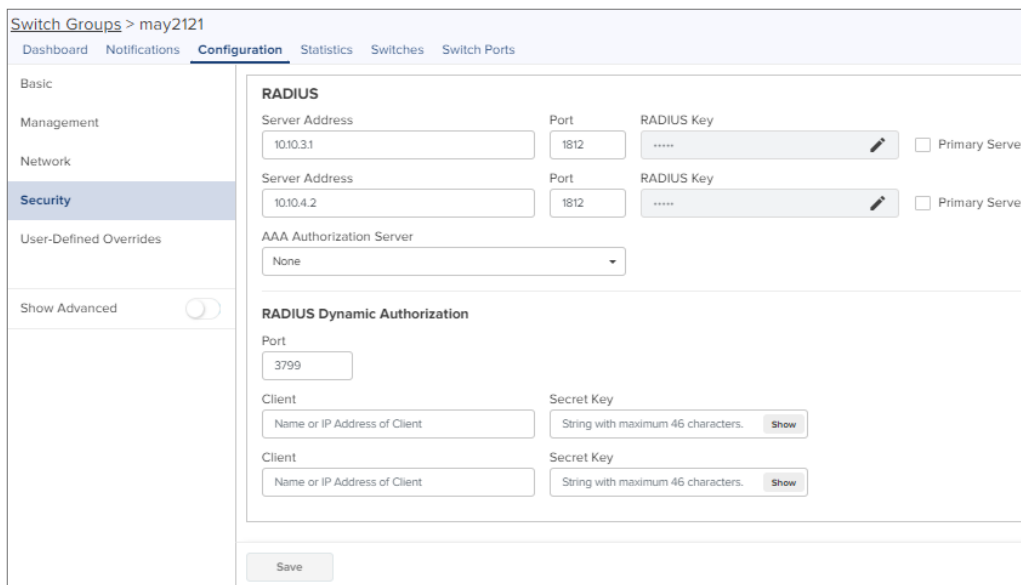
9. Click **Save**.

Security

In **Security** page user can configure **RADIUS** and **Access Control List (ACL)** details.

To configure Security:

1. Navigate to **Switch Groups > Configuration > Security** tab
2. Enter **Server Address**.
3. Enter **RADIUS Key**.
4. In **AAA Authorization Server** select **None** or **RADIUS** from the dropdown.
5. Enter **RADIUS Dynamic Authorization**.




Configuration page for "Switch Groups > may2121". The left sidebar shows tabs: Basic, Management, Network, **Security**, and User-Defined Overrides. The "Show Advanced" toggle is on. The main content area is titled "RADIUS" and contains the following fields:

- Server Address**: 10.10.3.1, **Port**: 1812, **RADIUS Key**: ***** (with edit icon), ☐ Primary Server
- Server Address**: 10.10.4.2, **Port**: 1812, **RADIUS Key**: ***** (with edit icon), ☐ Primary Server
- AAA Authorization Server**: None (dropdown)
- RADIUS Dynamic Authorization**:
 - Port**: 3799
 - Client**: Name or IP Address of Client, **Secret Key**: String with maximum 46 characters. (with Show button)
 - Client**: Name or IP Address of Client, **Secret Key**: String with maximum 46 characters. (with Show button)

At the bottom is a "Save" button.

6. In **IP ACL**, click **Add New**.



Dialog box titled "Add New ACL IP Rule" with a close button (X). It contains the following fields:

- ACL Name***: Text input field
- Protocol**: Dropdown menu showing "IP"
- Source IP/Mask***: Text input field with placeholder "xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy"
- Destination IP/Mask***: Text input field with placeholder "xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy"

At the bottom is a blue "Add" button.

- Enter **ACL Name**.
- Select the appropriate **Protocol** from the dropdown.
- Enter **Source IP/Mask**.
- Enter **Destination IP/Mask**.
- Click **Add**.

7. Click **Save**.

User-Defined Overrides



Note

The minimum device software version supported for this feature is 4.0.

User-Defined Overrides allows you to apply configuration in cnMatrix switches. 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.






























Switch Group Operations

Switch Groups can be Exported, Imported, Cloned, and Deleted.

Shared Settings > Switch Groups

[Learn more](#) about Switch Groups.

Search: Scope: All Accounts

Name	Offline Switches	Scope	Ports Up	VLANs	Active PoE Ports	Auto Sync	Last Edited	
Default Switch	0 of 0	Test_MSP-RGVN	0 of 0	1	0	On	Jun 02 2022 13:33:18	   
Default Switch	0 of 0	mispf	0 of 0	1	0	On	Jun 02 2022 10:13:12	   
3005225G	0 of 2	Shared	2 of 38	1,5,7	0	On	Jun 01 2022 10:04:30	   
2605225G	2 of 2	Shared	2 of 38	1	0	On	May 26 2022 13:36:30	   
Default Switch	0 of 0	Account_1	0 of 0	1	0	On	May 24 2022 15:22:48	   
Default Switch	0 of 0	FloorTest	0 of 0	1	0	On	May 23 2022 15:57:28	   
Default Switch	0 of 0	Indra	0 of 0	1	0	On	May 23 2022 15:57:06	   
MigrationTest-23May	0 of 0	Base Infrastructure	0 of 0	1-9	0	Off	May 23 2022 15:40:36	   
2305225G	0 of 0	Base Infrastructure	0 of 0	1	0	Off	May 23 2022 12:26:54	   
Default Switch	0 of 0	Base Infrastructure	0 of 0	1	0	On	May 18 2022 14:44:33	   

Showing 1 - 10 Total 50 < Previous 1 Next >

Export Switch Group

Click on the **Export** () icon in the Switch Group Table to download the configuration as a JSON file.

Import Switch Group

1. Click **Import Switch Group**. A dialogue box appears.
2. Select the **Scope** from dropdown.
3. Select **import.json** and import the file.

Import Switch Group

Name*

Scope

Shared

Shared Scope means the Switch Group is accessible to all Managed Accounts

Configuration file

Import .json

Import

4. Click **Import**.

Clone Switch Group

Click on the **Clone** (📄) icon in the Switch Group Table to make a copy of the Switch Group.

Delete Switch Group

To delete Switch Group from the list click **Delete** icon of the specific device row.

Configuration > Switch Groups

Learn more about Switch Groups.

Search

Clear

Scope: All Accounts

Add New

Import

Sync

Name	Offline Switches	Scope	Ports Up	VLANs	Active PoE Ports	Auto Sync	Last Updated	Last Updated By	Origin	
TQ-Lab2-cnMatrix-Main-SW	0 of 0 Offline	Shared	0 of 0	1,9,99,999,3999	0	OFF	Jul 11 2023 06:25:21		Custom	📄 🗑️ ✎
Bashin_Switch	0 of 0 Offline	Shared	0 of 0	1,2,10,20	0	OFF	Dec 21 2022 15:32:26		Custom	📄 🗑️ ✎
Duroa2_clone	0 of 0 Offline	Base Infrastructure	0 of 0	1,5,4066	0	ON	Oct 19 2021 16:08:09		Custom	📄 🗑️ ✎
dns.444	0 of 0 Offline	Shared	0 of 0	1,2,5,10	0	ON	Jun 03 2021 13:10:45		Custom	📄 🗑️ ✎
Tower1	0 of 0 Offline	Shared	0 of 0	1	0	OFF	Jun 03 2021 11:49:17		Custom	📄 🗑️ ✎
3-6-2021	0 of 0 Offline	Base Infrastructure	0 of 0	1	0	OFF	Jun 03 2021 10:50:16		Custom	📄 🗑️ ✎
test1234	0 of 0 Offline	Shared	0 of 0	1	0	OFF	Jun 03 2021 10:01:38		Custom	📄 🗑️ ✎
dns.f1	0 of 0 Offline	Base Infrastructure	0 of 0	1	0	OFF	May 20 2021 18:25:01		Custom	📄 🗑️ ✎
Complete_Configured	0 of 0 Offline	Base Infrastructure	0 of 0	1,4066	0	ON	May 20 2021 18:24:52		Custom	📄 🗑️ ✎
Migration_Test	0 of 0 Offline	Base Infrastructure	0 of 0	1-5	0	ON	Mar 27 2020 12:10:40		Custom	📄 🗑️ ✎

Showing 1 - 10 Total 13 10 < Previous 1 2 Next >

Retry Configure

When the user tries to apply any Switch Group on the device and if the job was skipped for the device as it was offline, the reason for the skip will be displayed as "Device was offline", in the Jobs page. In this case, when device comes Up and connects to cnMaestro, then cnMaestro will create an Auto-sync job for that device and pushes the Switch Group. (It will not apply to the switch group if the "Auto-Sync" was disabled in the switch group).



Note

The config update (auto-sync) will happen only when the **Auto-Sync** option was enabled in the Switch Groups page. If the device was skipped/failed because of any other reason other than the "Device was offline", then the device will not be updated.

Create a Configuration Job

Configuration job can be created from **System/Network/Tower/Site/Device Configuration** page. Select a device type and a set of devices along with switch groups to which they will be mapped. This can be done in three steps:

1. Select the Switch Group that needs to be pushed from dropdown.
2. Select the list of Switch Group **Device**.

3. Click **Apply Configuration**

The screenshot shows the 'System' configuration page. At the top, there are tabs for Dashboard, Notifications, Configuration (selected), Statistics, Report, Software Update, Clients, and Mesh Peers. Below the tabs, there are several configuration options: Device Type (cnMatrix), Managed Account (All Accounts), Configuration Method (Switch Group selected, Template unselected), and Switch Group (None). A search bar is present above a table. The table has columns: Device, Managed Account, Switch Group, Status, Sync Status, Network, and Tower/Site. One device is listed: cnMatrix-EX2016M-123, with Managed Account Base Infrastructure, Switch Group N/A, Status Online, Sync Status N/A, Network Durga, and Tower/Site cnMatrix. Below the table, there are options to Update (Now selected, Schedule unselected) and Job Options (Stop update on critical error unselected, Devices to update in parallel (1-500) set to 10). A Notes field is also present. At the bottom, a button says 'Apply Configuration to 0 device(s)'.

Synchronize (Sync) Configuration

Switch Groups can be configured to synchronize automatically or manually when they are updated. The setting is found in the Switch Group configuration.

Switches by default synchronize automatically (so any change of switch group, followed by a Save, will immediately push configuration to the devices without manual intervention).

Manual Synchronization

Manual configuration synchronization allows the user to synchronize any devices with a single action rather than updating each device separately. The page is located at **Administration > Sync Configuration**.

To sync the device manually, navigate to **Administration > Sync Configuration**. This location can also be accessed by clicking the **Sync** button on the **Switch Groups** page.

Figure 350 Sync Configuration page

The screenshot shows the 'Application > Sync Configuration' page. At the top, there is a note: 'AP Groups can be configured to synchronize automatically or manually when they are updated. [Learn more](#)'. Below this, there are filters for Device Type (All), Managed Account (All Accounts), and a search bar. A table lists devices with columns: Device, Type, Status, Managed Account, Network, Site, AP Group/Switch Group, and Sync Status. Five devices are listed: cnPilot-r195W-0A2D81 (Offline), TX2028RFP-FECB40 (Offline), DP3-7G45-223-Subnet (Online), E500-BB14FE (Online), and EX1010-240-subnet (Online). Below the table, there are options to Sync Now, Job Options (Stop update on critical error unselected, Devices to update in parallel (1-500) set to 10), and a Notes field.

Sync Configuration has the following fields:

- Device (Hostname)
- Type
- Status (Online/Offline)
- Network (Network in which device is present)
- Site (Site under which device is present)
- Configuration Group (AP Group/Switch Group to which device is mapped)
- Sync Status (Sync status will tell whether job is completed or failed)

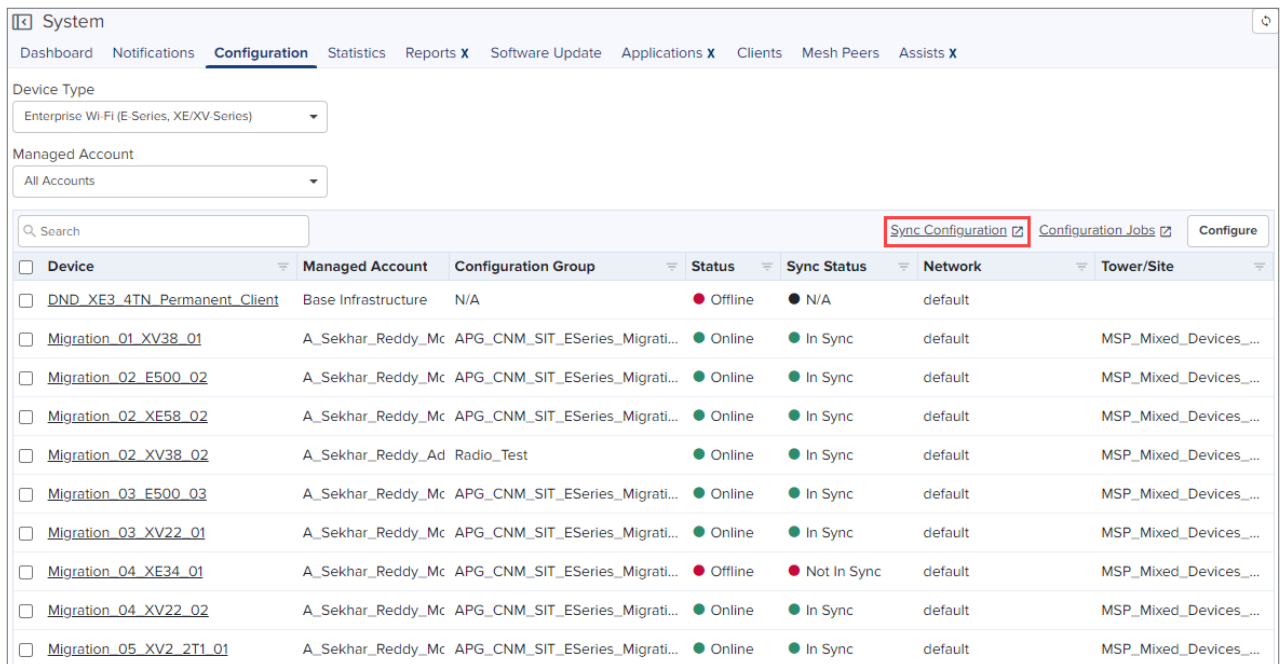
Table 76 Sync Configuration parameters

Parameter	Description
Configuration Group	AP Group or Switch Group to which the device is mapped.
Device	Name of the device or hostname.
Network	Network in which device is present.
Site	Site under which device is present.
Status	Status of device online or offline.
Sync Status	Sync status specifies whether job is completed or failed.
Type	Name of the device platform.

Steps to Sync Configuration:

Navigate to **Monitor and Manage > Network > Configuration** or the **Jobs** tab.

1. Navigate to **System > Configuration > Sync Configuration**.
2. Select the devices to synchronize and click **Sync Configuration**.



The screenshot shows the 'System' configuration page with the 'Configuration' tab selected. Under 'Configuration', the 'Sync Configuration' sub-tab is highlighted with a red box. Below the sub-tabs, there are filters for 'Device Type' (Enterprise Wi-Fi (E-Series, XE/XV-Series)) and 'Managed Account' (All Accounts). A search bar is present. The main table lists various devices, including 'DND_XE3_4TN_Permanent_Client' and several 'Migration' devices. The 'Status' column shows 'Offline' for the first device and 'Online' for others. The 'Sync Status' column shows 'N/A' for the first device and 'In Sync' for others. The 'Network' column shows 'default' for all devices. The 'Tower/Site' column shows 'MSP_Mixed_Devices_...' for all devices.

3. The **Administration > Sync Configuration** page is displayed.

Select the devices to synchronize.

Administration > Sync Configuration

AP Groups can be configured to synchronize automatically or manually when they are updated. [Learn more](#)

AP Group's: Search [] Device Type: All Managed Account: All Accounts

Device	Type	Status	Managed Account	Network	Site	AP Group/Switch Group	Sync Status
<input type="checkbox"/> EX2010-FF6C80-onboard	cnMatrix EX2010	Offline	Base Infrastructure	Durga_DataMigration	cnmatrix-lower	Test2	Not in Sync: Device's configuration changed outside of cnM
<input type="checkbox"/> E400-107_Http_From_APort	cnPilot e400	Offline	Base Infrastructure	DP1-1234	Clients	E400_Apgrp	Not in Sync: Configuration failed: Device was offline
<input type="checkbox"/> E425H-Edited	cnPilot e425h	Offline	Base Infrastructure	DP2	THOR	E400_Apgrp	Not in Sync: Configuration failed: Device was offline
<input type="checkbox"/> DP-Save	cnPilot e410	Offline	Base Infrastructure	default	adminuser	E400_Apgrp	Not in Sync: Configuration failed: Device was offline
<input type="checkbox"/> DP-Gamali	cnPilot e500	Offline	Base Infrastructure	default		E400_Apgrp	Not in Sync: Configuration failed: Device was offline
<input type="checkbox"/> #10E410-9597CB	cnPilot e410	Offline	Base Infrastructure	Bulk_E_series	Bulk_E_series_Site	Radio_off	Not in Sync: Configuration failed: Device was offline
<input type="checkbox"/> E400-9225EE	cnPilot e400	Offline	Base Infrastructure	Bulk_E_series	Bulk_E_series_Site	Radio_off	Not in Sync: Configuration failed: Device was offline
<input type="checkbox"/> E500-ASD4EE	cnPilot e600	Offline	Base Infrastructure	Bulk_E_series	Bulk_E_series_Site	Radio_off	Not in Sync: Configuration failed: Device was offline
<input type="checkbox"/> E400-922372	cnPilot e400	Online	Base Infrastructure	Bulk_E_series	Bulk_E_series_Site	Radio_off	Not in Sync: Configuration failed: key not in the table
<input type="checkbox"/> E400-9223E2	cnPilot e400	Online	Base Infrastructure	Bulk_E_series	Bulk_E_series_Site	Radio_off	Not in Sync: Configuration failed: key not in the table

Showing 1-10 Total: 12 10 * Previous 1 2 Next >

10 - Devices selected

Job Options

☐ Stop update on critical error

10 Devices to update in parallel (1-500)

Notes

Sync Now

4. Click **Sync Now**.

Application > Sync Configuration

AP Groups can be configured to synchronize automatically or manually when they are updated. [Learn more](#)

Search [] Device Type: All Managed Account: All Accounts

Device	Type	Status	Managed Account	Network	Site	AP Group/Switch Group/NSE Group	Sync Status
<input type="checkbox"/> Migration-cnMatrix-05	cnMatrix EX1028	Offline	Base Infrastructure	cnmatrix_network	cnmatrix_site	07Nov225G-209	Device out of sync : Device port channels were updated
<input type="checkbox"/> NSE-700328	NSE 3000	Online	Base Infrastructure	Rashin_Network	Rashin_Site	Rashin_NSE	Device out of sync : Configuration failed: Config timeout
<input type="checkbox"/> NSE-700360	NSE 3000	Online	Base Infrastructure	Rashin_Network	Rashin_Site	Rashin_NSE	Device out of sync : Configuration failed: Config timeout
<input type="checkbox"/> NSE-700300	NSE 3000	Online	Base Infrastructure	Rashin_Network	Rashin_Site	Rashin_NSE	Device out of sync : Configuration failed: Config timeout
<input type="checkbox"/> Migration-10-8209P-02	cnPilot r209P	Online	Base Infrastructure	default	Site_Test\$\$\$\$.n	Rseries_APGroup1	Device out of sync : Device's configuration changed outside of cnMaestro
<input type="checkbox"/> Migration-cnMatrix-01	cnMatrix TX20128-P	Online	Base Infrastructure	default		SwitchGroup27	Device out of sync : Configuration failed: ifMainEntry index 8 Invalid index, cannot create new rows
<input type="checkbox"/> Migration-cnMatrix-02	cnMatrix EX2010	Online	INDQA	default	Matrix	SwitchGroup27	Device out of sync : Device's configuration changed outside of cnMaestro
<input type="checkbox"/> Migration-XV2-210-Meshbase-01	XV2 210	Offline	Base Infrastructure	default	AOS_Site	Verify APG	Device out of sync : Device's configuration changed outside of cnMaestro

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

10 - Devices selected

Job Options

☐ Stop update on critical error

10 Devices to update in parallel (1-500)

Notes

Sync Now

User can also synchronize devices from **Application > Sync Configuration**.



Note

Sync configuration can only be used if a Switch Group is already mapped to the device.

Policy Based Automation (PBA)

Cambium Networks PBA feature fully automates commonly performed operations, improving network security while eliminating potential configuration errors. It allows the user to automatically configure switch port settings based on the device connected to the port. These dynamic PBA settings remain in-use for the duration of the device connection and are automatically cleared when the device disconnects from the switch.

PBA configuration is common to all switches within a Switch Group.



Note

Dynamic PBA updates are indicated by asterisk * on the Switch Dashboard and on the Switch Ports pages.

Configure the PBA as follows:

1. Navigate to **Configuration > Switch Groups > Network > Policy Based Automation.**
2. Navigate to **Rules** tab.

3. Click **Add New** to set the rules.

4. Click **Add**.
5. Navigate to **Actions** tab.

6. Click **Add New** to set the actions.

7. Click **Add**.
8. Navigate to **Policies**.

Policies

Rules

Actions

MAC Lists X

Add New

Name	Rule	Action	Precedence	Enabled
No Data Available				

Showing 0 - 0 Total: 0

10

< Previous

Next >

9. Click **Add New** to set the policies.

Add New Policy

☒ Enable

PBA Policies are an ordered list of PBA Rules(filters) and PBA Actions(configuration) that allow automatic configuration of ports based upon traffic. The policies are applied in increasing order of precedence until there is a positive match.

Name*

Enter alphanumeric string without spaces (max 32 chars)

Rule*

Criteria to detect connecting device by PBA. It is created in Rules tab.

Action*

Configuration to be updated when PBA is applied to a port. It is created in Actions tab.

Precedence

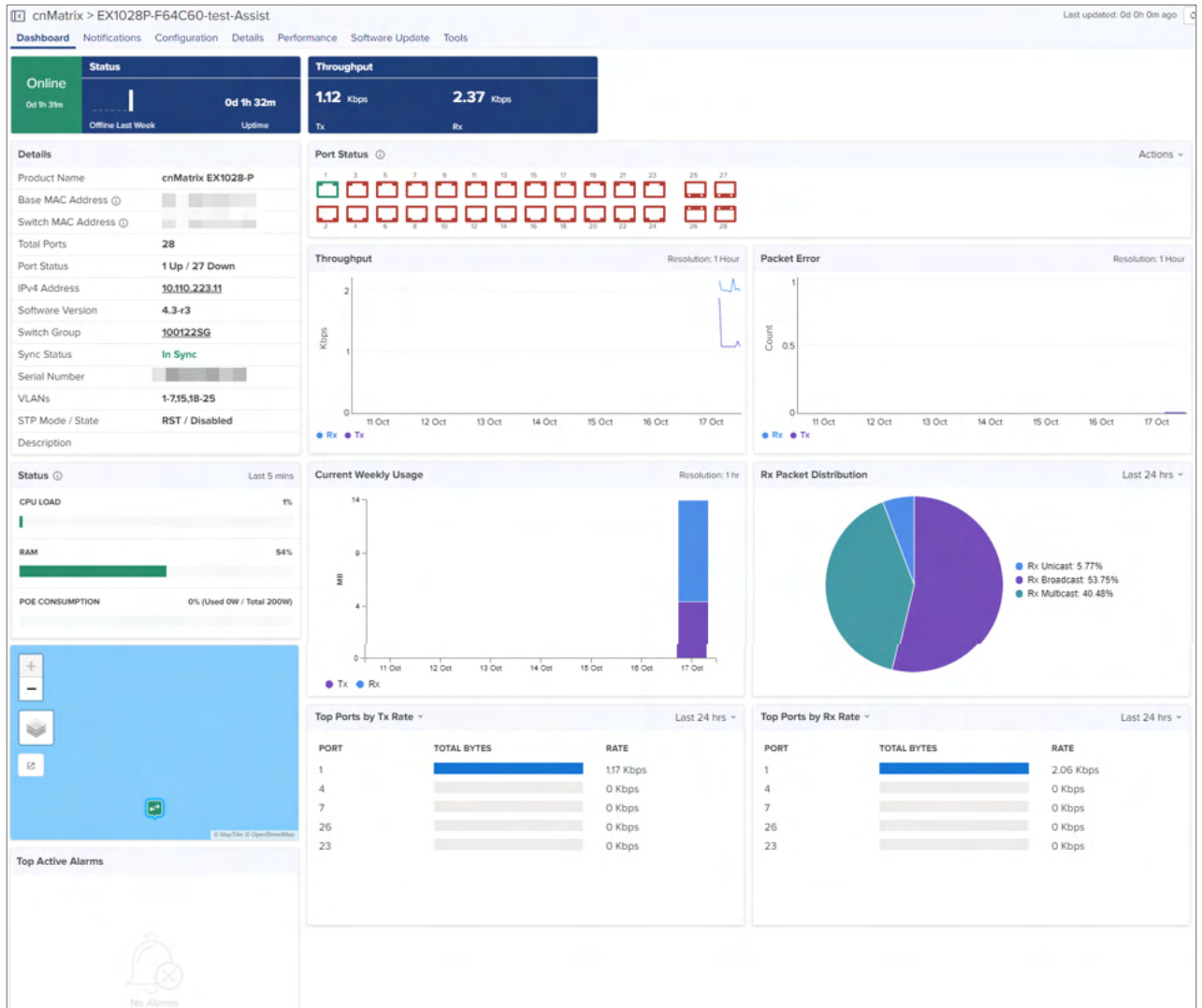
50

Evaluation order 1 (first) - 100 (last)

Policy Ports List

Port interfaces are specified using string format with interfaces and ranges in comma-separated (e.g., 'gi0/3,gi0/8-10,po123').
Note: This feature requires cnMatrix software version later than '5.0.1'.

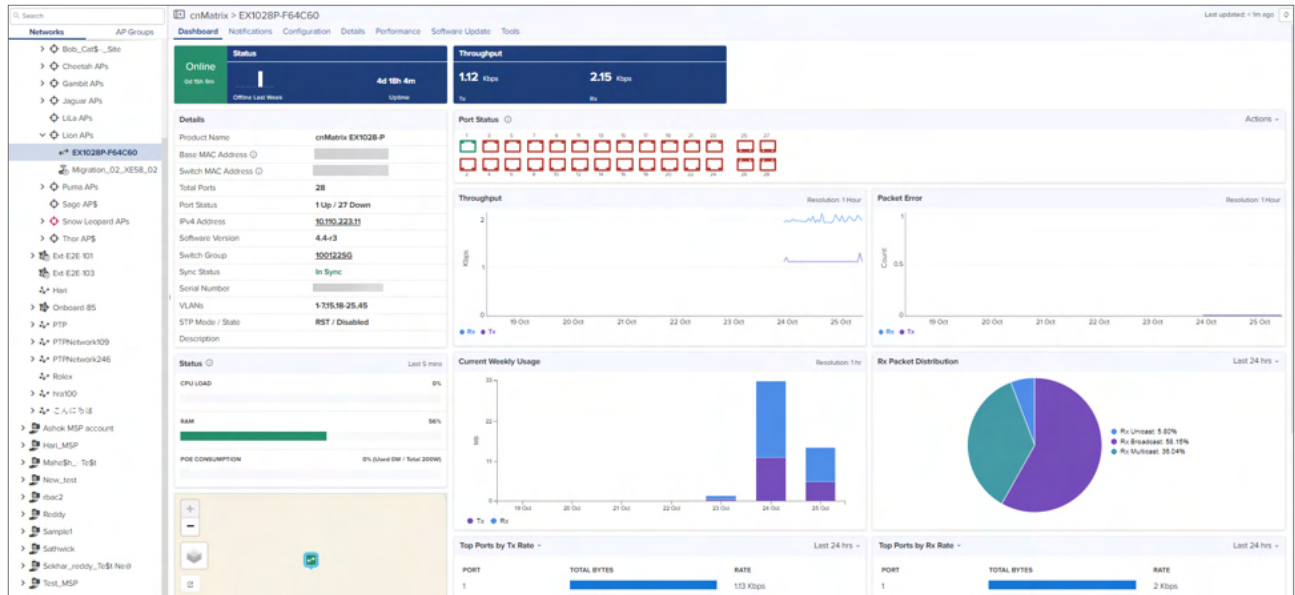
Add



10.

In the cnMatrix dashboard, user can navigate to the following pages using the **Action** dropdown menu in Port Status.

- [Port Configuration](#)
- [Port Statistics](#)
- [Topology](#)
- [Remote CLI](#)
- [Port Operations](#)



Switches

This section contains the following topics:

- [Export Switches](#)
- [cnMatrix Switches](#)
- [Action](#)
- [Switch Configuration](#)

The Switches page is accessed by selecting the **Switch Groups > Switches** tab lists all of the physical switches assigned to the Switch Group. The Switch Dashboard and switch override configurations settings are accessible through this page.

Switch overrides allows certain attributes for each switch to be configured individually.



Note

For configuration, a switch must belong to a Switch Group.

Configure the Switch Group as follows:


- Navigate to **Switch Groups** > select the switch from the list and click **Switches** page to view and edit the onboarded switches.

Device	MAC	Configuration Group	Status	Onboarding Status	Serial Number	IPv4 Address	IPv6 Address	S/W Version	Type	Sync Status	Location	Tower/Site
EX30528P-A5EF0Q		011thJun24	Online (0d 0h 0m)	Waiting for Approval		10.110.156.3	N/A	5.0.1+4	cnMatrix EX30528R-P	N/A		ABD

The Switches details view displays following fields by default:

- Device, Health, Onboarding Status, Serial Number, IP Address, Switch Group, Type, Site, and Action tab.

Action column can be used to edit or delete any device of the Switches.

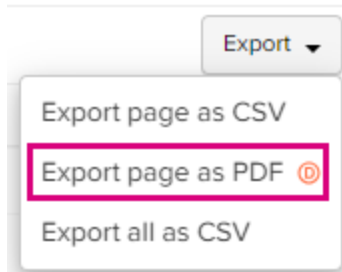
User can click  on top bar to include additional fields in Switches Detail view.

<input checked="" type="checkbox"/> General	
<input checked="" type="checkbox"/> Device	<input checked="" type="checkbox"/> IP Address
<input checked="" type="checkbox"/> Type	<input checked="" type="checkbox"/> Location
<input checked="" type="checkbox"/> Health	
<input checked="" type="checkbox"/> Health	<input checked="" type="checkbox"/> Switch Group
<input checked="" type="checkbox"/> Onboarding Status	<input checked="" type="checkbox"/> Serial Number
<input checked="" type="checkbox"/> Sync Status	<input checked="" type="checkbox"/> Tower/Site
<input type="checkbox"/> Maintenance	
<input type="checkbox"/> Onboard Date	<input checked="" type="checkbox"/> S/W Version
<input type="checkbox"/> Hardware	<input type="checkbox"/> Last Reboot
<input type="checkbox"/> DA Version	<input type="checkbox"/> Onboarded

Export Switches

Perform the following steps to export the Switch table:

1. Click **Export**. A dialogue box appears.

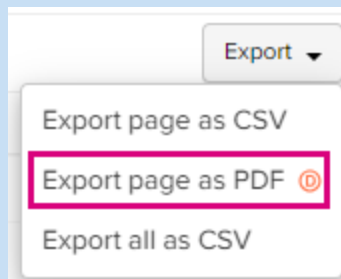


2. Select **Export page as CSV/all as CSV** and export the file.



Note

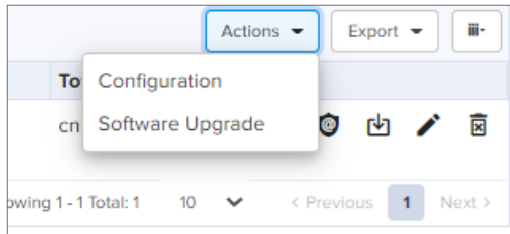
The **Export page as PDF** option is deprecated from cnMaestro release version 5.2.0 onwards. This option will be completely removed from the UI in release version 5.3.0.



Action

Action column can be used to edit or delete any device of the Switches.

1. Click **Action**. A dialogue box appears.



2. Select Configuration to edit the device details or click the edit (✎) icon.

A screenshot of the 'Configuration' dialog box in the cnMaestro Cloud interface. The dialog box has a title bar with 'Configuration' and a close button. Inside, there is a 'Switch Group' section with a dropdown menu showing '300522SG' and buttons for 'Edit' and 'Create'. Below this is a 'Job Options' section with two checkboxes: 'Stop update on critical error' (unchecked) and 'Start job now' (checked). There is also a text input field with the value '10' and a label 'Devices to update in parallel (1-500)'. At the bottom, there is a 'Notes' section with a text area. Two buttons are at the bottom: 'Apply Configuration to 1 device(s)' and 'View Configuration Jobs'.

3. Select Software Upgrade to update the device software or click the (⬇) icon.
4. Click the delete (🗑) icon to delete the selected device from the list.

Switch Configuration

To edit or configure the switches, click the **Edit** or **Configuration** from the **Action** dropdown.

Navigates to the Device **Configuration** page.

1. Enter the **Device Details**, **Set the service location** and **Device Configuration**.

cnMatrix > EX1028P-F64C60-test

Dashboard Notifications **Configuration** Details Performance Software Update Tools

Device Details

Managed Account
Base Infrastructure [Change](#)

Name
EX1028P-F64C60-test ⓘ

Network
Durga ▾

Tower/Site
cnMatrix (Site) ▾

Description

Latitude
 ⓘ

Longitude
 ⓘ

[Set the device location using a map](#)

Device Configuration [View Device Configuration](#)

Configuration Method
☒ Switch Group ☐ Template

Switch Group
Complete_Configured ▾ [Edit](#) [Edit Ports](#) [Create](#)

Note: Click on 'Edit Ports' link for Port configuration.
Warning: Current Port configurations will be reset on modifying the Switch Group and clicking on 'Edit Ports' link / 'Apply Configuration' button.

Advanced Settings

[Factory Reset](#)

[Apply Configuration](#) [View Configuration Jobs](#)

2. Click **Apply Configuration**.

In the Configuration page, you can override the group configuration with device-specific configuration:

- [Device Configuration](#)
- [Advanced Settings](#)
- [Factory Reset](#)

Device Configuration

Device Configuration allows you to configure the Configuration Method as Switch Group/Template.

Switch Group Configuration Method

Enable the Switch Group and select a device from the Switch Group dropdown.

Device Configuration [View Device Configuration](#)

Configuration Method
☒ Switch Group ☐ Template

Switch Group
 100/2295 ▾ [Edit](#) [Edit Ports](#) [Create](#)

Note: Click on 'Edit Ports' link for Port configuration.

Advanced Settings

VLANs Spanning Tree IP Routes General

VLAN ID	IGMP Snooping	IGMP Querier	Querier IP Address	Vlan Interface State	DHCP Client	IP Address	Subnet Mask	
1	Disabled	Disabled	N/A	Enabled	Enabled	10.110.223.22	255.255.255.0	

[Add New](#)

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

Factory Reset

[Apply Configuration](#) [View Configuration Jobs](#)

To Edit or Create a Switch Group. Refer to the [Switch Groups Configuration](#).

Advanced Settings

Navigate to the Advanced Settings and configure the following parameters:

- [VLANs](#)
- [Spanning Tree](#)
- [IP Routes](#)
- [General](#)

VLANs

VLANs interface allows the user to edit/Add the VLAN details such as **VLAN ID**, **DHCP Client**, **IP Address**, and **Subnet Mask**.

- Click **Advanced Settings** in **Configuration** page and navigate to **VLAN Interface** tab.

Advanced Settings

VLANs Spanning Tree IP Routes General

VLAN ID	IGMP Snooping	IGMP Querier	Querier IP Address	Vlan Interface State	DHCP Client	IP Address	Subnet Mask	
1	Disabled	Disabled	N/A	Enabled	Enabled	10.110.223.22	255.255.255.0	

[Add New](#)

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

- Click the edit () icon or **Add New**.
- Enter the required details and click **Add**

Add VLAN ✕

1 ▾

☒ IGMP Snooping

☒ IGMP Querier

Querier IP Address

☒ **Vlan Interface**

☒ Enable Administrative State

☒ DHCP Client

IP Address

Netmask

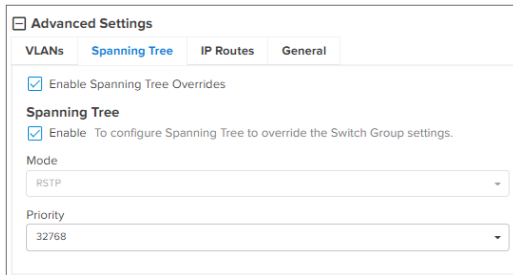
[Update](#)

Spanning Tree

Certain configuration parameters are different for each Switch, and these are highlighted within cnMaestro as Overrides.

Configure the spanning tree to override as follows:

- Click **Advanced Settings** in **Configuration** page and navigate to **General** tab.
- • Click **Enable Spanning Tree Overrides**.
- Select the **Spanning Tree** parameters.



The screenshot shows the 'Advanced Settings' page with the 'Spanning Tree' tab selected. The 'Enable Spanning Tree Overrides' checkbox is checked. Below it, the 'Spanning Tree' section has an 'Enable' checkbox checked with the text 'To configure Spanning Tree to override the Switch Group settings.' The 'Mode' dropdown is set to 'RSTP' and the 'Priority' dropdown is set to '32768'.



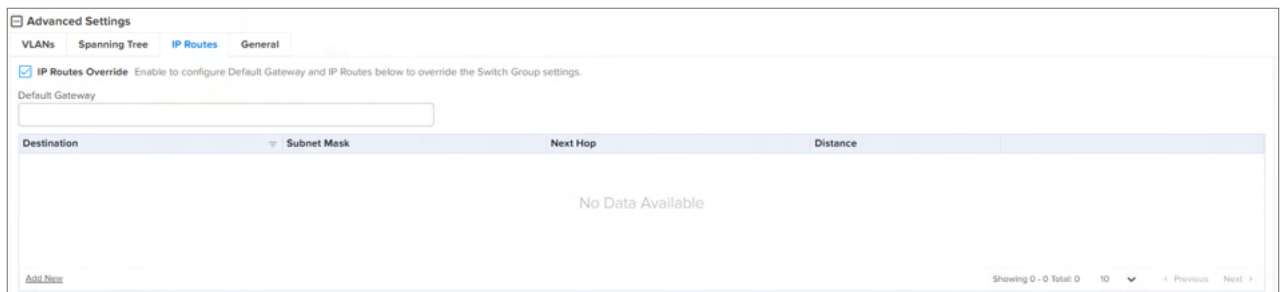
Note

If Spanning Tree is disabled the overrides feature will be disabled on the Switch configuration.

IP Routes

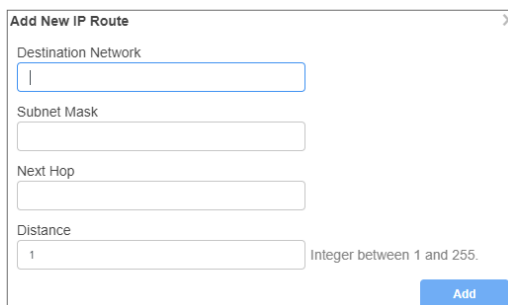
IP Routes allows the user to configure the Default Gateway and IP Routes to override the Switch Group.

- Configure the IP Route as follows:
- Enable the **IP Routes Override** and enter the **Default Gateway**.



The screenshot shows the 'Advanced Settings' page with the 'IP Routes' tab selected. The 'IP Routes Override' checkbox is checked with the text 'Enable to configure Default Gateway and IP Routes below to override the Switch Group settings.' Below this is a 'Default Gateway' text input field. A table with columns 'Destination', 'Subnet Mask', 'Next Hop', and 'Distance' is shown, currently displaying 'No Data Available'. At the bottom right, it says 'Showing 0 - 0 Total 0 10' with 'Previous' and 'Next' links.

- Click **Add New**.
- Enter the parameters such as Destination Network, Subnet Mask, Next Hop, and Distance.
- Click **Add**.



The screenshot shows the 'Add New IP Route' dialog box. It has four input fields: 'Destination Network', 'Subnet Mask', 'Next Hop', and 'Distance'. The 'Distance' field has a value of '1' and a hint 'Integer between 1 and 255.' There is an 'Add' button at the bottom right.

Default gateway IP will override the all IPs of the Switch Groups.

General

General tabs allows to configure PBA Localization settings to override the Switch Group settings.

To configure the PBA localization, perform as follows:

- Click **Advanced Settings** in **Configuration** page and navigate to **General** tab.

Search

cnMatrix > TX2028RFP-EC5D80

Dashboard Notifications **Configuration** Details Performance Software Update Tools Assists X

Networks AP Groups

System

default

Site123

TX2020RP-F9ACE0

TX2028RFP-EC5D80

Latitude
0.0

Longitude
0.0

Set the device location using a map

Device Configuration [View Device Configuration](#)

Configuration Method
☒ Switch Group ☐ Template

Switch Group
Default Switch [Edit](#) [Edit Ports](#) [Create](#)

Note: Click on 'Edit Ports' link for Port configuration.

Advanced Settings

VLANs Spanning Tree IP Routes **General** DHCP Pool

PBA Localization X

☐ Enable PBA localization overrides To configure PBA Localization settings to override the Switch Group settings.

PBA Uplink Ports
No Configured PBA Actions

WISP Configuration (For TX Models)

Factory Reset

[Apply Configuration](#) [View Configuration Jobs](#)

- Enable **PBA localization** overrides.
- Select **Use Site Name** or **Custom**.
- Enter **PBA Uplink Ports**.

Factory Reset

To erase all the configuration on the device and bring the device back to the default factory configuration, complete the following steps:

- Navigate to the cnMatrix device **Configuration** page.
- Expand the **Factory Reset** section. and click **Factory Reset**.

cnMatrix > Switch-7003E0-ESS

Dashboard Notifications **Configuration** Details Performance Software Update Tools Assists X

Set the device location using a map

Device Configuration [View Device Configuration](#)

Configuration Method
☒ Switch Group ☐ Template

Switch Group
 Rashin_Switch-1 [Edit](#) [Edit Ports](#) [Create](#)

Note: Click on 'Edit Ports' link for Port configuration.

Advanced Settings

Factory Reset

Warning: Before you get started, know that a factory reset will erase all the data on the device. You should first back up all your configuration data. The device may no longer be able to connect to the network (unless DHCP is set up correctly). Note: The minimum device software version required for this feature is '4.0'.

Factory Reset

Apply Configuration [View Configuration Jobs](#)

3. In the pop-up window that appears, Click **Yes, Factory reset**.

Please confirm factory reset

Are you sure you want to factory reset Switch-7003E0-ESS?

No **Yes, Factory reset**

Switch Ports

The **Switch Ports** table displays the list of Ports and the Port Channel assigned to the specific switch. The **Switch Ports** table allows administrators to configure the port settings by port ID for all ports within the **Switch Group**. By default, a port ID identifies the switch (by switch name) and port number.

For example: Gi0/1

It supports bulk editing of Switch Port settings across all physical switches.

To view the **Switch Ports**, navigate to **Configuration > Switch Groups > Switch Ports**.

Ports

The **Ports** table supports creating port channels, editing port configuration and configuring port parameters.

Switch Groups > 300522SG

Dashboard Notifications Configuration **Statistics** Switches **Switch Ports**

Configuration Statistics

Ports

Search

[Edit](#) [Create Port Channel](#) **General** Physical Network Security

Port	Switch	Tags	Description	Interface	Administrative State	Operational State	PoE Capable	
Gi0/1	DP3-7G45-223-Subnet	N/A	DP.DonotUse-EX2010-Management	RJ-45	Enabled	Up	No	
Gi0/2	DP3-7G45-223-Subnet	N/A	port-two0	RJ-45	Enabled	Down	No	
Gi0/3	DP3-7G45-223-Subnet	N/A	cnatrix-3	RJ-45	Enabled	Down	No	
Gi0/4	DP3-7G45-223-Subnet	N/A	32	RJ-45	Enabled	Down	No	
Gi0/5	DP3-7G45-223-Subnet	N/A	cambium6	RJ-45	Enabled	Down	No	
Gi0/6	DP3-7G45-223-Subnet	N/A	stats-6	RJ-45	Enabled	Down	No	
Gi0/7	DP3-7G45-223-Subnet	N/A	seven	RJ-45	Enabled	Down	No	
Gi0/8	DP3-7G45-223-Subnet	N/A		RJ-45	Enabled	Down	No	
Gi0/9	DP3-7G45-223-Subnet	N/A	ap-10	SFP	Enabled	Down	No	
Gi0/10	DP3-7G45-223-Subnet	N/A	trunkport	SFP	Enabled	Down	No	

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

Navigate to **Switch Ports > Configuration** tab, configure the following parameters:

- General
- Physical
- Network
- Security

General Tab

Switch Groups > Test123_clone

Dashboard Notifications Configuration Statistics Switches **Switch Ports**

Configuration Statistics

Ports

Q Search Edit Create Port Channel **General** Physical Network Security

Port	Switch	Tags	Description	Interface	Administrative State	Operational State	PoE Capable	
<input type="checkbox"/> Gi0/1	TX2012RP-AD7700	N/A	TX2020RP-B0E280-DND-De...	RJ-45	Enabled	Up	Yes	
<input type="checkbox"/> Gi0/2	TX2012RP-AD7700	N/A		RJ-45	Enabled	Down	Yes	
<input type="checkbox"/> Gi0/3	TX2012RP-AD7700	N/A		RJ-45	Enabled	Down	Yes	
<input type="checkbox"/> Gi0/4	TX2012RP-AD7700	N/A		RJ-45	Enabled	Down	Yes	
<input type="checkbox"/> Gi0/5	TX2012RP-AD7700	N/A		RJ-45	Enabled	Down	Yes	
<input type="checkbox"/> Gi0/6	TX2012RP-AD7700	N/A		RJ-45	Enabled	Down	Yes	
<input type="checkbox"/> Gi0/7	TX2012RP-AD7700	N/A		RJ-45	Enabled	Down	Yes	
<input type="checkbox"/> Gi0/8	TX2012RP-AD7700	N/A		RJ-45	Enabled	Down	Yes	
<input type="checkbox"/> Ex0/1	TX2012RP-AD7700	N/A		SFP+	Enabled	Down	No	
<input type="checkbox"/> Ex0/2	TX2012RP-AD7700	N/A		SFP+	Enabled	Down	No	

Showing 1 - 10 Total: 12 10 < Previous 1 2 Next >

Port Channel

Apply Configuration View Configuration Jobs

The **Ports** General details view displays following fields by default:

- Port, Tags, Description, Interface, Administrative State, Operational State, PoE Capable, and Edit.
- Click on **Apply Configuration** whenever you are sure to apply the modified configuration, preferably after all the port details are updated.

User can click on top bar to include additional fields in **Ports** General Detail view.

☒ **General**

☒ Interface ☒ Administrative State

☒ Operational State ☒ PoE Capable

☐ **Physical**

☐ PoE State ☐ PoE Priority

☐ PoE Mode ☐ Output signal

☐ Speed ☐ Duplex

☐ MTU

☐ **Network**

☐ Type ☐ VLANs

☐ Native VLAN ☐ Channel ID

☐ PBA Policy ☐ PBA State

☐ STP State ☐ STP Priority

☐ Expiration Reset ☐ Automatic LLDP-MED Voice

☐ STP BPDU Guard ☐ Broadcast

☐ Unknown Unicast ☐ Multicast

☐ Suppression Rate

☐ **Security**

☐ QoS Trust ☐ User Priority

☐ Dot1x port-control ☐ Host Mode

☐ MAC Auth Bypass ☐ Protected Port

☐ DHCP Snooping Trust ☐ ACL Name

Click the edit (✎) icon or Port device in the list to edit the Ports Configuration General tab details.

Navigate to **Switch Groups > Switches > Port Configuration**.

Switch Groups > Complete_Configured > Port Configuration

Basic
Physical
Network
Security

Switch Port(s) Configuration

EX2016MP-F457A1: [1]

Tags

Enter alphanumeric string for port identification and filtering.

Description

Enter string with max 32 characters.

Save

Enter the **Tags** and **Description** details and Click **Save**.



Note

After modifying the port or channel details, you can apply the configuration to the device by clicking the **Apply Configuration** button at the bottom of the **Switch Ports** page.

Physical Tab

The **Ports Physical** details view displays following fields by default:

- Port, Tags, Operational State, PoE State, PoE Priority, Speed, Duplex, MTU, and Edit.

Switch Groups > Complete_Configured

Dashboard Notifications Configuration Statistics Switches **Switch Ports**

Configuration Statistics

Ports

Port	Tags	Description	PoE State	PoE Priority	PoE Mode	Speed	Duplex	MTU	
EX2016MP-F457A1-1	N/A	DP-DonotUse-EX2010-Manag...	Enabled	Low		1 Gbps	Full	1500	✎
EX2016MP-F457A1-2	N/A	Desc-1	Enabled	Low		1 Gbps	Full	1500	✎
EX2016MP-F457A1-3	N/A		Enabled	Low		1 Gbps	Full	1500	✎
EX2016MP-F457A1-4	N/A		Enabled	Low		1 Gbps	Full	1500	✎
EX2016MP-F457A1-5	N/A	descr-5	Enabled	Low		1 Gbps	Full	1500	✎
EX2016MP-F457A1-6	N/A		Enabled	Low		1 Gbps	Full	1500	✎
EX2016MP-F457A1-7	N/A		Enabled	Low		1 Gbps	Full	1500	✎
EX2016MP-F457A1-8	N/A		Enabled	Low		1 Gbps	Full	1500	✎
EX2016MP-F457A1-9	N/A		Enabled	Low		2.5 Gbps	Full	1500	✎
EX2016MP-F457A1-10	N/A		Enabled	Low		2.5 Gbps	Full	1500	✎

Showing 1-10 Total: 16 10 < Previous 1 2 Next >


Port Channel

Channel ID	Switch	Tags	Description	VLANs	Native VLAN	Type	Administrative State	Mode	Ports	STP State	STP Priority	
1	EX2016MP-F457A1	Tag-123	desc-123	1	1	Access	Enabled	Manual	2,3	Disabled	128	✎ ✕
2	EX2016MP-F457A1	Tag-456	hello678	1	1	Hybrid	Enabled	Manual	4,5	Enabled	128	✎ ✕
10	EX2016MP-F457A1	N/A	N/A	1	1	Hybrid	Enabled	Active	10	Enabled	128	✎ ✕
30	EX2016MP-F457A1	port-3	hello-3	1-4066	1	Trunk	Disabled	Passive	6	Disabled	128	✎ ✕

Showing 1-4 Total: 4 10 < Previous 1 Next >

You can click  on top bar to include additional fields in **Ports** Physical Detail view.

<input type="checkbox"/> General	
<input type="checkbox"/> Interface	<input type="checkbox"/> Administrative State
<input type="checkbox"/> Operational State	<input type="checkbox"/> PoE Capable
<input checked="" type="checkbox"/> Physical	
<input checked="" type="checkbox"/> PoE State	<input checked="" type="checkbox"/> PoE Priority
<input checked="" type="checkbox"/> PoE Mode	<input type="checkbox"/> Output signal
<input checked="" type="checkbox"/> Speed	<input checked="" type="checkbox"/> Duplex
<input checked="" type="checkbox"/> MTU	
<input type="checkbox"/> Network	
<input type="checkbox"/> Type	<input type="checkbox"/> VLANs
<input type="checkbox"/> Native VLAN	<input type="checkbox"/> Channel ID
<input type="checkbox"/> PBA Policy	<input type="checkbox"/> PBA State
<input type="checkbox"/> STP State	<input type="checkbox"/> STP Priority
<input type="checkbox"/> Expiration Reset	<input type="checkbox"/> Automatic LLDP-MED Voice
<input type="checkbox"/> STP BPDU Guard	<input type="checkbox"/> Broadcast
<input type="checkbox"/> Unknown Unicast	<input checked="" type="checkbox"/> Multicast
<input type="checkbox"/> Suppression Rate	
<input type="checkbox"/> Security	
<input type="checkbox"/> QoS Trust	<input type="checkbox"/> User Priority
<input type="checkbox"/> Dot1x port-control	<input type="checkbox"/> Host Mode
<input type="checkbox"/> MAC Auth Bypass	<input type="checkbox"/> Protected Port
<input type="checkbox"/> DHCP Snooping Trust	<input type="checkbox"/> ACL Name

Click the edit () icon or Port device in the list to edit the Ports Configuration **Physical** tab details.

Switch Groups > Complete Configured > Port Configuration

Basic	Switch Port(s) Configuration EX1028P-F64C60-test: [1]
Physical	
Network	
Security	

Port Management
Administrative State
Enable
Speed
Auto
MTU
1500

PoE
Administrative State
Enable
PoE Priority
Low
PoE Mode
802.3

Save

Enter the **Port Management** and **PoE details** and click **Save**.

Network Tab

The **Ports Network** details view displays following fields by default:

- Port, Tags, Type, VLANs, Native VLAN, Channel ID, PBA Policy, PBA State, STP State STP Priority, and Edit.

Switch Groups > Complete_Configured

Dashboard Notifications Configuration Statistics Switches **Switch Ports**

Configuration Statistics

Ports

Search


Port	Tags	Description	Type	VLANs	Native VL...	Channel ID	PBA Policy	PBA State	STP State	STP Priority	STP BPOU ...	Broadcast	Unknown ...	Multicast	Suppressio...
<input type="checkbox"/> EX2016MP-F457A1-1	N/A	DP-DonotUse-EX...	Hybrid	1	1	N/A		Enabled	Enabled	N/A	Disabled	Disabled	Disabled	Disabled	N/A
<input type="checkbox"/> EX2016MP-F457A1-2	N/A	Desc-1	Hybrid	1	1	N/A		Enabled	Enabled	N/A	Disabled	Disabled	Disabled	Disabled	N/A
<input type="checkbox"/> EX2016MP-F457A1-3	N/A		Hybrid	1	1	N/A		Enabled	Enabled	N/A	Disabled	Disabled	Disabled	Disabled	N/A
<input type="checkbox"/> EX2016MP-F457A1-4	N/A		Hybrid	1	1	N/A		Enabled	Enabled	N/A	Disabled	Disabled	Disabled	Disabled	N/A
<input type="checkbox"/> EX2016MP-F457A1-5	N/A	descr-5	Hybrid	1	1	N/A		Enabled	Enabled	N/A	Disabled	Disabled	Disabled	Disabled	N/A
<input type="checkbox"/> EX2016MP-F457A1-6	N/A		Hybrid	1	1	N/A		Enabled	Enabled	N/A	Disabled	Disabled	Disabled	Disabled	N/A
<input type="checkbox"/> EX2016MP-F457A1-7	N/A		Hybrid	1	1	N/A		Enabled	Enabled	N/A	Disabled	Disabled	Disabled	Disabled	N/A
<input type="checkbox"/> EX2016MP-F457A1-8	N/A		Hybrid	1	1	N/A		Enabled	Enabled	N/A	Disabled	Disabled	Disabled	Disabled	N/A
<input type="checkbox"/> EX2016MP-F457A1-9	N/A		Hybrid	1	1	N/A		Enabled	Enabled	N/A	Disabled	Disabled	Disabled	Disabled	N/A
<input type="checkbox"/> EX2016MP-F457A1-10	N/A		Hybrid	1	1	N/A		Enabled	Enabled	N/A	Disabled	Disabled	Disabled	Disabled	N/A

Showing 1 - 10 Total 16 10 < Previous 1 2 Next >

Port Channel

Search

Channel ID	Switch	Tags	Description	VLANs	Native VLAN	Type	Administrative State	Mode	Ports	STP State	STP Priority
1	EX2016MP-F457A1	Tag-123	desc-123	1	1	Access	Enabled	Manual	2,3	Disabled	128
2	EX2016MP-F457A1	Tag-456	hello678	1	1	Hybrid	Enabled	Manual	4,5	Enabled	128
10	EX2016MP-F457A1	N/A	N/A	1	1	Hybrid	Enabled	Active	10	Enabled	128
30	EX2016MP-F457A1	port-3	hello-3	1-4066	1	Trunk	Disabled	Passive	6	Disabled	128

- User can click  on top bar to include additional fields in **Ports** Network Detail view.

☐ General

☐ Interface ☐ Administrative State

☐ Operational State ☐ PoE Capable

☐ Physical

☐ PoE State ☒ PoE Priority

☐ PoE Mode ☐ Output signal

☐ Speed ☐ Duplex

☐ MTU

☒ Network

☒ Type ☒ VLANs

☒ Native VLAN ☒ Channel ID

☒ PBA Policy ☒ PBA State

☒ STP State ☒ STP Priority

☐ Expiration Reset ☐ Automatic LLDP-MED Voice

☐ STP BPOU Guard ☐ Broadcast

☐ Unknown Unicast ☐ Multicast

☐ Suppression Rate


☐ Security

☐ QoS Trust ☐ User Priority

☐ Dot1x port-control ☐ Host Mode

☐ MAC Auth Bypass ☐ Protected Port

☐ DHCP Snooping Trust ☐ ACL Name

- Click the edit () icon or Port device in the list to edit the Ports Configuration Network tab details.

Switch Groups > May15th1 > Port Configuration

Basic
Physical
Network
Security

Switch Port(s) Configuration

TX2020RP-B0D980: [2]

VLANs

Type
Hybrid

VLANs
1 Available VLANs - 1

Native VLAN
1 ☐ Tagged

Rate limiting

Ingress Port Rate Limit
0


Egress Port Rate Limit
0

Egress Port Burst Size
0

Policy Based Automation

PBA port status
Enable

LLDP Actions

Expiration Reset 
Disable

Automatic LLDP-MED Voice
Enable

Storm Control

Suppression Rate
1-262143

Broadcast
Disable

Multicast

Save



Note

LLDP Actions > Expiration Rest option is a Pro feature.

Enter **VLANs**, **STP**, **Policy Based Automation**, and **Storm Control** details and click **Save**.

Security Tab

The **Ports Security** details view displays following fields by default:

- Port, Tags, QoS Trust, User Priority, Dot1x port-control, Protected Port, DHCP Snooping Trust, ACL Name, and Edit.

Switch Groups > Complete_Configured

Dashboard Notifications Configuration Statistics Switches **Switch Ports**

Configuration Statistics

Ports

Search

Port	Tags	Description	QoS Trust	User Priority	Dot1x port-control	Protected Port	DHCP Snooping Trust	ACL Name
EX2016MP F45761.1	N/A	DP Donetube-EX2016 Mana...	Untrust	0	forceAuthorized	Disabled	Untrusted	
EX2016MP F45761.2	N/A	Desc 1	Untrust	0	forceAuthorized	Disabled	Untrusted	
EX2016MP F45761.3	N/A		Untrust	0	forceAuthorized	Disabled	Untrusted	
EX2016MP F45761.4	N/A		Untrust	0	forceAuthorized	Disabled	Untrusted	
EX2016MP F45761.5	N/A	desc 5	Untrust	0	forceAuthorized	Disabled	Untrusted	
EX2016MP F45761.6	N/A		Untrust	0	forceAuthorized	Disabled	Untrusted	
EX2016MP F45761.7	N/A		Untrust	0	forceAuthorized	Disabled	Untrusted	
EX2016MP F45761.8	N/A		Untrust	0	forceAuthorized	Disabled	Untrusted	
EX2016MP F45761.9	N/A		Untrust	0	forceAuthorized	Disabled	Untrusted	
EX2016MP F45761.10	N/A		Untrust	0	forceAuthorized	Disabled	Untrusted	


Showing 1-10 Total: 10

Port Channel

Search

Channel ID	Switch	Tags	Description	VLANs	Native VLAN	Type	Administrative State	Mode	Ports	STP State	STP Priority
1	EX2016MP F45761	Tag 123	desc 123	1	1	Access	Enabled	Manual	2,3	Disabled	128
2	EX2016MP F45761	Tag 456	hello678	1	1	Hybrid	Enabled	Manual	4,5	Enabled	128
10	EX2016MP F45761	N/A	N/A	1	1	Hybrid	Enabled	Active	10	Enabled	128
30	EX2016MP F45761	port 3	hello 3	14066	1	Trunk	Disabled	Passive	6	Disabled	128

Showing 1-4 Total: 4

User can click  on top bar to include additional fields in **Ports** Security Detail view.

☐ General

☐ Interface ☐ Administrative State

☐ Operational State ☐ PoE Capable

☐ Physical

☐ PoE State ☐ PoE Priority

☐ PoE Mode ☐ Output signal

☐ Speed ☐ Duplex

☐ MTU

☐ Network

☐ Type ☐ VLANs

☐ Native VLAN ☐ Channel ID

☐ PBA Policy ☐ PBA State

☐ STP State ☐ STP Priority

☐ Expiration Reset ☐ Automatic LLDP-MED Voice

☐ STP BPDU Guard ☐ Broadcast

☐ Unknown Unicast ☐ Multicast

☐ Suppression Rate


☒ Security

☒ QoS Trust ☒ User Priority

☒ Dot1x port-control ☒ Host Mode

☒ MAC Auth Bypass ☒ Protected Port

☒ DHCP Snooping Trust ☒ ACL Name

Click the edit () icon or Port device in the list to edit the Ports Configuration Security tab details.

Switch Groups > Default Switch > Port Configuration

Basic

Physical

Network

Security

Switch Port(s) Configuration

DPI-X8MB-223-Subnet: [6]

802.1x Port Control

Port Control

Force-Authorized

Host Mode

Multi Host

MAC Authentication Bypass

Disable

DHCP Snooping Trusted State

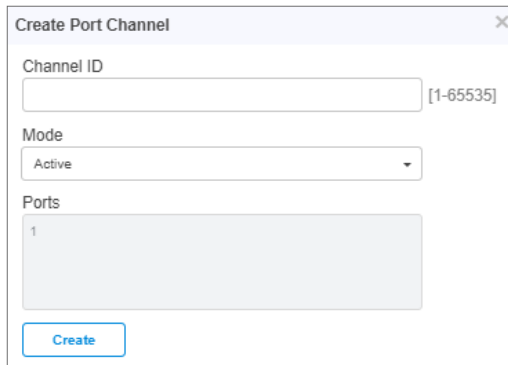
Port Trusted State

Untrusted

Enter **802.1xPort Control**, **DHCP Snooping Trusted State**, **QoS**, **Protected Port**, **Access Control List** details and click **Save**.

Port Channel

- To create a Port Channel, select a **Port** from the list under the specific parameters and click **Create Port Channel**.
- **Create Port Channel** window Pops-up, enter details.
- Click **Create**.

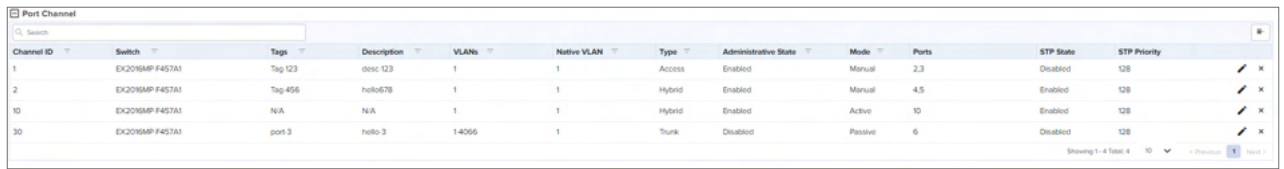


The 'Create Port Channel' dialog box contains the following fields:

- Channel ID:** A text input field with a placeholder value of [1-65535].
- Mode:** A dropdown menu currently set to 'Active'.
- Ports:** A list box containing the number '1'.
- Create:** A blue button at the bottom.

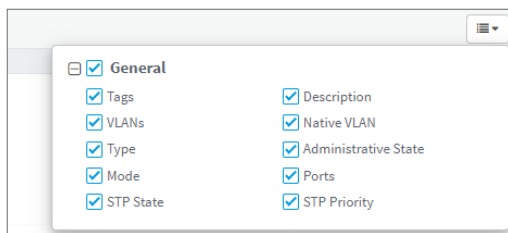
The **Port Channel** details view displays following fields by default:

- Channel ID, Switch, Tags, Description, VLANs, Native VLAN, Type, Administrative State, Mode, Ports, STP State, and STP Priority.



Channel ID	Switch	Tags	Description	VLANs	Native VLAN	Type	Administrative State	Mode	Ports	STP State	STP Priority
1	EX2095MP F457A1	Tag 123	desc 123	1	1	Access	Enabled	Manual	2,3	Disabled	128
2	EX2095MP F457A1	Tag 456	hello678	1	1	Hybrid	Enabled	Manual	4,5	Enabled	128
10	EX2095MP F457A1	N/A	N/A	1	1	Hybrid	Enabled	Active	10	Enabled	128
30	EX2095MP F457A1	port 3	hello-3	1-4096	1	Trunk	Disabled	Passive	6	Disabled	128

User can click  on top bar to include additional fields in **Port Channel** Detail view.



The field selection menu shows the following options, all of which are checked:

- ☒ General
- ☒ Tags
- ☒ VLANs
- ☒ Type
- ☒ Mode
- ☒ STP State
- ☒ Description
- ☒ Native VLAN
- ☒ Administrative State
- ☒ Ports
- ☒ STP Priority

Statistics

The **Statistics** page displays the latest data and statistics of each Port. Port statistics match the Client statistics and generate the Client View.

To view the Switch Ports Statics navigate to **Configuration > Switch Groups > Switch Ports > Statistics**.

Switch Groups > 4thApril-Hash

Dashboard Notifications Configuration Statistics Switches **Switch Ports**

Configuration **Statistics**

Apply Filter(s)

Port	Switch	Tags	Description	Rx Unicast Pkts	Rx Multicast Pkts	Rx Broadcast Pkts	Rx Errors	Rx Total Pkts	Tx Errors	Tx Total Pkts	Link Transitions
Gi0/1	EX2028P-FOC200	-		0	0	0	0	0	0	0	0
Gi0/2	EX2028P-FOC200	-	EX3052RP-A5F480-UpLink-DND	66348	11018	19555	0	96921	0	219127	1
Gi0/3	EX2028P-FOC200	-		0	0	0	0	0	0	0	0
Gi0/4	EX2028P-FOC200	port4		0	0	0	0	0	0	0	0
Gi0/5	EX2028P-FOC200	-		0	0	0	0	0	0	0	0
Gi0/6	EX2028P-FOC200	-		0	0	0	0	0	0	0	0
Gi0/7	EX2028P-FOC200	port7		0	0	0	0	0	0	0	0
Gi0/8	EX2028P-FOC200	-		0	0	0	0	0	0	0	0
Gi0/9	EX2028P-FOC200	-		0	0	0	0	0	0	0	0
Gi0/10	EX2028P-FOC200	-		0	0	0	0	0	0	0	0

Showing 1 - 10 Total: 80 10 < Previous 1 2 3 4 5 ... 8 Next >

To apply filters, follow the below steps:

1. Click on the **Apply Filter(s)** tab.
2. A new window titled **Filters** appears.

Filters

Port

Search

Switch

Search

Tags

Search


Description

Search

Reset

Apply Filter(s)

3. Enter information in any field based on your filtering needs.
4. Click on **Apply Filter(s)**.

User can click  on top bar to include additional fields in **Statistics** Detail view.

☐ General

☒ Port
 ☒ Tags
 ☒ Description
 ☐ Interface
 ☐ Operational State

☐ Statistics

☐ Rx Octets
 ☒ Rx Unicast Pkts
 ☒ Rx Multicast Pkts
 ☒ Rx Broadcast Pkts
 ☒ Rx Errors
 ☒ Rx Total Pkts
 ☐ Tx Octets Pkts
 ☐ Tx Unicast Pkts
 ☐ Tx Multicast Pkts
 ☐ Tx Broadcast Pkts
 ☒ Tx Errors
 ☒ Tx Total Pkts

Device Details

Details page provide the information about the switches **Overview**, **Topology**, and **Port Statistics**.

cnMatrix > cnMatrix-EX2016M-123

[Dashboard](#) [Notifications](#) [Configuration](#) [Details](#) [Performance](#) [Software Update](#) [Tools](#)

[Overview](#) [Topology](#) [Port Statistics](#)

System

Name	cnMatrix-EX2016M-123
Device Type	cnMatrix EX2016M-P
System Uptime	1d 0h 4m
Coordinates	[12.933791, 77.694211]
Description	
Hardware	Ethernet switch 8 copper 1G ports, 6 copper 2.5G ports, 2 SFP+ 10G ports, with 4PPoE
Hardware Version	01
DA Version	4.14
Manufacture Date	2020-04-07
Onboard Date	Oct 26 2021 14:46:15

Software Update

Active Software Version	4.1.1-r2
-------------------------	----------

History

Date	Status	Version
Tue Nov 02 2021 16:38:18 UTC +0530	Success	4.1.1-r2
Sat Oct 30 2021 10:15:13 UTC +0530	Success	4.1.2-r1
Thu Oct 28 2021 22:33:34 UTC +0530	Success	4.0-r4

Configuration Update

History

Date	Status	Template
Wed Nov 03 2021 12:18:35 UTC +0530	Success	cnMatrix - Syslog configuration
Tue Nov 02 2021 11:46:56 UTC +0530	Success	cnMatrix - Syslog configuration
Tue Nov 02 2021 10:55:39 UTC +0530	Success	Default Switch

Details Overview

To view the details of the overview page, navigate to the **Details > Overview** tab.

cnMatrix > cnMatrix-EX2016M-123

Dashboard Notifications Configuration **Details** Performance Software Update Tools

Overview Topology Port Statistics

System

Name	cnMatrix-EX2016M-123
Device Type	cnMatrix EX2016M-P
System Uptime	1d 0h 4m
Coordinates	[12.933791, 77.694211]
Description	
Hardware	Ethernet switch 8 copper 1G ports, 6 copper 2.5G ports, 2 SFP+ 10G ports, with 4PPoE
Hardware Version	01
DA Version	4.14
Manufacture Date	2020-04-07
Onboard Date	Oct 26 2021 14:46:15

Software Update

Active Software Version 4.1.1-r2

History

Date	Status	Version
Tue Nov 02 2021 16:38:18 UTC +0530	Success	4.1.1-r2
Sat Oct 30 2021 10:15:13 UTC +0530	Success	4.1.2-r1
Thu Oct 28 2021 22:33:34 UTC +0530	Success	4.0-r4

Configuration Update

History

Date	Status	Template
Wed Nov 03 2021 12:18:35 UTC +0530	Success	cnMatrix - Syslog configuration
Tue Nov 02 2021 11:46:56 UTC +0530	Success	cnMatrix - Syslog configuration
Tue Nov 02 2021 10:55:39 UTC +0530	Success	Default Switch

Topology

To view the details of the Topology page, navigate to the **Details > Topology** tab.

cnMatrix > Andriy-EX2052-F493E0

Dashboard Notifications Configuration **Details** Performance Software Update Tools Assists X

Overview **Topology** Port Statistics

Apply Filter(s)

ID	Name	Chassis ID	Description	MAC Address	IPv4 Address
GI0/1	TX2020RP-80E280-DND-Devices-Connected	bc:e6:7c:b0:e2:81	Cambium Networks cnMatrix TX2020R-P Ethernet Switch HW:02 SW:4.4-r3	bc:e6:7c:b0:e2:83	

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

To apply filters, follow the below steps:

1. Click on the **Apply Filter(s)** tab.
2. A new window titled **Filters** appears.

Filters

×

ID

Q Search

Name

Q Search

Chassis ID

Q Search

Description

Q Search

MAC Address

Q Search

IPv4 Address

Q Search

Reset

Apply Filter(s)

- Enter information in any field based on your filtering needs.
- Click on **Apply Filter(s)**.

Port Statistics

To view the details of the Port Statistics page, navigate to the **Details > Port Statistics** tab.

cnMatrix > Andriy-EX2052-F493E0

Dashboard

Notifications

Configuration

Details

Performance

Software Update

Tools

Assists X

Overview

Topology

Port Statistics

Apply Filter(s)

⊞

Port	Switch	Tags	Description	Rx Unicast Pkts	Rx Multicast Pkts	Rx Broadcast Pkts	Rx Errors	Rx Total Pkts	Tx Errors	Tx Total Pkts	Link Transitions
Ex0/4	Andriy-EX2052-F493E0	-		0	0	0	0	0	0	0	0
Ex0/3	Andriy-EX2052-F493E0	-		0	0	0	0	0	0	0	0
Ex0/2	Andriy-EX2052-F493E0	-		0	0	0	0	0	0	0	0
Ex0/1	Andriy-EX2052-F493E0	-		0	0	0	0	0	0	0	0
Gi0/48	Andriy-EX2052-F493E0	-		0	0	0	0	0	0	0	0
Gi0/47	Andriy-EX2052-F493E0	-		0	0	0	0	0	0	0	0
Gi0/46	Andriy-EX2052-F493E0	-		0	0	0	0	0	0	0	0
Gi0/45	Andriy-EX2052-F493E0	-		0	0	0	0	0	0	0	0
Gi0/44	Andriy-EX2052-F493E0	-		0	0	0	0	0	0	0	0
Gi0/43	Andriy-EX2052-F493E0	-		0	0	0	0	0	0	0	0

Showing 1 - 10 Total: 52

10

Previous

1

2

3

4

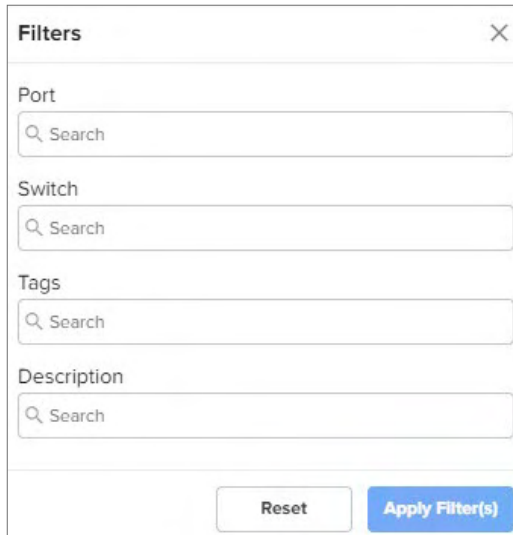
5

6

Next

To apply filters, follow the below steps:

- Click on the **Apply Filter(s)** tab.
- A new window titled **Filters** appears.



The image shows a 'Filters' dialog box with a close button (X) in the top right corner. It contains four search fields, each with a magnifying glass icon and the text 'Search':

- Port
- Switch
- Tags
- Description

At the bottom of the dialog, there are two buttons: a 'Reset' button and an 'Apply Filter(s)' button.

3. Enter information in any field based on your filtering needs.
4. Click on **Apply Filter(s)**.

60 GHz cnWave Network Configuration

cnWave 60 GHz operates with Cambium Networks cnMaestro management system. cnMaestro simplifies device management by offering full network visibility and zero-touch provisioning. Using cnMaestro, user can view network status and perform a full suite of wireless network management functions in real time including optimizing system availability, maximizing throughput, and meeting the emerging needs of business and residential customers.

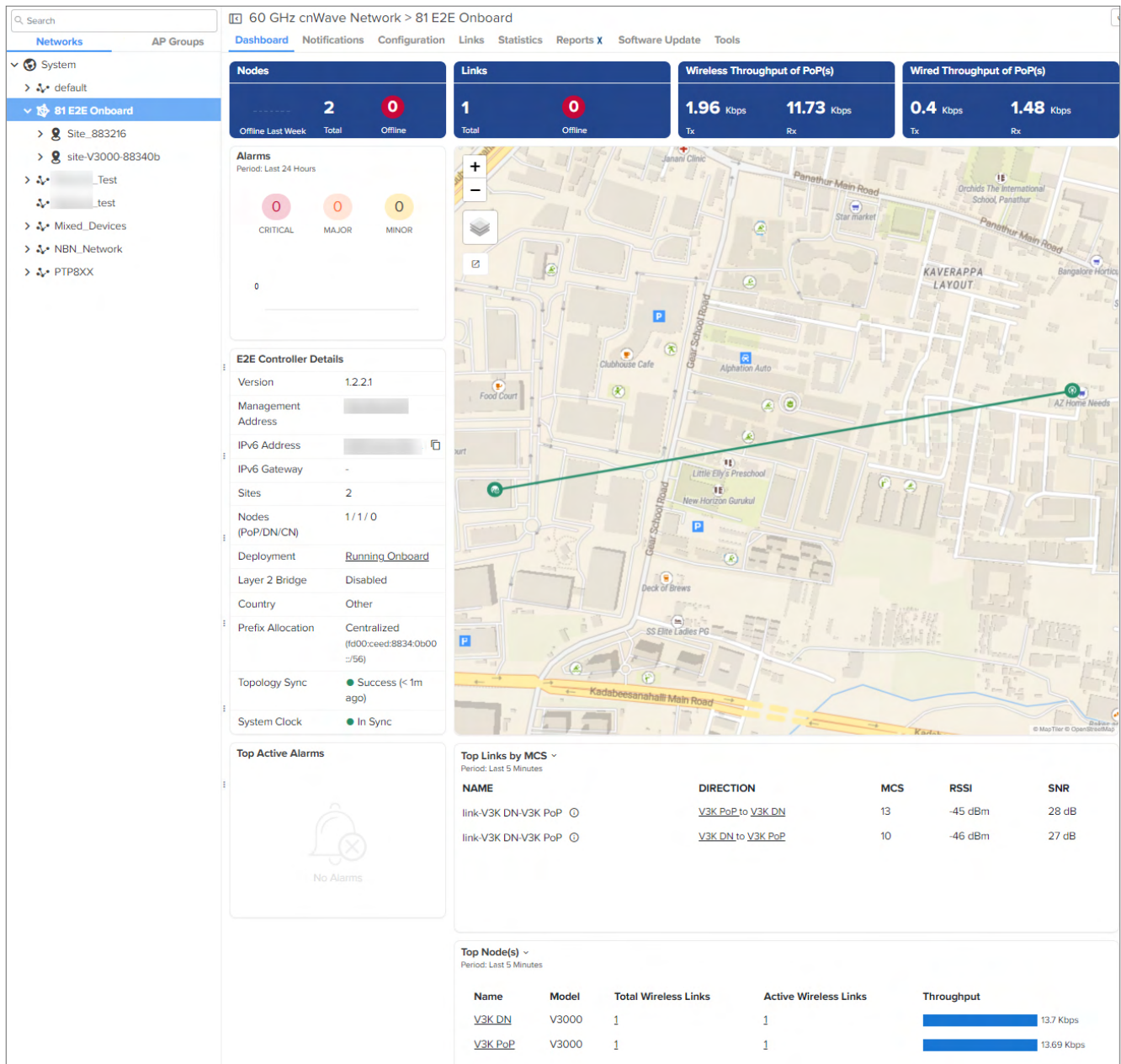
Managing E2E Network

The Monitor and Manage tab displays the monitoring panel of 60 GHz cnWave for cnMaestro. This section includes the following:

- [Dashboard](#)
- [Notifications](#)
- [Configuration](#)
- [Links](#)
- [Statistics](#)
- [Software Update](#)
- [Report](#)
- [Map](#)
- [Tools](#)

Dashboard

Dashboard pages are customized for each device type and aggregation level (such as E2E Network, Node, and Site). The dashboard section displays the **Nodes**, **Links**, **Wireless Throughput of PoP(s)**, **Wired Throughput of PoP(s)**, **Alarms**, **E2E Controller Details**, **Top Active Alarms**, **Map**, **Top Links by MCS**, **Top Links by RSSI**, **Top Links by SNR**, **Top Node(s)**, **Top PoP(s)**, **Top DN(s)**, and **Top CN(s)**.



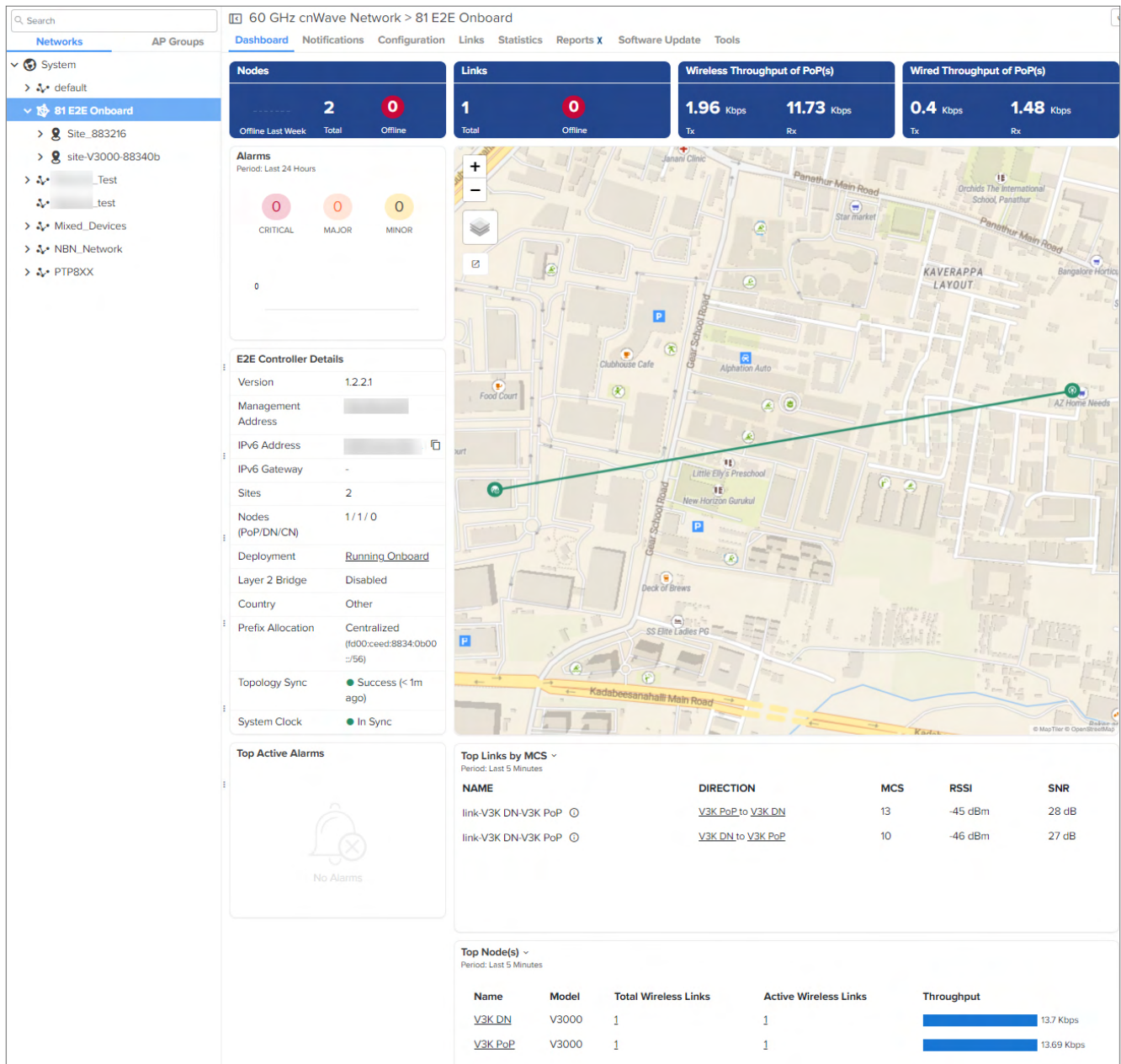
Note

Backup CN links are not shown as Offline links in links widget.

Auto Manage IPv6 Routes (E2E Controller ↔ Node)

The **External E2E Network** dashboard page displays the **Auto Manage IPv6 Routes (E2E Controller ↔ Node)** tab, if you enable **Auto Manage Routes** in the **Tools > Settings** page of **External E2E Network**.

This feature automates IPv6 routes for DNs and CNs based on status of the topology and PoP nodes. It is applicable only if PoP nodes and E2E Controller are in the same Network or containing the same prefix length.




Note

Auto Manage IPv6 Routes is not applicable for Onboard E2E Controller.



E2E Controller Details

E2E Controller Details displays the details such as **Version**, **Management Address**, **IPv6 Address**, **IPv6 Gateway**, **Sites**, **Nodes**, **(PoP/DN/CN)**, **Deployment**, **Layer 2 Bridge**, **Country**, **Prefix Allocation**, **Topology Sync**, and **System Clock**

- If Onboard E2E controller is enabled in device and managed by cnMaestro, it displays deployment as **Running Onboard**.

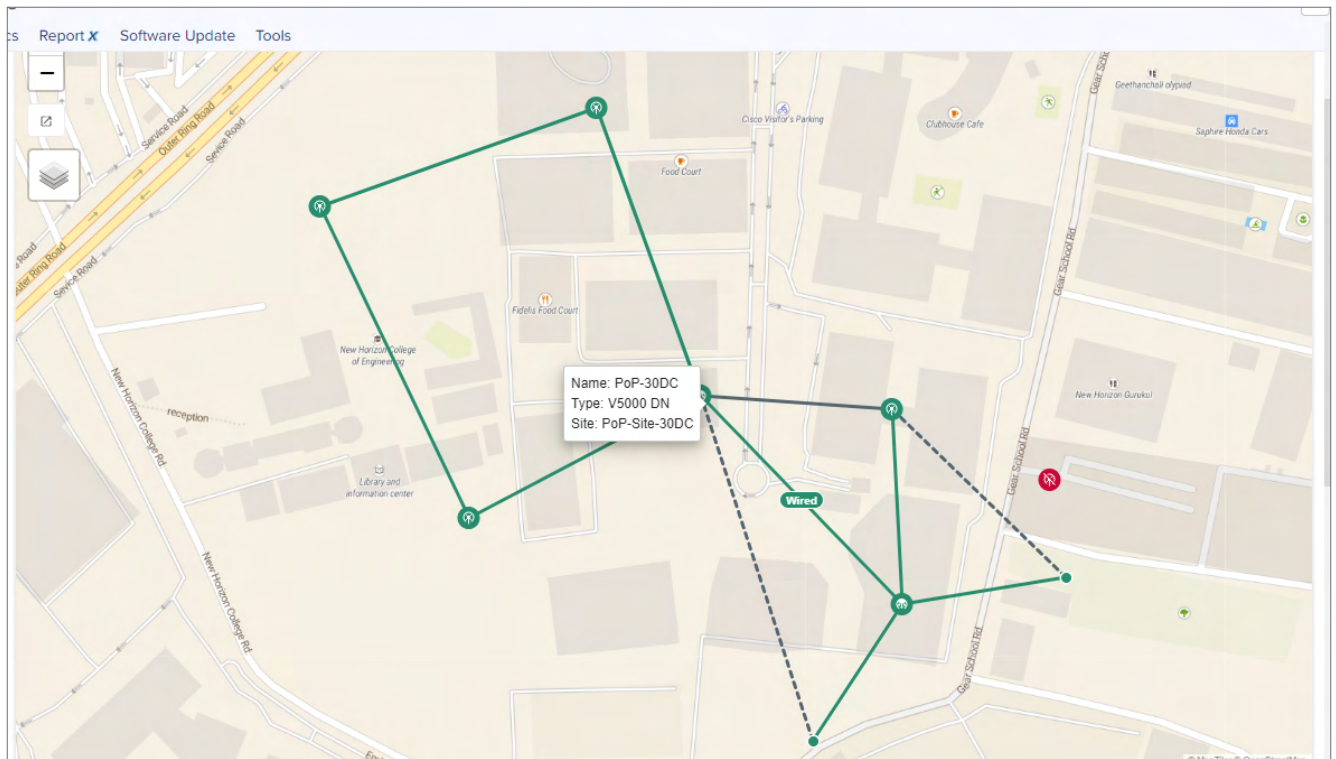
E2E Controller Details	
Version	1.1
Management Address	10.110.221.242
IPv6 Address	fd00:ba5e:88:3083::88:3... 
IPv6 Gateway	-
Sites	4
Nodes (PoP/DN/CN)	1 / 0 / 1
Deployment	Running Onboard
Layer 2 Bridge	Disabled
Country	Belgium
Prefix Allocation	Deterministic (fd00:ceed:8830:8300::/56)
Topology Sync	Success (6m ago)
System Clock	In Sync

- If External E2E controller is managed by cnMaestro, it displays deployment as **External**.

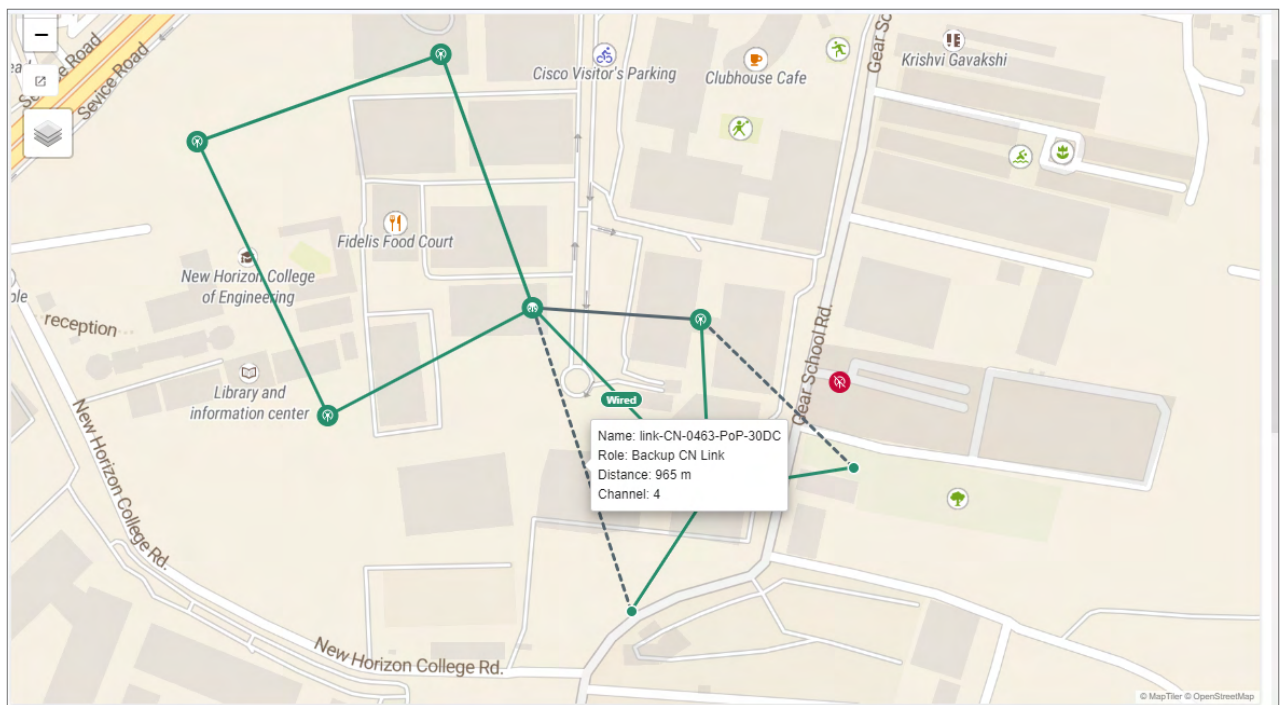
E2E Controller Details	
Version	1.1
Management Address	10.110.221.232
IPv6 Address	fd20:ba5e::100 
IPv6 Gateway	fd20:ba5e::5 
Sites	4
Nodes (PoP/DN/CN)	1 / 0 / 2
Deployment	External
Layer 2 Bridge	Disabled
Country	Other
Prefix Allocation	Centralized (fd00:ceed:17a1:1600::/56)
Topology Sync	Success (4m ago)
System Clock	In Sync

Dashboard Maps

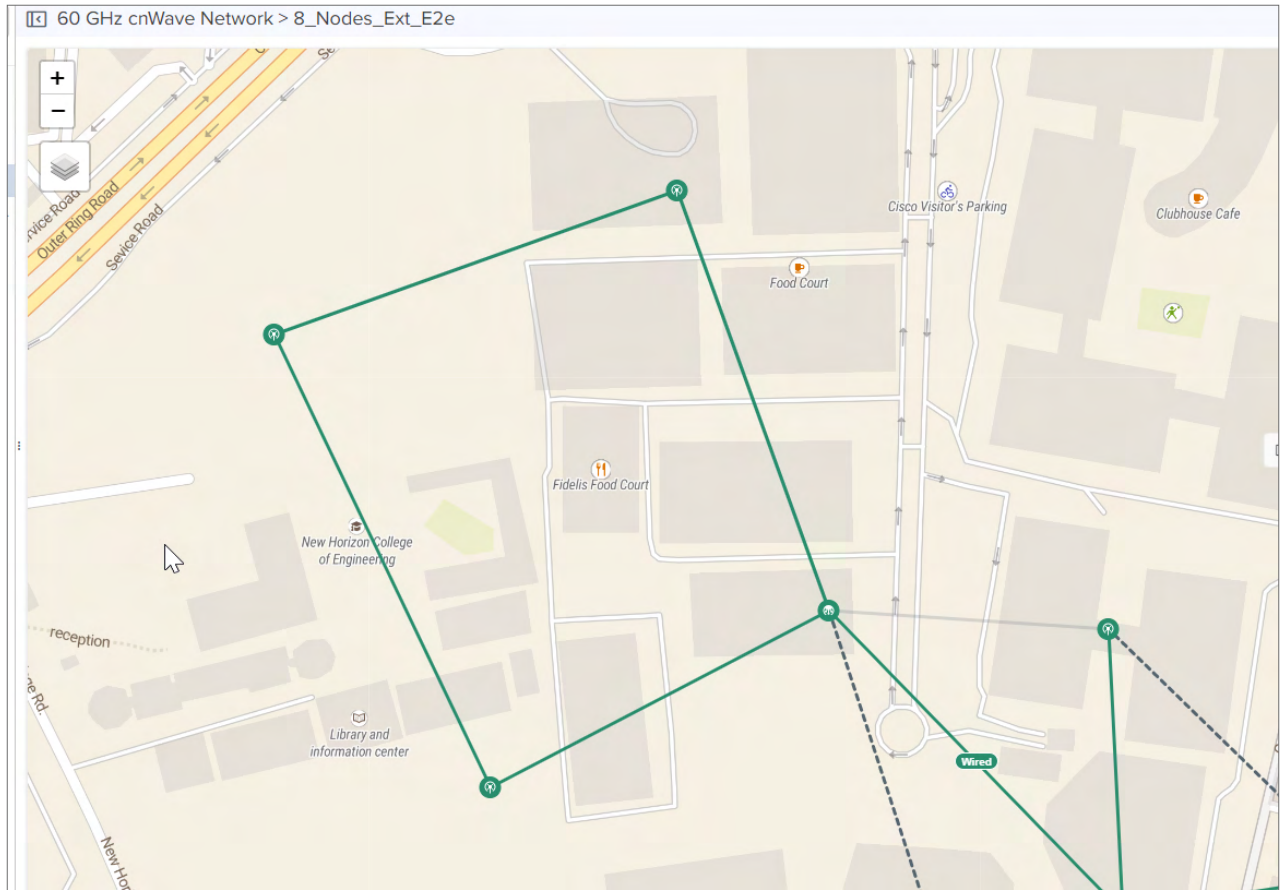
In the dashboard map, when user hovers on particular **PoP**, **DN** or **CN** it pops-up the device details. When user hovers on particular link it pops up the link details.



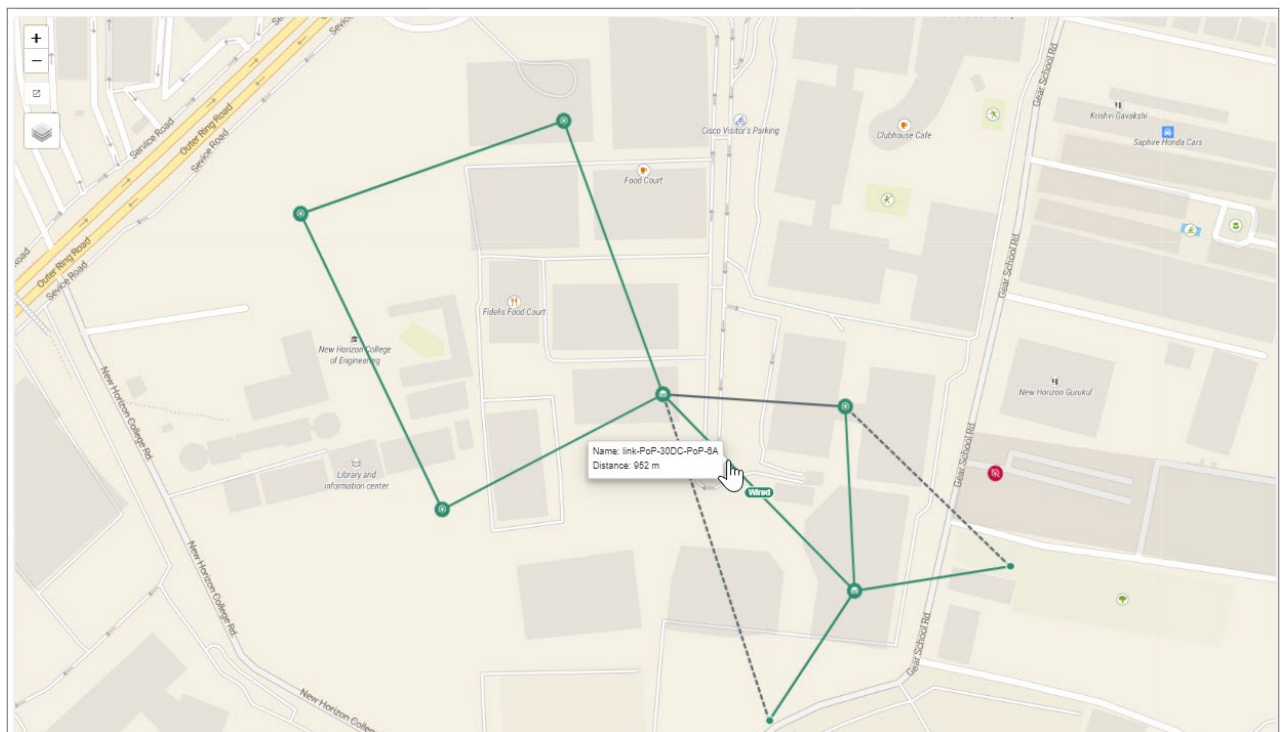
- Dotted line displays the Backup CN link between the DN and CN..



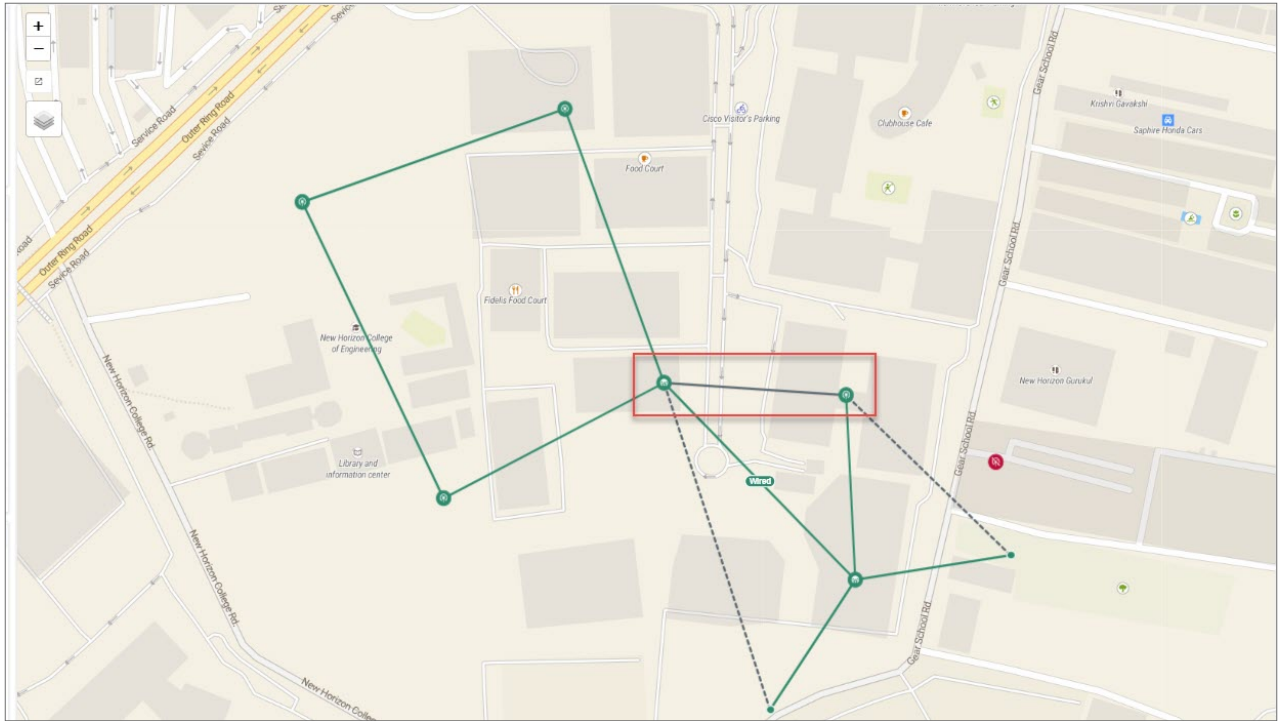
- Continuous line display the wireless link between PoP, DN, or CN..



- Continuous line with **Wired** tag displays the wired link between PoP, DN, or CN.



- Continuous line with gray color displays the **Disabled Ignition** link.



Notifications

Notifications are same as shown above for other devices, refer to [Notification](#) for more details.

Configuration

Configure the following after onboarding the External or Onboard E2E Controller:

- [Basic](#)
- [Management](#)
- [Radio](#)
- [Security](#)
- [Advanced](#)
- [E2E Controller](#)
- [High Availability X](#)



Note

Once user selects the **Auto-assign** IPv6 Addresses while configuring E2E Controller and PoP node. Use the same IPv6 during the prefix allocation.

Basic Configuration

1. Navigate to **Configuration > Basic** to configure basic settings of E2E Controller.

60 GHz cnWave Network > Ext-E2E-100

Dashboard Notifications **Configuration** Links Statistics Report X Software Update Tools

Basic Management Radio Security Advanced E2E Controller

Prefix Allocation

☐ Centralized ☒ Deterministic

Seed Prefix* [Generate](#) IPv6 'seed prefix' in CIDR format from which subnet prefixes are allocated to all DNs and CNs (e.g. fdce:b00c:cafe::/48)

Prefix Length Length of per-node allocated prefixes

Layer 2 Bridge

☐ Enable Selecting this option will enable Layer 2 network bridging (via automatically created tunnels) across all nodes connected to a PoP. This will facilitate bridging of IPv4 traffic across the wireless networks.

IPv6 Layer3 CPE Address

☒ SLAAC ☐ DHCPv6 Relay

CPE Prefix Zoning

Summarized CPE Prefix Prefix summarizing network wide customized CPE Prefixes/Prefixes allocated by DHCPv6 Relay (that fall outside Seed Prefix range).

Country

DNS Servers DNS server list, comma separated. IPv4 is only supported when Layer 2 bridge is enabled.

NTP Server* NTP Server hostnames or IP addresses, comma separated. IPv4 address is only supported when Layer 2 Bridge is enabled. Note: NTP should be enabled from E2E Network -> Tools -> Settings page.

Time Zone



Note

- **Prefix allocation** automatically gets updated, when E2E Controller is managed by cnMaestro.
- Prefix Length of 48 is supported in Seed Prefix configuration.

2. In the **Prefix Allocation**, select **Centralized** or **Deterministic** to allocate the loopback IPv6 address for the devices.
3. Enter the **Seed Prefix** and **Prefix Length**.
4. Enabling **Layer 2 Bridge** is optional.

Enabling this option will enable Layer 2 network bridging (via automatically created tunnels) connected across all nodes and facilitates bridging of IPv4 traffic across the wireless networks. It also enables the configuration of VLAN Management and Ports on all PoP, DN, and CN Nodes.

In **Layer 2 Bridge**, select the checkbox to enable Layer2 Network Bridging, choose **Tunnel Concentrator** as **Best PoP** or **Static**. If user selects Tunnel Concentrator as Static, enter an external switch or router IPv6 address.



Note

IPv6 Layer3 CPE Address can be enabled when E2E Controller is running 1.1 version and Layer 2 Bridge is disabled.

1. Select the **IPv6 Layer3 CPE Address** as **SLAAC** or **DHCPv6 Relay**.

If user selects **IPv6 Layer3 CPE Address** as **DHCPv6 Relay**, user can configure the DHCPv6 server address. The CPE device sends a DHCP request. The CN device uses the Address and Prefix from the corresponding DHCP pool and DHCPv6 server assigns address to the CPE device.



Note

- By default **Country** is **Other**, user can configure it.
- Enter the **Hostnames** or **IP address** of NTP server.

2. Select the **Country** from the dropdown.
3. Enter the **DNS Server**.
4. Enter **NTP Server**.
5. Select the **Time Zone** from the dropdown.



Note

By default **Wireless Scans** will be disabled.

6. Click **Save**.

Management

Management configuration allows user to configure and manage the credentials of the administrator and it allows enable **SNMP**.

1. Navigate to **Configuration > Management** to set the **Device GUI Passwords** and to enable the **SNMP**.

60 GHz cnWave Network > Ext-EZE-100

Dashboard Notifications **Configuration** Links Statistics Report X Software Update Tools

Basic **Management** Radio Security Advanced EZE Controller

Device GUI Users

Admin User Password

Installer User Password

Monitor User Password

SNMP

☐ Enable SNMP

System Contact

No Contact

System Location

No Location

Community

SNMP community string

IPv4 Source Address

Allowed IPv4 source address prefix

IPv6 Source Address

Allowed IPv6 source address prefix

SNMPv3 User

SNMPv3 Security Level

☐ None ☐ Authentication Only ☐ Authentication & Privacy

2. Click **Save**.

Radio

The Radio page manages the Radio related settings.

60 GHz cnWave Network > Onboard-Multi-PoP Raja

Dashboard Notifications **Configuration** Links Statistics Reports X Software Update Tools

Basic Management **Radio** Security Advanced E2E Controller

Wireless Scans

Scheduled Beam Adjustment
☒ Enabled ☐ Disabled

Scan Interval
 Interval between wireless scans in seconds

CN Channel Rescan

☐ Enabled ☒ Disabled

CN Channel Rescan timeout
 A CN without a wireless link established beyond this timeout will automatically initiate channel scanning.

Fast Acquisition

Mode
☐ Disabled Always scan all fixed beams and save active beam for future
☐ Compatibility Mode Associate on saved beam and perform full scan if unsuccessful
☒ Static Mode Associate on saved beam only. CN channel Rescan not supported

Asymmetric TDD

Duty Cycle

Other Settings

☒ Enable post acquisition beam refinement Disabling this control may reduce link budget by up to 2 dB.

- **Wireless Scans**

- **Enabled/Disabled**—Enable or disable scheduled beam adjustment.
- **Scan Interval**—Specify an interval between wireless scans, in seconds.

- **CN Channel Rescan**

- **Enabled/Disabled**—Enable or disable CN channel rescan.



Note

You can enable CN channel rescan only when Fast Acquisition is set to either **Disabled** or **Compatibility Mode**.

- **CN Channel Rescan timeout**—Specify a timeout interval for a CN that does not have a wireless link to reinitiate channel scanning, in seconds.

- **Fast Acquisition**



Note

Fast acquisition is supported only on 60 GHz cnWave devices running System Release version 1.3 or later.

- **Mode**

- **Disabled**—On link acquisition, performs IBF scan on 61 fixed beams. This is the default option.
- **Compatibility Mode**—On link acquisition, tries the last known (if present) beam index. If unsuccessful, tries normal IBF scan.

- **Static Mode**—On link acquisition, tries the last known (if present) beam index. If unsuccessful, the association fails.
- **Asymmetric TDD**
 - **Duty Cycle**—Select a duty cycle from the dropdown list. For example:
 - **60% Downlink / 40% Uplink**—Set 60% of physical bandwidth for downloading and 40% of the physical bandwidth for uploading.
- **Other Settings**
 - **Enable post acquisition beam refinement**—Select to enable.

Security

Security page allows the user to enable the wireless security **PSK** or **802.1x**. The disabled option connects as unsecure devices.

To **Enable PSK**, complete the following steps:

1. Navigate to **Configuration > Security** tab.
2. Select **PSK** in **Wireless Security**.

3. Enter the **Passphrase**.



Note

If **Passphrase** field is blank, default psk key is used.

4. Click **Save**.

To **Enable 802.1x**, complete the following steps:

1. Navigate to **Configuration > Security**.
2. Select **802.1x** in **Wireless Security**.

60 GHz cnWave Network > Ext-E2E-100

Dashboard Notifications **Configuration** Links Statistics Report X Software Update Tools

Basic Management Radio **Security** Advanced E2E Controller

Wireless Security
☐ Disabled ☐ PSK ☒ 802.1x Enable wireless security and set the method

Radius server IP
 IP address (IPv6/IPv4) of Auth/Radius server

Radius server port
 Auth server port

Radius server shared secret

☐ Disable GUI Login
☐ Disable SSH

Save **Reset**

3. Enter the **Radius server IP**.
4. Enter the **Radius Server port**.
5. Enter the **Radius Server Shared Secret**.
6. Click **Save**.

Advanced

Advanced tab allows the advanced user to edit the settings of the [Table](#) and [JSON](#) format of the E2E Controller.

It also allows to optimize the network using the following options:

- Optimize Control Superframe Allocation
- Optimize DPA Zone Allocation
- Clear Node Auto Configuration

60 GHz cnWave Network > Ext-E2E-100

Dashboard Notifications **Configuration** Links Statistics Report X Software Update Tools

Basic Management Radio Security **Advanced** E2E Controller

All the settings below are for advanced users only.

Base: Firmware: Hardware: Optimization **Table** JSON

Field	Description	Status	Value
assertParams.cambiumAssertRecoveryEnabled	Enables Cambium fw assert recovery.	set	true
bgpParams.allowNonDefaultRoutes	Allow non-default routes to be learned from BGP peers.	set	false
bgpParams.cpePrefixesAutoAdvertisement	Enable automatic advertisement of CPE prefixes, instead of static 'cpeNetworkPrefix'.	set	true
debugSysParams.cambiumSysMonitorEnabled	Enables Cambium System Monitor.	set	false
dhcpParams.dhcpGlobalConfigAppend	DHCP global config append.	unset	
dhcpParams.dhcpInterface	DHCP interface.	unset	
dhcpParams.dhcpNameServer	DHCP name server.	unset	
dhcpParams.dhcpPdDelegatedLen	DHCP PD delegated prefix length.	set	64
dhcpParams.dhcpPdPool	DHCP PD Pool.	unset	
dhcpParams.dhcpPreferredLifetime	DHCP lease preferred lifetime.	set	3600

Save **Reset**

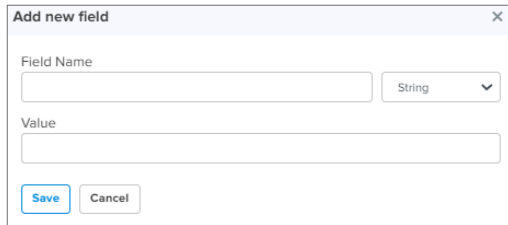
Device Logs
☐ Enable Recommended to be used only by Cambium Support Team.

Table

In the **Table** advanced user can view and edit **Field Name** and **Value**. The field names are sorted in alphabetical order.

To add a field:

1. Navigate to **Configuration > Advanced**.
2. Click **Add New**.
3. Enter the **Field Name** and **Value**.

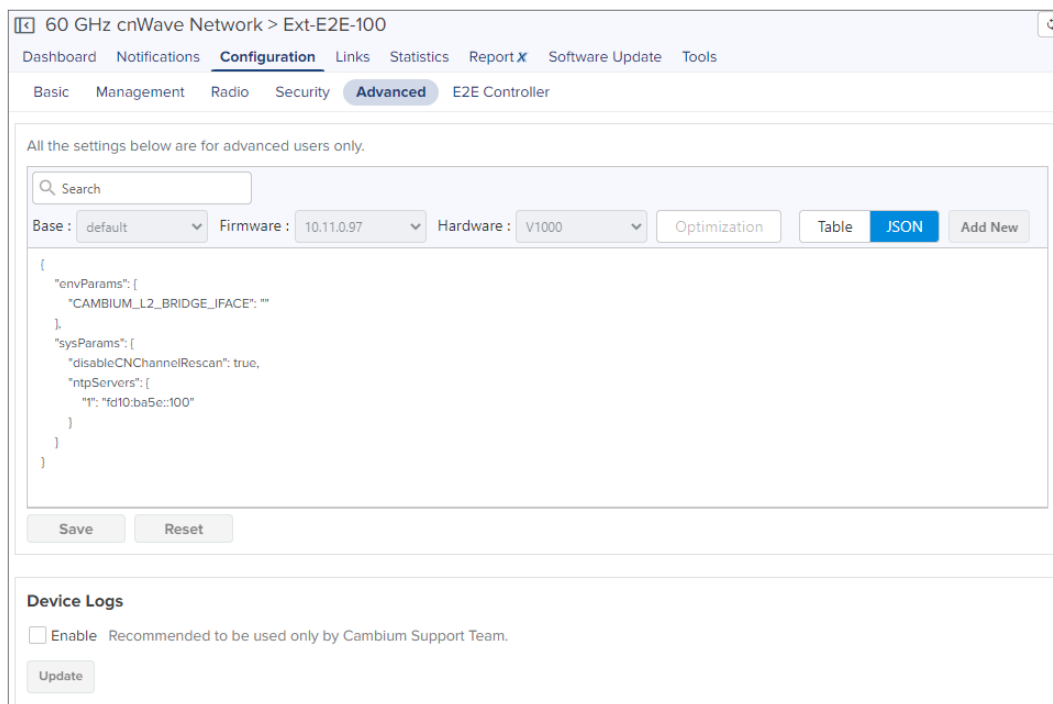


A dialog box titled "Add new field" with a close button (X) in the top right corner. It contains two input fields: "Field Name" and "Value". To the right of the "Field Name" input is a dropdown menu currently showing "String". At the bottom of the dialog are two buttons: "Save" (highlighted in blue) and "Cancel".

4. Click **Save**.

JSON

JSON allows Advanced user to download or view and edit in json format.



The screenshot shows the "60 GHz cnWave Network > Ext-E2E-100" configuration page. The top navigation bar includes "Dashboard", "Notifications", "Configuration" (active), "Links", "Statistics", "Report X", "Software Update", and "Tools". Below this is a sub-navigation bar with "Basic", "Management", "Radio", "Security", "Advanced" (active), and "E2E Controller". A message states: "All the settings below are for advanced users only." Below this is a search bar and a row of filters: "Base: default", "Firmware: 10.11.0.97", "Hardware: V1000", "Optimization", "Table", "JSON" (active), and "Add New". The main content area displays a JSON configuration file with the following structure:

```
{
  "envParams": {
    "CAMBIUM_L2_BRIDGE_IFACE": ""
  },
  "sysParams": {
    "disableCNChannelRescan": true,
    "ntpServers": [
      {
        "ip": "fd10:ba5e::100"
      }
    ]
  }
}
```

At the bottom of the JSON editor are "Save" and "Reset" buttons. Below the JSON editor is a "Device Logs" section with an "Enable" checkbox (unchecked) and a note: "Recommended to be used only by Cambium Support Team." An "Update" button is located below the checkbox.

To view or edit the JSON file:

1. Navigate to **Configuration > Advanced > JSON**.



Note

Enabling the Device Logs is supported only for External E2E Controller devices and it allows the Support team to view the logs.

2. Enable **Device Logs** and click **Update**.

E2E Controller

E2E Controller allows the advanced user to set the **Table** and download the **JSON** file.

Table

In **E2E Controller Table** user can edit or add **Field Name** and **Value**.

To Add Field:

1. Navigate to **Configuration > E2E Controller**.
2. Click **Add New**.

Field	Description	Status	Value
flags.airtime_alloc_update_interval	The minimum time interval at which the controller will recompute the airtime alloc...	unset	
flags.airtime_ul_dl_ratio	Percentage of uplink traffic to allow as a fraction of downlink traffic.	unset	
flags.app_router_port	The port controller listens on for apps.	unset	
flags.bstar_failover_missed_heartbeats	Number of missed heartbeats before declaring the other controller 'dead'.	unset	
flags.bstar_heartbeat_period_ms	Period for heartbeats between controllers, in milliseconds.	unset	
flags.bstar_peer_host	The hostname or IP address of the peer controller in the high availability configur...	unset	
flags.bstar_peer_ip	[DEPRECATED: use 'bstar_peer_host' instead] The IP address of the peer controller ...	unset	
flags.bstar_peer_pub_port	The publisher port on the peer controller in the high availability configuration.	unset	
flags.bstar_primary	The primary (true) or backup (false) controller in the high availability configuration.	unset	
flags.bstar_primary_recovery_heartbeats	If the backup is 'active' and the primary comes back online, the backup will yield t...	unset	

3. Enter the **Field Name** and **Value**.

4. Click **Save**.

JSON

JSON allows Advanced user to download or view and edit in JSON format. To view or edit the JSON file, navigate to **Configuration > E2E Controller > JSON**.

High Availability X

Using cnMaestro, you can enable and configure high availability (HA) support in a Multi-PoP Onboard E2E Controller that is running 60 GHz cnWave devices in a mesh network. This HA support configuration allows you to configure a primary (active mode) and a backup or secondary (passive mode) E2E Controller from cnMaestro.

If the active primary E2E Controller, with HA enabled and functioning, goes down, then the backup E2E Controller is active and manages the 60 GHz cnWave devices. All the devices report to the backup E2E Controller until the primary E2E Controller comes back.

This topic covers the following sections:

- [Theory of operation](#)
- [Configuring HA support](#)
- [Caveats of HA configuration](#)

Theory of operation

E2E Controllers use the high-availability protocol (primary-backup) and support the HA configuration. In such a primary-backup setup, two controllers (peers) run on separate PoP nodes and are designated as either primary or backup. If the primary controller catastrophically fails (for example, power outage, network failure, hardware failure), the backup controller assumes control of the cnWave 60 GHz network.

The HA configuration supports the following operational mechanisms for Onboard E2E Controller:

1. **Role designation:** At setup, one controller is statically designated as primary, and the other as backup. This designation determines their initial operational roles during network management.
2. **Initial state:** The primary controller starts in an active state, overseeing network configuration and collecting network statistics. The backup controller remains in a passive state, prepared to assume control if needed.
3. **Health monitoring:** Both primary and backup controllers monitor each other's status through regular heartbeat messages, sent every five seconds. These messages are crucial for detecting any disruptions or failures in the primary (active) controller.
4. **Data synchronization:** Both primary and backup controllers periodically synchronize topology and configuration data. This synchronization is key to enabling a fast and seamless transition from passive to active state, ensuring the backup controller can immediately manage the network with up-to-date settings and configurations.
5. **Failover process:** If the primary (active) controller fails, detected by a loss of heartbeat messages for 20 seconds, the backup controller automatically transitions from passive to active. This change ensures continuous network management without manual intervention.
6. **Recovery and Reversion:** After the failed primary controller is repaired and comes back online, it starts in a passive state. It remains in this passive state until it has successfully exchanged heartbeat messages for 150 seconds, ensuring stability. Following this period, a role reversal occurs where the primary controller transitions back to active and the backup controller reverts to passive.

Configuring HA support



Note

The HA support is applicable only to cnMaestro X accounts. Consider the following key points:

- The Onboard E2E Controller must be managed using cnMaestro.
- The Onboard network must have at least two PoP nodes to enable HA.
- The two PoP nodes are selected to host Primary. The backup controllers should be able to communicate over wire/ethernet.
- For HA, all the DN/CN nodes in network are expected to have a route to report to both the HA peers.
- The HA feature is supported in a network when devices are running 1.4 or above software version.

To enable the HA support for E2E Controller, complete the following steps:

1. From the Home page of cnMaestro, navigate to **Monitor and Manage > E2E Network > Configuration > High Availability X**.

The **Enable High Availability** checkbox appears.



2. To enable the HA support for E2E Controller, select the **Enable High Availability** checkbox.

The **High Availability X** page displays options to configure the backup Controller. By default, the current Onboard Controller is selected as the primary controller.

The screenshot shows the 'High Availability X' configuration page. The left sidebar lists various network components, with 'Onboard MultiPoP HA' selected. The main panel has tabs for 'Basic', 'Management', 'Radio', 'Security', 'Advanced', 'E2E Controller', and 'High Availability X'. Under 'High Availability X', there is a checkbox for 'Enable High Availability' which is checked. Below it, the 'Primary E2E Controller' is set to 'node-V5000-88384d'. The 'Backup E2E Controller*' is set to 'PoP2 V3K'. The 'Primary Controller IP address' is 'fd00:ba5e:010b:facb::0004:5688:38' and the 'Backup Controller IP address' is 'fd00:ba5e:010b:facb::0004:5688:34'. The 'HA Status' is 'Data in sync'. A 'Save' button is at the bottom.

- From the **Backup E2E Controller** dropdown list, select the required node that is connected to the complete network.

You can check the IP addresses (read only) of primary and backup controllers.

- Click **Save** to apply the changes.
- When you configure the HA support, ensure to check the **HA Status** parameter.

The **HA Status** parameter must display the green button, indicating that the HA support is functioning and data is in sync. If **HA Status** displays the red button, then it indicates that the HA support is not functioning.

You can also view the HA status in the **High Availability X** section on the **Dashboard** page.

The screenshot shows the 'Dashboard' page for the '60 GHz cnWave Network > Onboard MultiPoP HA'. The left sidebar has tabs for 'Dashboard', 'Notifications', 'Configuration', 'Links', 'Statistics', 'Reports X', 'Software Update', and 'Tools'. The 'E2E Controller Details' section shows: Version 1.4-dev21, Management Address 192.168.30.71, IPv6 Address fd00:ba5e:010b:facb::, IPv6 Gateway -, Sites 7, Nodes (PoP/DN/CN) 3 / 2 / 2, Deployment Running Onboard, Layer 2 Bridge Disabled, Country Other, Prefix Allocation Deterministic (fd00:ceed:8838:4d00::/56), Topology Sync Success (< 1m ago), and System Clock In Sync. The 'High Availability X' section shows: Primary node-V5000-88384d (Active), Backup PoP2 V3K, and Sync Status Data in sync. The right panel shows a map of the area with a green line connecting the primary and backup controllers. Below the map is a table of 'Top Links by MCS' and a section for 'Top Node(s)'.

NAME	DIRECTION	MCS	RSSI	SNR
link-Node_885c98-node-V5000-88384d	Node_885c98 to node-V5000-88384d	10	-62 dBm	12 dB
link-Node_88301a-node-V5000-88384d	Node_88301a to node-V5000-88384d	9	-46 dBm	27 dB
link-Node_885c98-node-V5000-88384d	node-V5000-88384d to Node_885c98	9	-58 dBm	16 dB
link-Node_88301a-node-V5000-88384d	node-V5000-88384d to Node_88301a	9	-46 dBm	26 dB
link-Node_883216-PoP2 V3K	Node_883216 to PoP2 V3K	9	-53 dBm	21 dB

The **Primary** field displays the primary node name. The **Backup** field displays the backup node name. Green bullets in **Primary** and **Backup** fields show the online/offline status of nodes. The keyword **Active** toggles between

Primary and **Backup** fields, indicating that the respective node is currently functioning as the active controller, managing the network and is connected to cnMaestro.

Caveats of HA configuration

Consider the following caveats of the HA configuration for cnWave 60 GHz devices:

Table 77 *Caveats of HA configuration*

Configuration	Caveats
Configuration backup and restoration	<ul style="list-style-type: none">• The configuration backups are supported when the HA is enabled.• The backup collected from a non-HA network can only be restored in a non-HA network.• The backup collected from a HA enabled network is restored only in a HA enabled network.• When HA is enabled, the restoration is allowed only when the primary node is active, managing the network and connected to cnMaestro.
Software update flow	<ul style="list-style-type: none">• When HA is enabled, it is recommended to update the nodes when primary is functioning as the active controller.• It is always recommended to run the HA Pairs in same version to avoid HA functionality issues.• Avoid downgrading the device version to less than 1.4 when HA is enabled in the network.• Avoid updating the device software from a device UI when HA is enabled. You must update the software from cnMaestro.
Device UI	<ul style="list-style-type: none">• It is always recommended to make changes in the network only from cnMaestro.• Making changes through device UIs may have issues in HA functionality.
cnMaestro X to Essentials downgrade	<ul style="list-style-type: none">• The HA functionality will be disabled leaving the current active controller that is connected to cnMaestro as the only controller in the network.• The HA functionality can be enabled back when the subscription is enabled.
Connecting a HA enabled E2E Controller network to an Essential cnMaestro account	<ul style="list-style-type: none">• The HA functionality will be disabled leaving the current active controller that is connected to cnMaestro as the only controller in the network.• The HA functionality can be enabled back when the network is connected to cnMaestro X account.

Links

Links provide the details about the link established between the nodes and also provides the option to create a new Wireless, Wired and Backup CN link.


- [List](#)
- [Statistics](#)

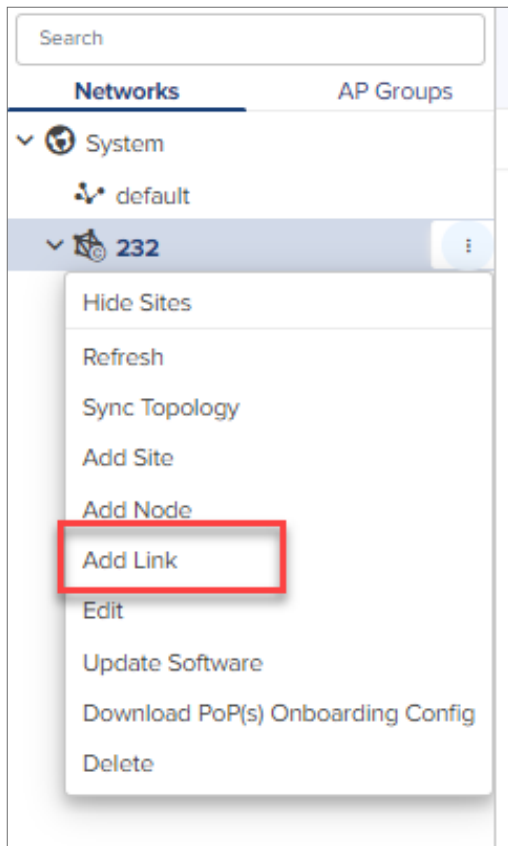
- [Events](#)

List

The **List** page provides details of **General**: Name, A-Node, Z-Node, A-Node MAC, Z-Node MAC, Alive, Link Time, Type, Ignition Attempts, Distance, Azimuth, Backup CN Link, and Ignition Status for each link of all the devices in the E2E Network in a page format.

To add a link, perform the following steps:

1. Navigate to the E2E Network tree menu click () icon and click **Add Link** from the dropdown or navigate to **Network > Links > List > Add New**.



2. **Add Link** window pops-up.
3. Select **Link Type** Wireless or Wired.

Figure 351 *Wireless link*

×

Add Link

Link Type

☒ Wireless
 ☐ Wired

A-Node

CN-0463

A-Node Sector

Sector 1 (12:04:56:8B:04:63)

Z-Node

DN-3183

Z-Node Sector

Sector 1 (12:04:56:88:31:83)

☐ Backup CN Link ⓘ

☐ Disable Ignition

Name

link CN-0463-DN-3183

Save

Cancel



Note

In Wired Link Type, add Sector is disabled.

Figure 352 *Wired link*

×

Add Link

Link Type

☐ Wireless
 ☒ Wired

A-Node

CN-0463

A-Node Sector

Z-Node

DN-3183

Z-Node Sector

☐ Backup CN Link ⓘ

Name

link CN-0463-DN-3183

Save

Cancel

⚠ Link created for Map visualization only. Relay port in the configuration should be enabled separately.

4. Select the **Node** from the dropdown in **A-Node**.

Add Link

Link Type
☒ Wireless ☐ Wired

A-Node
 Search
 CN-fa-cloud
 D4
 DN-D6
 PoP-Onboard-V5k-3083

A-Node Sector
 Z-Node Sector

Save Cancel

Map showing locations: New Delhi, Jaipur, Agra, Gwalior, Kanpur, Varanasi, Nepal, Kathmandu, Patna.

5. Select the **Sector** of the node from the dropdown in **A-Node Sector**.

Add Link

Link Type
☒ Wireless ☐ Wired

A-Node
 CN-0463

A-Node Sector
 Sector 1 (12:04:56:8B:04:63)

Z-Node
 DN-3183

☐ Backup CN Link ⓘ
☐ Disable Ignition

Name
 link-CN-0463-DN-3183

Save Cancel

Map showing location: New Horizon Gurukul.

6. Select the **Node** from the dropdown in **Z-Node**.

Add Link [X]

Link Type
☒ Wireless ☐ Wired

A-Node
 CN-fa-cloud

A-Node Sector
 Sector 1 (12:04:56:8B:00:FA)

Z-Node

Z-Node Sector

D4
 DN-D6
 PoP-Onboard-V5k-3083

7. Select the **Sector** of the node from the dropdown in **Z-Node Sector**.

Add Link [X]

Link Type
☒ Wireless ☐ Wired

A-Node
 CN 0463

A-Node Sector
 Sector 1 (12:04:56:8B:04:63)

Z-Node
 DN 3183

Z-Node Sector
 Sector 1 (12:04:56:8B:31:83)

☐ Backup CN Link ⓘ

☐ Disable Ignition

Name
 link: CN 0463-DN 3183

8. Enable the **Backup CN Link**.

- If the link between PoP or DN and CN gets disconnected. This Backup CN link provides the backup connectivity from DN or PoP to particular CN.

Add Link

Link Type
☒ Wireless ☐ Wired

A-Node
 CN-0463

A-Node Sector
 Sector 1 (12:04:56:88:04:63)

Z-Node
 DN-3183

Z-Node Sector
 Sector 1 (12:04:56:88:31:83)

☒ Backup CN Link ⓘ
☐ Disable Ignition

Name
 link: CN-0463-DN-3183

Save **Cancel**

Map showing node locations and link path.

9. If user selects **Disable Ignition** option, wireless link creates with disable ignition. User need to manual select **Enable Ignition** from link options.
10. Click **Save**.
11. Once the link is successful it displays the **Alive** status as **Yes**.

60 GHz cnWave Network > Onboard-Multi-PoP Raja

Dashboard Notifications Configuration **Links** Statistics Reports X Software Update Tools

List Statistics Events

Apply Filter(s)

Name	A-Node	Z-Node	A-Node MAC	Z-Node MAC	Alive	
link-CN@0d53-DN1@3000	CN@0d53	DN1@3000	12:04:56:88:0D:53	12:04:56:88:30:00	Yes	
link-DN-POP3-V2K-Wired@045673d00d-PoP2@3a5b	DN-POP3-V2K-Wired@045673d00d	PoP2@3a5b	12:04:56:73:D0:0D	12:04:56:88:3A:5B	Yes	
link-DN-POP3-V2K-Wired@045673d00d-PoP3@88aec8	DN-POP3-V2K-Wired@045673d00d	PoP3@88aec8	-	-	Yes	
link-DN-PoP2@4864-DN1@3000	DN-PoP2@4864	DN1@3000	-	-	Yes	2d 10h 58m
link-DN-PoP2@4864-PoP2@3a5b	DN-PoP2@4864	PoP2@3a5b	12:04:56:88:48:64	12:04:56:88:3A:5B	Yes	0d 11h 9m
link-DN1@3000-DN3@300c	DN1@3000	DN3@300c	12:04:56:88:30:00	22:04:56:88:30:0C	Yes	0d 11h 26m
link-DN1@3000-PoP1-onboard-309d	DN1@3000	PoP1-onboard-309d	22:04:56:88:30:00	12:04:56:88:30:9D	Yes	2d 10h 58m
link-DN2@3009-DN3@300c	DN2@3009	DN3@300c	22:04:56:88:30:09	12:04:56:88:30:0C	Yes	0d 11h 26m
link-DN2@3009-PoP1-onboard-309d	DN2@3009	PoP1-onboard-309d	12:04:56:88:30:09	22:04:56:88:30:9D	Yes	2d 10h 58m
link-PoP1-onboard-309d-V3K-CN@30f7	PoP1-onboard-309d	V3K-CN@30f7	22:04:56:88:30:9D	12:04:56:88:30:F7	Yes	2d 10h 58m

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

Available link options are:

- Send Assoc
- Send Dissoc
- Enable Ignition
- Disable Ignition
- Clear Fast Acquisition Beams

Delete Links

In the **Links** tab you can delete the E2E Controller Network Links.

To delete the links:

1. Navigate to **Links > List**.
2. In the **List** table select one or more links to delete. User can also delete individual link, by selecting delete (🗑️) icon in the table.

Name	A-Node	Z-Node	A-Node MAC	Z-Node MAC	Alive	Link Time
<input checked="" type="checkbox"/> link-CN-1-DN-AADD	CN-1	DN-AADD	12:04:56:88:30:1A	12:04:56:CC:AA:DD	Yes	2d 23h 57m
<input checked="" type="checkbox"/> link-DN-AADD-PoP	DN-AADD	PoP	22:04:56:CC:AA:DD	12:04:56:88:38:4D	Yes	2d 23h 58m
<input type="checkbox"/> link-PoP-cn-1k	PoP	cn-1k	22:04:56:88:38:4D	12:04:56:8B:03:49	Yes	2d 23h 55m
<input type="checkbox"/> link-PoP-v2k-new	PoP	v2k-new	12:04:56:88:38:4D	42:CB:C7:73:D0:00	Yes	2d 23h 28m

1. Click **Delete**.

Import List

In **Links** tab you can import the E2E Controller Network Links.

To import the links:

1. Navigate to **Links > List**.
2. Select **Import**.

Name	A-Node	Z-Node	A-Node MAC	Z-Node MAC	Alive	Link Time
<input checked="" type="checkbox"/> link-CN-fa-cloud-D4	CN-fa-cloud	D4	12:04:56:8B:00:FA	22:04:56:88:38:D4	Yes	0d 12h 42m
<input type="checkbox"/> link-D4-PoP-Onboard-V5k-3083	D4	PoP-Onboard-V5k-3083	12:04:56:88:38:D4	22:04:56:88:30:83	Yes	42d 16h 53m
<input type="checkbox"/> link-DN-D6-PoP-Onboard-V5k-3083	DN-D6	PoP-Onboard-V5k-3083	12:04:56:88:30:D6	12:04:56:88:30:83	Yes	42d 16h 53m

3. **Import Links** pops-up.

Import Links

Upload a file (csv) as per the format specified in the template.

File [Select File](#) [Download Template](#)

4. Click **Download Template** to download the sample template in .CSV format.

	A	B	C	D	E
1	A_NODE_NAME	A_NODE_MAC	Z_NODE_NAME	Z_NODE_MAC	LINK_TYPE
2	A node name of the device	Sector 1/2 MAC Address	Z node name of the device	Sector 1/2 MAC Address	Wireless or Wired
3	POP	12:04:56:88:38:4D	DN1	22:04:56:88:38:4D	wireless
4	DN1	12:04:56:88:38:4D	CN1	22:04:56:88:38:4D	wireless
5	DN1		CN2		wired
6					
7					

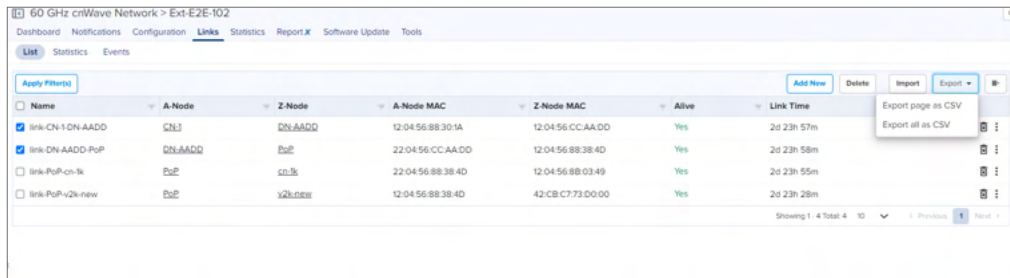
5. Select the file and click **Import**.

Export List

In **Links** tab you can export the E2E Controller Network Links.

To export the links:

1. Navigate to **Links > List > select Export.**



2. Data is exported in the CSV file format as shown below.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
LINK_NAME	A_NODE	I_A_NODE_I_Z	Node_I_Z	Node_I_Z_Link_Type	Alive	Ignition	Distance	Azimuth	Backup	C	Ignition	Timestamp		
Link Name	A node nai	Sector 1/2	Z node nai	Sector 1/2	Wireless o	Yes/No	Ignition At	Distance b	Azimuth (C	Yes/No	Enabled/D	Timestamp		
link-CN-fa-cloud-D4	CN-fa-clou	12:04:56:8	D4	22:04:56:8	Wireless	Yes	16	996	54.9	No	Enabled	2021-07-23T02:49:06.317Z		
link-D4-PoP-Onboard-V5k-3083	D4	12:04:56:8	PoP-Onbo	22:04:56:8	Wireless	Yes	0	988	158.8	No	Enabled	2021-07-23T02:49:06.317Z		
link-DN-D6-PoP-Onboard-V5k-3083	DN-D6	12:04:56:8	PoP-Onbo	12:04:56:8	Wireless	Yes	0	979	105.2	No	Enabled	2021-07-23T02:49:06.317Z		

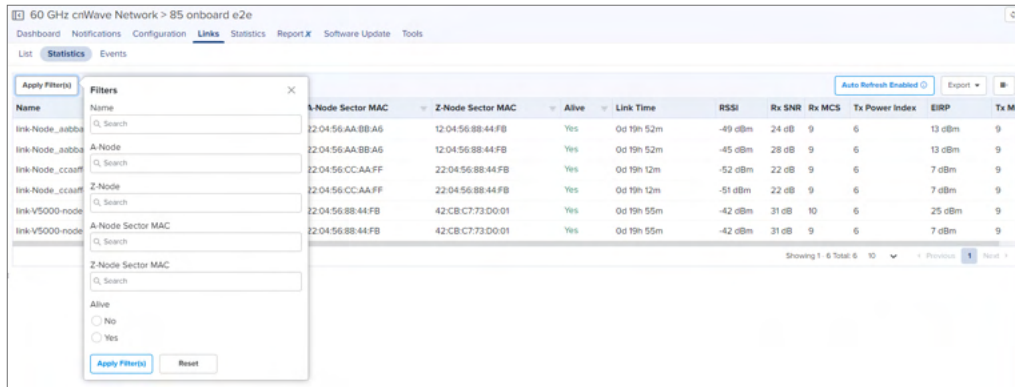
Statistics

Statistics pages provides details of **Basic**: Name, Direction, A-Node, Z-Node, Alive, Link Time, Type, Distance, Azimuth, Rx Golay, Tx Golay **Detailed Statistics**: A-Node Sector MAC, Z-Node Sector MAC, RSSI, Rx Airtime%, Rx Beam Azimuth Angle, Rx Beam Elevation Angle, Rx SNR, Rx MCS, Rx PER, Rx Scan Beams, Rx Throughput, Tx Airtime%, Tx Beam Azimuth Angle, Tx Beam Elevation Angle, Tx Power Index, EIRP, Tx MCS, Tx PER, Tx Scan Beams, Rx Errors, Rx Frames, Tx Errors, Tx Frames, Tx Throughput, and Link Fade Margin each link of all the devices in the E2E Network in a page format.

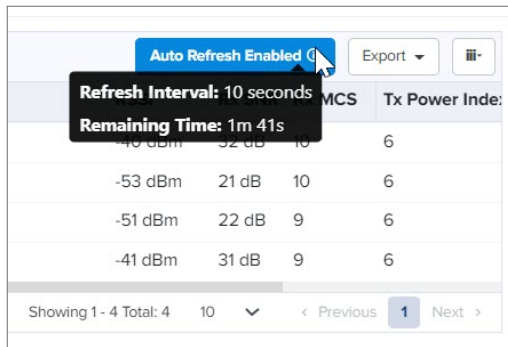
Name	Direction	A-Node Sector MAC	Z-Node Sector MAC	Alive	Link Time	RSSI	Rx SNR	Rx MCS	Tx Power Index	EIRP	Tx MCS
link-CN-1-DN-AADD	CN-1 to DN-AADD	12:04:56:88:30:1A	12:04:56:CC:AA:DD	Yes	3d 0h 6m	-38 dBm	32 dB	10	6	35 dBm	9
link-CN-1-DN-AADD	DN-AADD to CN-1	12:04:56:88:30:1A	12:04:56:CC:AA:DD	Yes	3d 0h 6m	-37 dBm	32 dB	10	6	13 dBm	9
link-DN-AADD-PoP	DN-AADD to PoP	22:04:56:CC:AA:DD	12:04:56:88:38:4D	Yes	3d 0h 7m	-40 dBm	32 dB	10	6	13 dBm	10
link-DN-AADD-PoP	PoP to DN-AADD	22:04:56:CC:AA:DD	12:04:56:88:38:4D	Yes	3d 0h 7m	-42 dBm	31 dB	10	6	13 dBm	10
link-PoP-cn-1k	PoP to cn-1k	22:04:56:88:38:4D	12:04:56:88:03:49	Yes	3d 0h 4m	-39 dBm	32 dB	9	6	13 dBm	9
link-PoP-cn-1k	cn-1k to PoP	22:04:56:88:38:4D	12:04:56:88:03:49	Yes	3d 0h 4m	-41 dBm	31 dB	10	6	13 dBm	9
link-PoP-v2k-new	PoP to v2k-new	12:04:56:88:38:4D	42:CB:C7:73:D0:00	Yes	2d 23h 37m	-48 dBm	25 dB	9	6	13 dBm	9
link-PoP-v2k-new	v2k-new to PoP	12:04:56:88:38:4D	42:CB:C7:73:D0:00	Yes	2d 23h 37m	-52 dBm	22 dB	10	6	13 dBm	9

You can **Apply Filter(s)** for Name, A-Node, Z-Node, A-Node Sector MAC, Z-Node Sector MAC, and Alive. The **Auto Refresh** option allows to refresh data automatically as per Refresh Interval, which is configured for five minutes. By default, Refresh Interval is 10 seconds. This option gets disabled after five minutes. Then you must click **Enable Auto Refresh** and specify the refresh intervals to enable this option. To **Enable Auto Refresh**, perform the following steps:

1. Click **Enable Auto Refresh**.
2. Select **Refresh Interval** from the dropdown.
 - 10 seconds
 - 30 seconds
 - 60 seconds
3. Click **Start** to start **Auto Refresh**.



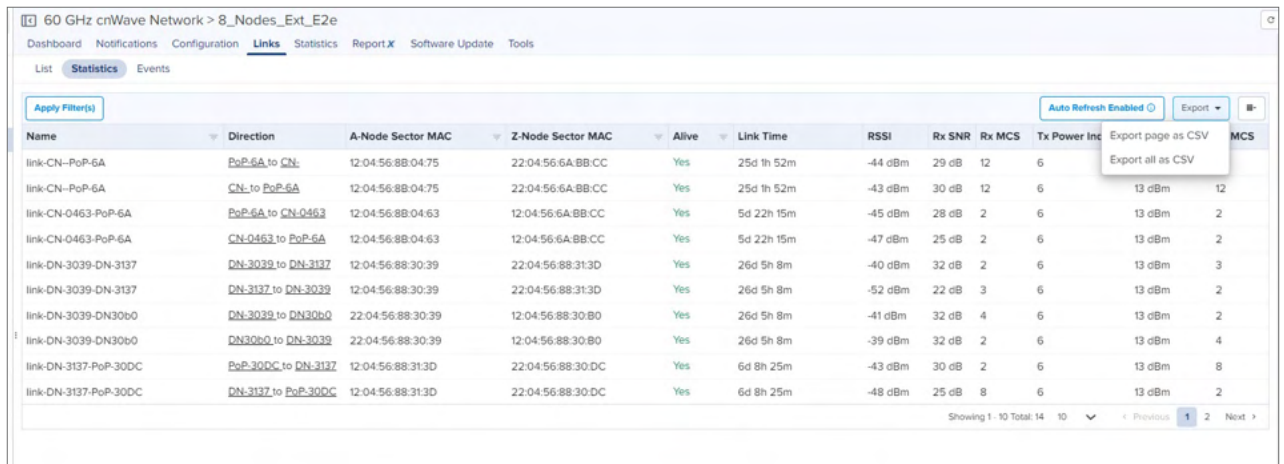
4. Click the info icon to view **Refresh Interval** and **Remaining Time**.



Export Statistics

To export the Statistics:

1. Navigate to **Links > Statistics** > select **Export**.



2. It exports .csv file format as shown below.

LINK NAME	DIRECTION	A_NODE_ID	Z_NODE_A	Z_NODE_B	ALIVE	TYPE	DISTANCE	AZIMUTH	RSSI	Rx_SNR	Rx_MCS	Rx_Pwr	Rx_Beam	Tx_PowerIndex	EIRP	Tx_MCS	Tx_Pwr	Tx_Beam	Rx_ErrorRate	Rx_PacketRate
link-APOP-DN-30	APOP to DN-30	APOP	DN-30	22:04:56:81:22:04:56:81	Yes	Wireless	147	83	-51	22	9	0.17	84	6	13	10	0.19	84	290	200%
link-APOP-DN-30	DN-30 to APOP	DN-30	APOP	22:04:56:81:22:04:56:81	Yes	Wireless	147	83	-51	22	9	0.2	84	6	13	9	0.21	84	374	148%
link-APOP-DN-80	APOP to DN-80	APOP	DN-80	22:04:56:81:22:04:56:81	Yes	Wireless	94	178.1	-40	32	9	0	32	6	13	9	0	35	92	300%
link-APOP-DN-80	DN-80 to APOP	DN-80	APOP	22:04:56:81:22:04:56:81	Yes	Wireless	94	178.1	-37	32	10	0	6	13	10	0	0	1332	918%	
link-CN-75-DN-80	DN-80 to CN-75	CN-75	DN-80	22:04:56:81:22:04:56:81	Yes	Wireless	171	151.2	-48	25	9	0.31	0	23	30	9	0.38	0	0	0
link-CN-75-DN-80	CN-75 to DN-80	CN-75	DN-80	22:04:56:81:22:04:56:81	Yes	Wireless	171	151.2	-41	12	8	0.42	0	6	13	9	0.35	0	1044	4432%
link-CN-83-DN-80	DN-80 to CN-83	CN-83	DN-80	22:04:56:81:22:04:56:81	Yes	Wireless	71	52.7	-53	21	9	0.81	58	6	35	9	0.06	58	385	204%
link-CN-83-DN-80	CN-83 to DN-80	CN-83	DN-80	22:04:56:81:22:04:56:81	Yes	Wireless	71	52.7	-49	23	9	0.04	112	6	13	9	0.08	112	0	339
link-CN-80463-DN-39	DN-39 to CN-80463	CN-80463	DN-39	22:04:56:81:22:04:56:81	Yes	Wireless	159	-45.2	-40	12	9	0	44	31	17	5	0.01	44	75	285%
link-CN-80463-DN-39	CN-80463 to DN-39	CN-80463	DN-39	22:04:56:81:22:04:56:81	Yes	Wireless	159	-45.2	-48	25	9	0.04	45	6	13	9	0.16	45	54	62
link-CN-39-DN-30	DN-30 to CN-39	CN-39	DN-30	22:04:56:81:22:04:56:81	Yes	Wireless	155	20.5	-40	12	9	0	15	6	13	9	0	24	23	50%
link-CN-39-DN-30	CN-39 to DN-30	CN-39	DN-30	22:04:56:81:22:04:56:81	Yes	Wireless	155	20.5	-43	30	9	0	0	6	13	10	0	0	164	232
link-CN-39-DN-80	DN-80 to CN-39	CN-39	DN-80	22:04:56:81:22:04:56:81	Yes	Wireless	100	-70.5	-45	28	9	0.06	35	6	13	9	0.02	34	73	56%
link-CN-39-DN-80	CN-39 to DN-80	CN-39	DN-80	22:04:56:81:22:04:56:81	Yes	Wireless	100	-70.5	-48	25	9	0.3	35	6	13	10	0.01	54	331	30%

Events

Events provide the details of link availability, hourly link availability in percentage, link availability in different time lines, and distance of the link.

Figure 353 *Links > Events*

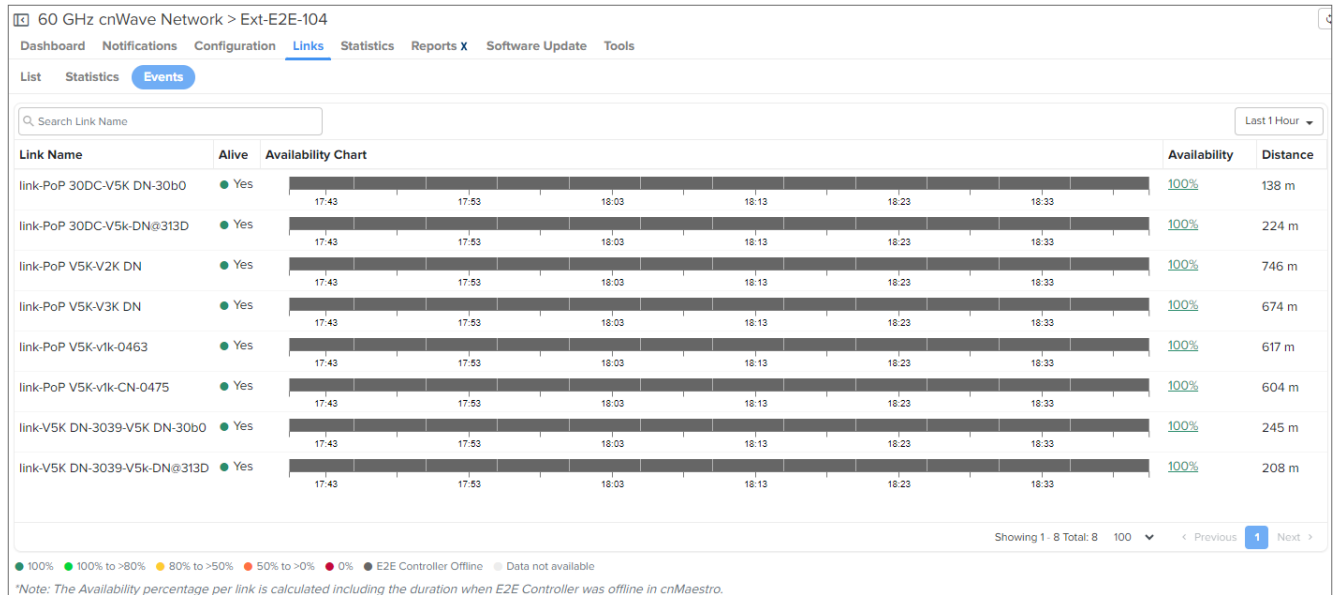


Table 78 *Events fields*

Field	Description
Link Name	Name of the link.
Alive	Status of the link (Yes or No).
Availability Chart	<p>Displays the link availability based on time range selected from the dropdown. When you hover the mouse on the Availability Chart, the link availability is shown as described:</p> <ul style="list-style-type: none"> If you select time range as Last 1 Hour, then link availability for every 5 minutes is displayed. If you select time range other than Last 1 Hour, then link availability for every 1 hour is displayed. <p>Hover on the link to see the hourly availability as shown in Figure 355.</p> <p>Clicking on percentage link availability displays pop-up window as shown in Figure 356</p> <p>Link availability is presented in different colors in the chart as shown in Figure 354</p>
Availability Percentage	Availability of link is shown in percentage in the Availability column as shown in Figure 355 .
Distance	Distance of the link in meters.

Figure 354 *Link Availability in Percentage*



link-DN-3183-PoP-6A - Availability (Last 7 Days)

Status	From	To	Duration
Online	Apr 06 2022 17:30:00	Apr 06 2022 17:56:20	26m 20s
Offline	Apr 06 2022 17:56:20	Apr 06 2022 17:56:24	< 1m
Online	Apr 06 2022 17:56:24	Apr 07 2022 13:50:27	19h 54m 3s
Offline	Apr 07 2022 13:50:27	Apr 07 2022 13:59:24	8m 56s
Online	Apr 07 2022 13:59:24	Apr 07 2022 15:11:30	1h 12m 5s
Offline	Apr 07 2022 15:11:30	Apr 07 2022 15:11:33	< 1m
Online	Apr 07 2022 15:11:33	Apr 07 2022 15:19:51	8m 17s
Offline	Apr 07 2022 15:19:51	Apr 07 2022 15:20:33	< 1m
Online	Apr 07 2022 15:20:33	Apr 07 2022 15:20:38	< 1m
Offline	Apr 07 2022 15:20:38	Apr 07 2022 15:20:55	< 1m
Online	Apr 07 2022 15:20:55	Apr 07 2022 15:21:41	< 1m
Offline	Apr 07 2022 15:21:41	Apr 07 2022 15:21:55	< 1m
Online	Apr 07 2022 15:21:55	Apr 07 2022 15:22:16	< 1m
Offline	Apr 07 2022 15:22:16	Apr 07 2022 15:22:30	< 1m
Online	Apr 07 2022 15:22:30	Apr 07 2022 15:28:41	6m 10s
Offline	Apr 07 2022 15:28:41	Apr 07 2022 15:30:31	1m 49s
Online	Apr 07 2022 15:30:31	Apr 07 2022 15:30:35	< 1m
Offline	Apr 07 2022 15:30:35	Apr 07 2022 15:30:41	< 1m
Online	Apr 07 2022 15:30:41	Apr 07 2022 15:30:45	< 1m
Offline	Apr 07 2022 15:30:45	Apr 07 2022 15:30:45	< 1m
Online	Apr 07 2022 15:30:45	Apr 07 2022 18:24:19	2h 53m 34s
Offline	Apr 07 2022 18:24:19	Apr 07 2022 18:24:25	< 1m
Offline	Apr 08 2022 19:17:51	Apr 08 2022 19:17:55	< 1m
Online	Apr 08 2022 19:17:55	Apr 11 2022 18:50:05	2d 23h 32m 9s
Offline	Apr 11 2022 18:50:05	Apr 11 2022 18:50:11	< 1m
Online	Apr 11 2022 18:50:11	Apr 12 2022 18:19:00	23h 28m 48s
Offline	Apr 12 2022 18:19:00	Apr 12 2022 18:19:06	< 1m
Online	Apr 12 2022 18:19:06	Apr 12 2022 20:22:46	2h 3m 39s
Offline	Apr 12 2022 20:22:46	Apr 12 2022 20:22:51	< 1m
Online	Apr 12 2022 20:22:51	Apr 13 2022 18:30:00	22h 7m 8s

Showing 1 - 25 Total 25

Availability percentage per link is calculated including the duration when E2E Controller was Offline in cnMaestro.

Figure 355 Link Availability

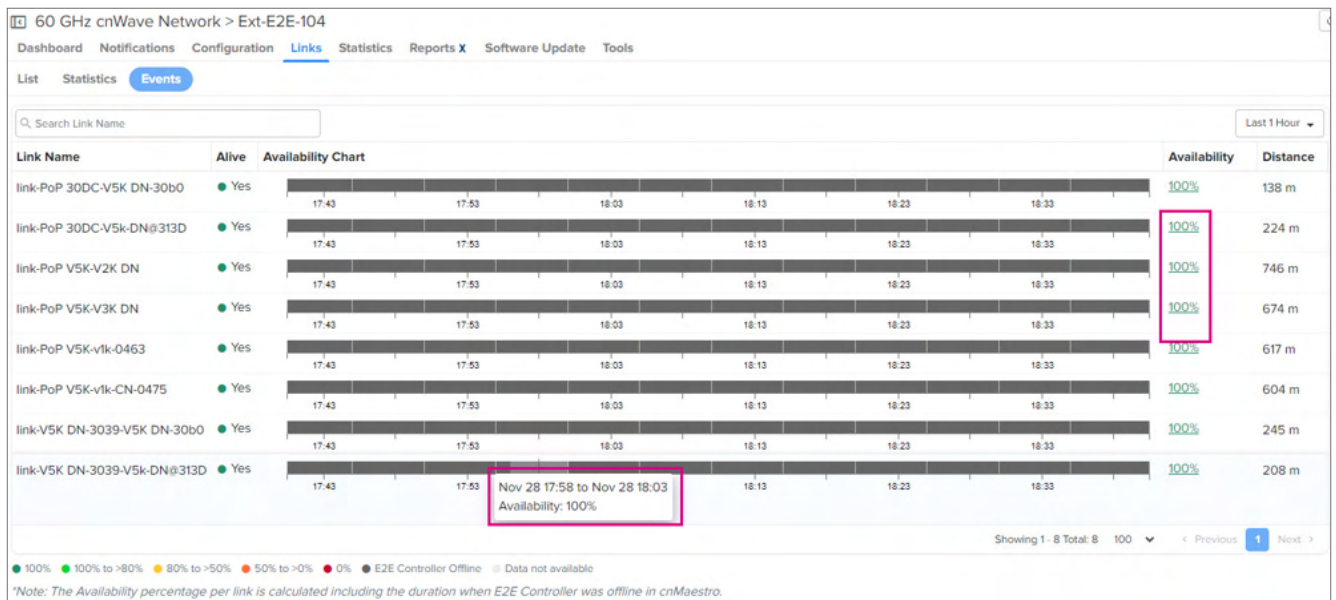


Figure 356 Link Status

link-V1K DN-V2K POP

Apr 23 14:30 to Apr 23 15:30

Availability: 100%
Online: 58m 5s
E2E Controller Offline: 1m 8s

Event	Time	Reason
Offline	Apr 23 2025 15:21:21	Unknown
E2E Controller Offline	Apr 23 2025 15:21:21	-
Online	Apr 23 2025 15:22:30	-

Showing 1 - 3 Total 3

Events details are available for Last 1 hour, Last 6 hours, Last 12 hours, Last 24 Hours, Last 2 days, Last 4 days, and Last 7 days.



Note

Event details for **Custom Range** and **Last 30 days** is available only for cnMaestro X users.

Statistics

The E2E Network provides the following statistics:

- [Nodes](#)
- [BGP](#)

Statistics

Nodes provide a tabular aggregation of data, including General information on the nodes monitored, as well as Wireless, Network, and Traffic metrics. Node Statistics pages provide details of **General**: Device, Serial Number, IPv6 Address, MAC, Mode, Model, Status, Status Time, Site, Zone, PoP Node, Software Version. **GPS**: Sync Mode, Fix Type, Satellites Tracked, Latitude, Longitude, Height. **Network**: Radios, Main Aux SFP, Sector Throughput (Tx), Sector Throughput (Rx), Ethernet Throughput (Tx), and Ethernet Throughput (Rx) each device in E2E Network, generally in a page format.

Figure 357 Nodes Statistics

60 GHz cnWave Network > Ext-E2E-101

Dashboard Notifications Configuration Links **Statistics** Reports x Software Update Tools

Nodes BGP

Apply Filter(s) Auto Refresh Enabled ⓘ

Device	MAC	IPv6 Address	Mode	Model	Status	Status Time	Site	Radios
PoP_V3K	(b) (6)	(f) (b) (6)	DN	V3000	Online	4d 23h 47m	PoP site	📶 ⓘ
V1k	(b) (6)	(f) (b) (6)	CN	V1000	Online	3d 9h 19m	Site_8b00fa	📶 ⓘ
V1K_8b00d6	(b) (6)	(f) (b) (6)	DN	V1000	Online	3d 9h 19m	Site_8b00d6	📶 ⓘ
V5K_DN	(b) (6)	(f) (b) (6)	DN	V5000	Online	3d 9h 20m	Site_8838d4	📶 📶 ⓘ
V5K_883083	(b) (6)	(f) (b) (6)	DN	V5000	Online	3d 10h 10m	DN_Site_V5K	📶 📶 ⓘ

Showing 1 - 5 Total: 5 10 < Previous 1 Next >

BGP

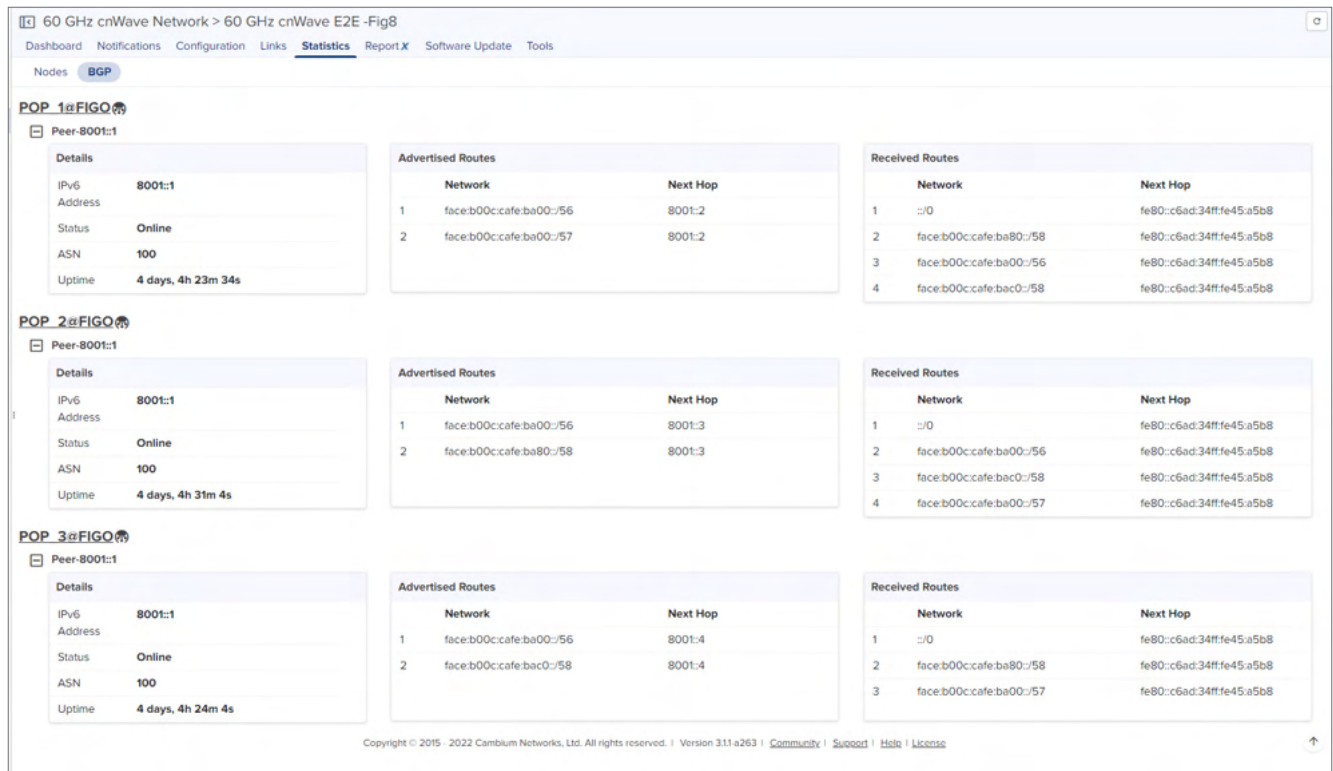


Note

BGP statistics displays only if BGP option is enabled in Routing in PoP configuration.

BGP provides the details of **Advertised Routes**, **Received Routes**, and **Peer** details.

Figure 358 BGP Statistics



A new **Link Fade Margin (LFM)** statistics has been added to the displayed **Link Statistics** tab in 60 GHz cnWave 1.2.2 software version release. This statistic is shown in units of dB, and it is meant to provide operators with a quick way to assess any additional **system gain** a RF link has available in order to help ride out potential RF link fades due to weather (most typical) or other temporary RF link impairments. The rough calculation for LFM is comprised of the RSSI received from a remote transmitter and assessing how much more TX power is available (from the remote transmitter) and how far away the RSSI value is from an established receiver sensitivity floor of -72 dBm. The LFM allows operators quickly assess if/where you may have some marginal RF links that need to be addressed in some way. Typical options would be changing an existing node out for a V3K (to get more margin) or possibly dropping in an intermediate DN node such that their RF paths are shorter, typically resulting in a much larger LFM.

Figure 359 Link Fade Margin



Software Update

The **Software Update** tab allows to update with the latest device software.

To update the software:

1. Select the **Network** and navigate to the **Software Update** tab.
2. In **Software Update** tab select the desired Versions from dropdown in **Versions** tab.
3. Select the **Device**.
4. In **Job Options**, do the following:

- Select **Batch Size**
- Enter **Upgrade Timeout**.
- Enter **Download Retry Limit**.
- Enter **Download Timeout**.
- Select the Download Protocol as **HTTPS** or **Torrent**.
- Enable the **Skip Failures** or **Skip PoP Failures**.

5. Click **Add Software Job to device**.

60 GHz cnWave Network > 7-Nodes-External-Smartwork

Dashboard Notifications Configuration Links Statistics Report X **Software Update** Tools

Versions: 1.2-dev59 (Recommended) (Beta) [Add New](#)

Search

Devices	Model	Mode	Status	Active
sdf	V5000	DN	Offline	
v1%CN-0463	V1000	CN	Offline	11-alpha2
v1%CN-0475	V1000	CN	Online	1.2-dev59
v2%CN-3183	V3000	CN	Online	1.2-dev59
v5%CN-3080	V5000	DN	Online	1.2-dev59
v5%CN-3130	V5000	DN	Online	1.2-dev59
v5%CN-3039	V5000	DN	Online	1.2-dev34
v5%PoP-300C	V5000	DN	Online	1.2-dev59

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

Update
☒ Now ☐ Schedule

Job Options

Batch Size
☒ Unlimited
☐ No Size Limit
☐ Limited

Upgrade Timeout
 The per-batch timeout for the upgrade operation (in seconds)

Download Retry Limit
 The maximum retry attempts for each node

Download Timeout
 The timeout for downloading the image (in seconds)

Download Protocol
☒ HTTPS
☐ Torrent

☒ Skip Failures
☒ Skip PoP Failures

Notes

[Add Software Job to 0 device\(s\)](#) [View Update Jobs](#)



Note

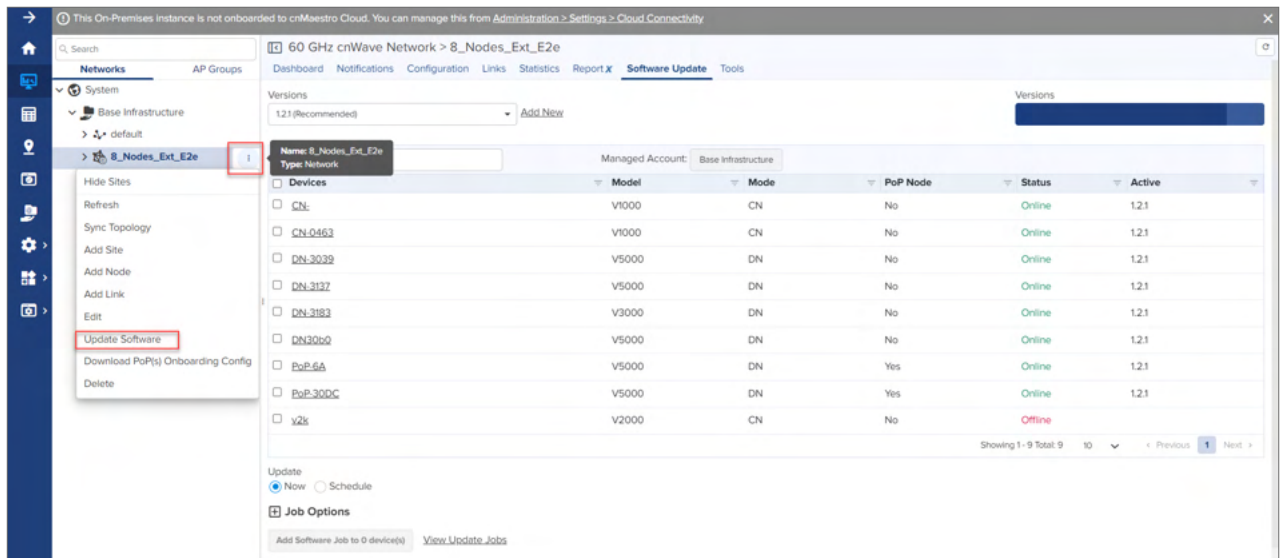
Onboard E2E controller will support only one synced image. If user needs to sync another image, select the image from **Versions** drop down and click **Sync Selected Image**.

The Software Update is performed on the devices managed by External E2E Controller and Onboard E2E Controller as follows:

External E2E Controller

1. In the **Networks**, select External E2E Controller and check the Software Version.
2. From External E2E Controller menu options, select **Update Software**.

Software Update page appears.



3. In **Versions** dropdown select the version and the devices in the network for software upgrade.

Device software update version check for External E2E Controller is described in [Table 79](#).

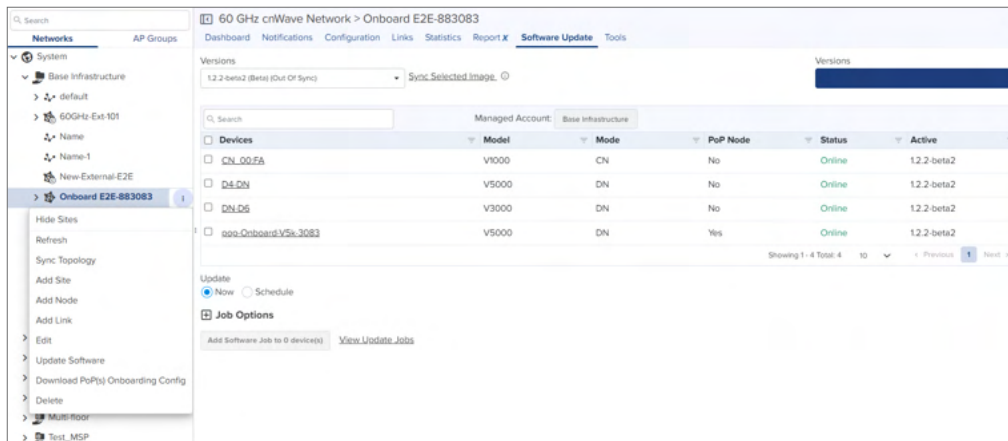
Table 79 Device Software Update: External E2E Controller

Version	Example
If Software Version of the device is less than the Software Version of the External E2E Controller then Software Upgrade is successful.	External E2E Controller software version: 1.2.1 When Device Software Version is selected as 1.2.1 or lower then Device Software is upgraded successfully.
If Software Version of the Device is selected higher than the External E2E Controller version then Software Upgrade fails.	E2E External Controller Software Version :1.2.1 When Device Software Version is selected as 1.2.2 or higher then Device Software upgrade fails. Error message: Device version should not be higher than External E2E Controller version 1.2.1

Onboard E2E Controller

1. In the **Networks**, select Onboard E2E Network and check the software version.
2. From Onboard E2E Network menu options, select **Update Software**.

Software Update page appears.



Device software update version check for Onboard E2E Controller is described in [Table 80](#).

Table 80 Device Software Upgrade: Onboard E2E Controller

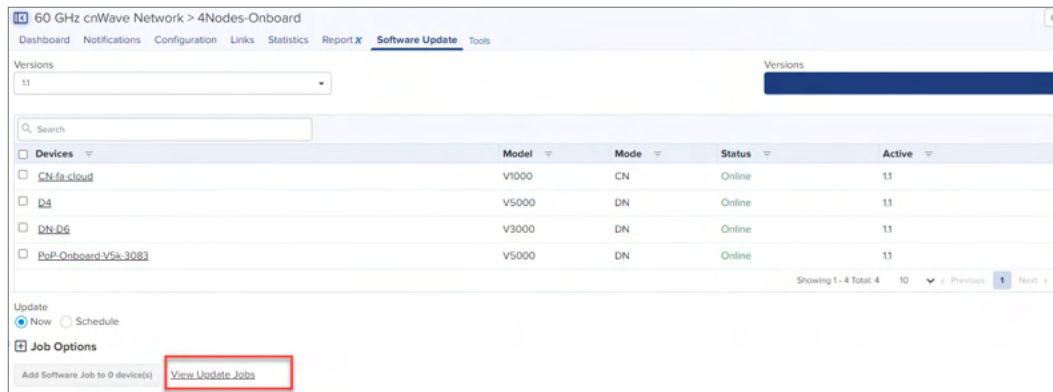
Software Upgrade	Example
If software version of Onboard PoP device is lower and upgraded to higher version then Software Upgrade is successful.	If the Onboard PoP device is running with 1.2, and selected software version is 1.2.1 or higher then Onboard PoP device is upgraded successfully.
If software version of all devices including Onboard PoP are lower and upgraded to higher version then Software Upgrade is successful.	If all the devices including the Onboard PoP are running with 1.2, and selected software version is 1.2.1 or higher then all the devices including PoP device are upgraded successfully.
If software version of all devices are higher and downgraded to lower version except Onboard PoP then Software Upgrade are successful.	If all the devices are running with 1.2.2, and selected software version is 1.2 then all the devices except PoP device are upgraded successfully.
If software version of all devices including PoP are higher and downgraded to lower version then Software Upgrade are successful.	If all the devices including PoP are running with 1.2.2, and selected software version is 1.2 then all the devices are upgraded successfully.
If software version of all devices including Onboard PoP are higher and downgraded to lower version then Software Upgrade should fail if one or more nodes running with higher version in list.	If all the devices including the Onboard PoP are running with 1.2.2, and selected software version is 1.2.1 then Software Upgrade should fail.
If software version of Onboard PoP device is higher and upgraded to lower version then Software Upgrade for PoP fails, only when other devices software version are higher.	If the Onboard PoP device is running with 1.2.2, and selected software version is 1.2.1 or lower then Software Upgrade of Onboard PoP device fails, only when the other devices software version is 1.2.2.
If software version of all devices are lower and upgraded to higher version except Onboard PoP then Software Upgrade should fail.	If all the devices including Onboard PoP are running with 1.2.2, and selected software version is 2.0 excluding PoP node, then Software Upgrade for all the devices should fail except PoP node.
If software version of all devices including PoP is running with same version, and when you select all nodes to upgrade, then PoP fails to upgrade. You need to manually upgrade the PoP node.	If all the devices including PoP are running with software version 1.1 and selected software version is 1.2. If PoP failed to upgrade, then you need to manually upgrade the PoP.

- From the **Versions** dropdown, select the version and the devices in the network for software upgrade.

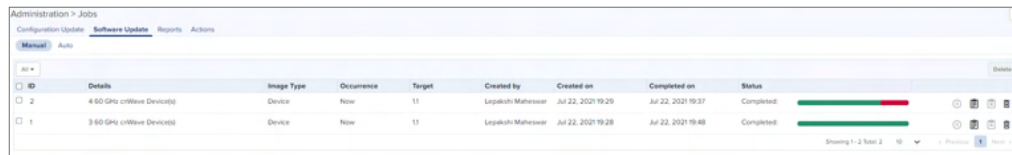
The Software Upgrade scenario for Onboard E2E Controller is explained in [Table 80](#).

View Update Jobs

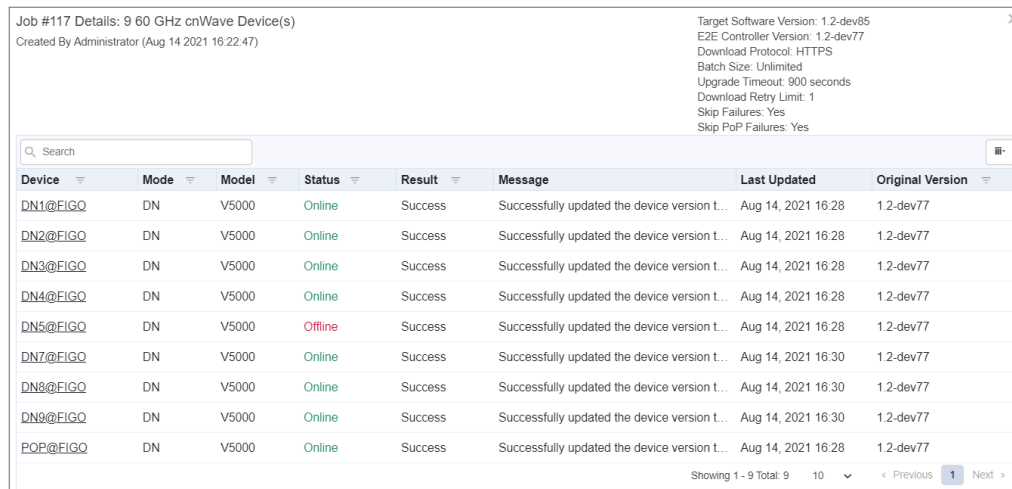
After adding the new Software Images, click **View Update Jobs**.



1. Navigate to the **Administration > Jobs > Software Update**.



2. Click **Show More** to view the Job Details.



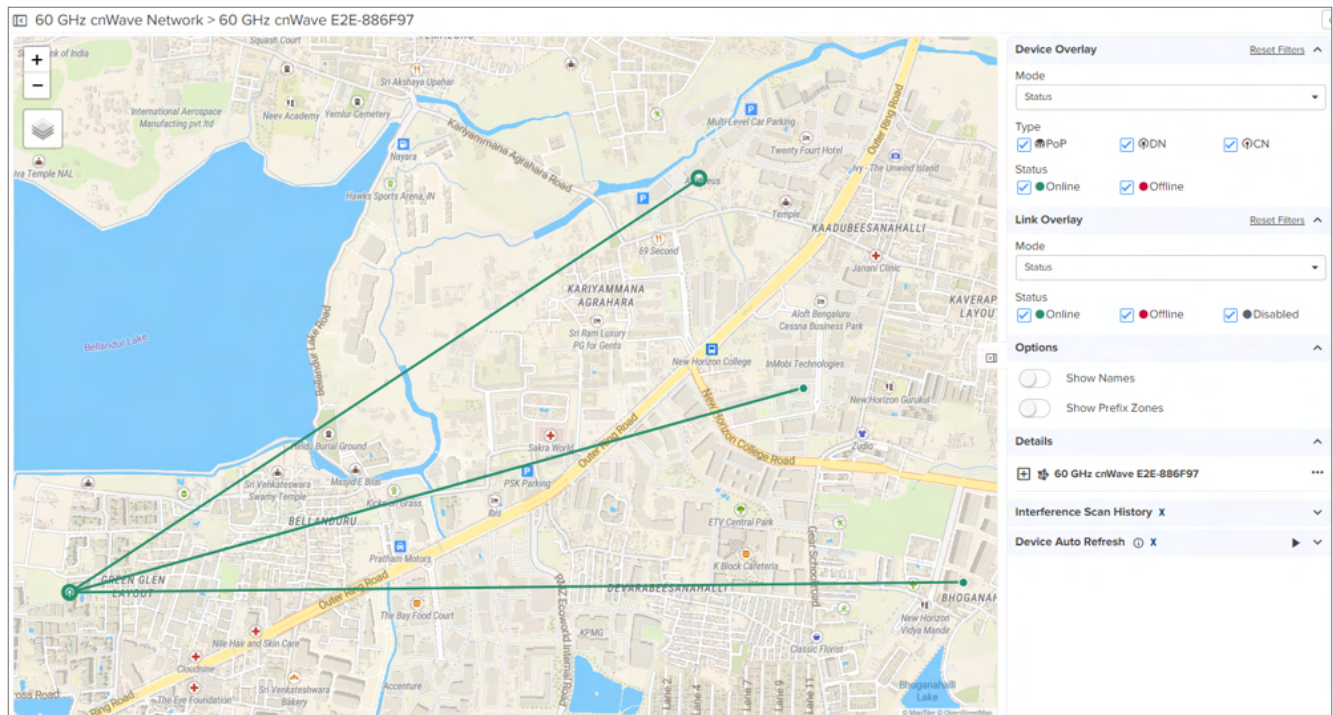
Reports

Reports page provides details on how to schedule and generate different types of data reports such as Devices, Active Alarms, Alarm History, and Events. For further details refer to [Reports](#).

Map

The Map page shows how devices are connected in an E2E network, the state of the devices, and links in the E2E network. To view the map, select the **Map** icon in the left pane of the homepage and navigate to **E2E Network** to view the 60 GHz cnWave devices and links (as shown in [Figure 360](#)).

Figure 360 Viewing E2E Network



Note

Gray color lines are unmanaged links and gray color nodes are unmanaged nodes.

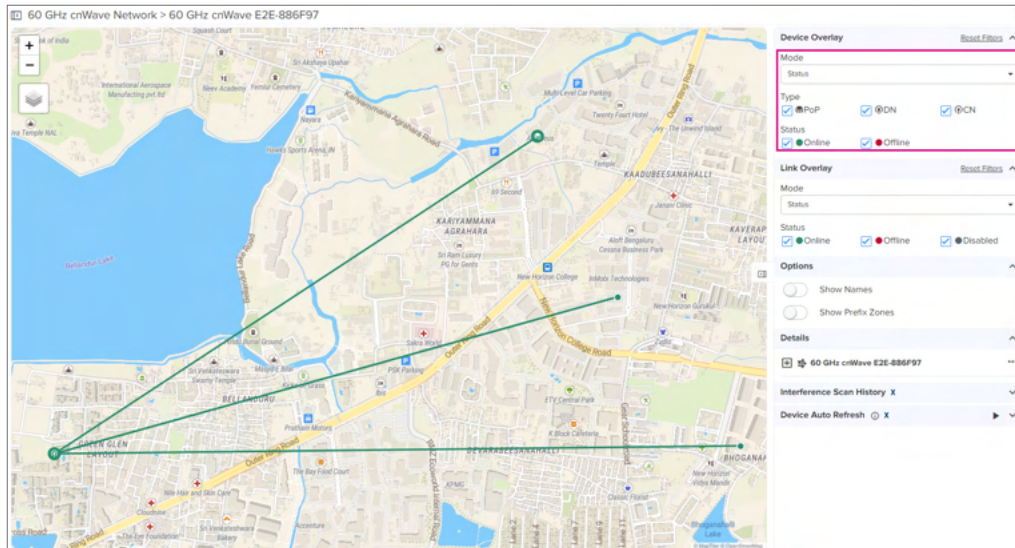
The following fields on the **Map** page provide details of the nodes and links:

- [Device Overlay](#)
- [Link Overlay](#)
- [Options](#)
- [Details](#)
- [Interference Scan History X](#)
- [Device Auto Refresh](#)



Device Overlay

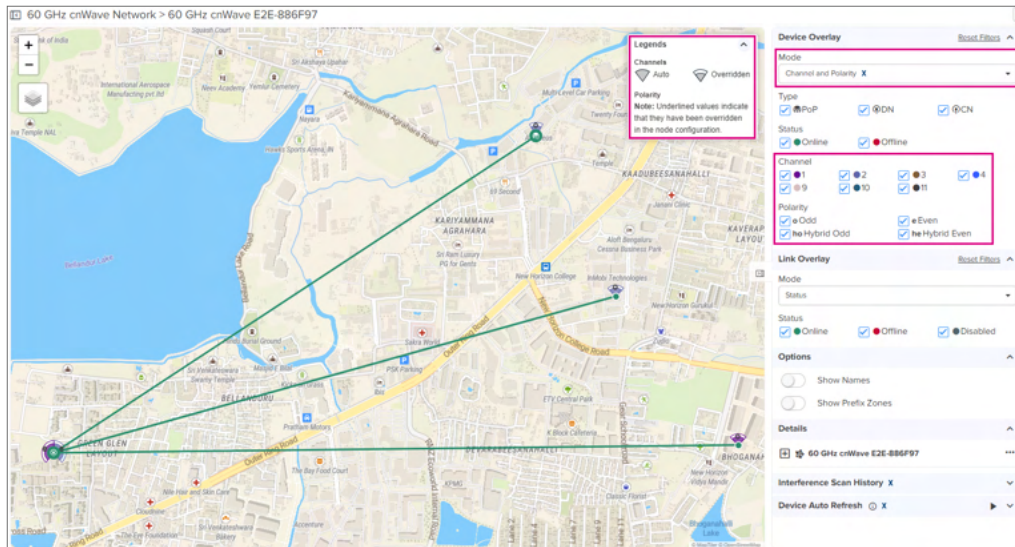
In the Device Overlay field section, complete the following steps:

1. Select the **Mode** type as **Status** to view the following:
 - Status: The device status is Online or Offline.
 - Type: The device types are PoP, CN, or DN in the E2E Network.



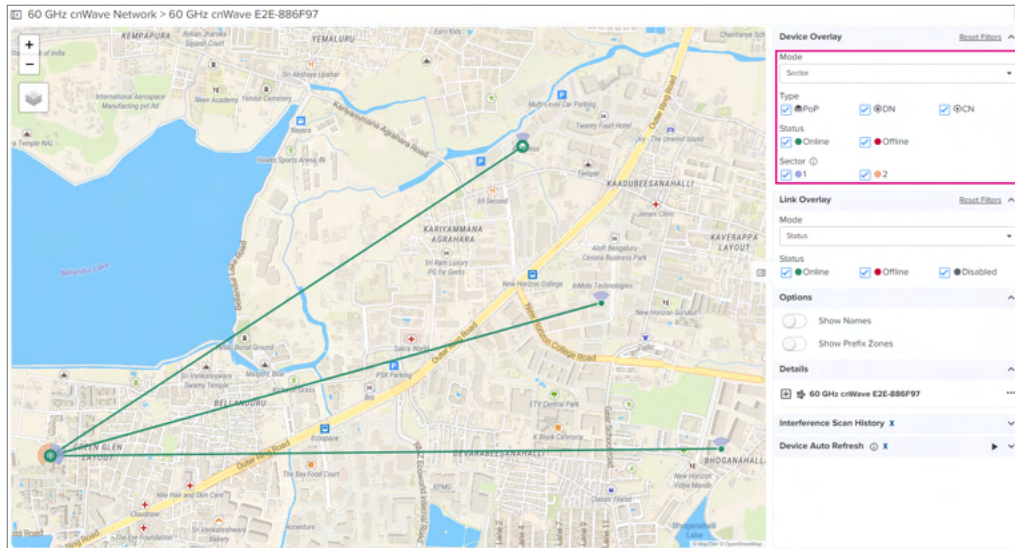
2. Select the **Mode** type as **Channel and Polarity** to view the following:

- Channel: The seven channels are represented in different color codes. Auto channel is indicated as  and Overridden channel is indicated as .
- Polarity: The polarity is represented as odd, even, hybrid odd, and hybrid even. Underlined values indicate they have been Overridden in the node configuration.

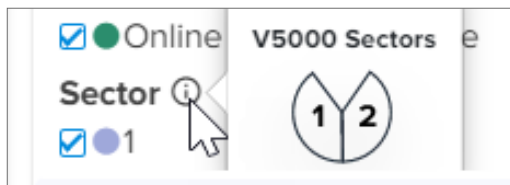


3. Select the **Mode** type as **Sector** to view the following:

Sector: The two sectors are represented in two different color codes.



V5000 Sectors is shown below:

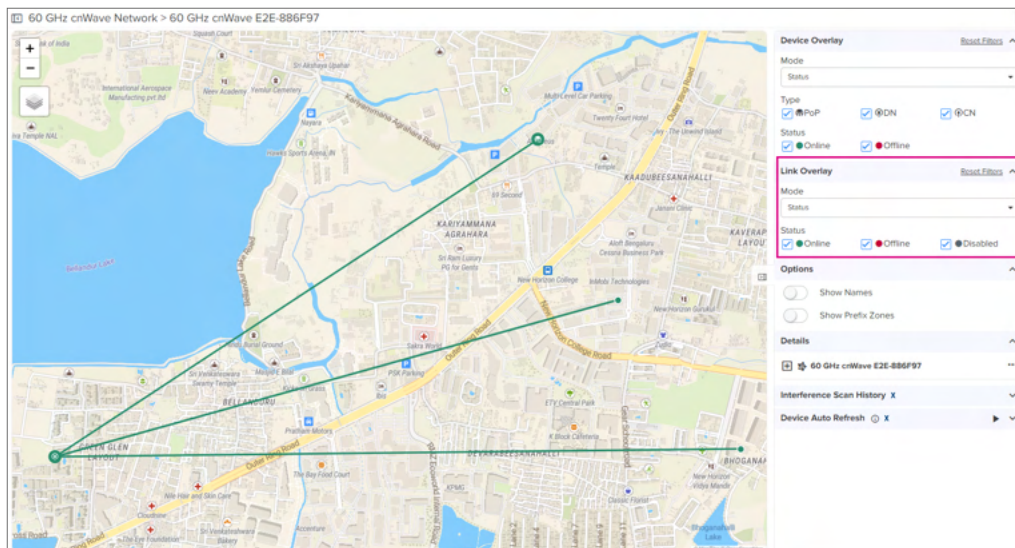


Link Overlay

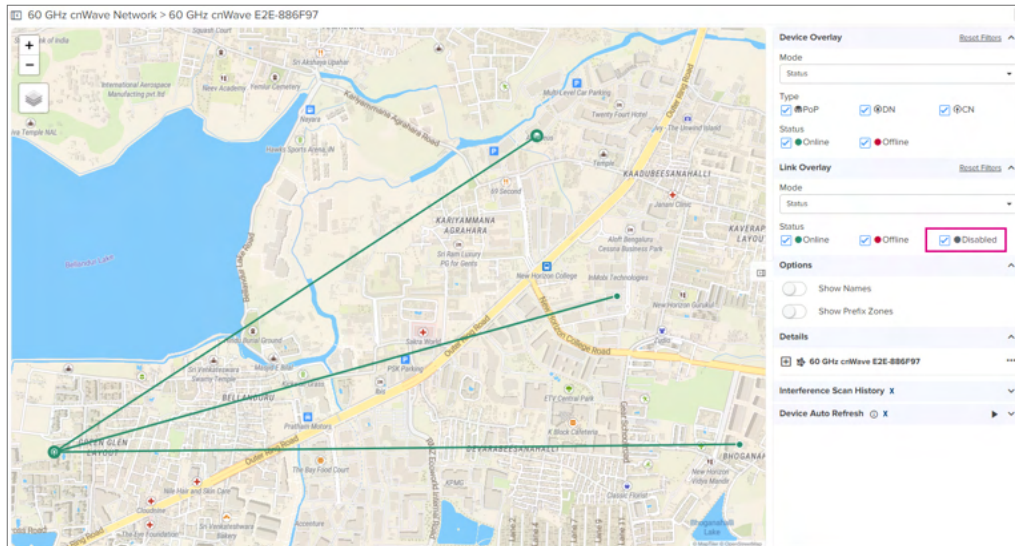
In the Link Overlay field section, complete the following steps:

1. Select the **Mode** type as **Status** to view the following:

Status: The link status is Online or Offline.

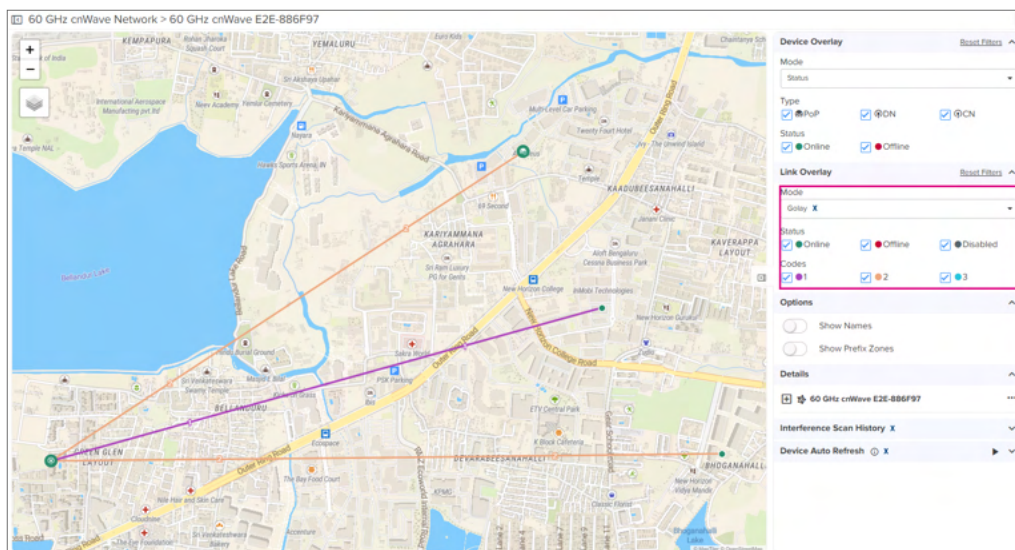


By default the **Disabled** option is selected, which appears in light gray.



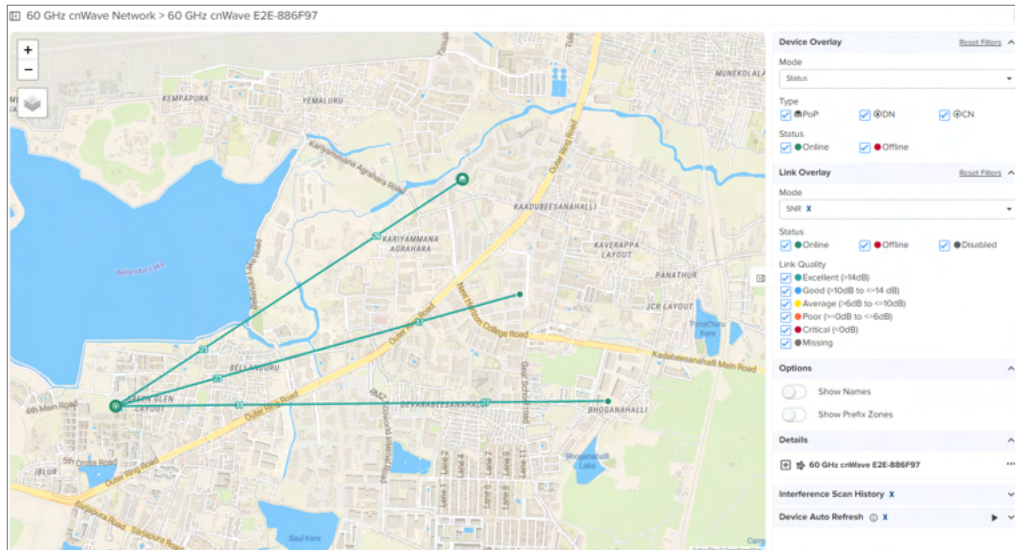
2. Select the **Mode** type as **Golay** to view codes.

Golay: The Golay mode is represented in color codes, as shown below:



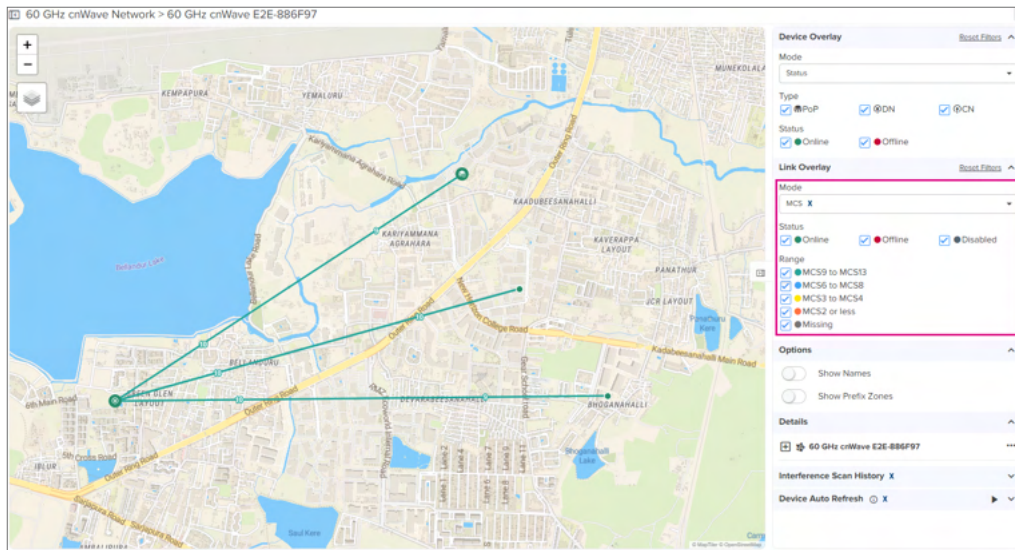
3. Select the **Mode** type as **SNR** to view link qualities.

SNR: Shows various SNR link qualities and is represented in different colors.



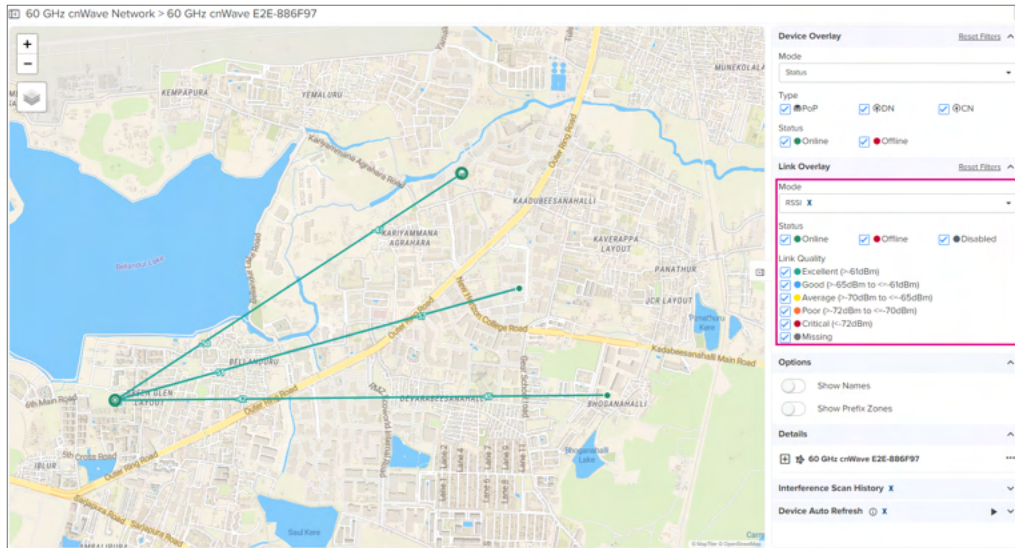
4. Select the **Mode** type as **MCS** to view link range.

MCS: Shows the link status and various link ranges represented in different colors.



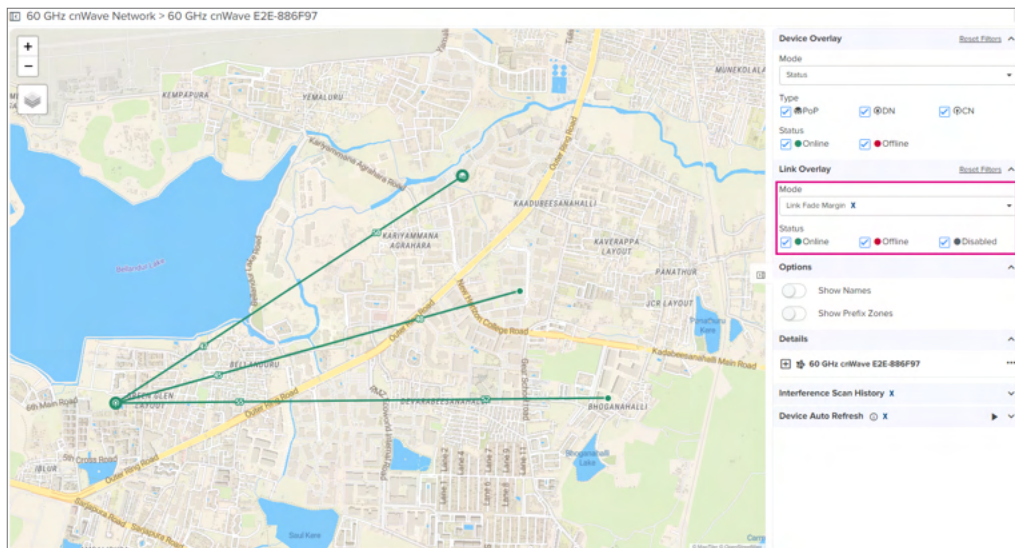
5. Select the **Mode** type as **RSSI** to view link qualities.

RSSI: Shows various RSSI link qualities represented in different colors.



6. Select the **Mode** type as **Link Fade Margin** to view link fade margins.

Link Fade Margin: calculates link fade margins between two devices. For details on overview and calculation, refer to the example described in [Figure 359](#).



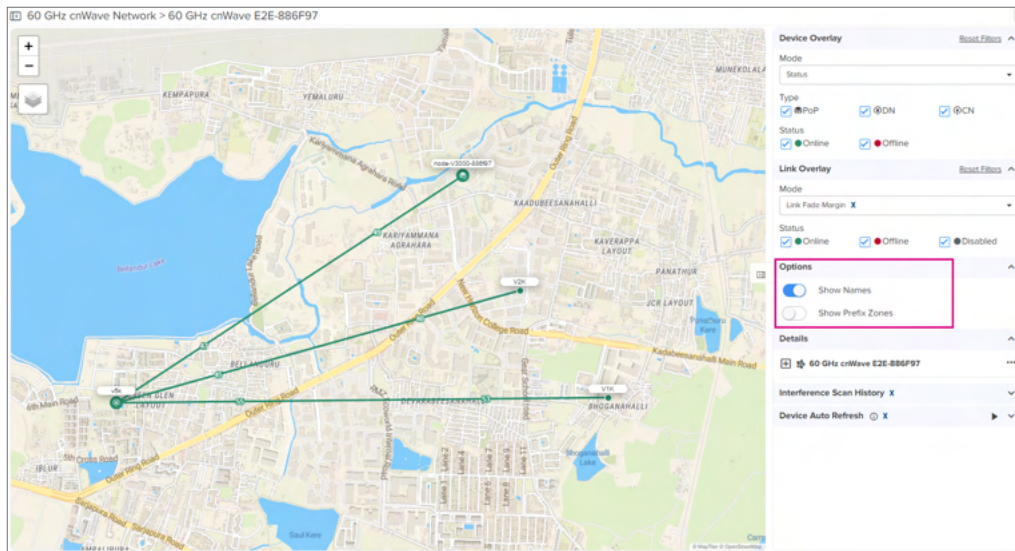
Note: Link Fade Margin is applicable only when E2E Controller and Device version are 1.2.2.

- Airtime%
- Throughput (Mbps)

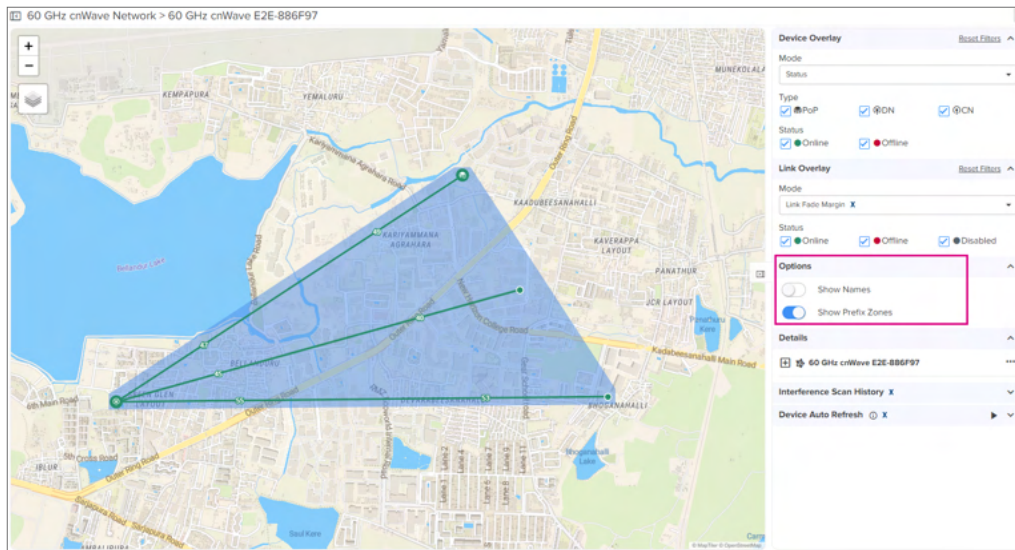
Options

The Options field supports UI controls to toggle between **Show Names** and **Show Prefix Zones**, as described:

- **Show Name:** shows the name of the nodes available in the E2E Network.



- **Show Prefix Zones:** shows the prefix zone of each PoP that is communicating with each other.

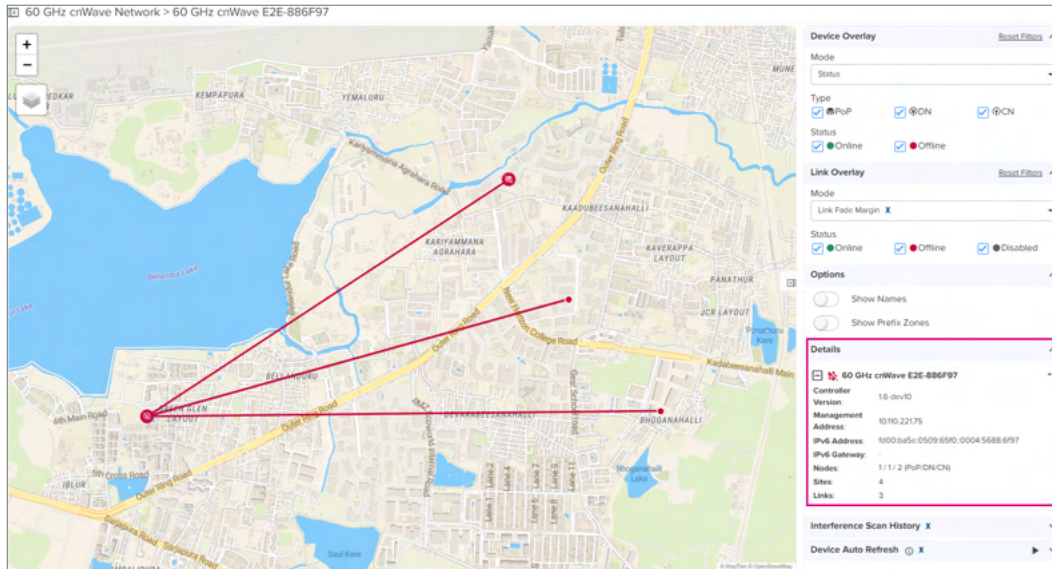


Note

Show Prefix Zones is enabled only if **Prefix Allocation** is set to **Deterministic**.

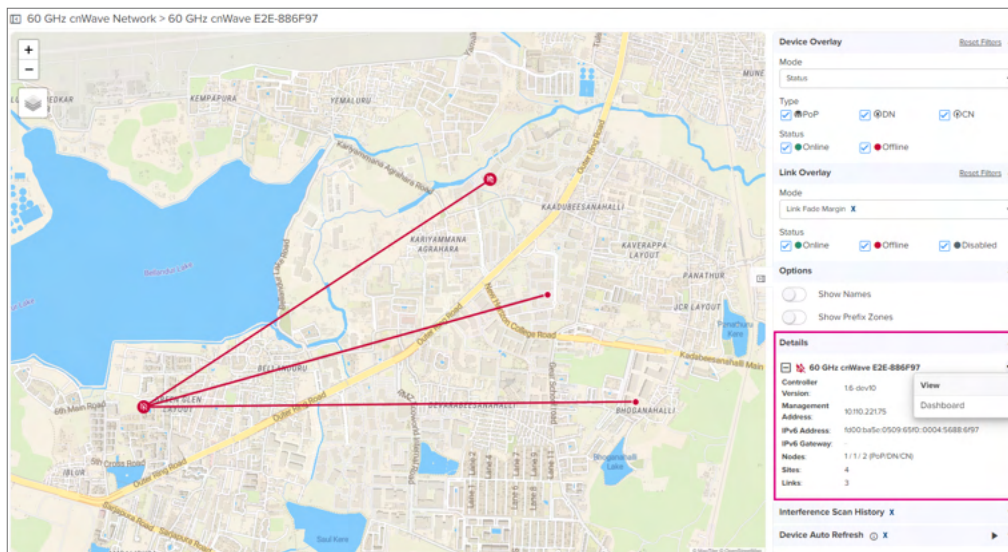
Details

The **Details** field displays the basic details of E2E Network when E2E Network is selected from the tree.



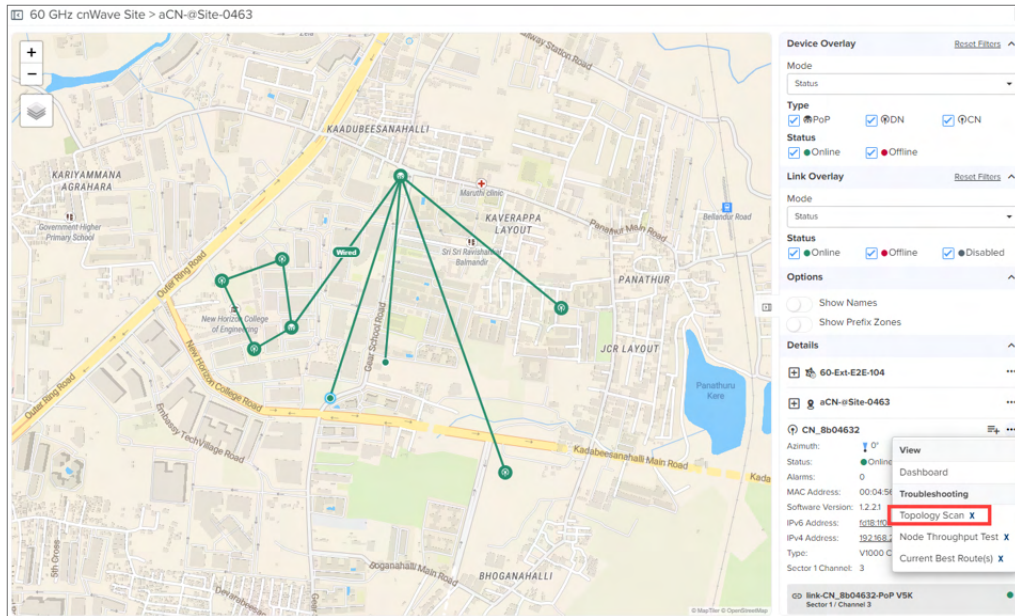
To view the details of nodes and links, complete the following steps:

1. Click the (...) icon in the **Details** section to view E2E Network Dashboard.



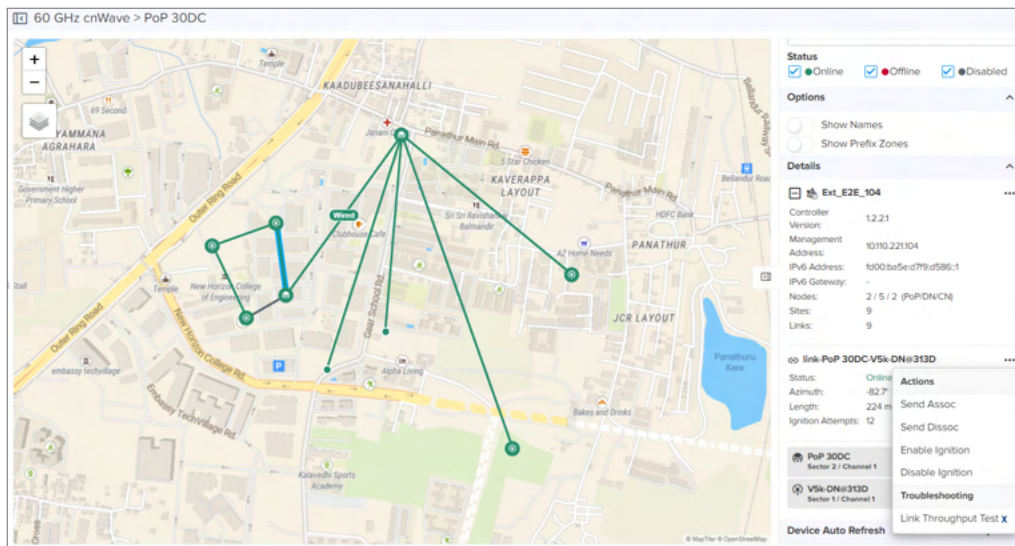
When a device is selected from the map, the device details are displayed.

2. Click the ... icon next to the device to view the device **Dashboard** and **Topology Scan**. For more details on how to troubleshoot a node using Topology Scan refer [Topology Scan](#)



Refer to [Node Throughput Test](#) and [Current Best Routes](#) in the [Troubleshooting](#) section.

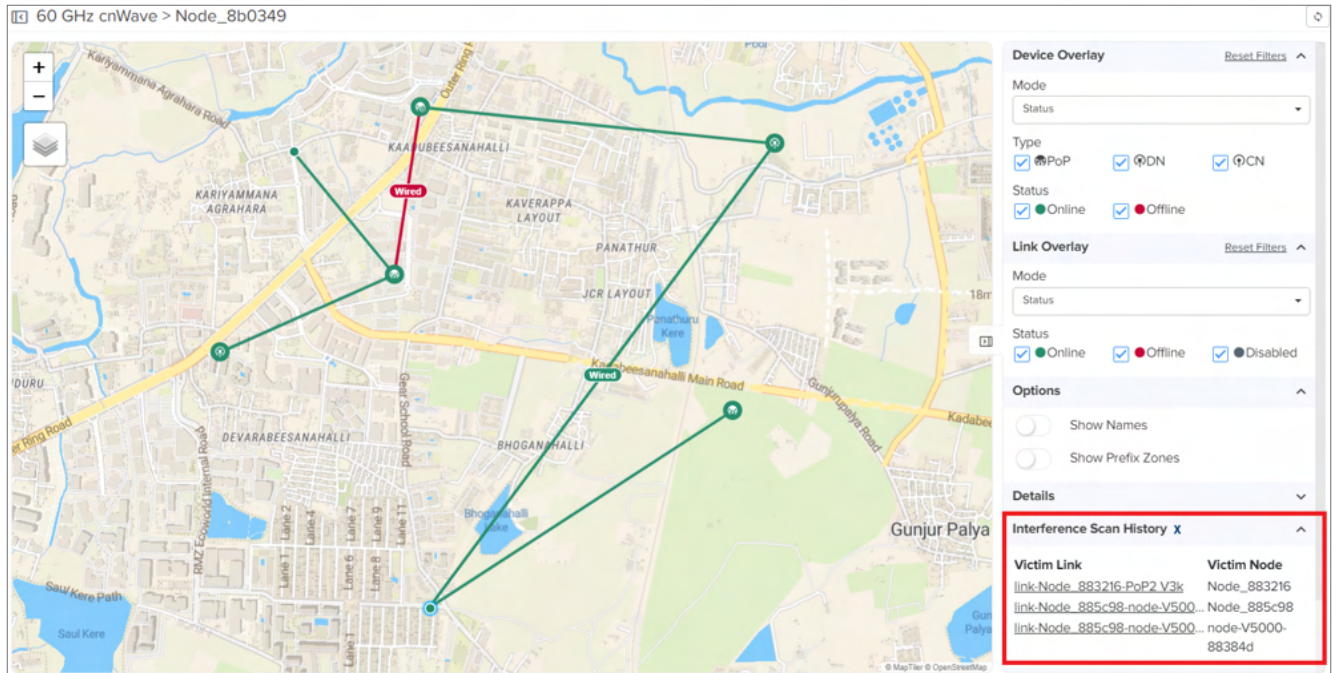
- When a link is selected from the map, link details are displayed. Click ellipsis (***) icon next to link to view the **Actions** details for the links.



Refer to [Link Throughput Test](#) in the [Troubleshooting](#) section.

Interference Scan History X

The **Interference Scan History X** field displays the last three scan results specific to interfering links for the whole 60 GHz cnWave network. For more details, refer to Interference Scan X. For detailed information about the feature, refer to [Interference Scan X](#) in the [Troubleshooting](#) section.



Device Auto Refresh

The Device Auto Refresh field allows to refresh data of the E2E Network automatically. In the Device Auto Refresh field section, complete the following steps:

1. Select the devices in the map and add it to the watch list for **Device Auto Refresh**.
2. Click the ▶ icon to start the auto refresh.
A maximum of 10 devices can be added to **Device Auto Refresh**.
3. Click the ⊖ icon to remove devices from **Auto Refresh**.



Note

- Channel and Polarity mode type are available for cnMaestro X users only.
- Airtime%, Golay, SNR, RSSI, MCS, Link Fade Margin, and Throughput (Mbps) are cnMaestro X features.

Using the **Details** section on the Map page, you can perform the following actions:

- [Troubleshooting](#)
- [Changing channel or Golay for specific 60 GHz cnWave links](#)
- [Setting the Last Resort Metric \(LRM\) for a cnWave 60 GHz link](#)

Troubleshooting

The **Troubleshooting** action allows you to run the following tests:

- [Topology Scan](#)
- [Node Throughput Test](#)
- [Current Best Routes X](#)
- [Link Throughput Test X](#)
- [Interference Scan X](#)

Topology Scan

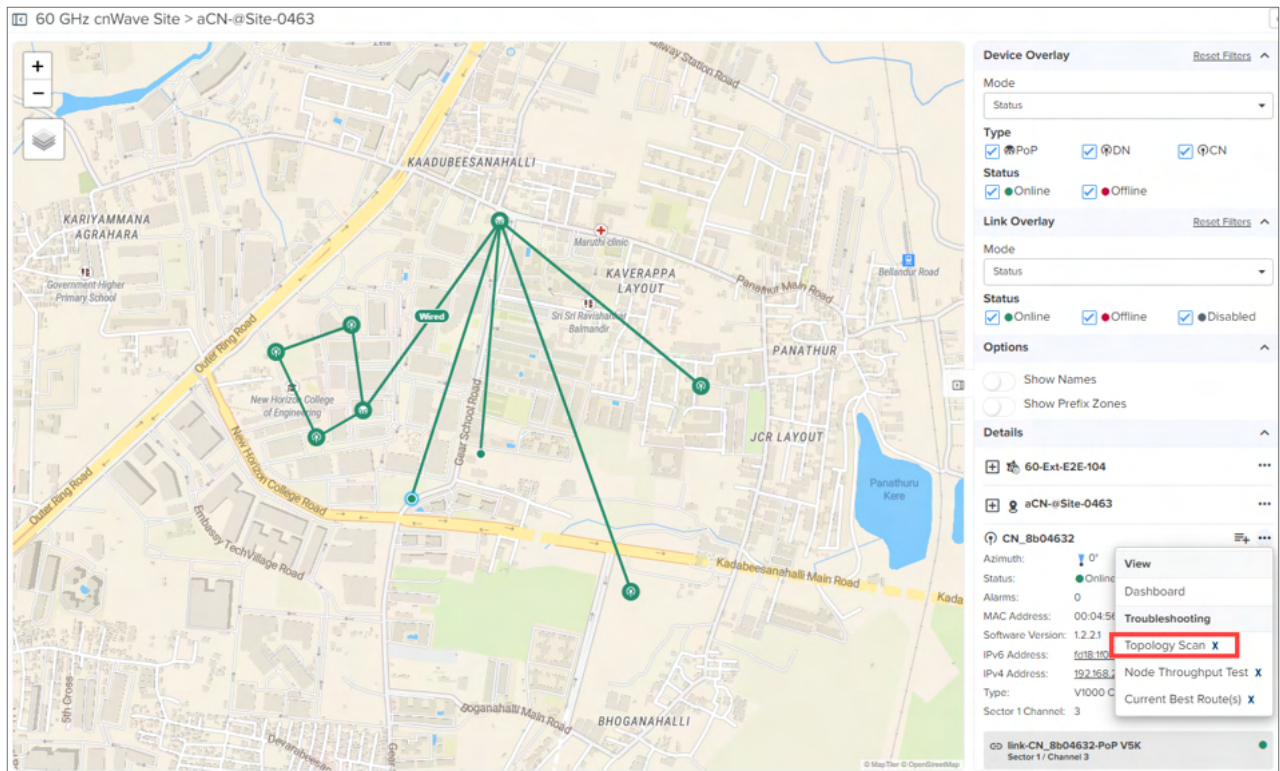
Topology Scan X allows you to discover your entire network and create comprehensive, detailed network topology maps. This tool will only detect nodes operating in responder mode. It will not detect CNs with a wireless link already established. Offline nodes with a configured channel override will not be detected on a different channel.



Note

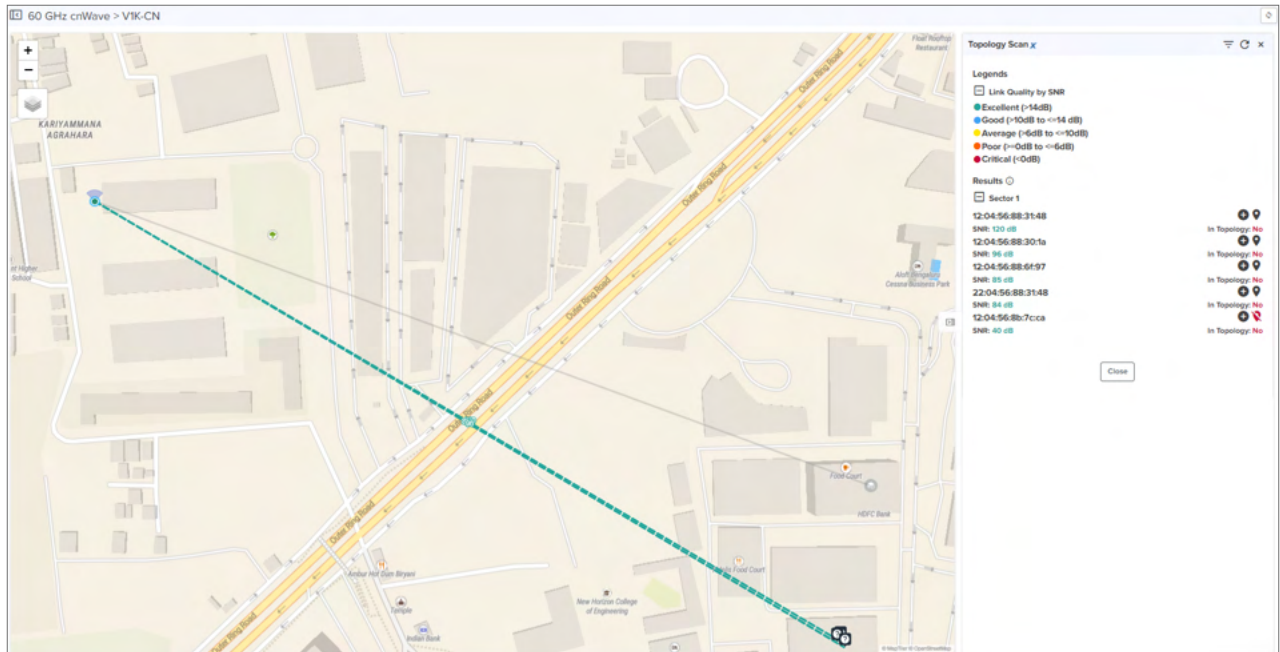
Topology Scan will cause a momentary throughput reduction in nearby links.



1. Select a node from the Map.
2. Click ellipsis (...) icon next to the device to select the **Troubleshooting > Topology Scan**.



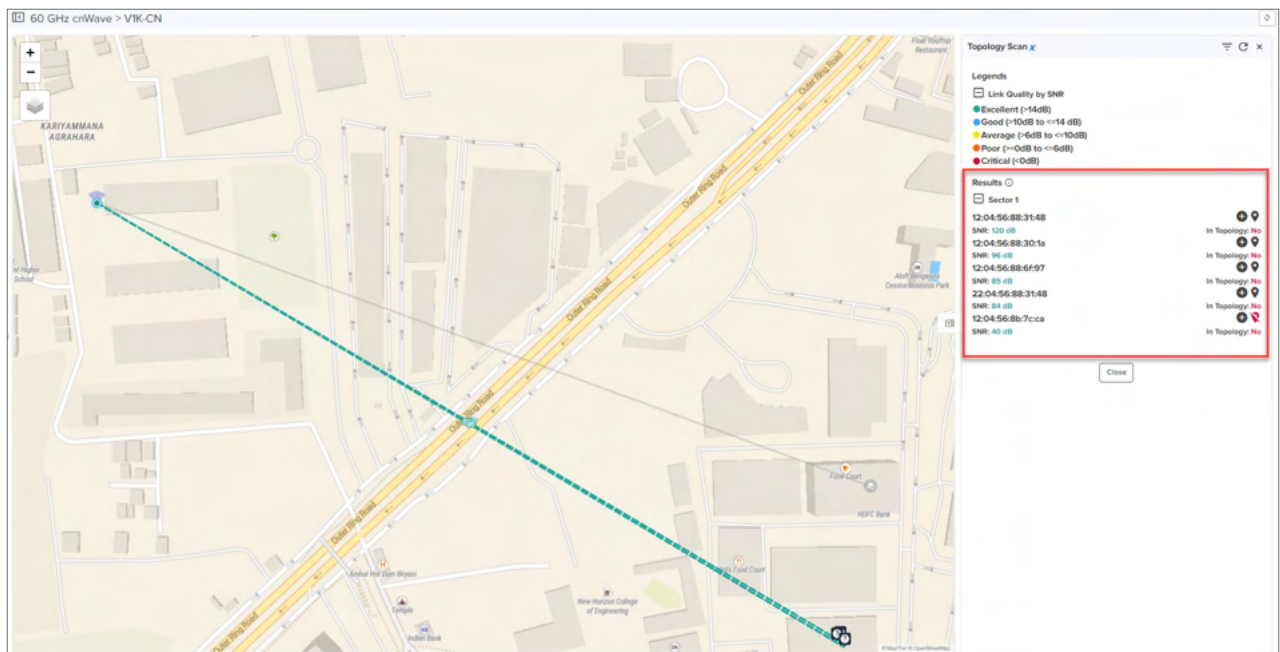
Topology Scan preview window is displayed towards the left pane.

3. Click **Start Topology Scan**. Topology Scan begins as shown in the following figure.



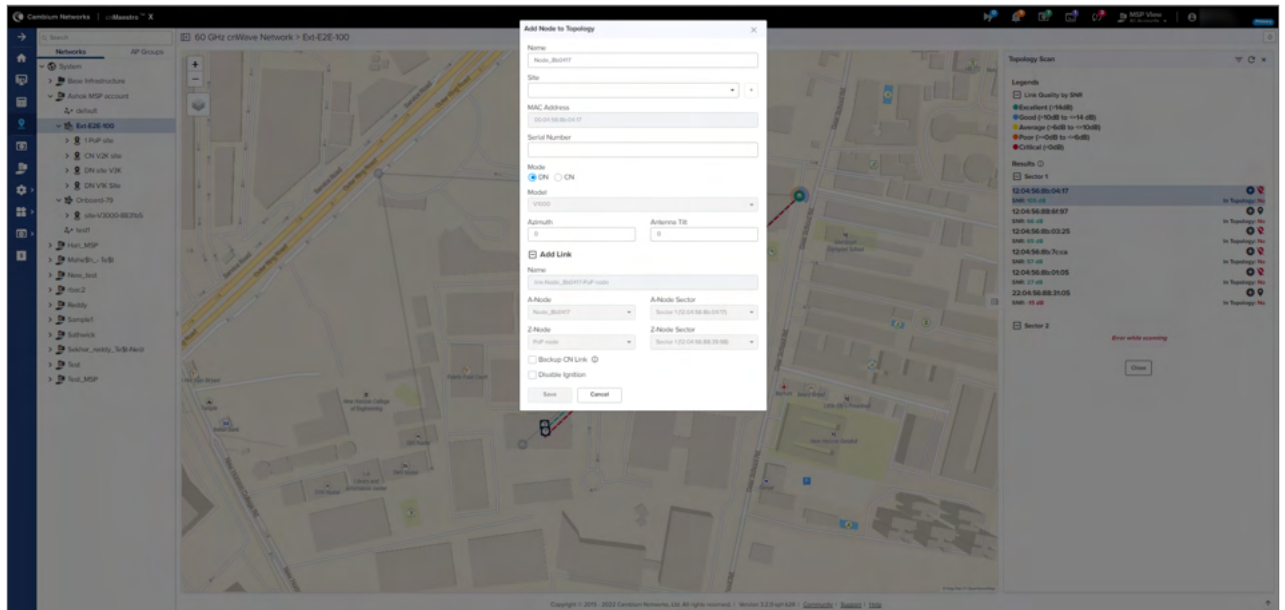
4. Click **Configure SNR Limit** () next to **Topology Scan** header to add new value or reset the existing value. By default SNR value is 5 dB.
5. Click () refresh icon to scan again.

The results are based on **Link Quality by SNR** and the results are shown in the left pane. MAC Address of the links and the Link Quality is displayed.



After topology scan, map displays available nodes and links in the network by Link Quality color codes. Only links available with GPS coordinates are shown in the map. You can add site, node, and link to the topology by clicking the plus sign **In Topology**.

6. **Add Node to Topology** window pops up.



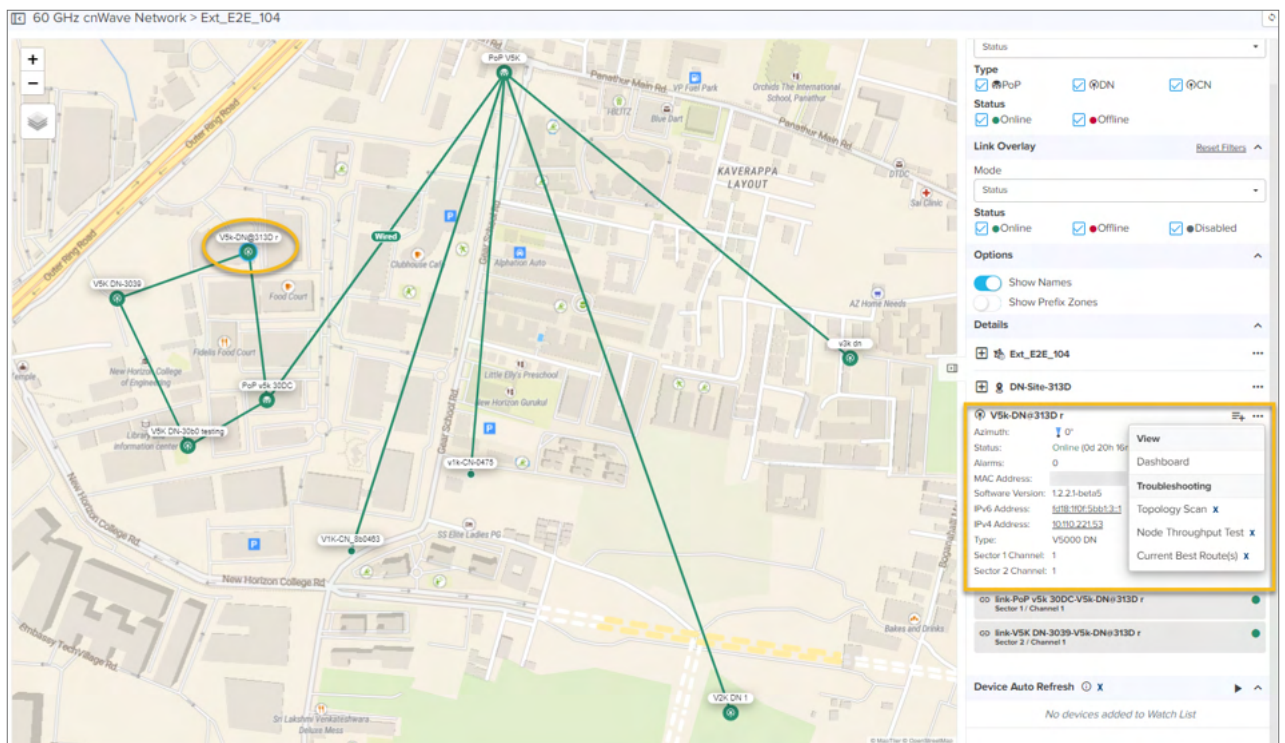
7. Enter the node and link details and click **Save**.

Node Throughput Test X

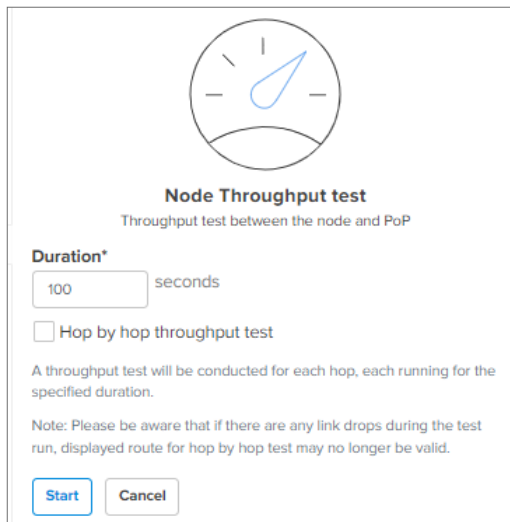
The **Node Throughput Test X** option allows you to test the throughput between a node and PoP. Using this option, you can conduct a throughput test for each hop seamlessly.


To run a node throughput test, complete the following steps:

1. Select a device except the POP Node from the Map.



2. Click ellipsis (***) icon next to the device name in the right pane, and select **Troubleshooting > Node Throughput Test X**





Node Throughput test

Throughput test between the node and PoP

Duration*

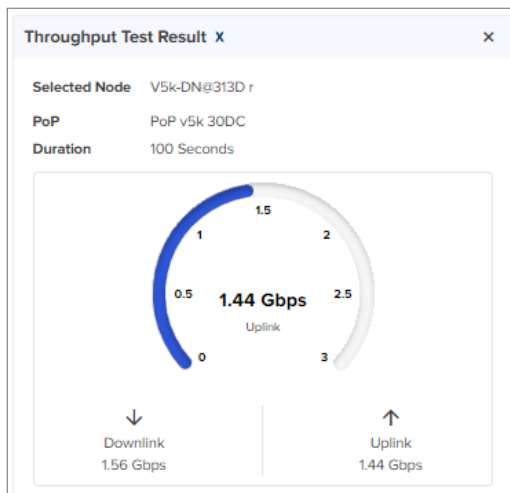
seconds

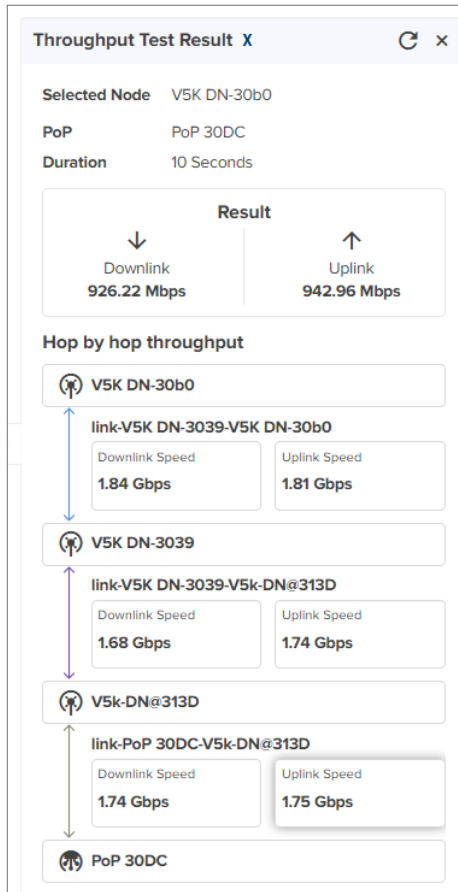
☐ Hop by hop throughput test

A throughput test will be conducted for each hop, each running for the specified duration.

Note: Please be aware that if there are any link drops during the test run, displayed route for hop by hop test may no longer be valid.

3. Enter the **Duration** between 5 to 300 seconds.
4. Select the **Hop by hop throughput test** checkbox to view the throughput for each hop separately.
5. Click **Start**.





Current Best Route(s) X

The Current Best Route(s) X feature is used to view the best route from a CN/DN to PoP. The **Current Best Route (s) X** map view displays statistics of the following parameters for uplink and downlink of wireless link of a node:

- Golay
- SNR
- MCS
- RSSI
- Throughput (Mbps)
- Airtime (%)
- Link Fade Margin (LFM)

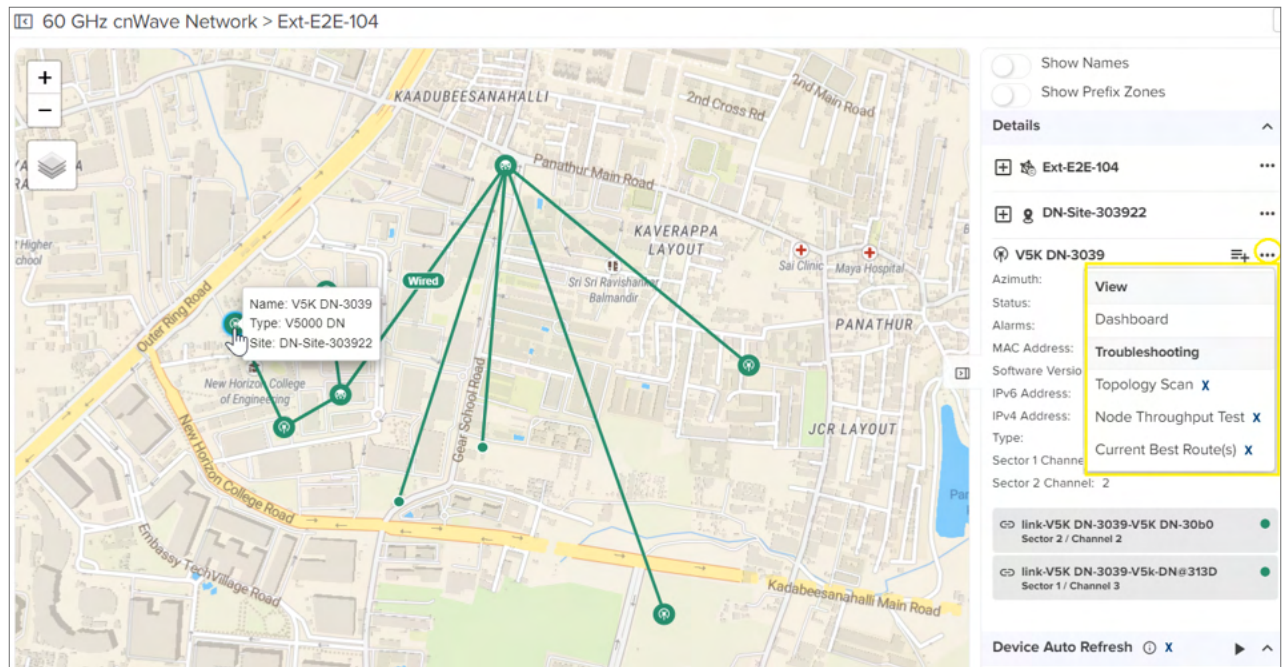


Note

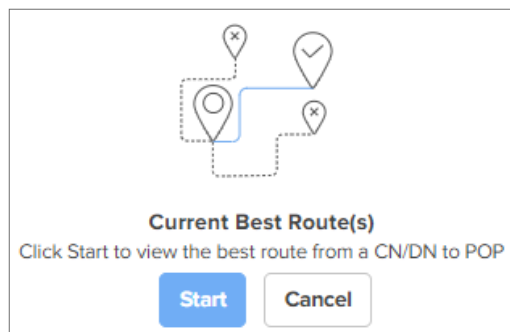
The **Current Best Route(s) X** feature is applicable only to X accounts. In addition, this feature is supported only on the E2E Controller (Onboard or external) running with software version 1.2.2.1 or later.

To view the current best routes, complete the following steps:

1. On the **Map** page, select a device node. The node details are displayed on the right side of the map.



2. Click the **...** icon next to the node name, and select **Troubleshooting > Current Best Route(s) X**. The **Current Best Route(s)** screen appears on the right side of the map.



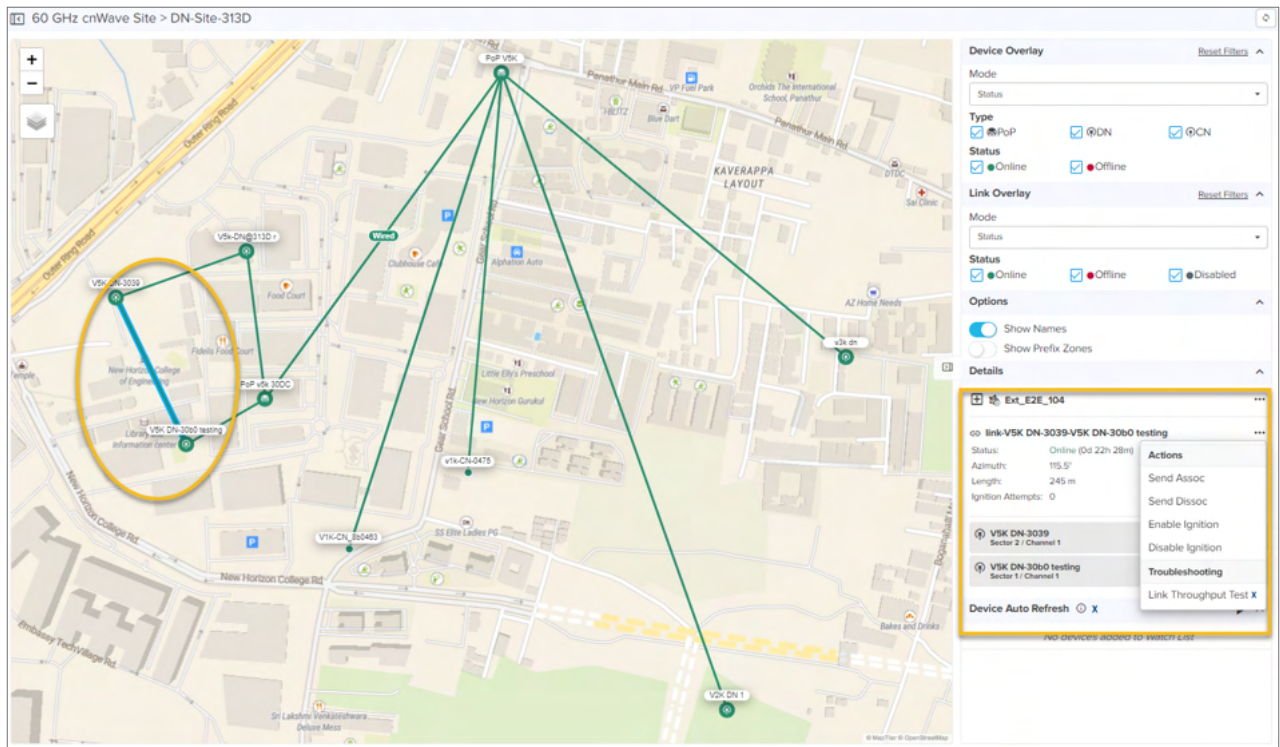
3. Click **Start**. The **Current Best Routes(s) X** section displays route details for the selected node.



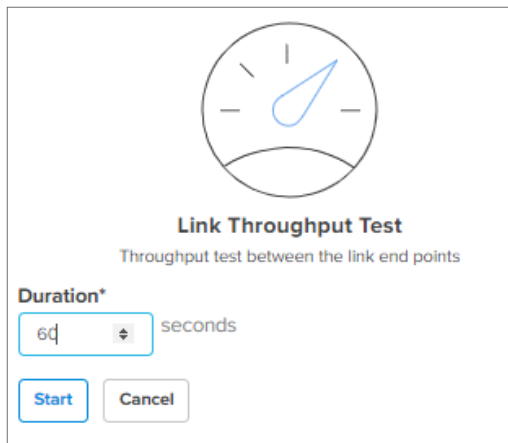
Link Throughput Test X

The **Link Throughput Test X** option allows you to test the throughput between the link end points. To run a link throughput test, complete the following steps:

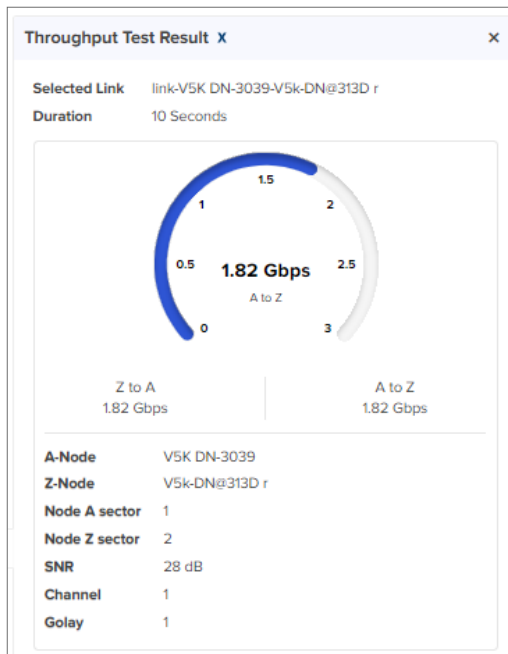
1. Select a Link from the Map.



2. Click ellipsis (...) icon next to the link, and select the **Troubleshooting >Link Throughput Test X**



3. Enter the **Duration** between 5 to 300 seconds.
4. Click **Start**.



Interference Scan X

Interference Scan (also known as Interference Management (IM) Scan) is an end-to-end, Controller-coordinated scan that aims at performing real-time measurements of interference affecting a specific interfered link (referred to as the victim link). The Controller filters the network topology to identify potential interfering links (known as aggressor links).

The Controller then issues batches of scan requests to the filtered aggressor nodes or sectors. These requests are transmitted using the antenna beams and transmit power intended for their data links. Meanwhile, the victim receiver listens for these scan requests (transmissions). The extent to which the victim receiver detects these scan requests determines the level of interference exerted by the aggressor links on the victim receiver.



Note

The **Interference Scan X** feature is applies only to X accounts and is available for 60 GHz cnWave software version 1.5 and later.

Output of Interference Scan

Using the cnMaestro UI, you can run the Interference Scan tool. The scan results show the victim link and its corresponding receiver MAC address (which serves as a unique identifier for the network devices).

It also provides a list of aggressor links along with their corresponding Signal-to-Noise Ratio (SNR) values relative to the victim receiver. SNR indicates the measurement of a signal strength compared to background noise, with higher values indicating better signal quality.

Impact on link performance

The interference from aggressor links impacts the maximum data rate that the victim link can achieve, determined by the Modulation and Coding Scheme (MCS). For instance, achieving MCS9 requires an SNR of at least 10 dB. However, if interference from an aggressor link reduces the SNR to 6 dB, the victim link will be limited to MCS4 or lower, resulting in slower data rates.

If the SNR is less than 0 dB, the interference is minimal and the aggressor links are unlikely to impact the victim link's performance.

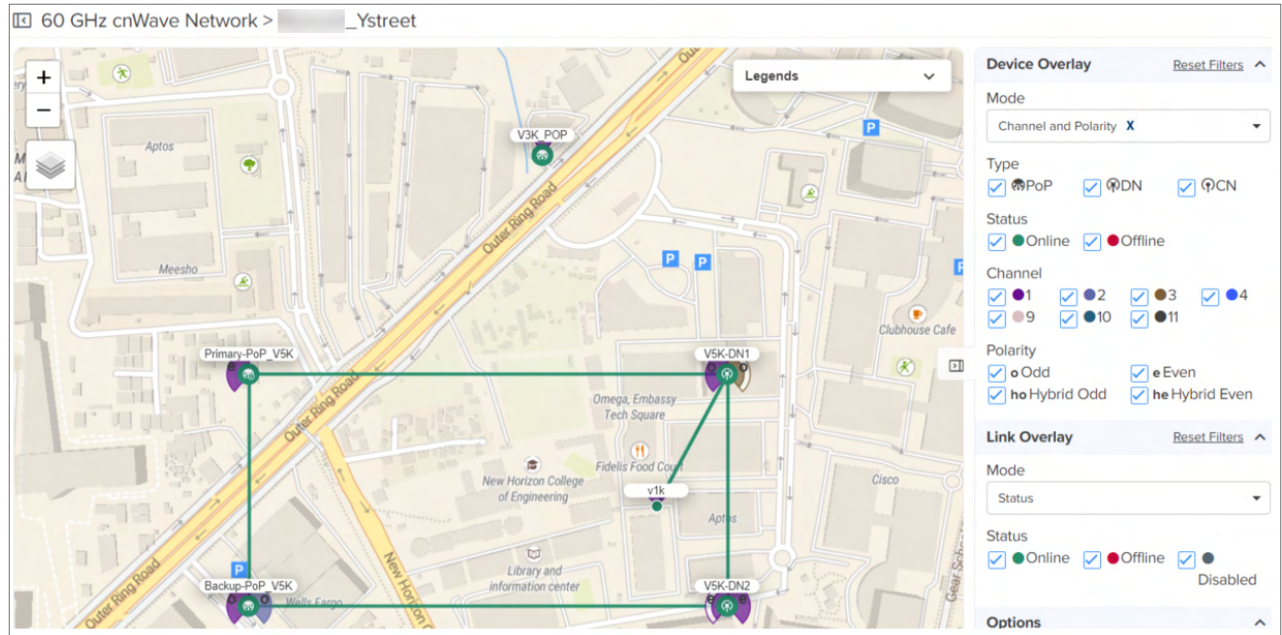
Running the Interference Scan tool

You can run the Interference Scan tool using the **Map** page in cnMaestro UI only. You can also view the last three scanned results for the cnWave network in the **Interference Scan History X** section in the **Map** page.

To run the Interference Scan tool, complete the following steps:

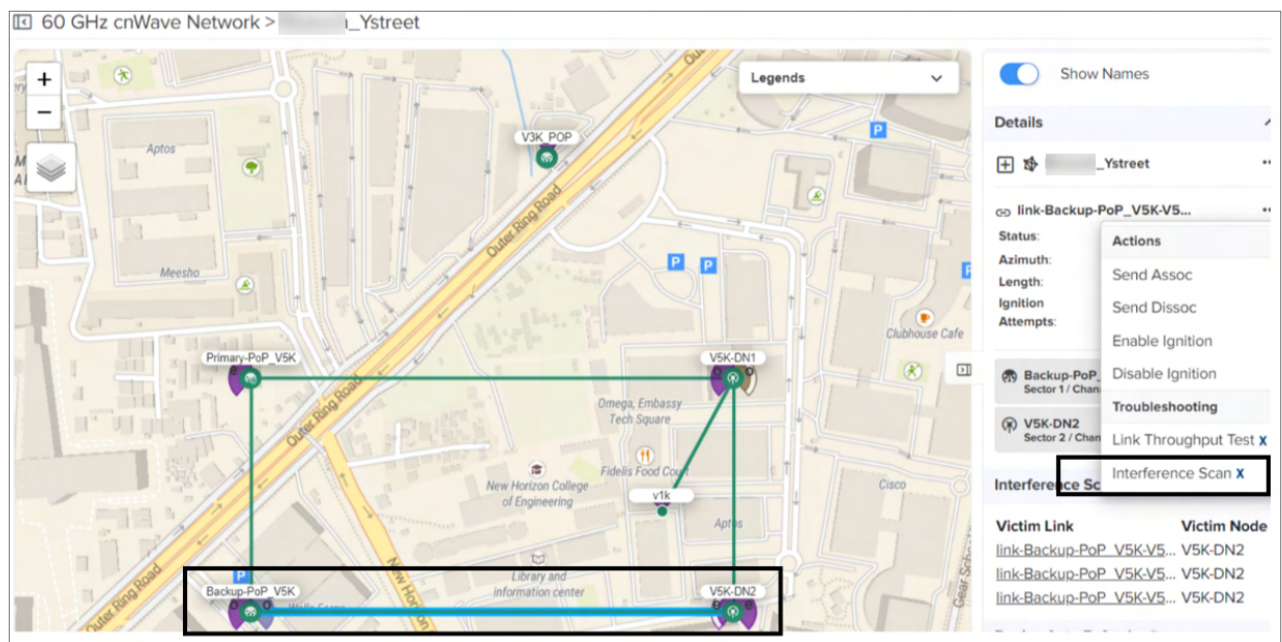
1. On the **Map** page, select a cnWave network and click on the link for which you want to run the interference Scan tool.

The **Details** section on the right side of the **Map** page displays the selected link information. For example, there is a Backup-POP_V5K linked to V5K-DN2 in the figure shown below.

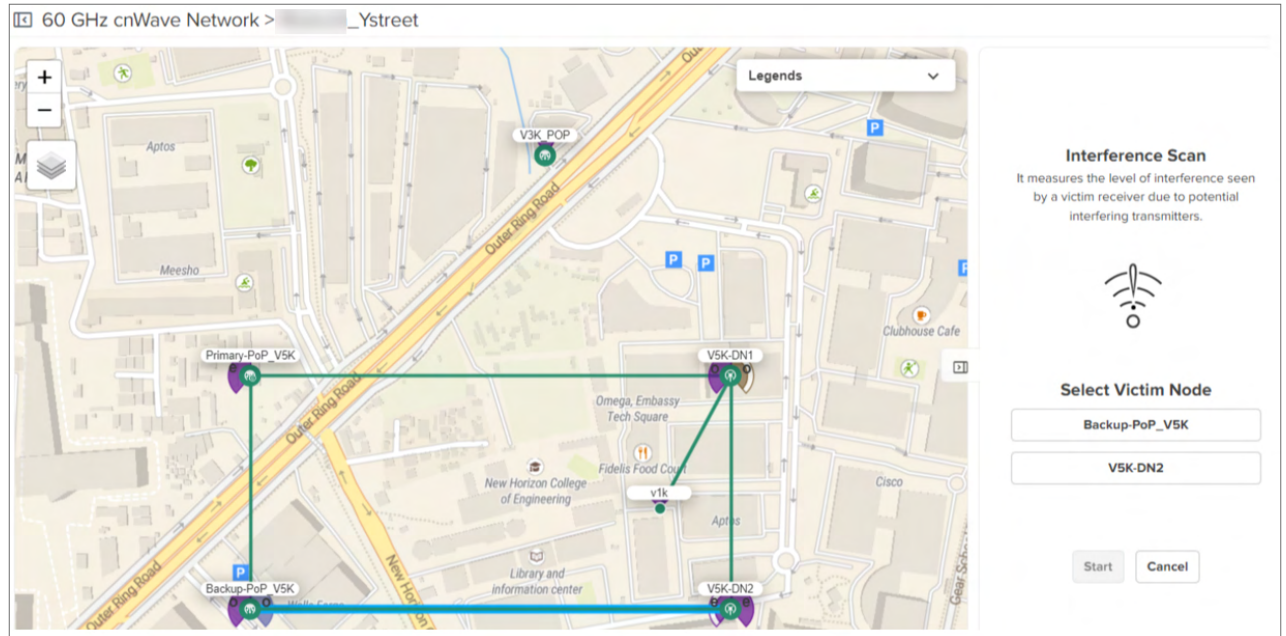


2. Click the **...** icon next to the link name and select **Interference Scan X** from the dropdown list.

For example, Interference Scan is used for the link highlighted between Backup-POP_V5K linked to V5K-DN2 in the figure shown below.

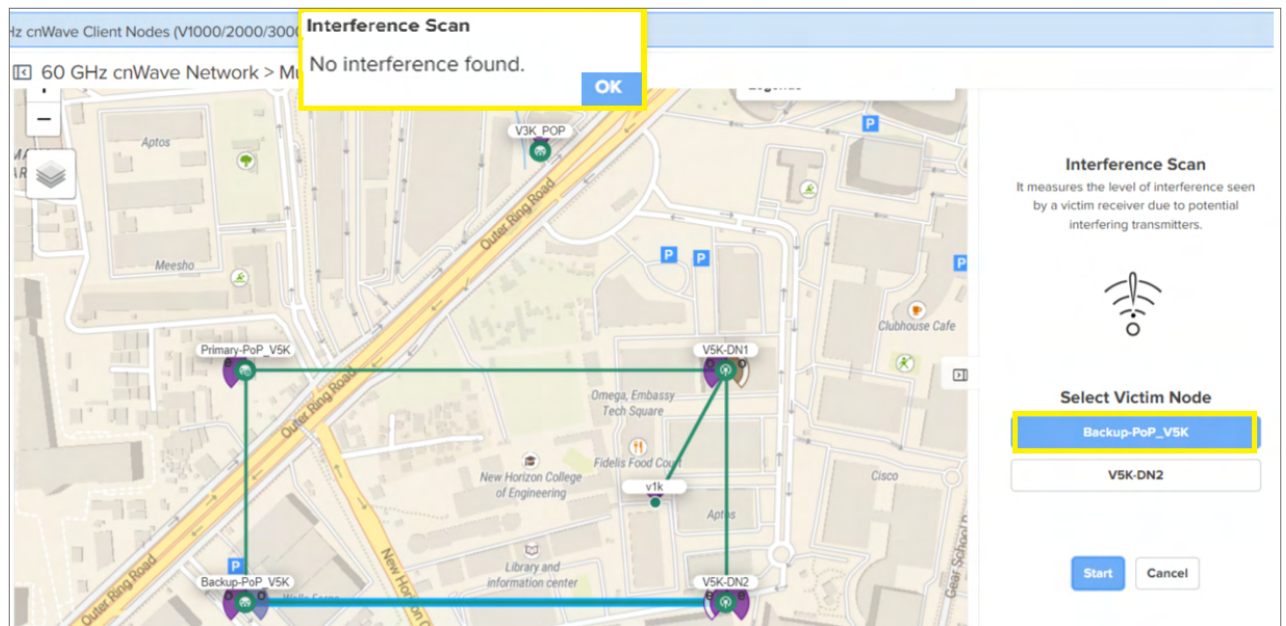


When **Interference Scan X** is selected, the **Interference Scan** section appears with the victim node names on the right side of the Map page (as shown in the figure below).



3. Select the required victim node and click **Start**.

The Interference Scan tool detects neighboring interfering links with wireless settings that may affect your network. The Interference Scan tool can be executed on any of the victim nodes. In the figure below, Interference Scan is executed on the first victim node Backup-POP_V5K. If no aggressor is found, a message appears stating that **no interference found**.

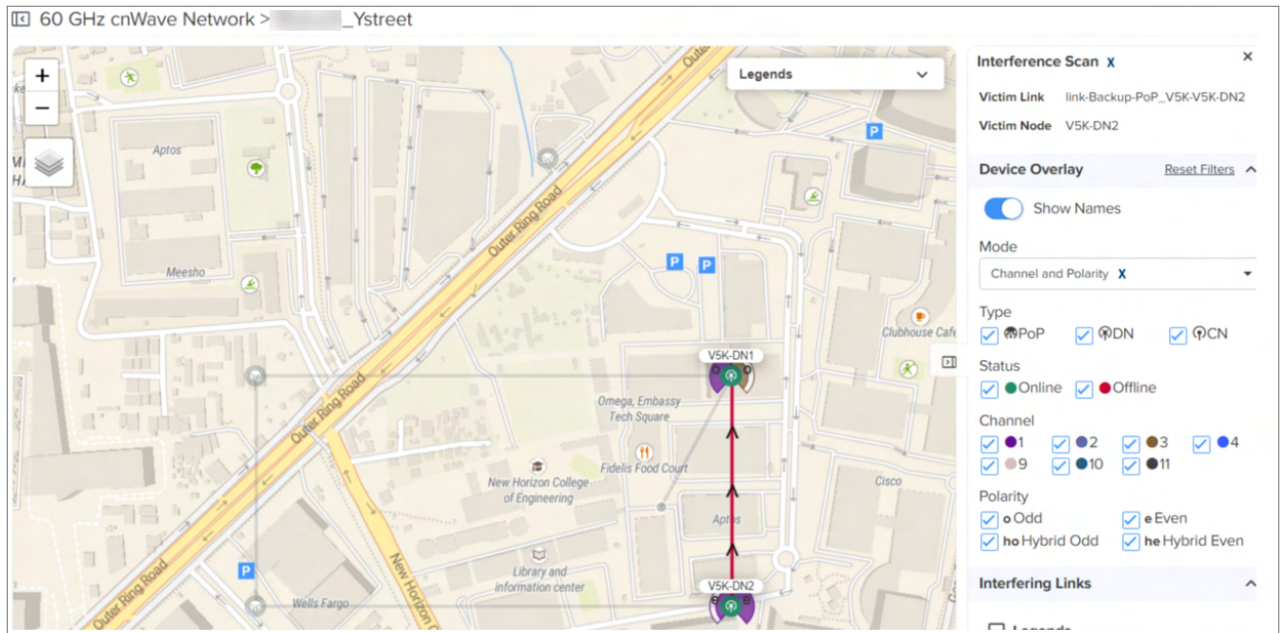


When you run the Interference Scan test on the second victim node (for example, V5K-DN2), the aggressor (if any) details are displayed as shown in the figure below. In this case, Backup-POP_V5K to V5K-DN2 uses channel 1 and V5K-DN2 to V5K-DN1 uses channel 1. The SNR values need to be analysed.



Note

The cnMaestro UI displays both a map view and a list view of the victim-aggressor relationship. The map is color-coded to show the severity of interference. The lower the SNR from aggressor links, the greater the interference on the victim link.



4. View the scan result for the selected victim node and take appropriate actions.

Changing channel or Golay for specific 60 GHz cnWave links

You have options on the **Maps** page in cnMaestro to perform the following operations:

- [Change Channel](#) for all links connected to a particular sector.
- [Change Golay](#) for a particular link connected between two nodes.

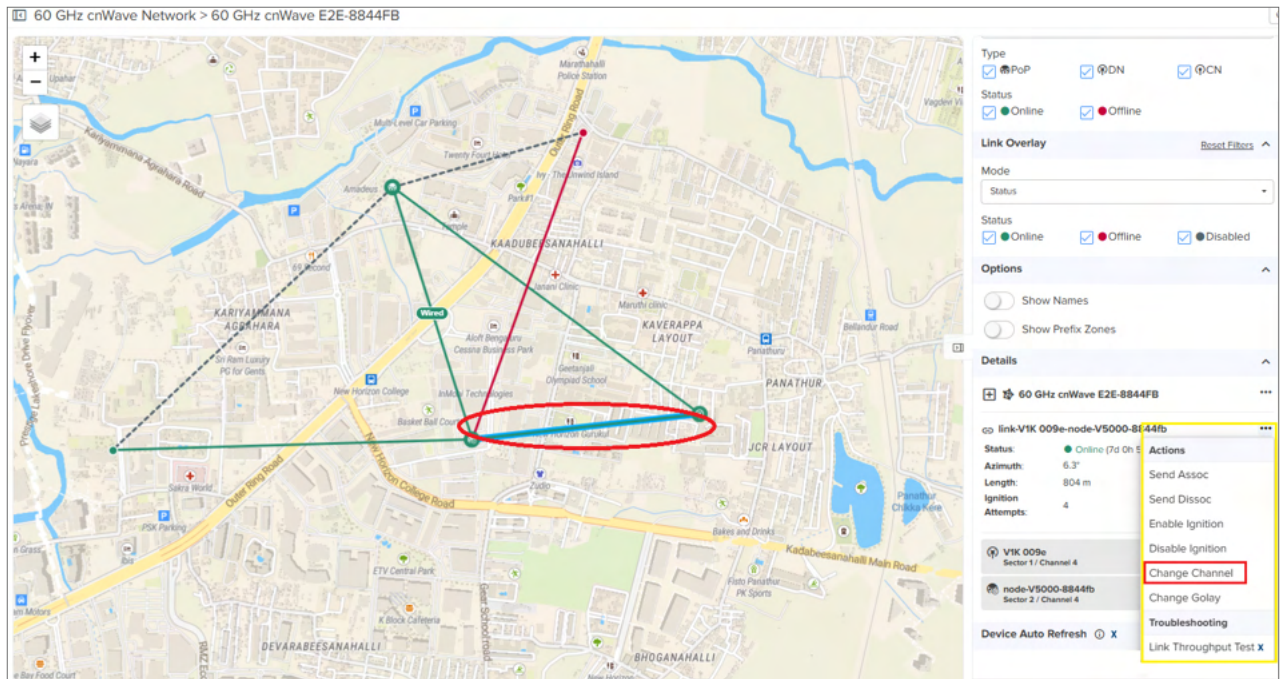
These operations help you to refrain from configuring the radio link for each node when there is any interference.

Change Channel

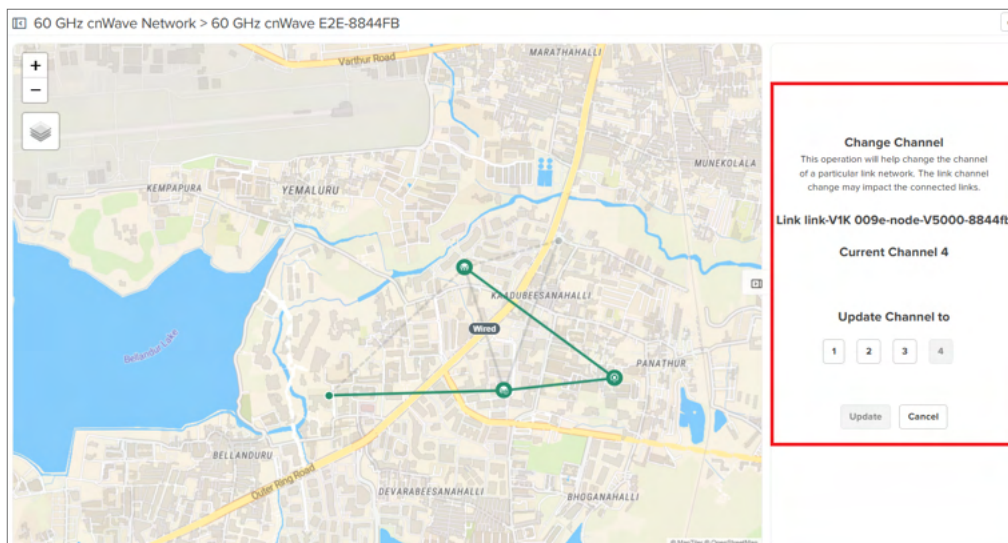
There may be an interference issue found when all the 60 GHz cnWave links in a **particular sector** have the same channel. In such a scenario, you can update or change the channel for all the links of a particular sector using the **Maps** page in cnMaestro UI.

Complete the following steps to change the channel:

1. On the **Map** page, select a cnWave network and click on the link for which you want to change the channel.
The **Details** section on the right side of the **Map** page displays information for the selected link.
2. Click the **...** icon next to the link name and select **Change Channel** from the **Actions** dropdown list.



When you select **Change Channel**, a screen appears on the right side of the **Maps** page displaying the current channel number used by the selected link. The Maps section highlights the other links that are using the current channel number in that particular sector.



3. Select the channel number and click **Update**.

The **Confirm** message box appears, indicating that the channel change is applicable to the highlighted links.

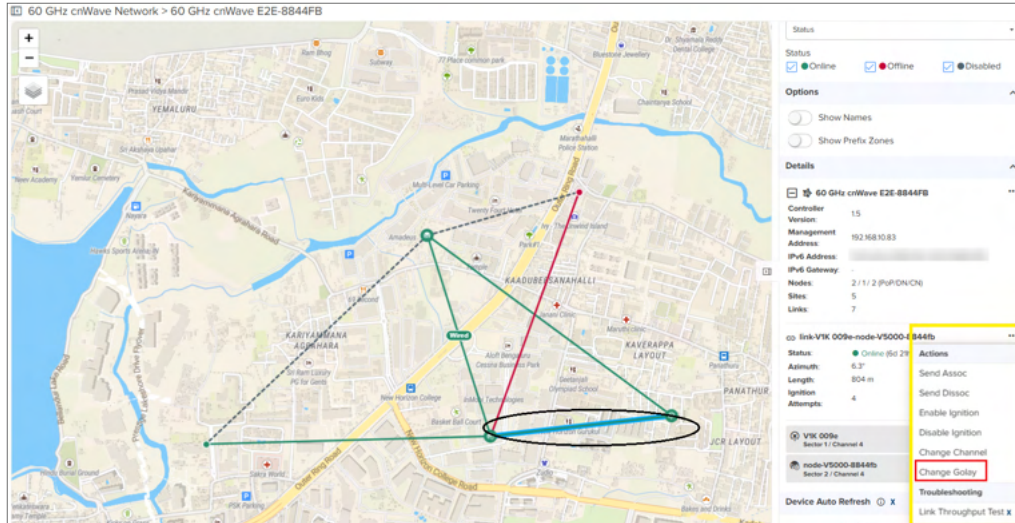
4. Click **Continue**.

A message appears, indicating the channel change is successful for the group of links in a sector.

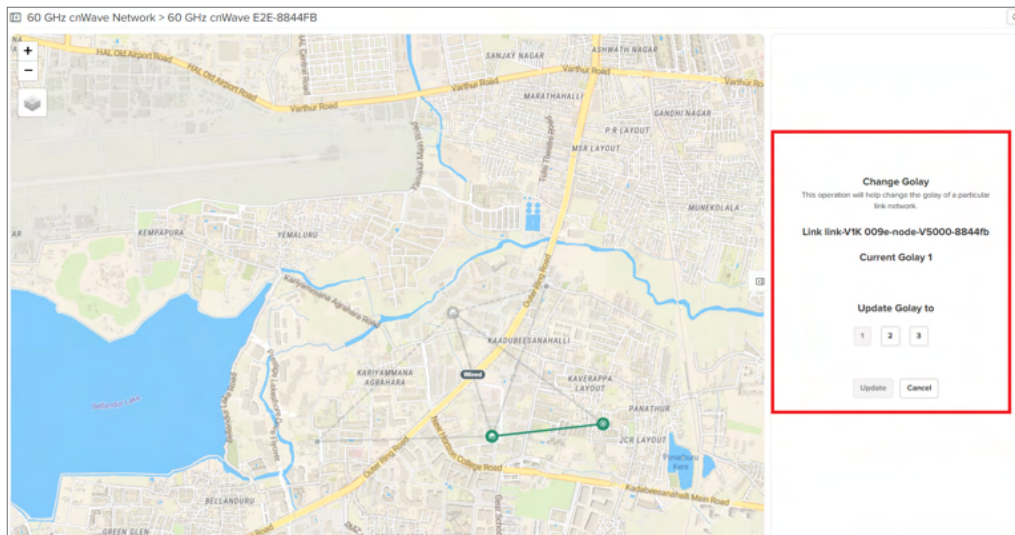
Change Golay

Using the **Maps** page in cnMaestro UI, you can change the Golay code for a **particular 60 GHz cnWave link** established between two nodes (not a sector) to avoid interference. Complete the following steps to change the Golay:

1. On the **Map** page, select a cnWave network and click on the link for which you want to change the Golay code. The **Details** section on the right side of the **Map** page displays information for the selected link.
2. Click the **...** icon next to the link name and select **Change Golay** from the **Actions** dropdown list.



When you select **Change Golay**, a screen appears on the right side of the **Maps** page displaying the current Golay code used by the selected link.



3. Select the required Golay code for the selected particular link.
4. Click **Update**.

The **Confirm** message box appears, indicating that the Golay change is applicable to the particular link.

5. Click **Continue**.

A message appears, indicating the Golay code change is successful for the particular link.

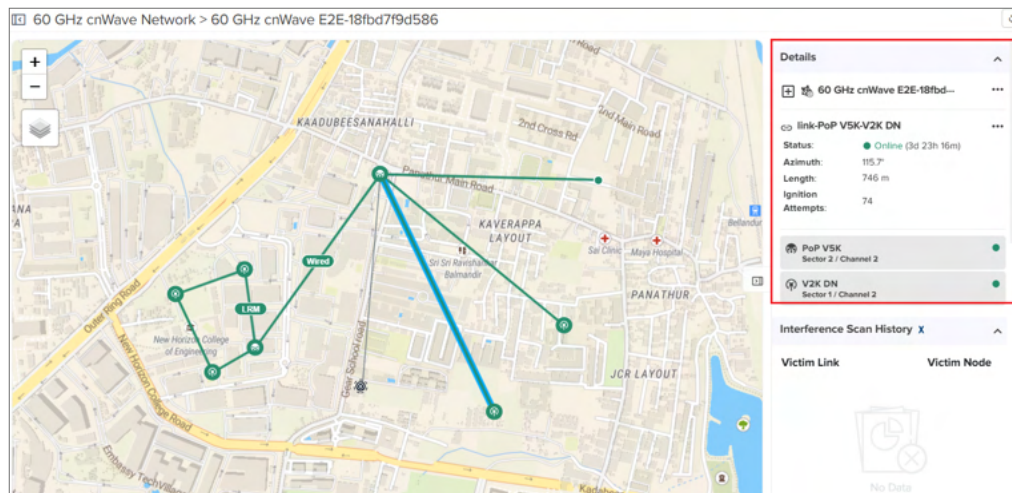
Setting the Last Resort Metric (LRM) for a cnWave 60 GHz link

You can set an extremely high Open/R metric for a wireless cnWave 60 GHz link using the **Maps** page in cnMaestro UI. This metric value is used as a last resort for routing traffic when all other paths are unavailable.

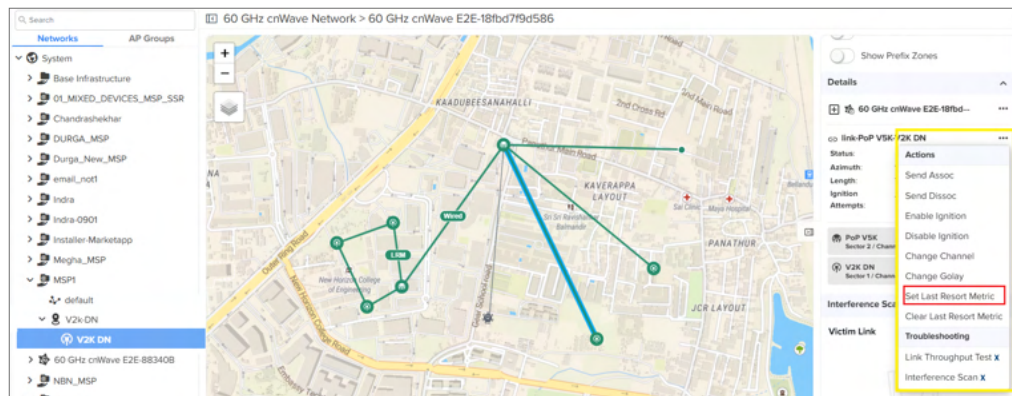
To set a last resort metric for a 60 GHz cnWave link, complete the following steps:

1. On the **Map** page, select a cnWave network and click on the link for which you want to set the last resort metric.

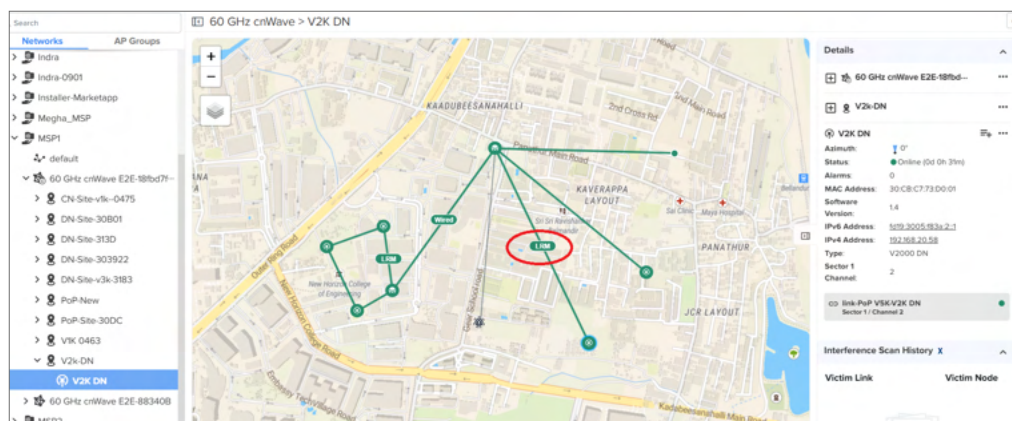
The **Details** section on the right side of the **Map** page displays information for the selected link.



2. Click the ... icon next to the link name and select **Set Last Resort Metric** from the **Actions** dropdown list.

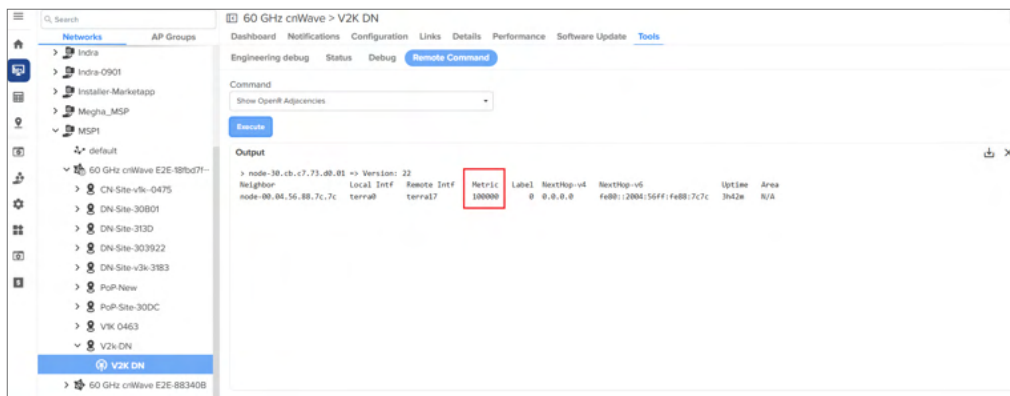


When you select the **Set Last Resort Metric** option, a message appears indicating that the last resort metric is set successfully. You can see an **LRM** indicator on the selected link, as shown in the figure below.



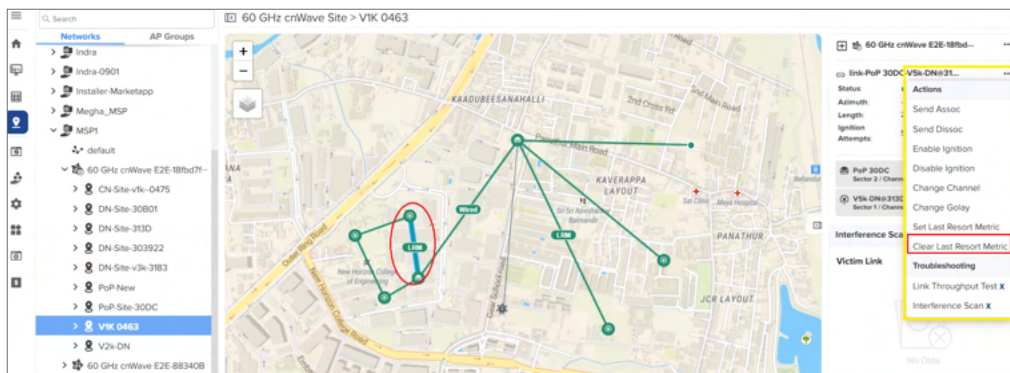
3. To verify the last resort metric that you set, navigate to the **Monitor and Manage > 60 GHz cnWave Network > Node > Tools > Remote Command**. The **Remote Command** page appears.
4. From the **Command** dropdown list, select **Show OpenR Adjacencies** and click **Execute**.

The **Remote Command** page displays the output, indicating the last resort metric value (which is 100000). This mechanism also indicates that the link with the highest metric value is the last preferred link for routing traffic when other links are unavailable.



For links that do not have the last resort metric set, the **Metric** field displays 1 as the value.

5. To **clear** the last resort metric for a link, select the required 60 GHz cnWave link on the **Maps** page.
6. Click the **...** icon next to the link name and select **Clear Last Resort Metric** from the **Actions** dropdown list.



When you select the **Clear Last Resort Metric** option, a message appears indicating that the last resort metric is cleared.

Tools

The Tools page allows the user to perform the following actions:

- [Operations](#)
- [Diagnostics](#)
- [Debug](#)
- [Remote Command](#)
- [Services](#)
- [Settings](#)

Operations

External E2E Controller deployment

If the device is deployed through **External E2E Controller** it displays the operations page as follows:

- **Restart E2E Controller** performs the **Restart**.
- A **System Backup and Restore** the entire state of a E2E Controller server as a file and file can be used to transfer data between two E2E Controller instances. It can be saved in local hard drive through the UI and restored into a new E2E Controller instance to re-create.
- The **Software Upgrade** is to upgrade E2E controller and can be done through E2E controller package.

Onboard E2E Controller deployment

If the device is running **Onboard E2E Controller** it displays the operations page as follows:

- **Operations** page allows the user to **Restart E2E Controller** and perform the **System Backup**. It also stores the entire state of a E2E Controller server as a file and file can be used to transfer data between two E2E Controller instances. It can be saved in local hard drive through the UI and restored into a new E2E Controller

instance to re-create the application state.

The screenshot shows the 'Tools' menu in the 60 GHz cnWave Network GUI. The 'Operations' sub-menu is active, displaying three sections: 'Restart E2E Controller', 'System Backup and Restore', and 'Onboard E2E Network to External E2E Network Migration'. The 'Restart E2E Controller' section has a 'Restart' button. The 'System Backup and Restore' section includes a 'Download' button for backup and a 'Restore' button next to a file selection input. The 'Onboard E2E Network to External E2E Network Migration' section contains a description, prerequisites (bullet points), warnings (triangle icons), and a 'Start Migration' button.

60 GHz cnWave Network > 85 onboard e2e

Dashboard Notifications Configuration Links Statistics Report X Software Update **Tools**

Operations Diagnostics Debug Remote Command Services Settings

Restart E2E Controller

Recommended to be used only by Cambium Support Team.

Restart

System Backup and Restore

A System Backup stores the entire state of a E2E Controller server as a file. This file can be downloaded to the local hard drive through the UI and restored into a new E2E Controller instance to re-create the application state.

Backup

Download

Restore

Select File

Restore

Onboard E2E Network to External E2E Network Migration

This migration will convert onboard E2E Controller network to a newly deployed external E2E Controller network by restoring the entire state of this onboard E2E Controller to external E2E Controller.

Prerequisites

- Applicable only on external E2E Controller running 1.2.2 version or later
- IPv6 reachability and routing configuration are the pre-requisites
- External E2E should have higher version than Onboard E2E
- PoP Devices IPv6 addresses must be connecting between each other

⚠ This will cause an outage of the network(s).

⚠ Migration to existing External E2E Controller will realign the existing seed prefix allocation of the nodes.

Start Migration

Onboard E2E to External E2E Migration

When you onboard an E2E Controller to External E2E Controller with or without sites, consider the following prerequisites:

- Applicable only on external E2E Controller running with 1.2.2 version or later.
- IPv6 reachability and routing configuration are pre-requisites.
- External E2E Controller should have higher version than Onboard E2E.
- PoP Devices IPv6 addresses must be connecting between each other.

When you onboard an E2E Controller to External E2E Controller with sites, consider the following prerequisites:

- Multiple Multi-PoP Networks must not be connected to same wired switch.
- Selected Onboard Network and External E2E Controller networks for migration should not have same site and device names.

Post Migration Steps:

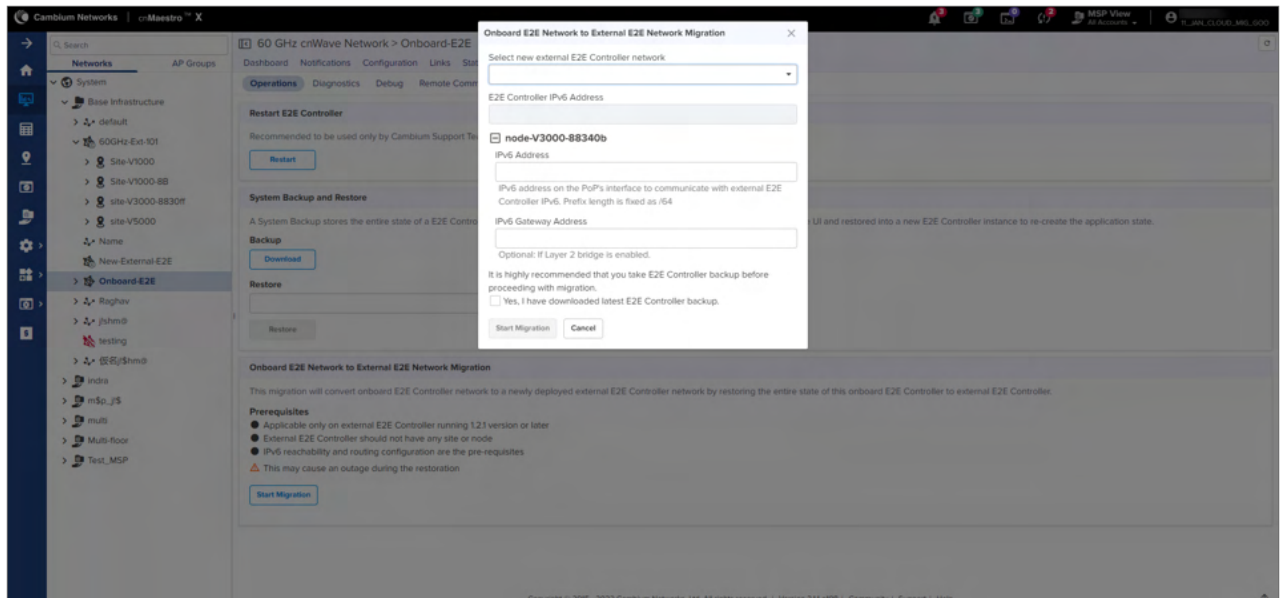
- Multi-PoP / Relay Port should be updated with the interface as in PoP interface configuration if not already done, to allow the connection between PoPs.
- If the existing E2E Network is configured with BGP, migrated PoP BGP Configuration must be updated in cnMaestro and then in POP GUI
- If the PoPs are not on the same L2 network:
 - Controller configuration about broadcast should be set to true.
 - If External E2E Controller and PoP devices are not connected/routed through a network router

- It is recommended to set Deterministic prefix algorithm
- Routes to each PoP with respective Seed Prefix should be added manually in E2E Controller.

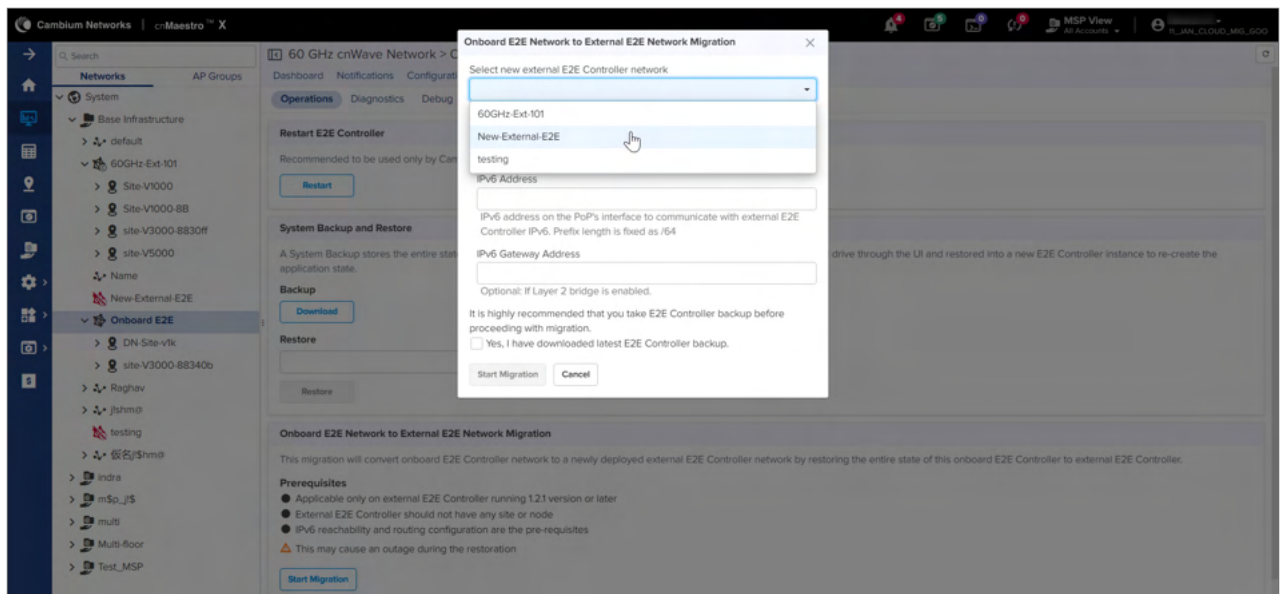
Perform the following steps to migrate Onboard E2E Controller to External E2E Controller:

1. Select Onboard E2E Network > **Tools** > **Operations**.
2. Click **Start Migration**.

The **Onboard E2E Controller to External E2E Migration** window appears.

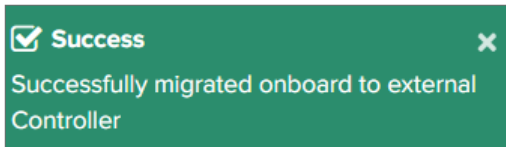


3. Select a new external E2E Controller network from the dropdown.

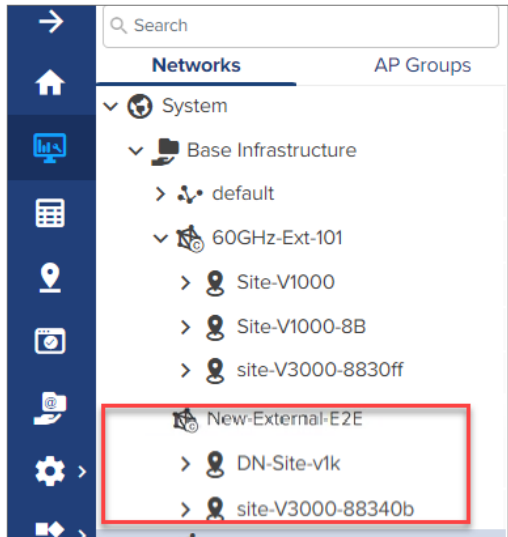


4. Enter **IPv6 Address**.
5. Enter **IPv6 Gateway Address** of PoP node, which is optional.
6. Select the checkbox next to **Yes, I have downloaded latest E2E Controller backup**.
7. Click **Start Migration**.

A successful message on migration process is displayed.



The Onboard E2E Controller network is migrated with all the sites and nodes into External E2E Controller, as shown below:



Fallback to Onboard E2E Network

The fallback process is applicable only for External E2E networks where Onboard to External E2E Network migrated. Perform the following steps to fallback to Onboard E2E Network after the migration from Onboard to External E2E Network.

1. Change the Controller IPv6 in the PoP from cnMaestro in External E2E Controller.
2. Go to PoP GUI and when the status displays as not connected, Enable Onboard E2E Controller.
3. Disconnect the External E2E controller from cnMaestro.
4. Delete the devices and sites in cnMaestro when the External Controller is offline, as they will conflict with Onboard E2E network devices when connected to cnMaestro.
5. In cnMaestro, approve the Onboard E2E network and restore the backup taken before the Migration.
6. Verify the Network and devices status in PoP device GUI and cnMaestro.

Scheduling configuration backup of E2E Controller

You can configure FTP or SFTP and schedule to backup the configuration of E2E Controller (onboard or external) using cnMaestro. The backup scheduling option allows you to schedule and save the automated configuration backup in a FTP or SFTP path (which you provided as an input during FTP or SFTP configuration). This scheduling option helps in availing the latest configuration backup and recovering the 60GHz cnWave network to the latest available configuration when E2E Controller crashes or rebuilt.



Note

- The scheduling option requires the SFTP or FTP configuration as the backups are uploaded to the SFTP or FTP remote path only.
- This backup scheduling option is supported for both Onboard and External E2E Controller deployments.

- FTP or sFTP Ports must be allowed in network firewall from a VM or device running E2E Controller service to the respective FTP or sFTP server.
- The backup scheduling option is supported in 5.1.0 Cloud and On-Premise cnMaestro release and 1.4 E2E Controller release.

To configure the FTP or sFTP settings and schedule the backup, complete the following steps:

1. From the **Home** page of cnMaestro, navigate to Monitor and Manage > E2E Network > Tools > Operations. The **Operations** page displays options to configure settings for E2E Controller.
2. In the **FTP Server Settings** section, configure a remote file server (FTP or sFTP) to upload the backups generated through the scheduled jobs.

The screenshot shows the 'Operations' page in the cnMaestro interface. The 'Scheduled Backup' section is highlighted with a yellow box and contains a table with backup schedules. The 'FTP Server Settings' section is highlighted with a red box and contains configuration fields for a remote file server.

Schedule	Date and Time	Status	Last Backup
<input checked="" type="checkbox"/> Daily Backup	05:53 PM	Scheduled (Apr 25, 2024 5:53 PM)	Failed (Apr 24, 2024 5:53 PM)
<input checked="" type="checkbox"/> Weekly Backup	05:57 PM Tuesday	Scheduled (Apr 30, 2024 5:57 PM)	Failed (Apr 23, 2024 5:57 PM)

FTP Server Settings
 Configure a remote file server (FTP/SFTP) to upload Backups generated through scheduled jobs.

Protocol
☒ FTP ☐ SFTP

Remote Host*

Port Number*

Username

Password

File Path*

Save

[Table 81](#) lists the parameters required for configuring the remote FTP or sFTP server.

Table 81 Parameters for FTP/sFTP server settings

Parameter	Description
Protocol	File protocol (FTP or sFTP) required for uploading the backup of E2E Controller over the network. Select the required protocol.
Remote Host	The remote host name of the FTP or sFTP file server. Provide IP or DNS resolvable host name in the text box. This is a mandatory parameter.
Port Number	The port number used to allow in network firewall from a VM or device running E2E Controller service to the respective FTP or sFTP server. This is a mandatory parameter.
Username	Username to log in to the remote FTP or sFTP server.

Table 81 Parameters for FTP/sFTP server settings

Parameter	Description
Password	Password that is required to authenticate the remote FTP or sFTP server.
File Path	The remote file path of FTP or sFTP server where the backups are uploaded automatically on scheduling.

3. Click **Save**.

The remote FTP or sFTP configuration is successfully updated.

4. To schedule the backup job, use the following options (either one or both) in the **Scheduled Backup** section:

- **Daily Backup:** For the daily backup, set the time (in 24-hours format) using the **Date and Time** parameter.
- **Weekly Backup:** For the weekly backup, set the time (in 24-hours format) and day.

The **Status** field in the **Scheduled Backup** section displays date and time of the scheduled job. Similarly, the **Last Backup** field displays date and time of the last failed job.

Diagnostics

Diagnostics page allows the user to gather Technical Support Dump and can be downloaded and sent to cambium support team.

All the events information of E2E controller can be viewed under E2E Events. In **E2E Events** tab user can view the **Event ID**, **Time**, **Device**, **Level**, **Source** and **Reason** of the E2E Network.

Figure 361 Diagnostics

Event ID	Time	Device	Level	Source	Reason
SET_LINK_STATUS	Aug 12 2021 17:37:10	v5k-DN-3039	INFO	ctrl-app-IGNITION_APP	Sending LINK_UP to link-vlk-CN-0463-v5k-DN-3039 View Details
LINK_STATUS	Aug 12 2021 17:37:08		ERROR	ctrl-app-TOPOLOGY_APP	link-vlk-CN-0463-v5k-DN-3039 is DOWN View Details
DRIVER_LINK_STATUS	Aug 12 2021 17:37:08	v5k-DN-3039	ERROR	minion-app-IGNITION_APP	Received LINK_DOWN for neighbor 12:04:56:8b:04:63 on interface terra17 (22:04:56:88:30:39) View Details
LINK_STATUS	Aug 12 2021 17:37:05		INFO	ctrl-app-TOPOLOGY_APP	link-vlk-CN-0463-v5k-DN-3039 is UP View Details
DRIVER_LINK_STATUS	Aug 12 2021 17:37:05	v5k-DN-3039	INFO	minion-app-IGNITION_APP	Received LINK_UP for neighbor 12:04:56:8b:04:63 on interface terra17 (22:04:56:88:30:39) View Details
MINION_SET_LINK_STATUS	Aug 12 2021 17:37:00	v5k-DN-3039	INFO	minion-app-IGNITION_APP	Sending assoc request for neighbor 12:04:56:8b:04:63 View Details
SET_LINK_STATUS	Aug 12 2021 17:37:00	v5k-DN-3039	INFO	ctrl-app-IGNITION_APP	Sending LINK_UP to link-vlk-CN-0463-v5k-DN-3039 View Details
LINK_STATUS	Aug 12 2021 17:36:58		ERROR	ctrl-app-TOPOLOGY_APP	link-vlk-CN-0463-v5k-DN-3039 is DOWN View Details
DRIVER_LINK_STATUS	Aug 12 2021 17:36:58	v5k-DN-3039	ERROR	minion-app-IGNITION_APP	Received LINK_DOWN for neighbor 12:04:56:8b:04:63 on interface terra17 (22:04:56:88:30:39) View Details
LINK_STATUS	Aug 12 2021 17:36:56		INFO	ctrl-app-TOPOLOGY_APP	link-vlk-CN-0463-v5k-DN-3039 is UP View Details

Debug

In **Debug** tab, you can view and download the Node logs by executing the following log:

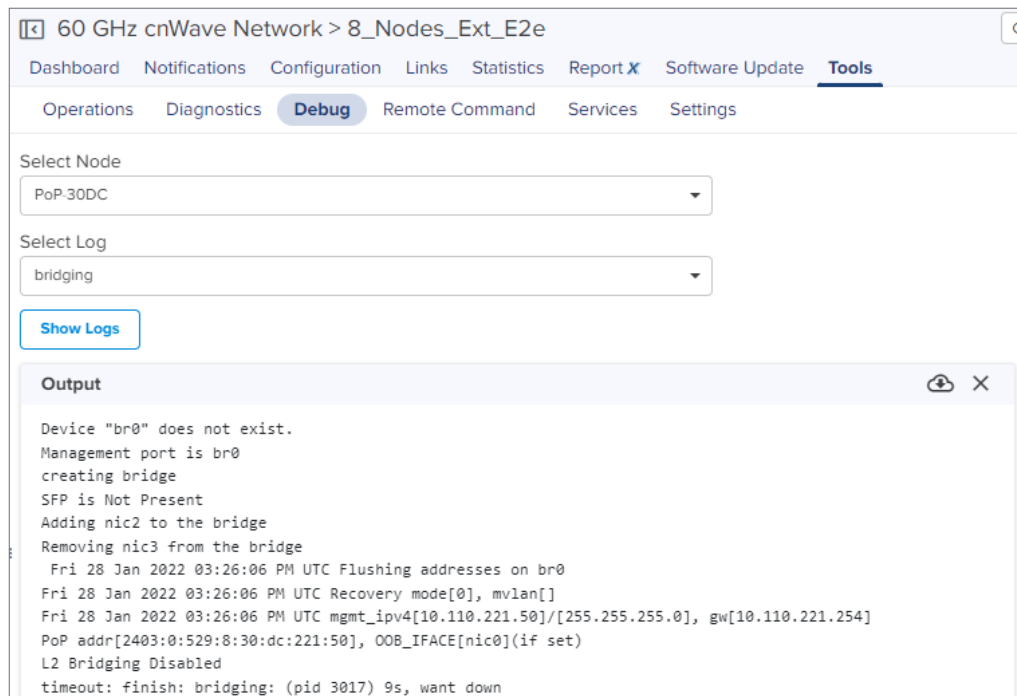
- bridging
- e2e_minion
- openr
- pop_config (available for PoP device)

- exabgp (available for PoP device)
- cnAgent (available for Onboard PoP device)
- e2e_controller (available for Onboard PoP device)

To view the logs:

1. Navigate to **Tools > Debug**.
2. Select a node name from the **Select Node** dropdown.
3. Select the required log name from the **Select Log** dropdown.
4. Click **Show Logs**.

The output for the selected criteria appears as shown:



- Click download (📄) icon to download the generated output.
- Click clear (X) icon to clear the output.

Remote Command

In **Remote Command** tab, user can view or download command logs by executing the following command:

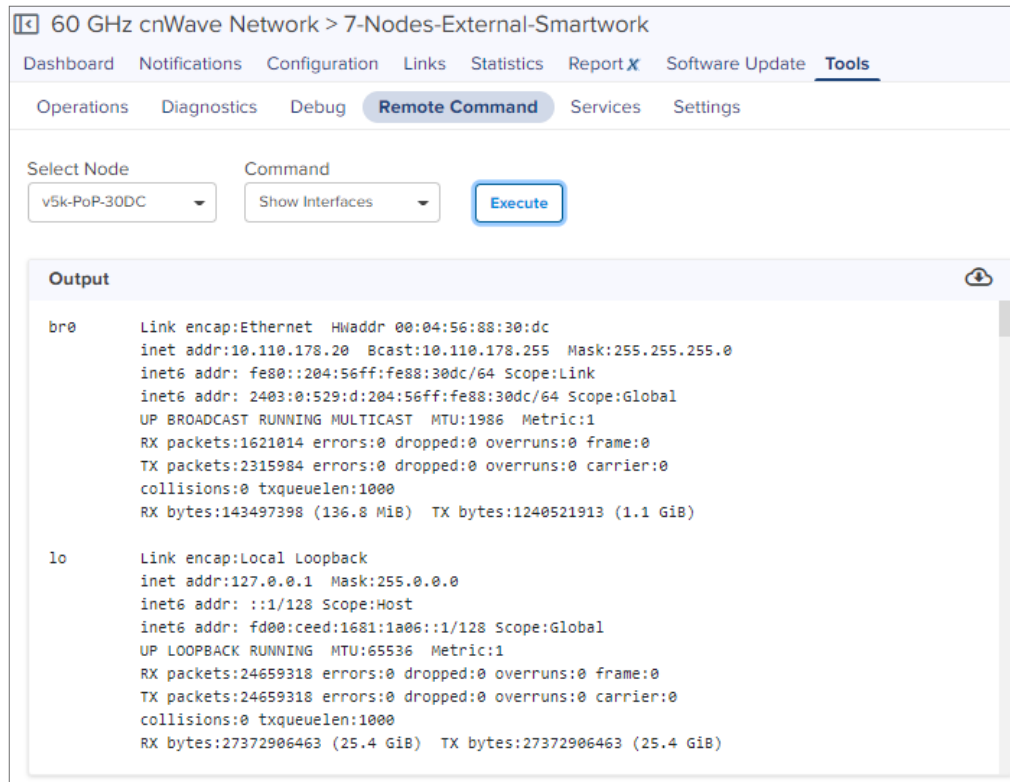
- Ping
- Show DHCP client lease (Applicable for only PoP node)
- Show IGMP Membership Table
- Show Interfaces
- Show IPv4 Neighbors
- Show IPv6 Neighbors
- Show MAC Address Table
- Show OpenR Adjacencies
- Show OpenR Prefixes

- Show Routes
- Show SFP Power Details (applicable for V5000 and V3000)
- Show Wired Interface State Changes

To execute the command:

1. Navigate to **Tools > Remote Command**.
2. Select a node name from the **Select Node** dropdown.
3. Select the required command from the **Command** dropdown.
4. Click **Execute**.

The output for the selected criteria appears as shown:



5. Click the download (📄) icon to download the generated output.
6. Click the clear (X) icon to clear the generated output.

To execute Ping command, perform the following steps:

1. Select the **Ping** command from dropdown.
2. Select **Node** or type of **IP address** (IPv4 or IPv6).
3. Select the following options:
 - Destination Node
 - Number of packets minimum 1 to maximum 10 (-c)
 - Buffer Size minimum 1 to maximum 65507 (-s)
4. Click **Start Ping**.

Output is displayed, as shown in [Figure 362](#).

Figure 362 Remote Command: Ping

60 GHz cnWave Network > Ext-E2E-102

Dashboard Notifications Configuration Links Statistics Report X Software Update **Tools**

Operations Diagnostics Debug **Remote Command** Services Settings

Select Node
DN-AADD

Command
Ping

☒ Node ☐ IPv4 ☐ IPv6

Destination Node
PoP

Number of Packets (-c)
3 Min = 1, Max = 10

Buffer Size (-s)
56 Min = 1, Max = 65507

Start Ping

Output

```

PING fd00:ceed:139b:1803::1(fd00:ceed:139b:1803::1) 56 data bytes
64 bytes from fd00:ceed:139b:1803::1: icmp_seq=1 ttl=64 time=0.366 ms
64 bytes from fd00:ceed:139b:1803::1: icmp_seq=2 ttl=64 time=2.47 ms
64 bytes from fd00:ceed:139b:1803::1: icmp_seq=3 ttl=64 time=0.976 ms

--- fd00:ceed:139b:1803::1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.366/1.269/2.465/0.881 ms

```

Services

In **Services** page user can view the services running in E2E Controller.

Figure 363 Services

60 GHz cnWave Network > 8_Nodes_Ext_E2e						
Dashboard Notifications Configuration Links Statistics Report X Software Update Tools						
Operations Diagnostics Debug Remote Command Services Settings						
Name	Version	Status	Uptime	CPU	Memory	
api_service	1.2.1	Running	32d 5h 29m	0.00%	0.31% [12.14MB]	
chihaya	v2.0.0-rc.2	Running	46d 22h 57m	0.01%	0.11% [4.457MB]	
cn-auto-routes	stable	Running	46d 22h 57m	6.11%	0.21% [8.34MB]	
cnagent	1.2.1-r4	Running	27d 4h 29m	0.09%	0.61% [24.06MB]	
e2e_controller	1.2.1	Running	32d 5h 29m	0.28%	9.13% [360.2MB]	
elasticsearch	7.9.0	Running	46d 22h 57m	6.93%	68.53% [1.371GB]	
fluentd	1.11-1	Running	46d 22h 57m	1.66%	3.81% [150.2MB]	
kibana	7.9.0	Running	46d 22h 57m	0.31%	6.93% [273.5MB]	
nms_aggregator	1.2.1	Running	32d 5h 28m	0.59%	0.70% [27.76MB]	
proxy-nginx	1.18.0	Running	32d 5h 27m	0.27%	0.10% [4.121MB]	
stats_agent	1.2.1	Running	32d 5h 29m	0.27%	0.30% [11.77MB]	
v6nat	stable	Running	46d 22h 57m	0.08%	0.13% [5.078MB]	

Settings



Note

E2E Settings are not applicable for Onboard E2E Controller deployment.

External E2E Controller deployment

External E2E Network displays the **Settings** page as follows:

Remote SSH Management allows the user to enable and disable **Remote SSH Management**.

The screenshot shows the 'Settings' page for a 60 GHz cnWave Network. The page is divided into two main sections: 'Network Configuration' and 'Remote SSH Management'.

Network Configuration

- E2E Controller IPv6 Address (eth0)**: A text field containing '2403:0:529:da00:27fe0t:212164'. A 'Generate' button is next to it. A note states: 'Changing IPv6 Address will disconnect all the nodes. E2E Controller Address configured in the PoP nodes should match.'
- IPv6 Routes**: A checkbox labeled 'Auto Manage Routes' is checked. A note states: 'Automated IPv6 Routes to DNs and CNs based on topology and PoP nodes status. Applicable only if PoP nodes and E2E Controller are in same Network/Prefix length.'
- Table**: A table with columns 'Destination', 'Gateway', and 'Type'. It has two rows: 'default' with 'dynamic' type, and an empty row with 'auto' type. An 'Add New' button is in the top right.
- Save**: A button at the bottom.

Remote SSH Management

- Disable**: A button.

Configure NTP Server

- Enabled**: A checkbox that is checked.
- NTP Server 1**: A text field containing 'time.google.com'.
- NTP Server 2**: A text field containing 'time.nist.gov'.
- NTP Server 3**: An empty text field.
- NTP Server 4**: An empty text field.
- Current System Time**: 'Thu, 12 Aug 2021 12:13:46 UTC'.
- Status**: 'In Sync'.
- Save**: A button at the bottom.

In **Network Configuration** user can configure the **E2E Controller IPv6 Address** and **IPv6 Routes**.

To change **E2E Controller IPv6 Address**, perform the following:

1. Navigate to **Tools > Settings > Network Configuration** tab.
2. Click **Generate** to automatically generate IPv6 address or manually change the IPv6 Address of E2E Controller.
3. Click **Save**.

To configure **IPv6 Routes**, perform the following:

You can also enable the **Auto Manage Routes**. This automates IPv6 Routes to DNs and CNs based on the topology and PoP nodes status. It is applicable only if PoP nodes and E2E Controller are in same Network/Prefix length.

If IPv6 routes is enabled as **Auto Manage Routes**, **Type** field displays as **Auto**.

To Enable Auto Managed Routes:

1. Navigate to **Tools > Settings > Network Configuration** tab.
2. Enable **Auto Manage Routes**.
3. Click **Save**.

Network Configuration

E2E Controller IPv6 Address (eth0)
2403:0:529:d:a00:27ff:1a01:212164 [Generate](#) Changing IPv6 Address will disconnect all the nodes. E2E Controller Address configured in the PoP nodes should match.

☒ IPv6 Routes
☒ Auto Manage Routes Automated IPv6 Routes to DNIs and CNIs based on topology and PoP nodes status. Applicable only if PoP nodes and E2E Controller are in same Network/Prefix length.

Destination	Gateway	Type	
default	fe80::ce16:7eff:fe6e:5b7f	dynamic	
fd00::ced:1681:1a00::56	2403:0:529:d:204:56ff:fe88:30dc	auto	

[Save](#)

To retain auto-managed routes, even after auto-managed routes is disabled, complete the following steps:

1. Navigate to **Tools > Settings > Network Configuration** tab.

Network Configuration

E2E Controller IPv6 Address (eth0)
2403:0:529:d:a00:27ff:1a01:212164 [Generate](#) Changing IPv6 Address will disconnect all the nodes. E2E Controller Address configured in the PoP nodes should match.

☐ IPv6 Routes
☐ Auto Manage Routes Automated IPv6 Routes to DNIs and CNIs based on topology and PoP nodes status. Applicable only if PoP nodes and E2E Controller are in same Network/Prefix length.
☒ Retain Auto-Managed Routes

Destination	Gateway	Type	
default	fe80::ce16:7eff:fe6e:5b7f	dynamic	
fd00::ced:1681:1a00::56	2403:0:529:d:204:56ff:fe88:30dc	auto	

[Save](#)

2. Enable **Retain Auto-Managed Routes**.
3. Click **Save**.

Please Wait ...

Deactivating Auto Manage Routes

Progress bar

4. Please wait pops-up.

Once the Auto Manage Routes is disabled, IPv6 routes can be managed through static routes and in type it displays as **Static**.

Network Configuration

E2E Controller IPv6 Address (eth0)
2403:0:529:d:a00:27ff:1a01:212164 [Generate](#) Changing IPv6 Address will disconnect all the nodes. E2E Controller Address configured in the PoP nodes should match.

☐ IPv6 Routes
☐ Auto Manage Routes Automated IPv6 Routes to DNIs and CNIs based on topology and PoP nodes status. Applicable only if PoP nodes and E2E Controller are in same Network/Prefix length.

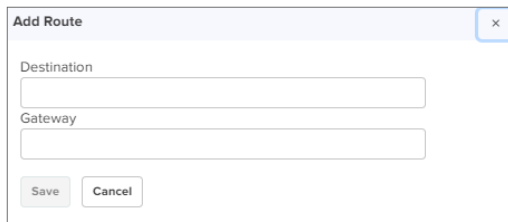
Destination	Gateway	Type	
default	fe80::ce16:7eff:fe6e:5b7f	dynamic	
fd00::ced:1681:1a00::56	2403:0:529:d:204:56ff:fe88:30dc	static	

[Save](#)

5. Click **Save**.

To add new static **IPv6 Routes**:

1. Click **Add New**.

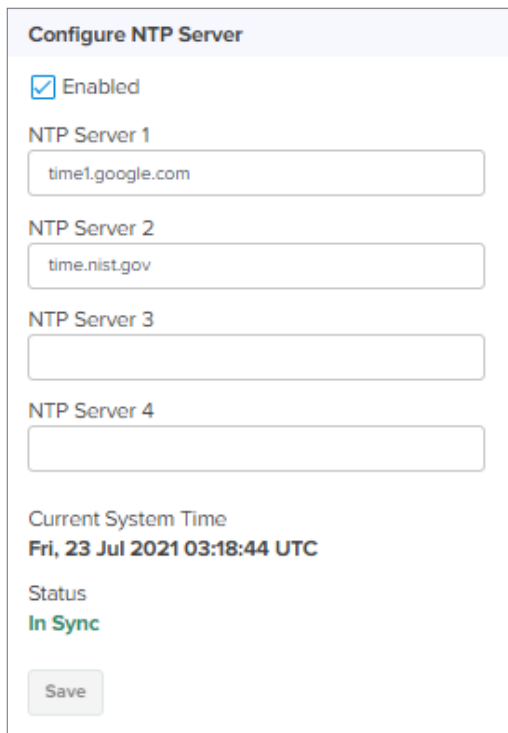
A dialog box titled "Add Route" with a close button (X) in the top right corner. It contains two text input fields: "Destination" and "Gateway". Below the fields are two buttons: "Save" and "Cancel".

2. Enter **Destination** and **Gateway**.
3. Click **Save**.

The user can configure the **NTP Settings** to configure the time configuration of the server with hostname or IP address.

To configure the NTP server:


1. Navigate to **Tools > Settings > NTP Settings** tab.
2. Enable the **NTP Settings**.
3. Enter **Host Name** or **IP Address**. It displays **Current System Time** and **Status** of the server.

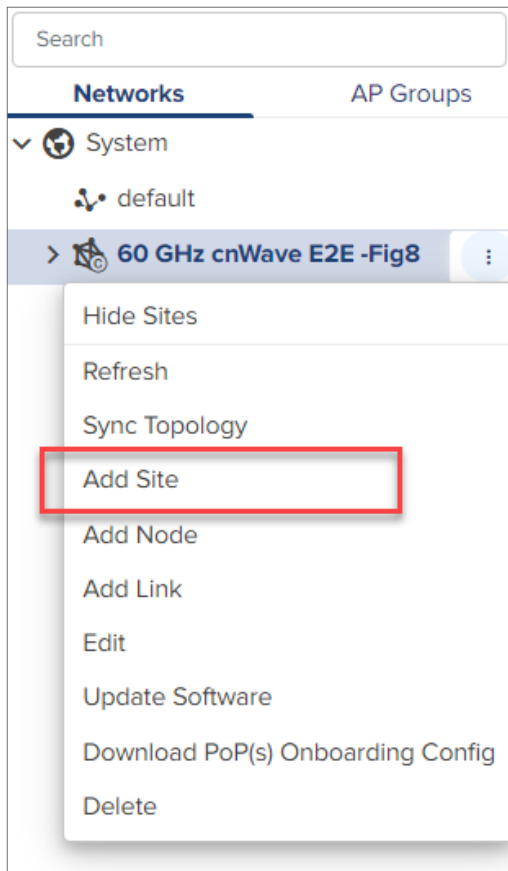
A dialog box titled "Configure NTP Server". It features a checkbox labeled "Enabled" which is checked. Below this are four text input fields for "NTP Server 1", "NTP Server 2", "NTP Server 3", and "NTP Server 4". The first two fields contain the text "time1.google.com" and "time.nist.gov" respectively. Below the input fields, it displays "Current System Time" as "Fri, 23 Jul 2021 03:18:44 UTC" and "Status" as "In Sync". A "Save" button is located at the bottom.

Site Configuration

Sites are located within the networks and wireless access points attached to it.

To Add a Site

1. Navigate to **Network** and click  icon.
2. Select **Add Site** from the dropdown.



3. Enter the **Name**, **Altitude**, and **Accuracy**.
4. Once the address is entered in the Map, Latitude and Longitude gets fetched automatically. You can also enter the details Manually.

The 'Add Site' dialog box is shown. It contains the following fields and controls:

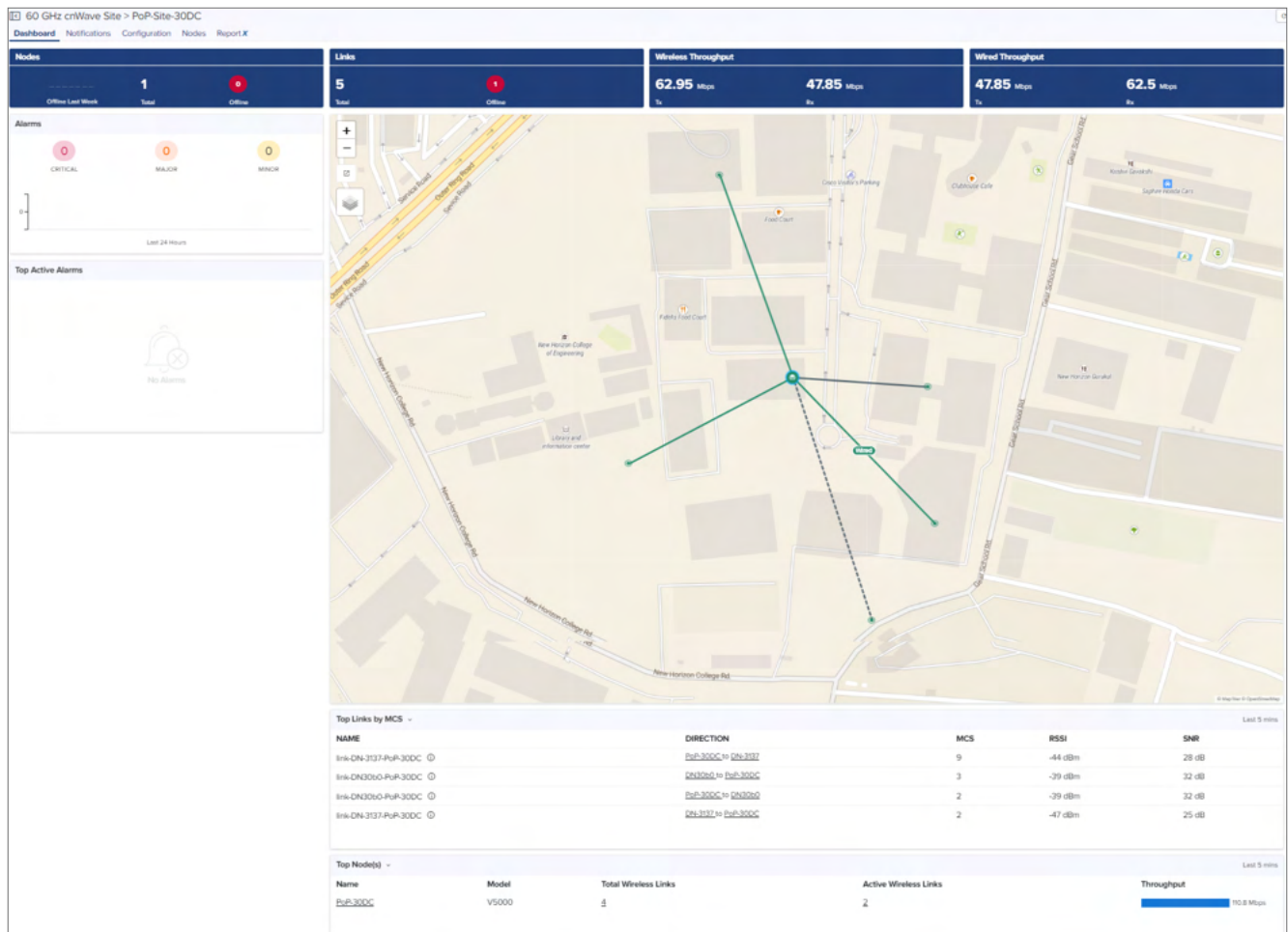
- Network:** 60 GHz cnWave E2E-883083
- Name:** (empty text field)
- Altitude:** (empty text field)
- Altitude description:** The altitude of the site (in meters above WGS84 ellipsoid).
- Accuracy:** 10000
- Accuracy description:** The accuracy of the given position (in meters).
- Latitude:** (empty text field) with a range of Min = -90, Max = 90
- Longitude:** (empty text field) with a range of Min = -180, Max = 180
- Map:** A map of India with a search bar labeled 'Search Address'. The map shows Nagpur, Bhilai, and Chandrapur.
- Buttons:** 'Save' and 'Cancel' buttons at the bottom.

5. Click **Save**. When the Site is configured it gets added under the E2E Network.


Site Dashboard

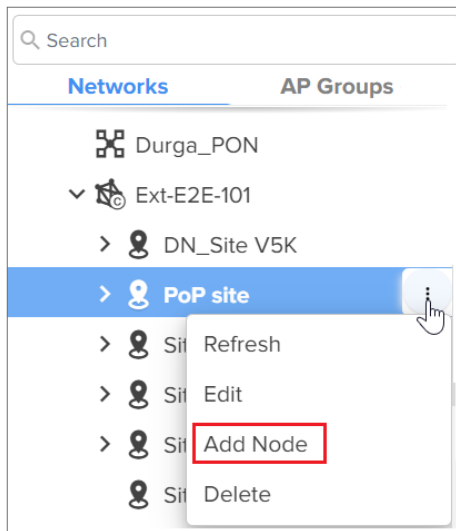
Dashboard pages are customized for each device type and aggregation level. The Site dashboard section displays the **Nodes**, **Links**, **Wireless Throughput**, **Wired Throughput**, **Alarms**, **Top Active Alarms**, **Top Links by MCS**, **Top Links by RSSI**, **Top Links by SNR**, **Top Node(s)**, **Top PoP(s)**, **Top DN(s)**, and **Top CN(s)**.

Figure 364 Site Dashboard



Node Configuration

Node can be configured through the **Site Menu** option by clicking the  icon in **Network** or **Site** tree menu or through **Network > Site > Nodes** and click **Add Node**.

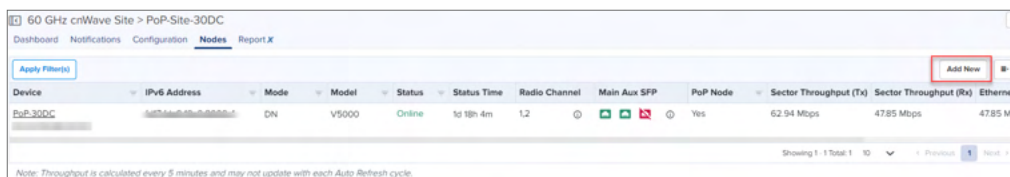


Note

From 3.1.1 release V2000 device (beta version) is supported.

To Add a Node:

1. Navigate to the **Network > Site > Nodes**.



Add Node window pops-up.

2. Click **Add new**.

Add Node

Name

Network

Ext-E2E-100

Site

Mode

☒ DN
 ☐ CN

☐ PoP Node

Serial Number

Azimuth

0

Antenna Tilt

0

IPv4 Management

Save

Cancel

3. Click  to add site.

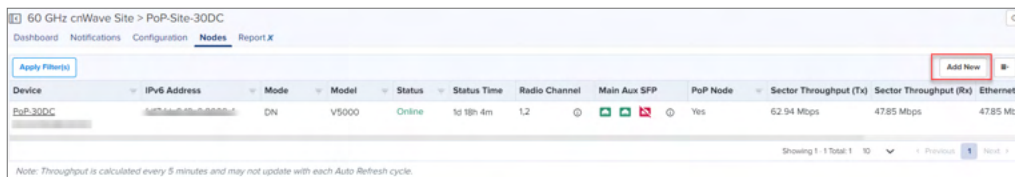
Adding the Node allows the user to create the different Nodes as shown below:

- PoP Node
- DN
- CN

PoP Node configuration

To add a PoP Node:

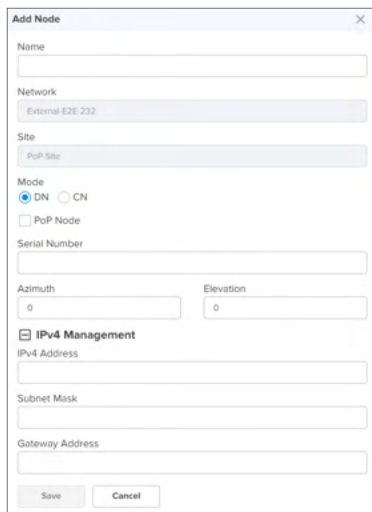
1. Navigate to the **Network > Site > Nodes**.
2. Click **Add New**.



Device	IPv6 Address	Mode	Model	Status	Status Time	Radio Channel	Main Aux SFP	PoP Node	Sector Throughput (Tx)	Sector Throughput (Rx)	Ethernet
PoP-30DC	2001:db8::1	DN	V5000	Online	1d 18h 4m	1.2	Yes	Yes	62.94 Mbps	47.85 Mbps	47.85 Mbps

Note: Throughput is calculated every 5 minutes and may not update with each Auto Refresh cycle.

3. **Add Node** window pops-up.



Add Node

Name:

Network:

Site:

Mode: ☒ DN ☐ CN

☒ PoP Node

Serial Number:

Azimuth: Elevation:

☒ IPv4 Management

IPv4 Address:

Subnet Mask:

Gateway Address:

Save Cancel

4. Enter the **PoP Name**, select the Mode **DN**.
5. Enable **PoP Node**.



Note

Once the PoP Node is enabled user needs to select the **Routing** and **Interface** details.

6. Enter the **Serial Number**.
7. Enter the **Azimuth** and **Elevation**.
8. In the **PoP Configuration** select **BGP** or **Static Routing**.
9. In **Interface** select **Aux** or **Main** or **SFP** or **Disabled**.

10. Enter the **IPv6** and **Gateway Addresses**.



Note

Generate IPv6 provides **Seed Prefix** in CIDR format from which subnet prefixes are allocated to all DNs and CNs (e.g. fdce:b00c:cafe:ba00::/56)

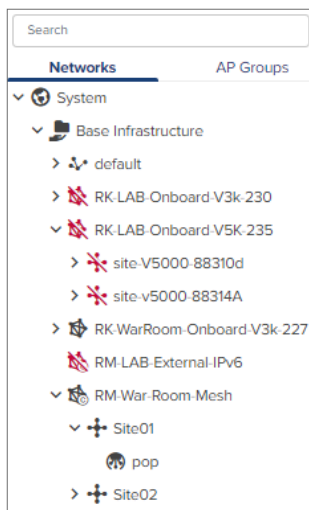
11. In IPv4 Management, enter the **IPv4 Address**, **Subnet Mask** and **Gateway Address**.
12. Click **Save**.



Note

Once the PoP Node is configured, **PoP(s) Onboarding Config.json** file gets downloaded automatically, which can be used to import and configure in the PoP Node UI.

Once the **PoP** node is configured it gets listed under the **Site**.



DN/CN Node configuration

To add DN/CN node:

1. Navigate to the **Network > Site > Nodes**.
2. Click **Add New**.

60 GHz cnWave Site > PoP-Site

Dashboard Notifications Configuration **Nodes** Report X

Search

Add New

Device	IPv6 Address	Mode	Model	Status	Status Time	Sync Mode	Radio Channel	Main Aux SFP	PoP Node	Fix Type
y5k-PoP-3840 00:04:56:88:38:40		DN	V5000	Online	0d 0h 20m	GPS	1.3	⊕ ⊗ ⊗	Yes	3D

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

3. **Add Node** window pops-up.

Add Node

Name

Network
External E26-232

Site
PoP-Site

Mode
☒ DN ☐ CN
☐ PoP Node

Serial Number

Azimuth
0

Elevation
0

IPv4 Management

IPv4 Address

Subnet Mask

Gateway Address

Save Cancel

4. Enter the **Node Name**, select the Mode **DN** or **CN**.

5. Enter the **Serial Number**.

6. Enter the **Azimuth** and **Elevation**.

Add Node

Name

Network
External E26-232

Site
PoP-Site

Mode
☒ DN ☐ CN
☐ PoP Node

Serial Number

Azimuth
0

Elevation
0

IPv4 Management

IPv4 Address

Subnet Mask

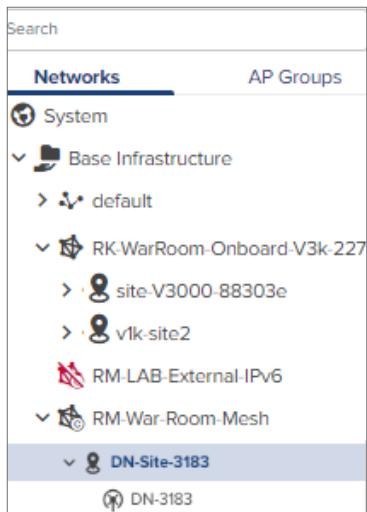
Gateway Address

Save Cancel

7. In IPv4 Management enter the **IPv4 Address**, **Subnet Mask** and **Gateway Address**.

8. Click **Save**.

9. Once the **DN/CN** node is configured, it gets listed under the Site.



Replace Node

Replace Node allows to replace the existing faulty nodes with new nodes along with the configuration and links of existing faulty nodes.




Note

New node should be replaced with same model as existing node.

To replace Node:

1. Navigate to **Node** tree menu and select the node.



2. Click  icon and Select **Replace Node** from the dropdown.
3. **Replace Node** window pops-up.

Replace Node

Current MAC address

00:04:56:88:31:22

New Serial number

ⓘ Device types should be same

Save

Cancel

4. Enter the **New Serial number**.

5. Click **Save**.

PoP Node

Once the PoP node is configured it displays the monitoring panel of the PoP node.

Dashboard

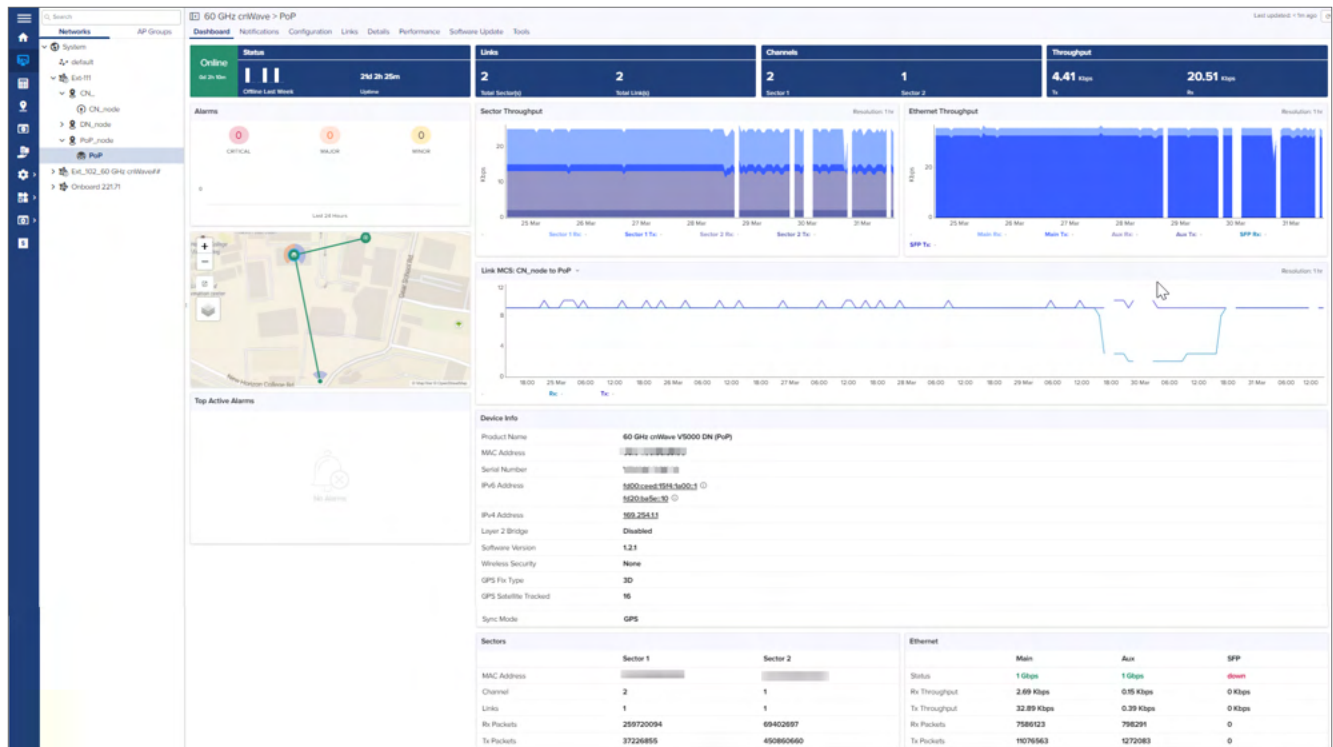
Dashboard pages can be customized for each device type and aggregation level. The PoP node dashboard section displays the **Status, Links, Channels, Throughput, Sector Throughput (Sector 1 and Sector 2), Ethernet Throughput (Main, Aux, SFP), Alarms, Top Active Alarms, Link MCS, Device Info, Sectors, and Ethernet**.



Note

- Sector Throughput (sector1) for V3000, V2000 and V1000.
- Sector Throughput (sector1 and sector2) for V5000.
- Ethernet Throughput graph with Main for V1000.
- Ethernet Throughput graph with Main, Aux, SFP for V5000 and V3000.
- Ethernet Throughput graph with Main and Aux for V2000.

Figure 365 PoP Node Dashboard



Configuration

Basic

It displays the basic details of PoP node such as **Name**, **Description**, **MAC Address**, **Azimuth**, and **Elevation**. It also allows to edit the name of the node.

Figure 366 Basic

The Basic configuration page allows users to edit the following fields:

- Name:** PoP-Onboard-V5k-3083
- Description:** (Empty field)
- MAC Address:** 00:04:56:88:30:83
- Azimuth:** 33
- Elevation:** 0

Buttons: Save, Reset

Radio

It allows the user to configure the **EIRP**, **Adaptive Modulation**, **Sectors (channels, Polarity and Link(s) Golay)**, and **GPS**.



Note

Antenna and PTP deployment Range options is available only for v3000.

Figure 367 Radio

60 GHz cnWave > PoP-30DC

DashboardNotificationsConfigurationLinksDetailsPerformanceSoftware UpdateTools

BasicRadioNetworkVLANSecurityAdvanced

EIRP

Maximum EIRP

Allowed range is 13 dBm to 38 dBm

IBF Transmit Power

☒ Short range (<25m) optimized ☐ Long range optimized Initial Beam Forming transmit power setting

Adaptive Modulation

Minimum MCS

Range - [2, 12]

Maximum MCS

Range - [2, 12]

Sector 1

Channel/Polarity should originate from leaf nodes. Please make sure to change on the CNs first and then higher up on the DNs.

Override	Name	Auto Configuration	Node Configuration
<input checked="" type="checkbox"/>	Channel	2	<input type="text" value="1"/>
<input type="checkbox"/>	Polarity	Even	<input type="text"/>

Sector 1 Link (s) Golay

Override	Name	Auto Configuration (Rx/Tx)	Node Golay Rx/Tx
<input type="checkbox"/>	link-CN-0463-PoP-30DC	1/1	<input type="text"/>
<input type="checkbox"/>	link-DN30b0-PoP-30DC	1/1	<input type="text"/>

Override All

Sector 2

Channel/Polarity should originate from leaf nodes. Please make sure to change on the CNs first and then higher up on the DNs.

Override	Name	Auto Configuration	Node Configuration
<input checked="" type="checkbox"/>	Channel	2	<input type="text" value="2"/>
<input checked="" type="checkbox"/>	Polarity	Even	<input type="text" value="Odd"/>

Sector 2 Link (s) Golay

Override	Name	Auto Configuration (Rx/Tx)	Node Golay Rx/Tx
<input type="checkbox"/>	link-DN-3137-PoP-30DC	1/1	<input type="text"/>
<input type="checkbox"/>	link-DN-3183-PoP-30DC	1/1	<input type="text"/>

Override All

GPS

☐ Force GPS Disable GPS sync at initiator/responder during assoc

Save

Reset

For V3000, MCS 13 is supported as seen the following UI:

60 GHz cnWave > V3K DN

Dashboard
Notifications
Configuration
Links
Details
Performance
Software Update
Tools

Basic
Radio
Network
VLAN
Security
Advanced

+ EIRP
+ Antenna
+ PTP Deployment Range
- Adaptive Modulation

Minimum MCS
Range - [2, 13]

Maximum MCS
Range - [2, 13]

+ Sector 1
+ Sector 1 Link (s) Golay
+ GPS

Save
Reset

Network

Network tab allows the user for the **PoP configuration**, **E2E Controller Configuration**, **BGP Configuration**, **IPv6 Layer 3 CPE**, **IPv4 Management**, **OOB**, **Other Settings (Multi-PoP or Relay Port, Enable Aux port power)**, **PTP External Failover**, **Ethernet Ports**, and **1G SFP**.



Note

When Layer 2 Bridge is enabled in E2E Controller, Layer 2 Bridge option will be available in PoP Network Configuration

Figure 368 Network

60 GHz cnWave > PoP2 V3x

Dashboard Notifications **Configuration** Links Details Performance Software Update Tools

Basic Radio **Network** VLAN Security Advanced

PoP Configuration

Routing
☐ Border Gateway Protocol (BGP) Routing ☒ Static Routing

Interface
☐ Aux ☒ Main ☐ SFP ☐ Disabled The interface that the PoP node uses to communicate with the upstream router

IPv6 Gateway Address
 A configured IPv6 Gateway Address must be reachable from the PoP for the system to function. This address can be left blank when layer 2 bridging is enabled.

IPv6 Address*
 IPv6 address on the interface that the PoP node uses to communicate with the upstream router. Prefix length is fixed as /64.

BGP Configuration

Local ASN
 The autonomous system number (ASN) assigned to the PoP nodes.

KeepAlive
 The BGP keepalive period in seconds.

IPv6 Layer 3 CPE

IPv6 CPE interface
☐ Aux ☒ Main ☐ SFP ☒ Disabled
 Choose the interface to run IPv6 SLAAC. Subnet allocated by the controller will be used as used as Prefix. This interface will not be part of Layer 2 bridge. Should be disabled for IPv4 CPE.

IPv4 Management

IP Assignment
☒ Static ☐ DHCP If the DHCP server is unreachable, the configured IP will serve as the fallback IP.

IPv4 Address
 IPv4 Management address is not accessible over Relay port (except for PoP interface), OOB interface and IPv6 CPE interface.

Subnet Mask

Gateway IP Address

Ethernet Ports

☒ Enable Main
☒ Enable Aux
☒ Enable SFP

10 SFP

☒ Enable 10Gbps SFP autoconfiguration This option will only have an effect when using a 10Gbps SFP module.

Other Settings

☐ Enable Aux port power Enables the power out on the Aux port

Multi-PoP / Relay Port

☒ Aux ☐ Main ☐ SFP ☐ Disabled
 Wired interface on which OpenR is run. Should be used when OMs are connected back to back and on PoPs in a multi-PoP network.

OOB

OOB interface
☐ Aux ☐ Main ☐ SFP ☒ Disabled
 Out of band management interface to access the device. Management VLANs will be bypassed and data traffic will not be routed or bridged on this interface.

PTP External Follower

External Follower Link
☐ Aux ☐ Main ☐ SFP ☒ Disabled

Configure the Network as shown below:

1. Navigate to the **Configuration > Network**.
2. In **PoP Configuration**:
 - Select the appropriate option in **Routing** and **Interface**.
 - Enter the **IPv6 Address**.
 - Enter **IPv6 Gateway Address** its optional.

60 GHz cnWave > PoP-Onboard-V5x-3083

Dashboard Notifications **Configuration** Links Details Performance Software Update Tools

Basic Radio **Network** VLAN Security Advanced

PoP Configuration

Routing
☐ Border Gateway Protocol (BGP) Routing ☒ Static Routing

Interface
☐ Aux ☒ Main ☐ SFP ☐ Disabled The interface that the PoP node uses to communicate with the upstream router

IPv6 Address
 IPv6 address on the interface that the PoP node uses to communicate with the upstream router. Prefix length is fixed as /64.

IPv6 Gateway Address
 A configured IPv6 Gateway Address must be reachable from the PoP for the system to function. This address can be left blank when layer 2 bridging is enabled.

3. In **E2E Controller Configuration**, enter the **IPv6 Address**.

E2E Controller Configuration

IPv6 Address

If empty or Onboard mode enabled, PoP Address will be used

4. In BGP Configuration add IPv6 Address.

BGP Configuration

Local ASN The autonomous system number (ASN) assigned to the PoP nodes

KeepAlive The BGP keepalive period in seconds

Summarized CPE Prefix Prefix summarizing network wide customized CPE Prefixes/Prefixes allocated by DHCPv6 Relay (that fall outside Seed Prefix range). Multiple prefixes require comma separation. E.g CN1 has 2001:XY:1110::/64, CN2 has 2001:XY:1110::/64. Summarized CPE Prefix would be 2001:XY:1110::/63

IPv6 Address	ASN
No Data	
Add New	

5. In **IPv6 Layer 3 CPE**

- Select **IPv6 CPE interface** as Aux, Main, or SFP.
- Enter **IPv6 CPE Prefix**.

IPv6 Layer 3 CPE

IPv6 CPE interface
☐ Aux ☐ Main ☒ SFP ☐ Disabled
 Choose the interface to run IPv6 SLAAC. Subnet allocated by the controller will be used as Prefix. This interface will not be part of Layer 2 bridge. Should be disabled for IPv4 CPE.

IPv6 CPE Prefix If empty, Subnet prefix allocated by the controller to the node will be used.

6. In the **IPv4 Management** section, the following options are supported:

- **Static:** If you select Static, enter the IPv4 address, Subnet mask, and Gateway IP address manually.
- **DHCP:** If you select DHCP, there is no need to set the IP address, Subnet mask, and Gateway IP address manually. These properties (IPv4 address, Subnet mask, and Gateway IP address) are automatically obtained from the DHCP server. Note that the DHCP configuration is available only for the PoP nodes. It is not available for CN and DN nodes.

IPv4 Management

IP Assignment
☒ Static ☐ DHCP If the DHCP server is unreachable, the configured IP will serve as the fallback IP.

IPv4 Address 192.168.30.81 IPv4 Management address is not accessible over Relay port (except for PoP interface), OOB interface and IPv6 CPE interface.

Subnet Mask 255.255.255.0

Gateway IP Address 192.168.30.254

7. In **Ethernet Ports** enable the appropriate option **Main** or **Aux** or **SFP**.

8. In **Layer 2 bridge** enable the appropriate options such as:

- Disable Broadcast Broadcast packets (except DHCP Offer and DHCP Ack) in the downlink direction including client to client packets will be dropped.
- Disable Downlink Multicast Flood - Multicast packets in the downlink direction including client to client packets will be dropped
- Disable Unknown Unicast Flood
- Disable IPv6
- Monitor PoP Interface Layer 2 tunnels will failover to next best PoP when the backhaul interface of this PoP is down.



Note

The configuration is applicable only when static routing is used and IPv4 gateway is configured..

- Insert DHCP Option 82

Layer 2 Bridge

☐ Disable Broadcast Broadcast packets (except DHCP Offer and DHCP Ack) in the downlink direction including client to client packets will be dropped.
 ☐ Disable Downlink Multicast Flood Multicast packets in the downlink direction including client to client packets will be dropped.
 ☐ Disable Unknown Unicast Flood
 ☐ Disable IPv6
 ☐ Monitor IPv4 Gateway
 In Layer 2 bridging with multiple POP nodes, enabling this feature will configure this POP to periodically ARP ping the configured IPv4 Gateway. If the ARP pings are to fail, all other nodes within the mesh network will choose one of the other available POP nodes to route to

DHCP Option 82
☐ Enabled ☒ Disabled DHCP option 82 will be inserted in the DHCP requests.

- In **Other Settings** enable **Enable Aux port power** and **Multi-PoP / Relay Port**.

Other Settings

☐ Enable Aux port power Enables the power out on the Aux port

Multi-PoP / Relay Port
☒ Aux ☐ Main ☐ SFP ☐ Disabled Wired interface on which OpenR is run. Should be used when DNs are connected back to back and on PoPs in a multi PoP network.

- In **OOB Interface** enable the appropriate option **Main** or **Aux** or **SFP**.

- Enter **IPv4 Address**.
- Enter **Subnet Mask**.

OOB

OOB Interface
☒ Aux ☐ Main ☐ SFP ☐ Disabled Out of band management interface to access the device. Management VLAN will be bypassed and data traffic will not be routed or bridged on this interface.

IPv4 Address

Subnet Mask

- Click **Save**.



Note

Once the configuration is updated successfully in cnMaestro, the same parameters needs to be entered in the UI of the **PoP Node GUI**.

VLAN



Note

From Software Update Version 1.1 of all nodes, supports configuration of the VLAN Management and Ports.

Virtual Local Area Networks (VLANs) is a broadcast domain in a Layer 2 network. A broadcast domain is the set of all devices that will receive broadcast frames originating from any device within the set and traffic will be tagged when transporting over wireless.



Note

Only PoP node Management VLAN can be configured, if Layer 2 Bridge is not enabled in **E2E Network > Configuration > Basic** page.

Node running version 1.0.1:

- When Layer2 bridge is disabled, Only PoP node Management VLAN ID can be configured.
- When Layer2 bridge is enabled, all nodes Management VLAN ID can be configured.

Node running version 1.1:

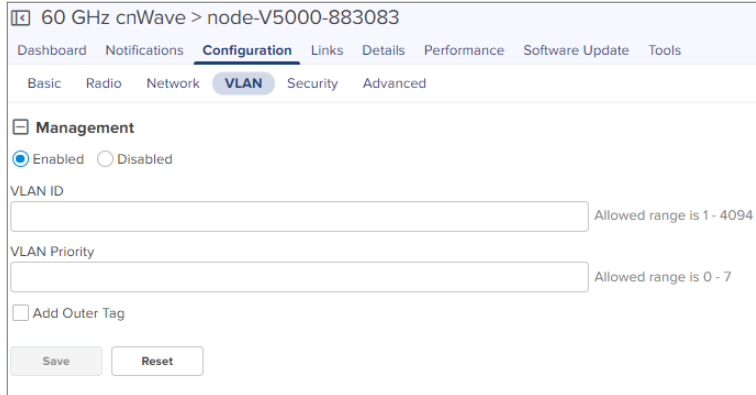
- When Layer2 bridge is disabled, Only PoP node Management VLAN ID, Priority with Outer Tag

can be configured.

- When Layer2 bridge is enabled, all node management VLAN and ports can be configured.

To add a Management VLAN:

1. Navigate to **Configuration > VLAN**.
2. Click Enabled.



60 GHz cnWave > node-V5000-883083

Dashboard Notifications **Configuration** Links Details Performance Software Update Tools

Basic Radio Network **VLAN** Security Advanced

Management

☒ Enabled ☐ Disabled

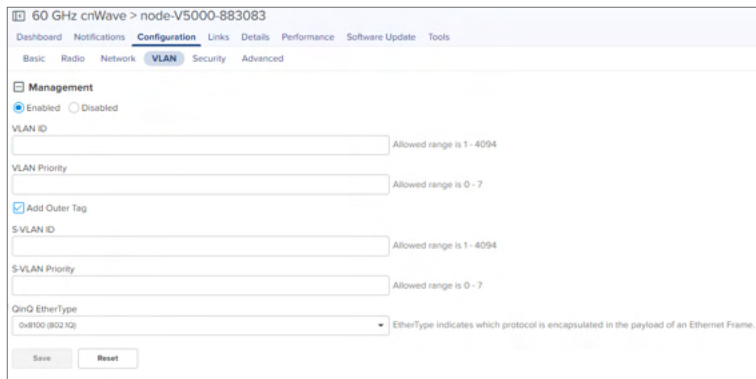
VLAN ID Allowed range is 1 - 4094

VLAN Priority Allowed range is 0 - 7

☐ Add Outer Tag

Save Reset

3. Enter the **VLAN ID** and **VLAN Priority**.
4. Enable **Add Outer Tag**.



60 GHz cnWave > node-V5000-883083

Dashboard Notifications **Configuration** Links Details Performance Software Update Tools

Basic Radio Network **VLAN** Security Advanced

Management

☒ Enabled ☐ Disabled

VLAN ID Allowed range is 1 - 4094

VLAN Priority Allowed range is 0 - 7

☒ Add Outer Tag

S-VLAN ID Allowed range is 1 - 4094

S-VLAN Priority Allowed range is 0 - 7

QinQ EtherType EtherType indicates which protocol is encapsulated in the payload of an Ethernet Frame.

Save Reset

5. Enter **S-VLAN ID**.
6. Enter **S-VLAN Priority**.
7. Enter **QinQ EtherType**.
8. Click **Save**.

If Layer 2 Bridge is enabled in **60 GHz cnWave Network > Configuration > Basic** page. User can configure Management VLAN and Ports of PoP node, DN and CN.



Note

VLAN settings are not applicable if Relay Port, SFP Port, or Aux Port is enabled on Network page.

60 GHz cnWave > test-pop2

Dashboard Notifications **Configuration** Links Details Performance Software Update Tools

Basic Radio Network **VLAN** Security Advanced

Management

☒ Enabled ☐ Disabled

VLAN ID Allowed range is 1 - 4094

VLAN Priority Allowed range is 0 - 7

☐ Add Outer Tag

Main Port

ⓘ VLAN settings are not applicable as PoP Interface is enabled on this port.

SFP Port

Type

☐ Q ☐ QinQ ☒ Transparent

Aux Port

Type

☐ Q ☐ QinQ ☒ Transparent

To add a VLAN:

1. Navigate to **Configuration > VLAN**.
2. Click Enabled.

60 GHz cnWave > test-pop2

Dashboard Notifications **Configuration** Links Details Performance Software Update Tools

Basic Radio Network **VLAN** Security Advanced

Management

☒ Enabled ☐ Disabled

VLAN ID Allowed range is 1 - 4094

VLAN Priority Allowed range is 0 - 7

☐ Add Outer Tag

Main Port

ⓘ VLAN settings are not applicable as PoP Interface is enabled on this port.

SFP Port

Type

☐ Q ☐ QinQ ☒ Transparent

Aux Port

Type

☐ Q ☐ QinQ ☒ Transparent

3. Enter the **VLAN ID** and **VLAN Priority**.
4. Enable **Add Outer Tag**.

60 GHz cnWave > test-pop2

Dashboard Notifications **Configuration** Links Details Performance Software Update Tools

Basic Radio Network **VLAN** Security Advanced

Management

☒ Enabled ☐ Disabled

VLAN ID Allowed range is 1 - 4094

VLAN Priority Allowed range is 0 - 7

☒ Add Outer Tag

S-VLAN ID Allowed range is 1 - 4094

S-VLAN Priority Allowed range is 0 - 7

QinQ EtherType EtherType indicates which protocol is encapsulated in the payload of an Ethernet Frame.

Main Port

⚠ VLAN settings are not applicable as PoP Interface is enabled on this port.

SFP Port

Type ☐ Q ☐ QinQ ☒ Transparent

Aux Port

Type ☐ Q ☐ QinQ ☒ Transparent

5. Enter **S-VLAN ID**.
6. Enter **S-VLAN Priority**.
7. Enter **QinQ EtherType**.



Note

VLAN settings configuration of Main Port, SFP Port, or Aux Port is similar.

8. Select Port **Q** or **QinQ** types.
 - a. If user selects **Q type** perform as follows:

Main Port

⚠ VLAN settings are not applicable as PoP Interface is enabled on this port.

SFP Port

Type ☒ Q ☐ QinQ ☐ Transparent

Untagged Packets ☐ Allow ☐ Drop

Native VLAN ID Allowed range is 1 - 4094

Native VLAN Priority Allowed range is 0 - 7

Allowed VLANs List of allowed VLANs. Comma separated, and/or range. e.g 100, 210-220

Ingress VLAN	Remark VLAN
No Data	
Add New	
Ingress VLAN	Override Priority
No Data	
Add New	

Aux Port

Type ☐ Q ☐ QinQ ☒ Transparent

- Select **Untagged Packets** Allow or Drop.
- Enter **Native VLAN ID**.
- Enter **Native VLAN Priority**.

- Enter **Allowed VLANs**.
- To add new **VLAN Remarking**.

Ingress VLAN	Remark VLAN
No Data	
Add New	

- Click Add New

Add

Ingress VLAN

Allowed range is 1 - 4094

Remark VLAN

Allowed range is 1 - 4094

- Enter **Ingress VLAN** and **Remark VLAN**.
- Click **Save**.

- To add new **VLAN Priority Override**.

Ingress VLAN	Override Priority
No Data	
Add New	

- Click **Add New**.

Add

Ingress VLAN

Allowed range is 1 - 4094

Override Priority

Allowed range is 0 - 7

- Enter **Ingress VLAN** and **Remark VLAN**.
- Click **Save**.
- Click **Save**.

b. If user selects **QinQ** type perform as follows:

SFP Port

Type

☐ Q
☒ QinQ
☐ Transparent

Untagged Packets

☐ Allow
☐ Drop

Single Tagged Packets

☒ Allow
☐ Drop

Native C-VLAN ID

Allowed range is 1 - 4094

Native C-VLAN Priority

Allowed range is 0 - 7

Native S-VLAN ID

Allowed range is 1 - 4094

Native S-VLAN Priority

Allowed range is 0 - 7

Allowed VLANs

List of allowed VLANs. Comma separated, and/or range. e.g 100, 210-220

QinQ EtherType

0x8100 (802.1Q)

▼

EtherType indicates which protocol is encapsulated in the payload of an Ethernet Frame.

Ingress VLAN	Remark VLAN	
No Data		
Add New		

Ingress VLAN	Override Priority	
No Data		
Add New		

Aux Port

Type

☐ Q
☐ QinQ
☒ Transparent

Save

Reset

- In **Untagged Packets** select **Allow** or **Drop**.
- In **Single Tagged Packets** select **Allow** or **Drop**.
- Enter **Native C-VLAN ID**.
- Enter **Native C-VLAN Priority**.
- Enter **Native S-VLAN ID**.
- Enter **Native S-VLAN Priority**.
- Enter **Allowed VLANs**.
- Enter **QinQ EtherType**.
- To add new **VLAN Remarking**.

Ingress VLAN	Remark VLAN	
No Data		
Add New		

- Click **Add New**.

Add

Ingress VLAN

Allowed range is 1 - 4094

Remark VLAN

Allowed range is 1 - 4094

- Enter **Ingress VLAN** and **Remark VLAN**.
- Click **Save**.
- To add new **VLAN Priority Override**.

Ingress VLAN	Override Priority
No Data	
Add New	

- Click **Add New**.

Add

Ingress VLAN

Allowed range is 1 - 4094

Override Priority

Allowed range is 0 - 7

- Enter **Ingress VLAN** and **Remark VLAN**.
- Click **Save**.
- Click **Save**.

Security

Security tab allows to reset the identity and password of the Radius user.

Figure 369 *Security*

60 GHz cnWave > test-pop2

Dashboard Notifications **Configuration** Links Details Performance Software Update Tools

Basic Radio Network VLAN **Security** Advanced

Radius user identity

Private key password

Radius Private key password

Radius user password

Radius user password

Advanced

Advanced tab allows the advanced user to edit the settings of the [Table](#) and [JSON](#) format of the PoP Nodes.

Table

In the **Table** user can view and edit **Field Name** and **Value**. You can sort field name in alphabetical order.

To add a field:

1. Navigate to **Configuration > Advanced**.
2. Click **Add New**.

60 GHz cnWave > test-pop2

Dashboard Notifications **Configuration** Links Details Performance Software Update Tools

Basic Radio Network VLAN Security **Advanced**

All the settings below are for advanced users only.

Search

Table JSON Add New

Field	Description	Status	Value	
logTailParams.sources.terragraph_openr_logs.enabled	Enable tailing from this source.	set	true	
logTailParams.sources.terragraph_openr_logs.filename	The log file name.	set	/var/log/openr/current	
logTailParams.sources.terragraph_kern_logs.enabled	Enable tailing from this source.	set	true	
logTailParams.sources.terragraph_kern_logs.filename	The log file name.	set	/var/log/kern.log	
logTailParams.sources.terragraph_minion_logs.enabled	Enable tailing from this source.	set	true	
logTailParams.sources.terragraph_minion_logs.filename	The log file name.	set	/var/log/e2e_minion/current	
snmpConfig.location	System location.	set	No Location	
snmpConfig.contact	System contact.	set	No Contact	
popParams.VPP_ADDR	The IP address of the interface within VPP on the POP node (Fast Path edge address).	unset		
popParams.POP_STATIC_ROUTING	Enable static routing on the POP.	modified	1	
popParams.POP_IFACE	The interface on the POP node that routes traffic to the Gateway.	modified	nic2	
popParams.POP_BGP_ROUTING	Enable BGP routing on the POP.	modified	0	
popParams.NAT64_POP_ENABLED	Enable NAT64 on POP interface for IPv6 <-> IPv4 NAT.	set	0	
popParams.NAT64_IPV6_PREFIX	NAT64 IPv6 prefix. Can use 64:ff9b::96 (well-known prefix).	unset		
popParams.POP_ADDR	The IP address of the interface on the POP node that routes to the Gateway.	modified	6400ba5e-88:3083:88:3083	

Save Reset

Show Full Configuration

3. Enter the **Field Name** and **Value**.

Add new field

Field Name

String

Value

Save Cancel

4. Click **Save**.

JSON

JSON allows advanced user to download or view the JSON format.

60 GHz cnWave > PoP-Onboard-V5k-3083

Dashboard Notifications **Configuration** Links Details Performance Software Update Tools

Basic Radio Network VLAN Security **Advanced**

All the settings below are for advanced users only.

Table JSON Add New

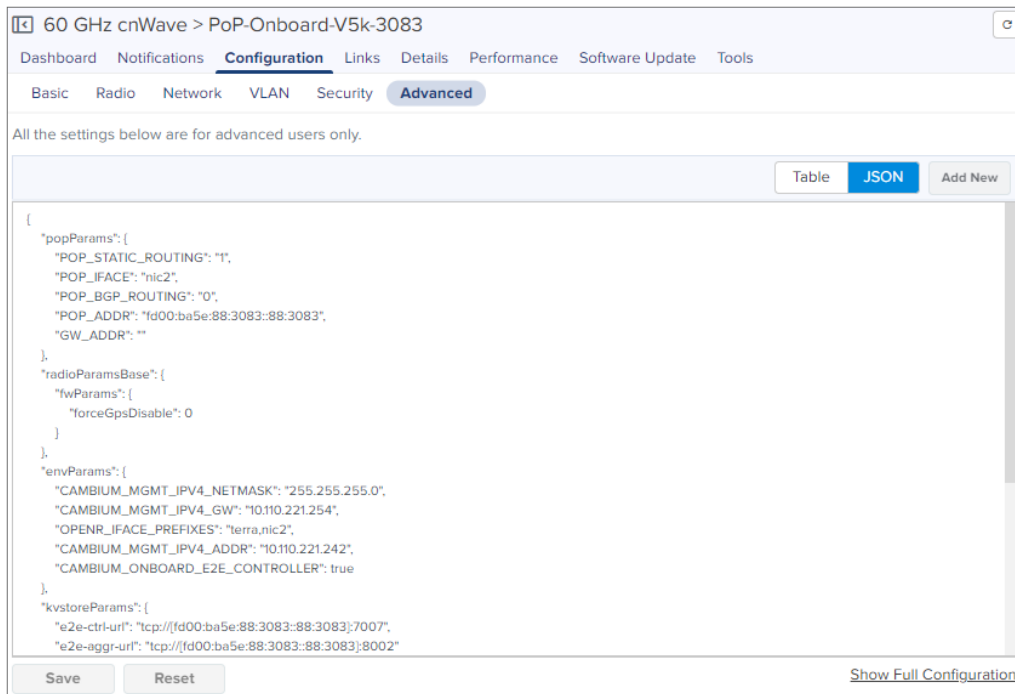
```
{
  "popParams": {
    "POP_STATIC_ROUTING": "1",
    "POP_IFACE": "nic2",
    "POP_BGP_ROUTING": "0",
    "POP_ADDR": "6400ba5e-88:3083:88:3083",
    "GW_ADDR": ""
  },
  "radioParamsBase": {
    "hwParams": {
      "forceGpsDisable": 0
    }
  },
  "envParams": {
    "CAMBIUM_MGMT_IPV4_NETMASK": "255.255.255.0",
    "CAMBIUM_MGMT_IPV4_GW": "10.110.221.254",
    "OPENR_IFACE_PREFIXES": "terra,nic2",
    "CAMBIUM_MGMT_IPV4_ADDR": "10.110.221.242",
    "CAMBIUM_ONBOARD_E2E_CONTROLLER": true
  },
  "kvstoreParams": {
    "e2e-ctrl-uri": "tcp://6400ba5e-88:3083:88:3083:7007",
    "e2e-aggr-uri": "tcp://6400ba5e-88:3083:88:3083:8002"
  }
}
```

Save Reset

Show Full Configuration

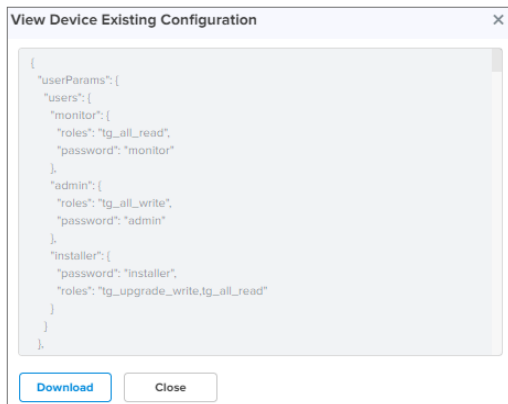
To download the file:

1. Navigate to **Configuration > Advanced > JSON**.



2. Click **Show Full Configuration**.

View Device Existing Configuration window pops up.



3. Click **Download**.

Links

Links provide the details about the links between nodes, statistics and events of the links in the E2E Network.

List

List provide the details about the links of the nodes and also provides the option to create a new link. User can delete the links in bulk by selecting the particular links. It also allows to export or import link details.

Figure 370 List

Name	A-Node	Z-Node	A-Node MAC	Z-Node MAC	Alive	Link Time
link-CN-0463-PoP-30DC	CN-0463	PoP-30DC	12:04:56:88:04:63	12:04:56:88:30:DC	No	20d 4h 38m
link-DN-3137-PoP-30DC	DN-3137	PoP-30DC	12:04:56:88:31:37	12:04:56:88:30:DC	Yes	1d 9h 25m
link-DN-3183-PoP-30DC	DN-3183	PoP-30DC	12:04:56:88:31:83	12:04:56:88:30:DC	No	20d 4h 37m
link-DN30b0-PoP-30DC	DN30b0	PoP-30DC	12:04:56:88:30:B0	12:04:56:88:30:DC	Yes	20d 7h 50m
link-PoP-30DC-PoP-6A	PoP-30DC	PoP-6A	-	-	Yes	23d 1h 5m

For more details about adding a link and deleting a link in the network, refer the [List](#) section.



Note

By default A Node is selected as node, when adding new link in the network.

Export List

Export list allow the user to export the PoP links list.

To export the links :

1. Navigate to **Links > List** > select **Export**.

Name	A-Node	Z-Node	A-Node MAC	Z-Node MAC	Alive	Link Time
link-CN-0463-PoP-30DC	CN-0463	PoP-30DC	12:04:56:88:04:63	12:04:56:88:30:DC	No	25d 4h 40m
link-DN-3137-PoP-30DC	DN-3137	PoP-30DC	12:04:56:88:31:37	12:04:56:88:30:DC	Yes	6d 9h 27m
link-DN-3183-PoP-30DC	DN-3183	PoP-30DC	12:04:56:88:31:83	12:04:56:88:30:DC	No	25d 4h 39m
link-DN30b0-PoP-30DC	DN30b0	PoP-30DC	12:04:56:88:30:B0	12:04:56:88:30:DC	Yes	25d 7h 52m
link-PoP-30DC-PoP-6A	PoP-30DC	PoP-6A	-	-	Yes	28d 1h 7m

2. It exports .csv file format as shown below.

LINK_NAME	A_NODE	I_A_NODE	I_Z_NODE	I_Z_NODE	I_LINK_TYPE	ALIVE	IGNITION	DISTANCE	AZIMUTH	BACKUP_C	IGNITION	TIMESTAMP
Link Name	A node nai Sector 1/2 Z node nai Sector 1/2 Wireless o Yes/No Ignition At Distance b Azimuth (C Yes/No Enabled/D Timestamp											
link-CN-fa-cloud-D4	CN-fa-clou	12:04:56:8	D4	22:04:56:8	Wireless	Yes	16	996	54.9	No	Enabled	2021-07-23T02:49:06.317Z
link-D4-PoP-Onboard-V5k-3083	D4	12:04:56:8	PoP-Onbo	22:04:56:8	Wireless	Yes	0	988	158.8	No	Enabled	2021-07-23T02:49:06.317Z
link-DN-D6-PoP-Onboard-V5k-3083	DN-D6	12:04:56:8	PoP-Onbo	12:04:56:8	Wireless	Yes	0	979	105.2	No	Enabled	2021-07-23T02:49:06.317Z

Import List

Import list allow the user to import the PoP links list.

1. Navigate to **Links > List > select Import.**

60 GHz cnWave Network > 8_Nodes_Ext_E2e

Dashboard Notifications Configuration **Links** Statistics Report X Software Update Tools

List Statistics Events

Apply Filter(s) Add New Delete **Import** Export

Name	A-Node	Z-Node	A-Node MAC	Z-Node MAC	Alive	Link Time
link-CN-0463-PoP-30DC	CN-0463	PoP-30DC	12-04-58-04-43	12-04-58-04-43	No	6d 3h 44m
link-CN-0463-PoP-6A	CN-0463	PoP-6A	12-04-58-04-43	12-04-58-04-43	Yes	8d 0h 1m
link-DN-3039-DN-3137	DN-3039	DN-3137	12-04-58-04-43	12-04-58-04-43	Yes	7d 5h 14m
link-DN-3039-DN30b0	DN-3039	DN30b0	12-04-58-04-43	12-04-58-04-43	Yes	7d 5h 14m
link-DN-3137-PoP-30DC	DN-3137	PoP-30DC	12-04-58-04-43	12-04-58-04-43	Yes	8d 6h 52m
link-DN-3183-PoP-30DC	DN-3183	PoP-30DC	12-04-58-04-43	12-04-58-04-43	No	6d 3h 43m
link-DN-3183-PoP-6A	DN-3183	PoP-6A	12-04-58-04-43	12-04-58-04-43	Yes	6d 2h 3m
link-DN30b0-PoP-30DC	DN30b0	PoP-30DC	12-04-58-04-43	12-04-58-04-43	Yes	6d 6h 56m

Showing 1 - 10 Total: 11 10 < Previous 1 2 Next >

Import Links window appears.

Import Links

Upload a file (csv) as per the format specified in the template.

File

Select File Download Template

Import

2. Click **Download Template** to download the .CSV format file.

	A	B	C	D	E
1	A_NODE_NAME	A_NODE_MAC	Z_NODE_NAME	Z_NODE_MAC	LINK_TYPE
2	A node name of the device	Sector 1/2 MAC Address	Z node name of the device	Sector 1/2 MAC Address	Wireless or Wired
3	POP	12-04-58-04-43	DN1	12-04-58-04-43	wireless
4	DN1	12-04-58-04-43	CN1	12-04-58-04-43	wireless
5	DN1		CN2		wired
6					
7					

3. Select the file and click **Import.**

Statistics

Links Statistics pages provides details of **Basic:** Name, Direction, A-Node, Z-Node Alive Link Time Type Distance Azimuth, Rx Golay, Tx Golay **Detailed Statistics:** A-Node Sector MAC, Z-Node Sector MAC, RSSI, Rx Airtime%, Rx Beam Azimuth Angle, Rx Beam Elevation Angle, Rx SNR, Rx MCS, Rx PER, Rx Scan Beams, Rx Throughput, Tx Airtime%, Tx Beam Azimuth Angle, Tx Beam Elevation Angle, Tx Power Index, EIRP, Tx MCS, Tx PER, Tx Scan Beams, Rx Errors, Rx Frames, Tx Errors, Tx Frames, Tx Throughput, Rx Time, Tx Time, and Link Fade Margin links created with PoP node, generally in a page format.

60 GHz cnWave Network > 8_Nodes_Ext_E2e

Dashboard Notifications Configuration **Links** Statistics Report X Software Update Tools

List **Statistics** Events

Apply Filter(s) Auto Refresh Enabled Export

Name	Direction	A-Node Sector MAC	Z-Node Sector MAC	Alive	Link Time	RSSI	Rx SNR	Rx MCS	Tx Power Index	EIRP	Tx MCS
link-CN-PoP-6A	PoP-6A to CN	12-04-58-04-43	12-04-58-04-43	Yes	6d 2h 21m	-46 dBm	27 dB	12	6	13 dBm	9
link-CN-PoP-6A	CN to PoP-6A	12-04-58-04-43	12-04-58-04-43	Yes	6d 2h 21m	-45 dBm	28 dB	9	6	13 dBm	12
link-CN-0463-PoP-6A	PoP-6A to CN-0463	12-04-58-04-43	12-04-58-04-43	Yes	8d 0h 23m	-47 dBm	25 dB	2	6	13 dBm	8
link-CN-0463-PoP-6A	CN-0463 to PoP-6A	12-04-58-04-43	12-04-58-04-43	Yes	8d 0h 23m	-47 dBm	26 dB	8	6	13 dBm	2
link-DN-3039-DN-3137	DN-3039 to DN-3137	12-04-58-04-43	12-04-58-04-43	Yes	7d 5h 37m	-40 dBm	32 dB	9	6	13 dBm	9
link-DN-3039-DN-3137	DN-3137 to DN-3039	12-04-58-04-43	12-04-58-04-43	Yes	7d 5h 37m	-53 dBm	21 dB	9	6	13 dBm	9
link-DN-3039-DN30b0	DN-3039 to DN30b0	12-04-58-04-43	12-04-58-04-43	Yes	7d 5h 37m	-40 dBm	32 dB	3	6	13 dBm	2
link-DN-3039-DN30b0	DN30b0 to DN-3039	12-04-58-04-43	12-04-58-04-43	Yes	7d 5h 37m	-39 dBm	32 dB	2	6	13 dBm	3
link-DN-3137-PoP-30DC	PoP-30DC to DN-3137	12-04-58-04-43	12-04-58-04-43	Yes	8d 7h 15m	-46 dBm	26 dB	2	6	13 dBm	6
link-DN-3137-PoP-30DC	DN-3137 to PoP-30DC	12-04-58-04-43	12-04-58-04-43	Yes	8d 7h 15m	-45 dBm	27 dB	6	6	13 dBm	2

Showing 1 - 10 Total: 14 10 < Previous 1 2 Next >

Export Statistics

Export list allow the user to export the PoP links Statistics.

To export the Statistics :

1. Navigate to **Links > Statistics > select Export**.

Name	Direction	A-Node Sector MAC	Z-Node Sector MAC	Alive	Link Time	RSSI	Rx SNR	Rx MCS	Tx Power Inc	MCS
link-DN-3137-PoP-30DC	DN-3137 to PoP-30DC	12:04:56:8 12:04:56:8	12:04:56:8 12:04:56:8	Yes	6d 9h 30m	-47 dBm	25 dB	8	6	
link-DN-3137-PoP-30DC	PoP-30DC to DN-3137	12:04:56:8 12:04:56:8	12:04:56:8 12:04:56:8	Yes	6d 9h 30m	-43 dBm	30 dB	2	6	13 dBm 8
link-DN30b0-PoP-30DC	DN30b0 to PoP-30DC	12:04:56:8 12:04:56:8	12:04:56:8 12:04:56:8	Yes	25d 7h 55m	-40 dBm	32 dB	2	6	13 dBm 3
link-DN30b0-PoP-30DC	PoP-30DC to DN30b0	12:04:56:8 12:04:56:8	12:04:56:8 12:04:56:8	Yes	25d 7h 55m	-39 dBm	32 dB	3	6	13 dBm 2

2. It exports .csv file format as shown below.

LINK_NAME	DIRECTION	A_NODE	Z_NODE	A_NODE_ID	Z_NODE_ID	ALIVE	TYPE	DISTANCE	AZIMUTH	RSSI	Rx_SNR	Rx_MCS	Rx_PER	Rx_BEAM	Tx_POWER	EIRP	Tx_MCS	Tx_PER	Tx_BEAM	Rx_ERROR	Rx_FRAME
link-APOP-DN-3D	APOP to DN-3D	APOP	DN-3D	22:04:56:8	12:04:56:8	Yes	Wireless	147	83	-52	21	9	0.17	64	6	13	10	0.19	64	290	20975
link-APOP-DN-3D	DN-3D to APOP	APOP	DN-3D	22:04:56:8	12:04:56:8	Yes	Wireless	147	83	-51	22	9	0.2	84	6	13	9	0.21	84	374	1488
link-APOP-DN-80	APOP to DN-80	APOP	DN-80	12:04:56:8	22:04:56:8	Yes	Wireless	94	-178.1	-40	32	9	0	32	6	13	9	0	35	92	30630
link-APOP-DN-80	DN-80 to APOP	APOP	DN-80	12:04:56:8	22:04:56:8	Yes	Wireless	94	-178.1	-37	32	10	0	0	6	13	10	0	0	1332	9183
link-CN-75-DN-80	DN-80 to CN-75	CN-75	DN-80	12:04:56:8	12:04:56:8	Yes	Wireless	171	-151.2	-48	25	9	0.31	0	23	30	9	0.38	0	0	0
link-CN-75-DN-80	CN-75 to DN-80	DN-80	12:04:56:8	12:04:56:8	Yes	Wireless	171	-151.2	-61	12	8	0.42	0	6	13	9	0.35	0	1944	443425	
link-CN-83-DN-80	DN-80 to CN-83	CN-83	DN-80	12:04:56:8	12:04:56:8	Yes	Wireless	71	52.7	-53	21	9	0.81	58	6	35	9	0.06	58	385	2043
link-CN-83-DN-80	DN-80 to CN-83	CN-83	DN-80	12:04:56:8	12:04:56:8	Yes	Wireless	71	52.7	-49	23	9	0.04	112	6	13	9	0.08	112	0	339
link-CN-8b0463-D	DN-39 to CN-8b0463	CN-8b0463	DN-39	12:04:56:8	22:04:56:8	No	Wireless	199	-45.2	-60	12	9	0	44	31	37	5	0.01	44	95	2856
link-CN-8b0463-D	CN-8b0463 to DN-39	DN-39	12:04:56:8	22:04:56:8	No	Wireless	199	-45.2	-48	25	9	0.04	45	6	13	9	0.56	45	54	62	
link-DN-39-DN-3D	DN-39 to DN-3D	DN-3D	12:04:56:8	22:04:56:8	Yes	Wireless	155	20.5	-40	32	9	0	15	6	13	9	0	24	23	504	
link-DN-39-DN-3D	DN-3D to DN-39	DN-39	12:04:56:8	22:04:56:8	Yes	Wireless	155	20.5	-43	30	9	0	0	6	13	10	0	0	164	232	
link-DN-39-DN-80	DN-80 to DN-39	DN-39	12:04:56:8	12:04:56:8	Yes	Wireless	100	-70.5	-45	28	9	0.06	35	6	13	9	0.02	34	73	567	
link-DN-39-DN-80	DN-39 to DN-80	DN-80	22:04:56:8	12:04:56:8	Yes	Wireless	100	-70.5	-48	25	9	0.3	55	6	13	10	0.01	54	331	303	

Events

Events provide the details of link availability, hourly link availability in percentage, link availability in different time lines, and distance of the link.

Figure 371 Link Events

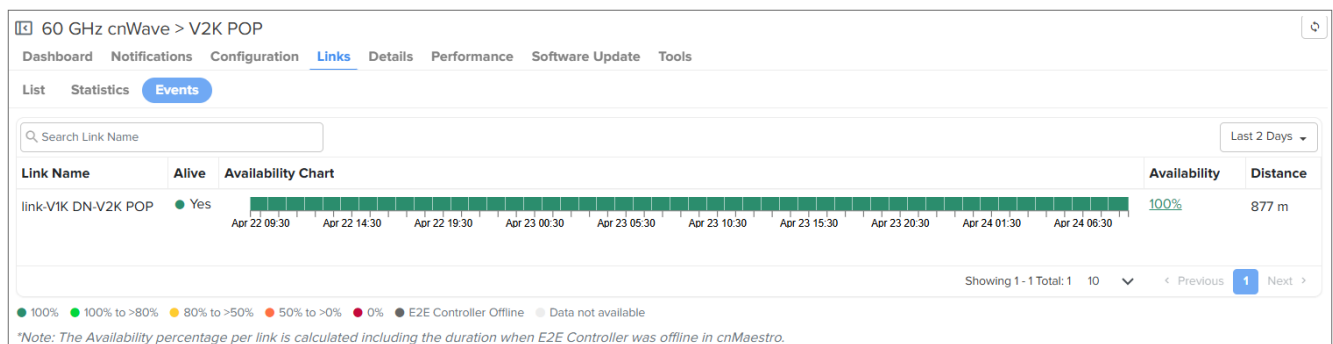


Table 82 Link > Events fields

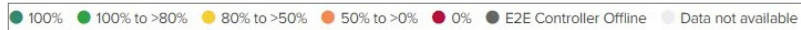
Field	Description
Link Name	Name of the link.
Alive	Status of the link (Yes or No).
Availability Chart	Displays the link availability duration (in chart format) based on time range selected from the dropdown list (located above the Distance field). This time range dropdown list supports the following options: Last 1 Hour, Last 6 Hours, Last 12 Hours, Last 24 Hours, Last 2 Days, Last 4 Days, Last 7 Days, and Last 30 Days X. You can also

Table 82 *Link > Events fields*

Field	Description
	<p>customize the time range using the Custom Range option from the dropdown list.</p> <p>Note: Custom Range and Last 30 days X are available only for cnMaestro X users.</p> <p>When you hover the mouse on the Availability Chart, the link availability is shown as described:</p> <ol style="list-style-type: none"> 1. If you select time range as Last 1 Hour, then link availability for every 5 minutes is displayed. 2. If you select time range other than Last 1 Hour, then link availability for every 1 hour is displayed.
Availability Percentage	Availability of link is shown in percentage in the Availability column, as shown in Figure 371 .
Distance	Distance of the link in meters.

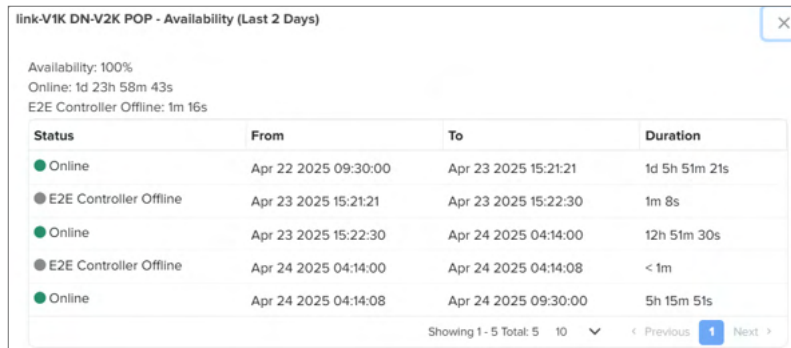
The **Availability Chart** field displays the link availability in percentage and different colors, as shown below,

Figure 372 *Link Availability in Percentage*



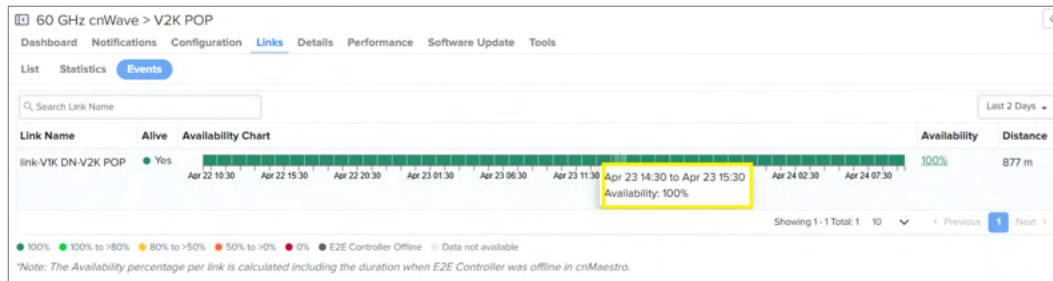
When you click on the percentage in the **Availability** column, you can view the detailed link availability information for the selected time range. Availability percentage per link is calculated, including the duration, when E2E Controller goes Offline in cnMaestro.

Figure 373 *Detailed link availability information*



You can hover your mouse on the link to view the hourly availability of the link, as shown in the figure below.

Figure 374 *Viewing the hourly availability status*



When you click on the hourly availability time on the chart (for example, Apr 23 14.30 to Apr 23 15.30 as shown in [Figure 374](#)), you can view the detailed link information for the selected one hour, including the link offline reason.

Figure 375 *Hourly details*

link-V1K DN-V2K POP		
Apr 23 14:30 to Apr 23 15:30		
Availability: 100%		
Online: 58m 51s		
E2E Controller Offline: 1m 8s		
Event	Time	Reason
Offline	Apr 23 2025 15:21:21	Unknown
E2E Controller Offline	Apr 23 2025 15:21:21	-
Online	Apr 23 2025 15:22:30	-
Showing 1 - 3 Total: 3 10 < Previous 1 Next >		

Details

Details page provides the following device information:

- [Overview](#)
- [Network](#)

Overview

Overview page provides the device details and it also details of the last 3 software update history.

Figure 376 *Details Overview Page*

60 GHz cnWave > PoP-30DC

Dashboard

Notifications

Configuration

Links

Details

Performance

Software Update

Tools

Overview

Network

System

Name

PoP-30DC

Product Name

60 GHz cnWave V5000 DN (PoP)

MAC Address

88:88:88:88:88:88

Health

Online (2d 20h 12m)

IPv6 Address

fd17:fde9:19c0:8000::1

Software Version

1.2.1

Firmware Version

10.11.0.87

Serial Number

888888888888

Onboard Date

Feb 11, 2022 13:02

Sync Mode

GPS

GPS

Latitude

12.933947

Longitude

77.6944181

Height

934 m

Fix Num Sat

15

Fix Type

3D

Links

Wireless

Wired

Total

4

1

Active

2

1

Sectors

Sector 1

Sector 2

MAC Address

88:88:88:88:88:88

88:88:88:88:88:88

Channel

1

2

Links

2

2

Rx Packets

2838722272

1123295081

Tx Packets

4489694042

161646818

Security

PSK

PSK

Error Association

0

0

Channel Last State

0

0

Software Update

Software Version

1.2.1

History

Date

Status

Version

Fri Feb 11 2022 13:39:29 UTC +0530

Success

1.2.1

Network

Network page provides the **Ethernet** details of **Main**, **Aux**, and **SFP**.

Figure 377 Details Network Page

60 GHz cnWave > PoP-Onboard-V5k-3083			
Dashboard Notifications Configuration Links Details Performance Software Update Tools			
Overview Network			
Ethernet			
	Main	Aux	SFP
Status	1000 Mbps	down	down
Rx Throughput	4.05 Kbps	0 Kbps	0 Kbps
Tx Throughput	1.37 Kbps	0 Kbps	0 Kbps
Rx Packets	385137	0	0
Tx Packets	140652	0	0
Rx Errors	7401	0	0
Tx Errors	0	0	0
Rx Drops	1872	0	0
Tx Drops	0	0	0
Rx Frames	0	0	0

Tools

In Tools page, you can view the **Status**, **Debug**, details and **Remote Command** results of the device.

Status

In **Status** tab you can view the status of the device:

- Critical alarms
- Download Tech Support File
- Online or Offline
- Restart minion
- Reboot the device.


60 GHz cnWave > PoP-Onboard-V5k-3083
Dashboard Notifications Configuration Links Details Performance Software Update **Tools**

Status Debug Remote Command

60 GHz cnWave V5000 DN (...)
PoP-Onboard-V5k-3083

Online

0



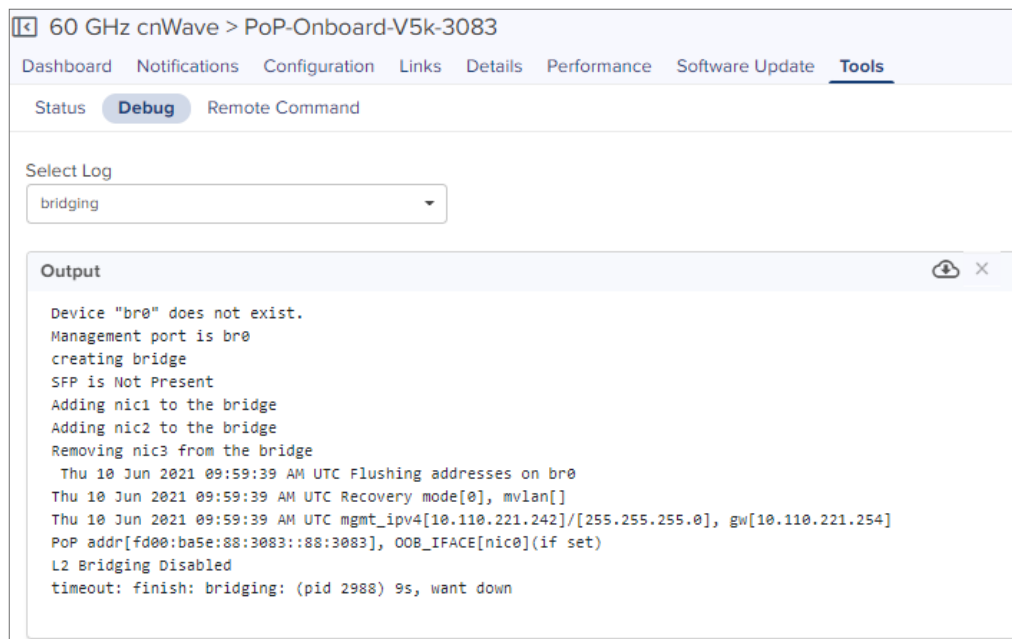
Debug



In **Debug** tab user view or download the PoP logs by executing the following log commands:

- Bridging
- pop-config
- e2e_minion
- openr
- exabgp
- cnAgent (available for Onboard PoP device)

To view the logs:

1. Navigate to **Tools > Debug**.
2. Select the required log name from the **Select Log** dropdown list.



- Click the download  icon to download the generated output.
- Click the clear  icon to clear the generated output.

Remote Command

In **Remote command** tab, user can view or download Command logs by executing the following commands:

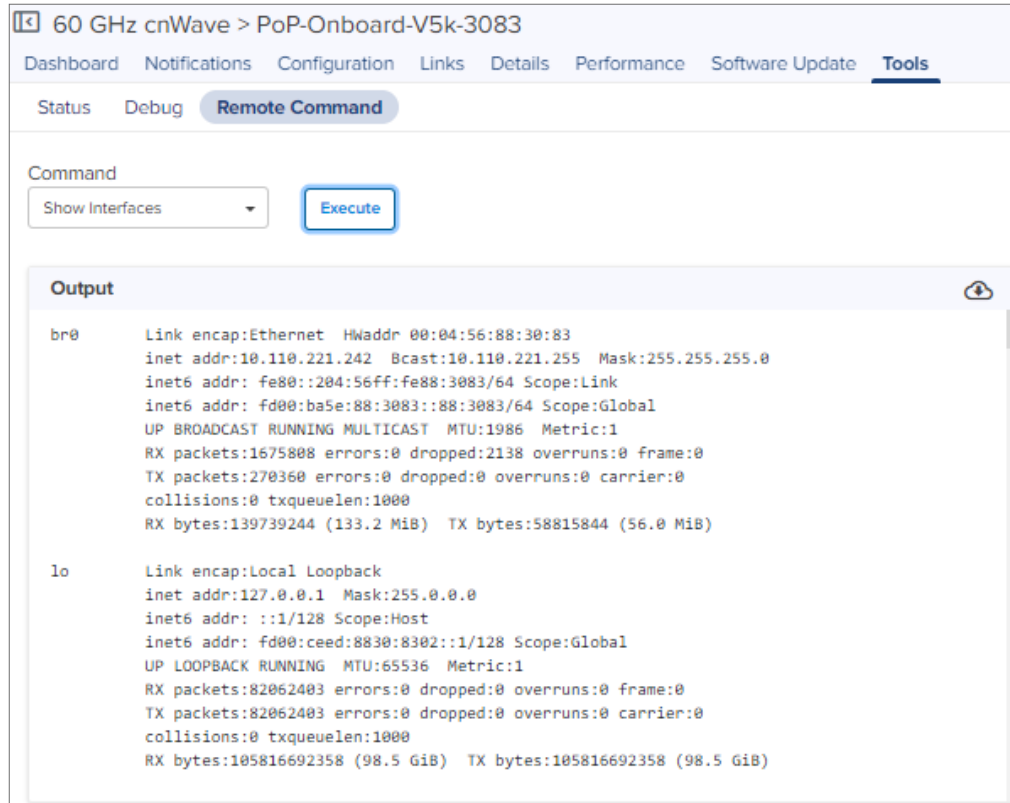
- Ping
- Show IGMP Membership Table
- Show Interfaces
- Show IPv4 Neighbors
- Show IPv6 Neighbors
- Show MAC Address Table
- Show OpenR Adjacencies
- Show OpenR Prefixes



- Show Routes
- Show SFP Power Details (applicable for V5000 and V3000)
- Show Wired Interface State Changes

To Execute the command:

1. Navigate to **Tools > Remote Command**.
2. Select the required command from the **Command** dropdown list.
3. Click **Execute**.

The output for the selected criteria appears as shown:



- Click the download  icon to download the generated output.
- Click the clear  icon to clear the generated output.

DN/CN Node

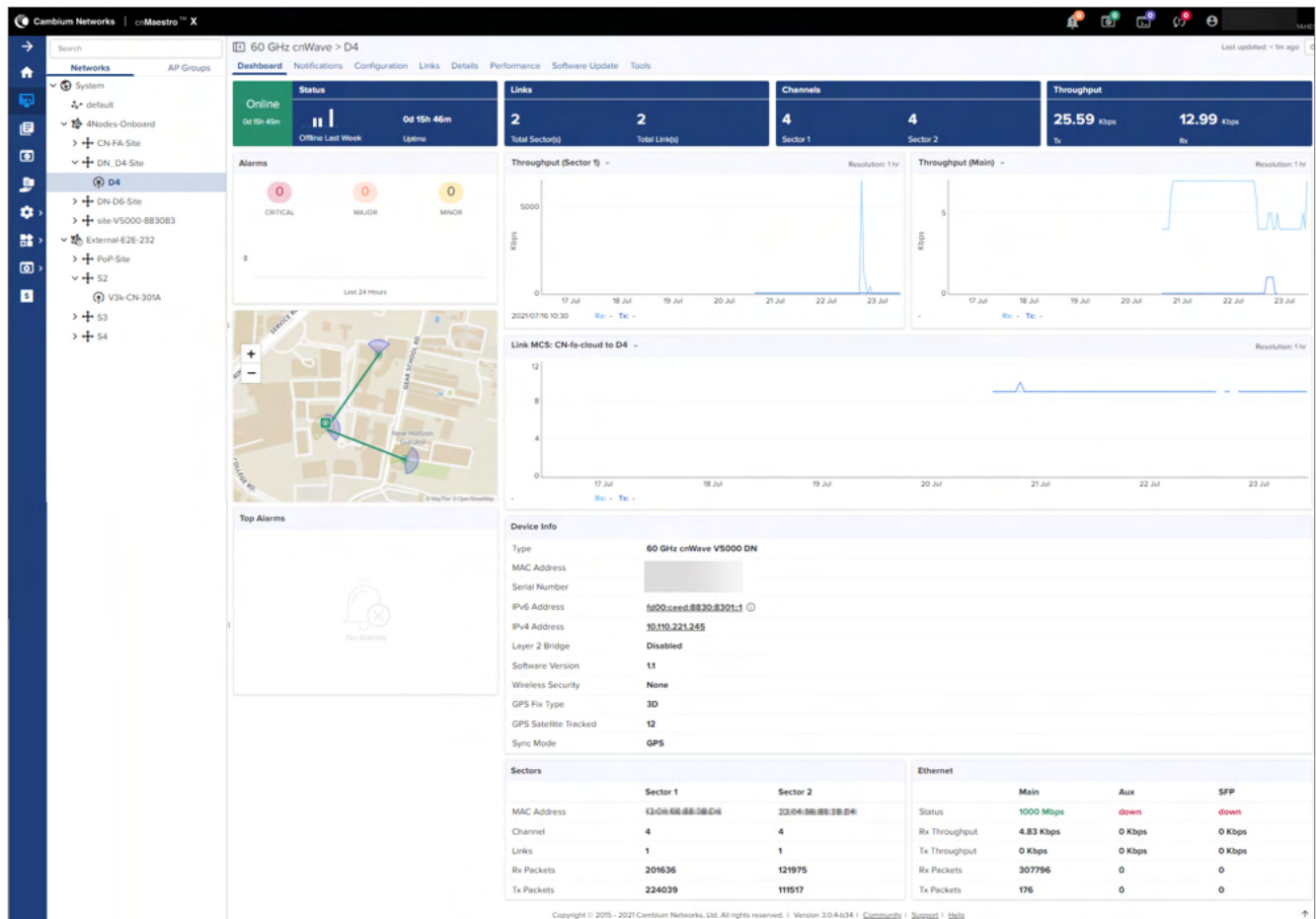
To create a new site, refer to [Site](#).

To create a node, refer to [DN/CN](#).

Dashboard

Dashboard pages are customized for each device type and aggregation level. The DN/CN node dashboard section displays the **Status, Links, Channels, Throughput, Sector Throughput (Sector 1 and Sector 2), Ethernet Throughput (Main, Aux, SFP), Alarms, Top Active Alarms, Link MCS, Device Info, Sectors, and Ethernet**.

Figure 378 DN/CN Node Dashboard



Configuration

Configuration page allows the user to configure the following details of CN/DN:

- [Basic](#)
- [Radio](#)
- [Network](#)
- [VLAN](#)
- [Security](#)
- [Advanced](#)

Basic

It allows to configure and reset the basic details of DN/CN node such as Name, Description, MAC Address, Azimuth, and Elevation. It also allows to edit the name of the node.

Figure 379 Basic

60 GHz cnWave > CN-fa-cloud

Dashboard Notifications **Configuration** Links Details Performance Software Update Tools

Basic Radio Network VLAN Security Advanced

Name
CN-fa-cloud

Description

MAC Address
00:04:56:8B:00:FA

Azimuth
0

Elevation
0

Save Reset

Radio



Note

GPS option is not enabled for v1000.

It allows the you to configure the **EIRP**, **Adaptive Modulation**, **Sectors (channels, Polarity and Link(s) Golay)**, and **GPS**.

Figure 380 Radio

60 GHz cnWave > DN-D6

Dashboard Notifications **Configuration** Links Details Performance Software Update Tools

Basic **Radio** Network VLAN Security Advanced

EIRP

Maximum EIRP
60 Allowed range is 35 dBm to 55 dBm

IBF Transmit Power
☐ Short range (<25m) optimized ☒ Long range optimized Initial Beam Forming transmit power setting

Antenna

Antenna Dish Gain
44.5 dBi

PTP Deployment Range

PTP Deployment Range
☒ Upto 1.5 km ☐ Upto 3.0 km ☐ Upto 4.5 km Deployment range applicable in Point to Point deployment. Please change for the far end node first.

Adaptive Modulation

Minimum MCS
2 Range - [2, 12]

Maximum MCS
12 Range - [2, 12]

Sector 1

Channel/Polarity should originate from leaf nodes. Please make sure to change on the CNs first and then higher up on the DNs.

Override	Name	Auto Configuration	Node Configuration
<input checked="" type="checkbox"/>	Channel	-	2
<input type="checkbox"/>	Polarity	Odd	

Sector 1 Link (s) Golay

Override	Name	Auto Configuration (Rx/Tx)	Node Golay Rx	Node Golay Tx
<input type="checkbox"/>	link DN-D6-PoP-Onboard-V5k-3083	1/1		

[Override All](#)

GPS

☐ Force GPS Disable GPS sync at initiator/responder during assoc

Save Reset

Network

Network tab allows the user to edit the **Layer 3 CPE**, **IPv4 Management**, **Ethernet Ports**, **PTP External Failover**, and **Other Settings**.

Figure 381 *Network*

60 GHz cnWave > DN-D6

Dashboard Notifications **Configuration** Links Details Performance Software Update Tools

Basic Radio **Network** VLAN Security Advanced

IPv6 Layer 3 CPE

IPv6 CPE interface
☐ Aux ☒ Main ☐ SFP ☐ Disabled Choose the interface to run IPv6 SLAAC. Subnet allocated by the controller will be used as Prefix. This interface will not be part of Layer 2 bridge. Should be disabled for IPv4 CPE.

IPv6 CPE Prefix
 If empty, Subnet prefix allocated by the controller to the node will be used.

IPv4 Management

IPv4 Address
 IPv4 Management access is not allowed over IPv6 CPE INTERFACE

Subnet Mask

Gateway IP Address

Ethernet Ports

☒ Enable Main
☒ Enable Aux
☒ Enable SFP

DHCP Option 82

Insert DHCP Option 82
☐ Enabled ☒ Disabled DHCP option 82 will be inserted in the DHCP requests.

Other Settings

☐ Enable Aux port power Enables the power out on the Aux port

Relay Port Interface
☐ Aux ☐ Main ☐ SFP ☒ Disabled Wired interface on which OpenR is run. Should be used when DNs are connected back to back and on PoPs in a multi PoP network.

VLAN

VLAN configuration of CN/DN is same as PoP Node VLAN as shown [above](#).



Note

Enable Layer 2 Bridge in **60 GHz cnWave > Configuration > Basic** page to configure the CN/DN VLAN.

Security

Security tab allows to reset the identity and password of the Radius user.

Figure 382 *Security*

60 GHz cnWave > DN-3D

Dashboard Notifications **Configuration** Links Details Performance Software Update Tools

Basic Radio Network VLAN **Security** Advanced

Radius user identity

Private key password
 Radius Private key password

Radius user password
 Radius user password

Advanced

Advanced tab allows the advanced user to set Field Name and Value.

1. Navigate to **Configuration > Advanced**.
2. Click **Add New**.

60 GHz cnWave > DN-3D

Dashboard Notifications **Configuration** Links Details Performance Software Update Tools

Basic Radio Network VLAN Security **Advanced**

All the settings below are for advanced users only.

Search Table JSON Add New

Field	Description	Status	Value	
snmpConfig.location	System location.	set	No Location	
snmpConfig.contact	System contact.	set	No Contact	
logTailParams.sources.terragraph_openr_logs.filename	The log file name.	set	/var/log/openr/current	
logTailParams.sources.terragraph_openr_logs.enabled	Enable tailing from this source.	set	true	
logTailParams.sources.terragraph_minion_logs.filename	The log file name.	set	/var/log/e2e_minion/current	
logTailParams.sources.terragraph_minion_logs.enabled	Enable tailing from this source.	set	true	
logTailParams.sources.terragraph_kern_logs.filename	The log file name.	set	/var/log/kern.log	
logTailParams.sources.terragraph_kern_logs.enabled	Enable tailing from this source.	set	true	
popParams.POP_STATIC_ROUTING	Enable static routing on the POP.	set	0	
popParams.POP_IFACE	The interface on the POP node that routes traffic to the Gateway.	unset		
popParams.VPP_ADDR	The IP address of the interface within VPP on the POP node (Fast Path edge address).	unset		
popParams.NAT64_IPV6_PREFIX	NAT64 IPv6 prefix. Can use 64:ff9b::96 (well-known prefix).	unset		
popParams.POP_BGP_ROUTING	Enable BGP routing on the POP.	set	0	
popParams.POP_ADDR	The IP address of the interface on the POP node that routes to the Gateway.	unset		
popParams.NAT64_POP_ENABLED	Enable NAT64 on POP interface for IPv6 to IPv4 NAT	set	0	

Save Reset [Show Full Configuration](#)

3. Enter the **Field Name** and **Value**.

Add new field

Field Name String

Value

Save Cancel

4. Click **Save**.

JSON

JSON allows Advanced users to view the JSON format.

60 GHz cnWave Network > Ext-E2E-100

Dashboard Notifications **Configuration** Links Statistics Report **X** Software Update Tools

Basic Management Radio Security **Advanced** E2E Controller

All the settings below are for advanced users only.

Search

Base : default Firmware : 10.11.0.97 Hardware : V1000 Optimization Table **JSON** Add New

```
{
  "envParams": {
    "CAMBIUM_L2_BRIDGE_IFACE": ""
  },
  "sysParams": {
    "disableCNChannelRescan": true,
    "ntpServers": [
      "f": "fd10:ba5e::100"
    ]
  }
}
```

Save Reset

Device Logs

☐ Enable Recommended to be used only by Cambium Support Team.

Update

To download the file, perform the following steps:

1. Navigate to **Configuration > Advanced > JSON**.

60 GHz cnWave Network > Ext-E2E-100

Dashboard Notifications **Configuration** Links Statistics Report **X** Software Update Tools

Basic Management Radio Security **Advanced** E2E Controller

All the settings below are for advanced users only.

Search

Base : default Firmware : 10.11.0.97 Hardware : V1000 Optimization Table **JSON** Add New

```
{
  "envParams": {
    "CAMBIUM_L2_BRIDGE_IFACE": ""
  },
  "sysParams": {
    "disableCNChannelRescan": true,
    "ntpServers": [
      "f": "fd10:ba5e::100"
    ]
  }
}
```

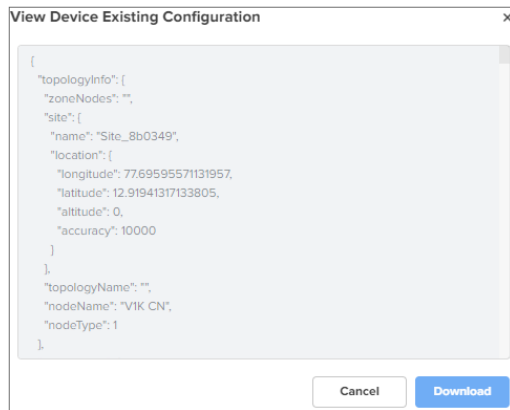
Save Reset

Device Logs

☐ Enable Recommended to be used only by Cambium Support Team.

Update

2. Click **Show Full Configuration**.
3. **View Device Existing Configuration** pops up.



4. Click **Download**.

Links

Links provide the details about links of the node and also provides the option to create a new link. User can delete the links in bulk by selecting the particular devices.

List

List provide the details about the links of the node and also provides the option to create a new link. User can delete the links in bulk by selecting the particular link.

Figure 383 *List*

Name	A-Node	Z-Node	A-Node MAC	Z-Node MAC	Alive	Link Time
link DN D6 PoP Onboard V5k 3083	DN D6	PoP Onboard V5k 3083			Yes	42d 20h 3m

Statistics

Links Statistics pages provides details of **Basic**: Name, Direction, A-Node, Z-Node Alive Link Time Type Distance Azimuth, Rx Golay, Tx Golay **Detailed Statistics**: A-Node Sector MAC, Z-Node Sector MAC, RSSI, Rx Airtime%, Rx Beam Azimuth Angle, Rx Beam Elevation Angle, Rx SNR, Rx MCS, Rx PER, Rx Scan Beams, Rx Throughput, Tx Beam Azimuth Angle, Tx Power Index, EIRP, Tx MCS, Tx PER, Tx Scan Beams, Rx Errors, Rx Frames, Tx Errors, Tx Frames, Rx Time, Tx Airtime%, Tx Beam Azimuth Angle, Tx Beam Elevation Angle, Tx Throughput, Tx Time, and Link Fade Margin links created with DN/CN node, in a page format.

Name	Direction	A-Node Sector M...	Z-Node Sector M...	Alive	Link Time	RSSI	Rx SNR	Rx MCS	Tx Power Index	EIRP	Tx MCS
link APOP DN B0	APOP to DN B0			Yes	1d 15h 58m	40 dBm	32 dB	10	6	13 dBm	9
link APOP DN B0	DN B0 to APOP			Yes	1d 15h 58m	37 dBm	32 dB	10	6	13 dBm	10
link CN 75 DN B0	CN 75 to DN B0			Yes	0d 5h 39m	62 dBm	12 dB	7	6	13 dBm	9
link CN 75 DN B0	DN B0 to CN 75			Yes	0d 5h 39m	48 dBm	25 dB	9	23	30 dBm	9
link CN 83 DN B0	CN 83 to DN B0			Yes	0d 13h 30m	53 dBm	21 dB	9	6	35 dBm	9
link CN 83 DN B0	DN B0 to CN 83			Yes	0d 13h 30m	49 dBm	23 dB	9	6	13 dBm	9
link DN 39 DN B0	DN 39 to DN B0			Yes	0d 9h 30m	48 dBm	25 dB	9	6	13 dBm	10
link DN 39 DN B0	DN B0 to DN 39			Yes	0d 9h 30m	45 dBm	28 dB	9	6	13 dBm	9

Events

Events provide the details of link availability, hourly link availability in percentage, link availability in different time lines, and distance of the link.

Figure 384 *Events*

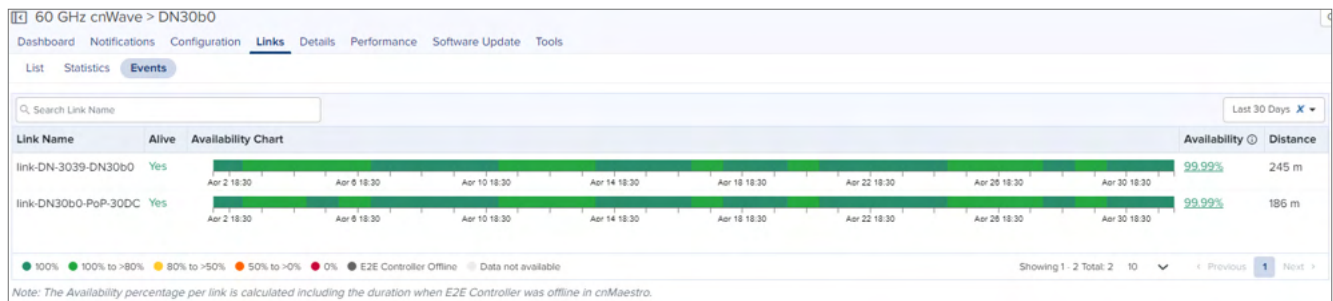


Table 83 *Events fields*

Field	Description
Link Name	Name of the link.
Alive	Status of the link (Yes or No).
Availability Chart	Displays the link availability based on time range selected from the dropdown. When you hover the mouse on the Availability Chart, the link availability is shown as described: <ol style="list-style-type: none"> If you select time range as Last 1 Hour, then link availability for every 5 minutes is displayed. If you select time range other than Last 1 Hour, then link availability for every 1 hour is displayed. <ul style="list-style-type: none"> Hover on the link to see the hourly availability as shown in Figure 355. Clicking on percentage link availability displays pop-up window as shown in Figure 356 Link availability is presented in different colors in the chart as shown in Figure 354
Availability Percentage	<ul style="list-style-type: none"> Clicking on percentage for the complete timeline link availability displays pop-up window as shown in Figure 386. Availability of link is shown in percentage in the Availability column as shown in Figure 355.
Distance	Distance of the link in meters.

Figure 385 *Link Availability in Percentage*



Figure 386 Link Availability details

Status	From	To	Duration
Online	Apr 06 2022 17:30:00	Apr 06 2022 17:56:20	26m 20s
Offline	Apr 06 2022 17:56:20	Apr 06 2022 17:56:24	< 1m
Online	Apr 06 2022 17:56:24	Apr 07 2022 13:50:27	19h 54m 3s
Offline	Apr 07 2022 13:50:27	Apr 07 2022 13:59:24	8m 56s
Online	Apr 07 2022 13:59:24	Apr 07 2022 15:11:30	1h 12m 5s
Offline	Apr 07 2022 15:11:30	Apr 07 2022 15:11:33	< 1m
Online	Apr 07 2022 15:11:33	Apr 07 2022 15:19:51	8m 17s
Offline	Apr 07 2022 15:19:51	Apr 07 2022 15:20:33	< 1m
Online	Apr 07 2022 15:20:33	Apr 07 2022 15:20:38	< 1m
Offline	Apr 07 2022 15:20:38	Apr 07 2022 15:20:55	< 1m
Online	Apr 07 2022 15:20:55	Apr 07 2022 15:21:41	< 1m
Offline	Apr 07 2022 15:21:41	Apr 07 2022 15:21:55	< 1m
Online	Apr 07 2022 15:21:55	Apr 07 2022 15:22:16	< 1m
Offline	Apr 07 2022 15:22:16	Apr 07 2022 15:22:30	< 1m
Online	Apr 07 2022 15:22:30	Apr 07 2022 15:28:41	6m 10s
Offline	Apr 07 2022 15:28:41	Apr 07 2022 15:30:31	1m 49s
Online	Apr 07 2022 15:30:31	Apr 07 2022 15:30:35	< 1m
Offline	Apr 07 2022 15:30:35	Apr 07 2022 15:30:41	< 1m
Online	Apr 07 2022 15:30:41	Apr 07 2022 15:30:45	< 1m
Offline	Apr 07 2022 15:30:45	Apr 07 2022 15:30:45	< 1m
Online	Apr 07 2022 15:30:45	Apr 07 2022 18:24:19	2h 53m 34s
Offline	Apr 07 2022 18:24:19	Apr 07 2022 18:24:25	< 1m
Offline	Apr 08 2022 19:17:51	Apr 08 2022 19:17:55	< 1m
Online	Apr 08 2022 19:17:55	Apr 11 2022 18:50:05	2d 23h 32m 9s
Offline	Apr 11 2022 18:50:05	Apr 11 2022 18:50:11	< 1m
Online	Apr 11 2022 18:50:11	Apr 12 2022 18:19:00	23h 28m 48s
Offline	Apr 12 2022 18:19:00	Apr 12 2022 18:19:06	< 1m
Online	Apr 12 2022 18:19:06	Apr 12 2022 20:22:46	2h 3m 39s
Offline	Apr 12 2022 20:22:46	Apr 12 2022 20:22:51	< 1m
Online	Apr 12 2022 20:22:51	Apr 13 2022 18:30:00	22h 7m 8s

Showing 1 - 25 Total: 25 < Previous 1 Next >

Availability percentage per link is calculated including the duration when E2E Controller was Offline in cnMaestro.

Figure 387 Link Availability

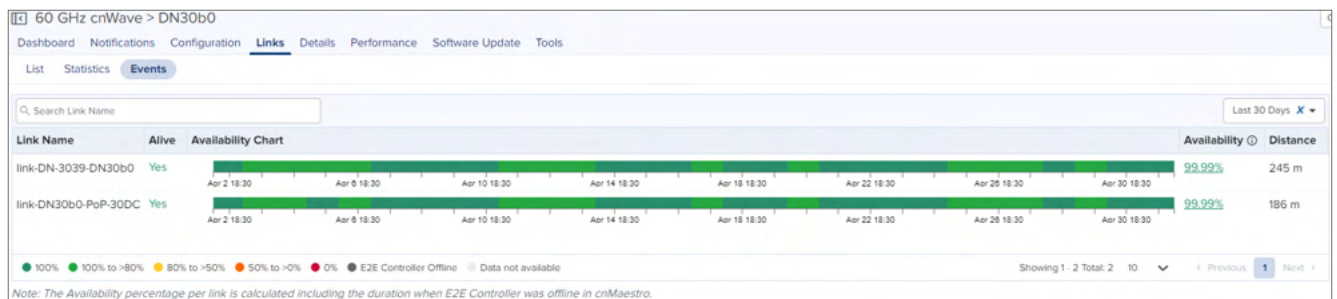
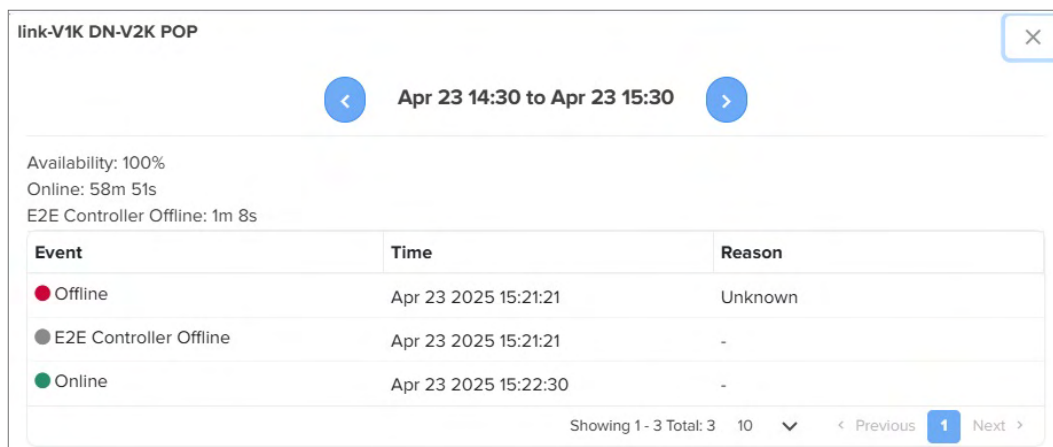


Figure 388 Link Status



Events details are available for Last 1 hour, Last 6 hours, Last 12 hours, Last 24 Hours, Last 2 days, Last 4 days, and Last 7 days.



Note

Event details for **Custom Range** and **Last 30 days** is available only for cnMaestro X users.

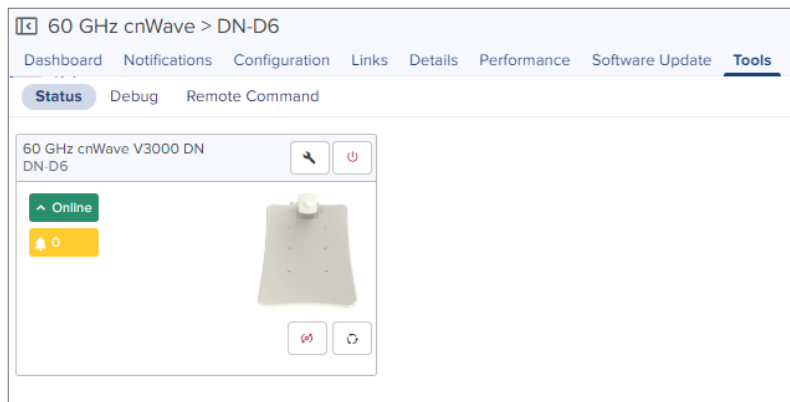
Tools

In Tools page you can view the **Status** and **Debug** details of the device.

Status

In **Status** tab you can view the status of the device:

- Critical alarms
- Download Tech Support File
- Online or Offline
- Reboot the device.
- Restart Minion
- Factory reset



Debug

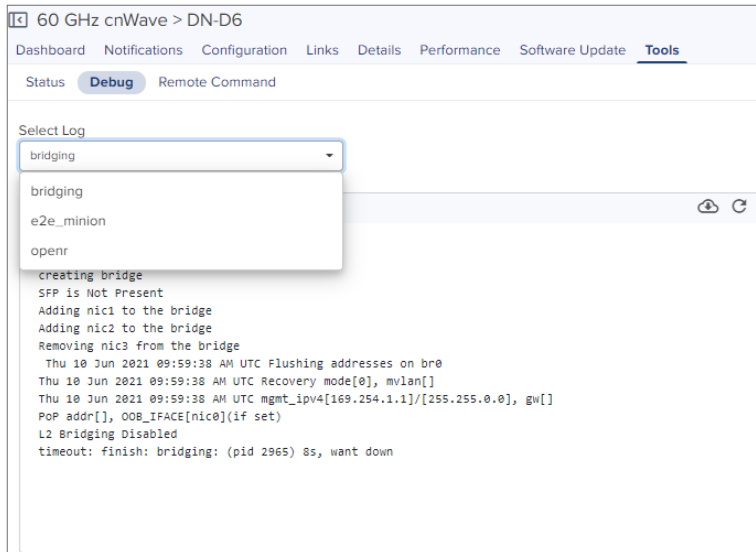
In **Debug** tab, you can view or download the DN or CN logs by executing the following log commands:



- Bridging
- e2e_minion
- openr

To view the logs:

1. Navigate to **Tools > Debug**.
2. Select the required log name from the **Select Log** dropdown list.

The output for the selected criteria appears as shown:



- Click the download  icon to download the generated output.
- Click the clear  icon to clear the generated output.

Remote Command

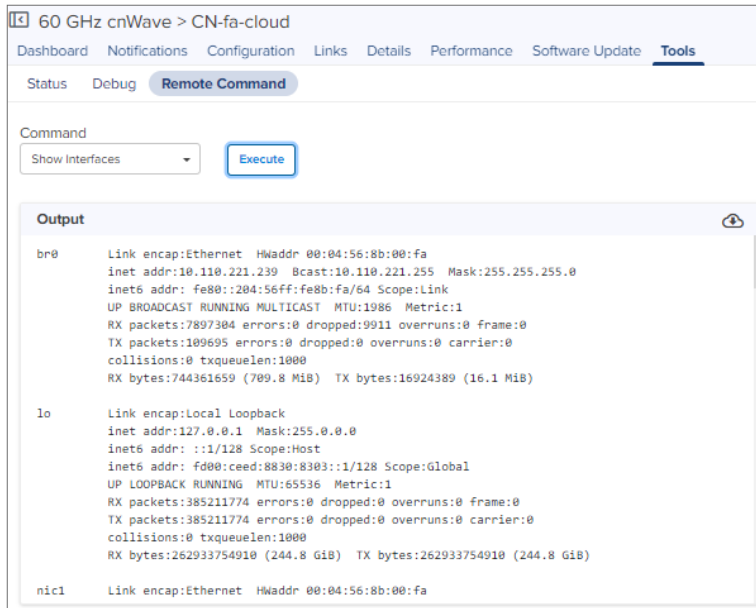
In **Remote command** tab, you can view and download Command logs by executing the following commands:



- Ping
- Show IGMP Membership Table
- Show Interfaces
- Show IPv4 Neighbors
- Show IPv6 Neighbors
- Show MAC Address Table
- Show OpenR Adjacencies
- Show OpenR Prefixes
- Show Routes
- Show SFP Power Details (applicable for V5000 and V3000)
- Show Wired Interface State Changes

To Execute the command:

1. Navigate to **Tools > Remote Command**.
2. Select the required command from the **Command** dropdown.
3. Click **Execute**.

The output for the selected criteria appears as shown:



- Click the download  icon to download the generated output.
- Click the clear  icon to clear the generated output.

Managing NSE 3000 using cnMaestro

NSE 3000 is managed using the cloud-hosted cnMaestro (a management solution from Cambium Networks).

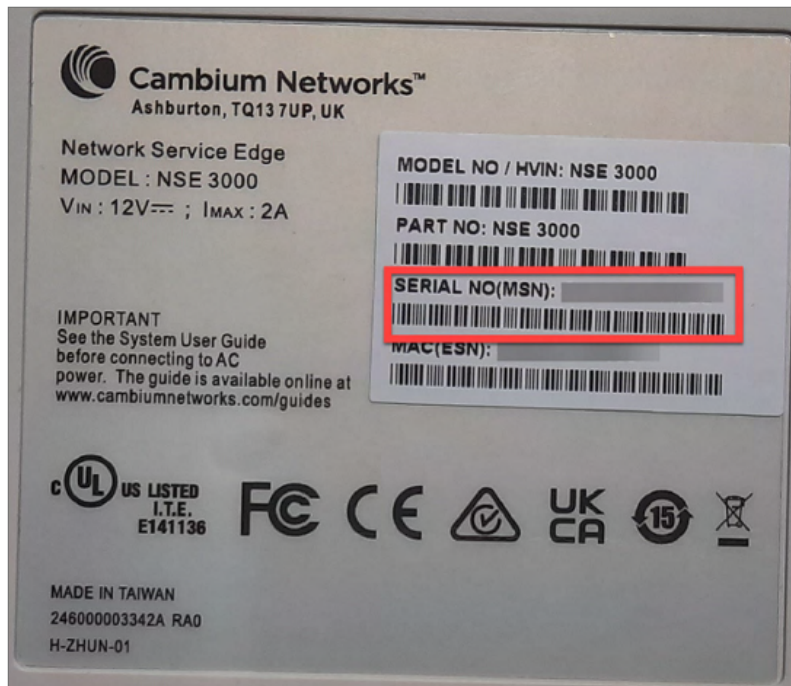
This section covers the following topics:

- [Claiming an NSE 3000 device associated with a site](#)
- [High availability support for NSE 3000](#)
- [Configuring NSE 3000](#)
- [Configuring WAN in the device UI](#)
- [Configuring Auto VPN](#)
- [Disabling or Enabling the Security Plus License Mode for NSE](#)

Claiming an NSE 3000 device associated with a site

A device manufacturer serial number (MSN) is required to claim an NSE 3000 device. You can find the device MSN at the bottom of the device as shown in [Figure 389](#).

Figure 389 MSN of the NSE 3000 device

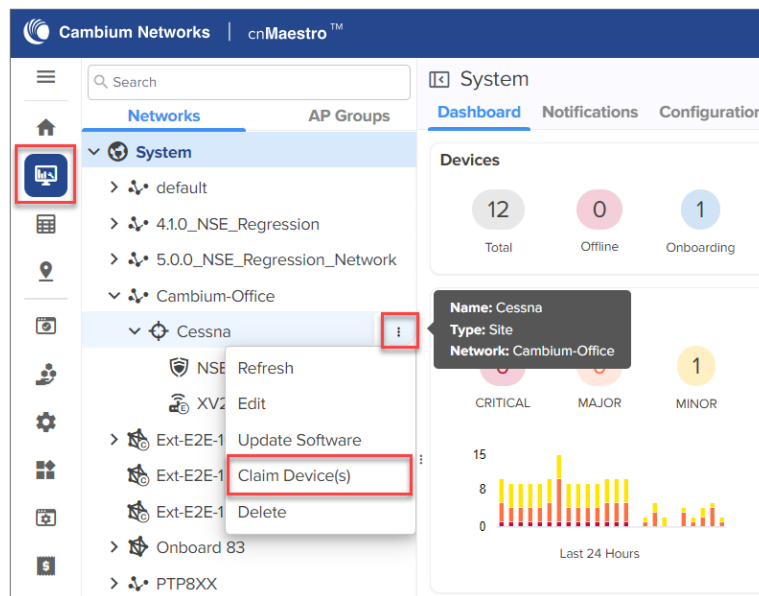


To claim an NSE 3000 device that is associated with a site, complete the following steps:

1. From the home page, navigate to **Monitor and Manage**.

The **System** page appears, as shown in [Figure 390](#).

Figure 390 The System page



2. On the left panel, in the **Networks** section, expand the site panel.
3. Click the actions (⋮) icon and select **Claim Device(s)**.

The **Claim Enterprise Devices** window appears, as shown in [Figure 391](#).

Figure 391 *The Claim Enterprise Devices window*

Claim Enterprise Devices

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

Managed Account: Base Infrastructure

Site: _Network_

Device Type
All

NSE Group
Default NSE (Default)

Switch Group
None

Enterprise (E-Series and XE/XV/X7-Series) AP Group
None

Enter / Place a cursor in the box and use a barcode scanner to quickly claim devices.

Note: The Bulk CSV Import feature is currently available only for specific device types. To use this feature, please select either cnMatrix or Enterprise Wi-Fi from the Device Type dropdown menu.

[Learn more](#)

Clear Cancel Claim Devices

- From the **NSE Group** dropdown list, select the required group.



Note

The selected NSE group is automatically pushed to the device while onboarding.

- In the **Enter** field, enter the MSN of the NSE 3000 device.
- Click **Claim Devices**.

The NSE 3000 device that is associated with a site is claimed successfully.

High availability support for NSE 3000

The high availability (HA) support allows two NSE 3000 devices to share health information when connected through a LAN port (Port-6). When the devices are connected as an HA pair, one is configured as **Primary** and the other as **Spare**. The **Spare** device serves as a backup in case of hardware failures.

If the **Primary** device goes down, the **Spare** device becomes active. When the **Primary** device is restored, it regains its active state and the **Spare** device reverts to a backup state.



Note

The HA support is available from NSE release version 1.7 and higher.

Licensing

An NSE 3000 device requires a Tier-30 license to onboard to cnMaestro.

An HA pair (Primary - Spare) requires only one Tier-30 license. The **Spare** device does not require an additional license as it inherits the license from the **Primary** device.

On the expiry of the license, the device management is deactivated using cnMaestro. However, the devices are not deleted from the device list in cnMaestro.

Constraints on NSE 3000 devices

The following are the constraints on NSE 3000 devices in cnMaestro:

- A site can have either a single NSE 3000 device or a single NSE 3000 HA pair.
- An HA pair can only be created under a site. NSE group is mandatory for all NSE 3000 devices to onboard to the cnMaestro cloud 5.1.1 version.
- An NSE 3000 device must exist (with an NSE group attached) under the site to form an HA pair.
- If a device is in the **Onboarding** state under a site, you cannot claim another device under the same site.

Creating an HA pair in cnMaestro

You can create an HA pair using either of the following options:

- **Onboard as HA spare** (from the Onboarding queue)
- **Claim Device(s)** (at the site level)

The HA pair configuration involves the following tasks:

- [Onboarding an NSE 3000 device as an HA spare](#)
- [Claiming an NSE 3000 device as an HA spare](#)
- [Moving the HA pair \(in the tree\)](#)
- [Deleting an NSE 3000 device from the HA pair](#)
- [Deprecation of device overrides](#)
- [Upgrading the firmware](#)
- [Viewing aggregated data of HA pair](#)
- [Creating Wireguard clients for NSE HA pair](#)

Onboarding an NSE 3000 device as an HA spare

The primary device onboards as a standalone device to cnMaestro. An additional NSE 3000 device can be brought into the onboarding queue (without Tier-30 license) either by bulk claim (on the Onboard page) or using cambium-id and password. An HA pair is formed using the **Onboard as HA spare** option from the **Approve Device** window.



Note

- The primary device must have the firmware that supports HA functionality.
- The spare device must have the same firmware as the primary device. Otherwise, the system automatically upgrades the firmware of the spare device to match with the primary device.
- The spare device must have the same model as the primary device. NSE 3000 device can be paired only with an NSE 3000 device model. It cannot be paired with an NSE 5000 device model.

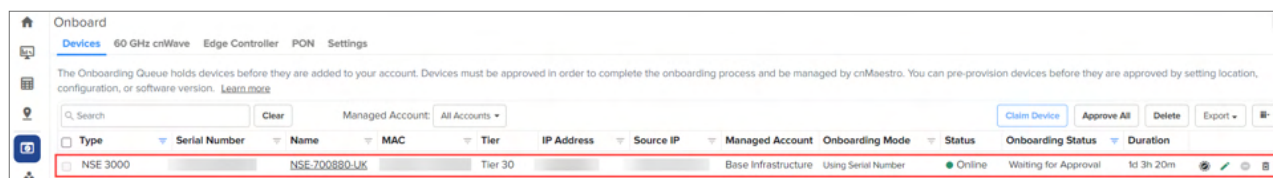
When onboarding an NSE 3000 device as a spare, the device automatically inherits the NSE group of the primary device. This holds good even if the devices are claimed at the site level. Additionally, any change in the NSE group of the primary device is automatically reflected in the spare device.

To onboard an NSE 3000 device as a spare device, complete the following steps:

1. From the home page, click the Onboard () icon.

The Onboard page appears.

Figure 392 *The Onboard page*



2. Click the approve device () icon of the NSE 3000 device.

The **Approve Device** window appears with the **Onboard as HA spare** option and shows all sites that have only one NSE device (as shown in [Figure 393](#)).

Figure 393 *The Approve Device window*



Note

The spare device has the same NSE group as that of the primary device.

3. Click **Save and Approve** from the **Approve Device** window (as shown in [Figure 393](#)).

The spare device is onboarded (as shown in [Figure 394](#)) without an additional Tier-30 license.

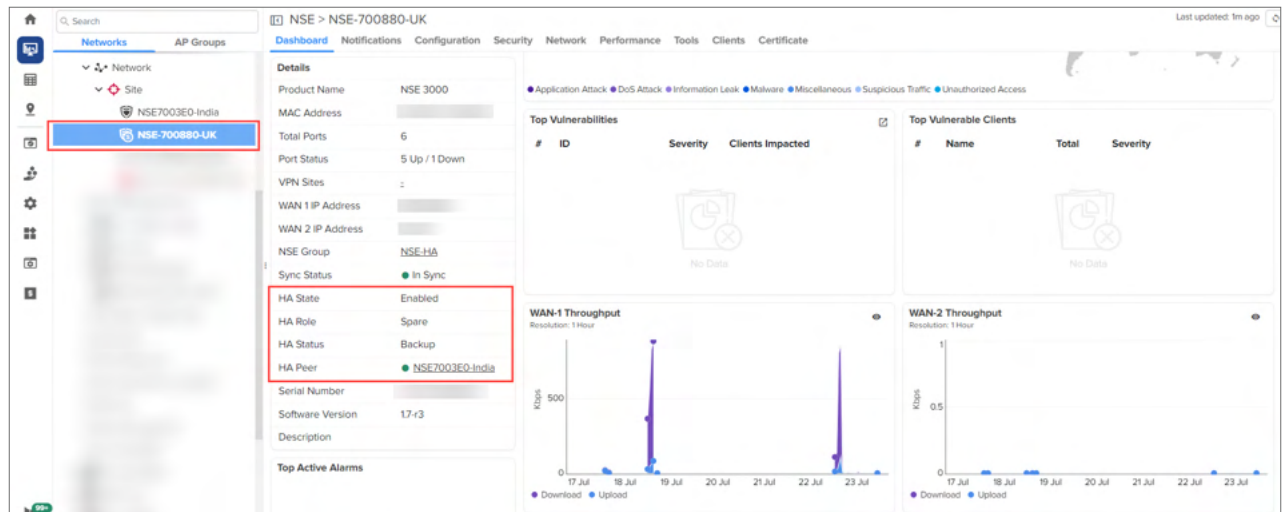
Figure 394 Spare device onboarded

Type	Serial Number	Name	MAC	Tier	IP Address	Source IP	Managed Account	Onboarding Mode	Status	Onboarding Status	Duration
NSE 3000	NSE-700880-UK			Tier 30			Base Infrastructure	Using Serial Number	Online	Onboarded	2d 2h 55m

- Click on the spare device name.

You can see the spare device under a site (as shown in [Figure 395](#)). You can view the HA details in the **Details** section of the dashboard (as shown in [Figure 395](#)).

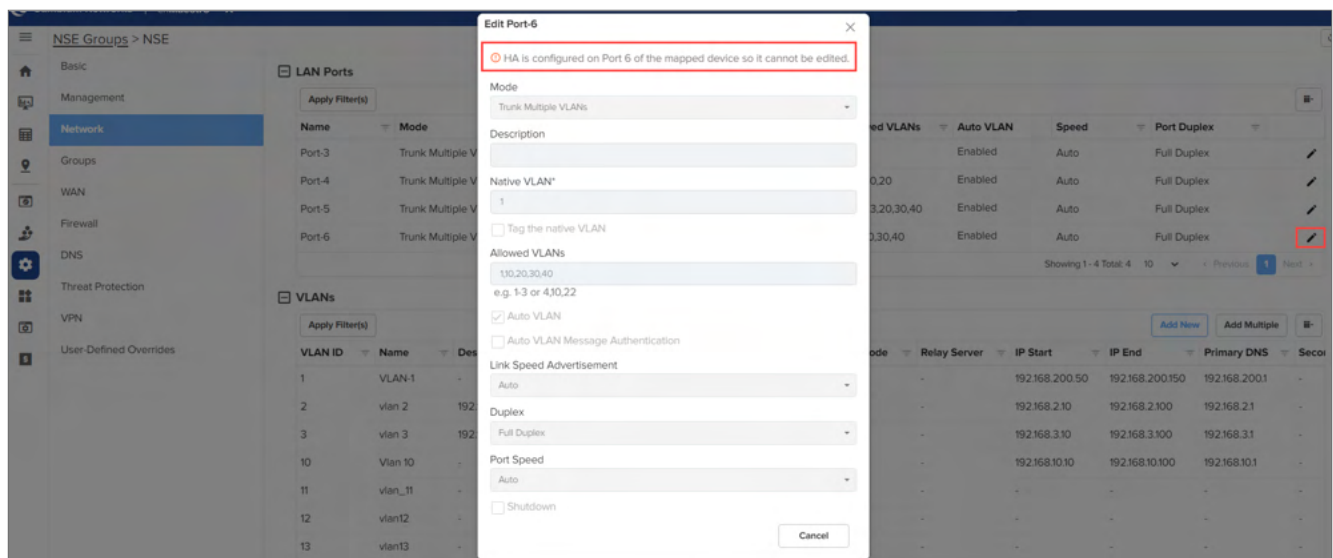
Figure 395 Details about HA for the Spare device



Note


When HA is configured on Port-6 of the mapped device, you cannot edit the Port-6 configuration. A message is displayed on the **Edit Port-6** window (as shown in [Figure 396](#)).

Figure 396 The Edit Port-6 window



Note



The fields in the **Approve Device** window (as shown in [Figure 393](#)) can also be configured using the

Edit Device () icon from the **Onboard** page.

Claiming an NSE 3000 device as an HA spare

An NSE 3000 HA pair can be additionally formed using the **Claim Device(s)** option at the site level. When a second NSE 3000 device is claimed (assuming the primary already exists under the site), you have the option to claim it as a spare. However, claiming a second NSE 3000 device under the same site as a regular device is restricted.

To claim an NSE 3000 device as an HA spare, complete the following steps:

1. From the home page, click the Monitor and Manage () icon.
The **System** page appears.
2. On the left panel, in the **Networks** section, expand the site panel.
3. Click the actions () icon and select **Claim Device(s)**.
The **Claim Enterprise Devices** window appears.
4. In the **Enter** field, enter the MSN of the NSE 3000 device.



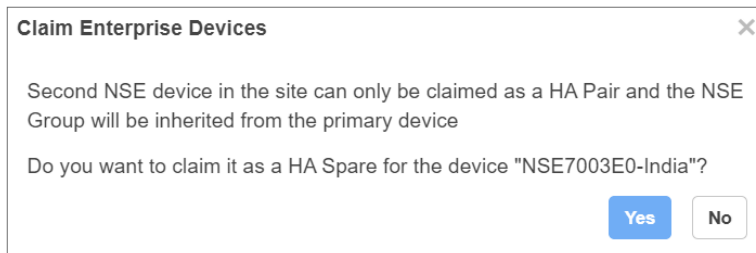
Note

You can find the device MSN at the bottom of the NSE 3000 device.

5. Click **Claim Devices**.

The **Claim Enterprise Devices** window appears.

Figure 397 The Claim Enterprise Devices window



Claim Enterprise Devices [X]

Second NSE device in the site can only be claimed as a HA Pair and the NSE Group will be inherited from the primary device

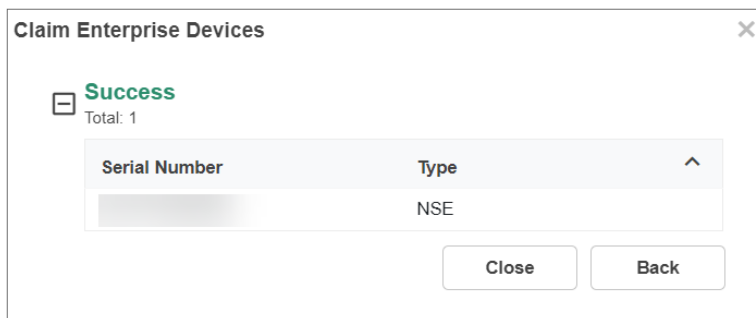
Do you want to claim it as a HA Spare for the device "NSE7003E0-India"?

Yes **No**


6. Click **Yes**.

The **Claim Enterprise Devices** window appears.

Figure 398 The Claim Enterprise Devices window



Claim Enterprise Devices [X]

 **Success**
Total: 1

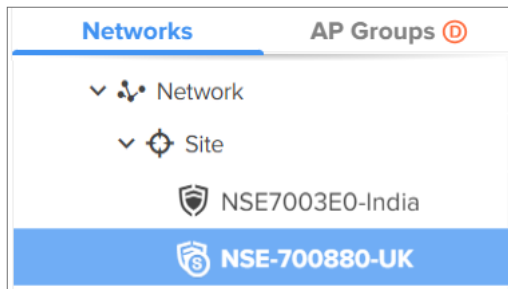
Serial Number	Type
[blurred]	NSE



Close **Back**

7. Click **Close**.

The device is claimed as an HA spare.

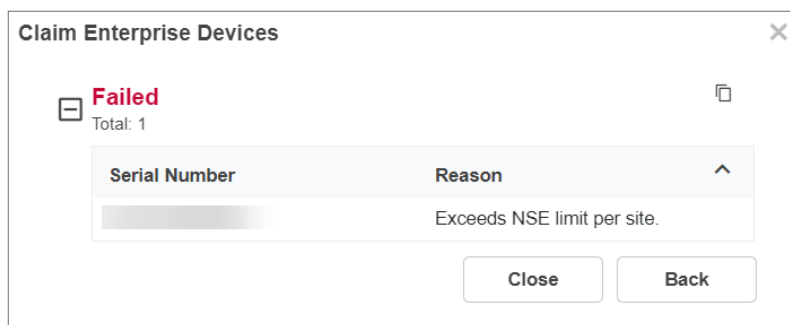
Figure 399 Device claimed as an HA spare



The () icon indicates the primary NSE 3000 device. The () icon indicates the spare NSE 3000 device.

When you click **No** in the **Claim Enterprise Devices** window (as shown in [Figure 397](#)), the **Claim Enterprise Devices** window appears (as shown in [Figure 400](#)). You cannot claim the device as an HA spare.

Figure 400 The Claim Enterprise Devices window



Moving the HA pair (in the tree)

The NSE 3000 HA pair can be moved as a single unit only. This can be done by changing the Network and Site for the primary device. The devices in the pair cannot be moved individually. Moreover, the NSE 3000 device or HA pair can only be moved to a site that has no NSE 3000 devices. Moving to a network is not allowed.



Note

An HA pair of NSE 3000 devices shares the same NSE group. Consequently, the NSE group selection for the spare device is disabled.

Deleting an NSE 3000 device from the HA pair

If one of the NSE 3000 devices in a pair is deleted, the other NSE 3000 device becomes standalone.

- When the primary device is deleted from the pair, the spare device becomes a standalone device and the pair's Tier-30 license is mapped to the spare device (instead of the primary device). Also, a configuration job for this standalone device with HA mode **Disable** is triggered.
- When the spare device is deleted from the pair, the primary device becomes a standalone device.
- When both primary and spare devices are deleted, a slot is released.

Deprecation of device overrides

The device overrides are removed from the Onboard page. The bulk overrides cannot be done for NSE 3000 devices.

When HA is enabled in the NSE group, the device overrides in the device context are hidden.

Figure 401 Device overrides are not applied when HA is enabled

NSE Groups > Add New

Basic

Management

Network

Groups

WAN

Firewall

Basic Information

Name*
Test_NSE
Maximum number of characters allowed is 64

Scope
Shared

☒ Auto Sync Automatically push configuration changes to devices sharing this NSE Group

☒ Enable HA With HA mode enabled, device overrides will not be applied (User-Defined overrides will continue to work).



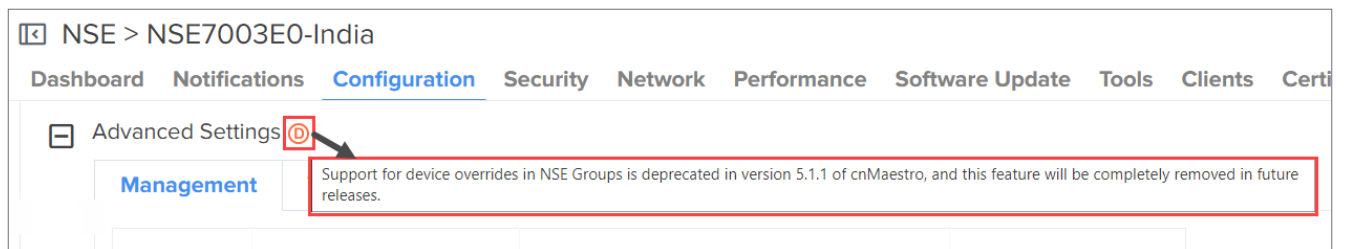
When HA is disabled in the NSE group, the deprecated icon () is shown. Device overrides are being deprecated for NSE devices in the 5.1.1 version. When you hover the cursor over the deprecated () icon, a message about the deprecation is displayed (as shown in [Figure 402](#)).

Figure 402 A deprecation message



Upgrading the firmware

When you upgrade the firmware on the primary device, the firmware on the spare device is automatically upgraded. This ensures that both primary and spare devices run the same version.



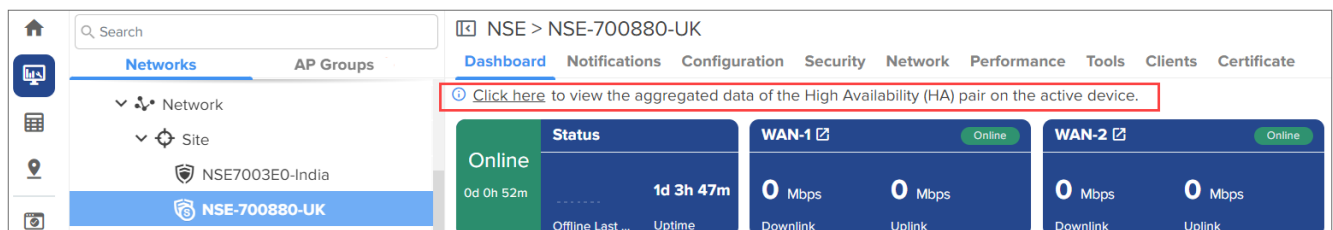
Note

The **Software Update** tab is available only for the primary device.

Viewing aggregated data of HA pair

In an HA pair, the active NSE 3000 device shows the aggregated data for the pair. In the spare NSE 3000 device, a banner provides a link to the active device's page (as shown in [Figure 403](#)) to view the aggregated data. The same banner is displayed under the **Security > Threats**, **Security > Vulnerabilities**, and **Clients > Local** tabs.

Figure 403 Banner



Note

- If the active device is offline, the aggregated data is not shown.

Creating Wireguard clients for NSE HA pair

When adding Wireguard clients from the **VPN** page, only the primary device is listed in the **Device** dropdown list (as shown in [Figure 404](#)).

Figure 404 The Add New User window -Wireguard

Add New User

Email ID*

Password*

☒ Enable WireGuard

☐ Enable Split Tunnel

Device

NSE7003E0-India

Domain name or IP4 address

Clients

Apply Filter(s) [Add New](#)

Name	IP Address	Client Public Key
No Data Available		

Showing 0 - 0 Total: 0 100 < Previous Next >

[Close](#) [Add](#)

Configuring NSE 3000

To configure NSE 3000 devices, create configuration profiles called NSE Groups. To create and configure a new NSE 3000 group, navigate to **Configuration > NSE Profiles**. Select the **NSE Groups** tab and click **Add New**.

Figure 405 Creating NSE groups

NSE Profiles

[NSE Groups](#) [Auto VPNs](#)

Change Filter(s) Clear Managed Account: All Accounts

[Add New](#) [Import](#)

Name	Device Status	Managed Account	Auto Sync	Last Updated	Last Updated By	Origin
NSE_RAGUL_LIMA_2_NEW	0 of 1 offline	Shared	ON	24 Apr 2025, 10:27 AM	Surya Kantha Rao	Custom
nse_auto_group_for_30-CB-C7-70-06-60_1	0 of 1 offline	Shared	ON	24 Apr 2025, 10:08 AM	app#ID0tHngxOzRPaHOM	Custom
nse_auto_group_for_30-CB-C7-70-05-10	0 of 1 offline	Shared	ON	24 Apr 2025, 10:07 AM	app#ID0tHngxOzRPaHOM	Custom
nse_auto_group_for_30-CB-C7-70-08-BQ	0 of 0 offline	Shared	ON	24 Apr 2025, 09:57 AM	app#ID0tHngxOzRPaHOM	Custom
nse_auto_group_for_30-CB-C7-70-06-60	0 of 0 offline	Shared	ON	24 Apr 2025, 09:54 AM	app#ID0tHngxOzRPaHOM	Custom
nse_auto_group_for_30-CB-C7-70-05-10_1	0 of 0 offline	Shared	ON	24 Apr 2025, 09:52 AM	app#ID0tHngxOzRPaHOM	Custom
Hub.NSE.Doc.Team	0 of 1 offline	NSE MSP	ON	23 Apr 2025, 05:30 PM	Vijay Yadav	Custom

For a new NSE group, you must configure parameters using the following tabs:

- [Basic](#)
- [Management](#)
- [Network](#)
- [Groups](#)
- [WAN](#)
- [Firewall](#)
- [DNS](#)
- [Threat Protection](#)
- [VPN](#)
- [User-Defined Overrides](#)

Basic

Using the **Basic** tab, you can configure basic group information, such as group name and group scope. You have the option to enable automatic synchronization of the configuration changes for devices associated with the NSE group.

To configure parameters on the **Basic Information** page, complete the following steps:

1. Navigate to **Configuration > NSE Groups** and click **Add New**

The **Basic Information** page appears, as shown in [Figure 406](#).

Figure 406 The Basic Information page

2. Configure the parameters, as described in [Table 84](#).

Table 84 Parameters on the Basic Information page

Parameter	Description
Name	Name for the NSE group.

Parameter	Description
	<p>This parameter allows a maximum of 64 characters.</p> <p>This is a mandatory parameter.</p>
Scope	<p>Scope determines the availability of the NSE group across different tenant accounts.</p> <p>By default, the following options are supported:</p> <ul style="list-style-type: none"> • Shared - Configured NSE group will be available to other tenant accounts. • Basic Infrastructure - Configured NSE group will be available only to the Basic Infrastructure user. Other tenant accounts will not have access to the NSE group.
Auto Sync	<p>Specifies whether the configuration changes made to the NSE group are automatically applied to all devices associated with the group.</p> <p>By default, auto sync is enabled.</p>
Enable HA	<p>Enables or disables the HA.</p> <p>By default, this parameter is disabled.</p> <p>Note:</p> <p>When this parameter is enabled, you must configure the IP Address (HA Spare) parameter by selecting the Static option from the IP Address Assignment dropdown list in the WAN Configurations section of the WAN screen (as shown in Figure 407).</p>

Figure 407 The WAN Configurations section

WAN Configurations

WAN-1 **WAN-2**

IP Address Assignment

Static

IP Address*

10.110.185.165

IP Address (HA Spare)*

10.110.185.163

Subnet Mask*

255.255.255.0

Default Gateway

10.110.185.254

3. Click **Save**.

Management

Using the **Management** tab, you can configure the profile-related parameters such as time settings and event logging.

To configure parameters on the **Management** page, complete the following steps:


1. On the **NSE Groups > Add New** page, select the **Management** tab.

The **Management** page appears, as shown in [Figure 408](#).

Figure 408 *The Management page*

2. Configure the parameters, as described in [Table 85](#).

Table 85 *Parameters on the Management page*

Parameter	Description
On the Management page, there are Management , Time Settings , and Event Logging sections.	
Management	
Admin Password	<p>The password used to authenticate the NSE 3000 users who access through SSH or web.</p> <p>This parameter allows a maximum of 32 characters.</p> <p>This is a mandatory parameter.</p> <p>Note: Click the edit  icon to reset the password.</p>
Time Settings	
Time Zone	<p>The time zone based on the installation location of the device.</p> <p>Select an appropriate time zone from the dropdown list to ensure that the device clock is synchronized with the wall clock time.</p>
NTP Server 1	The IPv4 address or domain name of the primary Network Time Protocol (NTP) server.
NTP Server 2	The IPv4 address or domain name of the secondary or a backup NTP server.
Event Logging	
Syslog Server 1	The IPv4 address or the domain name of the syslog server 1.
Port	<p>The port number of the syslog server 1 to which the syslog messages are sent.</p> <p>Supported value: 1 to 65535.</p>

Parameter	Description
Syslog Server 2	The IPv4 address or the domain name of the syslog server 2.
Port	The port number of the syslog server 2 to which the syslog messages are sent. Supported value: 1 to 65535.
Syslog Severity	The logs with the selected severity level that must be forwarded to the server. The following options are supported: <ul style="list-style-type: none"> • Emergency (Level 0) • Alert (Level 1) • Critical (Level 2) • Error (Level 3) • Warning (Level 4) • Notice (Level 5) • Info (Level 6) • Debug (Level 7)

3. Click **Save**.

Network

Using the **Network** tab, you can configure LAN ports, VLANs, and static routes.

To configure parameters on the **Network** page, complete the following steps:

1. On the **NSE Groups > Add New** page, select the **Network** tab.


The **Network** page appears, as shown in [Figure 409](#).


Figure 409 The Network page

2. Configure the parameters, as described in [Table 86](#).


Table 86 Parameters on the Network page



Parameter	Description
On the Network page, there are DHCP Server , LAN Ports , VLANs , and Static Routes sections.	
DHCP Server	


Parameter	Description
DHCP Authoritative	Indicates that the DHCP server is the primary and trusted source for IP address assignments in the network. This parameter is enabled by default.
LAN Ports Click the edit  icon to modify the configuration of the corresponding LAN port as shown in Figure 410 , and click Update to apply the changes.	
Name	Name of the LAN port. This parameter cannot be modified.
Mode	The VLAN mode of the port. The following options are supported: <ul style="list-style-type: none"> • Access Single VLAN: An access port which places all traffic on its configured VLAN and only passes untagged traffic. • Trunk Multiple VLANs: A trunk port which allows the selected port to accept or pass 802.1Q tagged traffic.
Description	A brief description of the LAN port.
VLAN	This parameter is applicable only when the Mode parameter is set to Access Single VLAN . By default, VLAN value is 1. VLAN value can be in the range: 1 to 4094 This is a mandatory parameter.
Native VLAN	Indicates that the traffic on the native VLAN is untagged. This parameter is applicable only when the Mode parameter is set to Trunk Multiple VLANs . The Native VLAN value can be in the range: 1 to 4094 This is a mandatory parameter.
Tag the native VLAN	This parameter is applicable only when the Mode parameter is set to Trunk Multiple VLANs . When the Tag the native VLAN parameter is enabled, the native VLAN traffic is tagged with 802.1Q.
Allowed VLANs	This parameter is applicable only when the Mode parameter is set to Trunk Multiple VLANs . This parameter supports a range or comma-separated list of VLANs. Example: 1-3 or 4, 10, 22
Auto VLAN	This parameter is applicable only when the Mode parameter is set to Trunk Multiple VLANs . This parameter facilitates automatic assignment of VLANs in cnMatrix switches and access points (APs). When this parameter is enabled, the cnMatrix switches and APs use the Link Layer Discovery Protocol (LLDP) packets to obtain a list of VLANs for automatic assignment. Note: Auto VLAN works only with cnMatrix switches and access points (APs). It does not work with any third-party switches and APs. Auto VLAN allows cnMatrix switch to


Parameter	Description
	<p>dynamically learn VLANs from an AP. The AP advertises the configured VLANs to the cnMatrix switch. The cnMatrix switch then advertises those VLANs to the uplink NSE 3000 device. This process ensures that VLANs are properly bridged.</p> <p>This parameter is enabled by default.</p>
Auto VLAN Message Authentication	<p>This parameter is applicable only when the Mode parameter is set to Trunk Multiple VLANs.</p> <p>This parameter enables authentication for the LLDP messages where the VLANs are advertised.</p> <p>This parameter is enabled by default.</p>
Link Speed Advertisement	<p>Indicates the port speed that must be configured for advertisement.</p> <p>Default: Auto</p> <p>The following options are supported:</p> <ul style="list-style-type: none"> • Auto • 10 Mbps • 100 Mbps • 1000 Mbps
Port Duplex	<p>Specifies the mode of port communication. The following options are supported:</p> <ul style="list-style-type: none"> • Full Duplex • Half Duplex
Port Speed	<p>Specifies the port speed.</p> <p>Default: Auto</p> <p>The following options are supported:</p> <ul style="list-style-type: none"> • Auto • 10 Mbps • 100 Mbps • 1000 Mbps
Shutdown	<p>Enables or disables the port.</p> <p>By default, this parameter is disabled.</p>
<p>VLANs</p> <p>Note: You can configure up to 128 VLANs.</p> <p>To add a new VLAN, click Add New. The Add New VLAN window appears, as shown in Figure 411.</p> <p>To edit an existing VLAN configuration, click the edit  icon and modify the parameters in the Edit VLAN window. Finally, click Update to apply the changes.</p>	
VLAN ID	<p>Indicates the VLAN ID.</p> <p>The VLAN ID value can be in the range: 1 to 4094</p> <p>This is a mandatory parameter.</p>

Parameter	Description
Name	Name of the new VLAN. This is a mandatory parameter.
Description	Displays the user-configured description for the VLAN.
IP Address	IPv4 address that is assigned to the VLAN. This is a mandatory parameter.
Subnet Mask	Subnet mask that is assigned to the VLAN. This is a mandatory parameter.
Management Access	Indicates whether the management access is enabled or disabled. By default, this parameter is enabled.
Enable Rate Limit	Indicates whether the rate limit is enabled or disabled. By default, this parameter is disabled. When you select the Enable Rate Limit checkbox, the Rate Limit parameter appears.
Rate Limit	Specifies the rate of requests sent or received. This parameter appears only when you enable the Enable Rate Limit parameter. This parameter supports only integer values. This is a mandatory parameter.
Enable Port Scan	A scan identifies open ports within a network and helps in detecting potential vulnerabilities that can be exploited by attackers. By default, this parameter is enabled.
DHCP mode	Specifies the DHCP mode. The following options are supported: <ul style="list-style-type: none"> • None • DHCP Server - When you select this option, the DHCP server-related parameters appear. • DHCP Relay - When you select this option, the Relay Server IP address parameter appears.
DHCP Server In addition to the below parameters, you must also configure the parameters in the DHCP Options and MAC Binding List sections, as shown in Figure 412 .	
Start IP address	Starting IPv4 address in the range. This is a mandatory parameter.
End IP address	Ending IPv4 address in the range. This is a mandatory parameter.
Primary DNS	The primary DNS server for clients on the network. If the DNS server option is enabled on the NSE, the IPv4 address configured for the VLAN can be provided as the DNS server for the network.
Secondary DNS	The secondary DNS server for clients on the network.

Parameter	Description
Domain	The DNS search domain for the network.
Lease Time	The DHCP lease expiry time for the DHCP pool (in days, hours, and minutes). This is a mandatory parameter.
DHCP Options <p>NSE allows configuration of standard and custom DHCP options.</p> <p>To add a new DHCP option, click Add New. The Add New DHCP Option window appears, as shown in Figure 413.</p> <p>To edit an existing DHCP option, click the edit  icon and modify the parameters in the Edit DHCP Option window. Finally, click Update to apply the changes.</p>	
Option	<p>The following DHCP options are supported:</p> <ul style="list-style-type: none"> • Log server(7) • Domain name(15) • NTP server(42) • Vendor specific information(43) • Vendor class identifier(60) • TFTP server name(66) • Boot file name(67) • Proxy auto config(252) • Custom <p>This is a mandatory parameter.</p>
Code	<p>A value for the code.</p> <p>This parameter allows a maximum value of 254.</p> <p>This is a mandatory parameter.</p>
Type	<p>The following options are supported:</p> <ul style="list-style-type: none"> • Text • IP Address • Integer <p>This is a mandatory parameter.</p>
Value	<p>A value in ASCII.</p> <p>This is a mandatory parameter.</p>
MAC Binding List <p>For every DHCP pool configured, the user can bind the client MAC address with an IPv4 address from the network. This enables the client to obtain the same IPv4 address whenever they connect to the NSE 3000 device.</p> <p>Following parameters are required to create the binding list:</p> <ul style="list-style-type: none"> • MAC address of the client 	

Parameter	Description
	<ul style="list-style-type: none"> IPv4 address from the configured pool <p>When you set MAC and IP address fields and click Add, the binding of MAC and IP address is added.</p> <p>Note: Upto 200 MAC to IP address bindings are supported per DHCP pool.</p> <p>Note: When you bind, the binding IP address should be outside the DHCP pool range.</p> <p>To add a new MAC binding, click Add New. The Add New MAC Binding window appears, as shown in Figure 414.</p> <p>To edit an existing MAC binding, click the edit  icon and modify the parameters in the Edit MAC Binding window. Finally, click Update to apply the changes.</p>
MAC	<p>The MAC address of the client.</p> <p>This is a mandatory parameter.</p>
IP Address	<p>The IPv4 address that must be assigned to the client.</p> <p>This is a mandatory parameter.</p>
Description	Displays the user-configured description.
Import	<p>Imports the MAC bindings.</p> <p>Note: The CSV file that you import must be in the three-column format, for example, MAC, IP address, and Description.</p> <p>To import MAC bindings, click Import. The Import MAC Bindings window appears, as shown in Figure 415.</p>
Replace existing list	<p>Indicates whether the imported bindings will overwrite the existing list or append to the list.</p> <ul style="list-style-type: none"> If enabled, the imported bindings will overwrite the existing list If disabled, the imported bindings will append to the existing list. <p>By default, this parameter is enabled.</p>
Export	<p>Exports the configured bindings list.</p> <p>The following options are supported:</p> <ul style="list-style-type: none"> Export all as CSV Export page as CSV <p>To export MAC bindings, click Export. The export options appear, as shown in Figure 416.</p>
DHCP Relay	<p>Indicates whether the DHCP relay unicasts the DHCP request to an external DHCP server.</p> <p>This is a mandatory parameter.</p>
Relay Server IP address	<p>IPv4 address of the external DHCP server.</p> <p>This is a mandatory parameter.</p>
Static Routes <p>To add a new route, click Add New. The Add New Route window appears, as shown in Figure 417.</p> <p>To edit an existing route, click the edit  icon and modify the parameters in the Edit Route window. Finally,</p>	

Parameter	Description
click Update to apply the changes.	
Destination Network	The IPv4 address of the destination network. This is a mandatory parameter.
Prefix Length	The prefix length for the network address. This parameter supports integer values and a maximum value of 32. This is a mandatory parameter.
Next Hop	The next hop IPv4 address for the route. This is a mandatory parameter.
Exit Interface	The exit interface through which the next hop is reachable. This is a mandatory parameter.
Metric	The metric for the route.
To add multiple VLANs, click the Add Multiple button. The Add Multiple VLANs window appears, as shown in Figure 418 .	
To edit an existing VLAN configuration, click the edit  icon and modify the parameters in the Edit VLAN window. Finally, click Update to apply the changes.	
Description	Displays the user-configured description for the VLAN.
First VLAN ID	Indicates the first VLAN ID. The supported VLAN ID value range is between 1 and 4094. This is a mandatory parameter.
Number of VLANs	Indicates the number of VLANs that you want to add. Note: You can configure up to 128 VLANs. This is a mandatory parameter.
Subnet The following options are supported: <ul style="list-style-type: none"> • IP Address and Netmask - When you select this option, the IP address and Netmask options appear. • Hosts per subnet - When you select this option, the First IP Address and Hosts per subnet options appear. 	
IP address	The IPv4 address of the first VLAN. This is a mandatory parameter.
Netmask	The netmask of the subnet. This is a mandatory parameter.
First IP Address	The first IPv4 address of the subnet. This is a mandatory parameter.
Hosts per subnet	The number of hosts that you want for the subnet. This is a mandatory parameter.
DHCP mode	Specifies the DHCP mode. The following options are supported:

Parameter	Description
	<ul style="list-style-type: none"> • None • DHCP Server - When you select this option, the DHCP server-related parameters appear. • DHCP Relay - When you select this option, the Relay Server IP address parameter appears.
Lease Time	<p>The DHCP lease expiry time for the DHCP pool (in days, hours, and minutes).</p> <p>This is a mandatory parameter.</p>
<p>DHCP Options</p> <p>NSE allows configuration of standard and custom DHCP options.</p> <p>To add a new DHCP option, click Add New. The Add New DHCP Option window appears, as shown in Figure 413.</p> <p>To edit an existing DHCP option, click the edit  icon and modify the parameters in the Edit DHCP Option window. Finally, click Update to apply the changes.</p>	
Option	<p>The following DHCP options are supported:</p> <ul style="list-style-type: none"> • Log server(7) • Domain name(15) • NTP server(42) • Vendor specific information(43) • Vendor class identifier(60) • TFTP server name(66) • Boot file name(67) • Proxy auto config(252) • Custom <p>This is a mandatory parameter.</p>
Code	<p>A value for the code.</p> <p>This parameter allows a maximum value of 254.</p> <p>This is a mandatory parameter.</p>
Type	<p>The following options are supported:</p> <ul style="list-style-type: none"> • Text • IP Address • Integer <p>This is a mandatory parameter.</p>
Value	<p>A value in ASCII.</p> <p>This is a mandatory parameter.</p>
DHCP Relay	<p>Indicates whether the DHCP relay unicasts the DHCP request to an external DHCP server.</p>

Parameter	Description
	This is a mandatory parameter.
Relay Server IP address	IPv4 address of the external DHCP server. This is a mandatory parameter.

Figure 410 *The Edit Port window*

×

Mode

Trunk Multiple VLANs

Description

Native VLAN*

1

☐ Tag the native VLAN

Allowed VLANs

e.g. 1-3 or 4,10,22

☒ Auto VLAN
☒ Auto VLAN Message Authentication

Link Speed Advertisement

Auto

Duplex

Full Duplex

Port Speed

Auto

☐ Shutdown

Cancel

Update

Figure 411 *The Add New VLAN window*

Add New VLAN

X

VLAN ID*

Minimum 1, Maximum 4094

Name*

Description

IP Address*

Subnet Mask*

☒ Management Access

☐ Enable Rate Limit Per client rate limit

☒ Enable Port Scan
Enable probe of devices to identify open ports on this network.

DHCP Mode

☒ None ☐ DHCP Server ☐ DHCP Relay

Cancel

Add

Figure 412 *DHCP Options and MAC Binding List*

Add New VLAN

VLAN ID*

Minimum 1, Maximum 4094

Name*

Description

IP Address* Subnet Mask*

☒ Management Access

☐ Enable Rate Limit Per client rate limit

☒ Enable Port Scan
Disable probe of devices to identify open ports on this network.

DHCP Mode

☐ None ☒ DHCP Server ☐ DHCP Relay

Start IP Address* End IP Address*

Primary DNS Secondary DNS

Make sure the client sends DNS request to LAN interface IP if you are using DNS filter

Domain

Lease Time

Days* Hours* Minutes*

0 2 0

DHCP Options

Apply Filter() Add New

Option	Code	Type	Value
No Data Available			

Showing 0 - 0 Total 0 10 Previous Next

MAC Binding List

Apply Filter() Add New Import Export

MAC	IP Address	Description
No Data Available		

Showing 0 - 0 Total 0 10 Previous Next

Cancel Add

Figure 413 *The Add New DHCP Option window*

Add New DHCP Option

Option*

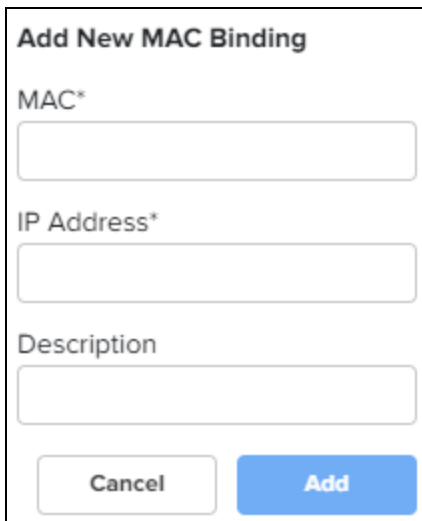
Code*

Type*

Value*

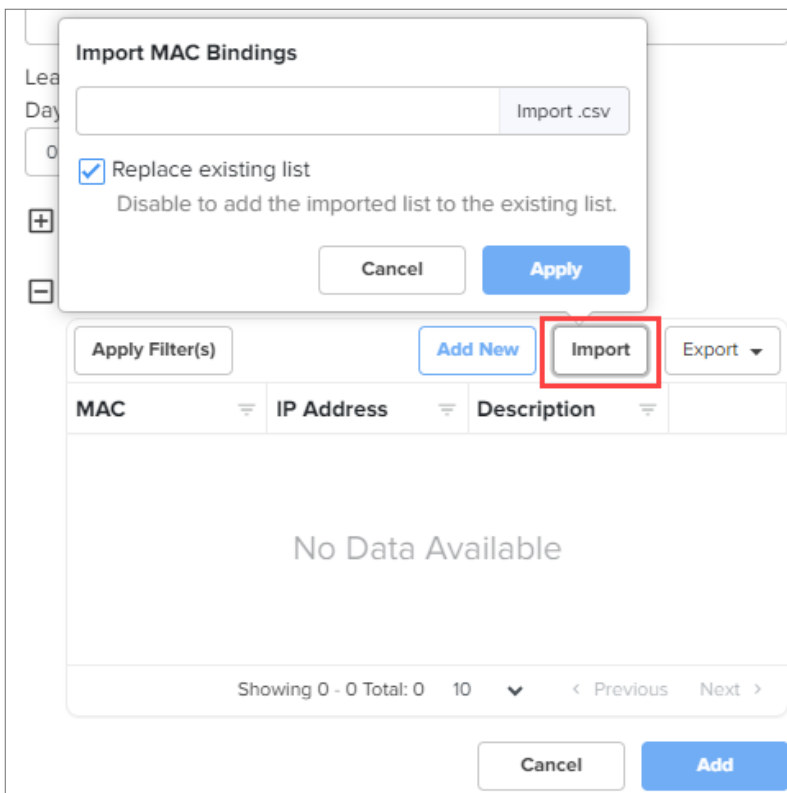
Cancel Add

Figure 414 The Add New MAC Binding window



The 'Add New MAC Binding' window is a modal dialog box. It contains three text input fields: 'MAC*', 'IP Address*', and 'Description'. At the bottom, there are two buttons: 'Cancel' and 'Add'.

Figure 415 The Import option in MAC Binding List



The image shows the 'Import MAC Bindings' dialog box overlaid on the 'MAC Binding List' table. The dialog box has a title bar, a file input field with an 'Import .csv' button, a checked checkbox for 'Replace existing list' with a sub-note 'Disable to add the imported list to the existing list.', and 'Cancel' and 'Apply' buttons. The background table has columns 'MAC', 'IP Address', and 'Description'. It shows 'No Data Available' and a status bar at the bottom indicating 'Showing 0 - 0 Total: 0'. The 'Import' button in the table's toolbar is highlighted with a red rectangle.

Figure 416 The Export option in MAC Binding List

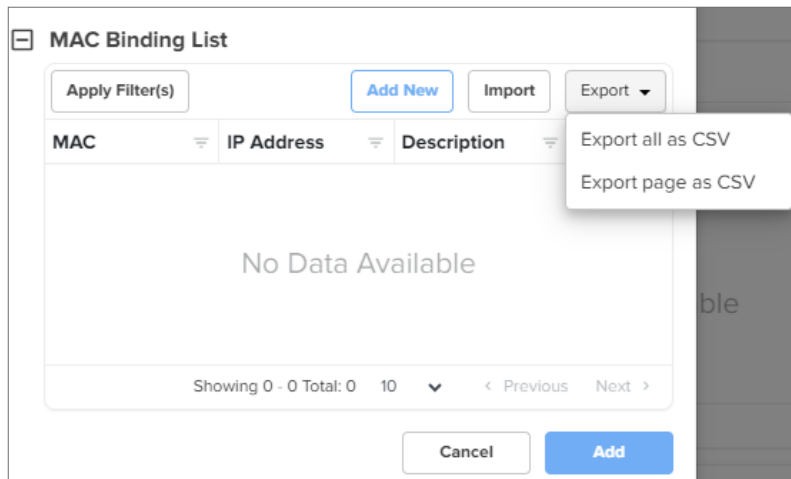


Figure 417 The Add New Route window

Add New Route [X]

Destination Network*

Prefix Length*

Next Hop*

Exit Interface*

Metric

[Cancel] [Add]

Figure 418 The Add Multiple VLANs window

Add Multiple VLANs [X]

Description

First VLAN ID* Number of VLANs*

Subnet

☒ IP Address and Netmask ☐ Hosts per subnet

IP Address* Netmask*

DHCP Mode

☐ None ☒ DHCP Server ☐ DHCP Relay

Lease Time

Days* Hours* Minutes*

0 2 0

☒ DHCP Options

[Cancel] [Add]

3. Click **Save**.

Groups

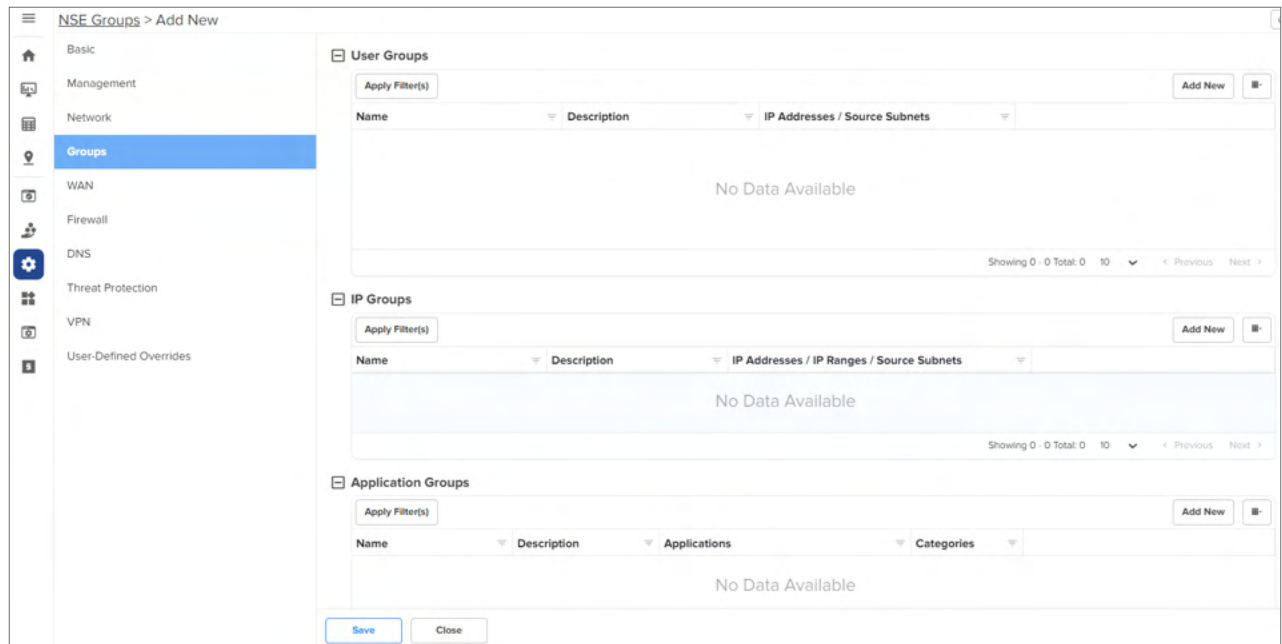
Using the **Groups** tab, you can configure user groups, IP groups, and application groups.

To view the **Groups** page, complete the following steps:

1. On the **NSE Groups > Add New** page, select the **Groups** tab.


The **Groups** page appears, as shown in [Figure 419](#).

Figure 419 The Groups page



2. Configure the parameters, as described in [Table 87](#).

Table 87 Parameters on the Groups page

Parameter	Description
On the Groups page, there are User Groups , IP Groups , and Application Groups sections.	
User Groups User groups are used to group locally configured networks and these groups can be used to associate with policies, especially application rules or DNS rules. To add a new user group, click Add New . The Add User Group window appears, as shown in Figure 420 . To edit a user group, click the edit  icon and modify the parameters in the Edit User Group window. Finally, click Update to apply the changes.	
Name	Name for the user group. This is a mandatory parameter.
Description	Description for the user group.
IP Addresses/Source	IPv4 addresses or source subnets for the user group. This is a mandatory parameter.



Parameter	Description
Subnets	
IP Groups <p>IP groups are used to group networks originating from the WAN, and can be used to attach port forwarding rules.</p> <p>To add a new IP group, click Add New. The Add IP Group window appears, as shown in Figure 421.</p> <p>To edit an IP group, click the edit  icon and modify the parameters in the Edit IP Group window. Finally, click Update to apply the changes.</p>	
Name	Name for the IP group.
Description	Description for the IP group.
IP Addresses/IP Ranges/Source Subnets	IPv4 addresses, IP ranges, or source subnets for the IP group. This is a mandatory parameter.
Application Groups <p>Application groups are used to group applications by using application names or categories, which can then be attached to a policy for permitting or denying access.</p> <p>To add a new application group, click Add New. The Add New Application Group window appears, as shown in Figure 422.</p> <p>To edit an application group, click the edit  icon and modify the parameters in the Edit Application Group window. Finally, click Update to apply the changes.</p>	
Name	Name for the application group.
Description	Description for the application group.
Applications <p>To add applications to the application group, select the required application(s) from the dropdown list and click Add New. The selected applications are added in the Name list.</p>	
Application Name	Applications for the new application group.
Categories <p>To include categories for the new application group, select the required categories.</p>	
Categories	Categories for the new application group.

Figure 420 The Add User Group window

Add User Group

Name*

Description

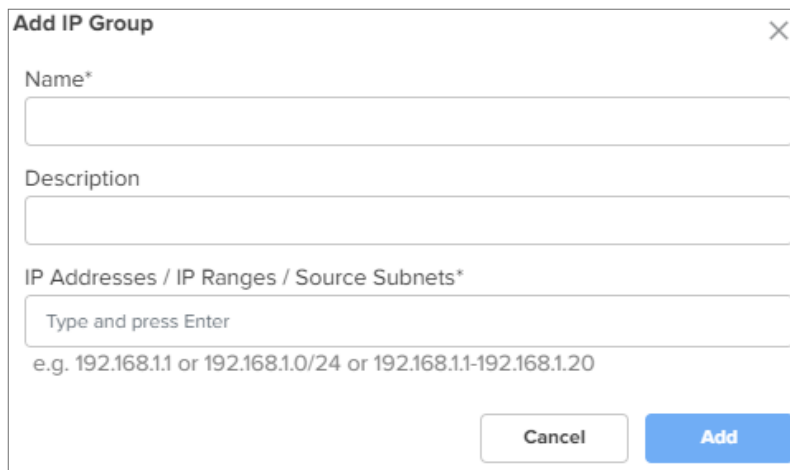
IP Addresses / Source Subnets*

Type and press Enter

Cancel

Add

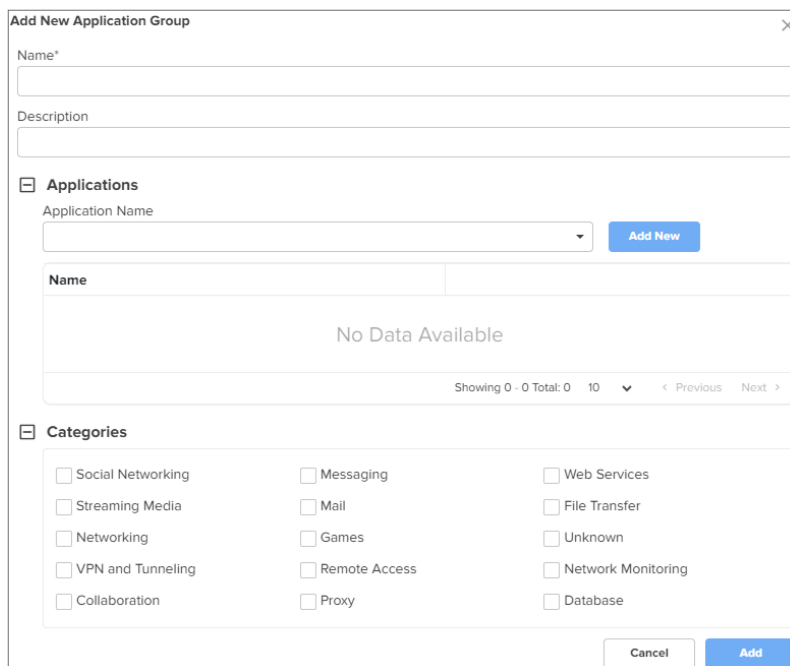
Figure 421 The Add IP Group window



The 'Add IP Group' window contains the following fields and controls:

- Name***: A text input field.
- Description**: A text input field.
- IP Addresses / IP Ranges / Source Subnets***: A text input field with placeholder text 'Type and press Enter' and an example 'e.g. 192.168.1.1 or 192.168.1.0/24 or 192.168.1.1-192.168.1.20'.
- Buttons**: 'Cancel' and 'Add' buttons at the bottom right.

Figure 422 The Add New Application Group window



The 'Add New Application Group' window contains the following fields and controls:

- Name***: A text input field.
- Description**: A text input field.
- Applications**: A section with an 'Applications' header, an 'Application Name' dropdown menu, an 'Add New' button, and a table with the following structure:

Name
No Data Available

Below the table is a pagination bar: 'Showing 0 - 0 Total: 0 10 < Previous Next >'.
- Categories**: A section with a 'Categories' header and a grid of checkboxes for various categories:

<input type="checkbox"/> Social Networking	<input type="checkbox"/> Messaging	<input type="checkbox"/> Web Services
<input type="checkbox"/> Streaming Media	<input type="checkbox"/> Mail	<input type="checkbox"/> File Transfer
<input type="checkbox"/> Networking	<input type="checkbox"/> Games	<input type="checkbox"/> Unknown
<input type="checkbox"/> VPN and Tunneling	<input type="checkbox"/> Remote Access	<input type="checkbox"/> Network Monitoring
<input type="checkbox"/> Collaboration	<input type="checkbox"/> Proxy	<input type="checkbox"/> Database
- Buttons**: 'Cancel' and 'Add' buttons at the bottom right.

3. Click **Save**.

WAN

Using the **WAN** tab, you can configure the settings related to the WAN interface.

To configure parameters on the WAN page, complete the following steps:

1. On the **NSE Groups > Add New** page, select the **WAN** tab.
The **WAN** page appears.

Figure 423 The WAN page

Figure 423 shows the WAN page configuration interface. The left sidebar contains navigation options: Basic, Management, Network, Groups, WAN (selected), Firewall, DNS, Threat Protection, VPN, and User Defined Overrides. The main content area is titled 'WAN Configurations' and includes tabs for WAN-1 and WAN-2. The configuration options are as follows:

- IP Address Assignment:** Dynamic (selected).
 - ☐ Enable 802.1q VLAN tagging of frames
 - Additional IP Addresses: [Empty field] (Additional WAN IP addresses used for Source NAT e.g. 50110 or 50110/29 or 50110-50117)
 - ☒ Enable Source NAT
- Source NAT Rules:** [Empty field] (Add New button)
- Precedence:** LAN Pool, WAN Pool (No Data Available)
- Connection Health:** [Empty field] (Add New button)
 - Monitor Hosts:** 8.8.8.8 (Showing 1 - 1 Total 1 10 Previous Next)
 - Number of Host Failures:** 1 (Configure the number of monitor hosts to fail to declare interface down (Default - 1))
 - Failure Detect Time:** 5 (Configure interval for declaring link DOWN (5 - 60) seconds)
 - Interval:** 2 (Configure interval at which hosts should be pinged (2 - 10) seconds)
 - Timeout:** 2 (Configure timeout for ping (1 - 10) seconds)
- Dynamic DNS:** [Empty field]
- Link Capacity:**
 - Uplink*: 1000 Mbps
 - Downlink*: 1000 Mbps
- Traffic Shaping:** [Empty field]
- Failover Policy:** [Empty field]
- WAN Speed Test:** [Empty field]
- Load Balancing:** [Empty field]
- Flow Preferences:** [Empty field]

Buttons: Save, Close


2. Configure the parameters, as described in [Table 88](#).

Table 88 Parameters on the WAN page

Parameter	Description
On the WAN page, there are WAN Configurations , LoadBalancing , and Flow Preferences sections.	
WAN Configurations	
In this section, you can configure the parameters in Connection Health , Dynamic DNS , Link Capacity , Traffic Shaping , Failover Policy , and WAN Speed Test subsections.	
The same parameters appear in both WAN-1 and WAN-2 tabs.	
IP Address Assignment	<p>Determines the mode of IP address assignment for the WAN interface.</p> <p>The following options are supported:</p> <ul style="list-style-type: none">• Dynamic: Dynamically learn the IP address and DNS from the DHCP server.• Static: Manually configure the IP address, gateway, and DNS server IP provided by the service provider.• PPPoE: When you configure PPPoE, you must provide the username and password of the service provider. While the account name and service name are not mandatory configurations, they may be required if the service provider enforces it. By default,

Parameter	Description
	the MTU is set to 1492 and the TCP MSS clamping is enabled. If required, you can also tag the packet on the WAN link to send.
Enable 802.1q VLAN tagging of frames	When this parameter is enabled, 802.1Q tag is inserted with configured VLAN ID for all the packets going out of the WAN interface. By default, this parameter is disabled.
VLAN ID	This parameter is applicable only when Enable 802.1q VLAN tagging of frames checkbox is selected. VLAN ID range: 1 and 4094. This is a mandatory parameter. When the 802.1Q header is configured, all transmitted frames are expected to include the 802.1Q header with the same VLAN ID.
Following parameters appear when you select Static from the IP Address Assignment dropdown list.	
IP Address	The IPv4 address of the WAN interface. This is a mandatory parameter.
IP Address (HA Spare)	This parameter appears only when Enable HA checkbox is selected from the Basic screen. The IPv4 address of the HA spare. This is a mandatory parameter.
Subnet Mask	The subnet mask for the IPv4 address of the WAN interface. This is a mandatory parameter.
Default Gateway	The IPv4 address of the default gateway for the WAN interface.
Primary DNS	The IPv4 address of primary upstream DNS server on this interface. This is a mandatory parameter.
Secondary DNS	The IPv4 address of secondary upstream DNS server on this interface.
Following parameters appear when you select PPPoE from the IP Address Assignment dropdown list.	
Account Controller Name	Name of the account controller. This parameter allows a maximum of 32 characters. This parameter is optional.
Service Name	Indicates the service name of the Account Controller. This parameter allows a maximum of 32 characters. The service name configuration is optional.
User	User name for PPPoE authentication. This is a mandatory parameter.
Password	Password for PPPoE authentication. This parameter is optional.
MTU	MTU for PPPoE interface. MTU ranges from 500 to 1492 bytes.

Parameter	Description
	Default: 1492 bytes.
TCP MSS Clamping	Indicates whether TCP MSS Clamping is enabled or disabled. By default, this parameter is enabled.
Additional IP Addresses	WAN IP addresses that are available for source NAT. Note: The WAN interface supports up to 16 IP addresses.
Enable Source NAT	Indicates whether the source NAT is enabled or disabled. When enabled, NSE 3000 device will replace the source IP address of the traffic routed from LAN to WAN with the WAN interface IP address. By default, this parameter is enabled.
Source NAT Rules Allows user to configure source NAT rules. User can choose the WAN IP addresses from the Additional IP Address for source NAT. User can configure WAN IP address(es) of their choice for source NAT. By default, all the LAN users' traffic will be source NATed to the configured WAN IP address(es). When LAN pool is configured, the traffic from the specified LAN networks will be source NATed to the configured WAN IP address(es). Note: Source NAT Rules supports up to 16 rules per WAN. To add a new source NAT, click Add New . The Add New Source NAT Rule window appears, as shown in Figure 424 .	
Precedence	The precedence value for the source NAT rule. The precedence value can be between 1 and 150. This is a mandatory parameter.
LAN Pool	The following options are supported: <ul style="list-style-type: none"> • All • IP Group • IP Address / Source Subnet
WAN Pool	The following options are supported: <ul style="list-style-type: none"> • Single IP Address • Multiple IP Addresses
IP Address	IPv4 address for the WAN pool. Applicable only when Single IP Address option is selected.
Start IP	Starting IP address in the range. This parameter is applicable only when Multiple IP Addresses option is selected. This is a mandatory parameter.
End IP	Ending IP address in the range. This parameter is applicable only when Multiple IP Addresses option is selected. This is a mandatory parameter.
IP Group	Select the IP group for the source NAT. IP groups are the ones that you configure in the Groups > IP Groups section.

Parameter	Description
	<p>This parameter is applicable only when IP Group option is selected.</p> <p>This is a mandatory parameter.</p>
IP Address / Source Subnet	<p>This parameter is applicable only when IP Address / Source Subnet option is selected.</p> <p>This is a mandatory parameter.</p>
Connection Health <p>This section is configured to monitor the WAN connection health.</p> <p>Click the edit  icon to modify the Monitor Host configuration, as shown in Figure 425. Finally, click Update to apply the changes.</p> <p>To add a new monitor host, click Add New. The Add New Monitor Host window appears, as shown in Figure 426.</p>	
Monitor Host	<p>The hosts used to monitor and collect network traffic data.</p> <p>Default: 8.8.8.8</p> <p>This is a mandatory parameter.</p>
Number of Host Failures	<p>The number of monitor hosts that fail to declare the link down.</p> <p>Default value: 1</p> <p>The maximum number of monitor hosts that can be configured to fail is 5.</p>
Failure Detect Time	<p>The time period (in seconds) during which the device waits for the response from the monitored host before declaring the link down.</p> <p>Default: 5. Range: 5 to 60</p>
Interval	<p>The time interval (in seconds) used by the device to check and reach the monitor hosts.</p> <p>Default: 2. Range: 2 to 10</p>
Timeout	<p>The time period (in seconds) the device waits for a response from the monitor host after which the connection is timed out.</p> <p>Default: 2. Range: 1 to 10</p>
Dynamic DNS	
Enable Dynamic DNS	<p>Indicates whether the dynamic DNS for the interface is enabled or disabled.</p> <p>By default, this parameter is disabled.</p>
Following parameters appear when Enable Dynamic DNS checkbox is selected.	
DNS Provider	<p>The following options are supported:</p> <ul style="list-style-type: none"> Cloudflare: Requires secret/access token and zone configuration. In the Cloudflare account, navigate to Profile > API Tokens to create a token. Following is the recommended setting: <ul style="list-style-type: none"> Permissions: Zone, DNS, Edit ZoneResource: Include, Specific Zone, <zone name> Godaddy: Requires API key, secret/access token, and zone configuration. In the Godaddy account, create an API key at https://developer.godaddy.com/keys

Parameter	Description
	<ul style="list-style-type: none"> • Hetzner: Requires secret/access token and zone configuration. In the Hetzner account, navigate to Profile > API Tokens and create an access token. • Namecheap: Requires password and zone configuration. <ol style="list-style-type: none"> 1. In the Namecheap account, navigate to Domains > Free DNS to manage external domains. 2. Before you update/create a record, a new record of type A must exist. To create a record, navigate to the dashboard, and then navigate to Products > Advanced DNS. Add a new record of type A. On the same page, enable Dynamic DNS and note the password. • Noip: Requires server name, username, and password configuration. • Route53: Requires API key, secret/access token, and zone configuration. <ol style="list-style-type: none"> 1. In the Route 53 account, navigate to route53 > Hosted Zones > Create Hosted Zone to create a zone. Use type Public hosted zone. Note the name servers in hosted zone details and the hosted zone ID. 2. Navigate to IAM > Users > Create user. Select attach policies directly. Create a policy. <p>The following is an example of a policy:</p> <pre>{ "Version": "2012-10-17", "Statement": [{ "Sid": "", "Effect": "Allow", "Action": ["route53:ListResourceRecordSets", "route53:GetChange", "route53:ChangeResourceRecordSets"], "Resource": ["arn:aws:route53:::hostedzone/<ZONE_ID>", "arn:aws:route53:::change/*"] }], { "Sid": "", "Effect": "Allow",</pre>

Parameter	Description
	<pre>"Action": ["route53:ListHostedZonesByName", "route53:ListHostedZones"], "Resource": "" }]</pre> <p>3. Replace ZONE_ID in the policy with the previously noted zone id. Select the new policy for the previously created user.</p> <p>4. To create access key, navigate to users, select the user, Security Credentials > Create Access Key.</p> <ul style="list-style-type: none"> • Porkbun: Requires API key, secret/access token, and zone configuration. In the Porkbun account, navigate to Account > API Access to create a token. Additionally, the domain configuration must be changed to enable API access. • Dyn: Oracle Dyn requires server name, username, and password configuration. • DynDNS2 compliant: Requires server name, username, and password configuration. <p>By default, Noip option is selected.</p>
DNS Hostname	Indicates the DNS host name.
Link Capacity	
Uplink	<p>The WAN uplink capacity in Mbps.</p> <p>Default:1000. Range: 1 to 1000</p> <p>This is a mandatory parameter.</p>
Downlink	<p>The WAN downlink capacity in Mbps.</p> <p>Default:1000. Range: 1 to 1000</p> <p>This is a mandatory parameter.</p>
Traffic Shaping Note: Traffic Shaping supports up to 16 rules per WAN. To add a new traffic shaping rule, click Add New , the Add New Traffic Shaping Rule window appears, as shown in Figure 427 .	
Enable Traffic Shaping	<p>Indicates whether traffic shaping is enabled or disabled.</p> <p>By default, this parameter is disabled.</p>
Precedence	<p>The precedence value for the traffic shaping rule.</p> <p>The precedence value can be between 1 and 150.</p> <p>This is a mandatory parameter.</p>
Description	Displays a user-configured description for the traffic shaping rule.

Parameter	Description
Uplink Bandwidth	Indicates the uplink bandwidth in Mbps. Range: 1 to 1000 This is a mandatory parameter.
Downlink Bandwidth	Indicates the downlink bandwidth in Mbps Range: 1 to 1000 This is a mandatory parameter.
DSCP	Differentiated Services Code Point (DSCP) can range from 0 to 63, with 0 being the lowest priority and 63 being the highest priority.
Type	Indicates the type of filter rule. The following options are supported: <ul style="list-style-type: none"> • IP Based – Allows you to configure Protocol parameter as TCP, UDP, or any. • Application Based – Allows you to configure Deep Packet Inspection (DPI) Type parameter as Application or Category.
Deep Packet Inspection (DPI) Type	This parameter is applicable only when Type parameter is Application Based . The following options are supported: <ul style="list-style-type: none"> • Application – Specific type of application within a category. • Category – All applications belonging to a category (For example, Social Messaging). This is a mandatory parameter.
DPI Application	This parameter is applicable only when Deep Packet Inspection (DPI) Type parameter is set to Application . This is a mandatory parameter.
DPI Category	This parameter is applicable only when Deep Packet Inspection (DPI) Type parameter is set to Category . This is a mandatory parameter.
Protocol	This parameter is applicable only when Type parameter is IP Based . The following options are supported: <ul style="list-style-type: none"> • TCP – Match TCP traffic. • UDP – Match UDP traffic. • any – Match any of the above protocol traffic.
Source IP Address	The source IPv4 address for the shaping rule. This is a mandatory parameter.
Mask	The subnet mask for the shaping rule. This is a mandatory parameter.
Port	Displays the source port from which IPv4 address messaging is sent. This is a mandatory parameter.
Destination IP Address	The destination IPv4 address for the shaping rule. This is a mandatory parameter.

Parameter	Description
Mask	The subnet mask for the shaping rule. This is a mandatory parameter.
Port	Displays the destination port to which IPv4 address messaging is sent. This is a mandatory parameter.
Failover Policy Note: Failover Policy supports up to 32 rules per WAN. To add a new failover policy, click Add New . The Add New Failover Policy window appears, as shown in Figure 428 .	
Enable Failover Policy	Indicates whether failover policy is enabled or disabled. By default, this parameter is disabled.
Precedence	The precedence value for the failover policy. The precedence value can be between 1 and 150. This is a mandatory parameter.
Description	A description for the policy.
Action	By default, this parameter is disabled.
Type	The type of failover rule. The following options are supported: <ul style="list-style-type: none"> • IP Based – Allows you to configure the Protocol parameter as TCP, UDP, or any. • Application Based – Allows you to configure Deep Packet Inspection (DPI) Type parameter as Application, Category, or Application Group.
Protocol	This parameter is applicable only when Type parameter is IP Based . The following options are supported: <ul style="list-style-type: none"> • TCP – Match TCP traffic. • UDP – Match UDP traffic. • any – Match any of the above protocol traffic.
Source IP Address	The source IPv4 address for the failover rule. This is a mandatory parameter.
Mask	The subnet mask for the failover rule. This is a mandatory parameter.
Port	The source port for the failover rule. This is a mandatory parameter.
Destination IP Address	The destination IPv4 address for the failover rule. This is a mandatory parameter.
Mask	The subnet mask for the failover rule. This is a mandatory parameter.
Port	Displays the destination port for the failover rule.

Parameter	Description
	This is a mandatory parameter.
Deep Packet Inspection (DPI) Type	<p>This parameter is applicable only when Type parameter is Application Based.</p> <p>The following options are supported:</p> <ul style="list-style-type: none"> • Application – Specific type of application within a category. • Category – All applications belonging to a category (For example, Social Messaging). • Application Group - All applications belonging to a group. <p>This is a mandatory parameter.</p>
Apply to	<p>This parameter is applicable only when Type parameter is Application Based.</p> <p>The following options are supported:</p> <ul style="list-style-type: none"> • All • User Group • IP Address / Source Subnet
User Group	<p>This parameter is applicable when User Group option is selected.</p> <p>This is a mandatory parameter.</p>
IP Address / Source Subnet	<p>This parameter is applicable when IP Address / Source Subnet option is selected.</p> <p>This is a mandatory parameter.</p>
WAN Speed Test	
Enable WAN Speed Test	<p>Enable or disable the WAN speed test.</p> <p>By default, this parameter is disabled.</p>

Figure 424 The Add New Source NAT Rule window

Figure 425 The Edit Monitor Host window

Figure 426 The Add New Monitor Host window

Figure 427 The Add New Traffic Shaping Rule window

Add New Traffic Shaping Rule

×

Precedence*

Description

Uplink Bandwidth*

Mbps

Downlink Bandwidth*

Mbps

DSCP

Type

IP Based

Protocol

any

Source IP Address*

Mask*

Port*

any

Specify IP address or 'any'

Specify subnet mask or 'any'

Specify port or 'any'

Destination IP Address*

Mask*

Port*

any

Specify IP address or 'any'

Specify subnet mask or 'any'

Specify port or 'any'

Cancel

Add

Figure 428 The Add New Failover Policy window

Add New Failover Policy

×

Precedence*

Description

Action

Deny

Type

IP Based

Protocol

any

Source IP Address*

Mask*

Port*

any

Specify IP address or 'any'

Specify subnet mask or 'any'

Specify port or 'any'

Destination IP Address*

Mask*

Port*

any

Specify IP address or 'any'

Specify subnet mask or 'any'

Specify port or 'any'

Cancel

Add

- Expand the **Load Balancing** section and configure the parameters, as described in [Table 89](#).

Table 89 *Parameters on the Load Balancing section*

Parameter	Description
Load Balancing	
WAN-1 Mode	<p>Determines the load balancing mode of device.</p> <p>By default, the WAN-1 Mode parameter is set to Shared.</p> <p>The following options are supported:</p> <ul style="list-style-type: none"> • Shared – Enables the WAN link to actively forward a percentage of user traffic. The percentage of user traffic on this link is set via the Traffic Share Percentage parameter. • Backup – The WAN link forwards user traffic only when all of the Shared WAN interfaces are down. • Disabled – Disables the WAN link from participating in WAN link load sharing, and failover procedures.
Traffic Share Percentage	<p>For the Shared mode, the traffic share percentage must be between 5 and 100.</p> <p>This is a mandatory parameter.</p>
WAN-2 Mode	<p>Determines the load balancing adjust mode of device.</p> <p>By default, the WAN-2 Mode parameter is set to Backup.</p> <p>The following options are supported:</p> <ul style="list-style-type: none"> • Shared – Enables the WAN link to actively forward a percentage of user traffic. The percentage of user traffic on this link is set via the Traffic Share Percentage parameter. • Backup – The WAN link forwards user traffic only when all of the Shared WAN interfaces are down. • Disabled – Disables the WAN link from participating in WAN link load sharing, and failover procedures.
Traffic Share Percentage	<p>For the Shared mode, the traffic share percentage between 5 and 100.</p> <p>This is a mandatory parameter.</p>

- Expand the **Flow Preferences** section and configure the parameters, as described in [Table 90](#).

Table 90 *Parameters on the Flow Preferences section*

Parameter	Description
Flow Preferences	
<p>Flow preferences support up to 30 rules for both WANs combined.</p> <p>To add a new flow preference, click Add New. The Add New Flow Preference window appears, as shown in Figure 429.</p>	
WAN Interface	<p>The following options are supported:</p> <ul style="list-style-type: none"> • WAN-1 • WAN-2
Description	Provide a description for the flow preference.

Parameter	Description
Policy	<p>The flow preference policy.</p> <p>The following options are supported:</p> <ul style="list-style-type: none"> • Flexible – Allow traffic to failover if the preferred WAN link goes down. • Strict – Traffic is dropped in strict mode, if the preferred WAN link goes down.
Type	<p>The flow preference type.</p> <p>The following options are supported:</p> <ul style="list-style-type: none"> • IP Based – Allows you to configure Protocol parameter as TCP, UDP, or any. • Application Based – Allows you to configure Deep Packet Inspection (DPI) Type parameter as Application or Category.
Protocol	<p>This parameter is applicable only when Type parameter is IP Based.</p> <p>The following options are supported:</p> <ul style="list-style-type: none"> • TCP – Match TCP preference. • UDP – Match UDP preference. • Any – Match any of the above preferences.
Source IP Address	<p>The source IPv4 address for the flow preference.</p> <p>This is a mandatory parameter.</p>
Mask	<p>The subnet mask for the flow preference.</p> <p>This is a mandatory parameter.</p>
Port	<p>The source port for the flow preference.</p> <p>This is a mandatory parameter.</p>
Destination IP Address	<p>The destination IPv4 address for the flow preference.</p> <p>This is a mandatory parameter.</p>
Mask	<p>The subnet mask for the flow preference.</p> <p>This is a mandatory parameter.</p>
Port	<p>The destination port for the flow preference.</p> <p>This is a mandatory parameter.</p>
Deep Packet Inspection (DPI) Type	<p>This parameter is applicable only when Type parameter is Application Based.</p> <p>The following options are supported:</p> <ul style="list-style-type: none"> • Application – Specific type of application within a category. • Category – All applications belonging to a category (For example, Social Messaging). <p>This is a mandatory parameter.</p>
DPI Application	<p>This parameter is applicable only when Deep Packet Inspection (DPI) Type parameter is set to Application.</p> <p>This is a mandatory parameter.</p>
DPI Category	<p>This parameter is applicable only when Deep Packet Inspection (DPI) Type parameter is set to Category.</p>

Parameter	Description
	This is a mandatory parameter.

Figure 429 The Add New Flow Preference window

5. Click **Save**.

Firewall

NSE 3000 firewall allows the user to configure the IP-based and application-based outbound rules, GEO IP filters, port forward rules, one-to-one NAT mappings, and one-to-many NAT mappings. All inbound connections are denied by default. You can configure port forwarding or NAT rules to allow inbound traffic. Outbound traffic is allowed by default. Using application-based outbound rules, users can create rules to block websites without specifying IP addresses or port ranges. Application-based rules allow the user to block a specific type of application within a category or all applications belonging to a category (For example, social messaging).



Note

Up to 150 outbound firewall rules are supported for an NSE Group including combinations of IP-based and application-based rules.

To configure parameters on the **Firewall** page, complete the following steps:

1. On the **NSE Groups > Add New** page, select the **Firewall** tab.

The **Firewall** page appears, as shown in [Figure 430](#).

Figure 430 *The Firewall page*

Cambium cnMaestro Cloud | User Guide

2. Configure the parameters, as described in [Table 91](#).

Table 91 *Parameters on the Firewall page*

Parameter	Description
On the Firewall page, there are Inbound Filter Rules , Outbound Filter Rules , Denial of Service (DoS) Protection , GEO IP WAN to LAN Filters , GEO IP LAN to WAN Filters , Port Forward Rules , NAT One-to-One , NAT One-to-Many , and Device Access sections.	
Inbound Filter Rules By default, NSE firewall routers are configured to function as stateful firewalls by dropping packets that are not related to an established connection.	
Allow traffic from WAN to LAN	An option to enable or disable the stateful firewall behavior. By default, this parameter is disabled. In special deployment cases, when NSE is positioned behind an MPLS uplink router, you can enable this behavior. To enable this behavior, select the Allow traffic from WAN to LAN checkbox. Additionally, you must disable source NAT on the WAN UI page to allow routing of traffic without NAT, originated on the LAN directed towards the WAN.
Outbound Filter Rules To add a new outbound filter rule, click Add New . The Add New Filter Rule window appears, as shown in Figure 431 .	
Precedence	The precedence value for the filter rule. The precedence value can be between 1 and 150. This is a mandatory parameter.
Description	Displays a user-configured description for the filter rule.
Action	Determines the action of filter. The following options are supported: <ul style="list-style-type: none"> • Permit - Allow traffic matching this filter rule. • Deny - Drop traffic matching this filter rule.
Type	The type of filter rule. The following options are supported: <ul style="list-style-type: none"> • IP Based – Configure Protocol parameter as TCP, UDP, ICMP or any. • Application Based – Configure Deep Packet Inspection (DPI) Type parameter as Application, Category, or Application Group
Protocol	This parameter is applicable only when Type parameter is IP Based . The following options are supported: <ul style="list-style-type: none"> • TCP: Match TCP traffic. • UDP: Match UDP traffic. • ICMP: Match ICMP traffic. • any: Match any of the above protocol traffic.
Source IP Address	The source IPv4 address for the filter rule.

Parameter	Description
	This is a mandatory parameter.
Mask	The source subnet mask for the filter rule. This is a mandatory parameter.
Port	This parameter is applicable only when Protocol parameter is TCP or UDP . Supported values: 1 to 65535 or any This is a mandatory parameter.
Destination IP Address	The destination IPv4 address for the filter rule. This is a mandatory parameter.
Mask	The destination subnet mask for the filter rule. This is a mandatory parameter.
Port	This parameter is applicable only when Protocol parameter is TCP or UDP . Supported values: 1 to 65535 or any This is a mandatory parameter.
Deep Packet Inspection (DPI) Type	This parameter is applicable only when Type parameter is Application Based . The following options are supported: <ul style="list-style-type: none"> • Application – Specific type of application within a category. • Category – All applications belonging to a category (For example, Social Messaging). This is a mandatory parameter.
DPI Application	This parameter is applicable only when DPI Type parameter is set to Application . This is a mandatory parameter.
DPI Category	This parameter is applicable only when DPI Type parameter is set to Category . This is a mandatory parameter.
Apply to	This parameter is applicable only when Type parameter is Application Based . The following options are supported: <ul style="list-style-type: none"> • All • User Group • IP Address / Source Subnet
User Group	This parameter is applicable when User Group option is selected. This is a mandatory parameter.
IP Address / Source Subnet	This parameter is applicable when IP Address / Source Subnet option is selected. This is a mandatory parameter.

Parameter	Description
Denial of Service (DoS) Protection	
IP Spoof	Enable or disable the IP spoof attack protection. By default, this parameter is disabled.
Smurf Attack	Enable or disable the smurf attack protection. By default, this parameter is disabled.
IP Spoof Log	Enable or disable IP spoof log messages. By default, this parameter is disabled.
ICMP Fragment	Enable or disable the fragmented ping attack. By default, this parameter is disabled.
GEO IP WAN to LAN Filters	
GEO IP WAN to LAN filters allows users to configure rules to permit/deny traffic based on the source country of inbound traffic.	
Mode	Specifies the mode for GEO IP WAN to LAN filters. The following options are supported: <ul style="list-style-type: none"> • Allow Only (Deny by default) – Allow traffic coming from the countries that are configured. The traffic coming from the countries which are not part of the configured countries will be dropped. • Deny Only (Allow by default) – Block traffic coming from the countries that are configured. The traffic coming from countries that are not part of the configured countries will be allowed. • None – Disables the feature. Traffic is allowed from all the countries.
Countries	The source countries from which the traffic originates.
Exceptions	
Exceptions allow users to configure source IP address ranges that are allowed in the inbound traffic. To add a new exception, click Add New . The Add New Exception window appears, as shown in Figure 432 .	
Start IP	Starting IPv4 address in the range. This is a mandatory parameter.
End IP	Ending IPv4 address in the range. This is a mandatory parameter.
GEO IP LAN to WAN Filters	
GEO IP LAN to WAN Filters allows users to configure rules to permit/deny traffic based on the destination country of outbound traffic.	
Mode	Specifies the mode for GEO IP LAN to WAN filters. The following options are supported: <ul style="list-style-type: none"> • Allow Only (Deny by default): Allow traffic destined to the countries matching the configured countries. The traffic destined for the countries which are not part of the configured countries will be dropped. • Deny Only (Allow by default): Block traffic destined to the countries

Parameter	Description
	<p>matching the configured countries. The traffic destined for the countries which are not part of the configured countries will be allowed</p> <ul style="list-style-type: none"> • None: Disables the feature. Traffic is allowed in all countries.
Countries	The destination countries to which the traffic is destined.
Exceptions <p>Exceptions allow users to configure destination IPv4 address ranges that are allowed in the outbound traffic. To add a new exception, click Add New. The Add New Exception window appears, as shown in Figure 432.</p>	
Start IP	<p>Starting IPv4 address in the range.</p> <p>This is a mandatory parameter.</p>
End IP	<p>Ending IPv4 address in the range.</p> <p>This is a mandatory parameter.</p>
Port Forward Rules <p>Port Forward Rules allow users to forward traffic destined to the WAN Interface IP address of NSE 3000 on a specific TCP or UDP port to any of the LAN IP address. Port Forward Rules provides remote access to internal resources.</p> <p>To add a new port forward rule, click Add New. The Add New Port Forward Rule window appears, as shown in Figure 433.</p>	
WAN	<p>The interface to forward inbound traffic to the internal host.</p> <p>The following options are supported:</p> <ul style="list-style-type: none"> • WAN-1 • WAN-2
Description	Displays the user-configured description for the port forward rule.
LAN IP Address	<p>The IPv4 address to which traffic will be forwarded.</p> <p>This is a mandatory parameter.</p>
LAN Port	<p>The LAN port to which the traffic will be forwarded.</p> <p>Supported values: 1 to 65535.</p> <p>This is a mandatory parameter.</p>
Protocol	<p>The protocol of forwarded traffic.</p> <p>The following options are supported:</p> <ul style="list-style-type: none"> • TCP • UDP
Port	<p>The destination port of the incoming traffic on the WAN interface.</p> <p>Supported values: 1 to 65535.</p> <p>This is a mandatory parameter.</p>
Apply To	<p>The following options are supported:</p> <ul style="list-style-type: none"> • All • IP Group

Parameter	Description
	<ul style="list-style-type: none"> • IP Address / Source Subnet
IP Group	This parameter is applicable only when IP Group option is selected.
IP Address / Source Subnet	<p>This parameter is applicable only when IP Address / Source Subnet option is selected.</p> <p>This is a mandatory parameter.</p>
NAT One-to-One <p>NAT One-to-One allows users to map an IP address on the WAN side to a LAN IP address. The IP address on the WAN side should be different from any of the WAN interface (WAN-1/WAN-2) IP addresses. NAT One-to-One rules provide remote access to any of the LAN resources.</p> <p>To add a new NAT one-to-one, click Add New. The Add New NAT One-to-One window appears, as shown in Figure 434.</p>	
WAN	<p>The following options are supported:</p> <ul style="list-style-type: none"> • WAN-1 • WAN-2
Public IP Address	<p>The public IPv4 address on the WAN side that is used to access the LAN resource.</p> <p>The public IPv4 address is different from the IPv4 address of the WAN (WAN-1/WAN-2) interfaces.</p> <p>This is a mandatory parameter.</p>
LAN IP Address	<p>The LAN IPv4 address of the server which is hosting the resource.</p> <p>This is a mandatory parameter.</p>
Protocol	<p>The protocol of the incoming traffic.</p> <p>The following options are supported:</p> <ul style="list-style-type: none"> • TCP • UDP
NAT One-to-Many <p>NAT One-to-Many provides remote access to internal resources. It maps a public IP address to multiple LAN IPs and ports.</p> <p>To add a new NAT one-to-many, click Add New, the Add New NAT One-to-Many window appears, as shown in Figure 435.</p>	
WAN	<p>The following options are supported:</p> <ul style="list-style-type: none"> • WAN-1 • WAN-2
Public IP Address	<p>The public IPv4 address on the WAN side that is used to access the LAN resource.</p> <p>The public IPv4 address is different from the IPv4 address of the WAN (WAN-1/WAN-2) interfaces.</p> <p>This is a mandatory parameter.</p>

Parameter	Description
LAN IP Address	The LAN IPv4 address of the server which is hosting the resource. This is a mandatory parameter.
LAN Port	The LAN Port which is hosting the resource. This is a mandatory parameter.
Protocol	The protocol of the incoming traffic. The following options are supported: <ul style="list-style-type: none"> • TCP • UDP
Port	The destination port of the incoming traffic on the WAN interface. This is a mandatory parameter.
Device Access	
Respond to ICMP pings from WAN	This parameter is disabled by default. When enabled, this service is enabled for all the sources, unless specific IP addresses or IP groups are configured in the IP Group and IP Address / Source Subnet parameters.
IP Group	Specifies the IP group for this service.
IP Address / Source Subnet	Specifies the IPv4 address or source subnet for this service.

Figure 431 The Add New Filter Rule window

Add New Filter Rule

Precedence*

Description

Action

Deny

Type

IP Based

Protocol

any

Source IP Address*

Specify IP address or 'any'

Mask*

Specify subnet mask or 'any'

Port*

any

Specify port or 'any'

Destination IP Address*

Specify IP address or 'any'

Mask*

Specify subnet mask or 'any'

Port*

any

Specify port or 'any'

Cancel

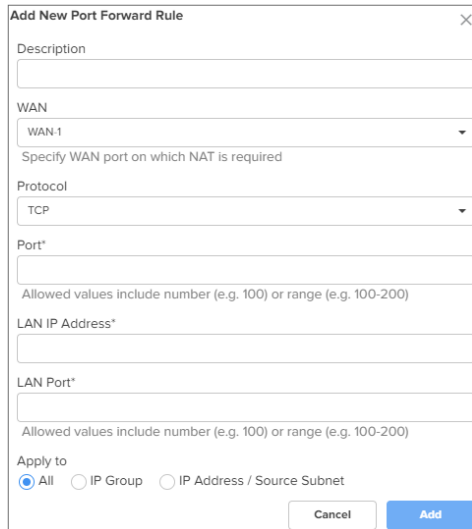
Add

Figure 432 *The Add New Exception window*



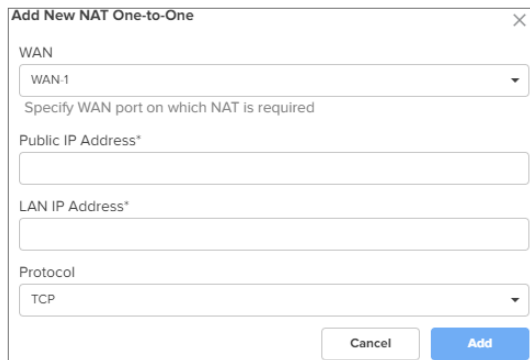
The 'Add New Exception' window is a simple form with a title bar containing a close button (X). It contains two text input fields: 'Start IP*' and 'End IP*'. At the bottom right, there are two buttons: 'Cancel' and 'Add'.

Figure 433 *The Add New Port Forward Rule window*



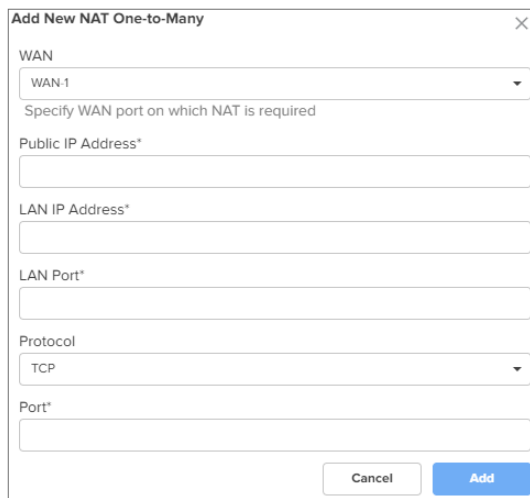
The 'Add New Port Forward Rule' window has a title bar with a close button (X). It contains several fields: a 'Description' text input; a 'WAN' dropdown menu currently showing 'WAN-1' with a subtext 'Specify WAN port on which NAT is required'; a 'Protocol' dropdown menu currently showing 'TCP'; a 'Port*' text input with a subtext 'Allowed values include number (e.g. 100) or range (e.g. 100-200)'; a 'LAN IP Address*' text input; and a 'LAN Port*' text input with the same subtext as the Port field. At the bottom, there is an 'Apply to' section with three radio buttons: 'All' (selected), 'IP Group', and 'IP Address / Source Subnet'. At the bottom right are 'Cancel' and 'Add' buttons.

Figure 434 *The Add New NAT One-to-One window*



The 'Add New NAT One-to-One' window has a title bar with a close button (X). It contains: a 'WAN' dropdown menu showing 'WAN-1' with subtext 'Specify WAN port on which NAT is required'; a 'Public IP Address*' text input; a 'LAN IP Address*' text input; and a 'Protocol' dropdown menu showing 'TCP'. At the bottom right are 'Cancel' and 'Add' buttons.

Figure 435 The Add New NAT One-to-Many window

The image shows a web-based configuration window titled "Add New NAT One-to-Many" with a close button (X) in the top right corner. The window contains several input fields and a dropdown menu. At the top, there is a "WAN" section with a dropdown menu currently showing "WAN-1". Below this is a text label "Specify WAN port on which NAT is required". The main configuration area includes four input fields: "Public IP Address*", "LAN IP Address*", "LAN Port*", and "Port*", each with an asterisk indicating it is a required field. Below the "LAN Port*" field is a "Protocol" dropdown menu currently set to "TCP". At the bottom right of the window are two buttons: "Cancel" and "Add".

3. Click **Save**.

DNS

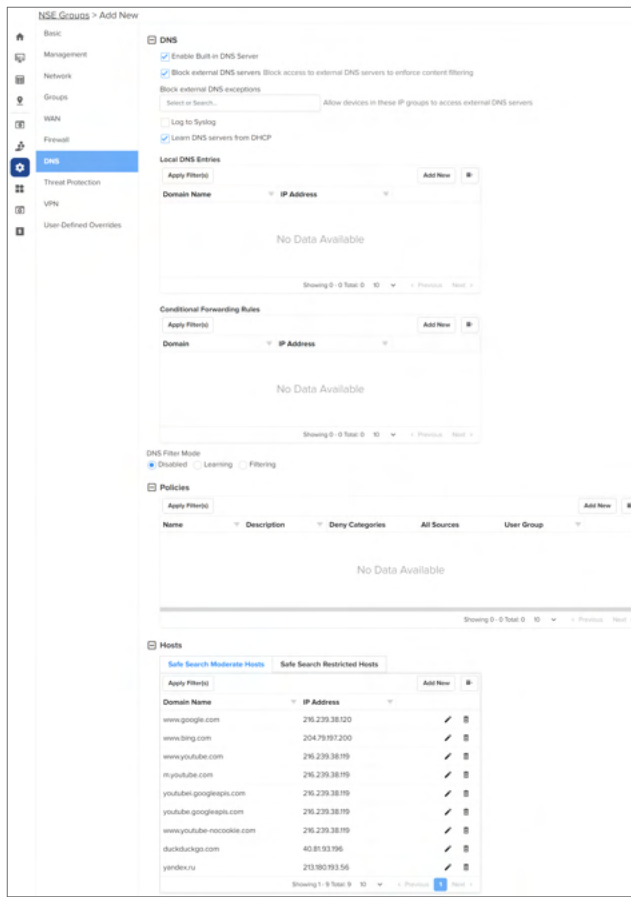
NSE 3000 supports DNS-based filters. DNS-based filters allow users to block certain category of websites. From the blocked list, users can still allow certain websites by adding them to the exception list. For example, if user blocks social-media category then all the social websites will be blocked including linkedin.com since linkedin.com belongs to social-media category. Adding linkedin.com to the Exception to filters list will allow access to linkedin.com while blocking other social-media websites.

To configure parameters on the **DNS** page, complete the following steps:

1. On the **NSE Groups > Add New** page, select the **DNS** tab.

The **DNS** page appears, as shown in [Figure 436](#).

Figure 436 *The DNS page*



2. Configure the parameters, as described in [Table 92](#).

Table 92 *Parameters on the DNS page*

Parameter	Description
On the DNS page, there are DNS , Policies , and Hosts sections.	
DNS	
Enable Built-in DNS Server	Indicates whether the on-board DNS server is enabled or disabled. By default, this parameter is enabled.
Block external DNS servers	Blocks the client to reach to any external DNS servers. By default, this parameter is enabled.
Block external DNS exceptions	Allows the clients added in the exceptions list to reach to any external DNS servers.
Log to Syslog	Specifies whether the DNS queries received from the client is logged to an external syslog server.
Learn DNS servers from DHCP	Dynamically learns the DNS server IP on WAN. By default, this parameter is enabled. When you disable this parameter, the Primary DNS and Secondary DNS parameters are displayed.

Parameter	Description
Primary DNS	The IPv4 address of the primary upstream DNS server.
Secondary DNS	The IPv4 address of the secondary upstream DNS server.
Local DNS Entries	
To add a new local host, click Add New . The Add New Local Host window appears, as shown in Figure 437 .	
Domain	A domain name for the local host. This is a mandatory parameter.
IP address	The IPv4 address of the local host. This is a mandatory parameter.
Conditional Forwarding Rules	
To add a new forwarding rule, click Add New . The Add New Forwarding Rule window appears, as shown in Figure 438 .	
Domain	A domain name for the forwarding rule. This is a mandatory parameter.
IP address	The IPv4 address of the server to which the DNS query is forwarded.
DNS Filter Mode	Specifies the mode for DNS filtering. The following options are supported: <ul style="list-style-type: none"> • Disabled: Disables DNS filter. By default, this option is selected. • Learning: Builds local cache for domain categories but does not filter requests. • Filtering: Filters requests based on configuration.
Policies	
To add a new policy, click Add New . The Add New Policy window appears, as shown in Figure 439 .	
Name	Name for the policy. This is a mandatory parameter.
Description	Description about the policy.
Deny categories	Categories to deny in the following sections: <ul style="list-style-type: none"> • Productivity • Privacy • Sensitive • Misc • IT Resources • Security Expand the sections and select individual categories. To select all categories in a section, select the checkbox provided for the section.
Safe Search Mode	The following options are supported:


Parameter	Description
	<ul style="list-style-type: none"> • Disabled: Disables safe search mode. By default, this option is enabled. • Moderate: Enable moderate safe search mode. • Restricted: Enable restricted safe search mode.
Allow Exceptions (List of Domain Names)	Enter the exempted domain names separated by a comma (,).
Apply to	<p>The following options are supported:</p> <ul style="list-style-type: none"> • All: Apply to all user groups. By default, this option is selected. • User Group: Apply to selected user groups.
User Group	<p>This parameter is applicable only when User Group option is selected for Apply to parameter.</p> <p>This is a mandatory parameter.</p>
<p>Hosts</p> <p>Hosts section contains two tabs - Safe Search Moderate Hosts and Safe Search Restricted Hosts</p> <p>The following parameters appear in both the tabs and can be configured as required.</p> <p>A list of hosts are already added by default. You can modify these hosts by clicking the edit  icon or you can add new hosts by clicking Add New in the respective tabs as shown in Figure 440 and Figure 441.</p>	
Domain Name	<p>The domain name for the safe search host</p> <p>This is a mandatory parameter.</p>
IP address	<p>The IPv4 address of the safe search host.</p> <p>This is a mandatory parameter.</p>

Figure 437 The Add New Local Host window



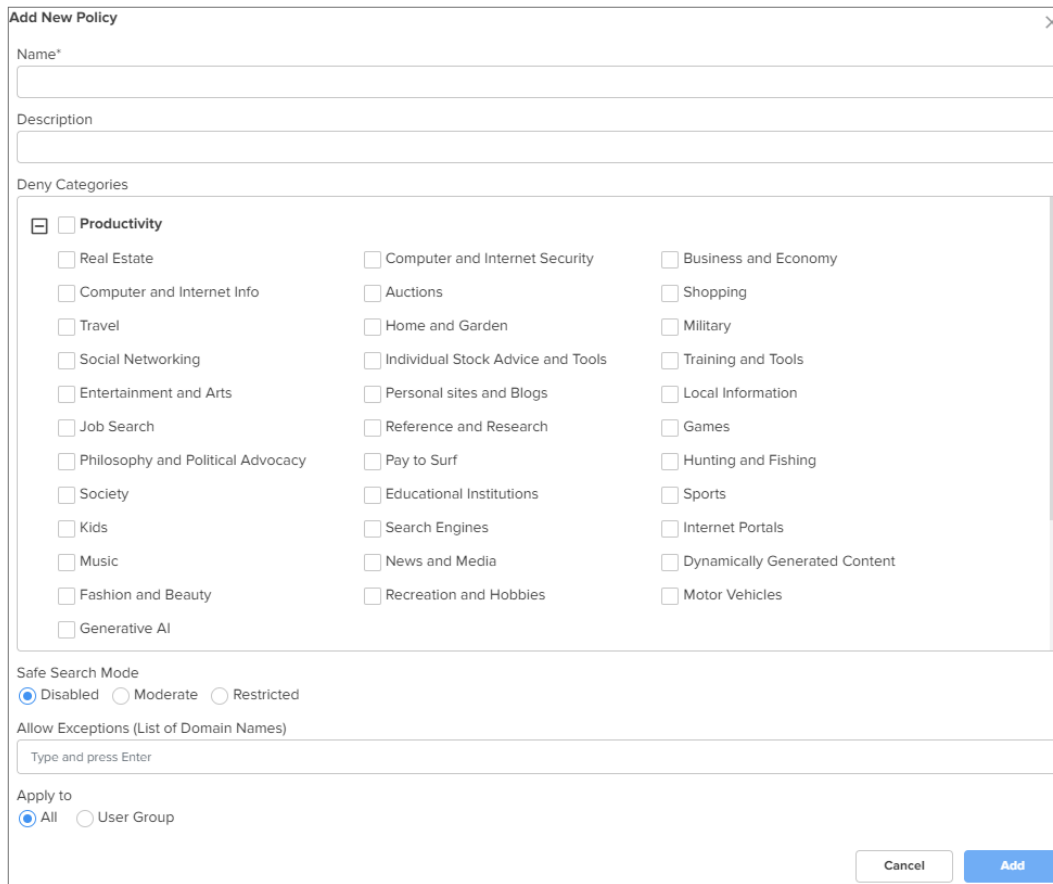
The 'Add New Local Host' window is a small dialog box with a title bar containing a close button (X). It contains two text input fields: 'Domain Name*' and 'IP Address*'. Below the input fields are two buttons: 'Close' and 'Add'.

Figure 438 The Add New Forwarding Rule window



The 'Add New Forwarding Rule' window is a small dialog box with a title bar containing a close button (X). It contains two text input fields: 'Domain*' and 'IP Address'. Below the 'IP Address' field is a placeholder text 'Type and press Enter'. At the bottom are two buttons: 'Close' and 'Add'.

Figure 439 *The Add New Policy window*

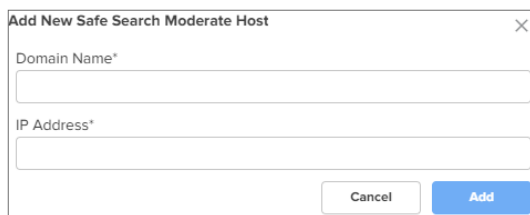


The 'Add New Policy' window contains the following fields and options:

- Name***: A text input field.
- Description**: A text input field.
- Deny Categories**: A list of categories with checkboxes, including:
 - ☐ Productivity
 - ☐ Real Estate
 - ☐ Computer and Internet Info
 - ☐ Travel
 - ☐ Social Networking
 - ☐ Entertainment and Arts
 - ☐ Job Search
 - ☐ Philosophy and Political Advocacy
 - ☐ Society
 - ☐ Kids
 - ☐ Music
 - ☐ Fashion and Beauty
 - ☐ Generative AI
 - ☐ Computer and Internet Security
 - ☐ Auctions
 - ☐ Home and Garden
 - ☐ Individual Stock Advice and Tools
 - ☐ Personal sites and Blogs
 - ☐ Reference and Research
 - ☐ Pay to Surf
 - ☐ Educational Institutions
 - ☐ Search Engines
 - ☐ News and Media
 - ☐ Recreation and Hobbies
 - ☐ Business and Economy
 - ☐ Shopping
 - ☐ Military
 - ☐ Training and Tools
 - ☐ Local Information
 - ☐ Games
 - ☐ Hunting and Fishing
 - ☐ Sports
 - ☐ Internet Portals
 - ☐ Dynamically Generated Content
 - ☐ Motor Vehicles

- Safe Search Mode**: Radio buttons for ☒ Disabled, ☐ Moderate, and ☐ Restricted.
- Allow Exceptions (List of Domain Names)**: A text input field with the placeholder 'Type and press Enter'.
- Apply to**: Radio buttons for ☒ All and ☐ User Group.
- Buttons**: 'Cancel' and 'Add' buttons at the bottom right.

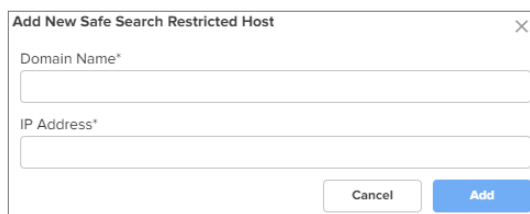
Figure 440 *The Add New Safe Search Moderate Host*



The 'Add New Safe Search Moderate Host' window contains the following fields and buttons:

- Domain Name***: A text input field.
- IP Address***: A text input field.
- Buttons**: 'Cancel' and 'Add' buttons at the bottom right.

Figure 441 *The Add New Safe Search Restricted Host*



The 'Add New Safe Search Restricted Host' window contains the following fields and buttons:

- Domain Name***: A text input field.
- IP Address***: A text input field.
- Buttons**: 'Cancel' and 'Add' buttons at the bottom right.

3. Click **Save**.

Threat Protection

Using the **Threat Protection** tab, you can configure the Intrusion Detection and Prevention system (IDS/IPS) parameters.

NSE 3000 supports IDS/IPS engine. IPS engine uses a series of rules that help define a malicious network activity. IPS engine supports rules from snort and emerging threats. The solution supports both community and licensed rules. The IPS engine uses these rules to find packets that match against them and generates alerts for users.

To configure parameters on the **Threat Protection** page, complete the following steps:

1. On the **NSE Groups > Add New** page, select the **Threat Protection** tab.

The **Threat Protection** page appears, as shown in [Figure 442](#).

Figure 442 *The Threat Protection page*

2. Configure the parameters, as described in [Table 93](#).

Table 93 *Parameters on the Threat Protection page*

Parameter	Description
IDS/IPS	
Enable IDS/IPS	<p>Indicates whether IDS/IPS is enabled or disabled.</p> <p>By default, this parameter is enabled <i>only in new NSE groups</i>.</p> <p>When this parameter is enabled, the following default settings apply:</p> <ul style="list-style-type: none"> • Mode: Detection • Rule Type: snort-community • Rules: Balanced • Auto Update: Enabled • Auto Update Interval: 24 Hrs
Mode	Specifies the IDS/IPS mode.

Parameter	Description
	<p>The following options are supported:</p> <ul style="list-style-type: none"> • Detection – Detects malicious activity and generates alerts for users. • Prevention – Detects malicious activity, generates alerts for users, and takes action to prevent attacks.
Rule Type	<p>Specifies the IDS/IPS rule type.</p> <p>The following options are supported:</p> <ul style="list-style-type: none"> • snort-community – The community rule set is a GPLv2 Talos certified rule set that is distributed free of charge and without any license restrictions. The rules are updated every Tuesday and Thursday. • snort-vrt – The Snort Subscriber rule set is developed by Talos research team and is governed by license agreement. The rule set is updated on Tuesday and Thursday. The snort-vrt rule set requires an oinkcode to download and activate rules. • emerging-threats open – Consists of signatures contributed from the community. The emerging-threats open rule sets are distributed free of charge. • emerging-threats pro – Consists of signatures created as a result of Proofpoint research. The rule sets are governed by license agreement. The emerging-threats pro rule set requires an oinkcode to download and activate the rules.
Rules	<p>Specifies the IDS/IPS rule policy. This parameter is applicable when Rule Type is snort-vrt or snort-community.</p> <p>The following options are supported:</p> <ul style="list-style-type: none"> • Connectivity – Policy designed to favor device performance over the security controls in the policy. • Balanced – This policy is the default policy that is recommended for initial deployments. The policy attempts to balance security needs and performance characteristics. • Security – This policy is designed for customer base that is extremely concerned about organizational security. This policy is deployed in networks that have higher security requirements.
Oink Code	This parameter is applicable when Rule Type is snort-vrt or emergency- threats pro .
Category	<p>Categories to select from the Category section. This parameter is applicable when Rule Type is snort-vrt, emerging-threats open, or emerging-threats pro.</p> <p>Note:</p> <p>The categories are same for emerging-threats open and emerging-threats pro rule types.</p> <p>You can select or clear all categories by using the Category checkbox.</p>
Rule Updates	
Auto Update	<p>Indicates whether the IDS/IPS rules must be automatically updated or not.</p> <p>By default, this parameter is enabled.</p> <p>When Auto Update is enabled, NSE 3000 will periodically download and activate the IDS/IPS rules.</p>
Auto Update	Time interval for the periodic updates of IDS/IPS rules.

Parameter	Description
Interval	<p>The following options are supported:</p> <ul style="list-style-type: none"> • 12 Hrs – Auto updates the rules every 12 hours. • 24 Hrs – Auto updates the rules every 24 hours. <p>By default, the 24 Hrs option is selected.</p>
IDS/IPS bypass list	<p>List of allowed IPv4 addresses or range of allowed IPv4 addresses.</p> <p>IDS/IPS operating in prevention mode blocks traffic from a host on detecting malicious traffic from the host.</p> <p>When an IPv4 address is part of allowed IP addresses, IDS/IPS will not block traffic from the host even when malicious traffic is detected.</p>

3. Click **Save**.

VPN

NSE 3000 provides an on-board VPN server that allows remote users to establish a connection using the native VPN client supported in most of the operating systems. The VPN server uses the L2TP/IPsec protocol with the IPsec encryption and hashing algorithms. The VPN server maintains a pool of IP addresses and leases the IP addresses from this pool for remote users.

NSE 3000 also provides an on-board RADIUS server that allows authentication and accounting of enterprise and remote users. The RADIUS server maintains user profiles in a central database.

The **VPN** page allows to set the following configurations:

- [Site-to-Site VPN configuration](#)
- [Client VPN configuration](#)
- [User configuration for Client VPN protocols](#)
- [RADIUS Client configuration](#)
- [VPN Server interface configuration](#)

Site-to-Site VPN configuration

IPsec tunnel is a VPN technology that provides a secure, encrypted connection between two devices or networks over the internet or another public network. It uses IPsec protocols to encrypt the traffic between two endpoints, making it difficult for anyone to intercept the communication.

IPsec site-to-site tunnel is used to connect two remote sites for secure communications. NSE allows setting up tunnels both in responder mode and initiator mode. Both, IKEv1 and IKEv2 are supported in the configuration. The default version is IKEv2.



Note

You can configure up to 100 IPsec site-to-site tunnels.

Pre-shared key is the authentication method supported by the NSE device. Each site can have its own pre-shared key. The site is identified by an identifier (string or the IP address of the site). Each site has to be configured with a local and remote site for the tunnel to establish.



Note

NSE supports VPN translation for a Site-to-Site configuration. The local subnets that are advertised to peers are configured to translate to a different equally sized subnet. This is useful in deployments

where the same local subnet is used in multiple locations. For example, the 192.168.200.0/24 network can be found in multiple locations as it is the default network configuration. If 192.168.200.0/24 is available in multiple locations, this can be configured to be translated to 10.10.10.0/24. to prevent address conflicts, The translation can also be 1 to M. In case of 1 to M, 192.168.200.0/24 can be configured to be translated to 10.10.10.10/32.

You can perform the following configurations:

- [Enabling a Site-to-site VPN configuration](#)
- [Switching to Auto VPN from Site-to-Site VPN](#)

Enabling a Site-to-site VPN configuration

To enable a site-to-Site VPN and configure the settings, complete the following steps:

1. On the **NSE Groups>Add New** page, select the **VPN** tab.

The **VPN** page appears, as shown in [Figure 443](#).

Figure 443 The VPN page

NSE Groups > Add New

Site-to-Site VPN

☐ Enable Site-to-Site VPN

Client VPN

WireGuard | **IPSec IKEV2** | **L2TP over IPSec**

☐ Enable WireGuard

Users

Apply Filter(s) Add New

Email ID

No Data Available

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

RADIUS Clients

Apply Filter(s) Add New

Name Address Prefix Length

No Data Available

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

VPN

VPN Server Interface

All

2. In the **Site-to-Site VPN** section, select the **Enable Site-to-Site VPN** checkbox to enable the site-to-site VPN configuration. By default, it is disabled. When you enable site-to-site VPN, you are allowed to add a new site-to-site VPN and configure parameters.
3. To add a new site-to-site VPN, click **Add New**. The **Add New Site-to-Site VPN** window appears, as shown in [Figure 444](#).

Figure 444 The Add New Site-to-Site VPN window

4. Configure the parameters, as described in [Table 94](#).

Table 94 Parameters for the Site-to-Site VPN configuration

Parameter	Description
Name	A name for the new site-to-site VPN. This is a mandatory parameter.
IKE version	The Internet Key Exchange (IKE) version for the site-to-site VPN. The following options are supported: <ul style="list-style-type: none"> • IKE v1 • IKE v2
Role	Specifies the role for the tunnels. The following options are supported: <ul style="list-style-type: none"> • Initiator • Responder Default role: Responder
Dead peer detection interval	The interval (in seconds) for detecting dead peers. Range: 30 - 600 seconds. Default: 120 seconds This is a mandatory parameter.
Remote ID	The remote ID. The value of 192.168.50.10 is pre-configured and is not modifiable. This is a mandatory parameter.
Local ID	The local ID. This is a mandatory parameter.
Local Subnets	This is a mandatory parameter. This parameter allows you to add multiple local subnets. To add new local subnets, complete the following steps: <ol style="list-style-type: none"> a. Click Add New. The Add New Local Subnet window appears.

Parameter	Description
	<p>b. In the Add New Local Subnet window, enter a valid address in the Local Subnets field. The VPN subnet field is optional. If the Local subnets have a VPN translation, then provide a VPN network address in the VPN subnet field or it can be left blank (empty). NSE supports the VPN translation feature.</p> <p>c. Click Add on the Add New Local Subnet window.</p>
Remote Subnets	<p>The comma-separated list of remote subnets.</p> <p>This is a mandatory parameter.</p>
Remote PSK	<p>The remote PSK.</p> <p>This is a mandatory parameter.</p>
Local PSK	<p>The local PSK.</p> <p>This is a mandatory parameter.</p>
The following parameters are common for both IKE Phase 1 and IKE Phase 2 .	
Encryption	<p>The following options are supported:</p> <ul style="list-style-type: none"> • aes128 • aes192 • aes256 • aes128-gcm16 • aes192-gcm16 • aes256-gcm16 • 3des
Integrity	<p>The following options are supported:</p> <ul style="list-style-type: none"> • md5 • sha1 • sha256
DH Group	<p>The following options are supported:</p> <ul style="list-style-type: none"> • 1 • 2 • 5 • 14 • 15
Key Lifetime	<p>The duration (in hours) for the pre-shared key.</p> <p>Range: 1 to 24</p>

5. Click **Add**. The new site-to-site VPN is added.
6. Click **Save** on the Add New page to apply the changes.
7. To view the IPsec tunnel statistics, navigate to the **NSE Group > Network > VPN Sites** tab, as shown in [Figure 445](#).

Figure 445 The VPN Sites page

Name	IKE State	IPsec State	Remote Host	Remote Port	Duration	Rx Bytes	Tx Bytes	Remote Subnets
Tunnel-to-mumbai	Established	Installed	10.110.200.40	4500	0d 0h 34m	0	0	172.16.10.0/24

Switching to Auto VPN from site-to-site VPN

Currently, NSE 3000 supports 100 site-to-site VPN tunnels. However, cnMaestro allows the Auto VPN configuration to simplify Site-to-Site configuration. The Auto VPN configuration is useful for device-level configuration, device-level monitoring, and debugging.

Consider the following key points:

- If there is an NSE device for which the Auto VPN is not configured, the **Site-to-Site VPN** section on the VPN page displays a message (as shown in [Figure 446](#)). This message indicates that you can add the Auto VPN configuration for this NSE device. When you configure an auto VPN group using the **Configuration > NSE Profiles > Auto VPN** page, the Site-to-Site VPN configuration changes are disabled for the NSE device.

Figure 446 The site-to-site VPN configuration before switching to Auto VPN

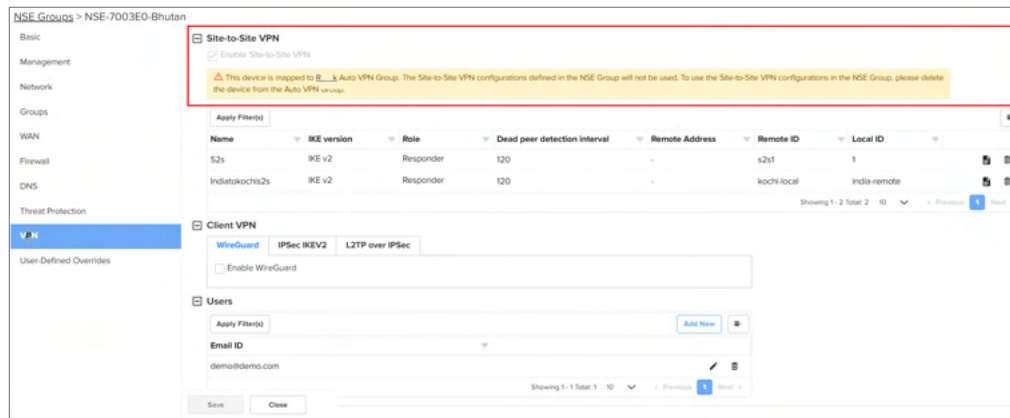
- If the sites are already added to an Auto VPN group, then you cannot use the Site-to-Site VPN configuration. A message is displayed in the **Site-to-Site VPN** section on the VPN page (as shown in [Figure 447](#)). You must delete the NSE device from the Auto VPN group on the **Auto VPN** page to use the Site-to-Site VPN configuration.



Note

You CANNOT configure a site-to-site VPN for the NSE 3000 device on which auto VPN is configured. You must delink the devices from Auto VPN group and then configure the Site-to-Site VPN feature.

Figure 447 The site-to-site VPN configuration after switching to Auto VPN



Client VPN configuration

To configure Client VPN specific parameters on the **VPN** page, complete the following steps:

1. On the **VPN** page (as shown in [Figure 443](#)), go to the **Client VPN** section.

The **Client VPN** section contains the following tabs:

- [WireGuard](#): A VPN protocol that is highly secure. It is simpler and more efficient than traditional IPSec. It is simpler and more efficient than traditional IPSec.
- [IPSec IKEV2](#)
- [L2TP over IPSec](#)

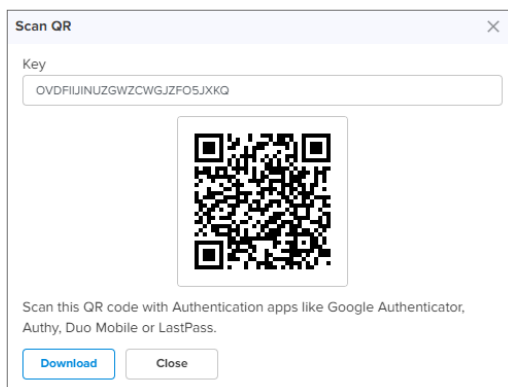
2. Configure the parameters, as described in [Table 95](#).

Table 95 Parameters for the Client VPN configuration

Parameter	Description
WireGuard	
Enable WireGuard	Indicates whether WireGuard is enabled or disabled. By default, this parameter is disabled.
Following parameters appear when you select Enable WireGuard checkbox.	
Port	Indicates the WireGuard listen port number. Default: 51820 This is a mandatory parameter.
Client Pool	Indicates the WireGuard interface IP for the device and the client IPs to be assigned for the WireGuard clients. This is a mandatory parameter.
Keep Alive	Periodic keep alive packets sent for the configured duration. Default: 5 seconds This is a mandatory parameter.
Enable Split Tunnel	Indicates whether the split tunnel is enabled or disabled. By default, this parameter is disabled. Note: When you enable split tunnel, only the traffic destined to tunnelled subnets is

Parameter	Description
	allowed. You can override the Enable Split Tunnel parameter at the user level.
Tunnelled Subnets	Specifies the list of local subnets in NSE that should be allowed access from the WireGuard clients. Note: The same Tunnelled Subnets field is auto-populated in the Add New User window. You can edit this field at the user level.
IPSec IKEV2	
Enable IPSec IKEV2	Indicates whether IPSec IKEV2 is enabled or disabled. By default, this parameter is disabled.
Following parameters appear when you select Enable IPSec IKEV2 checkbox.	
Client IP Pool Range Start	Starting IPv4 address in the range. This is a mandatory parameter.
Client IP Pool Range End	Ending IPv4 address in the range. This is a mandatory parameter.
L2TP over IPSec	
Enable L2TP over IPSec	Indicates whether L2TP over IPSec is enabled or disabled. By default, this parameter is disabled.
Following parameters appear when you select Enable L2TP over IPSec checkbox.	
Client IP Pool Range Start	Starting IPv4 address in the range. This is a mandatory parameter.
Client IP Pool Range End	Ending IPv4 address in the range. This is a mandatory parameter.
IPsec Shared Secret	Enter a pre-shared key string for the IPsec protocol. The shared secret is used between the VPN Client and Server for device authentication. This is a mandatory parameter.
Enable 2FA	Indicates whether two-factor authentication (2FA) is enabled or disabled. By default, this parameter is disabled.

- When you enable **two-factor authentication (2FA)**, scan the QR code to add a 16-digit key to a particular user's Google Authenticator app.



An email is also sent to the configured email address with the QR code and the 16-digit key. The two-factor authentication gets enabled for the user when the user tries to connect to the NSE 3000 device using the remote VPN client from the WAN side. Users on the LAN side do not require two-factor authentication (2FA).

4. Click **Save** on the Add New page to add the changes.

User configuration for Client VPN protocols

The **Users** section on the VPN page is common for all the three protocols - WireGuard, IPSec IKEV2, and L2TP over IPSec. To configure user specific parameters on the **VPN** page, complete the following steps:

1. On the **VPN** page (as shown in [Figure 443](#)), go to the **Users** section.
2. To add a new user, click **Add New**. The **Add New User** window appears, as shown in [Figure 448](#).

Figure 448 The Add New User window

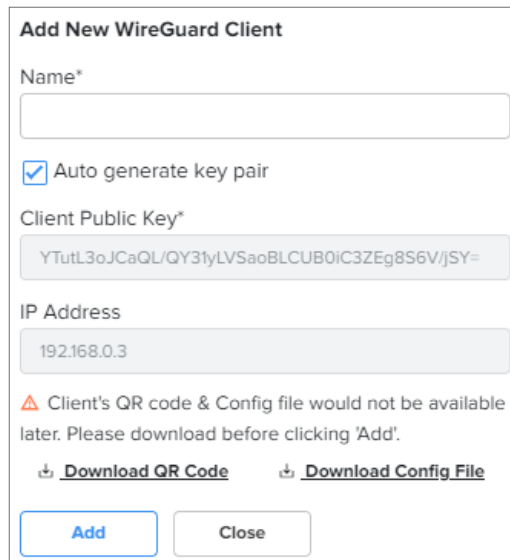
3. Configure the parameters, as described in [Table 96](#).

Table 96 Parameters for the user configuration

Parameter	Description
Users	
Email ID	Email ID of the user. User is either an enterprise user or a remote user. This is a mandatory parameter.
Password	Password for the user. This is a mandatory parameter.
Enable WireGuard	Indicates whether WireGuard is enabled or disabled. This parameter is visible on the Add New User window only if you have selected the Enable WireGuard checkbox in the Client VPN section. By default, this parameter is disabled.
Following parameters appear when Enable WireGuard checkbox is selected in the Add New User window.	
Enable Split Tunnel	Indicates whether split tunnel is enabled or disabled. By default, this parameter is enabled.
Tunnelled Subnets	Specifies the list of local subnets in NSE that should be allowed access from the WireGuard clients.

Parameter	Description
Device	<p>Indicates the NSE 3000 device.</p> <p>When you select an NSE 3000 device, the device's public key is populated in the [Peer]section of the WireGuard client configuration file.</p> <p>This is a mandatory parameter.</p>
WAN Interface	<p>WAN Interface of the NSE 3000 device.</p> <p>When you select a WAN interface, the NSE 3000 device's WAN IP is populated as the endpoint IP in the [Peer] section of the WireGuard client configuration file.</p> <p>The following WAN Interface options are supported:</p> <ul style="list-style-type: none"> • WAN-1 • WAN-2
<p>Clients: In this section, you have an option to add a new WireGuard client.</p> <p>To add a new WireGuard client, click Add New. The Add New WireGuard Client window appears, as shown in Figure 449.</p>	
Name	<p>Name for the new WireGuard client.</p> <p>This is a mandatory parameter.</p>
Auto generate key pair	<p>Generates a public and private key pair for the client. By default, this parameter is enabled.</p> <p>When this option is enabled, the Client Public Key field is auto-populated with the public key generated for that client.</p> <p>When this option is disabled, you need to provide the WireGuard client public key generated on the WireGuard client device.</p>
Client Public Key	<p>Public key of the client.</p> <p>This is a mandatory parameter.</p>
IP Address	Auto-generated IP address of the WireGuard client.
<p>Note: You have options to download QR code and configuration file in the Add New WireGuard Client window, as shown in Figure 449.</p>	

Figure 449 The Add New WireGuard client window



The 'Add New WireGuard Client' window contains the following elements:

- Name***: A text input field.
- ☒ **Auto generate key pair**: A checked checkbox.
- Client Public Key***: A text area containing the key `YTutL3oJCaQL/QY31yLVSaoBLCUB0iC3ZEg8S6V/jSY=`.
- IP Address**: A text area containing the address `192.168.0.3`.
- A warning message: **⚠ Client's QR code & Config file would not be available later. Please download before clicking 'Add'.**
- Two download links: [Download QR Code](#) and [Download Config File](#).
- Add** and **Close** buttons at the bottom.

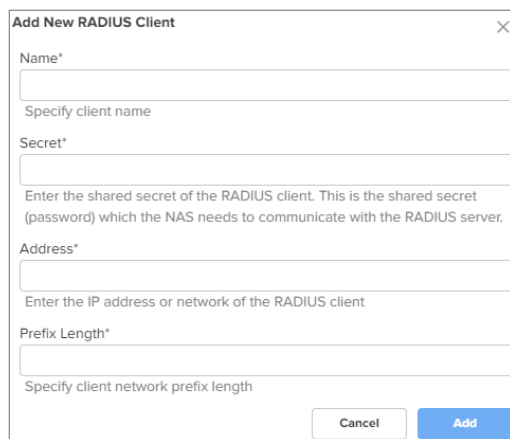
4. Click **Add**. The user configuration is added.
5. Click **Save** on the Add New page to apply the changes.

RADIUS Client configuration

To set the RADIUS client configuration on the VPN page, complete the following steps:

1. On the **VPN** page (as shown in [Figure 443](#)), go to the **RADIUS Clients** section.
2. To add a new RADIUS client, click **Add New**. The **Add New RADIUS Client** window appears, as shown in [Figure 450](#).

Figure 450 The Add New RADIUS Client window



The 'Add New RADIUS Client' window contains the following elements:

- Name***: A text input field with the placeholder 'Specify client name'.
- Secret***: A text input field with the placeholder 'Enter the shared secret of the RADIUS client. This is the shared secret (password) which the NAS needs to communicate with the RADIUS server.'
- Address***: A text input field with the placeholder 'Enter the IP address or network of the RADIUS client'.
- Prefix Length***: A text input field with the placeholder 'Specify client network prefix length'.
- Cancel** and **Add** buttons at the bottom.

3. Configure the parameters, as described in [Table 14](#).

Table 97 Parameters for the RADIUS Client configuration

Parameter	Description
RADIUS Clients	
Name	Name of the RADIUS client.

Parameter	Description
	This is a mandatory parameter.
Secret	The shared secret of the RADIUS client. This is the shared secret (password) that the NAS needs to communicate with the RADIUS server. This is a mandatory parameter.
Address	The IPv4 address or network address of the RADIUS client. This is a mandatory parameter.
Prefix Length	The client network prefix length. This is a mandatory parameter.

4. Click **Add** on the Add New RADIUS Client window.
5. Click **Save** on the Add New page to add the changes.

VPN Server interface configuration

To configure the VPN Server interface, complete the following steps:

1. On the **VPN** page (as shown in [Figure 443](#)), go to the **VPN** section.

The **VPN Server Interface** dropdown list is visible. This parameter displays the following options:

- **WAN-1** - The first WAN interface on your server.
- **WAN-2** - The second WAN interface on your server.
- **All** - Applies to all WAN interfaces.

2. Select the required option from the dropdown list.
3. Click **Save** on the Add New page to add the changes.

User-Defined Overrides

Using the **User-Defined Overrides** tab, you can configure the user-defined overrides.

To configure parameters on the **User-Defined Overrides** page, complete the following steps:

1. On the **NSE Groups > Add New** page, select the **User-Defined Overrides** tab.

The **User-Defined Overrides** page appears, as shown in [Figure 451](#).

Figure 451 *The User-Defined Overrides page*

NSE Groups > _Nse_165-NSE_Group-20240502125341

User-Defined Overrides

Advanced configuration settings entered below will be applied on top of the NSE 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

Configuration Variables are supported to insert device-unique values in this format:
\$(VARIABLE_NAME) or
\$(VARIABLE_NAME=default value)
VARIABLE_NAME should not contain dollar (\$), period (.) or spaces and it should not be more than 64 characters long.

Macros are also supported to automatically insert values taken from the device in the format:
%(ESN) for the MAC address.
%(esn) for MAC address in lowercase.
%(ESN-) for MAC address in separated by '-'.
%(esn-) for MAC address in lowercase separated by '-'.
%(ESN6) for the last 6 non-separator characters of the MAC address.
%(esn6) for the last 6 non-separator characters of the MAC address in lowercase.
%(MSN) for the serial number.
For more information please see the "Help" link at the bottom of this page.

⚠ 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 NSE Group is valid and safe to use.

```
!
interface eth 1
management-access all
!
!
interface eth 2
management-access all
!
```

Save Close

2. In the text box, enter the configuration that you want to apply to the device.
3. Click **Save**.

Configuring WAN in the device UI

In the **WAN** page, you can configure the device's IPv4 address based on the IP mode.



Note

If **PPPoE** is used as the WAN connection mode as shown in [Figure 452](#), make sure to configure the PPPoE username and password. Once you have configured the PPPoE user name and password, you can proceed to configure the NSE group by providing the same username and password and then attaching the default NSE group to the device.

Figure 452 PPPoE as WAN connection mode

The screenshot shows the Cambium Networks web interface. On the left is a navigation sidebar with links to Dashboard, Management, WAN (highlighted), Operations, and Troubleshoot. The main content area is titled 'WAN' and contains two tabs: 'WAN-1' and 'WAN-2'. Under the 'WAN-1' tab, the 'IP Mode' dropdown menu is set to 'PPPoE' and is highlighted with a red rectangle. Below this are input fields for 'Account Name', 'Service Name', 'User Name', and 'Password', each with a hint: 'Configure Account name (max 32 characters)', 'Configure Service name (max 32 characters)', and 'Configure MTU for PPPoE (500-1492 bytes)'. The 'MTU' field is set to '1492'. There is a checkbox for 'TCP MSS Clamping' with the label 'Enable/Disable TCP MSS Clamping'. At the bottom is a 'VLAN ID' field and a 'Save' button.

To view and configure the WAN settings, complete the following steps in the device UI:

1. From the main NSE 3000 dashboard page, click **WAN** tab from the left panel.

The **WAN** page appears, as shown in [Figure 453](#).



Note

By default, WAN-1 page appears. You can configure WAN on WAN-1 or WAN-2.

Figure 453 The WAN page

This screenshot shows the same WAN configuration page as Figure 452, but with the 'IP Mode' dropdown menu set to 'Dynamic'. The 'VLAN ID' field now has a hint: 'Minimum 1, Maximum 4094'. The 'Save' button remains at the bottom.

2. Configure the parameters, as described in [Table 98](#).

Table 98 *Parameters on the WAN page*

Parameter	Description
IP Mode	<p>Determines the network that must be configured to use IPv4 addresses.</p> <p>The following options are supported:</p> <ul style="list-style-type: none"> • Dynamic • Static • PPPoE <p>By default, the Dynamic mode is selected.</p>
VLAN ID	<p>The VLAN ID can range from 1 to 4094.</p> <p>The VLAN configuration is optional.</p> <p>When the 802.1Q header is configured, all transmitted frames are expected to include the 802.1Q header with the same VLAN ID.</p>
Following parameters appear only when you select the mode as Static from the IP Mode dropdown list, as shown in Figure 454 .	
IP Address	The 32-bit binary number that identifies a network element by both network and host.
Subnet Mask	The subnet mask for the destination IP/network for the route.
Gateway	The gateway for the destination IP/network for the route.
DNS	
Primary DNS	The IPv4 address of primary upstream DNS server.
Secondary DNS	The IPv4 address of secondary upstream DNS server.
Following parameters appear only when you select the mode parameter as PPPoE from the IP Mode dropdown list, as shown in Figure 455 .	
Account Name	<p>The name of Access Controller.</p> <p>This parameter allows a maximum of 32 characters.</p> <p>This parameter is optional.</p>
Service Name	<p>Service name of Access Controller.</p> <p>This parameter allows a maximum of 32 characters.</p> <p>This parameter is optional.</p>
User Name	<p>A user name for PPPoE authentication.</p> <p>This parameter is mandatory.</p>
Password	<p>A password for PPPoE authentication.</p> <p>This parameter is optional.</p>
MTU	<p>MTU for PPPoE interface in bytes.</p> <p>Default: 1492. Range: 500 to 1492</p>
TCP MSS Clamping	<p>Indicates whether TCP MSS Clamping is enabled or disabled.</p> <p>By default, this parameter is disabled.</p>

Figure 454 Static mode

The screenshot shows the Cambium Networks web interface. On the left is a navigation menu with links for Dashboard, Management, WAN (highlighted), Operations, and Troubleshoot. The main content area is titled 'WAN' and has two tabs: 'WAN-1' (selected) and 'WAN-2'. The configuration fields for 'WAN-1' are as follows:

- IP Mode:** A dropdown menu set to 'Static'.
- IP Address:** An empty text input field.
- Subnet Mask:** An empty text input field.
- Gateway:** An empty text input field.
- DNS:** A checkbox that is currently unchecked.
- VLAN ID:** An empty text input field with a note 'Minimum 1, Maximum 4094'.

At the bottom of the configuration area is a blue 'Save' button.

Figure 455 PPPoE mode

The screenshot shows the same Cambium Networks web interface as Figure 454, but with the 'WAN-1' configuration set to 'PPPoE' mode. The configuration fields are:

- IP Mode:** A dropdown menu set to 'PPPoE'.
- Account Name:** An empty text input field with a note 'Configure Account name (max 32 characters)'.
- Service Name:** An empty text input field with a note 'Configure Service name (max 32 characters)'.
- User Name:** An empty text input field.
- Password:** An empty text input field.
- MTU:** A text input field containing '1492' with a note 'Configure MTU for PPPoE (500-1492 bytes)'.
- TCP MSS Clamping:** A checkbox that is currently unchecked, with a note 'Enable/Disable TCP MSS Clamping'.
- VLAN ID:** An empty text input field with a note 'Minimum 1, Maximum 4094'.

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

3. Click **Save**.

Configuring Auto VPN

Site-to-site VPN is a secure way of connecting multiple networks across sites. Currently, NSE 3000 supports 100 site-to-site VPN tunnels. However, this site-to-site VPN has some problems specific to device-level configuration, device-level monitoring, and debugging.

As a solution, the **Auto VPN** feature of NSE offers simplified configuration, monitoring, and debugging of site-to-site tunnels. With this feature, NSE 3000 devices can be networked in either of the following modes: Hub and Spoke, Mesh, or Hybrid. For example, there is one NSE device (two in HA mode) present in one site. With Auto VPN configured, the NSE device connects multiple sites in either one of the modes (Hub and Spoke mode or Mesh' mode).

When Auto VPN is configured using cnMaestro, NSE automates the setting up of site-to-site tunnels for the VPN groups between Cambium NSE devices. Site-to-site tunnels can be deployed either in a Hub and Spoke mode or in full mesh mode.

Hub and Spoke mode

In the Hub and Spoke mode, 100+ NSE devices can be accommodated in the network, which are connected to a single hub node. There is no need to edit 100 NSE groups to connect all these devices.

The hub can be a non-Cambium device, allowing for greater flexibility in deployment scenarios.

Example: In current deployments of NSE 3000 devices, third-party firewalls are used as hubs and NSE 3000 devices as spokes. If the Hub and Spoke mode is configured, only a single hub (non-Cambium) is used and all the sites are connected to this single hub. In this mode, the spoke devices (NSE) establish secure connections with the hub.

Mesh mode

Full mesh deployments require configuring of the networks on each NSE device. When Auto VPN is configured, the devices in the group establish connectivity with the every other member in the group in a full mesh mode.

The Mesh mode is applicable only when the cambium hubs are used.



Note

You CANNOT configure a site-to-site VPN for the NSE 3000 device on which Auto VPN is configured. You must delink the devices from the Auto VPN group to configure the Site-to-Site VPN feature. The device cannot have both site-to-site VPN and auto VPN at the same time.

Using the cnMaestro UI, you can configure the Auto VPN feature of NSE. The Auto VPN configuration involves the following tasks:

- [Creating Auto VPN groups](#)
- [Adding hubs and spokes for sites](#)

Creating Auto VPN groups

With the flexibility of configuring modes for NSE devices, you can create an Auto VPN group for:

- **All Cambium hubs:** Create an Auto VPN group by disabling the **Use non-Cambium Hub** option. For details, see [Auto VPN group for all Cambium hubs](#).
- **A non-Cambium hub:** Create an Auto VPN group by enabling the **Use non-Cambium Hub** option. For details, see [Auto VPN group for a non-Cambium hub](#).

Auto VPN group for all Cambium hubs

For a traditional Cambium-only setup, you can create auto VPN groups by disabling the **Use non-Cambium Hub** option. Complete the following steps to configure the Auto VPN group for all Cambium hubs:

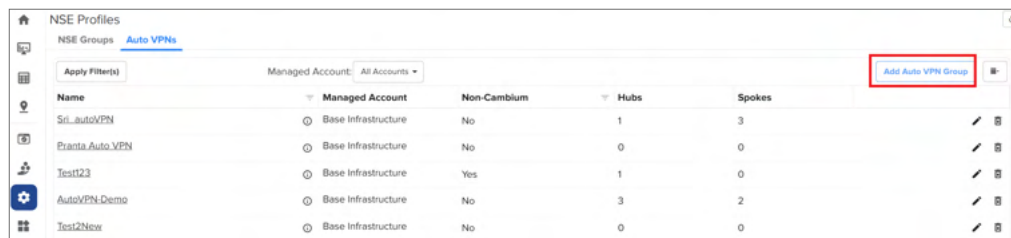
1. From the home page, navigate to **Configuration > NSE Profiles**.

The **NSE Profiles** page appears.

2. On the **NSE Profiles** page, click the **Auto VPNs** tab.

The **Auto VPNs** page appears.

Figure 456 The Auto VPN page

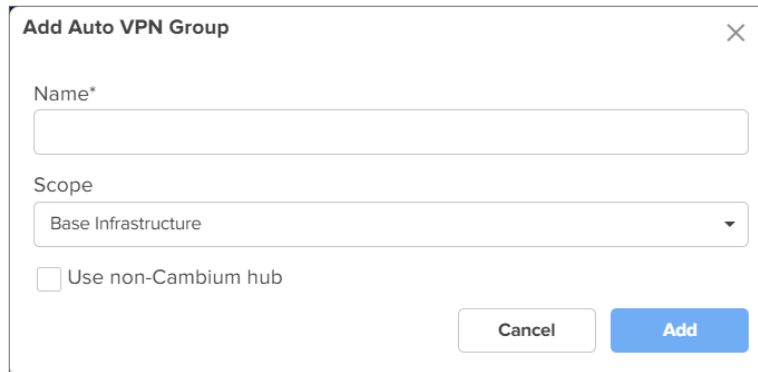


Name	Managed Account	Non-Cambium	Hubs	Spokes
Sci_AutoVPN	Base Infrastructure	No	1	3
Pranta Auto VPN	Base Infrastructure	No	0	0
Test123	Base Infrastructure	Yes	1	0
AutoVPN-Demo	Base Infrastructure	No	3	2
Test2New	Base Infrastructure	No	0	0

3. To create a new auto VPN group, click **Add Auto VPN Group**.

The **Add Auto VPN Group** window appears.

Figure 457 The Add Auto VPN Group window



Add Auto VPN Group

Name*

Scope

Base Infrastructure

☐ Use non-Cambium hub

Cancel Add

4. On the **Add Auto VPN Group** window, provide the values as described:
 - a. In the **Name** field, enter a valid name for the VPN group.
 - b. From the **Scope** dropdown list, select a name of the managed account.
 - c. To create the auto VPN group for all Cambium hubs, ensure that the **Use non-Cambium hub** checkbox is not selected.
5. Click **Add**.

The Auto VPN group for all Cambium hubs is created.

Auto VPN group for a non-Cambium hub

For a hybrid setup where a non-Cambium device serves as the hub, you must enable the **Use non-Cambium hub** option.

Complete the following steps to configure the Auto VPN group for a non-Cambium hub:

1. From the home page, navigate to **Configuration > NSE Profiles**.

The **NSE Profiles** page appears.
2. On the **NSE Profiles** page, click the **Auto VPNs** tab.

The **Auto VPNs** page appears.
3. To create a new auto VPN group, click **Add Auto VPN Group**.

The **Add Auto VPN Group** window appears.
4. On the **Add Auto VPN Group** window, perform the following steps:

- a. In the **Name** field, enter a valid name for the group.
 - b. Select the required option from the **Scope** dropdown list.
 - c. To create an auto VPN group for a non-Cambium hub, select the **Use non-Cambium hub** checkbox.
- Additional fields are displayed as shown in the figure below.

Figure 458 Additional fields specific to non-Cambium hub settings



Note

The **Address** and **PSK** fields are auto-populated.

PSK, a 12-character key, is auto-generated by cnMaestro for Cambium hubs only. This key is used as the local PSK and remote PSK for all the sites in the Auto VPN group.

- d. In the **Remote ID** field, enter an appropriate value. This is a mandatory parameter. The remote ID is the local ID of the non-cambium hub device. On creation of a hub or spoke, the local ID (generated sequentially) is assigned as local ID.
- e. Expand the **IKE Phase 1** panel.

The default configuration is displayed, as shown in [Figure 459](#).

Figure 459 Default configuration of the IKE Phase 1

- f. Using the **IKE Phase 1** panel, complete the following steps:

- i. In the **Encryption** field, select the required encryption method. By default, **aes192**, **aes192-gcm16**, **aes128-gcm16** are selected.
 - ii. In the **Integrity** field, select the required integrity method. By default, **sha256** is selected.
 - iii. In the **DH Group** field, select the required DH group option. Default value: 15.
 - iv. In the **Key Lifetime** field, enter a value. Default value: 4.
- g. Similarly, expand the **IKE Phase 2** panel and set the configuration.

The default configuration is shown in [Figure 460](#).

Figure 460 Default configuration of the IKE Phase 2

5. Click **Add**.

The Auto VPN group is created for a non-Cambium hub.

Adding hubs and spokes for sites

You must add hubs and spokes as part of the Auto VPN configuration. A site has to be linked at the time of creating a hub or a spoke. You must select a site from the list of sites and this site must have met the following criteria:

- The site should have an NSE device.
- An NSE group should be mapped to the NSE device.
- The site should not be part of any other Auto VPN group.



Note

- You must first add a hub before adding a spoke.
- You can add multiple hubs and spokes for all Cambium-hub Auto VPN groups.
- You can add multiple spokes for a non-Cambium hub Auto VPN groups.
- You can add only spokes for a non-Cambium hub Auto VPN group. Hubs cannot be added but their configuration can be updated.

This topic covers the following sections:

- [Adding a hub and a spoke for a Cambium-hub Auto VPN group](#)
- [Adding a spoke for a non-Cambium hub Auto VPN group](#)

Adding a hub and a spoke for a Cambium-hub Auto VPN group

You can add a single or multiple hubs and spokes for a Cambium-hub Auto VPN group.

Adding a hub

Complete the following steps to add a hub:

1. On the **NSE Profiles** page, click the **Auto VPNs** tab.

The Auto VPNs page appears with a list of auto VPN groups created.

Figure 461 *The Auto VPNs page*



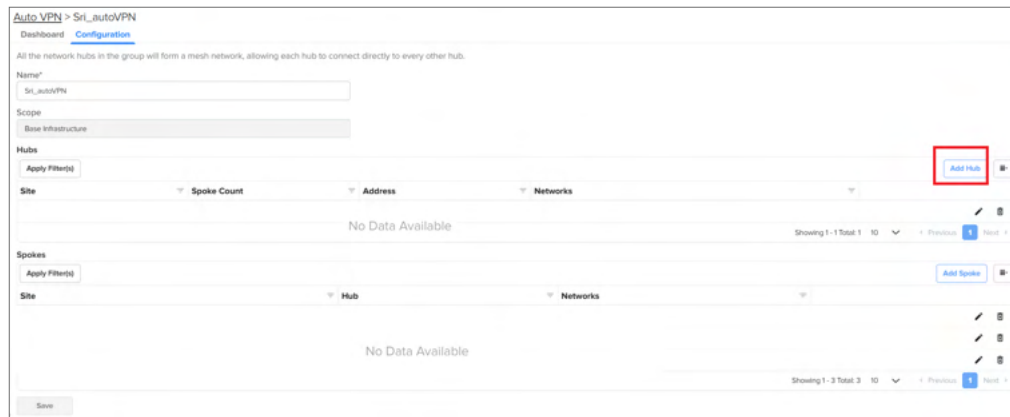
Name	Managed Account	Non-Cambium	Hubs	Spokes
Sri_autoVPN	Base Infrastructure	No	0	0
Pranta Auto_VPN	Base Infrastructure	No	0	0
Test123	Base Infrastructure	Yes	1	0
AutoVPN-Demo	Base Infrastructure	No	3	2

If the value of **Non-Cambium** field on the Auto VPN page is No, then it is a Cambium-hub Auto VPN group. Otherwise, it is a non-Cambium hub Auto VPN group (if the value of Non-Cambium is Yes).

2. Click on the required Cambium-hub Auto VPN group name.

The **Configuration** page appears for the selected auto VPN group.

Figure 462 *The Configuration page*



Auto VPN > Sri_autoVPN

Dashboard Configuration

All the network hubs in the group will form a mesh network, allowing each hub to connect directly to every other hub.

Name: Sri_autoVPN

Scope: Base Infrastructure

Hubs

Apply Filter(s)

Site	Spoke Count	Address	Networks
No Data Available			

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

Spokes

Apply Filter(s)

Site	Hub	Networks
No Data Available		

Showing 1 - 3 Total 3 10 < Previous 1 Next >

Save

3. Click **Add Hub**.

The **Add Hub** window appears.

Figure 463 *The Add Hub window*

4. To add a hub, provide the values as described:
 - a. From the **Site** dropdown list, select a site name. This is a mandatory field.

The Site dropdown list displays sites that have an NSE device and an attached NSE group.
 - b. In the **WAN Interface** field, select the required WAN option.
 - c. In the **Address** field, enter the host name or WAN IP address of the NSE 3000 device. This is a mandatory field.

This field auto-populates the value with WAN 1 or WAN 2 IPs if the static IPs are configured.
 - d. In the **Shared network over VPN** section, Click **Add New** to add VLAN IDs of required networks.

The **Add New Local Subnet** window appears. Using this window, you can add networks that the hub will advertise. You can add multiple networks.

Figure 464 *The Add New Local Subnet window*

- e. In the Add New Local Subnet window, enter a valid address in the **Local Subnets** field. The **Translated to Network/IP (optional)** field is optional. If the Local subnets have a VPN translation, then provide a VPN network address in the **Translated to Network/IP (optional)** field or it can be left blank (empty).
- f. Click **Add** on the Add New Local Subnet window.

The shared network details are added to the **Add Hub** window.

The NSE 3000 device communicates over the specified VLAN.



Note

NSE 3000 supports VPN translation. The local subnets that are advertised to peers are configured to translate into a different, equally sized subnet. This is useful in deployments where the same local subnet is used in multiple locations.

For example, the 192.168.200.0/24 network can be found in multiple locations as it is the default network configuration. If 192.168.200.0/24 is available in multiple locations, this can be configured to be translated to 10.10.10.0/24. to prevent address conflicts, The translation can also be 1 to M. In case of 1 to M, 192.168.200.0/24 can be configured to be translated to 10.10.10.10/32.

- g. Click **Add** on the Add Hub window.

A hub is added to the **Hubs** section on the **Configuration** page.

Figure 465 *The Hubs section*

Adding a spoke

Complete the following steps to add a spoke:

1. On the **NSE Profiles** page, click the **Auto VPN** tab.
The Auto VPN page appears with a list of auto VPN group created.
2. Click on the required auto VPN group name.

The **Configuration** page appears for the selected auto VPN group.

Figure 466 *The Configuration page - Add Spoke*

3. Click **Add Spoke**.

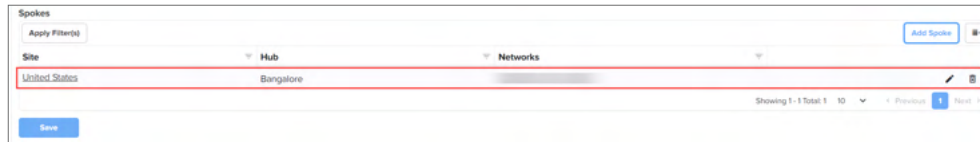
The **Add Spoke** window appears.

Figure 467 *The Add Spoke window*

4. Complete the following steps to add a spoke:
 - a. Select a site from the **Site** dropdown list. This is a mandatory field.
 - b. Select a hub from the **Hub** dropdown list. This is a mandatory field. You must select a hub to connect from the list of hubs, which are already created in the Auto VPN group.
 - c. In the **Shared network over VPN** section, Click **Add New**. The **Add New Local Subnet** window appears. Using this window, you can add networks that are local to the spoke. You can add multiple networks. If there are multiple hubs, these networks will be advertised by the hub they are connected to.
 - d. In the **Add New Local Subnet** window, enter a valid address in the **Local Subnets** field. The **Translated to Network/IP (optional)** field is optional. If the Local subnets have a VPN translation, then provide a VPN network address in the **Translated to Network/IP (optional)** field or it can be left blank (empty).
 - e. Click **Add** on the Add New Local Subnet window. The shared network details are added to the **Add Spoke** window. The NSE 3000 device communicates over the specified VLAN.
 - f. Click **Add** on the Add Spoke window.

A spoke is added to the **Spokes** section.

Figure 468 *The Spokes section*



5. Click **Save** on the Configuration page.

The figure below is an example of the **Configuration** page for a Cambium-hub Auto VPN group (after adding a hub and a spoke). You can add multiple hubs and spokes for a Cambium-hub Auto VPN group.

Figure 469 *The Configuration page for a Cambium-hub Auto VPN group*



6. Click **Save** on the Configuration page to apply the changes.
7. To view the dashboard page for the configured Auto VPN group, click on the **Dashboard** tab (located before the **Configuration** tab).

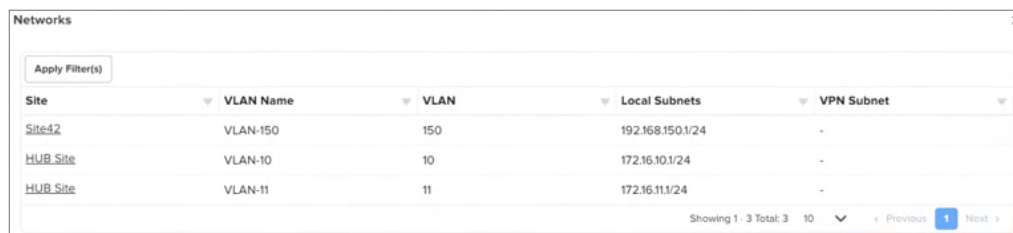
You can view the status of connection and tunnel type used by the NSE 3000 device for communication.

Figure 470 *The Dashboard page of an Auto VPN group*



8. On the **Dashboard** page, click on the ⓘ icon (next to **Tx Range**) to view the network details.

Figure 471 *The Networks page*



Adding a spoke for a non-Cambium hub Auto VPN group

You can add a single or multiple spokes for a non-Cambium hub Auto VPN group. You cannot add a hub but you can update or modify its configuration for a non-Cambium hub Auto VPN group.

Complete the following steps to add a spoke:

1. On the **NSE Profiles > Auto VPNs** page, select a non-Cambium hub Auto VPN group from the available list.
If the value of **Non-Cambium** field on the Auto VPNs page is Yes, then it is a non-Cambium hub Auto VPN group.

Figure 472 The Auto VPNs page - Non-Cambium hub

Name	Managed Account	Non-Cambium	Hubs	Spokes	
Test	NSE_AutoVPN Testin	No	0	0	
Nathan_Dennis_AutoVPN	NSE MSP	No	1	1	
MSP-Demo-AutoVPN	NSE MSP	No	0	0	
HA_Auto_VPN	NSE_AutoVPN Testin	No	0	0	
Rashin_Test_Final_Bulk_New22	Base Infrastructure	No	0	0	
Rashin_Multi_2	Base Infrastructure	Yes	1	0	
CALA-AUTOVPN	CALA_AUTOVPN	No	1	2	

2. Click on the required non-Cambium hub Auto VPN group name.
The **Configuration** page appears for the selected auto VPN group.

Figure 473 The Configuration page - Non-Cambium hub

Auto VPNs > Rashin_Multi_2

Dashboard Configuration

All the network hubs in the group will form a mesh network, allowing each hub to connect directly to every other hub.

Name* Rashin_Multi_2

Scope Base Infrastructure

Address* 172.16.8.13

Host Name or IP Address

PSK*

Remote ID* 192.168.1.1

IKE Phase 1

IKE Phase 2

Spokes

Apply Filter

Site Networks Local ID

No Data Available

Showing 0 - 0 Total 0 10 > Previous Next >

Save

The following parameters are already set at the time of creating a non-Cambium hub Auto VPN group:

- Name
- Scope
- Address
- PSK
- Remote ID
- IKE Phase 1 and IKE Phase 2

You can update or modify the hub-specific parameters except for Scope (disabled). For more information about these parameters, check [Auto VPN group for a non-Cambium hub](#).

3. To add a spoke for a non-Cambium hub Auto VPN group, click **Add Spoke** on the Configuration page.
The **Add Spoke** window appears.

Figure 474 The Add Spoke window - Non-Cambium hub

4. Complete the following steps to add a spoke:

- a. Select a site from the **Site** dropdown list. This is a mandatory field.
- b. In the **Shared network over VPN** section, Click **Add New**. The **Add New Local Subnet** window appears.

Using this window, you can add networks that are local to the spoke. You can add multiple networks. These networks will be advertised by the hub they are connected to.



Note

NSE 3000 supports VPN translation. For more information, check the note described [here](#).

- c. In the **Add New Local Subnet** window, enter a valid address in the **Local Subnets** field. The **Translated to Network/IP (optional)** field is optional. If the Local subnets have a VPN translation, then provide a VPN network address in the **Translated to Network/IP (optional)** field or it can be left blank (empty).
- d. Click **Add** on the Add New Local Subnet window. The shared network details are added to the **Add Spoke** window. The NSE 3000 device communicates over the specified VLAN.
- e. Click **Add** on the Add Spoke window.

A spoke is added to the **Spokes** section.

5. Click **Save** on the Configuration page to apply the changes.
6. To view the dashboard page for the configured Auto VPN group, click on the **Dashboard** tab (located before the **Configuration** tab).

On the **Dashboard** page, you can use the ⓘ icon (next to **Tx Range**) to view the network details.

Disabling or Enabling the Security Plus License Mode for NSE

Currently, a subscription is required to onboard and manage NSE 3000 using cnMaestro (both Essentials and X). This paid subscription license mode (with all features available) is referred to as **Security Plus**.

However, Cambium Networks also offers a flexibility to onboard and manage NSE 3000 devices using cnMaestro **without a subscription**. This subscription-free license mode is referred to as **Security**. The Security mode allows you to onboard and operate an NSE 3000 device with limited features.



Note

The Security Plus license mode is available for both cnMaestro Essentials and X. But the **Security** mode is available only for cnMaestro Essentials.

The table below lists some of the features available in the Security Plus license mode and the Security mode.

Table 99 List of feature sets available for NSE in different license modes

Feature sets available in the Security Plus license mode (Paid subscription)	Feature sets available in the Security mode (Subscription-free)
<ul style="list-style-type: none"> • Geo-IP Firewall • DNS Content Filtering <ul style="list-style-type: none"> ◦ 80+ categories ◦ Fast with data caches around the world • LAN Vulnerability Assessment • High Availability <ul style="list-style-type: none"> ◦ 1 + 1 in Active-Backup mode • Auto VPN <ul style="list-style-type: none"> ◦ One-click setup of VPN tunnels • IoT Device Identification • cnMaestro reports and analytics for DNS filtering, Geo-IP, LAN Vulnerability Assessment, and Device Identification 	<ul style="list-style-type: none"> • SD-WAN <ul style="list-style-type: none"> ◦ WAN Active-Active and Active-Backup ◦ Layer-3 and Layer-7 flow preferences • Site to Site VPNs <ul style="list-style-type: none"> ◦ IKEv1 ◦ IKEv2 • Remote VPN <ul style="list-style-type: none"> ◦ L2TP-IPSec ◦ IKEv2 ◦ WireGuard • Next-Gen Firewall <ul style="list-style-type: none"> ◦ Layer-3 and Layer-7 (Application based) • Intrusion Detection and Prevention <ul style="list-style-type: none"> ◦ Choice of free and commercial rule sets • Application Visibility and Control • LAN services (DHCP, DNS (Local Hosts), RADIUS) • cnMaestro Analytics (Dashboard, WAN performance, Client and VPN session, Application statistics, Threats, CPU, Available memory, Alarms, Alarms History, Events)

With the introduction of the new feature sets, the following three different account states are observed for NSE in cnMaestro:

1. **cnMaestro Essentials with Security:** Free subscriptions (1000 free slots) are granted for NSE devices.
2. **cnMaestro Essentials with Security Plus:** The user needs to activate Tier 30 licenses for all NSE devices.
3. **cnMaestro X with Security Plus:** The user needs to activate Tier 30 licenses for all NSE devices.

How does the Security Plus license mode work?

By default, the Security Plus license mode is enabled for NSE and all the features are available for existing and new user accounts. In this default license state, all the security features, such as Geo-IP firewall, DNS content filtering, high availability, LAN vulnerability assessment, device identification, device fingerprinting, and cnMaestro reports are enabled.

Using cnMaestro Essentials, you can disable the Security Plus mode and switch to the Security mode (subscription-free). You can also switch back (enable) to the Security Plus mode. For details, refer to [Disabling the Security Plus mode](#) and [Enabling the Security Plus mode](#).

How does the Security (subscription-free) mode work?

The subscription model for NSE devices remains unchanged but cnMaestro grants a free subscription if the user chooses to use only the Security mode in cnMaestro Essentials.

To switch to the Security mode, an account-level setting is required in the cnMaestro UI. When you select between Security and Security Plus modes, cnMaestro verifies before changing the mode and throws an error if any of the criteria fails.

On changing to the Security mode, cnMaestro activates 1000 (configurable) Tier 30 free slots with a rotating validity period (after which cnMaestro resets to a future date before a slot reaches its expiry). These free slots cannot be transferred to X unlike the regular Tier 30 slots.

When the Security mode is enabled, cnMaestro automatically disables all features that are supported in the Security Plus mode. For information on how to enable the Security mode, refer to [Disabling the Security Plus mode](#).



Note

If an account running in the Security mode (earlier) is upgraded to X, then cnMaestro automatically toggles it to the Security Plus mode.

How to switch back to Security Plus mode?

To switch back to (enable) the Security Plus mode, an account-level setting is required in the cnMaestro UI. However, the users should have activated sufficient number of Tier 30 licenses to meet their NSE device count (as a prerequisite task). On changing to the Security Plus mode, cnMaestro deactivates the grant (free subscription) and all features are available in this mode (by default). For information on how to switch back to the Security Plus mode in cnMaestro, refer to [Enabling the Security Plus mode](#).



Note

Fresh accounts are initialized with Essentials and Security Plus. That is, the user needs to activate Tier 30 licenses to manage an NSE device.

How do license modes work during a manual or automatic downgrade from X?

Automatic downgrade happens when all activated subscriptions (licenses) expire for the X account.

When automatically downgraded from X, the Security Plus mode is continued in Essentials and any devices without valid licenses are marked as expired. If you want to use the Security license mode, you must disable the Security Plus mode using the **Administration > Settings > General** page in cnMaestro UI. For details, refer to [Disabling the Security Plus mode](#).



Note

Switching to Security mode will automatically reactivate the expired devices.

A manual downgrade from X is possible under the following three conditions for NSE:

- If all required Tier 30 subscriptions are available, then the Security Plus mode can be continued in Essentials.
- If partial Tier 30 subscriptions are available, then cnMaestro continues in the Security Plus mode and devices without valid Tier 30 licenses are marked as expired.
- If no Tier 30 Subscriptions are available, then cnMaestro follows the automatic downgrade path.

Disabling the Security Plus mode

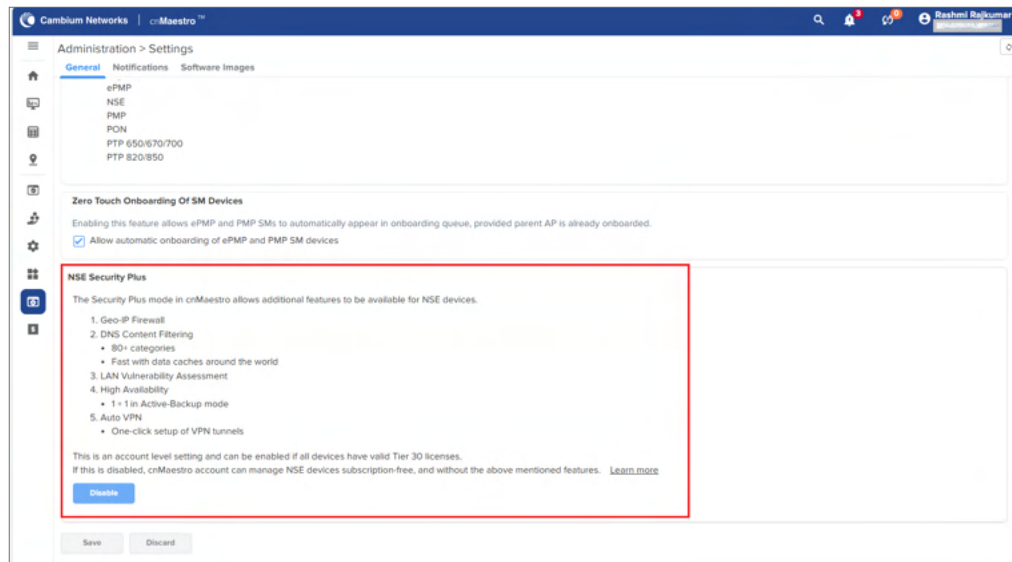
When you disable the Security Plus mode for NSE using cnMaestro Essentials, the Security mode (subscription-free) is enabled. Complete the following steps to disable the Security Plus mode:

1. Log in to cnMaestro Essentials using appropriate username and password.
2. From the home page, navigate to **Administration > Settings**. The **Settings** page appears with the following tabs: General, Notifications, and Software Images. By default, the **General** tab is selected.

The General page displays Time zone, Account view, Zero Touch Onboarding, and NSE Security Plus settings (default state).

3. On the **General** page, go to the **NSE Security Plus** section.

Figure 475 The NSE Security Plus section

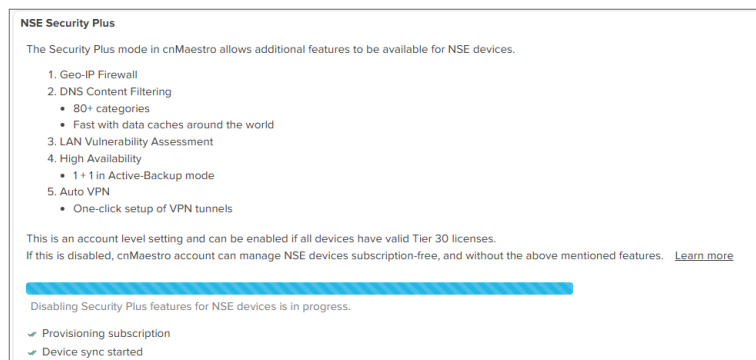


By default, the Security Plus mode is enabled for the NSE devices. In the NSE Security Plus section (as shown in [Figure 1](#)), you can view the details of features enabled.

4. To disable the Security Plus mode, click the **Disable** button.

The process begins, indicating the subscription provisioning and device sync as shown in [Figure 2](#).

Figure 476 Process of disabling the Security Plus mode

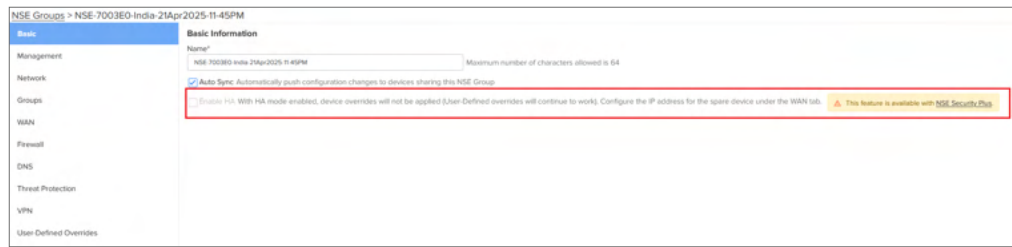


The **Security** license mode is enabled now. You can proceed with configuration of the related features on the **NSE Groups** page. For example, WAN and LAN services. Check [Table 99](#) for the list of feature sets available in the Security mode (subscription-free).

When the Security mode is enabled, the unsupported features are disabled in the cnMaestro UI. Feature-level messages are displayed on the UI as part of the configuration for the NSE device.

Based on the account level mode selection, the cnMaestro UI turns off (disable) and turns on (enable) the related features. For example, if you select the **Basic** tab on the NSE Groups page, a feature level message is visible, indicating that the high availability (HA) configuration is available only with the Security Plus mode. In addition, the HA configuration checkbox is disabled and provides an option (link) to enable the Security Plus mode (as shown in [Figure 3](#)).

Figure 477 Example of a feature-level message



Similarly, you can find such feature-level messages for specific configurations on **Firewall** and **DNS** pages for the Security mode. In addition, Vulnerabilities is not available at all levels, and Auto VPN, GEO IP Firewall, and DNS Content Filtering are also unavailable.

5. Configure the required features available in the Security mode.

cnMaestro grants 1000 free slots, which you can use to onboard and manage the NSE devices. To view the summary of grant, check the **Manage Subscriptions** page. [Figure 4](#) is an example of a grant summary, showing that one slot is used, and 1099 free slots are available for NSE devices. These free slots can be used to onboard and manage the NSE devices in cnMaestro.

Figure 478 Viewing the grant summary on the Manage Subscriptions page

The screenshot shows the 'Manage Subscriptions' page. It includes a 'Usage Summary' section with a bar chart and a table of subscriptions. The table has columns for Name, Type, Device Tier, Slots Used, Quantity, Status, Start Date, End Date, Validity, and Commercial ID. The first row shows a 'Grant' subscription for 'Tier 30' with 1000 slots used and 1000 quantity. The second row shows a 'Terminated' subscription for 'Tier 30' with 1000 slots used and 1000 quantity. The third row shows a 'New' subscription for 'Tier 30' with 100 slots used and 100 quantity. The table also shows a 'Showing 1 of 4 Total' and a '1' button.

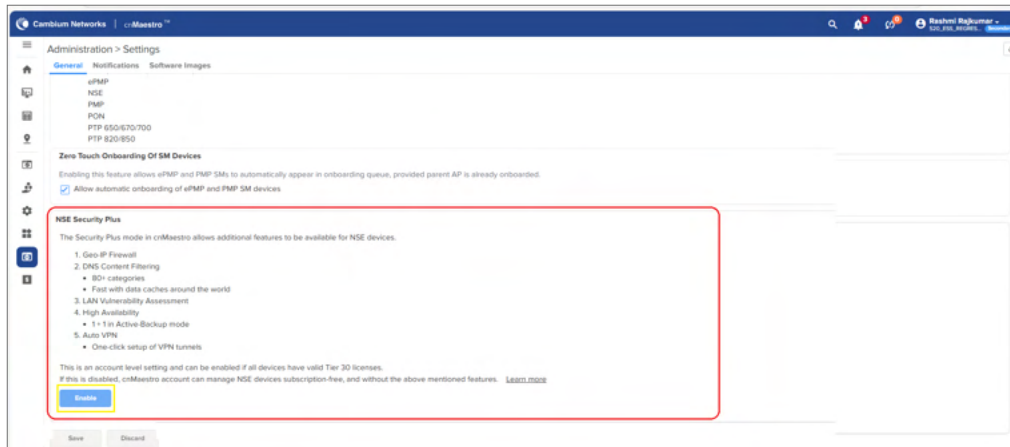
Enabling the Security Plus mode

You have an option to enable or switch back to the Security Plus mode in cnMaestro. With this action, the Security mode is disabled and all features (available in the Security Plus mode) are enabled automatically.

To switch back to or enable the Security Plus mode, complete the following steps:

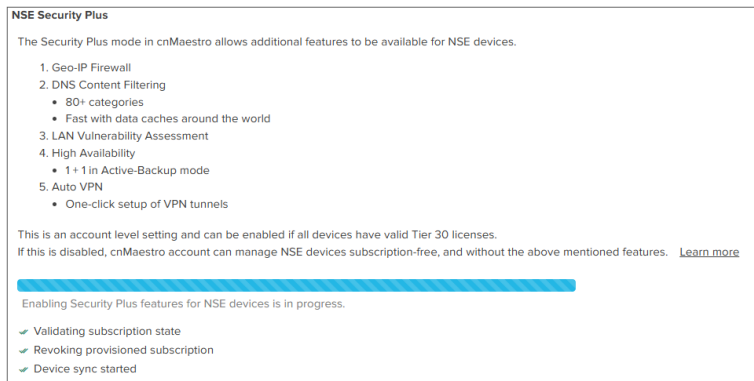
1. From the home page of cnMaestro Essentials, navigate to **Administration** > **Settings**. By default, the General tab is selected.
2. On the **General** page, go to the NSE Security Plus section.

Figure 479 The NSE Security Plus section with the Enable button



3. To enable the Security Plus mode, click the **Enable** button in the NSE Security Plus section.
The process of enabling the Security Plus mode begins, as shown in [Figure 6](#).

Figure 480 Enabling the Security Plus mode - cnMaestro Essentials



4. Click **Save** to apply the change when the process is complete.

You have now enabled the Security Plus mode for the NSE devices. With this action, all features, such as high availability, firewall settings, vulnerabilities, and Auto VPN, are enabled in the cnMaestro UI.

Configuring Advanced Features

To configure advanced features, navigate to **Configuration > Advanced Features** page.

Advanced Features

Enterprise

☒ Lock NSE/cnMatrix/Wi-Fi AP Device Configuration **X** Changes made outside (such as through the Device UI) of a mapped configuration group (NSE, Switch & Wi-Fi AP Groups) will be overwritten.

☐ Enable Strict Device Password Policy Store device administrator passwords as one-way hashes in NSE Groups, Switch Groups and Enterprise AP Groups (XE/XV/X7-Series).

ⓘ Do not enable this setting if you manage cnPilot E-Series devices (these do not support hashed administrator passwords, so enabling this will prevent configuration updates to them).

ⓘ You must update administrator passwords on your NSE Groups, Switch Groups and Enterprise AP Groups for this setting to take effect.

Save

Lock Device Configuration

To lock NSE, cnMatrix, and Wi-Fi device configuration, select the checkbox. Once you enable this checkbox, you cannot update the device-level configuration using the device UI or any other method. Only the configuration pushed from cnMaestro for NSE, switch, and Wi-Fi AP groups will be retained on the device.

Strict Device Password Policy

To enable strict password policy for Switch Groups or Enterprise AP Groups, select the **Enable Strict Device Password Policy** checkbox.

If you enable this option:

- The device administrator passwords are stored as one-way hashes for all NSE Groups, Switch Groups, and Enterprise AP Groups (XE/XV/X7-series).
- The administrator password has to be updated for all NSE Groups, Switch Groups, and Enterprise AP Groups under **Configuration > NSE Group > Management** page, **Configuration > Switch Group > Management** page, and **Configuration > Wi-Fi Profiles > AP Group > Management** page respectively for this setting to take effect.
- The configuration cannot be pushed to cnPilot E-series device.
- Device software versions must be at or above 1.3 for NSE, 4.6.1 for cnMatrix, and 6.5.3 for Enterprise Wi-Fi XE/XV/X7-Series to support the strict password policy. cnMaestro will not push any configuration to devices not meeting these requirements, including all cnPilot E-Series devices when the strict policy is enabled.

If you disable this option:

- The password must be updated for all NSE Groups, Switch Groups, and Enterprise AP Groups under the respective **Management** pages for this setting to take effect.

Auto-Provisioning

cnMaestro supports Auto-Provisioning for cnVision, Wireless LAN devices (Enterprise Wi-Fi, cnPilot R-Series, and Xirrus) and fixed devices (PMP and ePMP). It allows the user to automatically configure and approve devices based upon IP address.

Creating Auto-Provisioning Rule











To create a rule for Auto-Provisioning, perform the following steps:

1. Navigate to **Configuration > Auto-Provisioning** page.

Configuration > Auto-Provisioning x

Automatically configure devices based upon its source subnet. Approved devices will automatically be configured and onboarded. Unapproved devices will be added to the Onboarding Queue and must be manually approved prior to onboarding. [Learn more](#)

[Add New](#)

Subnet (CIDR)	Device Type	Managed Account	Network	Site/Tower	Profile/Template	Description	Approve	
10.110.224.0/24	cnPilot Home (R-Series)	NBN_MSP1	Network2	Home_site222	CNM_SIT_R-SE...	AUTO+PROV-R...	true	 
10.110.12/24	cnPilot Home (R-Series)	Base Infrastructure	default	-	R-Series_temp...	-	false	 
10.110.11/24	cnPilot Home (R-Series)	Base Infrastructure	default	-	-	-	false	 
10.110.13/24	cnPilot Home (R-Series)	Base Infrastructure	default	-	-	-	false	 
10.110.209.0/24	cnPilot Home (R-Series)	Base Infrastructure	default	home_site_defa...	CNM_SIT_R-SE...	-	true	 

[Save](#)

2. Click **Add New** and following window appears.

Figure 481 Auto-Provisioning for cnPilot Home (R-Series) devices

Add Auto-Provisioning Rules x

Subnet (CIDR) ⓘ
xxx.xxx.xxx.xxx/xx

Device Type
cnPilot Home (R-Series) ▼

Managed Account
Base Infrastructure ▼

Network
default ▼

Site
None ▼

Configuration Method
☒ AP Group ☐ Template

AP Group
None ▼

Description

☐ Approve

[Cancel](#) [Add](#)

Figure 482 Auto-Provisioning for all other devices

The screenshot shows a dialog box titled "Add Auto-Provisioning Rules". It contains the following fields and options:

- Subnet (CIDR):** A text input field with a placeholder "xxx.xxx.xxx.xxx/xx".
- Device Type:** A dropdown menu with "ePMP" selected.
- Managed Account:** A dropdown menu with "Base Infrastructure" selected.
- Network:** A dropdown menu with "default" selected.
- Tower:** A dropdown menu with "None" selected.
- Template:** A dropdown menu with "None" selected.
- Description:** A text input field.
- Approve:** A checkbox.
- Buttons:** "Cancel" and "Add" buttons at the bottom right.

3. Enter the following details:

- **Subnet (CIDR):** The subnet with CIDR of the devices to which the rule has to be applied.
- **Device Type:** Select the rule to be created for Enterprise Wi-Fi, Enterprise Wi-Fi (Xirrus-Series), cnVision, cnPilot Home (R-Series), ePMP, and PMP devices.
- **Managed Account:** Select the Managed Account from the list.
- **Network:** To which network the device should be onboarded, once device contacts the server.
- **Site:** Site under which the device must be onboarded, once device contacts the server.
Applicable for Enterprise Wi-Fi, Enterprise Wi-Fi (Xirrus-Series), and cnPilot Home (R-Series) devices.
- **Tower:** Site under which the device must be onboarded, once device contacts the server.
Applicable for ePMP AP, PMP AP, and cnVision devices.
- **Template:** Template to be applied on the device when onboarding, once device contacts the server.
Applicable for ePMP AP, PMP AP, cnVision, and cnPilot Home (R-Series).
- **AP Group:** AP Group to be applied on the device when onboarding, once device contacts the server.
Applicable for Enterprise (E-, XE-, XV-, and X7-Series), Xirrus, and cnPilot Home (R-Series).
- **Description:** Brief information about the device.
- **Approve:** Indicates whether the device is auto-approved or must be manual approved when onboarding.

4. Click **Add**.

Managing Home Mesh Router

The Home Mesh Router is engineered to provide superior Wi-Fi performance and mesh networking capabilities. It incorporates the advanced 802.11ax technology, ensuring it is fully compatible with a wide range of consumer devices while offering low latency and high throughput. These routers are specifically designed for comprehensive home coverage, supporting simultaneous operation on both 2.4 GHz and 5 GHz bands. This enables extended range, enhanced efficiency, and reduced interference compared to previous generations of Wi-Fi technology.

Additionally, the routers are configured to work in tandem, creating a seamless mesh network that covers the entire home, effectively eliminating areas with weak or no Wi-Fi signal.

The Home Mesh Routers can be configured using cnMaestro Cloud and the cnMaestro Subscriber application.

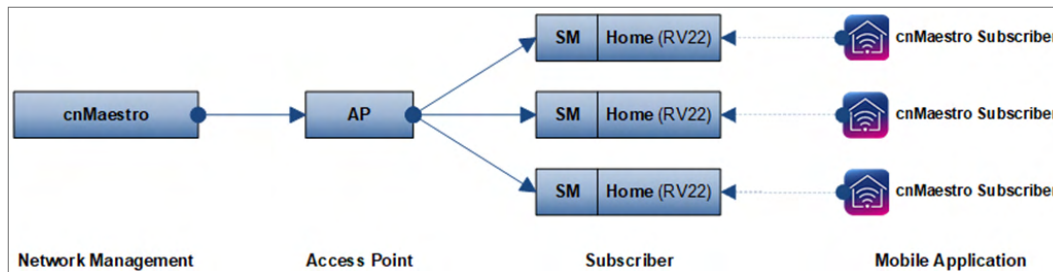
For information on supported platforms and hardware overview, see *Home Mesh Router User Guide*.



Warning

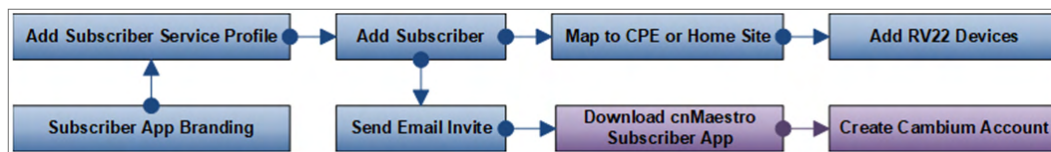
The WAN port of the Home Mesh Router may be damaged if a 48 VDC passive power (passive POE) is connected to the WAN port.

The basic architecture of the Home Mesh Router is as shown below.



The cnMaestro Subscriber application allows home customers to manage RV22 devices using their mobile phones. In the graphic above, the Subscriber is demarcated by the SM CPE. Alternatively, it could be mapped to a PON ONU, or to no explicit backhaul at all. In the latter case, the Subscriber would be attached to a new cnMaestro Home Site.

The workflow for creating and onboarding Subscribers, so customers can use the mobile application, has a cnMaestro (blue) and a customer (purple) component, as shown below.



A Subscriber is configured in cnMaestro Cloud, and an invite is sent to the customer's email address, which will enable home Wi-Fi management using the mobile application. The customer must download the cnMaestro Subscriber application from the Apple App store or Google Play Store. The "Site" in the application, which maps to the Subscriber, can be customized and branded.

Feature	Details
Onboarding	Supported using Cambium ID or Serial Number (MSN).
Dashboard	Dashboards tailored for Home Site and RV22 Home Mesh.
Configuration	Available through RV22 Home Mesh AP Groups.
Details	Overview and network information display.
Notifications	Alarms, AP Events, and Wi-Fi Events aggregated at System, Managed Account, Network, Site, and Device levels.
Performance	WAN Throughput, Wireless Throughput (downlink/uplink), Clients by Band, Noise Floor, Interference, and Airtime (2.4/5 GHz) performance graphs.
Statistics	System, Managed Service, and Network statistics available.
Software Update	Software update provided at System, Managed Account, Network, Site, and Device levels.

Feature	Details
Maps	Location of Home Sites and Devices.
Clients	Both Wired and Wireless Clients supported at Site and Device levels.
Tools	Status, Debug, Network Connectivity, Wi-Fi Analyzer, Speed Test, and Packet Capture tools available.
Reports	Data Reports downloaded from the System, Managed Service, Network, and Site levels.

This topic contains the following sections:

- [Configuring Home Mesh Router](#)
- [Viewing router system information and network traffic status](#)
- [Viewing, editing, and blocking connected clients](#)
- [Monitoring and troubleshooting the Home Mesh Router](#)

Configuring Home Mesh Router

Before shipping the Home Mesh Routers to the subscribers, they must be configured with AP groups, Wi-Fi profiles, and associated with the corresponding subscriber.

Configuring the routers involves the following steps:

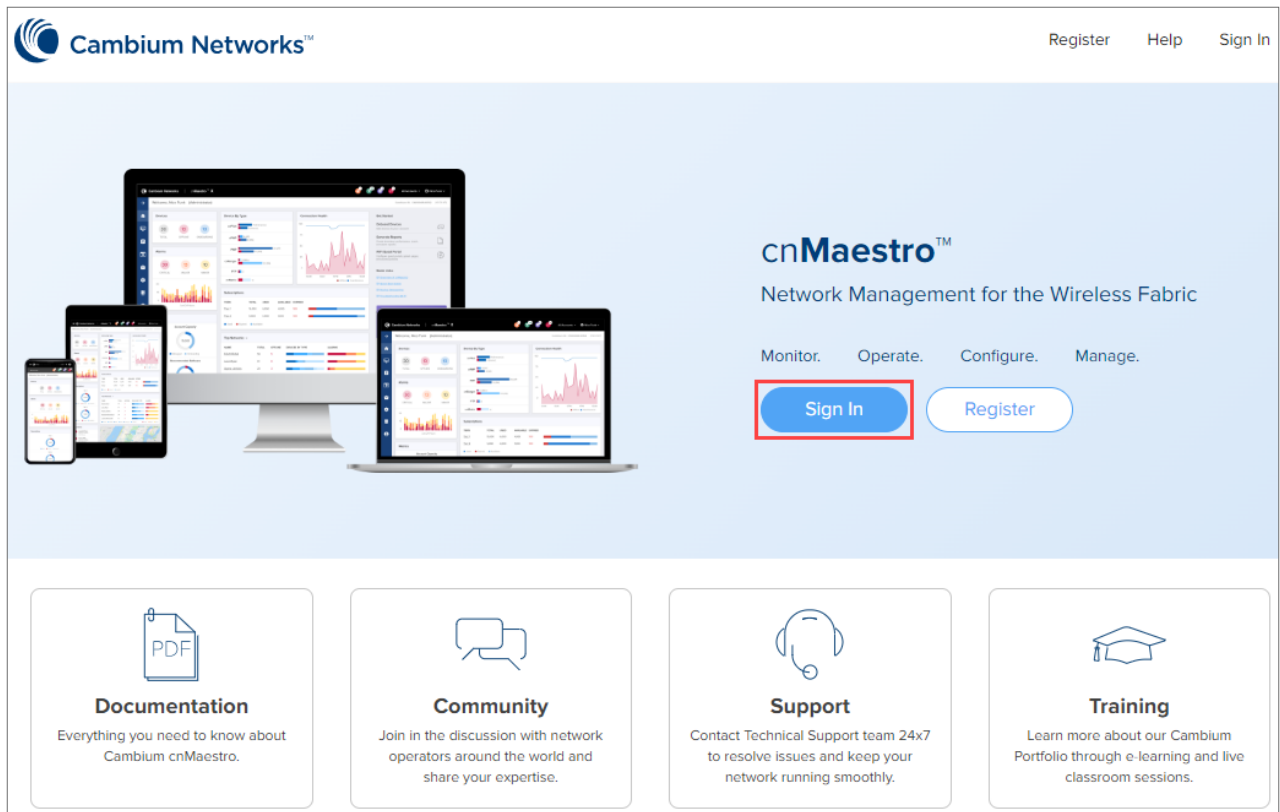
1. [Configuring WLAN profiles \(SSIDs\)](#)
2. [Configuring AP Groups](#)
3. [Onboarding the Home Mesh Router to cnMaestro](#)
 - a. [cnMaestro Subscriber application branding](#)
 - b. [Adding a Subscriber Service Profile](#)
 - c. [Adding a subscriber](#)
 - d. [Claiming the Home Mesh Router](#)

Configuring WLAN Profiles (SSIDs)

WLANs allow you to configure home and guest access SSIDs for the Home Mesh Router. This WLAN profile is associated with an AP group that contains configuration applied on the Home Mesh Routers. These SSIDs act as default SSIDs on all routers associated with the AP group.

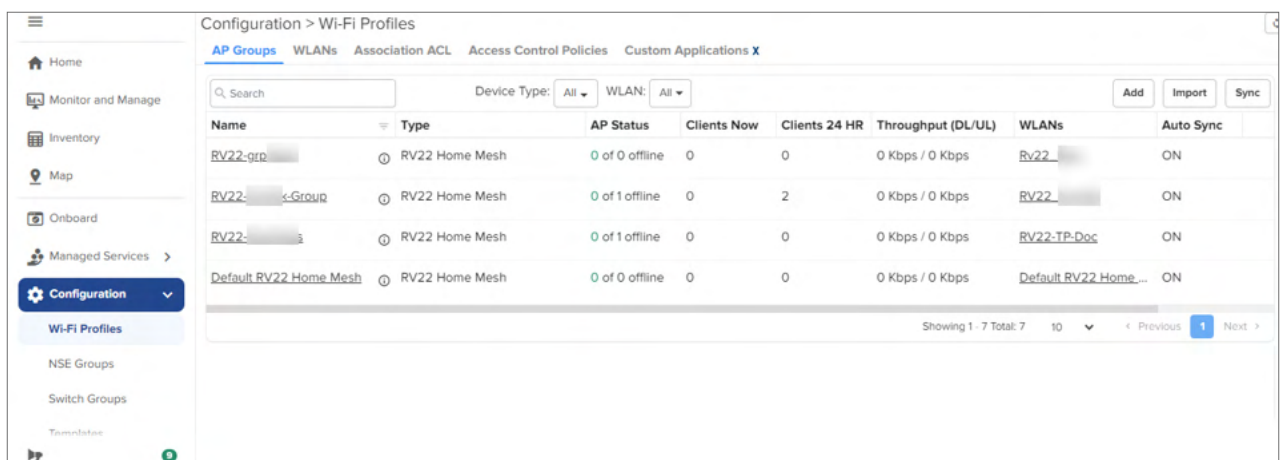
To configure a WLAN profile, complete the following steps:

1. Sign in to cnMaestro.
The home page appears.



2. Navigate to **Configuration > Wi-Fi Profiles**.

The **AP Groups** page under **Wi-Fi Profiles** appears, by default.



3. Click the **WLANs** tab.

The **WLANs** page appears.

Home

Monitor and Manage

Inventory

Map

Onboard

Managed Services

Configuration

Wi-Fi Profiles

NSE Groups

Configuration > Wi-Fi Profiles

AP Groups

WLANs

Association ACL

Access Control Policies

Custom Applications

Q Search

Device Type: All

AddImportSync

Name	Type	AP Status	Clients Now	Clients 24 HR	Throughput (DL/UL)	
	RV22 Home Mesh	0 of 0 offline	0	0	0 Kbps / 0 Kbps	
	RV22 Home Mesh	0 of 0 offline	0	0	0 Kbps / 0 Kbps	
RV22-TP-Doc	RV22 Home Mesh	0 of 1 offline	0	0	0 Kbps / 0 Kbps	
Default RV22 Home Mesh	RV22 Home Mesh	0 of 0 offline	0	0	0 Kbps / 0 Kbps	

4. Click **Add**.

The **WLANs > Add New** window appears.

In the **WLANs > Add New** window, configure the WLAN parameters as described in [Table 100](#).

WLANs > Add New

WLAN ⓘ

Basic Information

Type*
RV22 Home Mesh

Name*

Scope*

Shared scope means the AP Group is accessible to all Managed Accounts

Description

SSIDs

Home Access

SSID*

The SSID of this WLAN (up to 32 characters)

Security*
WPA2 Pre-Shared Key (AES, CCM)

Password*

Show

WPA2 Pre-shared security passphrase or key

Guest Access

Enable Guest Access

SSID

The SSID of this WLAN (up to 32 characters)

Passphrase

Show



Band Steering

Steering clients connectivity to 5 GHz band

Save

Close

Table 100 *WLAN parameters*

Parameter	Description
Basic Information	
Type	Type of device for which the WLAN profile is configured. Select RV22 Home Mesh from the dropdown list.
Name	Name of the WLAN profile.
Scope	<p>Specifies the availability of the WLAN profile across managed accounts.</p> <p>The following values are supported:</p> <ul style="list-style-type: none"> • Base Infrastructure—The WLAN profile is available only for the global account. It is not shared with other managed accounts. • Shared—The WLAN profile 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—The WLAN profile is available only for that specific managed account. <div>  <div> Note When the scope is configured for a WLAN profile, it cannot be modified. </div> </div>
Description	Brief description for the WLAN profile.
SSIDs—Home Access	
Configure the default SSID for connecting devices wirelessly. Only one home SSID can be configured.	
SSID	<p>Unique name of the SSID for this WLAN.</p> <p>Supports a maximum of 32 characters.</p> <p>You must either configure the default SSID or enter a customized SSID.</p> <p>The default SSID: RV22_<last 6 digits of device MAC>. For example, RV22_123456.</p>
Security	<p>Security method used for encryption.</p> <p>The following security methods are supported:</p> <ul style="list-style-type: none"> • Open • WPA Pre-Shared Key (AES, CCM) • WPA2 Pre-Shared Keys (AES, CCM) • WPA/WPA2 Pre-Shared Keys (TKIP, AES) • WPA Pre-Shared Key (TKIP, AES) <p>Default: WPA2 Pre-Shared Keys (AES, CCM)</p> <div>  <div> Note If you select Open, you must disable 802.11r roaming under AP Groups > Radio configuration. </div> </div>
Password	Security passphrase or key used to connect to this SSID.

Parameter	Description
	You must either configure the default password or enter a customized password. Default password: password
SSIDs—Guest Access Configure the guest SSID to allow any guest devices to access the wireless network.	
Enable Guest Access	Determines whether the guest access is enabled. Select the checkbox to enable guesst access.
SSID	Unique name of the guest SSID for this WLAN. Supports a maximum of 32 characters.
Password	Security passphrase or key used to connect to this guest SSID.
Band Steering	Determines whether the band steering is enabled for the wireless clients. When enabled, APs steer wireless clients to connect to the 5 GHz band.

5. Click **Save**.

Configuring AP Groups

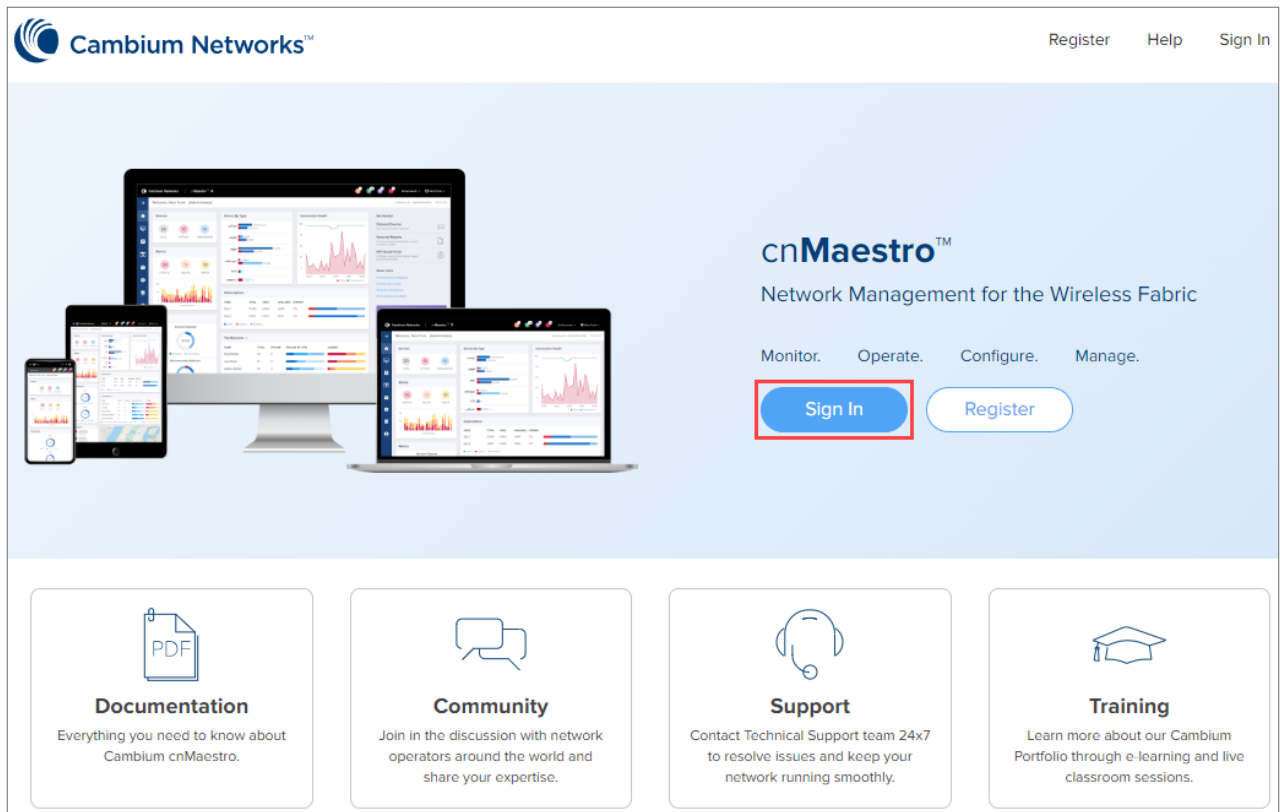
AP groups apply the same configuration to multiple Home Mesh Routers. AP groups contain configuration, such as administrator password, event logging, radio settings, WAN mappings, and DNS mode.

The following are part of the AP group:

- **Basic**
- **Management**
 - Administrator Access
 - Time Settings
 - Event Logging
 - SNMP
- **Radio**
- **Network**
 - WAN Configuration
 - LAN Configuration
- **Security**
 - DoS Protection
 - Access Control List (ACL)

To configure an AP group, complete the following steps:

1. Sign in to cnMaestro.
The home page appears.



2. Navigate to **Configuration > Wi-Fi Profiles**.

The **AP Groups** page under **Wi-Fi Profiles** appears, by default.

Name	Type	AP Status	Clients Now	Clients 24 HR	Throughput (DL/UL)	WLANs	Auto Sync
RV22-grp	RV22 Home Mesh	0 of 0 offline	0	0	0 Kbps / 0 Kbps	RV22_...	ON
RV22-...-Group	RV22 Home Mesh	0 of 1 offline	0	2	0 Kbps / 0 Kbps	RV22_...	ON
RV22-...	RV22 Home Mesh	0 of 1 offline	0	0	0 Kbps / 0 Kbps	RV22-TP-Doc	ON
Default RV22 Home Mesh	RV22 Home Mesh	0 of 0 offline	0	0	0 Kbps / 0 Kbps	Default RV22 Home...	ON

3. Click **Add**.

The **Add New** window appears with multiple tabs. By default, the **Basic** tab is selected.

4. In the **Add New** window > **Basic** tab, select **RV22 Home Mesh** in the **Type** dropdown list and configure the parameters described in [Table 101](#).

AP Groups > Add New

Basic

Management

Radio

Network

Security

Type

RV22 Home Mesh

Name*

Scope*

☒ Auto sync
 Automatically push configuration changes to devices sharing this AP Group

Country*

United States

☒ LED
 Whether the device LEDs should be ON during operation

Description


WLAN*



+

Save

Close

Table 101 Basic parameters

Parameter	Description
Type	Type of device for which the AP group is configured. Select RV22 Home Mesh from the dropdown list.
Name	Hostname of the device. Supports a maximum of 64 characters.
Scope	Specifies the availability of the AP group across managed accounts. The following values are supported: <ul style="list-style-type: none"> Base Infrastructure—AP group is available only for the global account. It is not shared with other managed accounts. Shared—AP group 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—AP group is available only for that specific managed account. <div>  <div> Note When the scope is configured for an AP group, it cannot be modified. </div> </div>
Auto sync	Specifies whether configuration is applied to the router automatically after saving. Select the checkbox to enable auto sync of configuration.
Country	Country from where the device is operated. This parameter must be configured only by the administrator. 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).

Parameter	Description
	 Note Radios remain disabled unless this parameter is configured.
LED	When enabled, turns on the device LEDs during operation.
Description	Brief description for the AP group.
WLAN	WLAN profile to be associated with this AP group. WLAN profile contains SSID details of the wireless network. Select the WLAN from the dropdown list. If no WLAN is configured, create one by clicking the add () icon. For more information, See Configuring WLAN profiles (SSIDs) .

- Click the **Management** tab on the left pane and configure the parameters described in [Table 102](#).

AP Groups > Add New

Basic
Management
Radio
Network
Security

Administrator Access

Admin Password* Configure password for authentication of GUI and CLI sessions (max 32 characters)

☐ Remote Management Access Enable remote access through WAN Interface

☐ SSH Enable SSH access to the device CLI

☐ HTTP Enable HTTP access to the device GUI

HTTP Port Port for HTTP access to the device GUI (1-65535)

☐ HTTPS Enable HTTPS access to the device GUI

HTTPS Port Port for HTTPS access to the device GUI (1-65535)

☐ Disable Hardware Reset Button When enabled the physical hardware reset button will not let the user to do factory-reset the device

Time Settings

Event Logging

SNMP

Save Close

Table 102 *Management parameters*

Parameter	Description
Administrator Access	
Admin Password	Password required for authentication of the router.
Disable Hardware Reset Button	Determines whether the reset button on the router is required to prevent a factory reset operation of the router. Select the checkbox to prevent the user from performing the factory reset operation.
Time Settings	


Parameter	Description
Time Zone	Time zone of the location where the router is installed. Select an appropriate time zone from the dropdown list.
NTP Server 1	Hostname or IPv4 address of the Network Time Protocol (NTP) server.
NTP Server 2	Hostname or IPv4 address of a second NTP server.
Event Logging	
Syslog Server	Hostname, IPv4, or IPv6 address of the Syslog server and the respective port number. Default port number: 514
Syslog Severity	The severity level of event that must be forwarded to the server. The supported severity levels (0-7) are based on RFC standards.
SNMP	
Enable	Determines whether SNMPv2c or SNMPv3 support on the router is enabled. Select the checkbox to enable SNMP support.
Trap Receiver IP	IPv4 address of the SNMP server to receive the SNMP traps. This parameter is applicable to both SNMP v2c and v3 versions.
Version	Specifies the SNMP version configured for the router. The following options are available: <ul style="list-style-type: none"> v2c v3
SNMPv2c	
SNMPv2c RO community	The SNMP v2c read-only community string used as a password when obtaining information from the router.
SNMPv2c RW community	The SNMP v2c read-write community string as a password when writing information to the router.
SNMPv3	
SNMPv3 Username	Username for the SNMPv3 server. Supports a maximum of 32 characters.
Enable Authentication	Indicates whether authentication is enabled for SNMP communication. Select the checkbox to enable authentication.
Authentication Protocol	Specifies the authentication protocol. The following options are available: <ul style="list-style-type: none"> MD5 SHA Cambium uses SHA-1 authentication protocol. By default, the SHA option is selected.
Authentication Password	Password used for authentication. Supports 8 to 32 characters.
Enable Encryption	Indicates whether encryption is enabled for SNMP communication.

Parameter	Description
	Select the checkbox to enable encryption.
Encryption Type	Specifies the encryption type. The following options are available: <ul style="list-style-type: none"> • AES • DES By default, the AES option is selected.
Encryption Password	Password used for encryption. Supports 8 to 32 characters.

6. Click the **Radio** tab on the left pane and configure the preferred radios (2.4 GHz or 5 GHz or both).
By default, both the radios are enabled. You can disable only the 2.4 GHz radio.
Configure the parameters (described in [Table 103](#)), which are similar across 2.4 and 5 GHz radios.

Table 103 *Radio parameters*

Parameter	Description
Enable	Enables the operation of radio.
Channel	This parameter cannot be modified. Specifies the 2.4 GHz channel that is used. Default: Auto
Auto Channel Frequency Coordination	Enable to prevent router from self-interference with upline wireless network infrastructure.
Channel Width	Operating channel width of the selected radio. Following channel widths are supported:

Parameter	Description
	<ul style="list-style-type: none"> For 2.4 GHz—20 MHz and 40 MHz. Default: 20 MHz For 5 GHz—20 MHz, 40 MHz, 80 MHz, and 160 MHz. Default: 80 MHz
Transmit Power	<p>Transmit power of the router in percentage (%).</p> <p>The following options are available:</p> <ul style="list-style-type: none"> Auto 20 40 60 80 100
802.11r	<p>Enables the 802.11r Fast Transition (FT) mechanism for faster roaming between Home Mesh routers in a network.</p> <div>  <div> <p>Note</p> <p>Disable 802.11r roaming when the WLAN security is configured as Open under WLANs > Home Access > SSID.</p> </div> </div>
Candidate Channels	<p>This parameter is applicable only to 5 GHz radio.</p> <p>Configures whether all channels in the 5 GHz band are used or not.</p> <p>Following are the supported values:</p> <ul style="list-style-type: none"> All—Includes all channels supported in the 5 GHz band. Prefer Non-DFS—Excludes the DFS channels (radar channels) and includes only the non-DFS channels.

- Click the **Network** tab on the left pane and configure the WAN mode and IP address assignment parameters.

AP Groups > Add New

Basic
Management
Radio
Network
Security

AP Mode
☒ Router ☐ Bridge

WAN Configuration

WAN Mode
☒ DHCP ☐ PPPoE ☐ Static

LAN Configuration

☒ IPv4

☒ Auto ☐ Manual

Local IP Address*

Local Subnet

Address Range Start*

Address Range End*

Domain Name

DNS Mode*

- The **AP Mode** is pre-configured as **Router** and cannot be modified.
- In the **WAN Configuration** section, select the required WAN mode and configure the corresponding parameters.

This mode selects the mode of IP address assignment for the WAN interface. The following WAN modes are supported:

- **DHCP**—This mode is selected by default.
No additional parameter configuration is required.
- **PPPoE**—Configure the PPPoE parameters as described in [Table 104](#).

AP Groups > Add New

Basic
Management
Radio
Network
Security

AP Mode
☒ Router ☐ Bridge

WAN Configuration

WAN Mode
☐ DHCP ☒ PPPoE ☐ Static

Service Name

Configure PPPoE service name parameters (max 32 characters)

Username*

Password*
 Show

☐ Passthrough

PPP Connection Trigger
☒ Auto Connect ☐ On Demand

Idle Timeout
 Seconds

MTU

Table 104 WAN Mode: PPPoE parameters

Parameter	Description
PPPoE-related parameters	
Service Name	Name of the PPPoE service name. Supports a maximum of 32 characters.
Username	Username of the PPPoE service required for authentication.
Password	Password of the PPPoE service required for authentication.
Passthrough	Indicates whether the clients must directly establish connection with the service provider. Select the checkbox to enable passthrough.
PPP Connection Trigger	Indicates the connection method for the router for keeping the connection intact. The following options are supported: <ul style="list-style-type: none"> • Auto Connect • On Demand
Idle Timeout	This parameter is mandatory when you select On Demand type of PPP Connection Trigger . Specifies the duration (in seconds) after which PPPoE keep-alive packets must be sent to keep the connection intact. Default: 300
MTU	Maximum size (in bytes) of each packet sent in a single transmission between connected devices. Default: 1492

- **Static**—Configure the Static parameters as described in [Table 105](#).

AP Groups > Add New

Basic
Management
Radio
Network
Security

AP Mode
☒ Router ☐ Bridge

WAN Configuration
WAN Mode
☐ DHCP ☐ PPPoE ☒ Static

☒ **IPv4**
IP Address*

Subnet Mask*

Gateway*

Primary DNS*

Secondary DNS*

MTU

Table 105 WAN Mode: Static parameters

Parameter	Description
Static-related parameters	
IP Address	IPv4 address assigned to the router.
Subnet Mask	Subnet mask assigned to the router's IPv4 address.
Gateway	IPv4 address of the gateway used for communication.
Primary DNS	IPv4 address of the primary DNS server.
Secondary DNS	IPv4 address of the secondary DNS server.
MTU	Maximum size (in bytes) of each packet sent in a single transmission between connected devices. Default: 1492



Note

If you select **PPPoE** or **Static** mode, you must preconfigure the settings in the router before shipping the routers to customers. Complete the following steps before shipping the Home Mesh Router to the customers:

1. Onboard the Home Mesh Router using the standard WAN mode as **DHCP**.
2. After the Home Mesh Router is onboarded, set the WAN mode to **PPPoE** or **Static**.
3. Configure the username and password credentials.
The configuration and the credentials are applied on the Home Mesh Router.
4. Disconnect the Home Mesh Router and ship it to the customer.

When the customer connects the router to the PPPoE authenticated network, the Home Mesh Router uses the PPPoE credentials to authenticate.

- c. In the **LAN Configuration** section, configure the mode of IP address assignment for connecting devices to **Auto** or **Manual**.

If you select Manual mode of assignment, configure the following parameters:

Table 106 LAN Configuration parameters for Manual mode

Parameter	Description
IPv4-related parameters	
Local IP Address	Local IPv4 address assigned to the router.
Local Subnet	Subnet mask assigned to the router's IPv4 address.
Address Range Start	Starting IPv4 address in the address pool.
Address Range End	Ending IPv4 address in the address pool.
Domain Name	The domain name.
DNS Mode	DNS mode used for IP address resolution. Following are the supported options: <ul style="list-style-type: none"> • Auto • Manual • Proxy

8. Click the **Security** tab on the left pane and configure protection against different types of attacks, such as Smurf attack and ICMP fragment.

Select the checkbox corresponding to the DoS protection options.

Table 107 Security parameters: DoS Protection

Parameter	Description
IP Spoof	Enable protection against IP spoof attacks. When enabled, the router checks whether the spoofed IP address is reachable before accepting.

Table 107 *Security parameters: DoS Protection*

Parameter	Description
Smurf Attack	Enable protection against Smurf attacks. When enabled, the router does not respond to the broadcast ICMP.
IP Spoof Log	Enable logging of IP spoof addresses. When enabled, the router logs the unroutable source IP address.
ICMP Fragment	Enable protection against ICMP fragmented ping attack. When enabled, the router drops the fragmented ICMP packets.

9. Click **Add New** in the **ACL** section and configure the parameters as described in [Table 107](#).

Table 108 *Security parameters: Access Control List (ACL)*

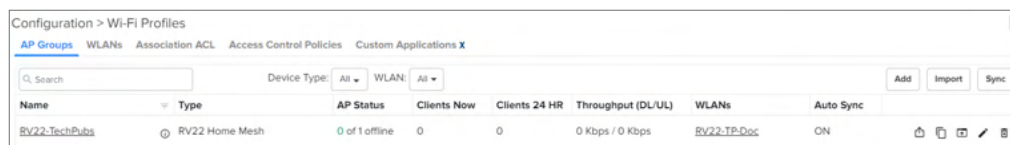
Parameter	Description
Precedence	Specifies the priority of the rule configured. Select the precedence from the dropdown list.
Policy	Indicates the action to be taken for the policy. The following are the supported actions: <ul style="list-style-type: none"> • Accept • Drop • Reject
Direction	Direction to which the policy must be applied. The following are the supported options: <ul style="list-style-type: none"> • WAN to LAN • LAN to WAN • WAN to Router • Router to WAN

Table 108 *Security parameters: Access Control List (ACL)*

Parameter	Description
Type	<p>Type of traffic to which the policy must be applied.</p> <p>The following are the supported options:</p> <ul style="list-style-type: none"> • IP • IPv6 • MAC • Protocol • Protocolv6 <p>Additional parameters are enabled when you select the type.</p>
Source IP/Mask Destination IP/Mask	<p>This field is applicable when you select the Type as IP, IPv6, Protocol, or Protocolv6.</p> <p>Specifies the source IPv4 or IPv6 address and the destination IPv4 or IPv6 address for the policy.</p> <p>You can configure Any if there is no specific IP address to apply the policy to any source IP address.</p>
Source MAC/Mask Destination MAC/Mask	<p>This field is applicable when you select the Type as MAC.</p> <p>Specifies the source MAC address and the destination MAC address for the policy.</p> <p>You can configure Any if there is no specific MAC address to apply the policy to any source IP address.</p>
Protocol	<p>Type of protocol for which the policy must be applied.</p> <p>The following are the supported options:</p> <ul style="list-style-type: none"> • TCP • UDP • ICMP • Any <p>Additional parameters are enabled when you select the protocol.</p>
Source Port	<p>This field is applicable when you select the Protocol as TCP, UDP, or Any.</p> <p>Specifies the source port number for the policy.</p>
Destination Port	<p>This field is applicable when you select the Protocol as TCP, UDP, or Any.</p> <p>Specifies the source port number for the policy.</p>
Description	Description for the rule.

10. Click **Save**.

The AP group is successfully created with the configured parameters.



Onboarding the Home Mesh Router to cnMaestro

After creating a WLAN profile and an AP group, you must now create a subscriber profile and associate it with the subscriber. Finally, you must onboard the router(s) to the corresponding subscriber.

Adding a subscriber and onboarding the router involves the following steps:

1. [cnMaestro Subscriber application branding](#)
2. [Adding a Home Site](#)
3. [Adding a Subscriber Service Profile](#)
4. [Adding a subscriber](#)
5. [Claiming the Home Mesh Router](#)

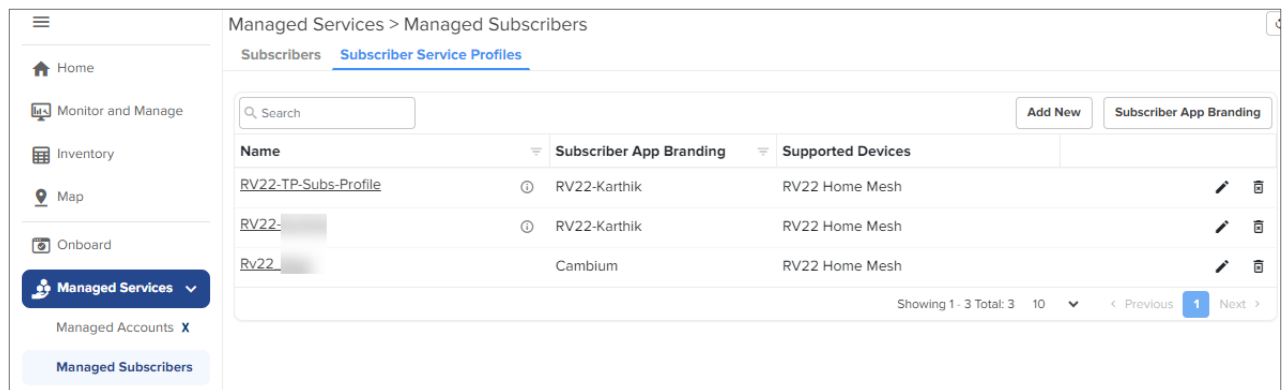
cnMaestro Subscriber application branding

Customize the cnMaestro Subscriber mobile application with your company name, brand logo, and other details, such as support contact information and hours. This branding can be associated with individual subscriber service profiles.

To add brand details to the cnMaestro Subscriber application, complete the following steps:


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

The **Subscriber Service Profiles** page appears.



Name	Subscriber App Branding	Supported Devices
RV22-TP-Subs-Profile	RV22-Karthik	RV22 Home Mesh
RV22-	RV22-Karthik	RV22 Home Mesh
Rv22-	Cambium	RV22 Home Mesh

2. Click **Subscriber App Branding**.

3. Click the add () icon.

The **Subscriber App Branding** window appears. Configure the following parameters as described in [Table 109](#).

Table 109 *Subscriber App Branding parameters*

Parameter	Description
Name	Name of the application branding.
Logo	Brand logo displayed in the cnMaestro Subscriber application. Maximum size of the image supported is 1 MB. Only JPEG, JPG, PNG, and SVG file formats are supported.
Support Email	Email address for customer support team displayed in the application.
Support Phone Number	Phone number for customer support team displayed in the application.
Support Hours	Contact hours for the customer support team. <ul style="list-style-type: none"> Select the Weekdays checkbox and configure the week days on when the customer support team is available. You can also configure the time using the time picker tool. Select the Weekends checkbox and configure the weekend days on when the customer support team is available. You can also configure the time using the time picker tool.


You can preview your branding updates by scrolling through the images in the preview window on the right.

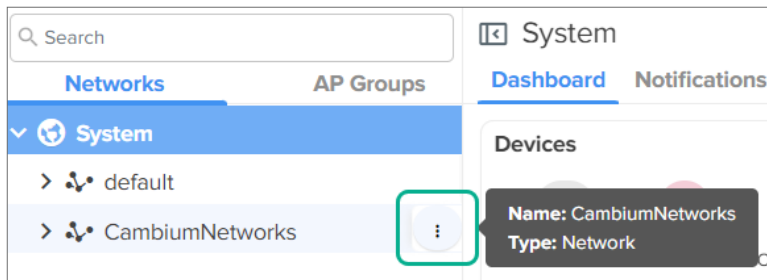
4. Click **Save**.

Adding a Home Site

A home site is required to associate the subscriber's device with the device configuration.

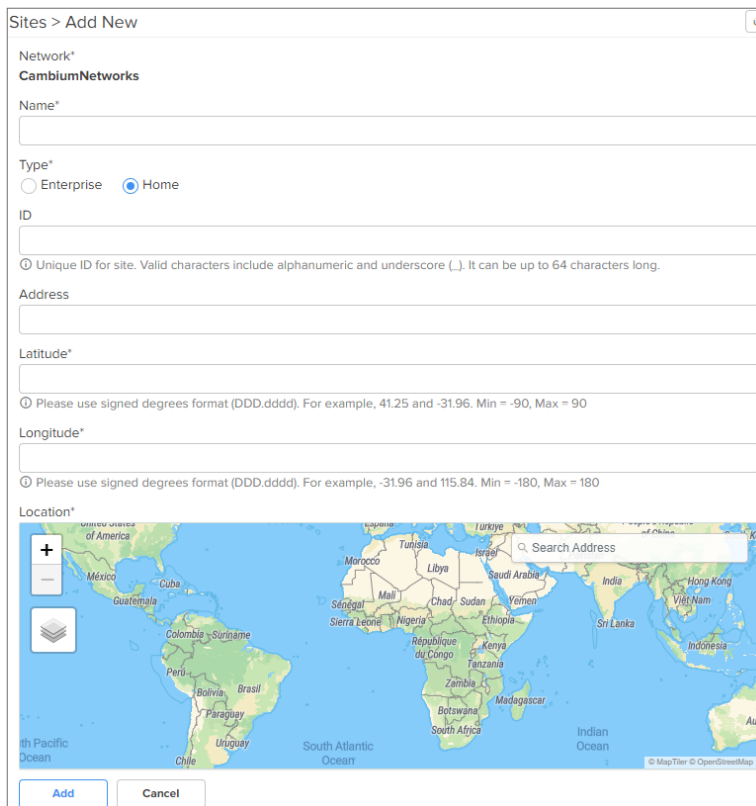
To create a home site, complete the following steps:

1. Click **Monitor and Manage** (.
2. In the **Networks** tab, search for the network and hover over the network name.



3. Click the actions () icon and select **Add Site**.

The **Sites > Add New** page appears.



4. Select the **Home** option in the **Type** field.
5. Enter the location details in the **Longitude** and **Latitude** fields.
You can also search for the location in the map to fill in the details.
6. Click **Add**.

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:

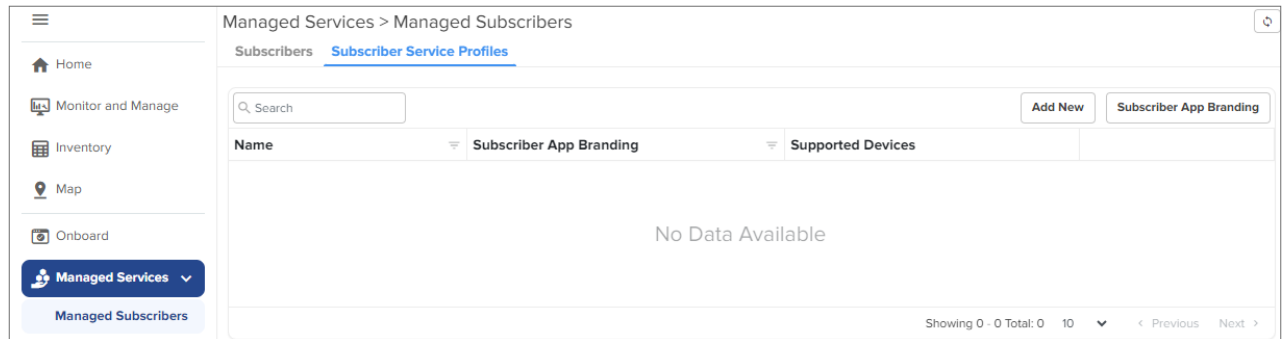
1. [Adding a Subscriber Service Profile](#)
2. [Adding a subscriber](#)
 - a. [Modifying the owner details for the Subscriber App](#)
3. [Claiming the Home Mesh Router](#)

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.

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 110](#).

Table 110 *Subscriber Service Profile parameters*

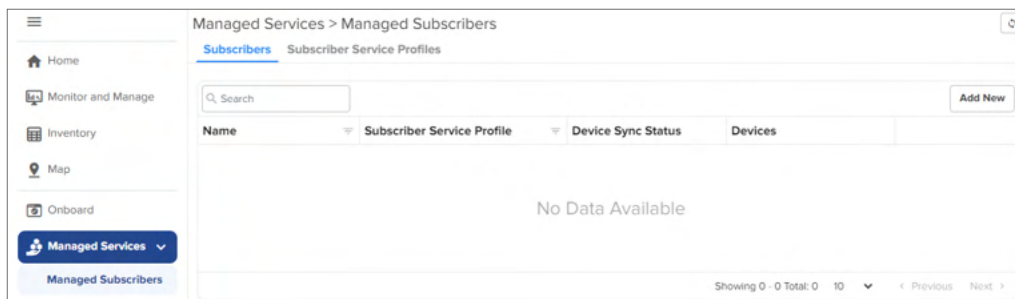
Parameter	Description
Name	Name of the subscriber service profile.
Description	Brief description for the subscriber service profile.

Parameter	Description
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 dropdown 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 dropdown list. If no branding is present, create one by clicking the add () icon. See cnMaestro Subscriber application branding for more information.

- Click **Save**.

Adding a subscriber

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



- Click **Add New**.

The **Add Subscriber** window appears.

Add Subscriber

Basic Information

Service Configuration

Full Name*

Scope

Base Infrastructure

Email*

Phone Number

Customer ID


External system customer ID

Address*

Next

- In the **Add Subscriber** window, configure the details of the subscriber in the **Basic Information** section, as described in [Table 111](#).

Table 111 *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>
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.

- Click **Next**.

The **Service Configuration** tab is displayed.

Add Subscriber

Basic Information

Service Configuration

Subscriber Service Profile*

Download (Mbps)*

Upload (Mbps)*

AP Group

☒ Home Wi-Fi Devices Setting Override

Previous Save

9. Select the subscriber service profile to be associated with this subscriber from the **Service Profile** dropdown 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**.

Add Subscriber

Basic Information

Service Configuration

Devices

Deployment Type

☐ Fiber ☐ Fixed Wireless ☒ Home Site

Home Site*

Search name of Home Site

Add New

Name	Serial Number	MAC Address	Mesh Type	Status
No Data Available				

Previous Save

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 a sidebar on the left containing 'Basic Information', 'Service Configuration', and 'Devices' (highlighted in blue with a red exclamation mark icon). The main area has a 'Deployment Type' section with radio buttons for 'Fiber', 'Fixed Wireless', and 'Home Site' (selected). Below is a 'Home Site*' search bar with a magnifying glass icon and a '+' button. The central part is titled 'Add Devices to Subscriber' and contains a table with columns: 'Name', 'Serial Number', 'MAC Address', 'Mesh Type', 'Status', and an empty column. The table is currently empty, displaying 'No Data Available'. An 'Add New' button is in the top right of the table area. At the bottom right 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'. There is a large text input box with a placeholder: '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

Q

Enter Device name, MAC Address or Serial Number of RV22 Home Mesh

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	<div>Onboarded</div>	



Note

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

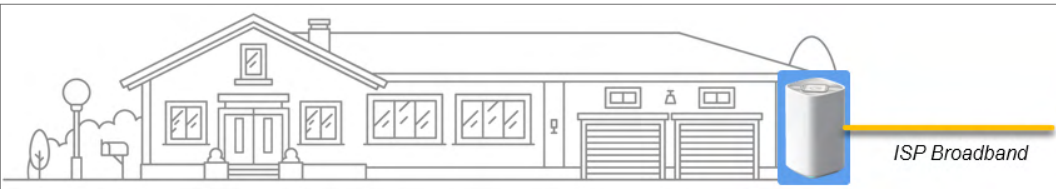
Setting up the Home Mesh Router

Home Mesh Routers can be deployed in one of the following modes:

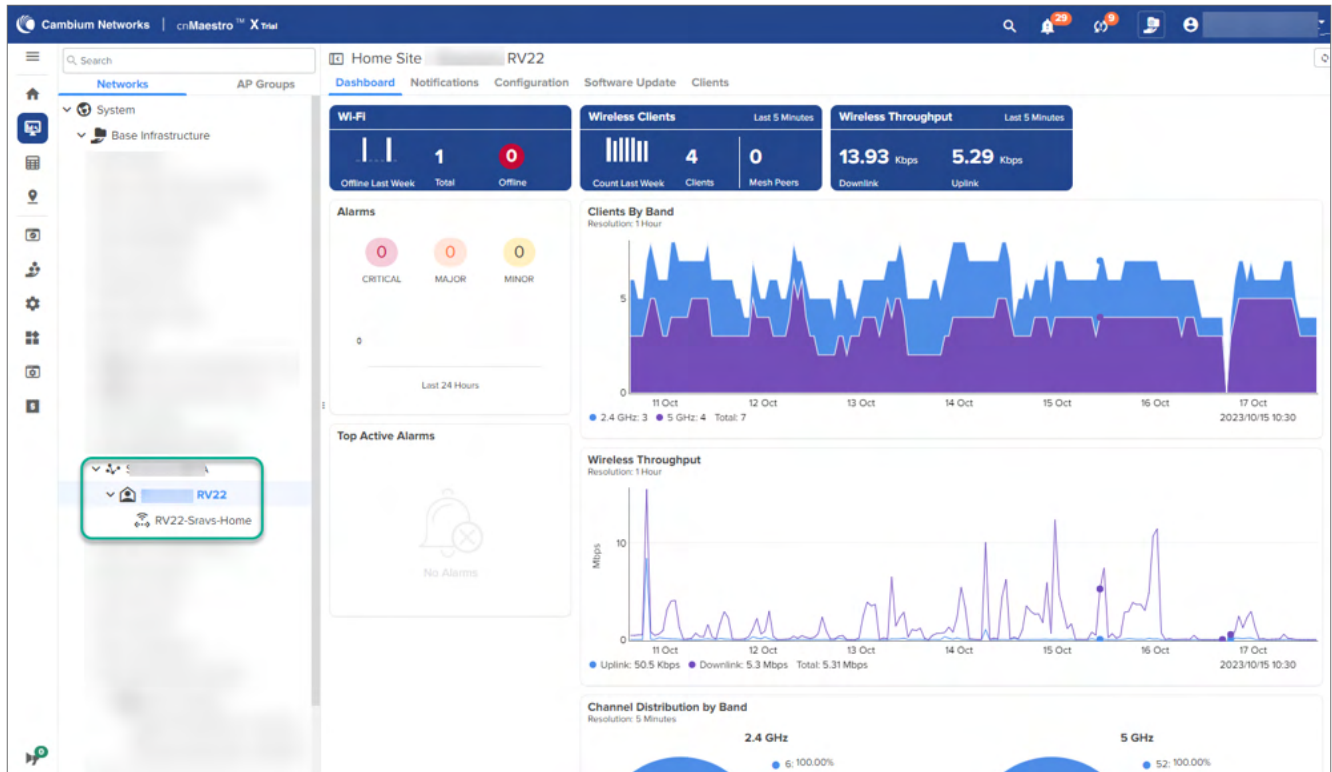
- [Setting up the Home Mesh Router—Standalone mode](#)
- [Setting up the Home Mesh Router—Wireless Mesh Mode](#)
- [Setting up the Home Mesh Router—Wired Mesh Mode](#)

Setting up the Home Mesh Router—Standalone mode

In standalone mode of deployment, there is only one Home Mesh Router deployed. A sample scenario is shown in the following figure:



A sample cnMaestro dashboard for the standalone mode of deployment is shown in the following figure:



Setting up the Home Mesh Router—Wireless Mesh Mode

To configure a wireless mesh, onboard the routers to a site—Claim all the routers, which you want to be part of the mesh, on cnMaestro in the subscriber workflow. See [Claiming the Home Mesh Router](#). Connect the mesh base router to the internet and wirelessly connect the node routers. The AP group mapped to the subscriber is applied to all the routers to sync the configuration.

Following are some of the wireless mesh configuration scenarios and the corresponding dashboards and hierarchy in cnMaestro:

- [Wireless mesh: 1-1 deployment](#)
- [Wireless mesh: 1-1-1 deployment](#)
- [Wireless mesh: 1-2 deployment](#)
- [Wireless and wired mixed mesh 1-2 deployment](#)

Wireless mesh: 1-1 deployment

In this deployment, the base router is connected to one node router, thereby creating a wireless 1-1 mesh deployment.

Figure 483 *Wireless mesh: 1-1 deployment*



[Figure 484](#) displays a sample cnMaestro dashboard for the wireless mesh 1-1 deployment.

Figure 484 Sample dashboard for wireless mesh: 1-1 deployment

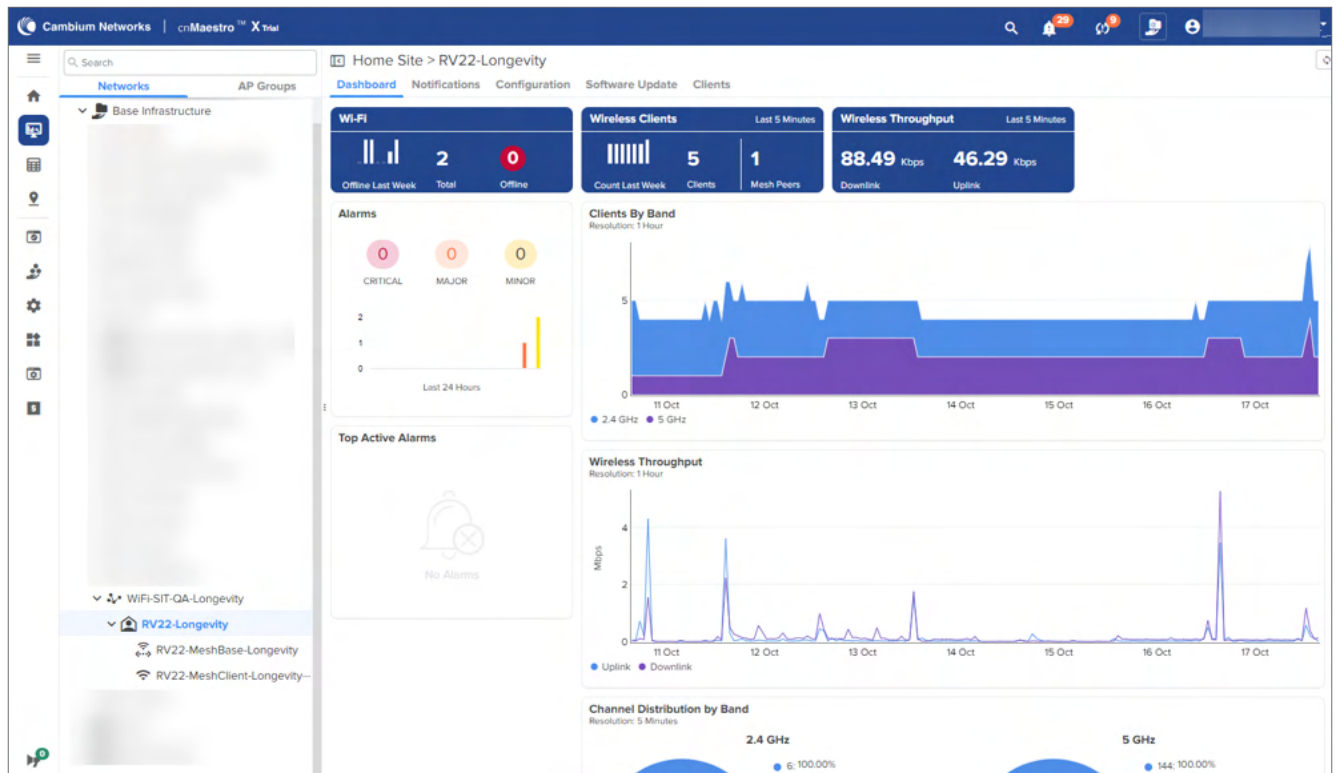
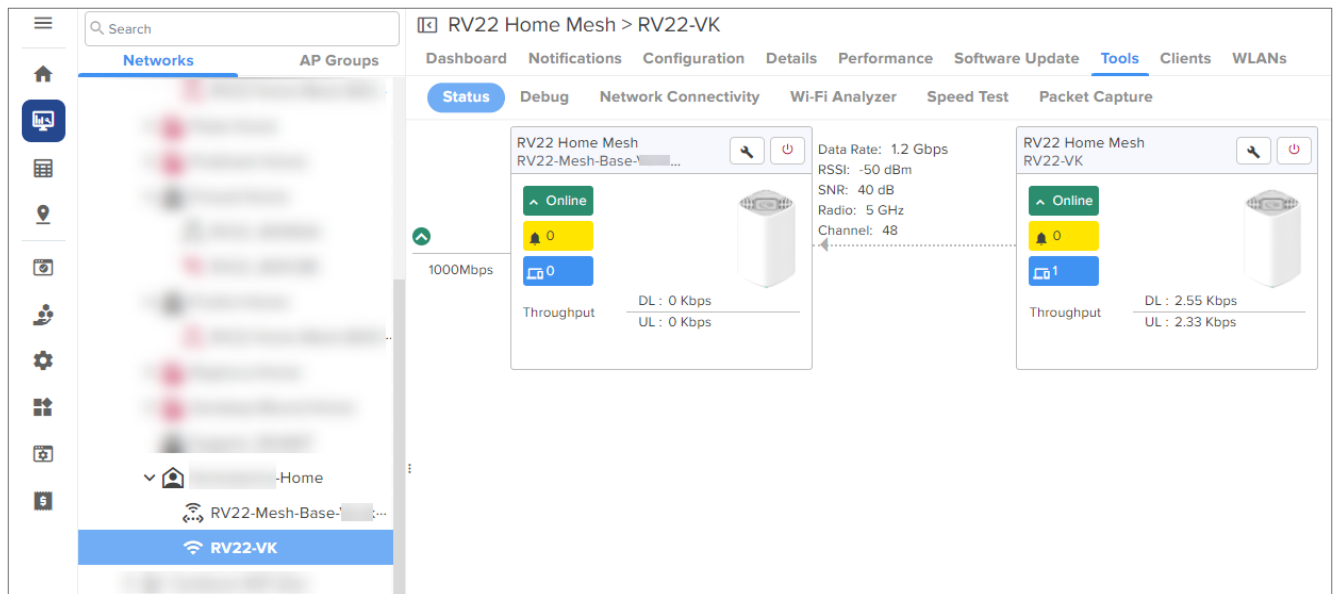


Figure 485 displays a sample cnMaestro status page for the wireless mesh 1-1 deployment.

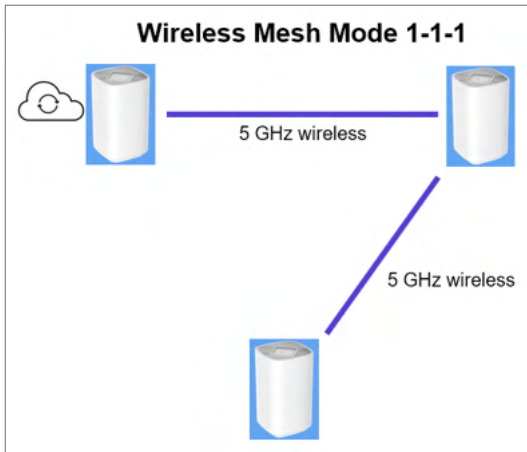
Figure 485 Sample status page for wireless mesh: 1-1 deployment



Wireless mesh: 1-1-1 deployment

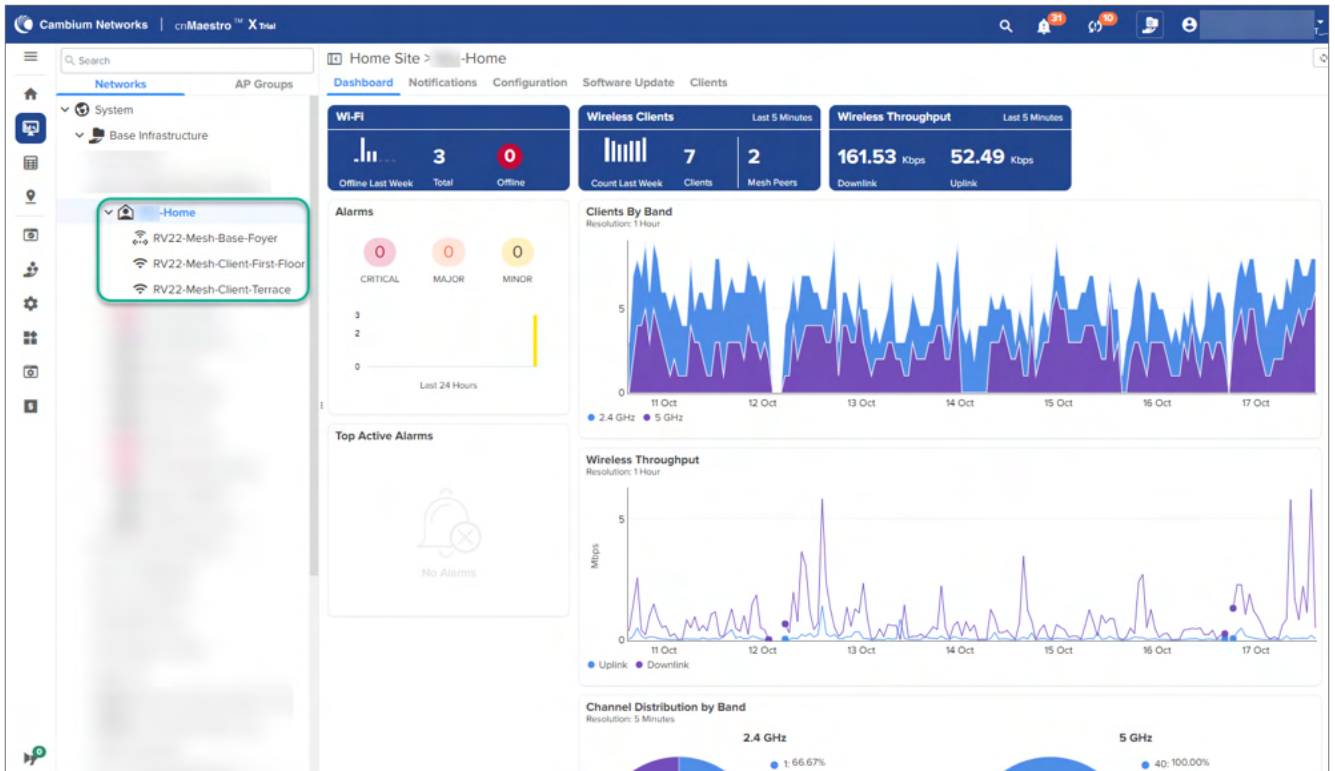
In this deployment, the base router is connected wirelessly to only one of the node routers, which is in turn connected to another node router, thereby creating a wireless 1-1-1 mesh deployment.

Figure 486 *Wireless mesh: 1-1-1 deployment*



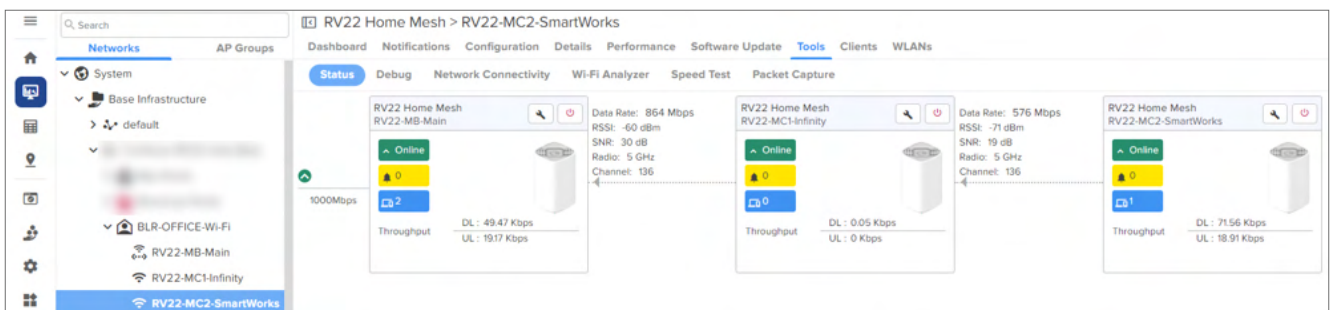
[Figure 487](#) displays a sample cnMaestro dashboard for the wireless mesh 1-1-1 deployment.

Figure 487 *Sample dashboard for wireless mesh: 1-1-1 deployment*



[Figure 488](#) displays a sample cnMaestro status page for the wireless mesh 1-1-1 deployment.

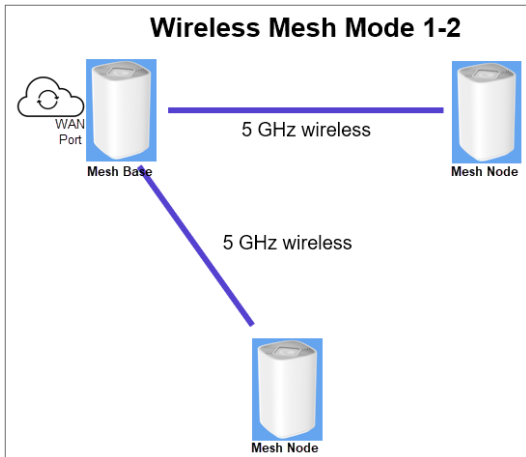
Figure 488 *Sample status page for wireless mesh: 1-1-1 deployment*



Wireless mesh: 1-2 deployment

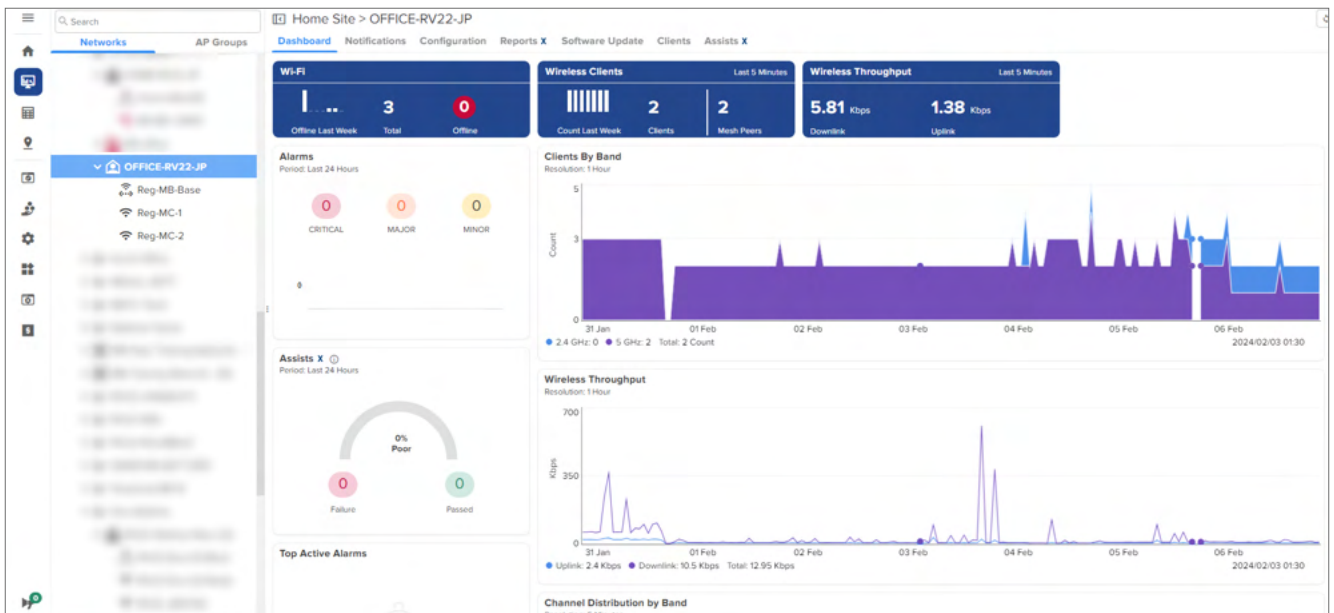
In this deployment, the base router is connected to two node routers simultaneously, thereby creating a wireless 1-2 mesh deployment.

Figure 489 *Wireless mesh: 1-2 deployment*



[Figure 490](#) displays a sample cnMaestro dashboard for the wireless mesh 1-2 deployment.

Figure 490 *Sample dashboard for wireless mesh: 1-2 deployment*

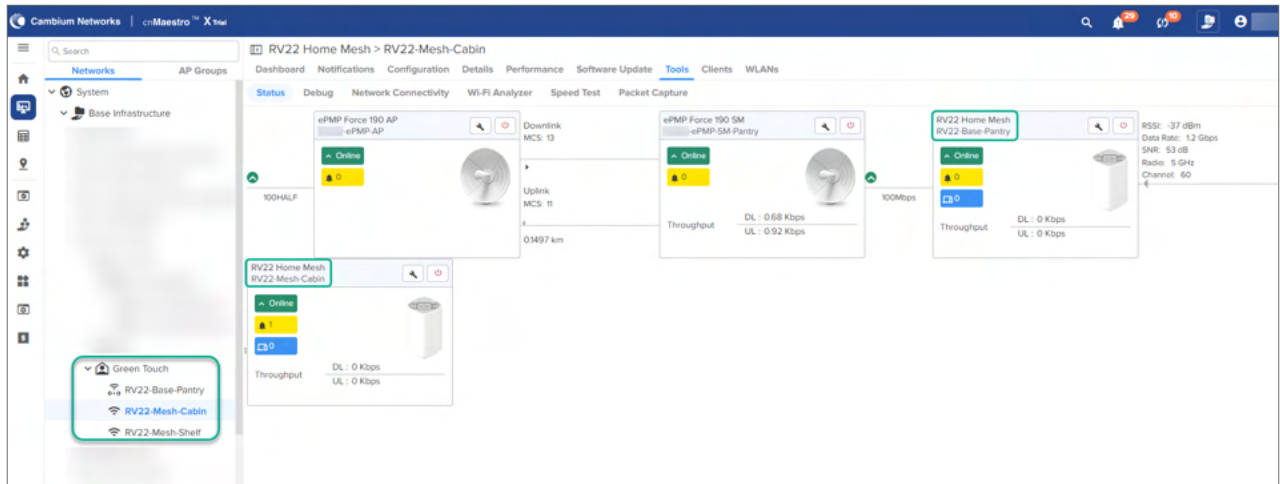


[Figure 491](#) and [Figure 492](#) display sample status pages for the node routers in a wireless mesh 1-2 deployment.

In the following status samples, the **RV22-Base-Pantry** router is connected to both **RV22-Mesh-Shelf** and **RV22-Mesh-Cabin** routers, forming a 1-2 multi-mesh topology.

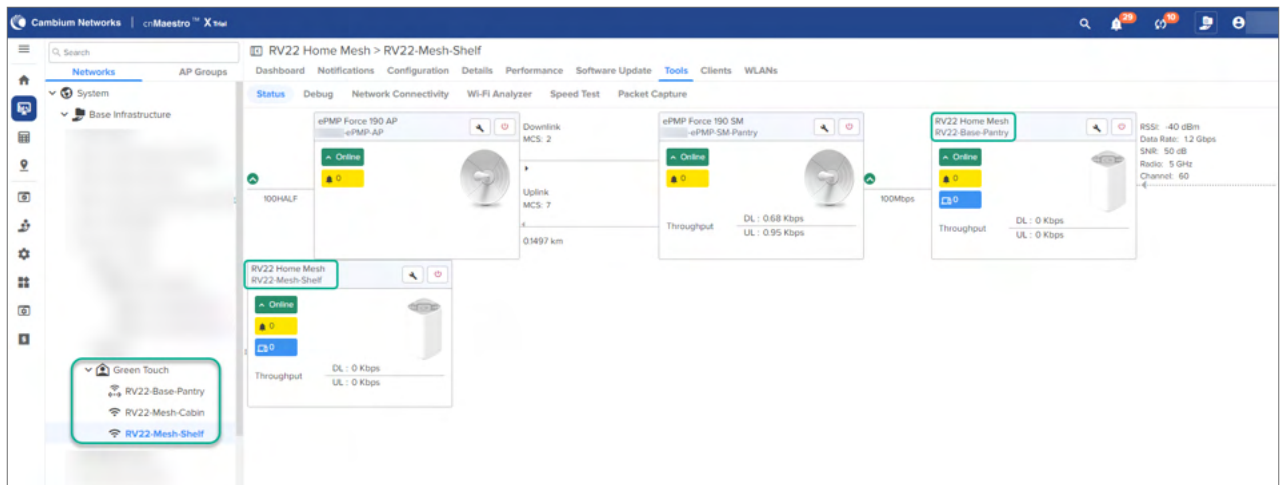
- Network topology for the **RV22-Mesh-Cabin** router

Figure 491 Sample status page for RV22-Mesh-Cabin node router in a wireless mesh: 1-2 deployment



- Network topology for the **RV22-Mesh-Shelf** router

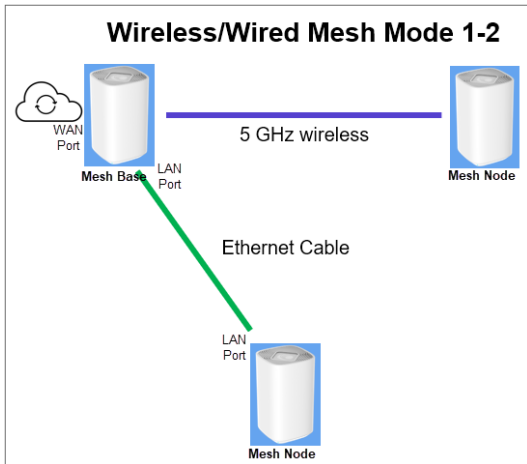
Figure 492 Sample status page for RV22-Mesh-Shelf node router in a wireless mesh: 1-2 deployment



Wireless and wired mixed mesh 1-2 deployment

In this deployment, the base router is connected to one node router wirelessly and simultaneously to another by a wired connection, thereby creating a mixed 1-2 mesh deployment.

Figure 493 *Wireless and wired mixed mesh: 1-2 deployment*

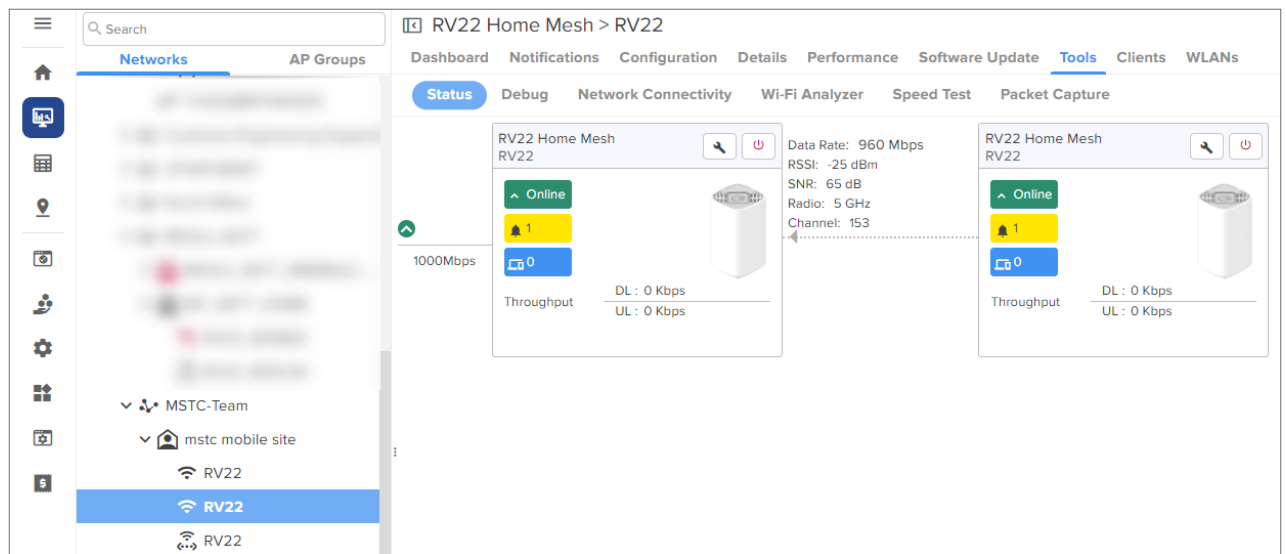


[Figure 491](#) and [Figure 492](#) display sample status pages for the node routers in a mixed mesh 1-2 deployment.

In the following status samples, one RV22 base router is connected to one RV22 node router wirelessly and simultaneously to another RV22 node router by a wired connection.

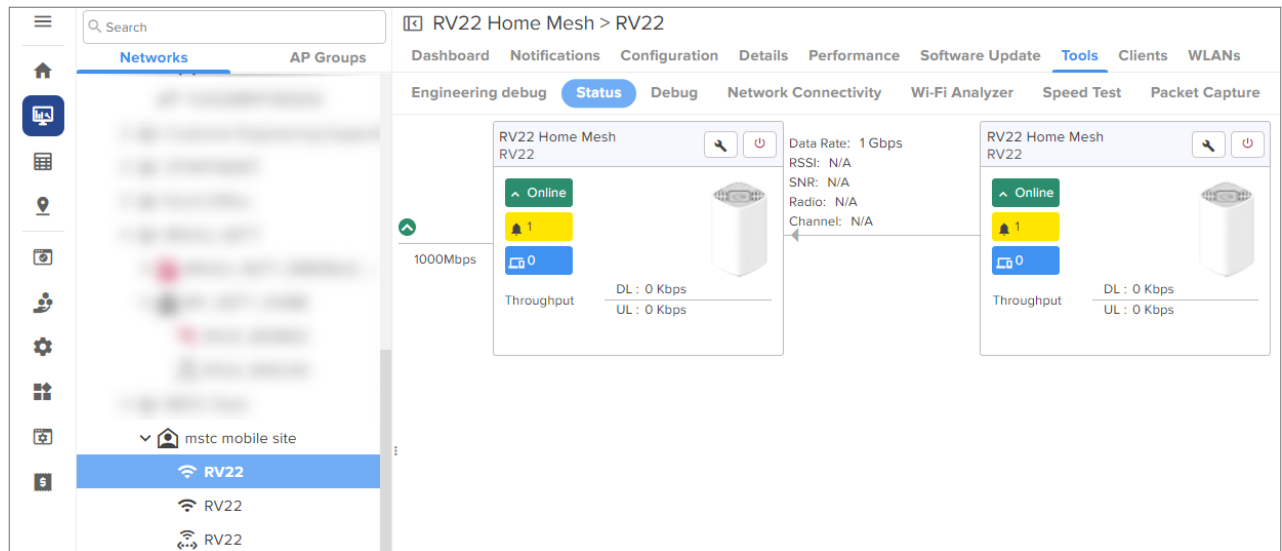
- Network topology for the wireless RV22 node router

Figure 494 *Sample status page for the wireless RV22 node router in a mixed mesh: 1-2 deployment*



- Network topology for the wired RV22 node router

Figure 495 Sample status page for the wired RV22 node router in a mixed mesh: 1-2 deployment



Setting up the Home Mesh Router—Wired Mesh Mode

To configure a wired mesh, onboard the routers to a site—Claim the routers, which you want to be part of the mesh, on cnMaestro in the subscriber workflow. See [Claiming the Home Mesh Router](#). Connect the mesh base router to the internet and connect the mesh node routers to the base router using Ethernet cables. The AP group mapped to the subscriber is applied to all the routers to sync the configuration.

No configuration changes are required for RV22 routers to work in both wired and wireless mesh modes. Use any LAN port on the mesh base and any LAN port on the mesh node routers to establish a wired mesh connection. When a mesh node router detects an RV22 neighbor on its LAN port, it automatically establishes a wired mesh link using the LAN ports.



Note

You must not use the WAN port on the mesh node router to establish a wired mesh.

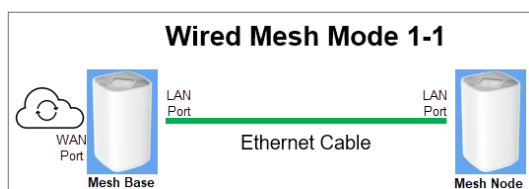
Following are some of the wired mesh configurations supported:

- [Wired mesh: 1-1 deployment](#)
- [Wired mesh: 1-1-1 deployment](#)
- [Wired mesh: 1-2 deployment](#)

Wired mesh: 1-1 deployment

In this deployment, the base router is connected to one node router using an Ethernet cable (between any LAN ports on both routers), thereby creating a wired 1-1 mesh deployment.

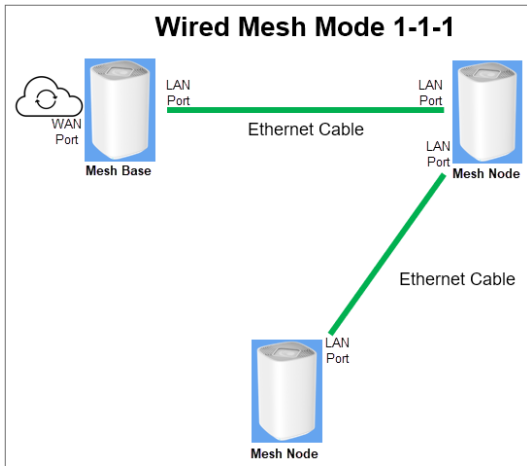
Figure 496 Wired mesh: 1-1 deployment



Wired mesh: 1-1-1 deployment

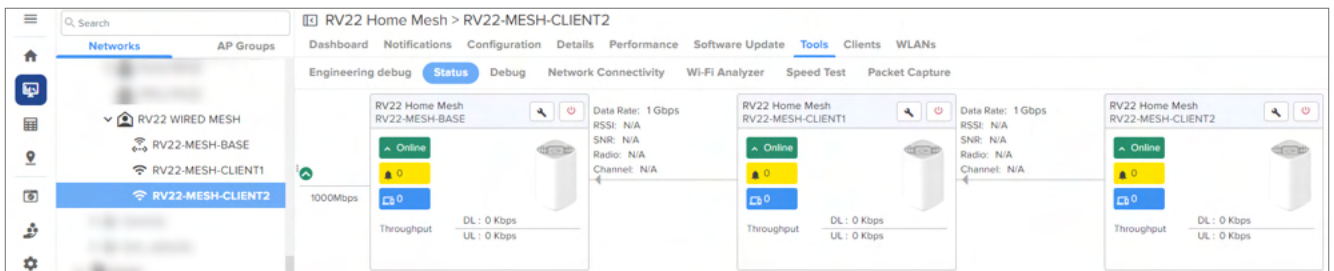
In this deployment, the base router is connected to only one of the node routers, which is in turn connected to another node router, by a wired connection (between any LAN ports on the routers), thereby creating a wired 1-1-1 mesh deployment.

Figure 497 *Wired mesh: 1-1-1 deployment*



[Figure 498](#) displays a sample cnMaestro status page for the wired mesh 1-1-1 deployment.

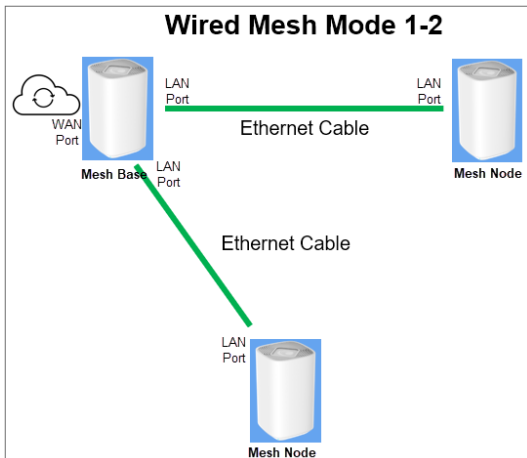
Figure 498 *Sample status page for wired mesh: 1-1-1 deployment*



Wired mesh: 1-2 deployment

In this deployment, the base router is connected to two node routers simultaneously by a wired connection, thereby creating a wired 1-2 mesh deployment.

Figure 499 *Wired mesh: 1-2 deployment*

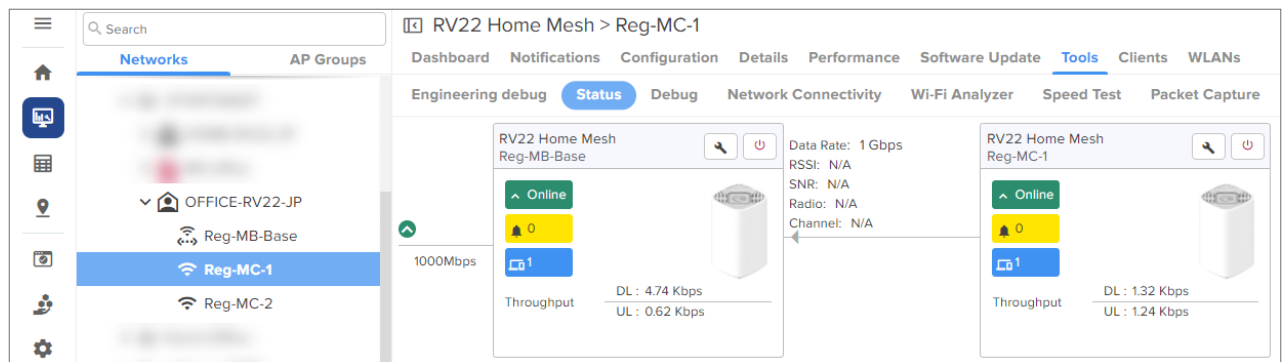


[Figure 500](#) and [Figure 501](#) display sample status pages for the node routers in a wired mesh 1-2 deployment.

In the following status samples, the **Reg-MB-Base** router is connected to both **Reg-MC-1** and **Reg-MC-2** routers using Ethernet cables, forming a wired 1-2 multi-mesh topology.

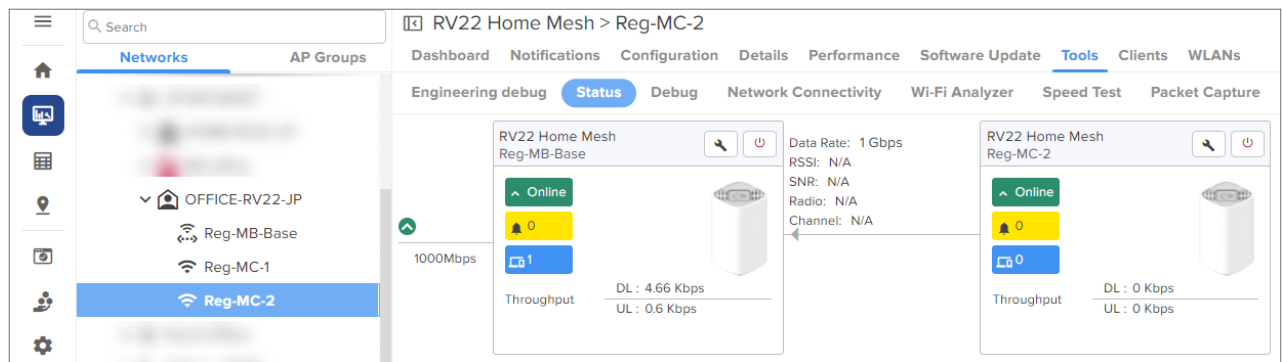
- Network topology for the **Reg-MC-1** router

Figure 500 Sample status page for Reg-MC-1 node router in a wired mesh: 1-2 deployment



- Network topology for the **Reg-MC-2** router

Figure 501 Sample status page for Reg-MC-2 node router in a wired mesh: 1-2 deployment



Viewing router system information and network traffic status

When the customer configures the Home Mesh Router and connects to the internet, you can check the connection of the router in cnMaestro. You can also check the details of the clients that are connected.

To view router system information and the connection status, navigate to **Monitor and Manage** > **<Home-Mesh-Router-name>** > **Details** tab.

The **Details** page displays information in the following tabs:

- **Overview**

This page displays information in the following sections:

- **System**—Displays information, such as router name, MAC address, health of the router (online, offline), software version, and location.
- **Radio**—Displays radio details, such as the running bands, RF quality, count of clients connected to each radio, and the average throughput.
- **Configuration Update**—Displays the history of configuration updates to the router.
- **Software Update**—Displays the currently running software version and a history of software updates that were performed and the status.

RV22 Home Mesh > RV22-Mesh-Base-Foyer

Dashboard
Notifications
Configuration
Details
Performance
Software Update
Tools
Clients
WLANs

Overview
Network Info

System

Name	RV22-Mesh-Base-Foyer
Product Name	RV22 Home Mesh
MAC Address	
Health	● Online (2d 23h 16m)
Uptime	2d 23h 16m
IPv4 Address	192.168.20.54
Software Version	1.0.0-b21
Serial Number	
Hardware	RV22 Wi-Fi 6 Home MESH Router 2x2 dual band
DA Version	4.107
Last Reboot	Sat Oct 14 2023 17:07 (Device reboot due to Power Cycle)
Location	
Onboard Date	27 Sep 2023, 04:07 PM
Description	
Available Memory	50%
CPU Utilization	20%

Configuration Update

History

Date	Status	AP Group
17 Oct 2023, 02:27 PM	Success	RV22 Bijju Home Profile
17 Oct 2023, 02:27 PM	Success	RV22 Bijju Home Profile
17 Oct 2023, 03:04 PM	Success	RV22 Bijju Home Profile

Radio Details

Radio	Radio 1	Radio 2
Band	2.4 GHz	5 GHz
State	ON	ON
Channel	1	40
Channel Width	20 MHz	80 MHz
Power	14 dBm	15 dBm
MAC Address		
RF Quality	📶 Average	📶 Average
WLANs	1	1
Mesh	OFF	BASE
Clients	1	1
UL Throughput	0.12 Kbps	16.26 Kbps
DL Throughput	0.25 Kbps	59.63 Kbps

Software Update

Active Software Version	1.0.0-b21
Inactive Software Version	1.0.0-b20_1012_1

History

Date	Status	Version
12 Oct 2023, 12:10 PM	Success	1.0.0-b20_1012_1
12 Oct 2023, 03:01 PM	Success	1.0.0-b20_1012_1
13 Oct 2023, 01:56 PM	Success	1.0.0-b21

• Network Info

This page displays information in the following sections:

- **WAN**—Displays collective statistics about total number of transmitted and received data packets, data bytes, packets dropped, maximum and average speeds
- **IPv4 Routes**—Displays the IPv4 routes configured for the router.
- **DNS Server(s)**—Displays the details of the DNS servers.
- **LAN**—Displays details of the LAN interfaces, their status, total number of transmitted and received data packets and size (in bytes), packet errors and drops.
- **DHCP Server**—Displays details of the DHCP servers, start and end IP address in the range used for allocation, and the lease time.

RV22 Home Mesh > RV22-Mesh-Base-Foyer

DashboardNotificationsConfigurationDetailsPerformanceSoftware UpdateToolsClientsWLANs

OverviewNetwork Info

WAN

IPv4 Address	IPv6 Address	MAC	Link Status	Tx Bytes	Rx Bytes	Tx Avg (Kbps)	Tx Max (Kbps)	Tx Min (Kbps)	Rx Max (Kbps)	Rx Avg (Kbps)	R
192.168.20.54			UP	3837701583	22853270234	116	105862	0	145606	696	0

IPv4 Routes

Destination	Mask	Gateway	Flags	Metric	Interface
0.0.0.0	0.0.0.0	192.168.20.1	UG	0	eth1.2
192.168.11.0	255.255.255.0	0.0.0.0	U	0	br0
192.168.20.0	255.255.255.0	0.0.0.0	U	0	eth1.2
239.0.0.0	255.0.0.0	0.0.0.0	U	0	br0

DNS Server(s)

IP Address	Resolve Status
192.168.20.1	SUCCESS

LAN

Interface Name	Link Status	Tx Bytes	Rx Bytes	Rx Errors	Tx Errors	Tx Drops	Rx Drops	Rx Packets	Tx Packets	Speed	Duple
lan1	DOWN	0	0	0	0	0	0	0	0		
lan2	DOWN	0	0	0	0	0	0	0	0		
lan3	DOWN	0	0	0	0	0	0	0	0		

DHCP Server

Type	Start Address	End Address	Network Mask	Lease Time	Prefix Length	MAC Address	IP Address
v4	192.168.11.2	192.168.11.254	255.255.255.0	3600	-		192.168.11.1

Viewing, editing, and blocking connected clients

cnMaestro allows you to view details of clients (both wired and wireless) connected to the router and edit the name of clients. You can also block certain clients that you do not want to be connected to your wireless networks.

This topic contains the following sections:

- [Viewing connected clients](#)
- [Editing client host name](#)
- [Blocking clients](#)

Viewing connected clients

To view the list of connected clients, both wired and wireless, navigate to **Monitor and Manage** > *<Home-Mesh-Router-name>* > **Clients** tab.

The **Details** page displays information in the following tabs:

- **Wireless Clients**

This page displays information about the wireless clients connected to the router, such as the host name, MAC address, IPv4 address assigned, the router it is connected to, and the status of connection with the router (online, offline).

Host Name	Managed Account	AP	IPv4 Address	MAC	Manufacturer	Capability	SSID	Base
's iPhone	Base Infrastructure	RV22-Mesh-Base-Foyer			unknown	axa	RV22	Home 5 C
IN01-5TY70J3	Base Infrastructure	RV22-Mesh-Base-Foyer			Intel Corporate	axa	RV22	Home 5 C
Samsung Refrigerator	Base Infrastructure	RV22-Mesh-Base-Foyer			S.J.I Industry Company	gn	RV22	Home 2.4
iPhone	Base Infrastructure	RV22-Mesh-Base-Foyer			unknown	axa	RV22	Home 5 C
iPhone Air	Base Infrastructure	RV22-Mesh-Client-First-Floor			Apple, Inc.	ac	RV22	Home 5 C
android-dhco-12	Base Infrastructure	RV22-Mesh-Client-Terrace			unknown	ac	RV22	Home 2.4
unknown	Base Infrastructure	RV22-Mesh-Client-First-Floor			unknown	an	RV22	Home 5 C

• Wired Clients

This page displays information about the wired clients connected to the router, such as the host name, MAC address, IPv4 address assigned, port number to which it is connected, the manufacturer of device connected, last connected duration, and the download and upload data size (in MB).

Host Name	Managed Account	IPv4 Address	MAC	Port	Manufacturer	Last Duration	Download	Upload
Cambium-cnMatrix-FX2K	Base Infrastructure			Ethernet LAN 2	Cambium Networks Limited	0d 2h 42m	393.2 MB	54.5 MB
XV2-2-540556	Base Infrastructure			Ethernet LAN 2	Cambium Networks Limited	0d 2h 42m	393.2 MB	54.5 MB
XV2-2IX-E5386F	Base Infrastructure			Ethernet LAN 2	Cambium Networks Limited	0d 2h 42m	393.2 MB	54.5 MB

Editing a client's host name

To edit the host name of a connected client, click the edit client name (✎) icon corresponding to the client.

Enter the name in the **Host Name** field and click **Save**.

Blocking clients

To block a connected client, click the block (🚫) icon corresponding to the client.

Monitoring and troubleshooting the Home Mesh Router

You can monitor and perform troubleshooting tasks on the Home Mesh Router using cnMaestro. This topic covers the following sections

- [Monitoring the Home Mesh Router](#)
- [Troubleshooting the Home Mesh Router](#)
- [Upgrading the Home Mesh Router firmware](#)

Monitoring the Home Mesh Router

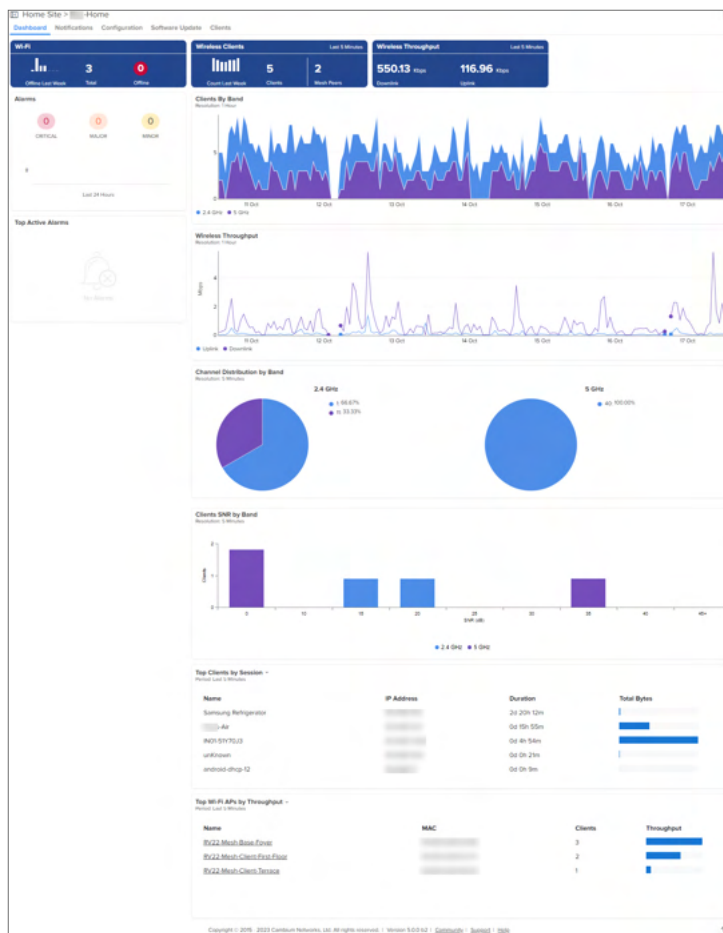
When the device is onboarded to cnMaestro, based on the deployment type, the router is displayed under the site that it is configured.

Using the following pages in cnMaestro, monitor and view details of the router and the deployment.

- [Home Site Dashboard](#)
- [Notifications](#)
- [Software Update](#)
- [Performance](#)

Home Site Dashboard

To view the site dashboard, access the **Dashboard** page under **Monitor and Manage** > <Home-site-name> > **Dashboard**.



Notifications

The Notifications page displays current alarms, previous alarms, Wi-Fi-related events, and other device-related events.

cnMaestro displays the following types of notifications:

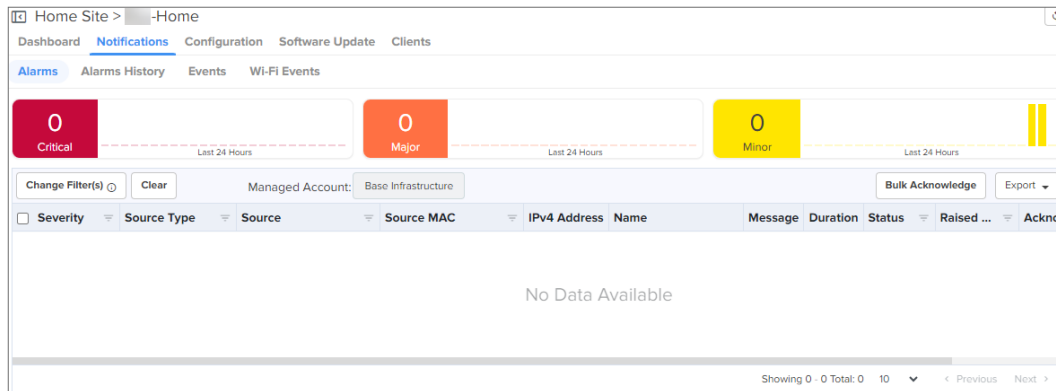
- [Alarms](#)
- [Alarms History](#)

- [Events](#)
- [Wi-Fi Events](#)

Alarms

The Alarms page displays the number of critical, major, and minor events observed for the Home Mesh Router. You can also view the details of the events, such as severity level, name of the event, time and action taken.

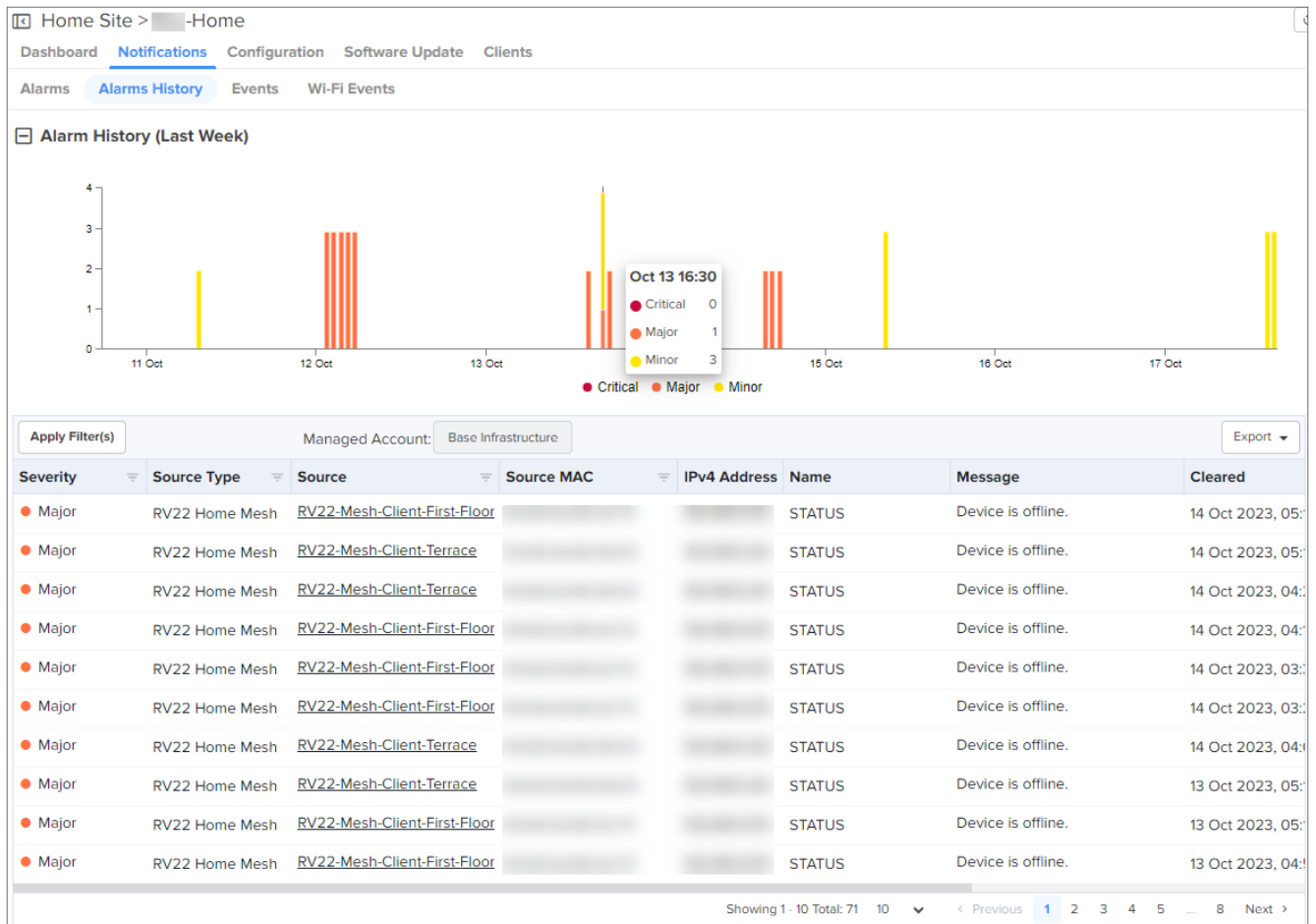
To view the alarms raised, access the **Alarms** page under **Monitor and Manage** > <Home-site-name> > **Notifications** > **Alarms**.



Alarms History

The Alarms History page displays the number of critical, major, and minor events observed in the previous week.

To view the alarms history displayed as a graphical representation, access the **Alarms History** page under **Monitor and Manage** > <Home-site-name> > **Notifications** > **Alarms History**.



Events

The Events page displays Home Mesh Router-related events, such as its status, if there were any changes in bandwidth, and when the DHCP server IP was assigned to the connected clients.

To view the events, access the **Events** page under **Monitor and Manage** > <Home-site-name> > **Notifications** > **Events**.

RV22 Home Mesh > RV22_8001D2

Dashboard **Notifications** Configuration Details Performance Software Update Tools Clients WLANs

Alarms Alarms History **Events** Wi-Fi Events

Apply Filter(s) Managed Account: Base Infrastructure Delete Export

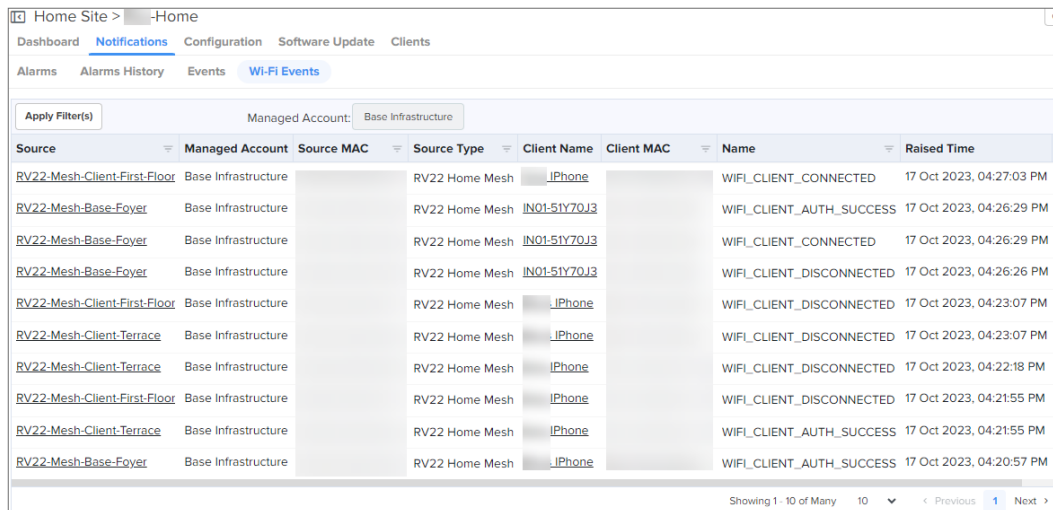
<input type="checkbox"/>	Severity	Category	Event Type	Name	Raised Time	Message	
<input type="checkbox"/>	Notify	WIRELESS	Status	WIFI_ACS_TRIGGERED	09 May 2024, 11:35 AM	Triggered ACS on radio [2] band [5G]	
<input type="checkbox"/>	Notify	WIRELESS	Status	WIFI_ACS_TRIGGERED	09 May 2024, 11:35 AM	Triggered ACS on radio [1] band [2.4G]	
<input type="checkbox"/>	Notify	NETWORK	Status	WANLB_WANLB_LINK_UP	09 May 2024, 11:35 AM	WAN interface [eth1.2] up	
<input type="checkbox"/>	Notify	NETWORK	Status	STATUS_UP	09 May 2024, 11:35 AM	Device is online.	
<input type="checkbox"/>	Major	NETWORK	Status	STATUS_DOWN	09 May 2024, 11:32 AM	Device is offline.	
<input type="checkbox"/>	Notify	NETWORK	Status	STATUS_UP	08 May 2024, 05:24 PM	Device is online.	
<input type="checkbox"/>	Major	NETWORK	Status	STATUS_DOWN	08 May 2024, 05:18 PM	Device is offline.	
<input type="checkbox"/>	Notify	NETWORK	Status	STATUS_UP	08 May 2024, 03:35 PM	Device is online.	
<input type="checkbox"/>	Major	NETWORK	Status	STATUS_DOWN	08 May 2024, 03:34 PM	Device is offline.	
<input type="checkbox"/>	Notify	WIRELESS	Status	WIFI_ACS_TRIGGERED	08 May 2024, 11:42 AM	Triggered ACS on radio [1] band [2.4G]	

Showing 1 - 10 Total: 22 10 < Previous 1 2 3 Next >

Wi-Fi Events

The Wi-Fi Events page displays client-related events, such as when the client connected to the network, when it was disconnected, and authentication events.

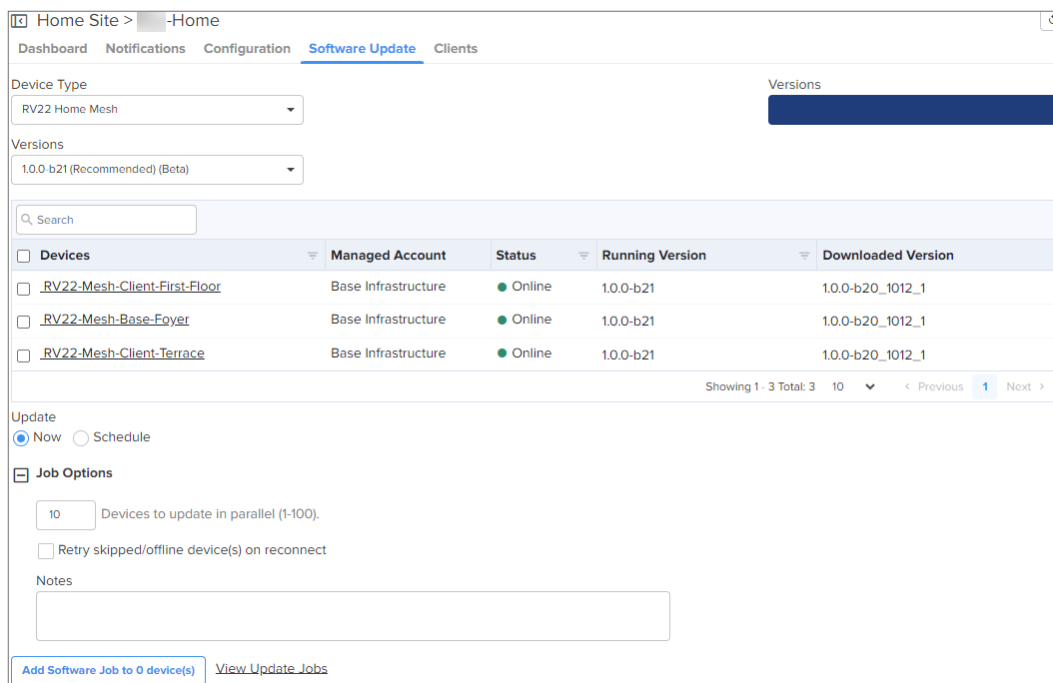
To view the Wi-Fi events, access the **Wi-Fi Events** page under **Monitor and Manage** > <Home-site-name> > **Notifications** > **Wi-Fi Events**.



Source	Managed Account	Source MAC	Source Type	Client Name	Client MAC	Name	Raised Time
RV22-Mesh-Client-First-Floor	Base Infrastructure		RV22 Home Mesh	iPhone		WIFI_CLIENT_CONNECTED	17 Oct 2023, 04:27:03 PM
RV22-Mesh-Base-Foyer	Base Infrastructure		RV22 Home Mesh	IN01-51Y70J3		WIFI_CLIENT_AUTH_SUCCESS	17 Oct 2023, 04:26:29 PM
RV22-Mesh-Base-Foyer	Base Infrastructure		RV22 Home Mesh	IN01-51Y70J3		WIFI_CLIENT_CONNECTED	17 Oct 2023, 04:26:29 PM
RV22-Mesh-Base-Foyer	Base Infrastructure		RV22 Home Mesh	IN01-51Y70J3		WIFI_CLIENT_DISCONNECTED	17 Oct 2023, 04:26:26 PM
RV22-Mesh-Client-First-Floor	Base Infrastructure		RV22 Home Mesh	iPhone		WIFI_CLIENT_DISCONNECTED	17 Oct 2023, 04:23:07 PM
RV22-Mesh-Client-Terrace	Base Infrastructure		RV22 Home Mesh	iPhone		WIFI_CLIENT_DISCONNECTED	17 Oct 2023, 04:23:07 PM
RV22-Mesh-Client-Terrace	Base Infrastructure		RV22 Home Mesh	iPhone		WIFI_CLIENT_DISCONNECTED	17 Oct 2023, 04:22:18 PM
RV22-Mesh-Client-First-Floor	Base Infrastructure		RV22 Home Mesh	iPhone		WIFI_CLIENT_DISCONNECTED	17 Oct 2023, 04:21:55 PM
RV22-Mesh-Client-Terrace	Base Infrastructure		RV22 Home Mesh	iPhone		WIFI_CLIENT_AUTH_SUCCESS	17 Oct 2023, 04:21:55 PM
RV22-Mesh-Base-Foyer	Base Infrastructure		RV22 Home Mesh	iPhone		WIFI_CLIENT_AUTH_SUCCESS	17 Oct 2023, 04:20:57 PM

Software Update

To upgrade the router firmware, go to the **Software Update** page. See [Upgrading the Home Mesh Router firmware](#) for more information.



Devices	Managed Account	Status	Running Version	Downloaded Version
<input type="checkbox"/> RV22-Mesh-Client-First-Floor	Base Infrastructure	Online	1.0.0-b21	1.0.0-b20_1012_1
<input type="checkbox"/> RV22-Mesh-Base-Foyer	Base Infrastructure	Online	1.0.0-b21	1.0.0-b20_1012_1
<input type="checkbox"/> RV22-Mesh-Client-Terrace	Base Infrastructure	Online	1.0.0-b21	1.0.0-b20_1012_1

Performance

To view the performance of the router, access the **Wi-Fi Events** page under **Monitor and Manage** > <Home-Mesh-Router-name> > **Performance**.

The page displays the following graphical information:

Table 112 *Performance page graphs—Base and Node routers*

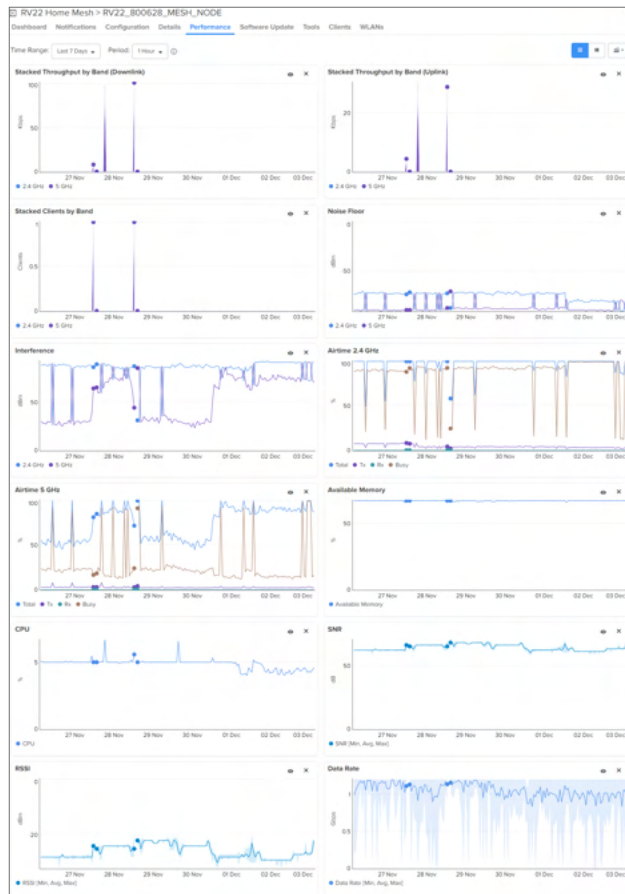
Parameter	Description	Router (Base / Node / Both)
Stacked WAN Throughput	Hourly throughput for both downlink and uplink in the WAN interface for each band of the mesh base router.	Base only
Stacked Throughput by Band (Downlink)	Downlink speed in each band.	Both
Stacked Throughput by Band (Uplink)	Uplink speed in each band.	Both
Stacked Clients by Band	Count of number of clients connected in each band.	Both
Noise Floor	Amount of background noise (in dBm) or interference created by devices in the same frequency.	Both
Interference	Interference (in dBm) caused by other wireless signals and devices interrupting the router's Wi-Fi signal.	Both
Airtime 2.4 GHz	Capacity utilization (in %) of the 2.4 GHz band for effective transmission.	Both
Airtime 5 GHz	Capacity utilization (in %) of the 5 GHz band for effective transmission.	Both
Available Memory	Amount of router memory (in %) available for use.	Both
CPU	Router CPU utilization in percentage (%).	Both
SNR	Minimum, average, and maximum SNR values (in dB) for the mesh node router.	Node only
RSSI	Received Signal Strength Indicator (RSSI) value (in dBm) for the mesh node router.	Node only
Data Rate	Minimum, average, and maximum data rates (in Mbps or Gbps) provided by the mesh node router to the client devices.	Node only

Following are sample performance graphs for base and node routers:

- Performance of the base router in a mesh deployment



- Performance of the node router in a mesh deployment



Troubleshooting the Home Mesh Router

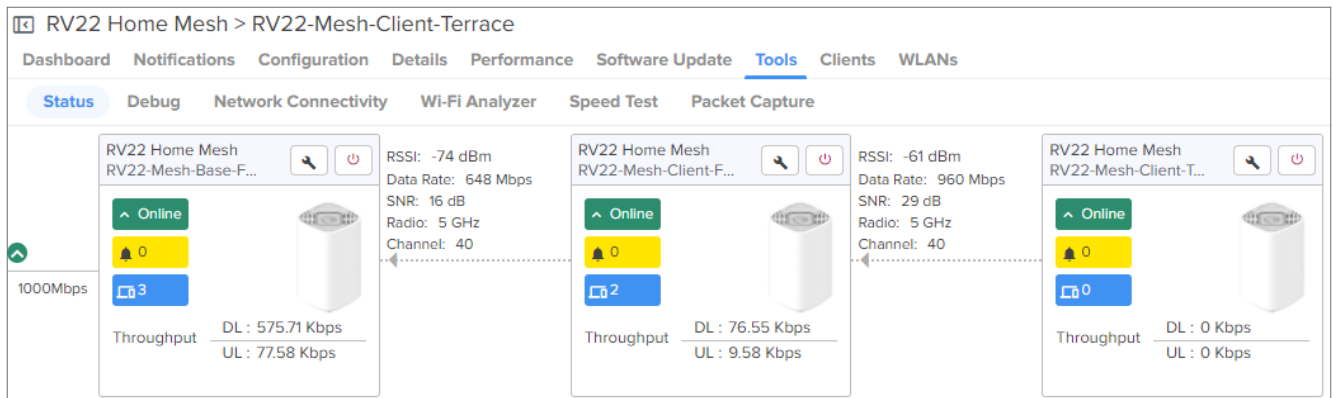
cnMaestro provides the following troubleshooting options for the router:

- [Status](#)
 - [Downloading tech support file](#)
- [Debug](#)
- [Network Connectivity](#)
- [Wi-Fi Analyzer](#)
- [Speed Test](#)
- [Packet Capture](#)


Status

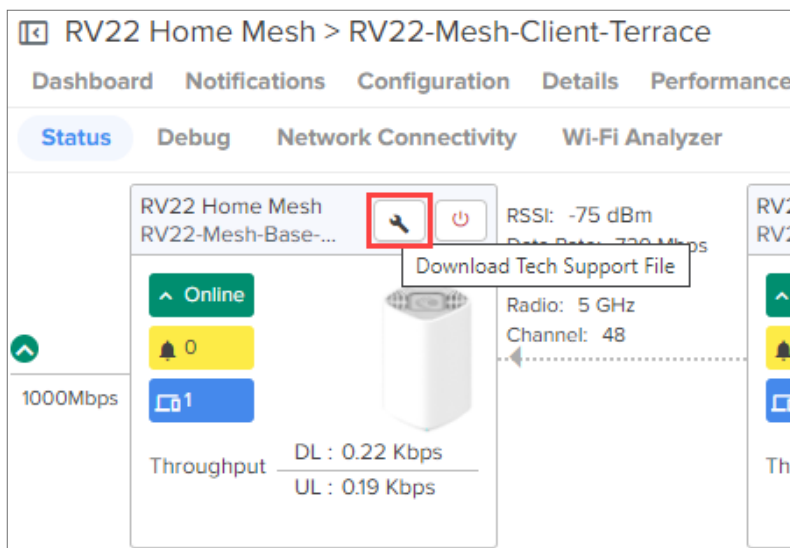
The Status page displays the status of link between the Home Mesh Router base and client devices.

To view the status of the link between the Home Mesh base and client devices, access the **Status** page under **Monitor and Manage** > <Home-Mesh-Router-name> > **Tools**.



Downloading tech support file

To download the tech support file, click the Download Tech Support File () icon on the **Status** page.

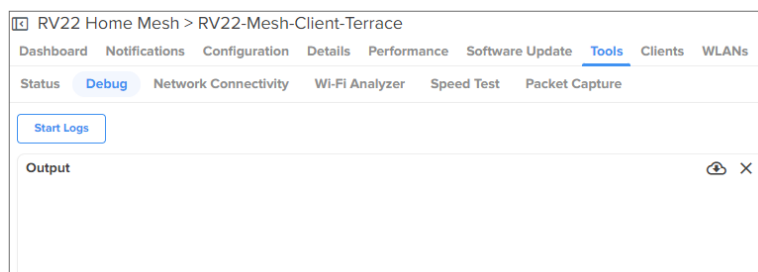


Debug

The Debug page displays log information of the Home Mesh Router. To view the debug information, complete the following steps:

1. Navigate to the **Monitor and Manage** > <Home-Mesh-Router-name> > **Tools** > **Debug** tab.
2. Click **Start Logs**.

The log information is displayed in the **Output** window.



Network Connectivity

The Network Connectivity page provides network connectivity information of the Home Mesh Routers.

cnMaestro supports the following tests to provide connectivity information for the Home Mesh Routers:

- Ping
- DNS Lookup
- Traceroute

To test network connectivity of the router, complete the following steps:

1. Navigate to the **Monitor and Manage** > <Home-Mesh-Router-name> > **Tools** > **Network Connectivity** tab.
2. Select the required test type from the **Test Type** dropdown list and configure the corresponding parameters required for the test.
3. Click **Start Test**.

cnMaestro initiates the test and displays the result in the <Test Type> **Result** window.

The screenshot shows the 'RV22 Home Mesh > RV22-Mesh-Client-Terrace' interface. The 'Tools' tab is selected, and the 'Network Connectivity' sub-tab is active. The 'Test Type' dropdown is set to 'Ping'. The 'IP Address or Hostname*' field contains 'www.cambiumnetworks.com'. The 'Number of Packets (-c)' is set to '3' (with a range of Min = 1, Max = 10). The 'Buffer Size (-s)' is set to '56' (with a range of Min = 1, Max = 65507). A 'Start Ping' button is visible. Below the configuration, a 'Ping Result' window is open, displaying the following text:

```
Ping Result
Complete
Hostname www.cambiumnetworks.com
common_ping: hostname www.cambiumnetworks.com
PING www.cambiumnetworks.com (141.193.213.10): 56 data bytes
64 bytes from 141.193.213.10: seq=0 ttl=57 time=26.367 ms
64 bytes from 141.193.213.10: seq=1 ttl=57 time=24.968 ms
64 bytes from 141.193.213.10: seq=2 ttl=57 time=25.795 ms
--- www.cambiumnetworks.com ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 24.968/25.710/26.367 ms
```

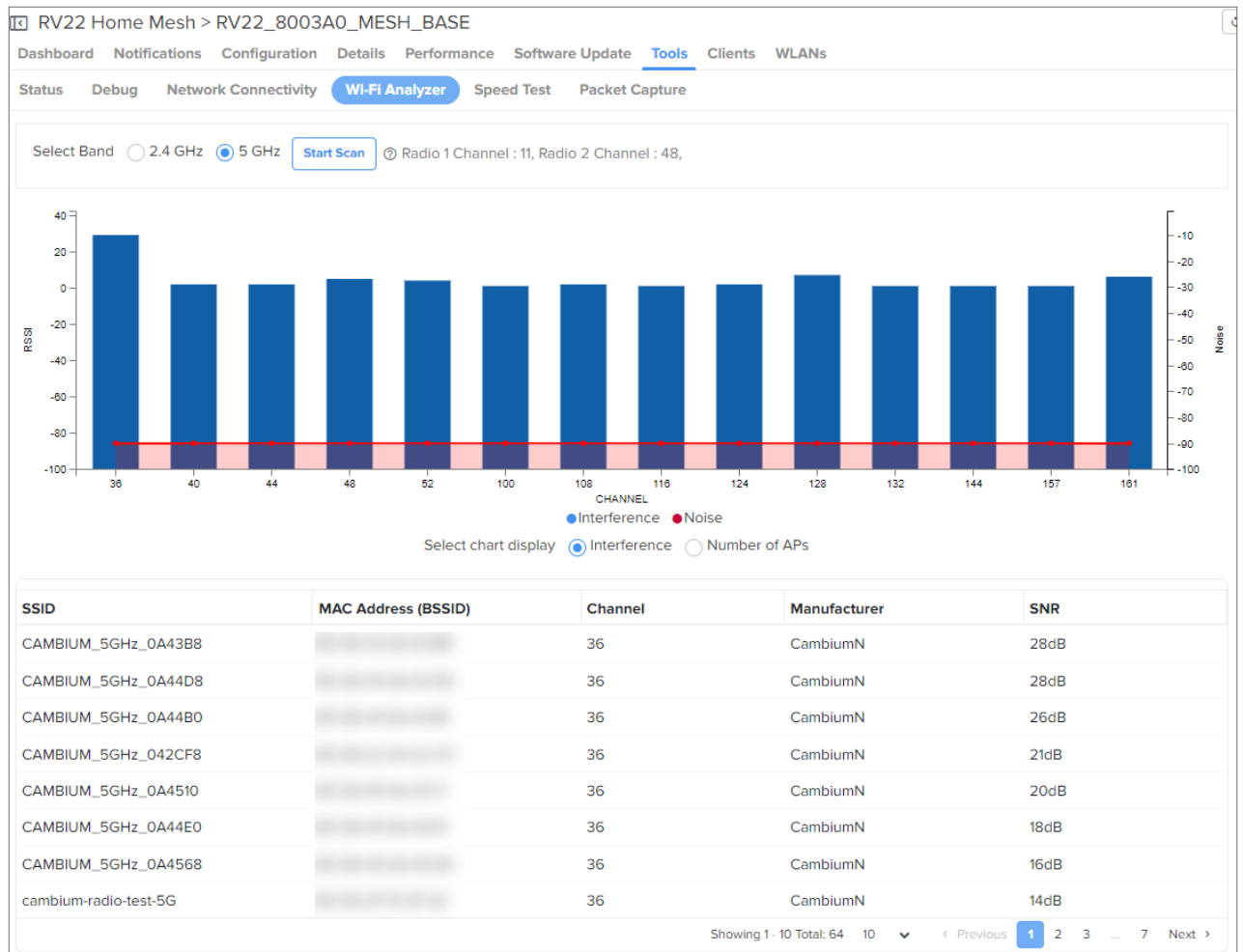
Wi-Fi Analyzer

The Wi-Fi Analyzer page displays radio traffic and signal information for the selected band. It displays the interference and noise measured for the selected band.

To view the Wi-Fi Analyzer details, complete the following steps:

1. Navigate to the **Monitor and Manage** > <Home-Mesh-Router-name> > **Tools** > **Wi-Fi Analyzer** tab.
2. Select the required band (2.4 or 5 GHz).
3. Click **Start Scan**.

cnMaestro analyzes the band and displays the result in a table.



Speed Test

The Speed Test page displays the internet speed provided by the Home Mesh Router.

To know the speed of the router, complete the following steps:

1. Navigate to the **Monitor and Manage** > <Home-Mesh-Router-name> > **Tools** > **Speed Test** tab.
2. Configure the required values for testing the speed.
3. Click **Start Speed Test**.

cnMaestro checks the speed and displays both download and upload speeds in megabits per second (Mbps).

The screenshot shows the 'Speed Test' configuration page in the cnMaestro interface. The breadcrumb trail at the top is 'RV22 Home Mesh > RV22-Mesh-Client-Terrace'. The main navigation bar includes 'Dashboard', 'Notifications', 'Configuration', 'Details', 'Performance', 'Software Update', 'Tools' (which is active), 'Clients', and 'WLANS'. Below this, a sub-navigation bar shows 'Status', 'Debug', 'Network Connectivity', 'Wi-Fi Analyzer', 'Speed Test' (which is active), and 'Packet Capture'. The configuration area contains four input fields: 'Duration (Seconds)' with a value of 15 and a range of 'Min = 1, Max = 60'; 'Parallel Streams' with a value of 3 and a range of 'Min = 1, Max = 10'; 'Download Size (MB)' with a value of 20 and a range of 'Min = 1, Max = 1000'; and 'Upload Size (MB)' with a value of 20 and a range of 'Min = 1, Max = 1000'. At the bottom left of the configuration area is a blue button labeled 'Start Speed Test'.

The speed test option is also available on the **Subscriber** page in the **Home Wi-Fi Devices Setting Override** section.

To avail this speed test option, complete the following steps:

1. Navigate to the **Manage Service Providers > Managed Subscribers > Subscribers** tab.
2. From the list of subscribers, click the subscriber name for which you want to configure the speed test.
The **Edit <Subscriber-name>** window is displayed.
3. Click the **Service Configuration** tab.
4. In the **Home Wi-Fi Devices Setting Override** section, click the **Speed Test** tab.

[Subscribers](#) > Edit Subscriber

Basic Information
Service Configuration
Devices

Subscriber Service Profile*
tesr-service-profile
Download (Mbps)*
123
Upload (Mbps)*
345
AP Group
Test12

Home Wi-Fi Devices Setting Override

Radio
Network
WLANs
Speed Test
Management

☐ Schedule Background Testing

Options

Duration
15
Seconds (between 1 and 60)
Parallel Streams
3
No of parallel streams to run the test (between 1 and 10)
Download Size
20
Upload Size
20
MB (between 1 and 10000)

Save
Close

- To schedule the speed test at a particular duration, select the **Schedule Background Testing** checkbox.
- Select the start and end time for performing the speed test on the router.

Radio
Network
WLANs
Speed Test
Management

☒ Schedule Background Testing

Between
01:00 AM
to
04:00 AM


Packet Capture

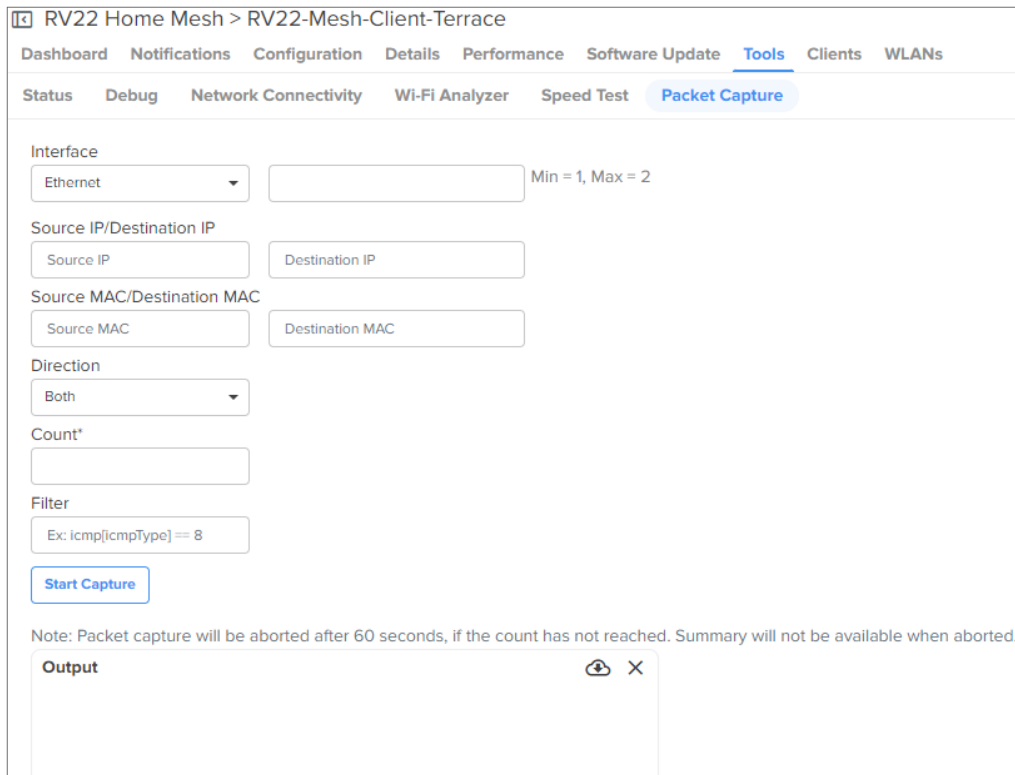
The Packet Capture page allows the user to capture all packets on a specified interface.

To capture packet data, complete the following steps:

- Navigate to the **Monitor and Manage** > <Home-Mesh-Router-name> > **Tools** > **Packet Capture** tab.
- Select the required interface, and provide the source and destination IP address or MAC address.
- Provide the number of packets that must be captured.
- Click **Start Capture**.

cnMaestro displays the information in the **Output** window.

5. To download the PCAP file, click the download () icon.



Upgrading the Home Mesh Router firmware

To upgrade the firmware of Home Mesh routers present in a home site, complete the following steps:

1. Navigate to **Monitor and Manage** > <Home-site-name> > **Software Update**.
The Software Update page appears.
2. Select **RV22 Home Mesh** from the **Device Type** dropdown list.
3. Select the software version from the **Versions** dropdown list.
4. In the list of devices table, select the checkboxes corresponding to the devices for which you want to upgrade the firmware.

You can also select one router to upgrade the firmware of only that router.

5. Select the **Now** option in the **Update** field to upgrade the firmware immediately.
To schedule the upgrade job, select the **Schedule** option and configure the required date and time.
6. Click **Add Software Job to** <number of devices> **device(s)**.
The upgrade is scheduled to run at the specified date and time.

To view the status of the update jobs, click **View Update Jobs**.

Home Site > -Home

Dashboard

Notifications

Configuration

Software Update

Clients

Device Type

RV22 Home Mesh

Versions

1.0.0-b21 (Recommended) (Beta)

Search

<input type="checkbox"/> Devices	Managed Account	Status	Running Version	Downloaded Version
<input type="checkbox"/> RV22-Mesh-Client-First-Floor	Base Infrastructure	Online	1.0.0-b21	1.0.0-b20_1012_1
<input type="checkbox"/> RV22-Mesh-Base-Foyer	Base Infrastructure	Online	1.0.0-b21	1.0.0-b20_1012_1
<input type="checkbox"/> RV22-Mesh-Client-Terrace	Base Infrastructure	Online	1.0.0-b21	1.0.0-b20_1012_1

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

Update

☒ Now ☐ Schedule

Job Options

10

Devices to update in parallel (1-100).

☐ Retry skipped/offline device(s) on reconnect

Notes

Add Software Job to 0 device(s)

[View Update Jobs](#)

Assurance X

This chapter covers the following topics:

- [Site-level Assurance](#)
- [Client-level Assurance](#)

Analyzing Connection Failures of Wi-Fi Clients and Poor Performance of Wi-Fi Networks

The Wi-Fi Assurance X feature provides deep visibility into the health of Wi-Fi client connections, including root cause analysis of failures and possible remediations. It also provides analytics on aggregated data that can help to improve client connectivity in the Wi-Fi network.

This section covers the following topics:

- [Overview](#)
- [Use cases](#)
 - [Resolve connectivity issues](#)
 - [Address poor performance of applications](#)
 - [Identify OS, SSID, and AP-specific issues](#)
- [Accessing the Assurance X page](#)
- [Accessing Site-level consolidated details at the System- and MSP-levels](#)
- [Setting filters to view the connection data](#)
- [Viewing the connection events](#)
 - [Dashboard page](#)
 - [Assurance X page](#)
 - [Connection tab](#)
 - [Disconnection tab](#)
 - [Viewing a client or host-specific connection or disconnection event](#)
 - [Viewing an event-based connection or disconnection event](#)
 - [Viewing AP-specific information](#)

Overview

The Assurance X 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 failures.
- **Poor Performance**—Low RSSI, low data rate, high retry rate, and high latency in AAA, DHCP, DNS, and applications.

You can use this feature to detect and analyze common network problems that occur in your wireless networks.

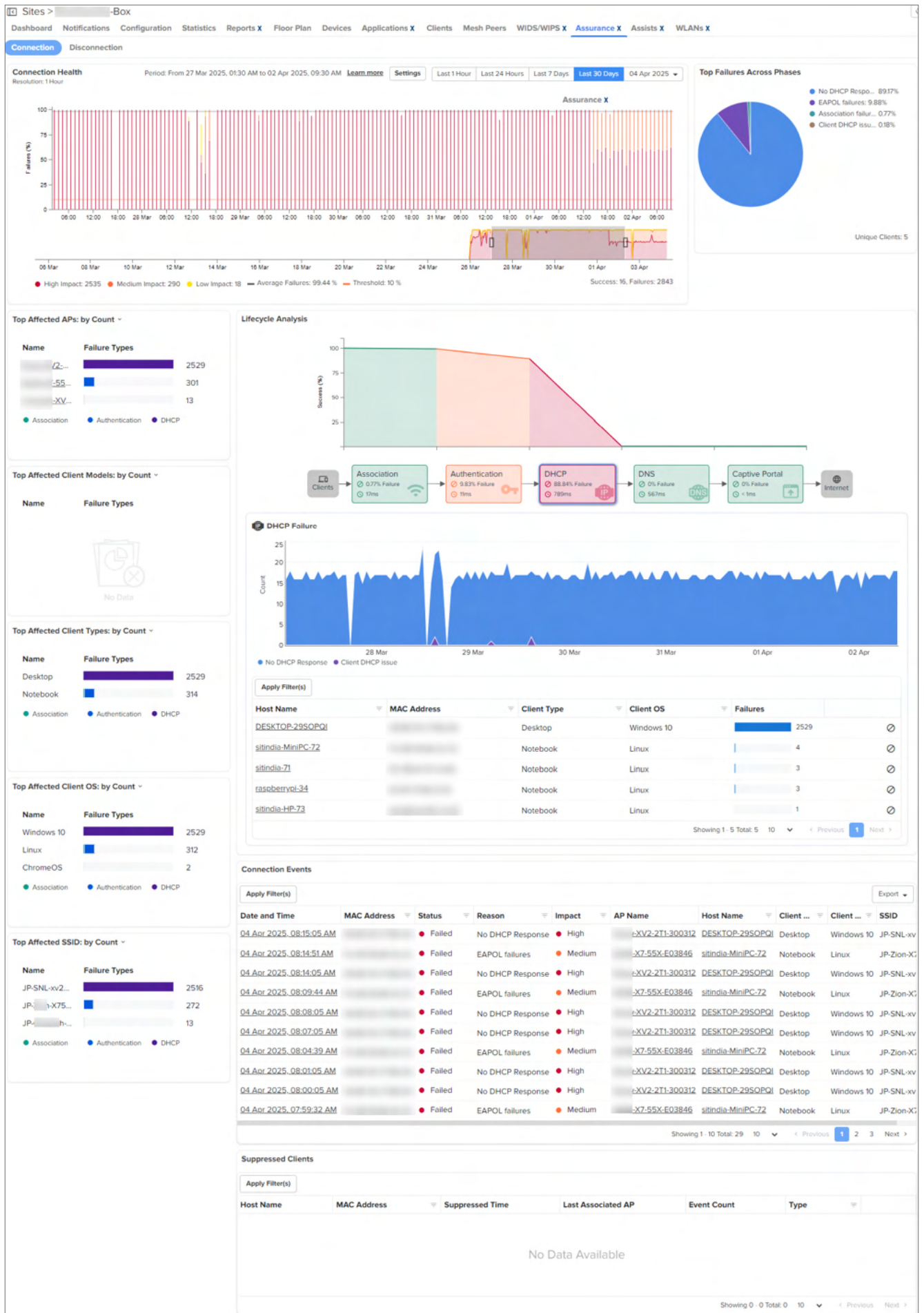
**Note**

Assurance X is supported only for XV and XE devices.

The **Assurance X** page reports the following data for the Wi-Fi clients:

- Statistics of successful connections per connection type such as new, reconnection, and roaming.
- Statistics of failed connections and disconnections, such as reason codes for association, EAP/EAPOL handshake, DHCP, DNS, and Captive Portal failures.

Figure 502 *The Assurance X page*



Use cases

Following are some of the **use cases**, to identify the connectivity issue and analyze the root cause:

Resolve connectivity issues

The **Assurance X** page provides visual analytics of client connection failures in each phase such as baseline performance and key metrics in the form of graphs and tables with multiple data filters. You can easily identify the root cause based upon the phase of the Wi-Fi connection lifecycle.

- **Association**—Accessing the AP may fail if the client has low RSSI; if the request for capabilities is not supported by the AP; or if the AP is already handling the maximum number of clients.
- In such cases, you can use the **Lifecycle Analysis** widget on the **Assurance X** page. This widget displays the statistics of 802.11 authentication and association failures in percentage. In addition, you can use the **Events** page to analyze the reason, cause, impact, and the recommended action.
- **Authentication**—Authentication may fail when 802.1X or EAP key is incorrect; the RADIUS server cannot be reached; or the WPA2-PSK or WPA3-SAE key derivation is invalid.
- In such cases, the **Lifecycle Analysis** widget displays the RADIUS authentication failure count in percentage.
- **Network connection**—When a client is successfully authenticated, it must be assigned an IP address by the DHCP server and provided networking information such as for DNS and Gateway. When the DHCP server fails, connectivity to the network cannot be established.
- In such cases, the **Lifecycle Analysis** widget can help identify that the DHCP server failure, and the **Events** page can analyze the reason and cause.
- **Aggressive roaming**—Time sensitive applications such as voice and video require uninterrupted connectivity. To ensure this, Wi-Fi clients monitor the RSSI from local APs and probe better APs when the connection degrades. The RSSI threshold at which a client moves from the current AP to another AP may be different for each client and is vendor specific. Some clients may have aggressive roaming where they move frequently across APs. This can result in increased contention in the network and longer delay for other clients connecting or transmitting data. The client drill down presents the association, authentication, and network connectivity events generated due to aggressive roaming.
- You can use the **Lifecycle** page to analyze the RSSI ranges, roam quality, and lifecycle events.
- **DHCP, AAA, or DNS latency**—Each of the association, authentication, and network connectivity stages might add latency to the total connection time.
- The **Lifecycle Analysis** widget and the **Events** page display statistics for the DHCP, AAA, and DNS latencies.

Address poor performance of applications

Wi-Fi clients may use a wide range of advanced video coding (AVC) applications such as Google Meet, Microsoft Teams, Zoom, Skype, YouTube, and multiple e-commerce applications such as Flipkart and Amazon. In such scenarios, clients may experience poor network performance or network disconnection due to low RSSI or bad roam quality.


You can view the **Session Timeline** section in the **Lifecycle** page to analyze the RSSI ranges, and events such as success, failed, connected, disconnected, and roam quality. This analysis helps you to understand the cause and take recommended actions.

Identify OS, SSID, and AP-specific issues

Apart from run-time metrics, the **Connection Health** widget provides filters to identify performance issues with a specific vendor, operating system, and associated AP and SSID.

Accessing the Assurance X page

To access the Assurance X page:

1. On the left navigation pane, click the **Monitor and Manage** () icon.
2. In the **Networks** tab, select either a **System**, **MSP**, or **Network**, and then a **Site** node in the tree.



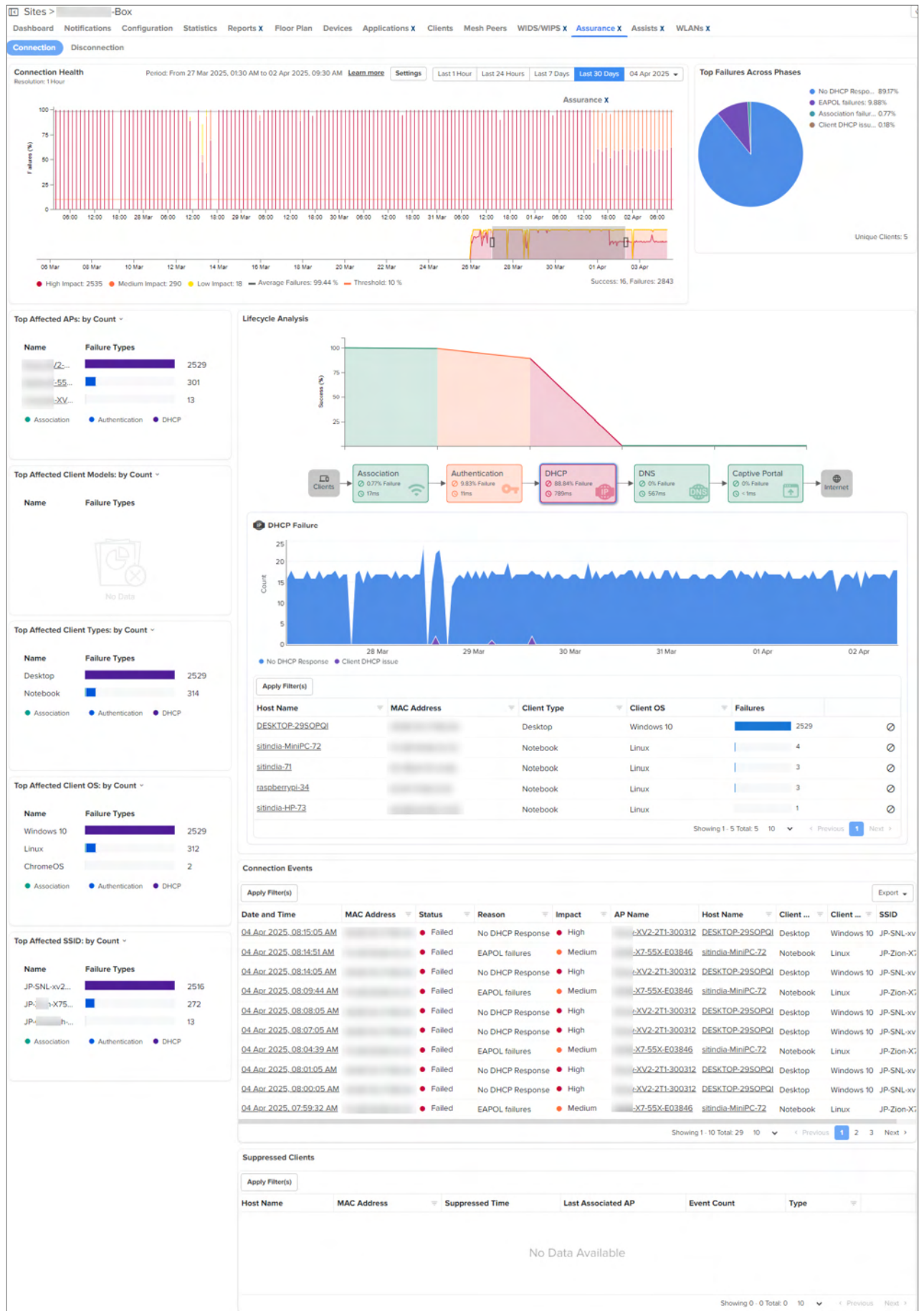
Note

The **Assurance X** page is available only at the site and client levels.

The **Dashboard** tab displays the default Wi-Fi connection statistics.

3. Click the **Assurance X** tab.

The **Assurance X > Connection** page is displayed.



Accessing Site-level consolidated details at the System- and MSP-levels

cnMaestro allows you to access consolidated information from all sites located in an account- or at the MSP-level. The information is displayed in a tabular format including details, such as the Managed Account name, the network to which the site belongs, failure threshold and what percentage of events have crossed this threshold, and the high, medium, and low impact events.



Note

Consolidated information from all sites at the System- and MSP-levels are available only for those sites where devices are onboarded and clients are connected.

To view consolidated site-level information, complete the following steps:

1. Navigate to **Monitor and Manage**.
2. In the **Networks** tab, select one of the following options:
 - To view account-level information, click **System** > **Assurance X**.

The **Assurance X** page is displayed with consolidated information from all the sites in that account. At the system-level, data is aggregated from all sites including sites under MSP accounts. However, at the MSP-level, data is aggregated from only those sites under the MSP account.

Figure 503 System-level information from all sites and MSP accounts

Site	Network	Managed Account	Failure Threshold	Above Failure Threshold	High Impact	Success	Connection Summary	Most Failures
Regression Rack	JP-Wi-Fi-SIT	Base Infrastructure	10%	Yes (100%)	4 (100%)	0 (0%)	4	Authentication (50%)
MSP_Site2	MSP_Network1	_MSP	10%	Yes (99.12%)	4490 (98.36%)	40 (0.88%)	4565	Authentication (98.42%)
Smartworks-Box	JP-Wi-Fi-SIT	Base Infrastructure	10%	Yes (98.26%)	4187 (77.45%)	94 (1.74%)	5406	DHCP (81.24%)
RCA_Site2	Megha_Network	Base Infrastructure	10%	Yes (95.19%)	7848 (77.79%)	485 (4.81%)	10089	Authentication (57%)
_Site	Megha_Network	Base Infrastructure	10%	Yes (95.17%)	3597 (93.48%)	186 (4.83%)	3848	Captive Portal (93.43%)
MSP_Site3	MSP_Network2	_MSP	10%	Yes (88.37%)	263 (72.85%)	42 (11.63%)	361	Authentication (75.9%)
RCA_Site1	Megha_Network	Base Infrastructure	10%	Yes (87.98%)	10879 (86.69%)	1509 (12.02%)	12550	Authentication (73.16%)
_Site	default		10%	Yes (86.21%)	25 (86.21%)	4 (13.79%)	29	Captive Portal (82.76%)
MSP_Site1	MSP_Network1	_MSP	15%	Yes (85.01%)	6596 (83.75%)	1181 (14.99%)	7876	Authentication (61.77%)
Viky-Regression-Setup	Viky-SIT	Base Infrastructure	10%	Yes (78.02%)	252 (78.02%)	71 (21.98%)	323	DHCP (77.09%)

- To view MSP-level information, click **<MSP-Name>** > **Assurance X**.

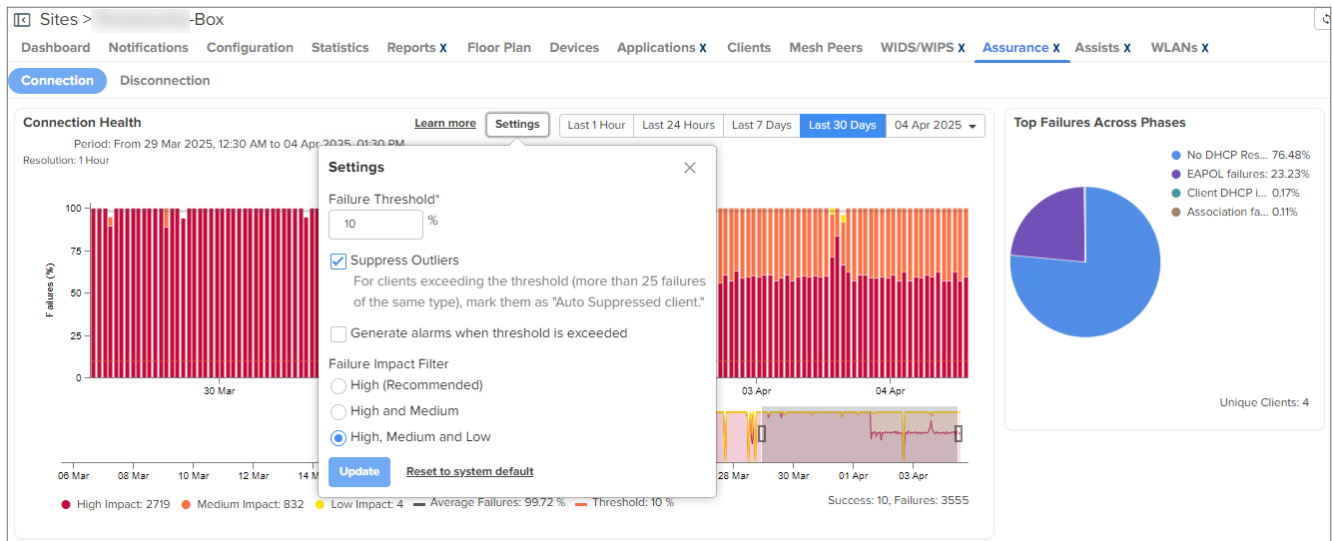
The **Assurance X** page is displayed with consolidated information about from all the sites in that account.

Figure 504 MSP-level information from all sites in that MSP

Site	Network	Managed Account	Failure Threshold	Above Failure Threshold	High Impact	Success	Connection Summary	Most Failures
MSP_Site1	MSP_Network1	_MSP	15%	Yes (42.7%)	18 (20.22%)	51 (57.3%)	89	Association (33.71%)

Setting filters to view the connection data

After accessing the **Assurance X** page, you may change the default threshold for failed connections and set the period to view the connection events such as 1 hour, 24 hours, 7 days, or 30 days.



To set failure threshold and period:

1. Navigate to the **Connection** tab
2. Click **Settings** located inside the **Connection Health** widget.
3. Enter the **Failure Threshold**.

The default value is 10% and higher. To reset the threshold, click **Reset to system default**.

4. Select or clear the **Suppress Outliers** checkbox to exclude or include, respectively, the suppressed clients from the **Connection Health** dashboard.

When enabled (by default), cnMaestro suppresses or excludes those clients that are repeatedly generating the same type of failures from the **Connection Health** dashboard.

For more information about suppressed clients, see [Suppressed clients](#).

5. Select the **Generate alarms when threshold is exceeded** checkbox to generate a System Alarm whenever the threshold is surpassed.
6. Select the **Failure Impact Filter** as one of the following options:
 - High (Recommended)
 - High and Medium
 - High, Medium and Low

Default value: **High (Recommended)**

7. To apply the configuration changes, click **Update**.
8. To view the connection or disconnection events for a specific period, click one of the following options:
 - Last 1 Hour
 - Last 24 hours (Resolution 1 Hour)
 - Last 7 days (Resolution 1 Hour)
 - Last 30 days (Resolution 1 Hour)—Data is available for the last 30 days. However, at any instance the data displayed in the **Connection Health** graph is for a maximum of seven days only.

The smaller graph below the main graph displays data for the last 30 days. Set the duration by dragging the time range selector as shown in the following figure.

Minimum days to be selected in the selector is one. Maximum is seven days.

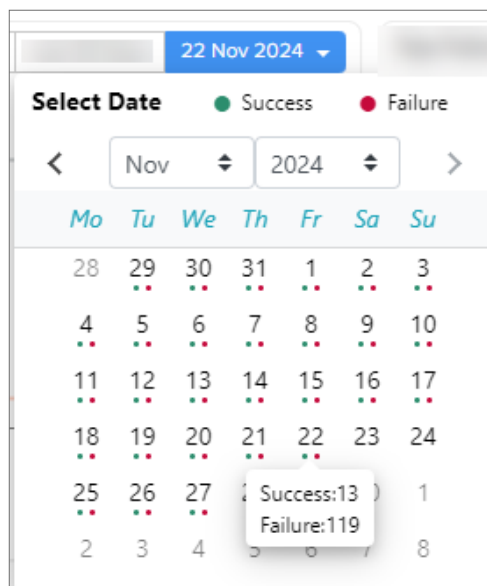


- **Date**—To view the connection or disconnection data for a specific date, select the required date from the date picker.

You can select a date upto last 30 days.

In the date picker dropdown, hover over a date to view the success and failure counts on that date.

Figure 505 *Date picker*



Based on the failure threshold, failure Impact filter, and the period, the **Dashboard** and **Assurance X** pages display the Wi-Fi client's connection data. Whenever the failure percentage exceeds the configured failure threshold, the Assurance X page automatically generates alerts.



Note

Consider the following key points specific to impact level failures:

- **High impact failure**—Occurs when a client is unable to establish a connection with an access point or transmit data over a connection. These failures are typically permanent until the underlying problem is resolved. High impact failures include incorrect pre-shared key (PSK); the VLAN not being configured or present on the switch; and AP software issues.
- **Medium impact failure**—Occurs when a client is intermittently unable to connect to a network, and the time to connect is relatively short (sub-seconds). These failures may not be noticed by end users. They are caused by transient issues such as the moving client or when an access point locks the necessary information during the initial connection attempt. Medium impact failure events include fast transition (FT); authentication failure; missed packets during the four-

way handshake; DHCP request process; or momentary interference from other wireless devices.

- **Low impact failure**—Occurs when a client is unable to connect to a network, without causing any noticeable impact for end users. These failures may arise due to specific wireless LAN features or configurations, such as band steering. These failures are expected, based upon the Wireless LAN protocols, and do not impact the user experience. In some cases, adjusting WLAN configuration can resolve such failure issues.

Suppressed clients

When a client attempts to connect to an AP, failures may occur. If a few clients repeatedly experience the same failure, they can disproportionately increase the overall failure percentage in site-level analytics, leading to misleading data. To address this, cnMaestro classifies such clients as suppressed clients and exclude their failure events from the site-level analytics data.

This section describes the following topics:

- [Classifying clients as suppressed](#)
- [Viewing suppressed clients and events](#)
- [Removing a manually suppressed client from the Suppressed Clients list](#)

Classifying clients as suppressed

Clients can be classified as suppressed clients in one of the following ways:

- **Automatically suppressed clients**—When a client generates the same failure event more than 25 times within one hour, cnMaestro automatically classifies the client as Auto Suppressed client and adds it to the Suppressed Clients list.

To enable automatic suppressing of clients, select the **Suppress Outliers** checkbox in the **Connection Health** dashboard > **Settings** window.



Note

This setting is enabled, by default, for all sites in an account.

Settings

Failure Threshold*

10 %

☒ Suppress Outliers
For clients exceeding the threshold (more than 25 failures of the same type), mark them as "Auto Suppressed client."

☐ Generate alarms when threshold is exceeded

Failure Impact Filter

☐ High (Recommended)

☐ High and Medium

☒ High, Medium and Low

Update [Reset to system default](#)

An auto suppressed client remains in the Suppressed Clients list as long as it generates the same failure event. The auto suppressed client cannot be manually removed from the Suppressed Clients list. An auto suppressed client is automatically removed from the Suppressed Clients list when the client:

- generates a success event, or
- generates a different failure event, or

- does not generate any event for one hour
- Manually suppressed clients—A user manually classifies a client that generates a failure event multiple times, as suppressed.

To manually classify a client as suppressed, click the **Mark as suppressed** (🔒) icon, available for clients listed in the site **Assurance X** page > **Lifecycle Analysis** widget.



Note

- Only successful events generated by manually suppressed clients are included in the site-level analytics data. However, a successful event does not remove the client from the Suppressed Clients list.
- For removing the manually suppressed clients from the Suppressed Clients list, see [Removing a manually suppressed client from the Suppressed Clients list](#).
- All failure events generated by manually suppressed clients are discarded from the site-level analytics data.


Viewing suppressed clients and events

Suppressed clients and the corresponding failure events are displayed in the following pages in cnMaestro:

- Site > **Assurance X** > **Connection** dashboard—under the **Suppressed Clients** table—Lists all clients that are suppressed either automatically or manually.


Suppressed Clients						
Apply Filter(s)						
Host Name	MAC Address	Suppressed Time	Last Associated AP	Event Count	Type	
		04 Apr 2025, 05:14:17 PM	XV2-2-64996B-site6	3	Manual	
Showing 1 - 1 Total: 10 < Previous 1 Next >						

The details of the list are described in the following table:

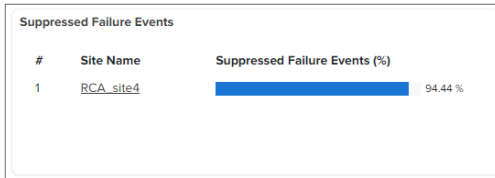
Filter name	Description
Host Name	Host name of the suppressed client.
MAC Address	MAC address of the suppressed client.
Suppressed Time	Timestamp when the client was suppressed.
Last Associated AP	Host name of the AP to which the suppressed client was last associated with.
Event Count	Number of failure events that were suppressed.
Type	Specifies the type of suppression of the client. The following values are displayed: <ul style="list-style-type: none"> Auto—Client is suppressed automatically Manual—Client is suppressed manually
	Allows to remove the manually suppressed clients from this list.

- Client's **Dashboard X** tab

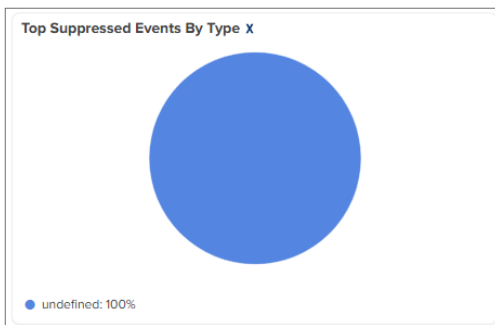
- Client Details** section—Displays if the client is suppressed or not in the selected site. If suppressed, it also displays if it suppressed automatically or manually.

Site > RCA_site4 > Clients (30 Days) >	
Dashboard X Applications X Performance X Lifecycle X	
Failure Impact Filter:	High (Recommended)
Time Range:	Last 30 Days
Connection	Reassociations
 Disconnected	1
N/A	Different APs
Client Details	
Name	
IPv4 Address	172.40.0.179
IPv6 Address	-
MAC Address	
Manufacturer	
Type	
Model	
Operating System	Linux
OS Version	
Last Seen	04 Apr 2025, 05:59 PM
Capability	
Suppression Type	Yes (Manual)

- **Suppressed Failure Events** widget—Displays the percentage of suppressed failure events for each of the sites that the client is associated with.



- **Top Suppressed Events By Type X** widget—Displays the top events that were suppressed categorized by the event type.



- **Lifecycle Events X** section > **Suppressed** column—This column displays if the failure event is a suppressed event or not. If yes, then it also displays if it is an event generated by an automatically suppressed client or a manually suppressed client.

The same information is also displayed in the Client's **Lifecycle X** tab.

Lifecycle Events X

Apply Filter(s)

Export

Timestamp	Type	Status	Im...	AP Name	IPv4 Add...	Radio ID	Band	RSSI	Session Duration	Total Bytes	VLAN	Suppress...
04 Apr 2025, 05:28:26 PM	Connect	Failed	High	XV2-2-64996B	site6	2	5 GHz	-	-	-	-	Yes (Manual)
04 Apr 2025, 05:28:26 PM	Connect	Failed	High	XV2-2-64996B	site6	2	5 GHz	-	-	-	-	Yes (Manual)
04 Apr 2025, 05:26:29 PM	Connect	Failed	High	XV2-2-64996B	site6	2	5 GHz	-	-	-	-	Yes (Manual)
04 Apr 2025, 05:26:29 PM	Connect	Failed	High	XV2-2-64996B	site6	2	5 GHz	-	-	-	-	Yes (Manual)
04 Apr 2025, 05:24:31 PM	Connect	Failed	High	XV2-2-64996B	site6	2	5 GHz	-	-	-	-	Yes (Manual)
04 Apr 2025, 05:24:31 PM	Connect	Failed	High	XV2-2-64996B	site6	2	5 GHz	-	-	-	-	Yes (Manual)
04 Apr 2025, 05:22:57 PM	Connect	Failed	High	XV2-2-64996B	site6	2	5 GHz	-	-	-	-	Yes (Manual)
04 Apr 2025, 05:22:57 PM	Connect	Failed	High	XV2-2-64996B	site6	2	5 GHz	-	-	-	-	Yes (Manual)
04 Apr 2025, 05:21:12 PM	Connect	Failed	High	XV2-2-64996B	site6	2	5 GHz	-	-	-	-	Yes (Manual)
04 Apr 2025, 05:21:12 PM	Connect	Failed	High	XV2-2-64996B	site6	2	5 GHz	-	-	-	-	Yes (Manual)

Showing 1 - 10 Total: 403

10

< Previous

1

2

3

4

5

...

41

Next >

Removing a manually suppressed client from the Suppressed Clients list



Note

An auto suppressed client is automatically removed from the Suppressed Clients list when the client:

- generates a success event, or
- generates a different failure event, or
- does not generate any event for one hour

To remove a manually suppressed client from the Suppressed Clients list, complete the following steps:

1. Navigate to **Manage and Monitor** > Site > **Assurance X** > **Connection** dashboard.
2. Under the **Suppressed Clients** table, click the **Remove Suppressed Client** (🗑️) icon corresponding to the client you want to remove from this list.
3. Click **Yes** in the confirmation box.

Viewing the connection events

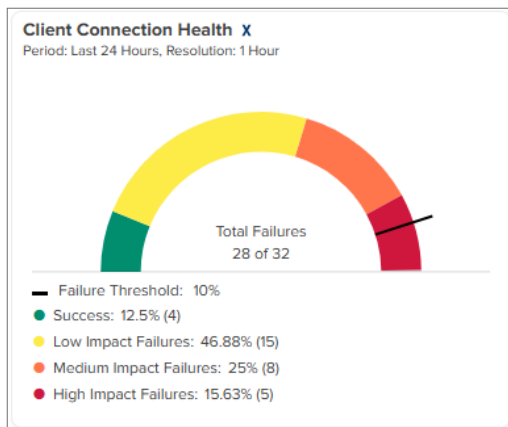
You can view and analyze the Wi-Fi connection events using the following UI pages:

- [Dashboard page](#)
- [Assurance X page](#)

Dashboard page

The site **Dashboard** page displays the following widgets:

- **Client Connection Health**—Displays overall statistics for connection events through a gauge or a dial chart. Based on the impact level filter set on the **Assurance X** > **Settings** page, this widget displays the statistics for failed connections.



Note

The default impact filter for a Site is **High**.

The resolution of this chart is 1 hour, which means every 1 hour this chart is updated. This chart displays the data based on the threshold and the impact level filter you set.

- Number and percentage of successful connections.
- Number and percentage of impact level failures for failed connections.



Note

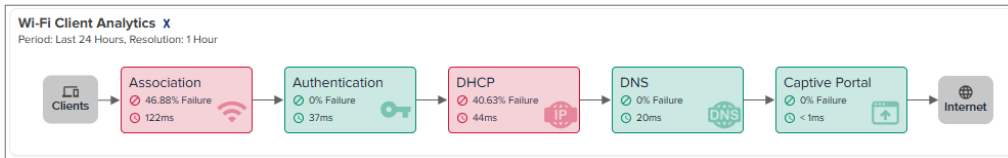
The **Client Connection Health** widget score is calculated, as follows.

$$\text{Score} = (\text{Failures} * 100) / (\text{Failures} + \text{Success}) \%$$

Depending on the selection of the impact level filter on the **Assurance X** > **Settings** page, the failure count is calculated as follows:

- **High Impact**—Includes high impact failures only.
- **High and Medium Impact**—Includes medium and high impact failures.
- **High, Medium, and Low Impact**—Includes all failures: high, medium, and low impact.

- **Wi-Fi Client Analytics X**—Indicates the percentage of failed connections at each step in the client lifecycle.



The phase-wise chart displays the current status by highlighting the phase in:

- **Red**—If the failure percentage exceeds the configured failure threshold configured in **Assurance X> Settings** page,
- **Orange**—If the failure percentage falls within the range of 80-100% of the configured failure threshold,
- **Green**—If the failure percentage is below 80% of the configured failure threshold.

The **Wi-Fi Client Analytics X** widget displays the connection state of clients to the Internet in the following phases:

- Duration in each phase indicates the average time taken by the clients in the respective phase.
- **Association**—Indicates the percentage of failed connections during the association phase.
- **Authentication**—Indicates the percentage of failed client authentications such as EAP, RADIUS, and authentication key derivation (EAPOL) failures.
- **DHCP**—Indicates the percentage of failed DHCP request or responses from or to the client.
- **DNS**—Indicates the percentage of failed DNS request or responses from or to the client.
- **Captive Portal**—Indicates the percentage of failed captive portal accesses.



Note

A captive portal is a web page launched in a browser that enables access to a public network. For example, business centers, airports, hotel lobbies, coffee shops, and other public venues use captive portals to offer free Wi-Fi hotspots for internet users.

Assurance X page

After accessing the **Assurance X** page and setting the failure threshold percentage, failure impact filter, and duration, you can analyze the connection events using the following tabs:

- [Connection](#)—Provides statistics for the connection events.
- [Disconnection](#)—Provides statistics for the disconnection events.

In addition to the data presented in the above tabs, more detailed information about the connection and disconnection events are available when you click an hour bar in the **Connection Health** or the **Disconnection** graphs. For information, refer [Viewing hourly data and corresponding events](#).



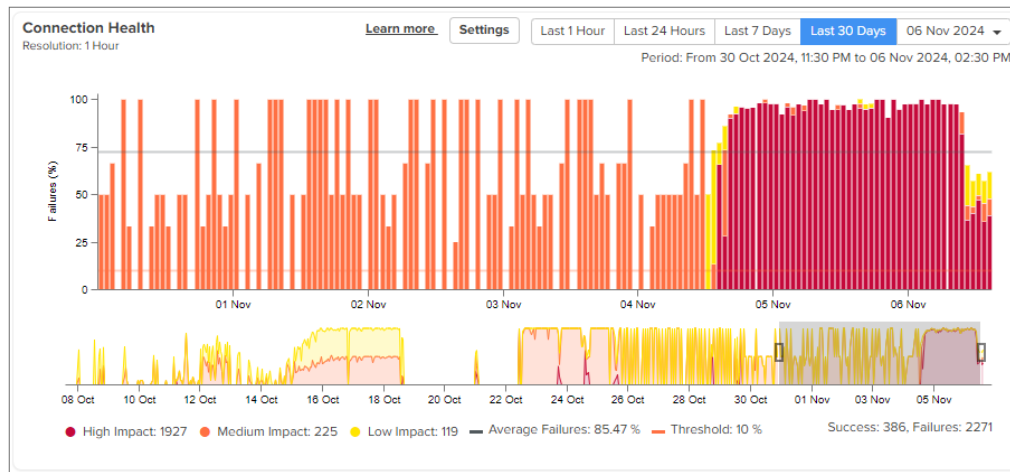
Note

The Assurance X page retains the connection and disconnection data for a maximum of 30 days.

Connection tab

Following widgets on the **Connection** tab show connection failure events for the configured duration:

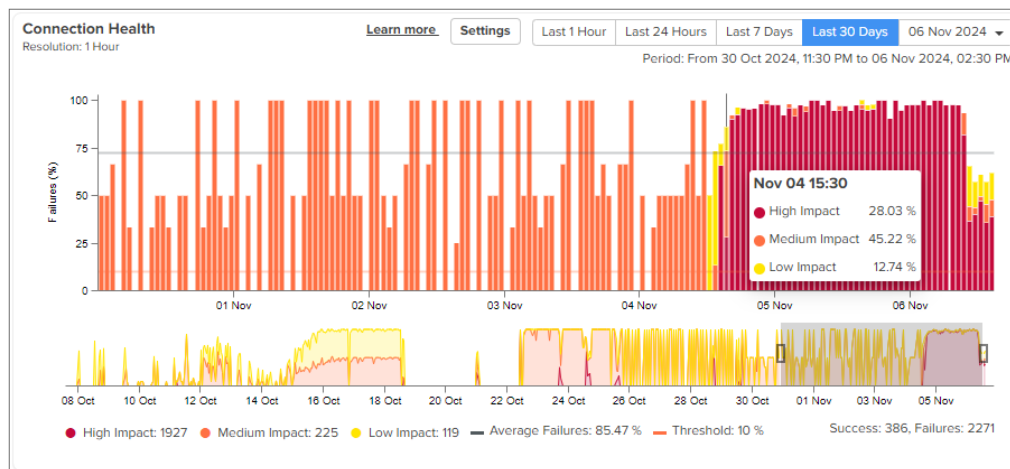
- **Connection Health**—Displays statistics of the failed connections in a bar chart, based on the threshold you set and the impact level failures in percentage.



The **Connection Health** bar chart represents the following data:

- Percentage of failed connections in a specific period for each failure impact—High, Medium, and Low.
- Percentage of average failures highlighted by a grey line.
- Percentage of high, medium, and low impacted connections in different colors.
- Failure threshold percentage configured indicated by an orange line.

To view the connection statistics for a particular date and time (at a particular hour), click on a bar in the chart, the chart displays the connection statistics for the selected date and hour.



When you click an hour bar on the **Connection Health** chart, the following widgets display failure data for that hour:

- Top Failures Across Phases
- Lifecycle Analysis
- Top Affected APs
- Top Affected Client Models
- Top Affected Client Types
- Top Affected Client OS
- Top Affected SSID
- Connection Events

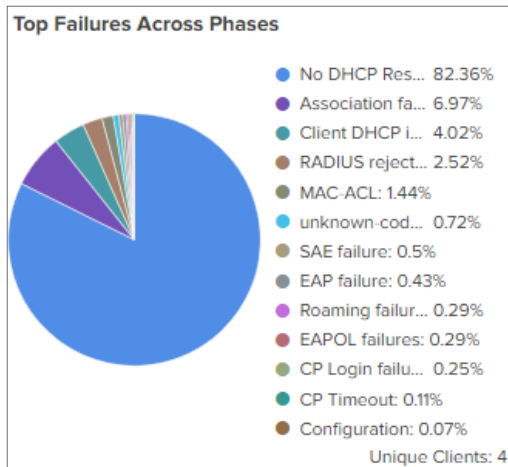
To view the events that have occurred in an hour's duration, refer <>.



Note

Click the refresh (🔄) icon, located on the top right corner of the **Assurance X** page, to refresh the page.

- **Top Failures Across Phases**—Displays statistics of top failed connections in a pie chart, indicating failure reasons across phases in percentage.



When you select any top failure slice on the pie chart, the following widgets display data for the selected top failure:

- Lifecycle Analysis
 - Top Affected APs
 - Top Affected Client Models
 - Top Affected Client Types
 - Top Affected Client OS
 - Top Affected SSID
- **Lifecycle Analysis**—Displays statistics for failed connections that help you analyze the life cycle of an event. By default, the phase with highest failure percentage is selected and highlighted.



This **Lifecycle Analysis** widget displays data through the following formats:

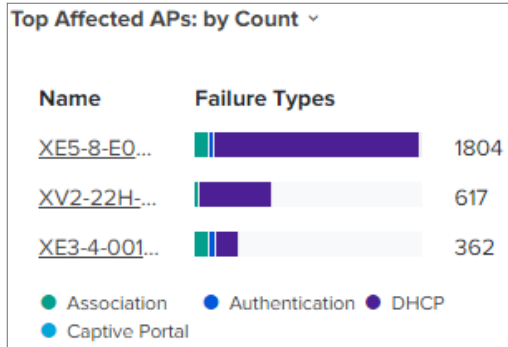
- **Phase-wise chart**—Displays the phase-wise chart that indicates the percentage of failed Wi-Fi client connections. When you click on a phase, the line graph below the phase-wise chart displays the corresponding data.
- **Line graph**—Displays the count of failed connections based on the date and time.
- Table with data corresponding to the failure selected.

The following details are displayed in the table:

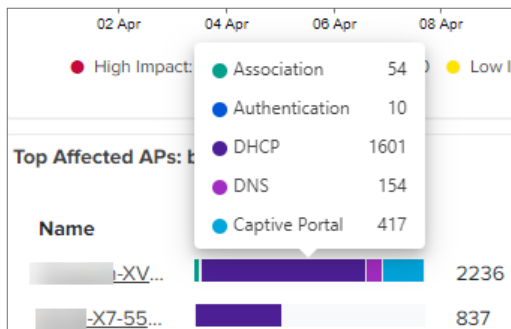
Filter name	Description
Host Name	The name of the host. Click the host name link to view the site-specific Clients page that displays the connection data for the selected host.
MAC Address	The MAC address of the client.
Client	Type of device used for the connection.

Filter name	Description
Type	
Client OS	The operating system (OS) running on the client.

- **Top Affected APs**—Displays the name of top affected APs and the statistics for the failed connection.



To view the statistics of top affected APs in percentage or count, click the collapse (▼) icon next to the widget title. Hover over on any color bar to view the failure type and the corresponding count of disconnection events. Click the link in the **Name** column to view the site-specific **Wi-Fi** dashboard with the AP information.



- **Top Affected Client Models**—Displays details of the most affected client models with the failure type.

To view the statistics of top affected client models in percentage or count, click the collapse (▼) icon next to the widget title. Hover over on any color bar to view the failure type and the corresponding count of disconnection events.

- **Top Affected Client Types**—Displays the name of top affected client types and the statistics for the failed connection.

To view the statistics of top affected client types in percentage or count, click the collapse (▼) icon next to the widget title. Hover over on any color bar to view the failure type and the corresponding count of disconnection events.

- **Top Affected Client OS**—Displays the name of top affected OS and the statistics for the failed connection.

To view the statistics of top affected client OS in percentage or count, click the collapse (▼) icon next to the widget title. Hover over on any color bar to view the failure type and the corresponding count of disconnection events.

- **Top Affected SSID**—Displays details of the most affected SSIDs with the failure type.

To view the statistics of top affected SSIDs in percentage or count, click the collapse (▼) icon next to the widget title. Hover over on any color bar to view the failure type and the corresponding count of disconnection events.

- **Connection Events : Last 1 Hour**—A table with filters displays the details of successful or failed connection events that occurred in the last one hour.



Note

Failure events per AP, Client type, and Client OS are displayed only when you click an hour bar in the **Connection Health** graph.

To use filters and view the connection details for the last one hour, perform the following steps:

1. Inside the **Connection Events : Last 1 Hour** widget, click **Apply Filters**.
2. To search and view data for the last one hour, enter one or more of the following details:

Filter name	Description
MAC Address	The MAC address of the device with connection events.
Success	Select whether you want to view successful or failed connection events. <ul style="list-style-type: none"> • Success • Failed
Reason	Select the required reason type from the dropdown list such as MAC-ACL, MAC-AUTH, QoS failure, Passpoint failure, Capability mismatch, L2 Auth failure, Association failure, Roaming failure, SAE failure, Cipher failure, or TDLS failure.
Impact	Select the required impact type from the list: <ul style="list-style-type: none"> • Low • Medium • High
Host Name	The name of the host for which you want to view the connection state.
Client Type	The type of device used for the connection.
Client OS	The operating system (OS) running on the client.

3. Click **Apply Filter(s)** to apply the changes.

The table displays the connection event details with date, time, and AP names for the searched criteria.

Connection Events									
Period: Last 1 Hour									
Change Filter(s)					Export				
Date and Time	MAC Address	Status	Reason	Impact	AP Name	Host Name	Client Type	Client OS	SSID
06 Nov 2024, 10:39:17 PM		Failed	No DHCP Resp...	High	XV2-22H-Ro...		Appliance	Other	diva_open_rca
06 Nov 2024, 10:38:16 PM		Failed	No DHCP Resp...	High	XV2-22H-Ro...		Appliance	Other	diva_open_rca
06 Nov 2024, 10:37:16 PM		Failed	No DHCP Resp...	High	XV2-22H-Ro...		Appliance	Other	diva_open_rca
06 Nov 2024, 10:36:20 P...		Failed	Association fail...	Low	XE5-8-E002...	:	Appliance	Other	diva_open_rca
06 Nov 2024, 10:36:20 P...		Failed	Association fail...	Low	XE3-4-0017E5	IN01-GJM0LR2	Notebook	Linux	diva_wpa2_ent_rca
06 Nov 2024, 10:36:20 P...		Failed	Association fail...	Low	XE5-8-E002...	:	Appliance	Other	diva_open_rca
06 Nov 2024, 10:36:20 P...		Failed	Association fail...	Low	XE5-8-E002...	IN01-9KBBGL3	Notebook	Linux	diva_wpa2_ent_rca
06 Nov 2024, 10:36:20 P...		Failed	Association fail...	Low	XE3-4-0017E5	IN01-GJM0LR2	Notebook	Linux	diva_wpa2_ent_rca
06 Nov 2024, 10:36:20 P...		Failed	Association fail...	Low	XE3-4-0017E5	IN01-GJM0LR2	Notebook	Linux	diva_wpa2_ent_rca
06 Nov 2024, 10:36:20 P...		Failed	Association fail...	Low	XE3-4-0017E5	IN01-9KBBGL3	Notebook	Linux	diva_wpa2_ent_rca



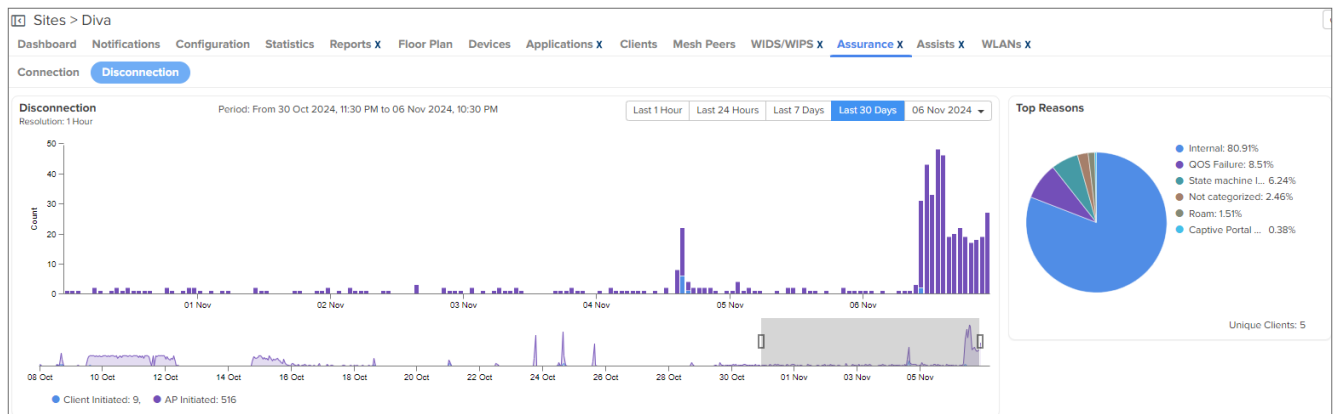
Note

You can also click the icon in the table to quickly search for status, reason, impact level, AP name, host name, client type, and client OS.

- When you click on any date and time, the **Events** page displays connection state data for the selected date and time. Refer [Viewing an event-based connection or disconnection event](#).
- When you click on any AP name, the site-specific **Wi-Fi** dashboard displays the AP or device information.
- When you click on a host name, the site-specific **Clients** page displays the connection data for the selected host.

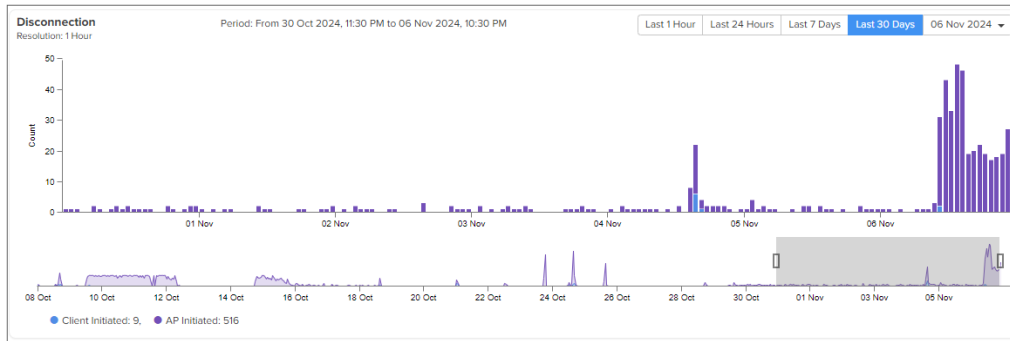
Disconnection tab

On accessing the **Assurance X** page, click on the **Disconnection** tab and set the time filter by choosing the required time period as last 1 hour, last 24 hours, last 7 days, last 30 days or select a custom date from the date picker. The **Disconnection** tab displays the data for the selected time period.



The following widgets on the **Disconnection** page support root cause analysis:

- **Disconnection**—Displays the count of client disconnections initiated by either the clients or the APs.



When you click on a bar in the chart, the chart displays the count of disconnection events initiated by the clients and the APs at the specific date and time.

Click any hour bar on the **Disconnection** chart to view the corresponding data in the following widgets:

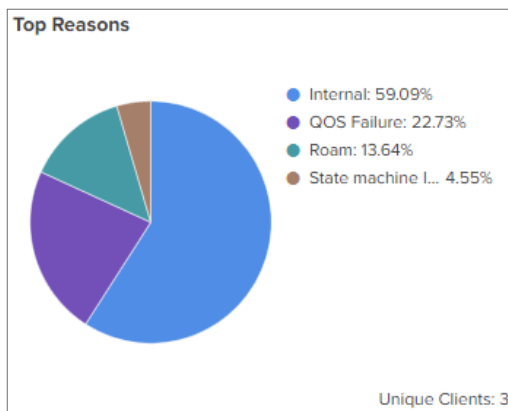
- Analytics
- Top Reasons
- Top Reporting APs by Count
- Top Reporting Client Models by Count
- Top Reporting Client Types by Count
- Top Reporting Client OS by Count
- Top Affected SSID by Count



Note

Click the refresh (🔄) icon, located on the top right corner of the **Assurance X** page, to refresh the page.

- **Top Reasons**—Displays statistics of top failure reasons such as state machine issues, roam, QoS failures, and timeout failures.




When you select any top failure slice on the pie chart, the following widgets display data for the selected top failure:

- Top Reporting APs by Count
- Analytics

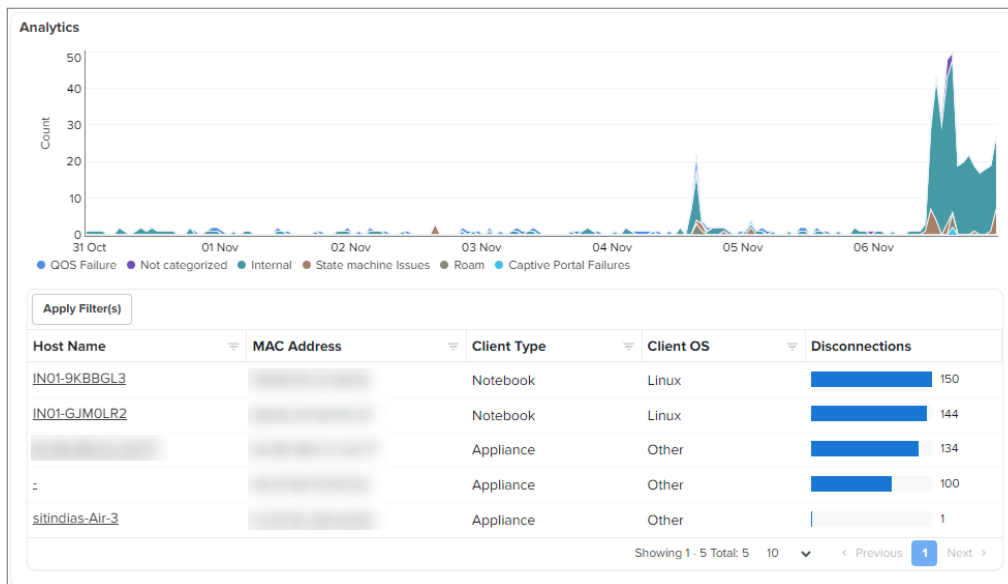
- Top Reporting Client Models by Count
- Top Reporting Client Types by Count
- Top Reporting Client OS by Count
- Top Affected SSID by Count



Note

Click the refresh () icon, located on the top right corner of the **Assurance X** page, to refresh the page.

- **Analytics**—Displays statistics for disconnections to help analyze failure events in detail.



This widget displays data in the following formats:

- **Line graph**: Displays the count of disconnections, including the date, time, and failure reasons in different colors.
- **Filters to view the required disconnection in detail**: A table with filters displays detailed information of a disconnection event.

To use filters and view the details of a disconnection event, perform the following steps:


1. Inside the **Analysis** widget, click **Apply Filters** located below the line graph section.
2. To search for and view data of the required client's disconnection state, enter one or more of the following:

Filter name	Description
Host Name	The name of the host for which you want to view the disconnection details.
MAC Address	The MAC address of the device for which you want to view the disconnection details.
Client Type	Type of device used for the connection.
Client OS	The operating system (OS) running on the client.

3. Click **Apply Filter(s)** to apply the changes.

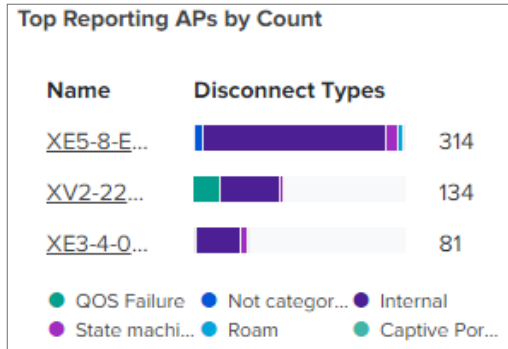


Note

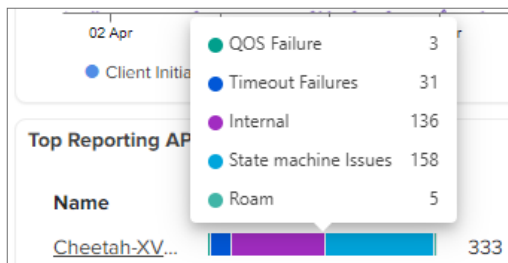
You can also click the  icon in the table to quickly search for MAC address, client type, client OS, and disconnection count.

When you click on a host name, the site-specific **Clients** page displays the disconnection state data for the selected host.

- **Top Reporting APs by Count**—Displays the names of top APs and the count of disconnections in different colors based on the disconnection types.



Hover over on any color bar to view the failure type and the corresponding counts of disconnection events.



- **Top Reporting Client Models by Count**—Displays the names of the top device model names and the count of disconnections in different colors based on the disconnection reasons. Hover over on any color bar to view the failure type and the corresponding counts of disconnection events.
- **Top Reporting Client Types by Count**—Displays the names of the top device types and the count of disconnections in different colors based on the disconnection reasons. Hover over on any color bar to view the failure type and the corresponding counts of disconnection events.
- **Top Reporting Client OS by Count**—Displays the names of top OS and the count of disconnections. Different colors are used to highlight the disconnection reasons. Hover over on any color bar to view the failure type and the corresponding counts of disconnection events.
- **Top Affected SSID by Count**—Displays the top SSIDs and the count of disconnections in different colors based on the disconnection reasons. Hover over on any color bar to view the failure type and the corresponding counts of disconnection events.
- **Disconnect Events: Last 1 Hour**—A table with filters displays the data of disconnection events that occurred in the last one hour.

To use filters and view the disconnection state details for the last one hour, perform the following steps:

1. Inside the **Disconnection Events : Last 1 Hour** widget, click **Apply Filters**.
2. To search for and view data of the disconnection events, enter one or more of the following:

Filter name	Description
MAC Address	The MAC address of the client for which you want to view the disconnection events.
Reason	Select the type of reason from dropdown list such as Unknown-disc-O, QoS failure, Radius failures, TDLS failures, timeout failures, state machine issues, AP Resource failures, AP assisted roaming, and roam.
Host Name	The name of the host for which you want to view the disconnection state.
Client Type	Type of device used for the connection.
Client OS	The operating system (OS) running on the client.


- Click **Apply Filter(s)** to apply the changes.

The table displays the disconnection state with date, time, and AP names for the searched criteria.

Disconnect Events							
Period: Last 1 Hour							
Apply Filter(s)						Export ▾	
Date and Time	MAC Address	Reason	AP Name	Host Name	Client Type	Client OS	SSID
06 Nov 2024, 10:53:41 PM		Internal	XE5-8-E002A0	IN01-GJM0LR2	Notebook	Linux	diva_wpa2_ent_rca
06 Nov 2024, 10:48:36 PM		Internal	XE3-4-0017E5	IN01-GJM0LR2	Notebook	Linux	diva_wpa2_ent_rca
06 Nov 2024, 10:44:06 PM		Roam	XE5-8-E002A0	IN01-GJM0LR2	Notebook	Linux	diva_wpa2_ent_rca
06 Nov 2024, 10:43:23 PM		State machin...	XE3-4-0017E5	IN01-GJM0LR2	Notebook	Linux	diva_wpa2_ent_rca
06 Nov 2024, 10:42:54 PM		Roam	XE3-4-0017E5	IN01-9KBBGL3	Notebook	Linux	diva_wpa2_ent_rca
06 Nov 2024, 10:41:47 PM		Internal	XE5-8-E002A0	IN01-GJM0LR2	Notebook	Linux	diva_wpa2_ent_rca
06 Nov 2024, 10:37:57 PM		QOS Failure	XE5-8-E002A0	IN01-9KBBGL3	Notebook	Linux	diva_wpa2_ent_rca
06 Nov 2024, 10:37:02 PM		Roam	XE5-8-E002A0		Appliance	Other	diva_open_rca
06 Nov 2024, 10:32:16 PM		Internal	XE3-4-0017E5	IN01-GJM0LR2	Notebook	Linux	diva_wpa2_ent_rca
06 Nov 2024, 10:30:16 PM		Internal	XE5-8-E002A0	IN01-9KBBGL3	Notebook	Linux	diva_wpa2_ent_rca
Showing 1 - 10 Total: 26 10 ▾ < Previous 1 2 3 Next >							



Note

You can also click the  icon in the table to quickly search for MAC address, reason, AP name, client type, client OS, and disconnection count.

- When you click on any date and time, the **Events** page displays the disconnection state data for the selected date and time.
- When you click on any AP name, the site-specific **Wi-Fi** dashboard displays the AP or device information.
- When you click on a host name, the site-specific **Clients** page displays the disconnection state data for the selected host.

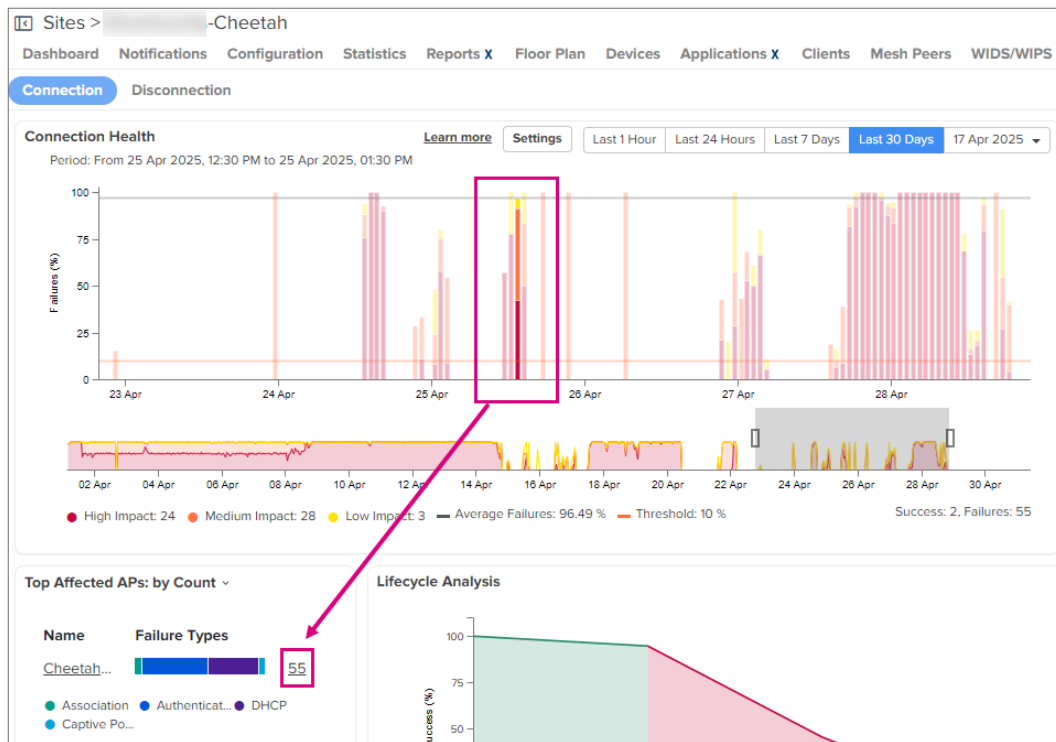
Viewing hourly data and corresponding events

When you click an hour bar in the **Connection Health** or the **Disconnection** graphs on the **Connection** and **Disconnection** tabs respectively, the following widgets display a link corresponding to the count of failures:

- Connection** tab
 - Top Affected APs
 - Top Affected Client Models

- Top Affected Client Types
- Top Affected Client OS
- Top Affected SSID
- **Disconnection** tab
 - Top Reporting APs by Count
 - Top Reporting Client Models by Count
 - Top Reporting Client Types by Count
 - Top Reporting Client OS by Count
 - Top Affected SSID by Count

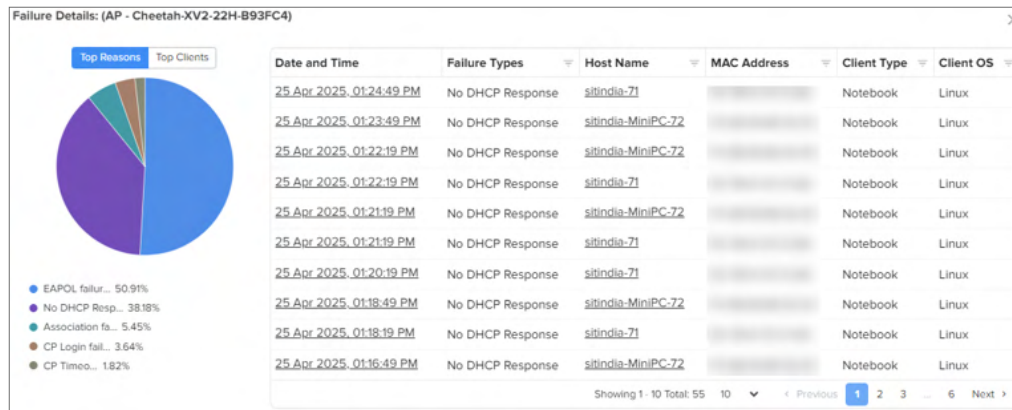
For example,



To view failure details for the corresponding entity depending on the widget you click the link, perform the following steps:

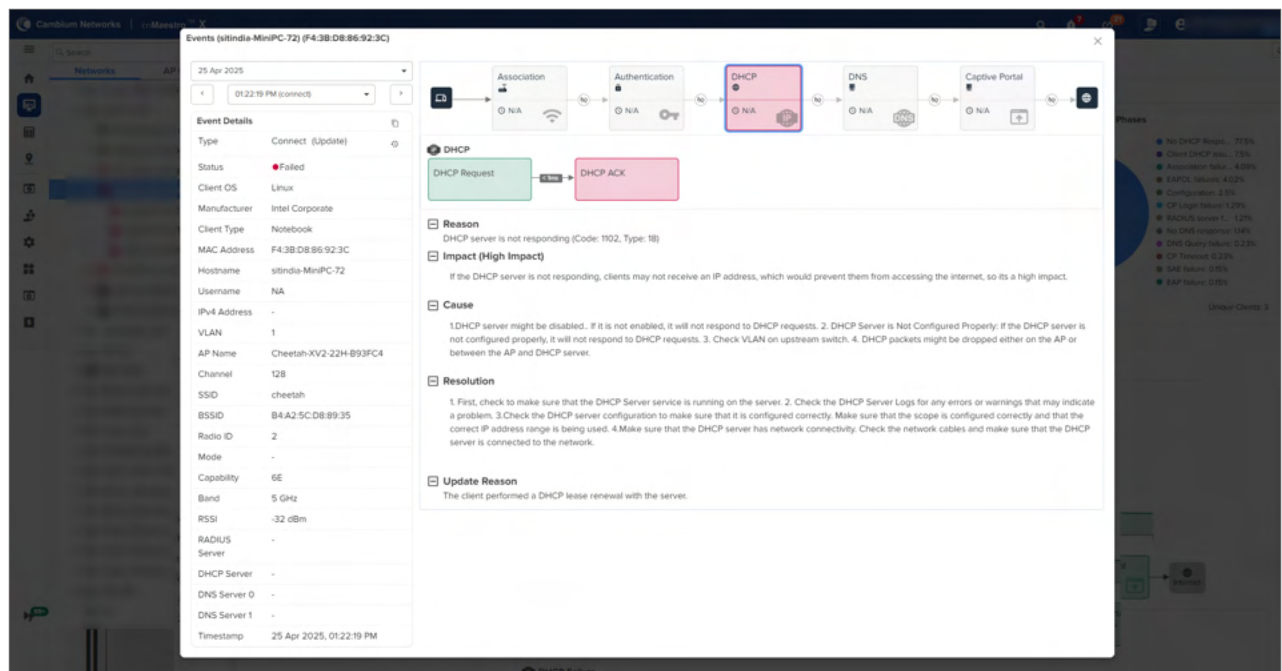
1. Navigate to **Site > Assurance X > Connection** or **Disconnection** tab.
2. In the **Connection Health** or the **Disconnection** widget, select the time duration for which you want to view the data.
3. In the bar graph, click an hour bar.
4. In the widgets listed above, click the link corresponding to the failure count or percentage.

The **Failure Details** page is displayed.



5. From the **Date and Time** column, click any timestamp link to view the event details.

For more information, refer [Viewing an event-based connection or disconnection event](#).



Viewing a client or host-specific connection or disconnection event

You can analyze client or host-specific connection or disconnection events in detail and take appropriate actions.

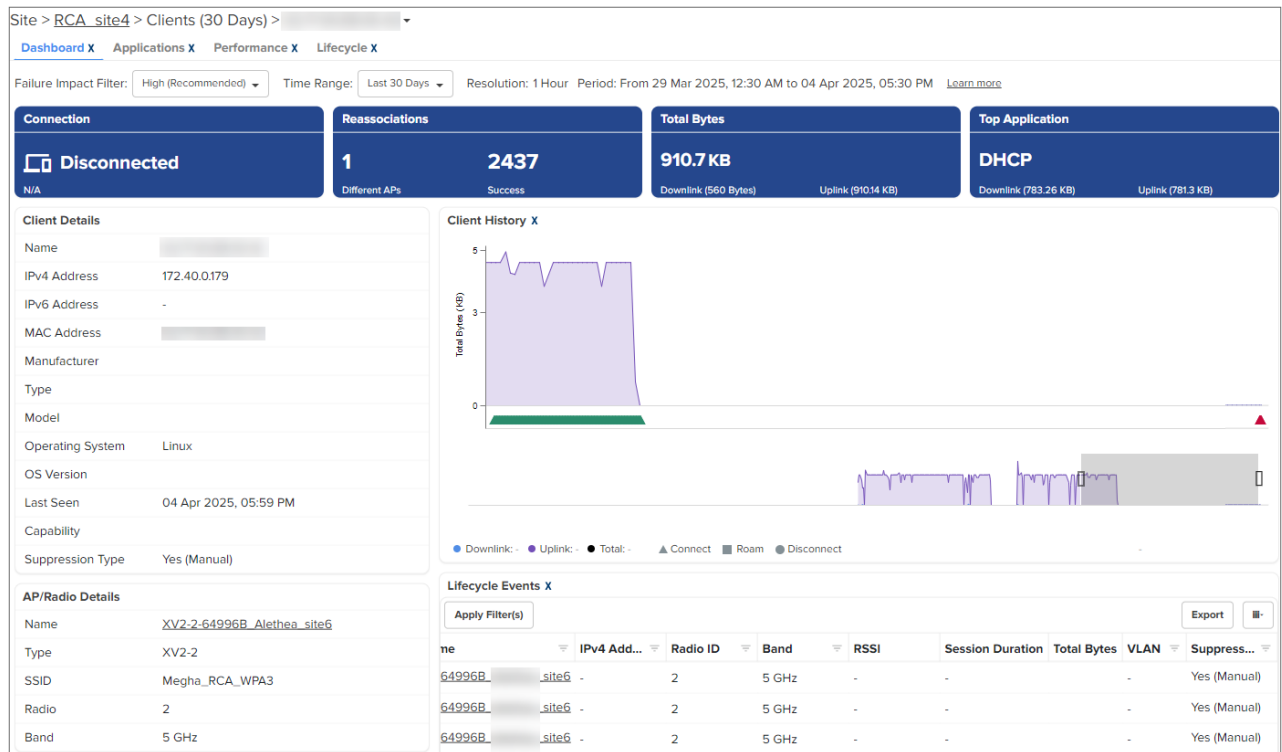
To view client or host-specific information, perform the following steps:

1. Click on a host name to view the connection or disconnection state in detail.

You can locate the host names in the following widgets:

- **Lifecycle Analysis** on the Connection page—host names are available in a table below the line graph section.
- **Connection Events: Last 1 Hour** on the Connection page.
- **Analytics** on the Disconnection page.
- **Disconnect Events: Last 1 Hour** on the Disconnection page.

When you click the required host name, the site-specific **Clients** page displays detailed information for the selected host. The following figure is an example of the site-specific **Clients** page:

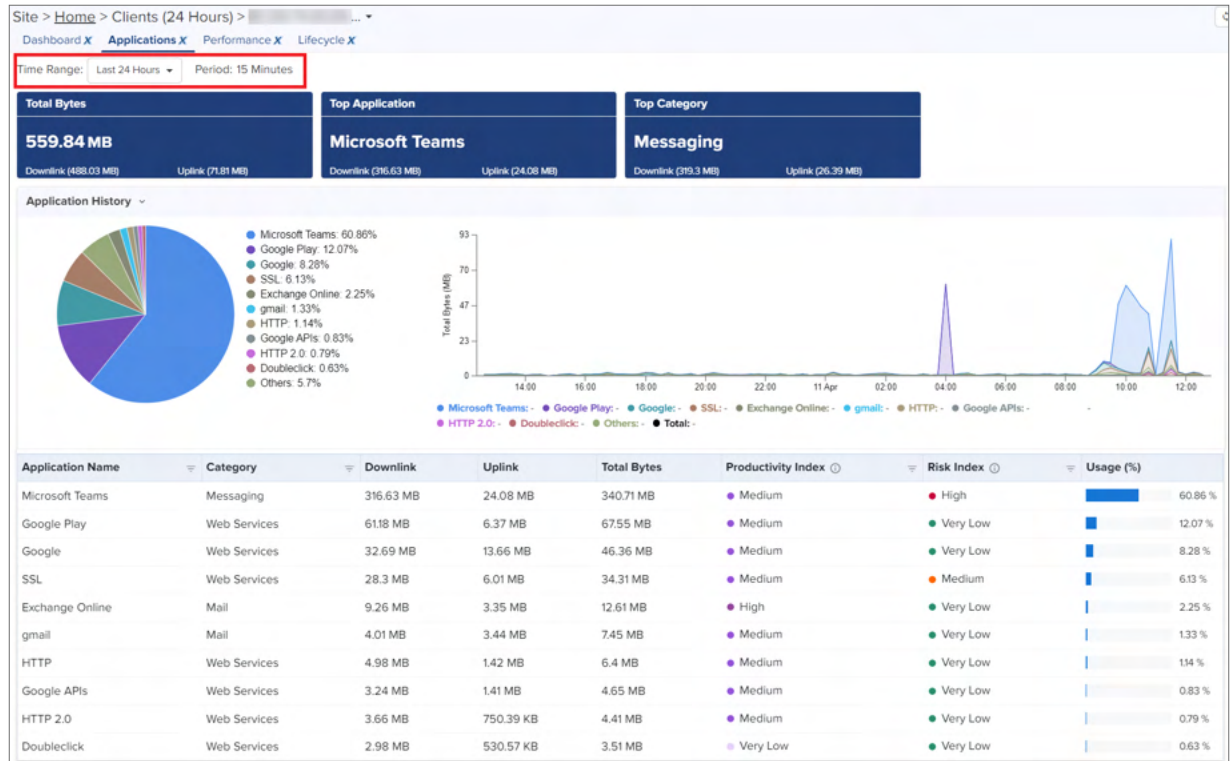


This site-specific **Clients** page contains the following tabs:

- **Dashboard X**—Provides a summary of the client connection or disconnection events such as Client history or lifecycle events.

By default, the **Dashboard** tab is visible when the site-specific **Clients** page appears. Based on the time period (Last 24 Hours, Last 7 Days, or Last 30 days) you select from the **Time Range** filter, the site-specific client **Dashboard** page displays the Wi-Fi client information in the following widgets:

- Connection
- Reassociations
- Total Bytes
- Top Application
- Client Details
- Client History X
- AP/Radio Details
- Lifecycle Events X
- Suppressed Failure Events
- Connection Success Rate X
- Top Failures Across Phases
- Top Suppressed Events By Type X
- Top Applications
- Top Categories
- **Applications X**—Provides detailed information of top applications used for the connection.

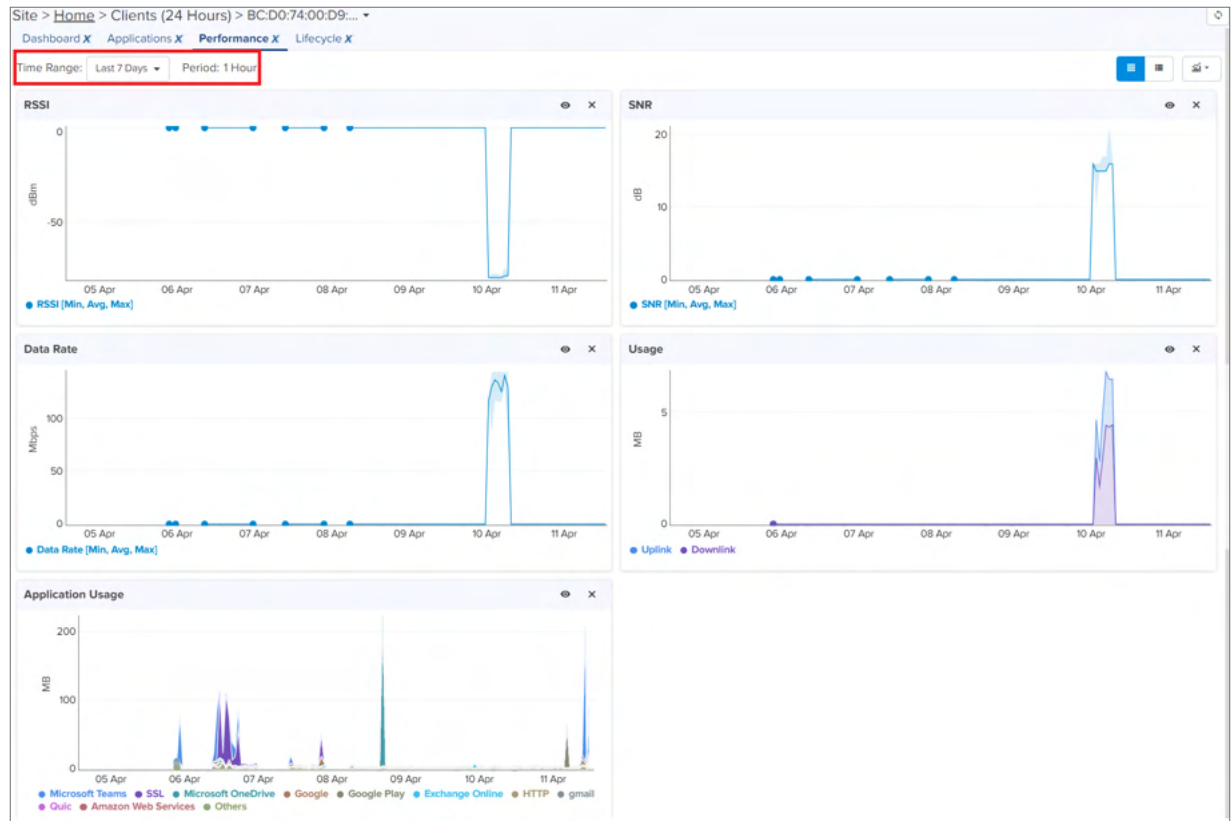


Based on the time period (Last 24 Hours, Last 7 Days, or Last 30 days) you select from the **Time Range** filter, the site-specific client **Applications** page displays the application information for the Wi-Fi client in the following widgets:

- Total Bytes
- Top Application
- Top Category
- Application / Category History


Click the ▾ icon next to the **Application History** title to view the details category-wise.

- **Performance X**—Provides detailed information of RSSI, SNR, date rate, usage in uplink and downlink, and the application usage.

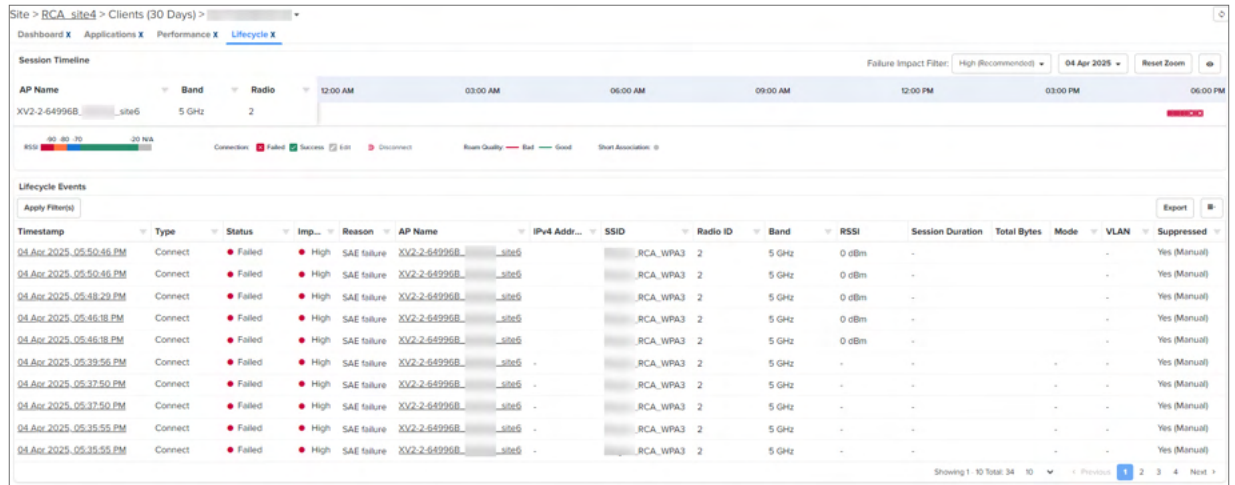


Based on the time period (Last 24 Hours, Last 7 Days, or Last 30 days) you select from the **Time Range** filter, the site-specific client **Performance** page displays the network performance for the Wi-Fi client in the following widgets:

- RSSI
- SNR
- Data Rate
- Usage
- Application Usage

You can click the  icon (Data point selector) to filter and view the required options specific to performance in the widgets.

- **Lifecycle X**—Provides detailed information of the client's connection or disconnection events.



Based on the date and impact levels you select from the date picker and **Failure Impact Filter** dropdown list, the site-specific client **Lifecycle** page displays the session timeline and the lifecycle events of the Wi-Fi client for the selected date.

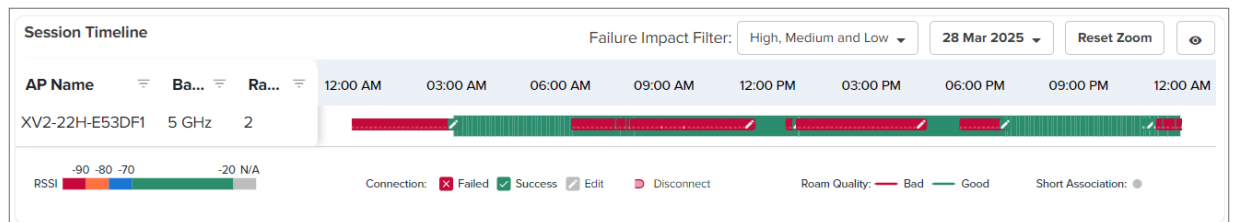


Note

Lifecycle data is available for a maximum of up to 30 days.

In the **Session Timeline** section, you can find the AP names, band used, and the radio index. In addition, different indicators mark RSSI, the connection event as failed or success, the disconnection event, the roam quality as bad or good, and short association.

For example, in the following UI page, the RSSI ranges and the roam quality are highlighted using different colors.



- Placing the cursor on the icon, displays date and time of the succeeded event.
- Placing the cursor on the icon, displays the reason and cause for the failed event.
- Clicking or icon in the **Session Timeline** section, displays the **Events** page with detailed information for the selected event.
- Clicking the disconnect () icon, displays details about the event and disconnection reason.
- The short association () icon denotes that the client connected and disconnected within a minute.
- The edit () icon denotes that the client connection failed in DHCP, DNS or Captive portal phase in the first connection attempt but succeeded later.



Note

A client connection is considered failed in DHCP, DNS, or CP, if the client fails to complete the phase within 45-60 secs.

The **Lifecycle Events** section provides detailed information of the client's connection and disconnection events such as timestamp, connection type, connection status, AP name, IPv4 address, radio ID, impact of the event, band used, RSSI, session duration, total bytes, wireless mode used, VLAN used, and WLAN details.


You can also use the filters to view and analyze the required event information. To view the required lifecycle event using filters, perform the following steps:

- a. In the **Lifecycle Events** section, click **Apply Filter(s)**.
- b. Enter one or more of the following details:

Filter name	Description
Timestamp	Time period for which you want to view the data: <ul style="list-style-type: none"> • Between • After • Before
Type	Type of event for which you want to view the data: <ul style="list-style-type: none"> • Roam • Connect • Disconnect
Status	State of the event: <ul style="list-style-type: none"> • Success • Failed
AP Name	Name of the AP that is used in the event.
IPv4 Address	The IPv4 address used for the connection.
Radio ID	ID of the radio used in the event.
Impact	Impact level of the event. <ul style="list-style-type: none"> • Low • Medium • High
Band	The bandwidth used for the connection.
Mode	The standard wireless mode used for the connection. For example, 802.1ac
VLAN	The VLAN ID used for the connection.
WLAN	The WLAN ID used for the connection.



Note

You can also click the  icon in the **Lifecycle Events** table to quickly search for type, status, AP name, IPv4 address, radio ID, impact, band, RSSI, VLAN, and WLAN.

- c. Click **Apply Filter(s)**.

The table in the **Lifecycle Events** section is updated with the required information for the client or host.

You can also drill-down an event to view what went wrong during the connection or the reason for the disconnection event. Refer [Viewing an event-based connection or disconnection event](#).

2. Analyze the data for the required client or host and take actions.

Viewing an event-based connection or disconnection event

After viewing the lifecycle events for a specific client or host, you can drill-down an event to analyze what caused a failed connection or a disconnection.

To view an event-based connection or disconnection state, perform the following steps:

1. Click the timestamp present in either the **Date and Time** or **Timestamp** columns to view the connection or disconnection event in detail.

You can locate a date or timestamp in the following widgets:

- **Date and Time** column in the **Connection Events: Last 1 hour** on the **Connection** page (data is available only when you click any of the hour bars in the **Connection Health** graph)

Date and Time	MAC Address	Status
10 Apr 2025, 09:29:33 PM	E4:5F:01:B4:31:1D	Failed
10 Apr 2025, 09:29:22 PM	F4:3B:D8:86:92:3C	Failed
10 Apr 2025, 09:28:50 PM	08:8E:90:37:B6:DA	Failed
10 Apr 2025, 09:28:33 PM	E4:5F:01:B4:31:1D	Failed
10 Apr 2025, 09:27:22 PM	F4:3B:D8:86:92:3C	Failed
10 Apr 2025, 09:26:33 PM	E4:5F:01:B4:31:1D	Failed
10 Apr 2025, 09:25:52 PM	F4:3B:D8:86:92:3C	Failed
10 Apr 2025, 09:25:03 PM	E4:5F:01:B4:31:1D	Failed

- **Date and Time** column in the **Disconnect Events: Last 1 hour** widget on the **Disconnection** page (data is available only when you click any of the hour bars in the **Disconnection** graph)

Date and Time	MAC Address	Status
28 Apr 2025, 06:22:27 PM	F4:3B:D8:86:92:3C	Failed
28 Apr 2025, 06:01:22 PM	F4:3B:D8:86:92:3C	Failed
28 Apr 2025, 06:01:09 PM	F4:3B:D8:86:92:3C	Failed
28 Apr 2025, 06:00:55 PM	F4:3B:D8:86:92:3C	Failed

- **Timestamp** column in the **Lifecycle Events** widget available on both the client > **Dashboard** page and the client > **Lifecycle** page.

- client > **Dashboard** page

Site > **-Cheetah** > Clients (30 Days) > sitindia-71

Dashboard X Applications X Performance X Lifecycle X

Failure Impact Filter: High (Recommended) Time Range: Last 7 Days Resolution: 1 Hour [Learn](#)

System

OS Version

Last Seen 28 Apr 2025, 06:37 PM

Capability axa

Suppression No

Type

AP/Radio Details

Name **Cheetah-XV2-22H-B93FC4**

Type XV2-22H

Downlink: - Uplink: - Total: - Connect

Lifecycle Events X

Apply Filter(s)

Timestamp	Type
28 Apr 2025, 06:37:59 PM	Roam (Update)
28 Apr 2025, 06:34:29 PM	Roam (Update)
28 Apr 2025, 06:33:59 PM	Roam (Update)
28 Apr 2025, 06:33:29 PM	Roam (Update)

- client > **Lifecycle** page

Site > **-Cheetah** > Clients (30 Days) > sitindia-71

Dashboard X Applications X Performance X **Lifecycle X**

Session Timeline

AP Name B... R... 01:45 AM 02:00

-XV2-22H-B93FC4 5 GHz 2

-XV2-22H-B93FC4 2.4 GHz 1

RSSI -90 -80 -70 -20 N/A

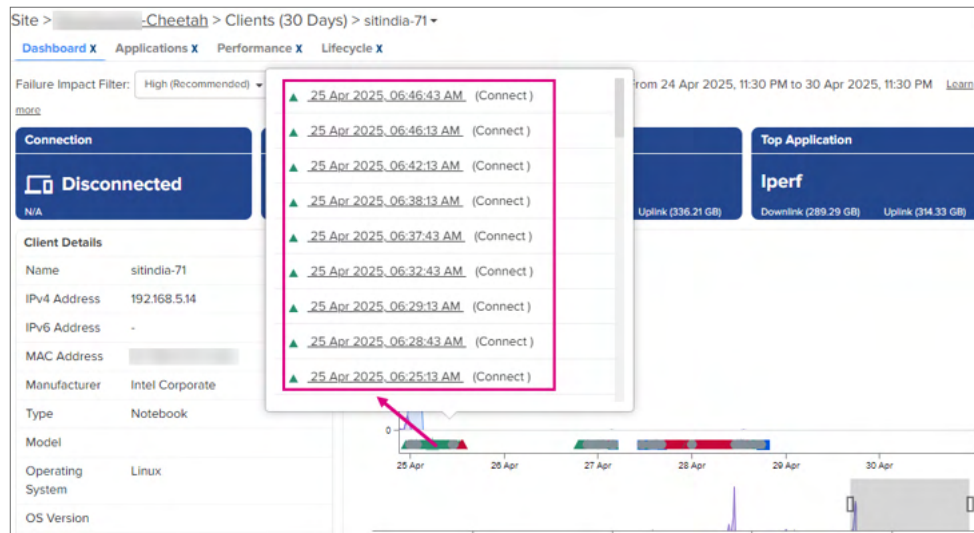
Connection: X Failed S Success

Lifecycle Events

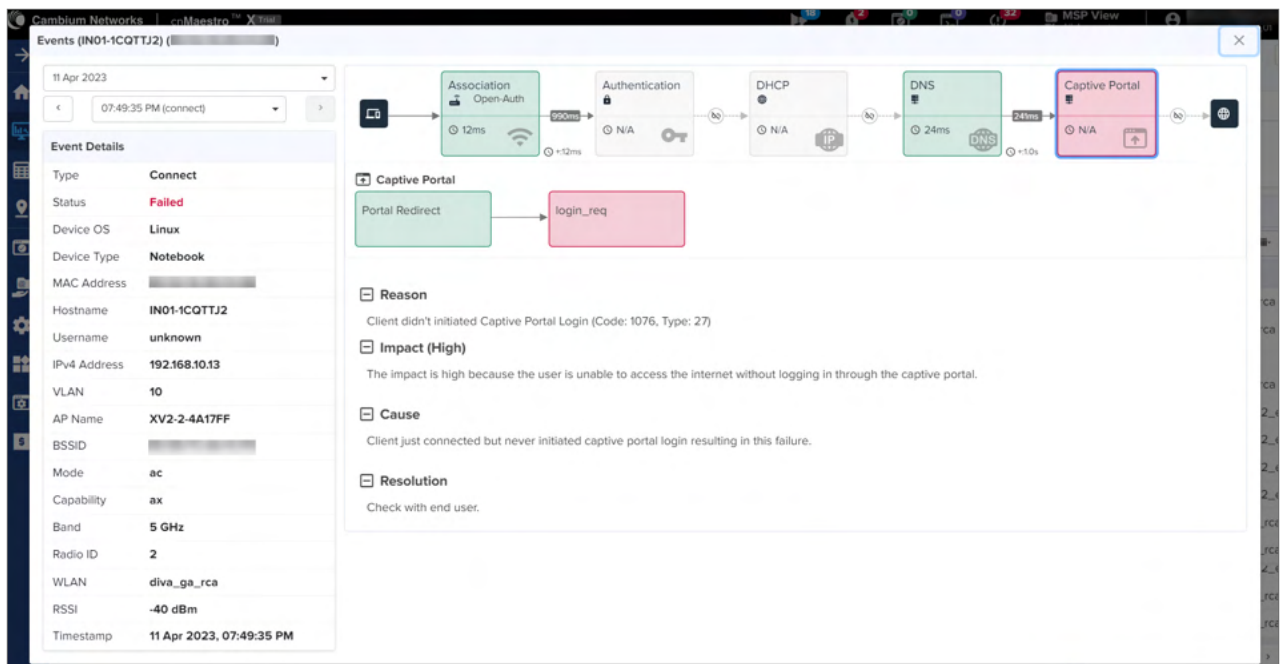
Change Filter(s) Clear

Timestamp	Type	Status	Im...
10 Apr 2025, 03:04:42 AM	Connect (Update)	Success	-
10 Apr 2025, 02:59:42 AM	Connect (Update)	Success	-
10 Apr 2025, 02:56:12 AM	Connect (Update)	Success	-

- Timestamp listed in the pop-up window when you click a point in the **Client History X** graph in the client > **Dashboard** page.



When you click on **Timestamp** or **Date and Time**, the **Events** screen displays the detailed event information.



The **Events** page provides phase-wise information with complete event details such as reason, impact, cause, and resolution. These event-based details help with troubleshooting any issues.

- To view an event for a specific date, you can select the required date from the date dropdown list.

The screenshot displays the 'Events (IN01-1CQTTJ2)' page. At the top, a date filter is set to '10 Apr 2023' and a time filter is set to '06:28:31 PM (connect)'. The 'Event Details' sidebar on the left lists the following information:

- Type: Connect
- Status: Failed
- Device OS: Linux
- Device Type: Notebook
- MAC Address: [Redacted]
- Hostname: IN01-1CQTTJ2
- IPv4 Address: -
- VLAN: 0
- AP Name: XV2-2-4A17FF
- BSSID: [Redacted]
- Mode: [Redacted]
- Capability: ax
- Band: 2.4 GHz
- Radio ID: 1
- WLAN: [Redacted]
- RSSI: -42 dBm
- Timestamp: 10 Apr 2023, 06:28:31 PM

The main content area shows a timeline of events: Association (Open-Auth), Authentication, DHCP, DNS, and Captive Portal. Below the timeline, the 'Reason' section states: 'Client connection failed as it doesn't send an assoc request frame to continue the connection process. (Code: 1079, Type: 7)'. The 'Impact (Low)' section notes: 'The client could potentially reconnect to a different access point, or there could be interference in the medium causing it to miss the association request. However, it may be able to reconnect in the next attempt.' The 'Cause' section explains: 'RF medium may be congested or client may be moved to another Access Point after sending authentication frame to this Access Point or may be some issue with the client state machine issue, AP didn't receive the Assoc Request frame.' The 'Resolution' section suggests: 'Most likely a transient problem. If you see this problem consistently with multiple clients, please contact Cambium support.'

Similarly, you can use < or > to view time-based events for a client. You can also select the time-based events from the dropdown list.

3. Click the ✕ icon to close the **Events** page.

Viewing AP-specific information

You can view an AP-specific information for the required client or event and analyze the connection or disconnection data. This analysis helps identify device details used for the connection.

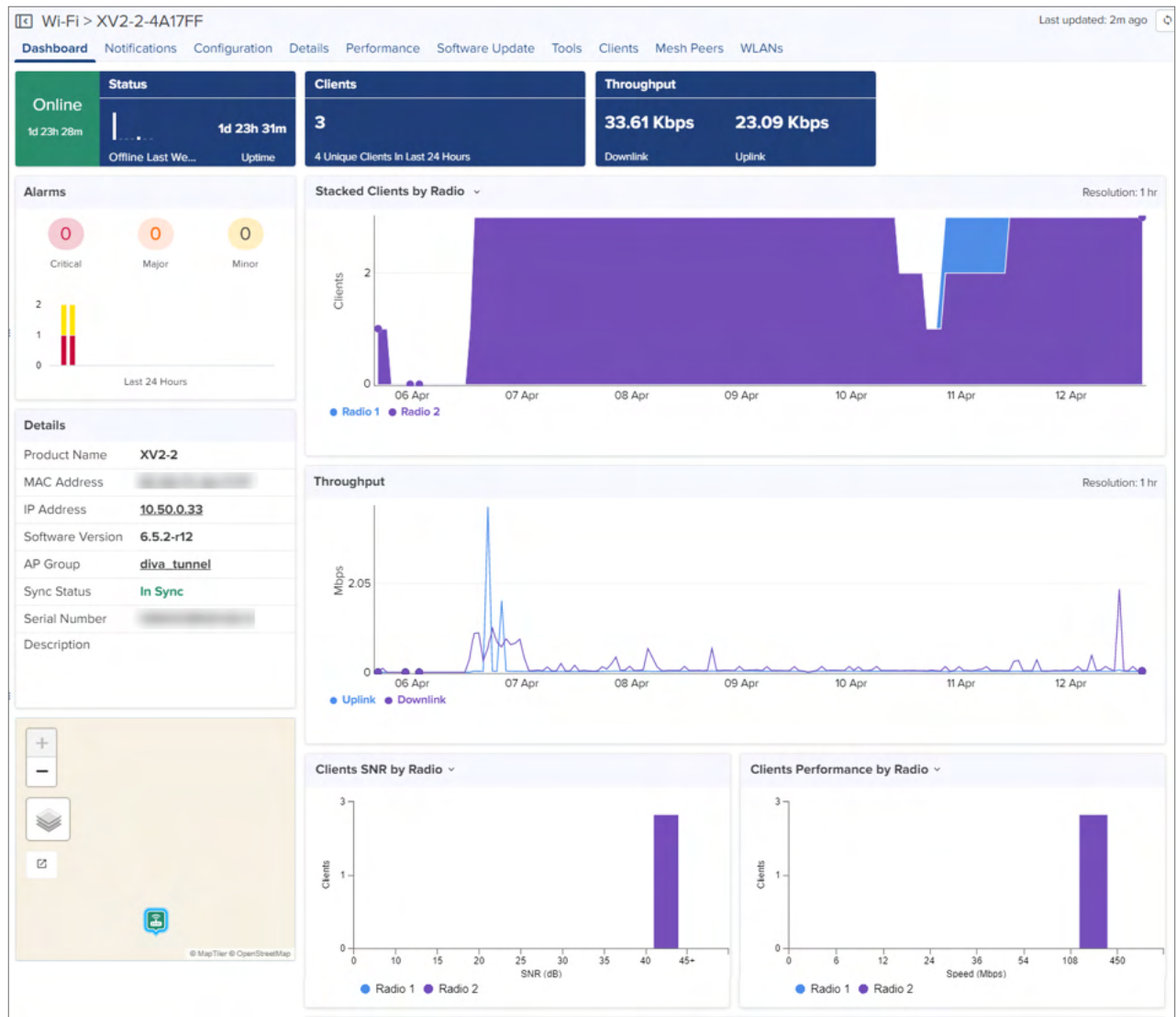
To view AP-specific information, perform the following steps:

1. Click the **AP Name** to view the data.

You can locate an AP name in the following widgets:

- Top Affected APs on the **Connection** page
- Connection Events—Last 1 Hour on the **Connection** page
- Top Reporting APs on the **Disconnection** page
- Disconnect Events—Last 1 Hour on the **Disconnection** page
- Lifecycle Events on both the **Connection** and **Disconnection** pages

When you click on the required AP name, the site-specific **Wi-Fi** dashboard displays the AP or device information.



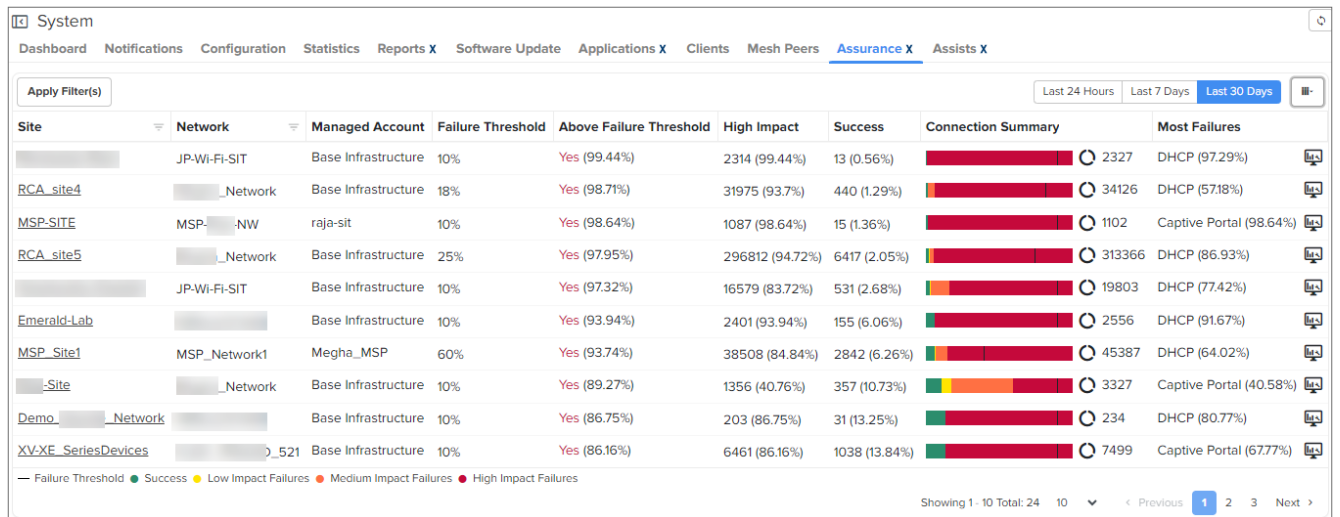
For more information on the AP (or device) specific dashboard, refer to the Wireless LAN Dashboards section of cnMaestro Cloud User Guide.

2. Analyze the AP data and take appropriate actions.

System-level Assurance

The System-level **Assurance X** page provides the consolidated data of all the site analytics. For more information, refer to [Assurance X page](#).

Figure 506 *System Assurance*



Managed Services

This section includes the following topics:

- [Managed Accounts](#)
- [Managing subscribers \(end-customer\)](#)

Managed Accounts

This section includes the following topics:

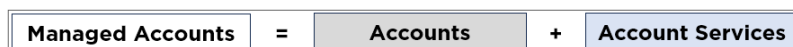
- [Overview](#)
 - [Managed Accounts](#)
 - [Accounts](#)
 - [Managed Account Service](#)
 - [Account Service Users \(Administrators\)](#)
- [Configuring Managed Account Services](#)
 - [Enable Managed Accounts](#)
 - [Creating Managed Account Services](#)
 - [Creating Account](#)
 - [Validating Account Users](#)
- [Managed Account Administration](#)
 - [Overview](#)
 - [System Dashboard](#)
 - [Account Administration](#)
 - [Device Management](#)
 - [Swap 60 GHz cnWave Accounts](#)
 - [Disabling the Managed Accounts feature](#)

Overview

Managed Accounts allow the cnMaestro owner to partition their installation into independent accounts with their own administrators and configuration. This feature is for MSPs who want to provision a full cnMaestro account for their customers, while still maintaining control over the global deployment.

Managed Accounts

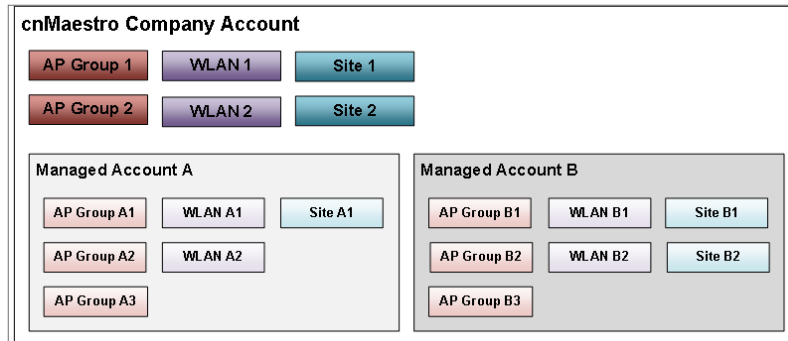
The Managed Accounts feature combines Accounts with Account Services.



Accounts

Managed Accounts group cnMaestro devices and configuration objects (such as AP Groups, WLANs, and Sites) into administration domains within a single cnMaestro deployment. Accounts are independent, and the devices added to them are configured using the objects in the Account.

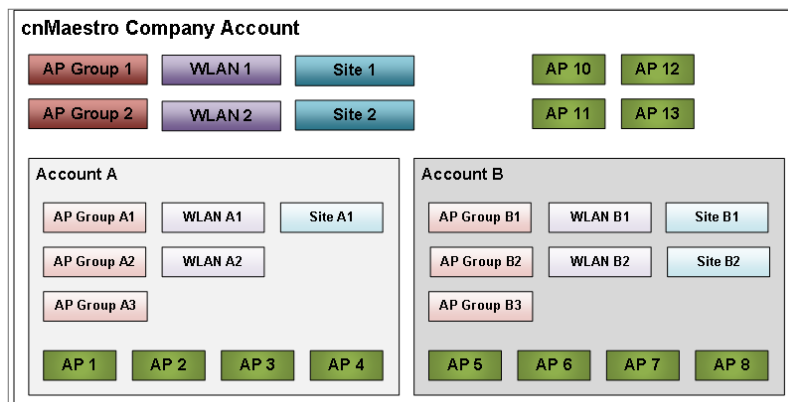
Figure 507 *Accounts*



Access Points

Access Points exist in the global Company Account, or they can be added to a single Managed Account. Access Points in a Managed Account are configured using the Wi-Fi Profiles in that Managed Account.

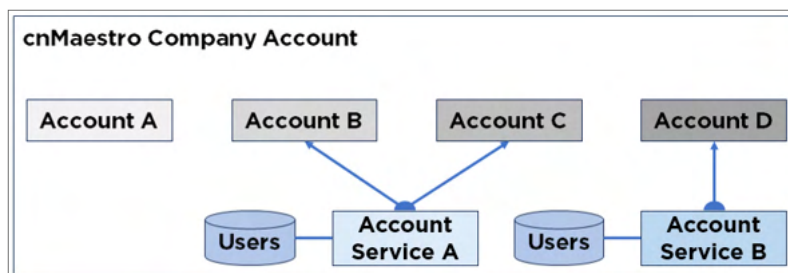
Figure 508 *Access Points*



Managed Account Service

A Managed Account Service creates a branded version of the cnMaestro UI. Each Account Service can be mapped to multiple Accounts.

Figure 509 *Account Service*



Each Managed Account Service adds the following support to an Account:

Support	Details
Administrator Database	Each Account Service has its own independent database of users who can be shared across multiple Accounts.
Custom Login URL	The path of the login URL used by the Account Service Administration can be tailored to the Account Service. The path must be unique across all cnMaestro.
Branded UI	The Account UI is customized for the Account Service through graphics, colors, and text.
Account Service Users	List of all the users mapped to the Managed Account Service. They may be mapped to zero or more associated Accounts.

Account UI

The Account UI can be customized to represent the service brand. A sample Account UI is shown below:

Figure 510 Account UI - Sample 1

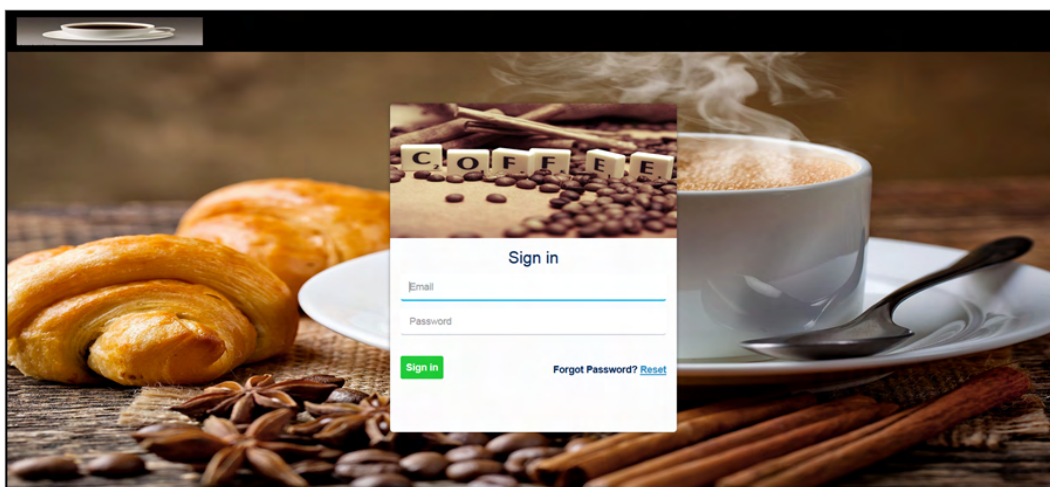
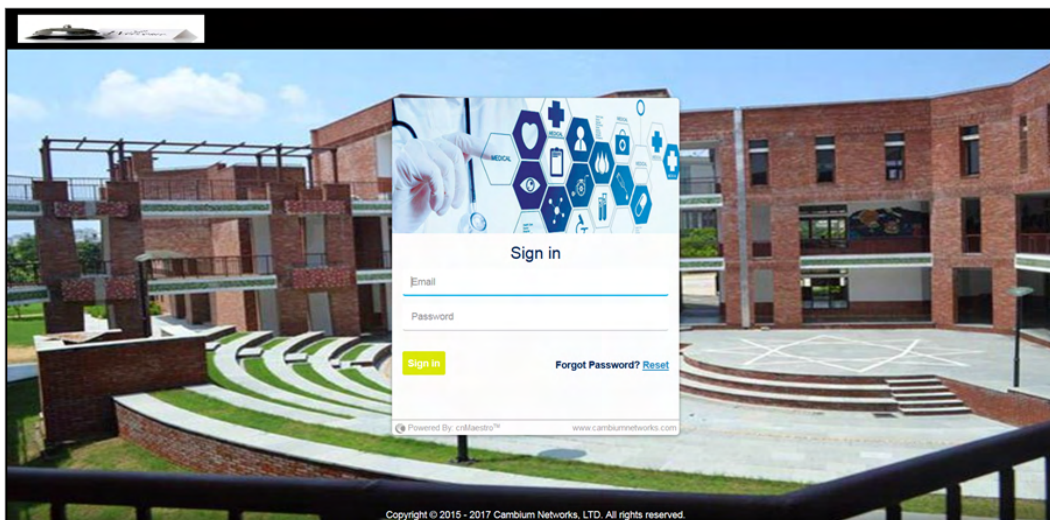


Figure 511 Account UI - Sample 2



Account Service Users (Administrators)

Account Service Users are assigned to Accounts. They access similar features as the Global cnMaestro Administrators, except they are only allowed to manage the subset of devices and objects (AP Groups, WLAN, Sites, etc.).

Account Service Users (Administrators) Roles

Account Service Users can be assigned one of three roles as shown below for each account:

- Administrator
- Monitor
- Operator

The authorizations for each Role are listed in the table below:

Table 113 *Tenant Administrator Roles*

Feature	Description	Administrator	Operator	Monitor
AAA Services (Global cnMaestro administrator only)	Add AAA services	None	None	None
Administration Settings (Global cnMaestro administrator only)	Change global application configuration, Onboarding settings like password change	None	None	None
API Management (Global cnMaestro administrator only)	Create API clients	None	None	None
Application Operations 1	Create Networks, Towers, and Sites	All	View	View
Application Operations 2	Tech Dump, import/export server data, change Account Type (Enterprise or Access and Backhaul)	None	None	None
Association ACL	Configure MAC list on the controller	All	View	None
Auto- provisioning (Global cnMaestro administrator only)	Support for global auto-provisioning rules	All	View	None
Audit logs	Logs user action of different features	All	All	All
Device Operations	Reboot device, link test, connectivity test	All	All	None
Device Override	Per-device configuration changes	All	All	View
Global Configuration	Apply Configuration through Templates and AP Group	All	View	View
Guest Access	Guest Access	All	View	View

Table 113 *Tenant Administrator Roles*

Feature	Description	Administrator	Operator	Monitor
Portal				(Sessions)
Monitoring	Access Device Statistics Data	All	All	View
Notifications	View Alarms and Events	All	All	View
Onboarding	Approve Device Onboards	All	All	None
Reporting	Generate reports	All	All	All
Software Images (Global cnMaestro administrator only)	Download device software images	All	None	None
Software Upgrade	Upgrade device	All	All	View
System Operations	Reboot VM, change log level, system upgrade, system monitoring	None (Except System Monitoring)	None (Except System Monitoring)	None (Except System Monitoring)
User Management	Manage users, roles, and sessions	All	None	None

Configuring Managed Account Services

This section provides the following details on configuration of Account Services in cnMaestro:

- [Enable Managed Accounts](#)
- [Creating Managed Account Services](#)
- [Creating Account](#)
- [Validating Account Users](#)

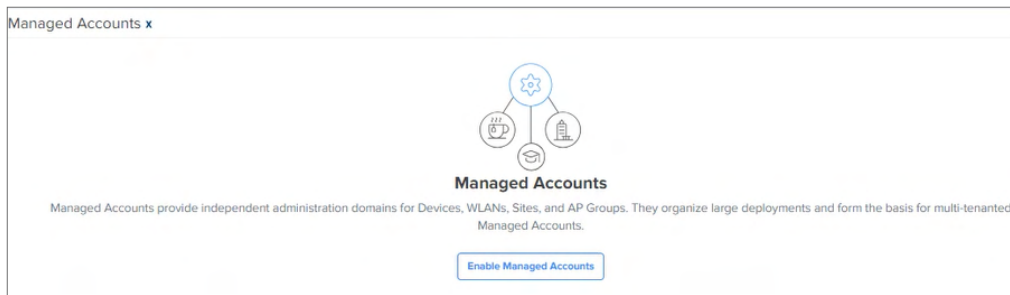
Enable Managed Accounts

By default, Account Services is disabled in the cnMaestro UI.

To enable Account Services:

1. Navigate to **Managed Services > Managed Accounts**.
2. Click the **Enable Managed Accounts**.

Figure 512 *Enabling Managed Accounts*



Note

Account Services provide independent administration domains for Devices, WLANs, Sites, and AP Groups. They organize large deployments and form the basis for multi-tenanted Account Services.

Additions in the cnMaestro UI when Managed Accounts is Enabled

- Once Managed Accounts is enabled, **Accounts** and **Account Services** tabs appear in the cnMaestro UI.

Figure 513 *Accounts and Account Services tabs*

Managed Services > Managed Accounts x

[Accounts](#) [Account Services](#)

Accounts group cnMaestro devices and configuration objects (such as AP Groups, WLANs, and Sites) into independent administration domains within a single cnMaestro.

[New Account](#) [Disable Managed Accounts](#)

Name	Friendly Name	Account Service	Status	Users	Networks	Devices	Alarms	
			Enabled	0	1	0 of 1 offline	0 0	
test	_2_test	<input type="checkbox"/> cbrs-mssp	Enabled	0	1	0 of 0 offline	0 0	
MSP		<input type="checkbox"/>	Enabled	1	1	0 of 0 offline	0 0	
CNM_SIT_TEST	CNM_SIT_TEST	<input type="checkbox"/> CNM_SIT_TEST	Enabled	0	1	0 of 0 offline	0 0	
CnWave_SIT	cnwave_sit_testing	<input type="checkbox"/>	Enabled	2	1	0 of 0 offline	0 0	
GETT MSP-INDRA	IR		Enabled	0	2	0 of 0 offline	0 0	
GHQ-QA-Cloud		<input type="checkbox"/> ghqqacloud	Enabled	1	1	2 of 2 offline	0 1	
	user	<input checked="" type="checkbox"/>	Enabled	1	3	0 of 0 offline	0 0	
A-12	IR	<input type="checkbox"/>	Enabled	1	3	0 of 2 offline	0 0	
OLT		<input type="checkbox"/>	Enabled	0	1	0 of 0 offline	0 0	

Showing 1 - 10 Total: 34 10 < Previous 1 2 3 4 Next >

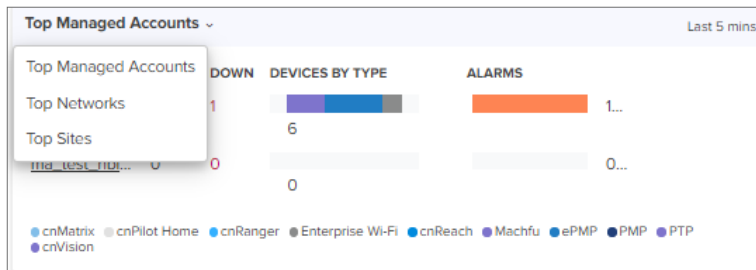
- The Header adds a select box that allows the Global Administrator to enter the context of Account selected.

Figure 514 *Managed Accounts Component in Header*



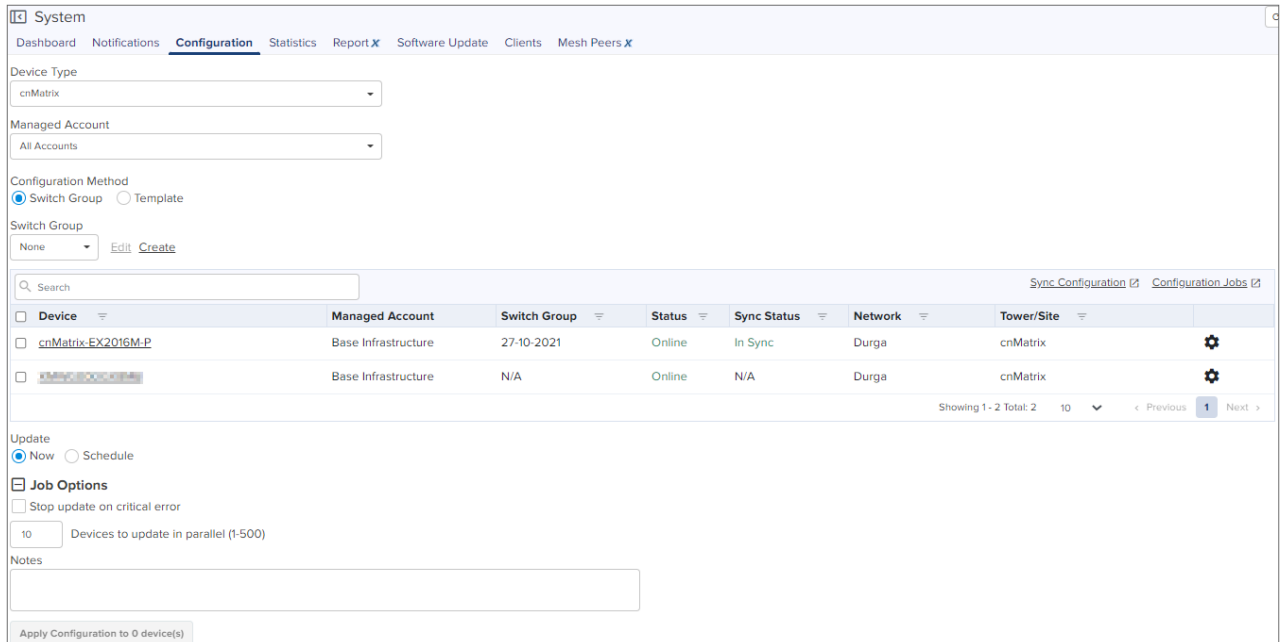
- The System Dashboard adds a Health component for Top Managed Accounts.

Figure 515 *Dashboard > Top Managed Accounts*



- Global tabs in the UI are updated with a Managed Account column.

Figure 516 *Managed Account Column*



Creating Managed Account Services

The user can create an Account Service and map it to an Account. The Account Service supports an independent user database and a customized user interface. There is a default Account Service, so creating a new one is optional.

To create an Account Service:

1. Navigate to **Managed Services > Managed Accounts > Account Services** tab.

Account Services Tab

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	
ayae	#25478D	https://cloud.cambiumnetworks.com:443/msp/aya	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	
gfjyhgbl	#213F79	https://cloud.cambiumnetworks.com:443/msp/gfjyhgbl	0	0	
ghhgaccloud	#25478D	https://cloud.cambiumnetworks.com:443/msp/ghhgaccloud	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	
	#64edff	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 >

2. Click **New Account Service**.

The **Add Account Service** window is displayed.

Add Account Service Window

Add Account Service

Name

Login Path
https://qa.cloud.cambiumnetworks.com:443/msp/

The Login URL is used to access Managed Accounts. It must be unique in cnMaestro.

Preview


Add Cancel

3. Enter the following details:

Table 114 Parameters in the Add Account Service Window

Parameter	Description
Name	Name of the service. This name is visible to Account Administrators.

Table 114 *Parameters in the Add Account Service Window*

Parameter	Description
	A maximum of 64 characters are supported for the name.
Login Path	<p>Account Administrators log into cnMaestro using a standard URL with an additional Path that defines the Account Service.</p> <p>For example, <code>https://<cnmaestro cloud URL>/msp/<branded_service_path></code></p> <div>  <div> <p>Note</p> <ul style="list-style-type: none"> The Path name must be unique across all Account Service accounts hosted of Cambium Cloud. A maximum of 16 characters are supported for the path name. </div> </div>

- Click **Add**.

Creating Account

To create an Account:

- Navigate to **Managed Accounts > Accounts** tab.

Figure 517 *Accounts Tab*

Managed Services > Managed Accounts x

[Accounts](#) [Account Services](#)

Accounts group cnMaestro devices and configuration objects (such as AP Groups, WLANs, and Sites) into independent administration domains within a single cnMaestro.

[New Account](#) [Disable Managed Accounts](#)

Name	Friendly Name	Account Service	Status	Users	Networks	Devices	Alarms	
			Enabled	0	1	0 of 1 offline	0 0	
test	_2_test	<input type="checkbox"/> cbrs-msp	Enabled	0	1	0 of 0 offline	0 0	
MSP		<input type="checkbox"/>	Enabled	1	1	0 of 0 offline	0 0	
CNM_SIT_TEST	CNM_SIT_TEST	<input type="checkbox"/> CNM_SIT_TEST	Enabled	0	1	0 of 0 offline	0 0	
CnWave_SIT	cnwave_sit_testing	<input type="checkbox"/>	Enabled	2	1	0 of 0 offline	0 0	
GETT MSP-INDRA	IR		Enabled	0	2	0 of 0 offline	0 0	
GHH-QA-Cloud		<input type="checkbox"/> ghgqacloud	Enabled	1	1	2 of 2 offline	0 1	
	user	<input checked="" type="checkbox"/>	Enabled	1	3	0 of 0 offline	0 0	
A-12	IR	<input type="checkbox"/>	Enabled	1	3	0 of 2 offline	0 0	
OLT		<input type="checkbox"/>	Enabled	0	1	0 of 0 offline	0 0	

Showing 1 - 10 Total: 34 10 < Previous 1 2 3 4 Next >

- Click **New Account**.

The **Add Account** window is displayed.

Figure 518 *Add Account window*

Add Account [X]

Name*

Friendly Name

Status
☒ Enabled ☐ Disabled

Account Service
aye ▼
ⓘ The Account Service supports unique UI branding and Login URL.

Email

Role
Administrator ▼
ⓘ Access all functionality, including adding/deleting local users.

3. Enter the following details:

Table 115 *Parameters in the Add Account Window*

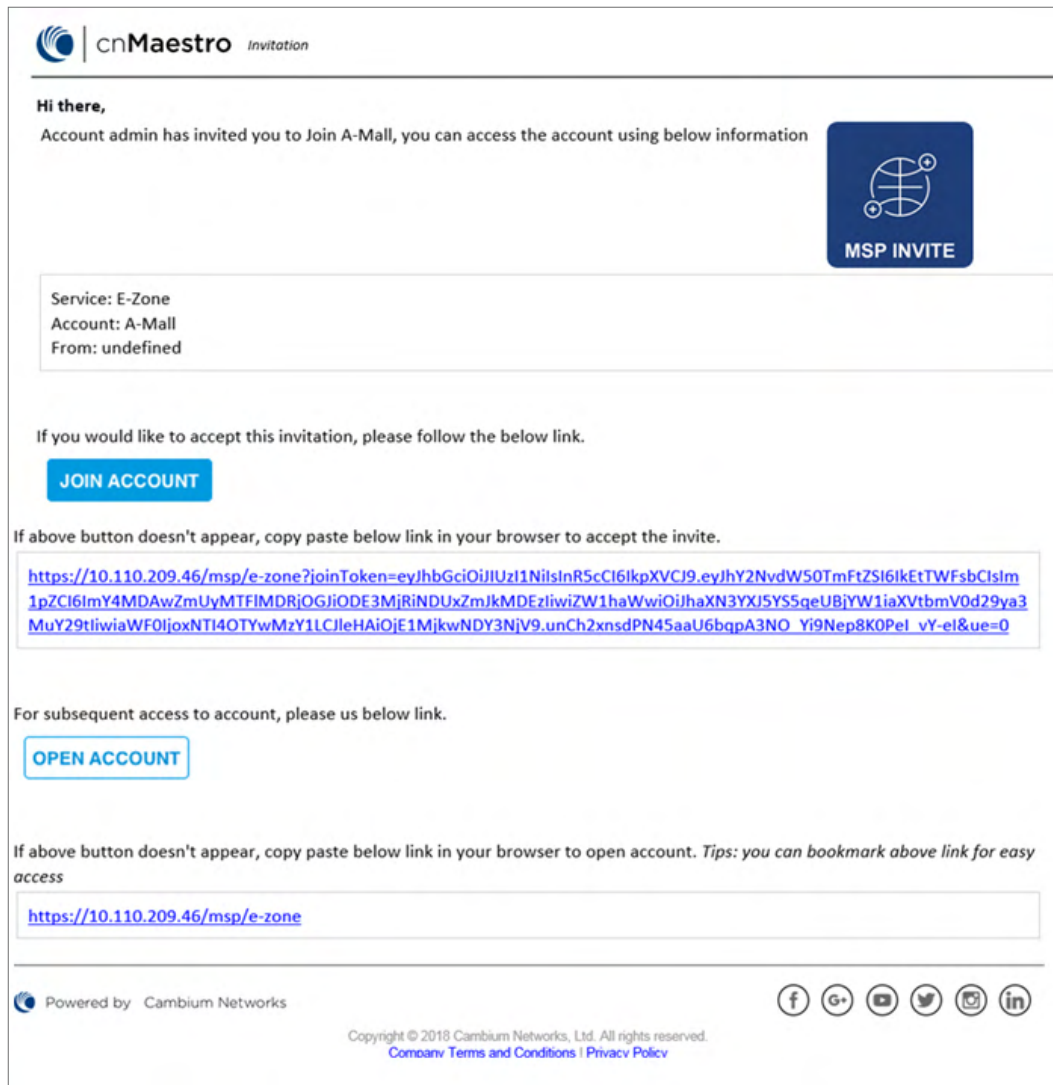
Parameter	Description
Name	Name of the Account. This is sent in the invitation email when users are invited to the account.
Friendly Name	The Friendly Name will be sent in the invitation email.
Status	Determines whether the account is enabled or disabled. When an account is disabled, all Account Users (users) are logged out.
Account Service	The Account Service used for branding and authentication.
Email	The email address of the first Account User. You can add more users after the account has been created.

4. Click **Add**.

Validating Account Users

Once an Account is created, the Account User is sent an email invitation. The email provides directions on how to access the Account UI and set their password.

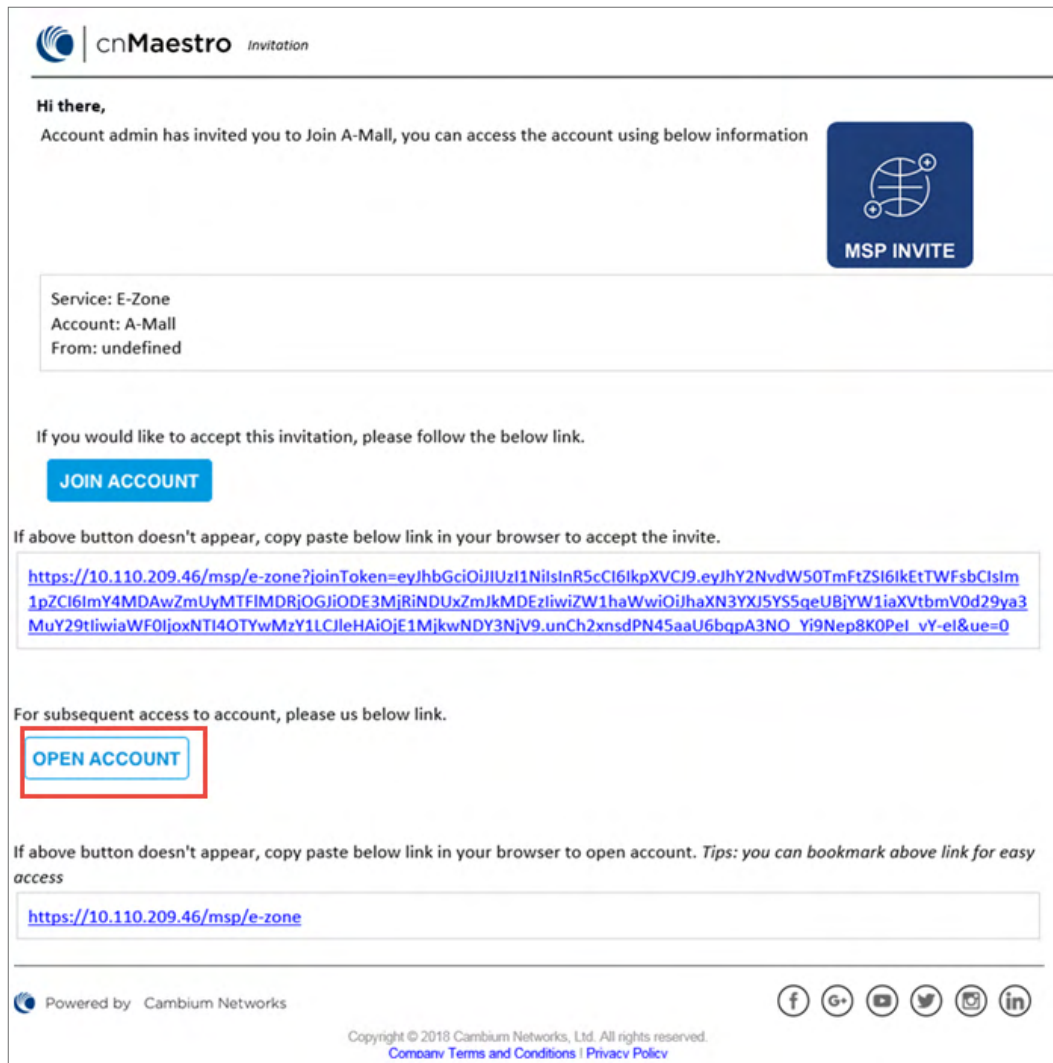
Figure 519 Sample Email Invitation



Check Email for Invite

An email is sent inviting the Account User to view their new Managed Account. It has a link that must be clicked to enable access.

Figure 520 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 521 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	 
gfjyhgj	#213F79	https://cloud.cambiumnetworks.com:443/msp/gfjyhgj	0	0	 
ghhgaccloud	#25478D	https://cloud.cambiumnetworks.com:443/msp/ghhgaccloud	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](#)
- Users 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 522 System View

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 523 Account View

Managed Accounts > BULK move

Dashboard Notifications **Configuration** Statistics Reports X Software Update Clients Mesh Peers Assists X

Account Users Devices WLANs AP Groups Guest Portals

Name
BULK move

Friendly Name

Account Service
default
☐ [Edit](#) [Create](#)

Login Path
<https://.../dqihd>

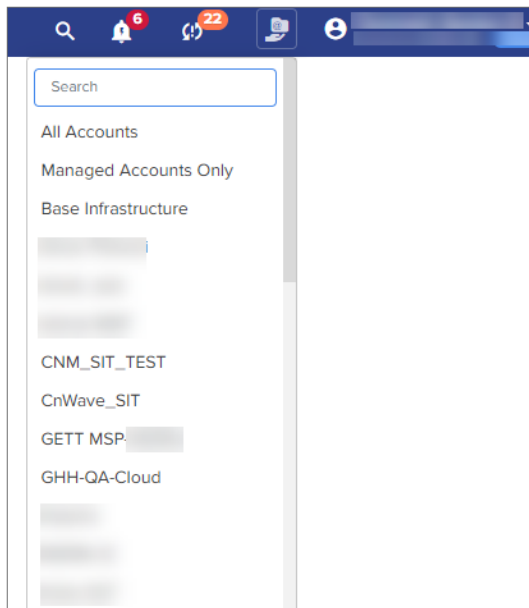
Status
☒ Enabled ☐ Disabled

[Save](#)

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 dropdown 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 524 Managed Account Administrator (User) View



Users View

On the Managed Account **Configuration > Users** page, you can invite users via Email. Once invited, they receive an automated email. Upon accepting the invitation, they are granted access to the designated MSP account.



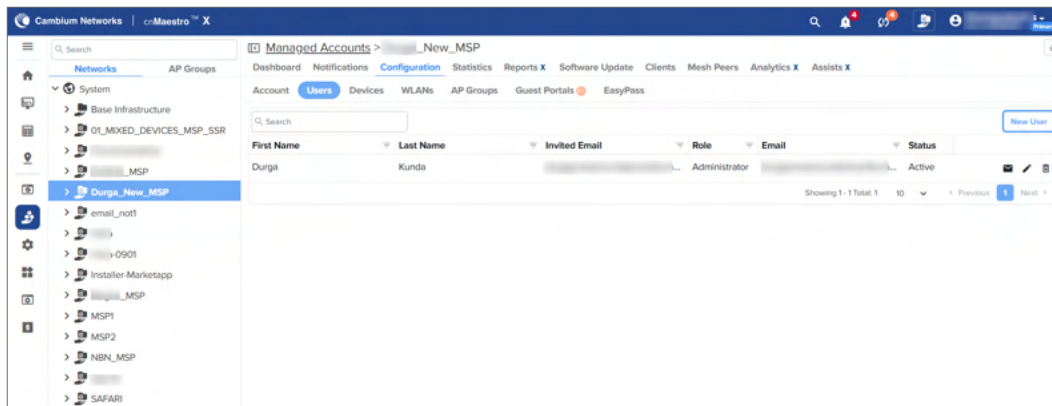
Note

You can invite multiple users simultaneously by entering their email IDs in the Email text box or Copy and paste the multiple email IDs as a comma-separated input.

You can add a maximum of 20 email IDs at a single time.

You can add maximum of 200 users to the cnMaestro account.

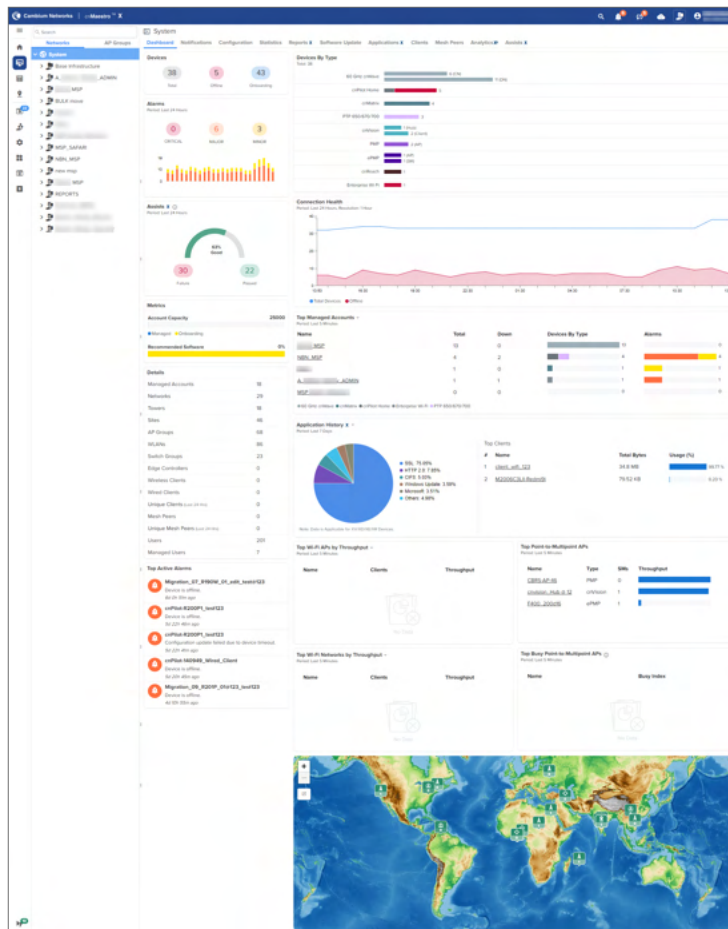
Figure 525 Users



System Dashboard

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

Figure 526 System Dashboard



Account Administration

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

Table 116 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.

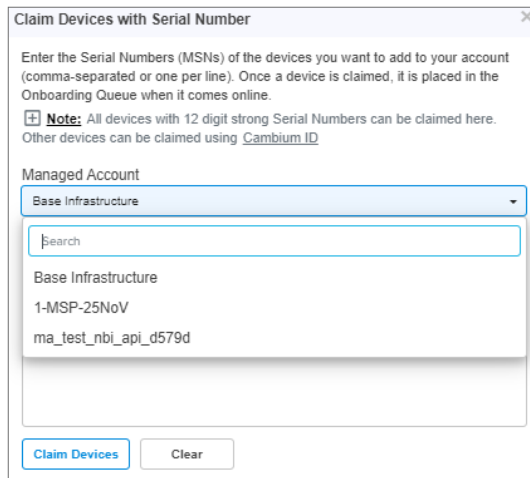
Device Management

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 527 *System Onboarding*



The dialog box titled "Claim Devices with Serial Number" contains the following elements:

- Instructions: "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 dropdown menu showing "Base Infrastructure".
- Search input field.
- Search results list showing "Base Infrastructure", "1-MSP-25NoV", and "ma_test_nbi_api_d579d".
- "Claim Devices" and "Clear" buttons.

Device Onboarding

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



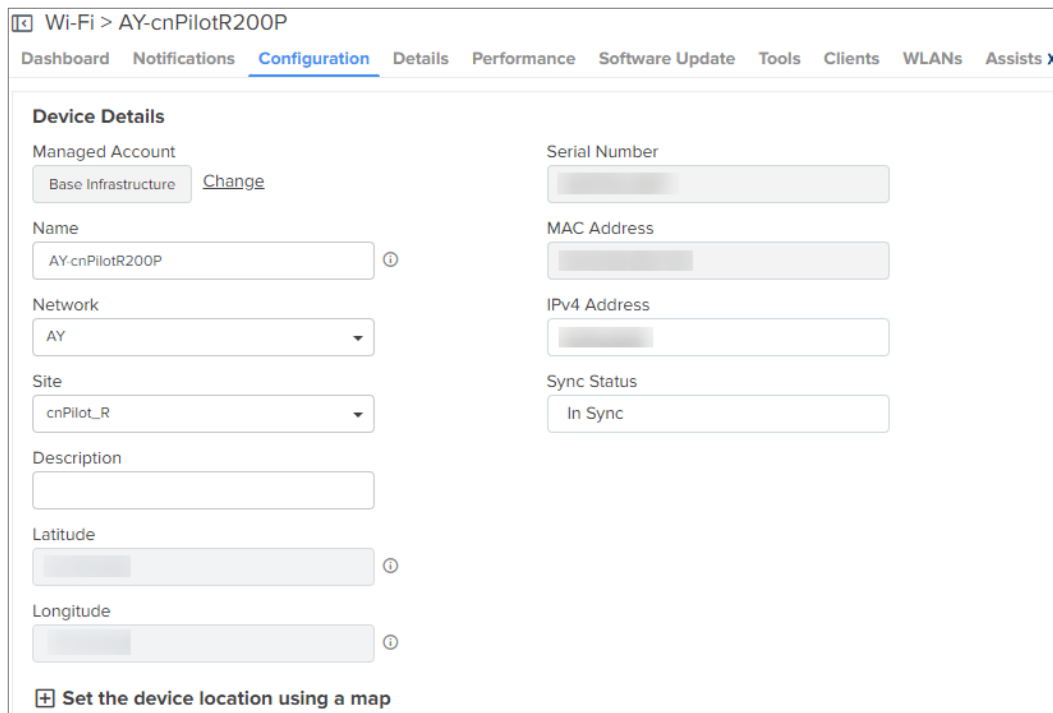
Note

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 528 *Moving a Device Between Accounts*



The screenshot shows the "Configuration" tab for a device named "AY-cnPilotR200P". The page includes the following fields and options:

- Managed Account: "Base Infrastructure" with a "Change" link.
- Name: "AY-cnPilotR200P" (with a help icon).
- Network: "AY" (dropdown menu).
- Site: "cnPilot_R" (dropdown menu).
- Description: Empty text field.
- Latitude: Empty text field (with a help icon).
- Longitude: Empty text field (with a help icon).
- Serial Number: Empty text field.
- MAC Address: Empty text field.
- IPv4 Address: Empty text field.
- Sync Status: "In Sync" (dropdown menu).
- Buttons: "Set the device location using a map" (with a plus icon).


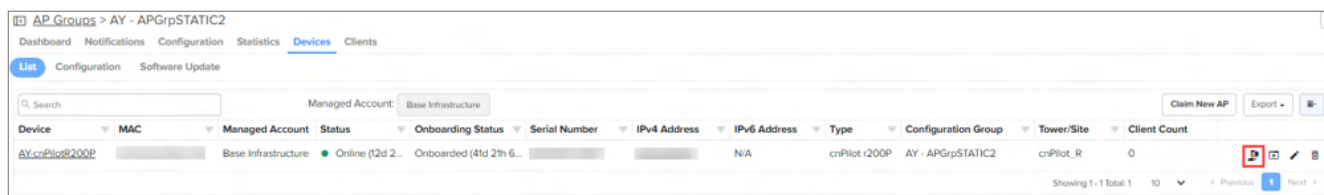
In Enterprise view, the device can be moved between Accounts using the **Managed Account** () icon in the **AP Groups > <AP-group-name> > Devices > List** tab.

Figure 529 *Moving a device between Accounts in Enterprise View*



Account Deletion

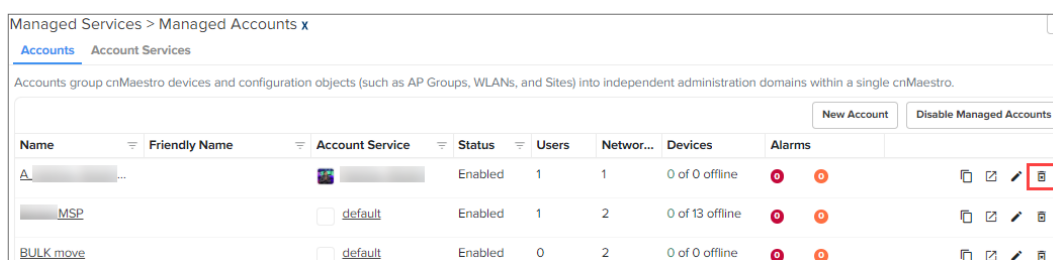


Note

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 530 *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.

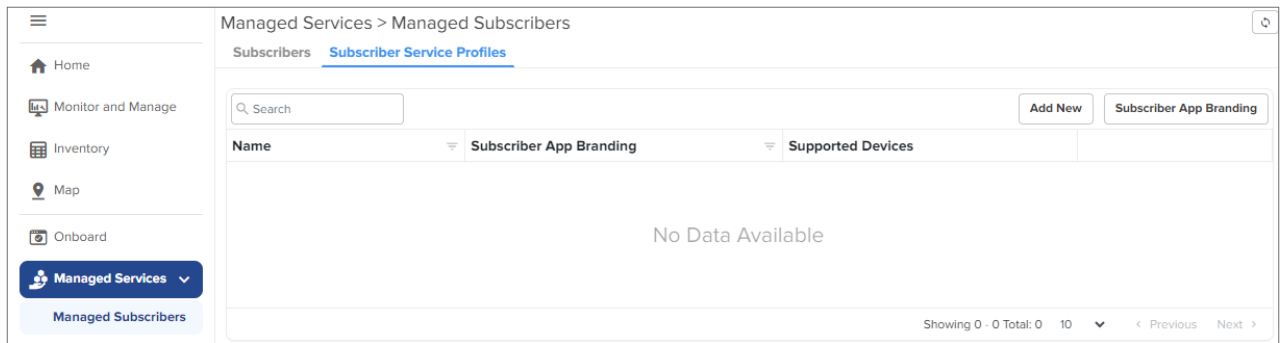
This process involves the following actions:

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.

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 117](#).

Table 117 *Subscriber Service Profile parameters*

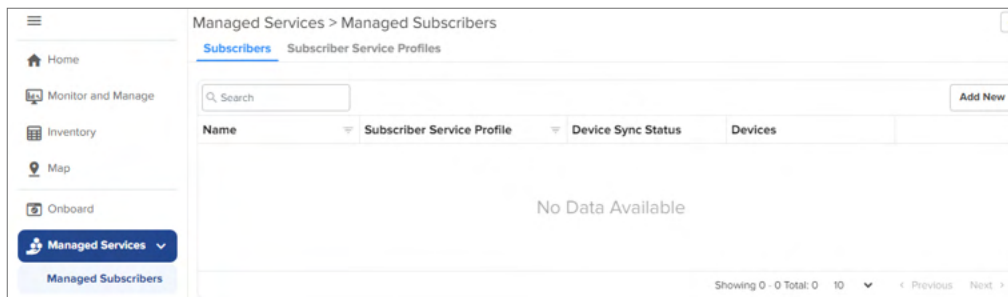
Parameter	Description
Name	Name of the subscriber service profile.
Description	Brief description for the subscriber service profile.
Download (Mbps)	Download speed (in Mbps) configured for the profile.
Upload (Mbps)	Upload speed (in Mbps) configured for the profile.
Type	Displays the device type as RV22 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 dropdown list.
Subscriber App Branding	Specifies the cnMaestro Subscriber application branding that must be used in this profile.

Parameter	Description
	<p>All routers sent to subscribers in this service profile contain the selected branding logo and information.</p> <p>Select the required branding from the dropdown list.</p> <p>If no branding is present, create one by clicking the add () icon. See cnMaestro Subscriber application branding for more information.</p>

- Click **Save**.

Adding a subscriber

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




- Click **Add New**.

The **Add Subscriber** window appears.

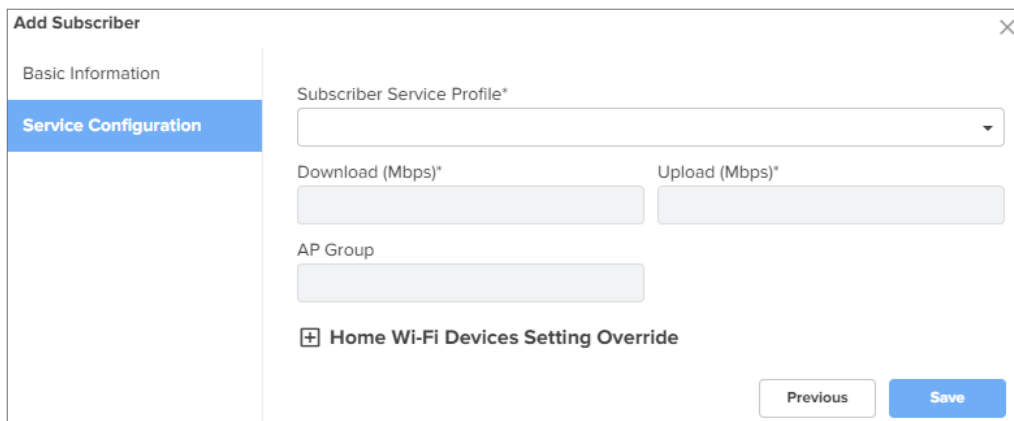
- In the **Add Subscriber** window, configure the details of the subscriber in the **Basic Information** section, as described in [Table 118](#).

Table 118 *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>
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.

- Click **Next**.

The **Service Configuration** tab is displayed.



Add Subscriber

Basic Information

Service Configuration

Subscriber Service Profile*

Download (Mbps)*

Upload (Mbps)*

AP Group

☐ Home Wi-Fi Devices Setting Override

Previous Save

- Select the subscriber service profile to be associated with this subscriber from the **Service Profile** dropdown list.
- 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.
- Click **Devices**.

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.

[Subscribers](#) > Edit new-sub

Basic Information

Service Configuration

Devices

Full Name*

new-sub

Scope

Base Infrastructure

Email*

Phone Number

Subscriber App Status: [Pending](#) [Change Owner](#)

Customer ID

External system customer ID

Address*

cambium

Close Save

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

The Change Owner window is displayed.

Change Owner

⚠ Warning: All old primary and secondary subscriber users will be deleted.

Email*

Close Update

- Enter the new email ID for the subscriber.
- 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:

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

Add Subscriber

Basic Information

Service Configuration

Devices !

Deployment Type

☐ Fiber ☐ Fixed Wireless ☒ Home Site

Home Site*

+

Add Devices to Subscriber Add New

Name	Serial Number	MAC Address	Mesh Type	Status
No Data Available				

Previous Save

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.

Add New Device(s)

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

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.

Device Type

RV22 Home Mesh

Place a cursor in the box and use a barcode scanner to quickly claim devices.

Cancel

- 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

Q

Enter Device name, MAC Address or Serial Number of RV22 Home Mesh

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	<div>Onboarded</div>	



Note

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

Network Services

This section includes the following topics:

- [API Client](#)
- [RESTful API](#)
- [EasyPass](#)
- [CBRS](#)
- [Organization](#)
- [LTE](#)
- [Managing Edge Controller](#)
- [Installation 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](#).

Network Services > API Clients x

cnMaestro supports a RESTful API, allowing customers to read data and perform operations programmatically using their client applications. The API is supported over HTTPS, and messages are exchanged in JSON format. Refer to [Swagger API documentation](#) for RESTful APIs. [Learn more](#)

[Add API Client](#)

Application Name	Application Description	Client Id	Swagger	
Test	N/A	hc0JEq80FbFseE2q	Try it out	✎ 🗑
Test	N/A	YkiOqA20d30OOOh	Try it out	✎ 🗑
34c5c6789	N/A	aXYhziPRmU8792NG	Try it out	✎ 🗑
test_api	N/A	Y8ILma2ilcLd5mtk	Try it out	✎ 🗑
test	N/A	nRLSoqnteTGpocJA	Try it out	✎ 🗑
Test22	N/A	bb0gUCFjFDGOpc1x	Try it out	✎ 🗑
nbn_client1	N/A	IrlJagjdoUifbOm	Try it out	✎ 🗑
itest	N/A	JmHFmc2NUz7Ko2	Try it out	✎ 🗑
test	N/A	koPPXonKkHM2Jle4	Try it out	✎ 🗑
Test	N/A	HmgQnPomfqUON28d	Try it out	✎ 🗑

Showing 1 - 10 Total: 23 10 < Previous 1 2 3 Next >

To add an **API Client**:

1. Navigate to **Network Services > API Clients**.
2. Click **Add API Client**.

Network Services > API Clients x

cnMaestro supports a RESTful API, allowing customers to read data and perform operations programmatically using their client applications. The API is supported over HTTPS, and messages are exchanged in JSON format. Refer to [Swagger API documentation](#) for RESTful APIs. [Learn more](#)

[Add API Client](#)

Application Name	Application Description	Client Id	Swagger	
Test	N/A	hc0JEq80FbFseE2q	Try it out	✎ 🗑
Test	N/A	YkiOqA20d30OOOh	Try it out	✎ 🗑
34c5c6789	N/A	aXYhziPRmU8792NG	Try it out	✎ 🗑
test_api	N/A	Y8ILma2ilcLd5mtk	Try it out	✎ 🗑
test	N/A	nRLSoqnteTGpocJA	Try it out	✎ 🗑
Test22	N/A	bb0gUCFjFDGOpc1x	Try it out	✎ 🗑
nbn_client1	N/A	IrlJagjdoUifbOm	Try it out	✎ 🗑
itest	N/A	JmHFmc2NUz7Ko2	Try it out	✎ 🗑
test	N/A	koPPXonKkHM2Jle4	Try it out	✎ 🗑
Test	N/A	HmgQnPomfqUON28d	Try it out	✎ 🗑

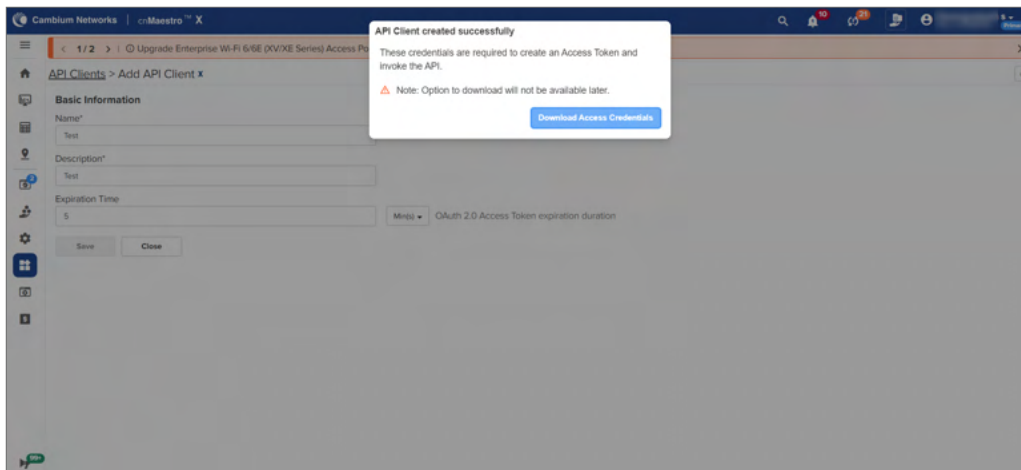
Showing 1 - 10 Total: 23 10 < Previous 1 2 3 Next >

3. **Add API Client** window appears.

4. Enter **Name**.
5. Enter **Description**.
6. Select **Day(s)**, **Hour(s)**, and **Min(s)** from the dropdown list and enter the **Expiration Time**.
7. Click **Save**.

API Client created successfully window pops up.

8. Click **Download Access Credentials**.

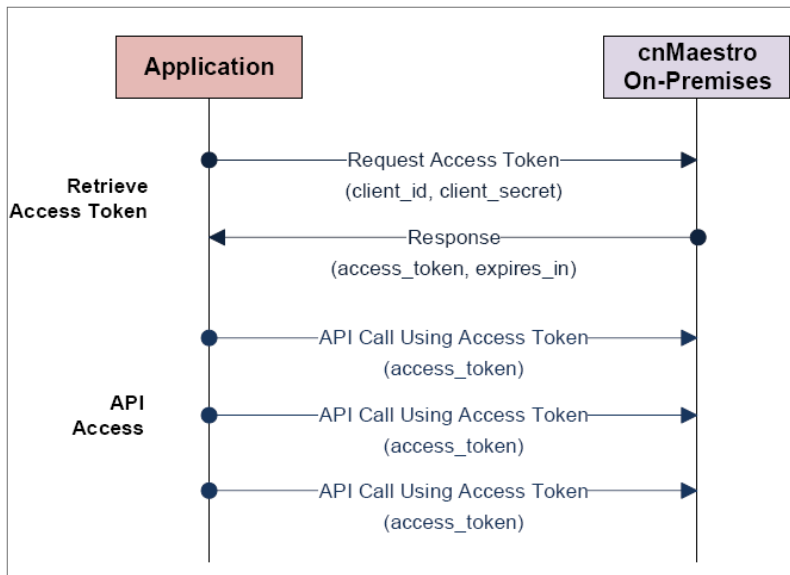


Once the API Clients is added, you can edit, view client Id, or expire all tokens from the **Edit API Client** page.

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	

HTTP Response Status Code	Response Headers	Explanation	Action to be taken
		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)`\n
    """
    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\n
        `host` - host for the url\n
        `path` - path for the url\n
        `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()

```

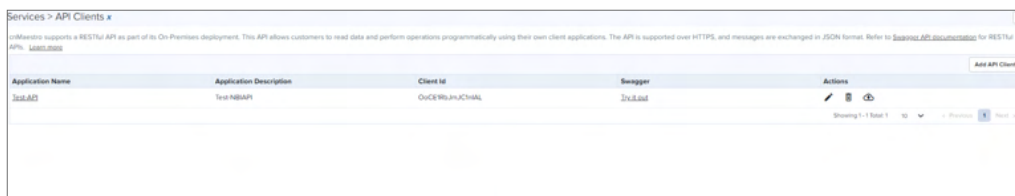
Swagger API

Introduction

Swagger API is a tool set that simplifies the process of RESTful web service documentation. It contains a standardized framework that allows visualization and interaction with API resources.

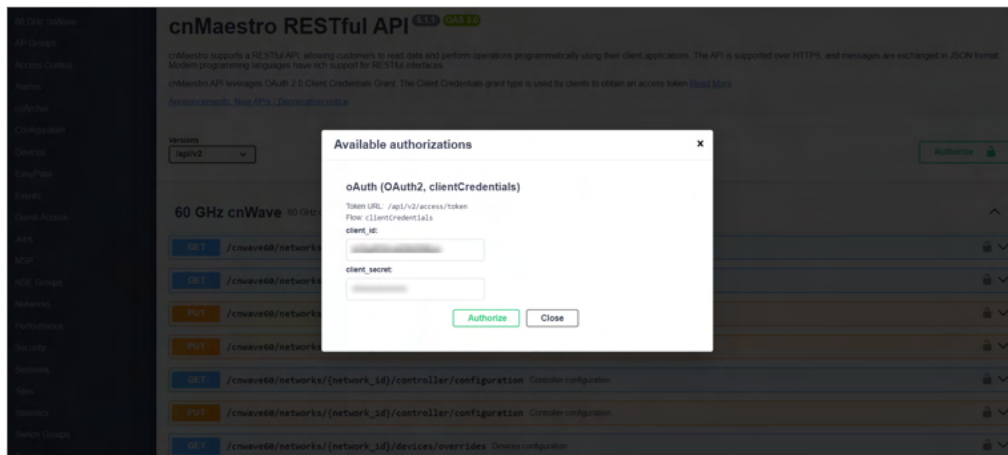
To access Swagger API, perform the following steps:

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



2. Click **Try it out** to open the Swagger UI.

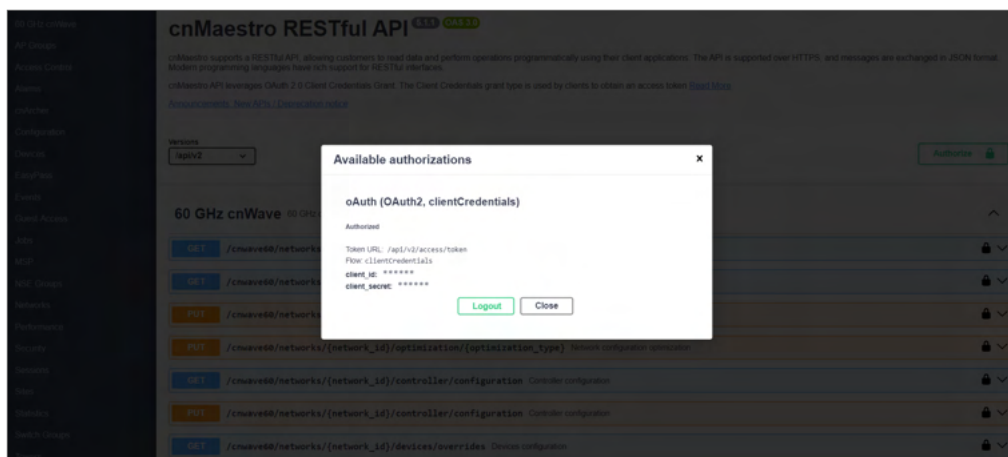
The **Available authorizations** window appears.



3. Enter **client_secret**.

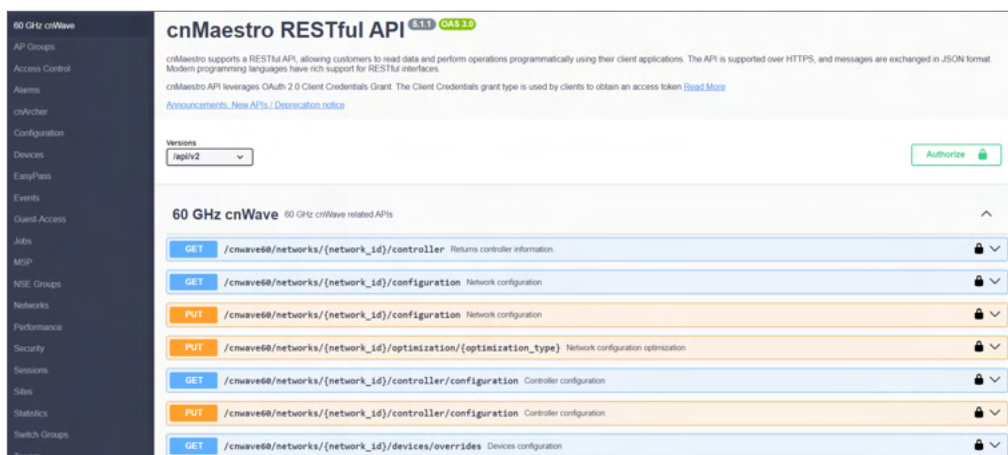
4. Click **Authorize**.

On successful authorization, an **Authorized** message appears in the **Available Authorization** window.



5. Click **Close**.

The authorized **cnMaestro RESTful API** page appears.



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 119 *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 120](#) lists the response codes that are supported in cnMaestro and may be returned through the HTTP protocol.

Table 120 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.
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 121](#) lists the HTTP request codes supported in cnMaestro.

Table 121 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 122 *Resource*

Context	Details
alarms	Current active alarms.
alarms/history	Historical alarms, including active alarms.
devices	Devices, including ePMP, PMP, and WiFi.
events	Historical events.
msp	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 123 *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 124 *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 125](#) describes the standard filtering parameters as shown below:

Table 125 *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 126](#) are not specified, then the start or stop times will be open-ended.

Table 126 *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 127 *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 128 *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 129 *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 130](#) describes about the header and its values as shown below:

Table 130 *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

<pre>grant_type=client_credentials&client_id=s6BhdRkqt3&client_secret=7Fjfp0ZBr1KtDRbnfVdmIw</pre>
--

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.
<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
<pre>/api/v2/access/validate_token</pre>

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: Bearere4e077cf457196eb4d27cf6f02686dc07763059"</pre>
Response
<pre>{"expires_in":85643}</pre>

API Changes

This topic lists the changes made to the cnMaestro APIs.

- [Sunsetted APIs/Fields](#)
- [Deprecated APIs/Fields](#)

Sunsetted APIs/Fields

The following API fields have been removed from their respective APIs.

Request Method	Path	Details
GET	/api/v2/devices	The deprecated field <code>ap_group</code> has been removed in cnMaestro release 5.2.0. Use the <code>profile_attached</code> key as the replacement.
GET	/api/v2/devices/{mac}/performance	The deprecated fields <code>rx</code> , <code>tx</code> , <code>max_rx</code> , <code>min_rx</code> , <code>max_tx</code> , <code>min_tx</code> have been removed in cnMaestro release 5.2.0. Use the fields <code>rx_bps</code> , <code>tx_bps</code> , <code>max_rx_bps</code> , <code>min_rx_bps</code> , <code>max_tx_bps</code> , <code>min_tx_bps</code> as the replacement
GET	/api/v2/devices	The deprecated field <code>Location.type</code> has been removed in cnMaestro release version 5.2.0.
GET	/api/v2/devices	The deprecated field <code>status</code> has been removed in cnMaestro release version 5.2.0. Use the <code>online</code> field as the replacement.

Deprecated APIs/Fields

The following API fields have been deprecated and are scheduled for removal in future releases.

Request Method	Path	Details
GET	/devices/clients	The <code>ap_mac</code> field is deprecated and replaced with a new generic field, <code>device_mac</code> , to accommodate other non-Wi-Fi device types, such as NSE. For a similar reason, <code>rx_bytes</code> and <code>tx_bytes</code> fields have also been taken out of the radio property of an AP device. These deprecations will be removed in cnMaestro release 5.3.0.
GET	/devices/wired_clients	The <code>ap_mac</code> field is deprecated and replaced with a new generic field, <code>device_mac</code> , to accommodate other non-Wi-Fi device types, such as NSE. This deprecation will be removed in cnMaestro release version 5.3.0.

For a detailed overview of all new API changes, updates to existing APIs, and deprecations, see [cnMaestro 5.2.1 API Swagger Announcements](#).

Devices, Statistics, and Performance APIs

Overview

cnMaestro APIs are defined within the Swagger tool, accessed here <https://docs.cloud.cambiumnetworks.com/api/5.2.0/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 not 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	W i- Fi	cnRea ch	cnVisi on	PT P	PT P 8x x	cnMat rix	60 GHz cnWa ve	cnWa ve 5G Fixed	NS E
cbrs_state	CBRS state		✓									
cbrs_status	CBRS status		✓									
config.sync_reason	Configuratio n synchronizat ion reason	✓	✓	✓	✓	✓	✓	✓	✓			✓
config.sync_status	Configuratio n synchronizat ion status	✓	✓	✓	✓	✓	✓	✓	✓			✓

Name	Details	ePM P	PM P	W i- Fi	cnRea ch	cnVisi on	PT P	PT P 8x x	cnMat rix	60 GHz cnWa ve	cnWa ve 5G Fixed	NS E
config.variables	Device is 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	✓	✓	✓	✓	✓	✓		✓		✓	✓
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	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Name	Details	ePM P	PM P	W i- Fi	cnRea ch	cnVisi on	PT P	PT P 8x x	cnMat rix	60 GHz cnWa ve	cnWa ve 5G Fixed	NS E
network	Network	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
onboarding.error_code	Error code if the device onboarding fails See Device onboarding failure error codes .	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
onboarding.state	Onboarding state of the device See Supported values for onboarding state .	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
online	Offline or online	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
product	Product name	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
profile_attached	Profile attached to the device			✓								✓
registration_date	Registration date	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
role	Role of the device [PTP Slave, PTP Master]						✓					
site	Site			✓					✓	✓		✓
site_id	Site unique identifier			✓					✓	✓		
software_version	Active Software version	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
status_time	Uptime/downtime interval (seconds)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
temperature	Temperature							✓				

Name	Details	ePM P	PM P	W i- Fi	cnRea ch	cnVisi on	PT P	PT P 8x x	cnMat rix	60 GHz cnWa ve	cnWa ve 5G Fixed	NS E
tower	Tower	✓	✓		✓	✓	✓	✓	✓		✓	
type	Device type See Supported values for device type .	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Supported values for onboarding state

Onboarding State	Details
IN_QUEUE	Device is in queue waiting for cnMaestro claim process to start.
WAITING_FOR_DEVICE	cnMaestro is trying to establish connection with the claimed device.
WAITING_FOR_APPROVAL	Device is waiting to be approved in cnMaestro.
UPDATING	Device software is being updated prior to getting onboarded.
ONBOARDED	Device is onboarded successfully.
ONBOARDED_WITH_ERRORS	Device is onboarded to cnMaestro but with errors.
WAITING_FOR_CLOUD_SYNC	Device is waiting for cnMaestro cloud sync process to acquire a subscription slot.
CLOUD_SYNC_ERROR	Device onboarding failed due to cloud sync error. For error details, see Device onboarding failure error codes .

Supported values for device type

- epmp
- pmp
- wifi-home
- wifi-enterprise
- cnreach
- ptp
- cnmatrix
- 60ghz-cnwave
- nse
- wifi-xirrus
- ptp 820/850
- cnWave 5G Fixed
- cnvision

Device onboarding failure 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_TYPE	Unsupported device type in current account view - {{view}}.
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 On-Premises instance.
SUBSCRIPTION_FAIL_TOO_MANY ASSOCS	Device is mapped to another On-Premises instance.

Statistics API Response (v2 Format)

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

- [60 GHz cnWave](#)
- [cnMatrix](#)
- [cnReach](#)
- [Fixed Wireless \(cnVision, ePMP and PMP\)](#)
- [PTP 650/670/700](#)
- [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

Name	Details	Mode
mac	MAC address	All
IP	IP address	All
managed_account	Managed account name	All
memory	Available memory	All
mode	Device mode	All
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

General

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

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

Name	Details	cnVision	ePMP	PMP
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
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- tls] 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	

Name	Details	cnVision	ePMP	PMP
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
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, Standard WiFi]	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			SM

Name	Details	cnVision	ePMP	PMP
	MIMO-B)]			
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	
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

Name	Details	Mode
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 [up, down]	All
interfaces[].port_duplex	Interface duplex type [Half, Full, Auto]	All
interfaces[].speed	Interface speed	All

Wi-Fi

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

Name	Details	Mode
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
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

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
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

Name	Details	Mode
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
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 is shown for the following devices:

- [60 GHz cnWave](#)
- [cnMatrix](#)
- [cnReach](#)
- [Fixed Wireless \(cnVision, ePMP and PMP\)](#)
- [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[].port	Port name	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

Name	Details
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
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

Name	Details	Mode
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
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

Name	Details	cnVision	ePMP	PMP
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
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[].pkt_error	Ports packet error	All
ethports[].port	Port name	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

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
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

cnWave 5G Fixed

General




Name	Details	Mode
mac	Device 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	Duration (seconds) that the device has been online	All
cpe_registered	Count of CPEs registered with the BTS	BTS
cpe_connected	Count of CPEs connected with the BTS	BTS
cpe_registrationCnt	Number of times the CPE has registered with the BTS	CPE

Radio

Name	Details	Mode
ul_throughput	Uplink throughput of BTS	BTS
dl_throughput	Downlink throughput of BTS	BTS
cpe_ul_throughput	Uplink throughput of CPE	CPE
cpe_dl_throughput	Downlink throughput of CPE	CPE
cpe_ul_evm	Uplink Error Vector Magnitude (EVM) of CPE	CPE
cpe_dl_evm	Downlink EVM of CPE	CPE
cpe_ul_mcs	Uplink Modulation Coding Scheme (MCS) of CPE	CPE
cpe_dl_mcs	Downlink MCS of CPE	CPE
cpe_ul_rxPower	Uplink receive power of CPE	CPE
cpe_dl_rxPower	Downlink receive power of CPE	CPE

Client API Response (v2 Format)

Client details API Response v2 format are shown below:

Name	Details
address_type	IP address type (DHCP/Static)
ap_mac	<div>  <div> Note This field has been deprecated since release 5.0.0 and will be fully removed in release 5.3.0. Use the <code>device_mac</code> field instead. </div> </div>
age	Client session duration in seconds
auth_status	Client authentication status
auth_type	Client authentication type
client_type	Client type (Client Guest Client)
expires	Client expiration duration
guest_access_type	Type of guest access in portal
interface	Interface to which the client is connected
ip	IP address of client
mac	Client MAC address
managed_account	Managed account name
managed_account-2	Managed account name
manufacturer	Manufacturer name
name	Client name
os	Operating system running on the client
portal_mode	Mode of the portal to which the client is connected
radio.band	Band (2.4 GHz/5 GHz)
radio.id	ID of the radio
radio.rssi	RSSI
radio.snr	SNR
radio.ssid	SSID
radio.tx_bytes	<div>  <div> Note This field has been deprecated since release 5.0.0 and will be fully removed in release 5.3.0. Use the <code>tx_bytes</code> field instead. </div> </div>
radio.rx_bytes	<div>  <div> Note This field has been deprecated since release 5.0.0 and will be fully removed in release 5.3.0. Use the <code>rx_bytes</code> field instead. </div> </div>
tx_bytes	Transmit bytes
rx_bytes	Received bytes
total_quota	Total quota

Name	Details
total_quota_balance	Total quota balance
upload_quota	Upload quota
upload_quota_balance	Upload quota balance
download_quota	Download quota (Note: Applicable only for guest client)
download_quota_balance	Download quota balance (Note: Applicable only for guest client)
user	User ID that is used to authenticate the client
vlan	VLAN ID assigned
ipv6	Client IPv6 address
device_mac	AP MAC address

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
e88916f5b663clea966af835c8a0a19c20d17686" -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.

Status	Description
3	RADIUS timeout, AP didn't received the RADIUS response.
4	Missing RADIUS server config on the WLAN config of the AP.
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. prefixQs and action 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

The screenshot shows the configuration interface for a 60 GHz cnWave Network. The 'Advanced' tab is selected under the 'E2E Controller' section. A modal window is open for the field `radioParamsBase.fwParams.wsecEnable`, displaying its value as 1, its description 'Enable airlink encryption (0: Disabled, 1: Enabled, 2: Enabled with 802.1X)', its action 'Reload firmware when changed', and its overrides 'Base value: 0' and 'Network override: not set'.

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`

60 GHz cnWave Network > 8_Nodes_Ext_E2e

Dashboard Notifications **Configuration** Links Statistics Report.X Software Update Tools

Basic Management Security **Advanced** E2E Controller

All the settings below are for advanced users only.

Search Base: default Firmware: 10.6.0 Hardware: V1000 Optimization Table JSON Add New

Field	Description	Status	
assertParams.cambiumAssertRecoveryEnabled	Enables Cambium fw assert recovery.	set	Optimize Control Superframe Allocation
assertParams.fwAsserts.1	List of Assert codes for recovery.	set	Optimize DPA Zone Allocation
assertParams.fwAsserts.2	List of Assert codes for recovery.	set	Clear Node Auto Configuration
assertParams.fwAsserts.3	List of Assert codes for recovery.	set	0x4606
assertParams.fwAsserts.4	List of Assert codes for recovery.	set	0xfbde
assertParams.fwAsserts.5	List of Assert codes for recovery.	set	0x460c
assertParams.fwAsserts.6	List of Assert codes for recovery.	set	0x401f
assertParams.fwAsserts.7	List of Assert codes for recovery.	set	0xe00a
assertParams.fwAsserts.8	List of Assert codes for recovery.	set	0x4065
bgpParams.allowNonDefaults	na	set	false
bgpParams.cpePrefixesAutoAdvertisement	Enable automatic advertisement of CPE prefixes, instead of static 'cpeNetworkPrefix'.	set	true

Save Reset

Device Logs

☒ Enable Recommended to be used only by Cambium Support Team.

Update

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

The screenshot shows the configuration interface for a 60 GHz cnWave device. The 'Advanced' tab is selected, displaying a table of configuration fields. A search bar at the top left contains the text 'linkParamsBase.fwParams'. The table has two columns: 'Field' and 'Description'. The first row shows the field 'linkParamsBase.fwParams.minTxPower' with the description 'The minimum Tx power index assigned when TPC algorithm is enabled.' To the right of the table, a modal window displays the configuration details for this field, including its value (7), allowed ranges (0,31), and a description of the field's function.

Field	Description
linkParamsBase.fwParams.minTxPower	The minimum Tx power index assigned when TPC algorithm is enabled.



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"
  }
}
```

60 GHz cnWave Network > E2E-Ext-Network-WithoutInternet

Dashboard Notifications **Configuration** Links Statistics Report X Software Update Tools

Basic Management Security Advanced **E2E Controller**

All the settings below are for advanced users only.

Search prefixAllocParams.seedPrex Base Fields : Show All

Field	Description	Status
prefixAllocParams.seedPrefix	Network seed prefix used for centralized and determ...	modified

Save Reset

Value (prefixAllocParams.seedPrefix)

fd00:ceed:8b03:2400::/56

Regular expression: ([0-9a-fA-F:]+)([0-9]+)

Save Close

Description
Network seed prefix used for centralized and deterministic prefix allocation.

Action
Update prefix alloc params when changed

Overrides
Base value: undefined
Override: fd00:ceed:8b03:2500::/56



Warning

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

EasyPass

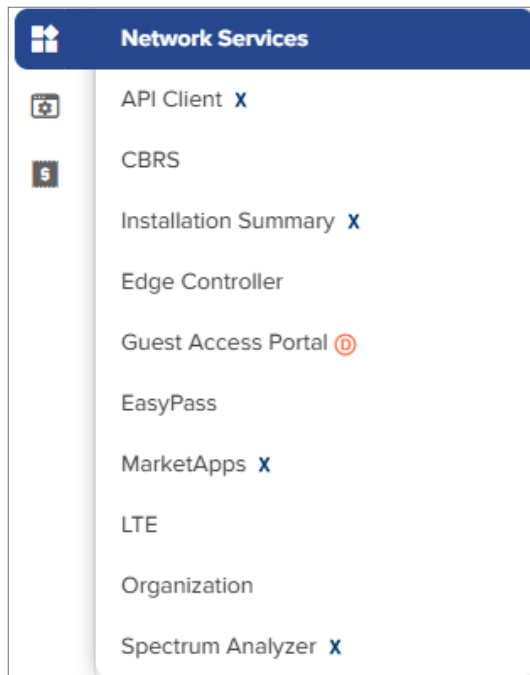
cnMaestro supports a guest access solution which provides an intuitive interface for various guest access methods used in the customer deployments. It allows the clients to connect to the internet through free tiers, vouchers, or paid access types. It also creates a separate network for guests by providing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



Note

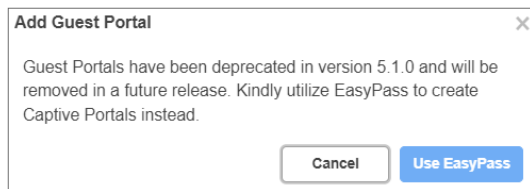
From cnMaestro 5.1.0 release onwards, the **Guest Access Portal** configuration wizard is deprecated and a new wizard, **EasyPass**, is introduced (as shown in [Figure 531](#)).

Figure 531 *Network Services > EasyPass*



When you create a new portal in the **Guest Access Portal** page, a window appears notifying that guest portals are deprecated and **EasyPass** must be used (as shown in [Figure 532](#)).

Figure 532 *The Add Guest Portal window*



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

[Table 131](#) lists the supported devices and their compatibility with EasyPass.

Table 131 *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.



Note

The **Social Login** option is available only in cnMaestro Cloud accounts.

- 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



Note

The portal types listed under the **Employee/Student Access** category are available only in cnMaestro Cloud accounts.

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.
- Onboarding **X**—Clients can register on an open SSID with their email, Google Workspace, or Microsoft Azure (Office 365) credentials to receive an enhanced pre-shared key (ePSK), which can be used to connect to a secure network SSID.

**Note**

- Microsoft Azure **X** and Google Login **X** are supported on APs running firmware version 6.x or later.
- Onboarding **X** is supported only on Wi-Fi 6 and 6E APs running firmware version 6.6.2 or later.

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**

- cnMaestro Essentials supports a maximum of four EasyPass portals.
- cnMaestro X supports a maximum of 500 EasyPass portals.

The following table lists the support of EasyPass portal types across Cloud and On-Premises accounts.

Table 132 *EasyPass portal types supported on Cloud and On-Premises*

EasyPass portal type	cnMaestro Cloud	cnMaestro On-Premises
Guest/Public Access		
Self Registration X	✓	✓
Sponsored Guest X	✓	✓
Voucher	✓	✓
One Click	✓	✓
Social Login (Google and Facebook) Available on the Design page in the following portals: <ul style="list-style-type: none"> • One Click • One Click + Voucher • One Click + Paid X 	✓	
Paid X	✓	✓
WiFi4EU	✓	✓
Employee/Student Access		
Microsoft Azure X	✓	
Google Login X	✓	
Onboarding X	✓	
Combined		
One Click + Voucher	✓	✓
One Click + Paid X	✓	✓
Voucher + Paid X	✓	✓

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	IoT Device
Self Registration X		✓				✓	✓	✓	✓	✓	
Sponsored Guest X			✓								
Voucher			✓			✓	✓	✓			
One Click							✓	✓	✓	✓	
Paid X		✓				✓		✓		✓	
WiFi4EU										✓	
Microsoft Azure X	✓				✓						
Google Login X	✓				✓	✓					
Onboarding 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 Onboarding X portal](#)
 - [Adding a new user](#)
 - [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 One Click screen parameters](#)
 - [The Plans screen parameters](#)
- [Accessing the common tabs](#)
 - [Sessions](#)
 - [Guests](#)
 - [Adding a new guest user](#)
 - [Vouchers](#)
 - [Paid Transactions X](#)
 - [Users X](#)

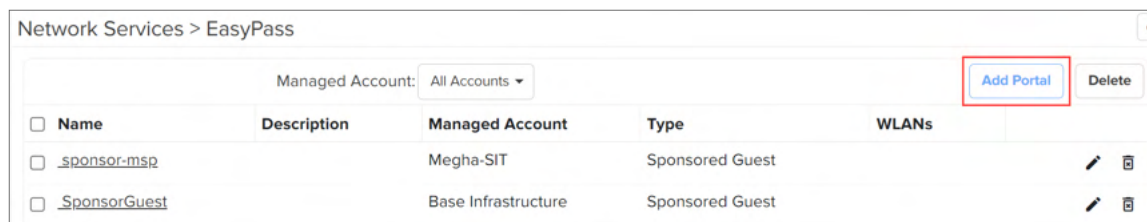
Creating a portal

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 533 *The EasyPass screen*



2. Click **Add Portal**.

The **Select Portal Type** window appears.



Note

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

[Figure 534](#) displays the options available for cnMaestro Essentials.

Figure 534 The Select Portal Type window—cnMaestro Essentials

Figure 535 displays the options available for cnMaestro X.

Figure 535 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** dropdown 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 **Save and Continue**.

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.



Note

- For **One Click** portal, go to [step 8](#) and configure the parameters on the **Limits** screen.
- The **Voucher**, **One Click + Voucher**, and **Voucher + Paid X** portal types have a few 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 a few common parameters that you must configure on their respective **Plans** screens. For information on parameters of the **Plans** screen, see [The Plans screen parameters](#).
- The **One Click + Voucher**, and **One Click + Paid X** portal types have a few common parameters that you must configure on their respective **One Click** screens. For information on parameters of the **One Click** screen, see [The One Click screen parameters](#).

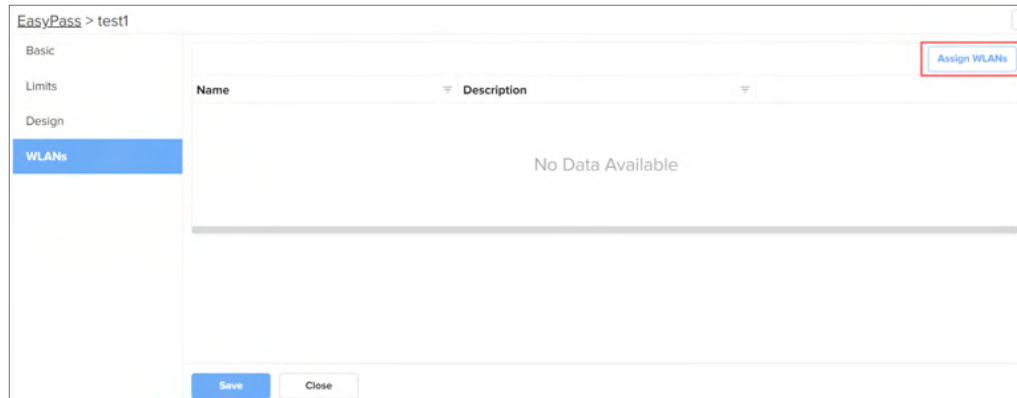
Depending on the portal type you selected, you will either see a **Limits** screen or portal-specific screen.

- For the **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 **Paid X** portal type, follow the additional steps described in [Creating Paid X 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](#).
- For the **Onboarding X** portal type, follow the additional steps described in [Creating Onboarding X portal](#).
- For the **One Click + Voucher** portal type, follow the additional steps described in [Creating One Click + Voucher portal](#).
- For the **One Click + Paid X** portal type, follow the additional steps described in [Creating One Click + Paid X portal](#).

- For the **Voucher + Paid X** portal type, follow the additional steps described in [Creating Voucher + Paid X portal](#).
- Configure the parameters of the **Limits** screen as described in [The Limits screen parameters](#).
 - Click the **Design** tab and configure the parameters as described in [The Design screen parameters](#).
 - Click the **WLANS** tab.

The **WLANS** screen appears.

Figure 536 *The WLANS screen*



Note

- The **WLANS** screen is different for the **Onboarding X** portal type. When the **Enable Self-Onboarding** checkbox is selected from the **Onboarding** screen, the **WLANS** screen displays the **Network SSID** and **Registration SSID** sections.

- Click **Assign WLANS**.

The **Assign WLANS** window appears.

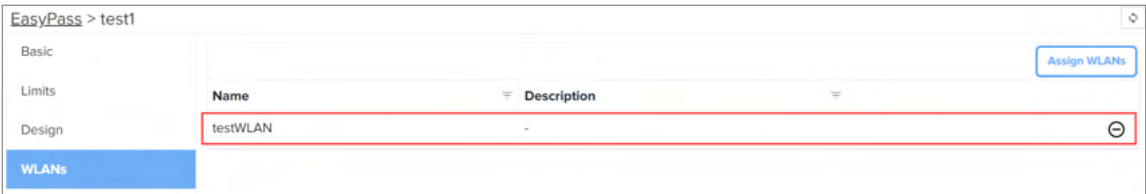
Figure 537 *The Assign WLANS window*

Assign WLANS						
<input type="text" value="Search"/>						
<input type="checkbox"/> Name	Description	Portal Ac...	Portal Mode	Portal Name	AP Group	
<input type="checkbox"/> Default Enterprise	-	Disabled	Internal Access Point	-	Default Enterprise_diva_bkp_311_RTL	
<input type="checkbox"/> API-Test	-	Enabled	cnMaestro	EOG	API-Test_Try_Try1	
<input type="checkbox"/> toh-nv12	home wpa2 psk native vlan ssid.	Disabled	Internal Access Point	-	TOH 3SSIDs GL FLs TOH 3SSIDs GL FLs	
<input type="checkbox"/> toh-psk2	home wpa2 psk ssid.	Disabled	Internal Access Point	-	TOH 3SSIDs GL FLs TOH 3SSIDs GL FLs	
<input type="checkbox"/> toh-eap2	home wpa2 eap ssid.	Disabled	Internal Access Point	-	TOH 3SSIDs GL FLs TOH 3SSIDs GL FLs	
<input type="checkbox"/> Raja-WLAN1-Open	-	Disabled	cnMaestro	400-NewPortal	GA-Paid_Raja-Network	
<input type="checkbox"/> OS2-WPA2-EAP_Osnabruck	WPA2EAP_1tr_all	Disabled	Internal Access Point	-	Jaguar_OS2_Osnabruck_Tiger_OS2_Os	
<input type="checkbox"/> toh-eap401	toh-eap2 ssid for 4.0.1 testing.	Disabled	Internal Access Point	-	TOH 3SSIDs 401 TOH 4SSIDs 6E	
<input type="checkbox"/> toh-psk401	toh-psk2 ssid for 4.0.1 testing	Disabled	Internal Access Point	-	TOH 3SSIDs 401 TOH 4SSIDs 6E	

- Select the required WLANS and click **Assign**. For example, **testWLAN**.

The selected WLAN is added to the WLANS page.

Figure 538 *Assigned WLAN*



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

These buttons are available across all portal types.

13. 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 One Click screen parameters](#)
- [The Plans screen parameters](#)

The Basic screen parameters

[Figure 539](#) displays the **Basic** screen parameters.

Figure 539 *The Basic screen*

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

**Note**

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

The Limits screen parameters

[Figure 540](#) displays the **Limits** screen parameters.

**Note**

The parameters in the Limits screen differs based on the portal type you select. Refer to the table below for more details.

Figure 540 *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	The specified duration after which a user's session automatically expires, disconnecting the user from the Wi-Fi network. The following options are supported:

Table 135 *The Limits screen parameters*

Parameter	Description
	<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 dropdown list.</p> <p>Note: When you select the Custom option, you can configure the minimum duration value to 1 for Days, Hours, and Minutes.</p>
Lockout Time	<p>The lockout time restricts the ability to create a new session for the specified duration when a session expires.</p> <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 dropdown list.</p> <p>Note: The Lockout Time parameter is not available for Self Registration X, Sponsored Guest X, Voucher, Paid X, Microsoft Azure X, Google Login X, and Onboarding 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>

Table 135 *The Limits screen parameters*

Parameter	Description
	Maximum value: 1000000
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 dropdown 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. 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 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>Minimum value: 1</p> <p>Maximum value: 200</p>

**Note**

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

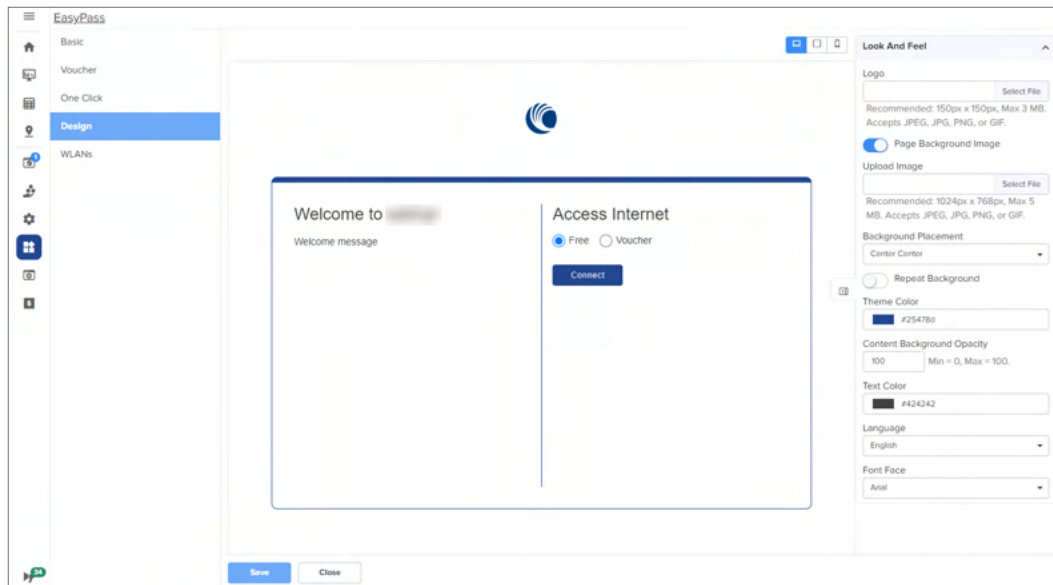
The Design screen parameters

[Figure 541](#) displays the **Design** screen parameters.

**Note**

The layout of the preview window differs based on the portal type you select.

Figure 541 *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	<p>Logo for the portal.</p> <p>Recommended size: 150 x 150 pixels</p> <p>Maximum file size: 3 MB</p> <p>Supported formats: JPEG, JPG, PNG, or GIF</p>
Page Background Image	<p>A page background image allows you to enhance the visual appearance of your portal. You can upload an image or a pattern to create a unique and engaging backdrop.</p> <p>The Page Background Image option is disabled by default. Enable the Page Background Image option and select an image file to upload.</p>
Upload Image	<p>This parameter is applicable only when the Page Background Image option is enabled.</p> <p>Select an image file to upload.</p> <p>Recommended size: 1024 x 768 pixels</p> <p>Maximum file size: 5 MB</p> <p>Supported formats: JPEG, JPG, PNG, or GIF</p>
Background Placement	<p>Background placement for the selected image.</p> <p>Select the required background placement option from the Background Placement dropdown list.</p> <p>The following options are supported:</p> <ul style="list-style-type: none"> • Left Top • Left Center

Table 136 *The Design screen parameters*

Parameter	Description
	<ul style="list-style-type: none"> • Left Bottom • Right Top • Right Center • Right Bottom • Center Top • Center Center • Center Bottom <p>By default, the Center Center option is selected.</p>
Repeat Background	<p>This parameter is applicable only when the Page Background Image option is enabled.</p> <p>Enable the Repeat Background option to repeat the selected background.</p> <p>The Repeat Background option allows you to repeat a small image or pattern across your portal, creating a continuous background.</p> <p>Note: This feature is beneficial for smaller backgrounds or patterns, as it enhances the overall appearance without the need to enlarge or stretch the image, which could cause distortion or pixelation.</p>
Theme Color	Theme color for the design page.
Content Background Opacity	<p>A value to increase or decrease the background opacity on the portal.</p> <p>Default value: 100</p> <p>Minimum value: 0</p> <p>Maximum value: 100</p>
Text Color	Color of the text on the portal.
Language	<p>Language for the content displayed on the EasyPass portal.</p> <p>The following languages are supported:</p> <ul style="list-style-type: none"> • English • French • German • Italian • Korean • Polish • Spanish

Table 136 *The Design screen parameters*

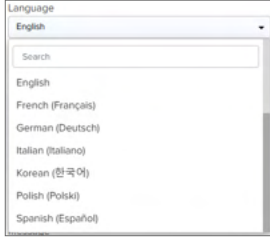
Parameter	Description
	 <p>Default is English.</p> <p>When you change the language to a value other than English, the design page parameters are updated in the selected language, except the Title, message, and any terms and conditions that you might have added. You must manually enter these contents in the selected language.</p>
Font Face	<p>Type of font to be used for the portal.</p> <p>The following options are supported:</p> <ul style="list-style-type: none"> • Arial • Times New Roman • Verdana • Tahoma
Title	Title name to be displayed on the portal.
Message	Welcome message for the portal.
Terms and Conditions	Terms and conditions to be displayed on the portal.
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 fields to include in the design page by clicking Add Custom Field.</p> <p>The following options are supported:</p> <ul style="list-style-type: none"> • Text • Number • Email • Phone • Date • Name
Connect	<p>An option to provide access for users to the internet.</p> <p>Click Connect to access the internet.</p> <p>This is the default option available on the design page.</p>
Social Login	Enable or disable the social login option to log in to the

Table 136 *The Design screen parameters*




Parameter	Description
	<p>EasyPass portal.</p> <p>This option is available only in cnMaestro Cloud accounts.</p> <p>The following social login options are supported:</p> <ul style="list-style-type: none"> • Google • Facebook <p>When the social login option is enabled, the portal page contains Sign in with Facebook and/or Sign in with Google options.</p>  <p>Note: When the social login option is enabled, Sign in with Facebook and/or Sign in with Google buttons replace the Connect button.</p>
Custom Styling (CSS)	<p>Enable the Custom Styling (CSS) option and select a CSS file to upload.</p> <p>You also have an option to download a sample CSS file.</p>
Device-specific view options of the design page 	<p>The view options on the design page are tailored for various devices.</p> <p>The following options are supported:</p> <ul style="list-style-type: none"> • Desktop View • Tablet/iPad View • Mobile View <p>By default, desktop view is selected.</p> <p>Note: The device-specific view options are available across all portal types on their respective Design screens.</p>
View in new tab and Copy to clipboard options of the design page 	<p>The following options are available across all portal types on their respective Design screens once you save the Design page.</p> <ul style="list-style-type: none"> • View in new tab • Copy to clipboard
Collapse/Expand details panel	An option to collapse or expand the details panel.

Table 136 *The Design screen parameters*

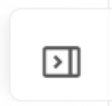
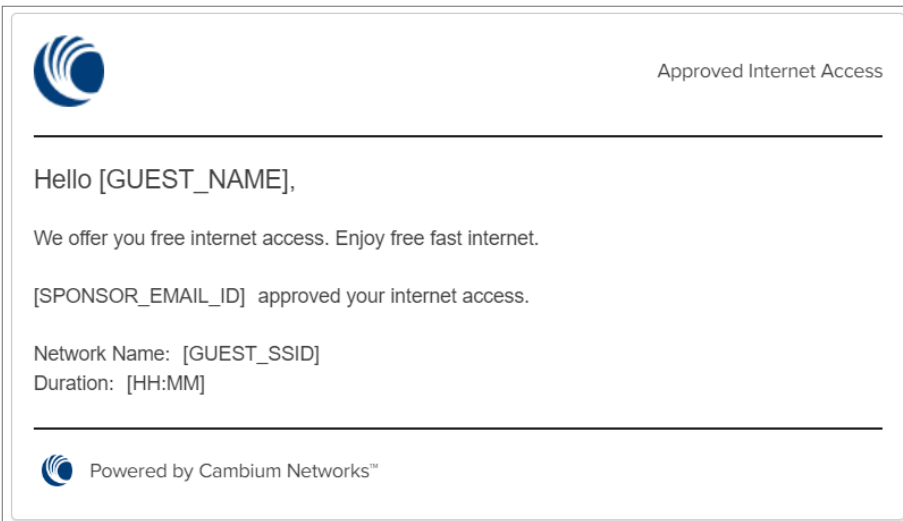
Parameter	Description
	
Note: For the Self RegistrationX portal type, you must also configure additional parameters using the Preview tab and the Email Template tab.	
Preview tab The Preview tab is selected, by default. The following fields appear on the design page.	
Email	Enter the email ID. This field 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:	
	
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. 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 dropdown list.
Payment Code	The payment code of the plan.

Table 136 *The Design screen parameters*

Parameter	Description
	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 Onboarding X portal type, the following option is available:	
Connect	You must enter the email ID and name before you click the Connect button.
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 10](#) 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	<p>Name of the voucher plan.</p> <p>Note: This parameter supports:</p> <ul style="list-style-type: none"> A minimum of one and maximum of 64 characters. Only alphanumeric, underscore (_), and dashes (-). <p>This parameter is mandatory.</p>
Quantity	<p>Quantity (in integers) of the voucher.</p> <p>Minimum value: 1</p>

Table 137 *The Voucher screen parameters*

Parameter	Description
	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 checkbox, you can connect unlimited number of devices.

The One Click screen parameters

[Figure 542](#) displays the **One Click** screen parameters.



Note

The **One Click** screen appears only when you select either **One Click + Voucher** or **One Click + Paid X** portal types.

Figure 542 *The One Click screen*

[Table 135](#) describes the parameters that appear only for **One Click + Voucher** or **One Click + Paid X** portal types on the respective **One Click** screens.

Table 138 *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 dropdown list.</p>
Lockout Time	<p>The lockout time restricts the ability to create a new session for the specified duration when a session expires.</p> <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 dropdown list.</p>

Table 138 *The Limits screen parameters*

Parameter	Description
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 dropdown 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. A minimum of 1 GB and a maximum of 8000 GB.

**Note**

After configuring the parameters in the **One Click** screen, continue to [step 9](#) to configure the parameters in the **Design** and **WLANs** screens.

The Plans screen parameters

[Figure 543](#) 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 543 *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 **Add Plan** (as shown in [Figure 543](#)).

The **Add New Plan** window appears.

Figure 544 *The Add New Plan window*

[Table 139](#) 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 139 *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	

Table 139 The Add New Plan window parameters

Parameter	Description
Total	<p>Enable or disable the parameter.</p> <p>If you disable the checkbox, you must specify the device limit.</p> <p>If you enable the checkbox, you can connect unlimited number of devices.</p>
Device Limit	
Unlimited	


- Click **Add** (as shown in [Figure 544](#)).

The plan is added.

Figure 545 Plan added



Note

Use the edit () icon to modify a plan.

- Select the required payment gateway option from the **Payment Gateway** dropdown list (as shown in [Figure 546](#)) and configure corresponding parameters as described in the following sections..

Figure 546 Payment gateway options

The following options are supported:

- [IP Pay](#)
- [Quickpay](#)
- [PayPal](#)



Note

Set the mandatory fields for the selected payment gateway options.

IP Pay

[Figure 547](#) displays the parameters available for the **IP Pay** payment gateway.

Figure 547 IP Pay payment gateway

The screenshot shows a configuration form for the IP Pay payment gateway. It includes a dropdown menu for 'Payment Gateway*' set to 'IP Pay'. Below it is a 'Callback URL' field with a long URL and a note to configure it as the Callback URL under IPPay application settings. There are input fields for 'Paypage URL*', 'Paypage API*', 'Merchant ID*', 'Customer ID*', and 'Terminal ID*'. The 'Terminal ID*' field is pre-filled with a blue bar. At the bottom is a 'Password*' field with a 'Show' button.

Configure the IP Pay parameters described in [Table 140](#).

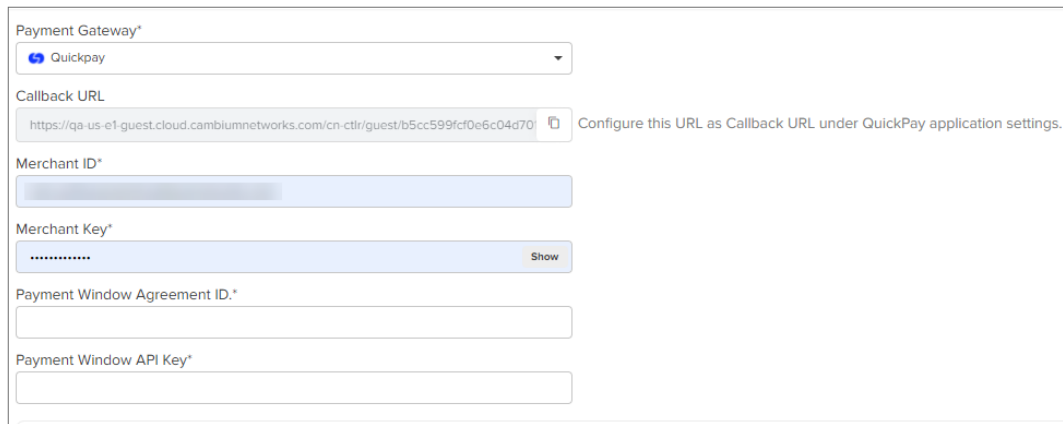
Table 140 IP Pay parameters description

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.
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.	

Quickpay

[Figure 548](#) displays the parameters available for the **Quickpay** payment gateway.

Figure 548 Quickpay payment gateway



The screenshot shows a configuration form for the Quickpay payment gateway. It includes a dropdown menu for 'Payment Gateway*' with 'Quickpay' selected. Below it is a 'Callback URL' field containing a long URL, with a note to 'Configure this URL as Callback URL under QuickPay application settings.' followed by a document icon. There are input fields for 'Merchant ID*', 'Merchant Key*' (with a 'Show' button), 'Payment Window Agreement ID.*', and 'Payment Window API Key*'. The fields for Merchant ID and Merchant Key are currently empty.

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

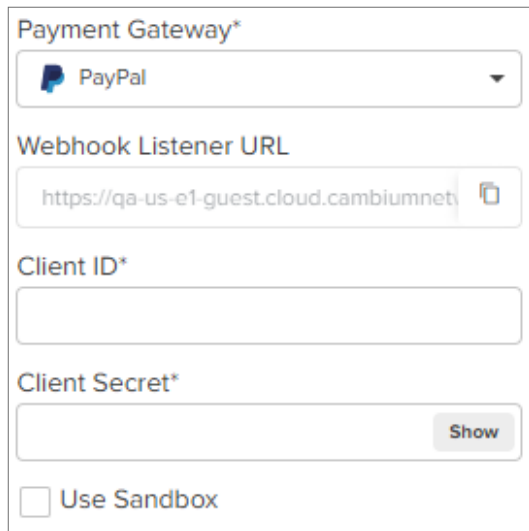
Table 141 Quickpay parameters description

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.	

PayPal

[Figure 549](#) displays the PayPal payment gateway screen.

Figure 549 PayPal payment gateway



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

Table 142 PayPal parameters description

Parameter	Description
Webhook Listener URL	URL used by the payment gateway to call back after a transaction is processed. This field is automatically generated, by default, and cannot be modified. Configure this URL in the PayPal application settings when creating the PayPal API client.
Client ID	ID that the PayPal API uses to identify the client. This value is available in the PayPal application.
Client Secret	Secret key that the PayPal API uses to authenticate the client's identity. This value is available in the PayPal application.
Use Sandbox	Select this checkbox if you want to use the PayPal developer account.
Note: The parameters of the PayPal option are also applicable to One Click + Paid X and Voucher + Paid X portal types.	



Note

After configuring the parameters in the **Plans** screen, continue to [step 9](#) to configure the parameters in the **Design** and **WLANS** screens.

Accessing the common tabs

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

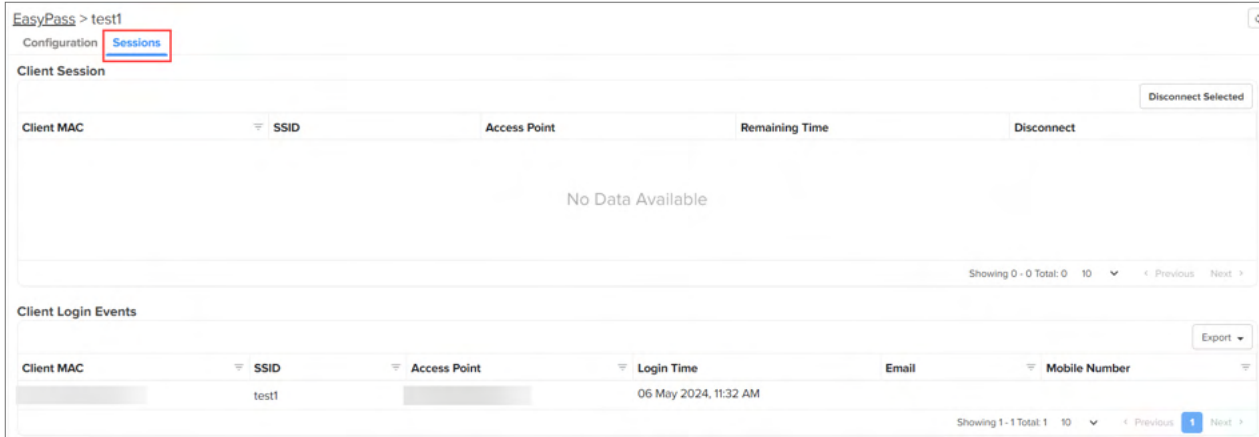
- [Sessions](#)
- [Guests](#)
 - [Adding a new guest user](#)
- [Vouchers](#)
 - [EasyPass](#)

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

Sessions

You can access the **Sessions** page using the **Sessions** tab from, as shown in [Figure 550](#), from any of the portals.

Figure 550 *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** checkbox 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.

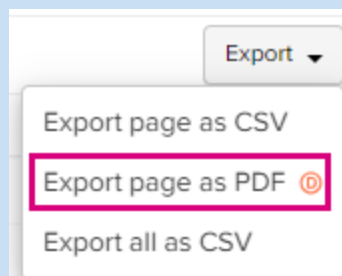
Administrators can export the client login events using the following options:

- Export page as CSV
- Export all as CSV



Note

The **Export page as PDF** option is deprecated from cnMaestro release version 5.2.0 onwards. This option will be completely removed from the UI in release version 5.3.0.

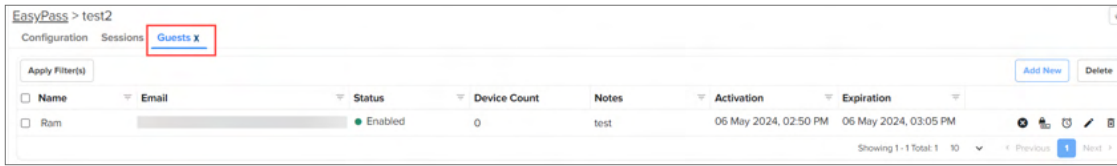


Guests

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 551](#)).

Figure 551 *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 552 *The Add New User window*

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 **Add**.

The **User added successfully** window appears with a message showing a new password (as shown in [Figure 553](#)).

Figure 553 *The User added successfully window*

6. Click **OK**.

A new guest user is added (as shown in [Figure 554](#)).

Figure 554 *The new guest user details*



Name	Email	Status	Device Count	Notes	Activation	Expiration
[Redacted]	[Redacted]	Expired	0	test	06 May 2024, 02:50 PM	06 May 2024, 03:05 PM
Mike	[Redacted]	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 554](#)).

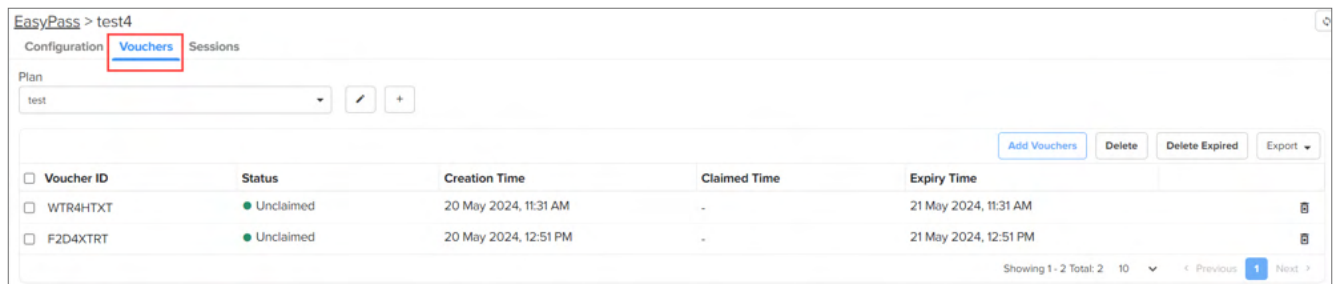
- Use the disable access (🚫) icon to disable access.
- Use the reset password (🔑) icon to reset a password.
- Use the extend session (🕒) icon to extend a session.
- Use the edit (✎) icon to edit the user details.
- Use the delete (🗑️) icon to delete a user.

Vouchers

You can access the **Vouchers** page using the **Vouchers** tab (as shown in [Figure 555](#)).

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 vouchers.

Figure 555 *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



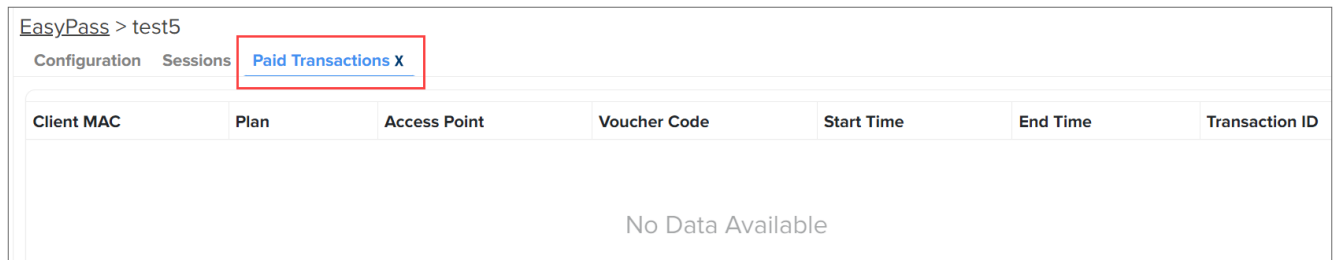
Note

- The **Vouchers** tab appears only for the **Voucher**, **One Click + Voucher**, and **Voucher + Paid X** portal types.
- The maximum number of vouchers that users are allowed to create per Voucher portal is as follows:
 - cnMaestro X—30,000
However, users are allowed to create a maximum of 2,000 vouchers at a single time.
 - cnMaestro Essentials—4,000
However, users are allowed to create a maximum of 1,000 vouchers at a single time.

Paid Transactions X

You can access the **Paid Transactions X** page using the **Paid Transactions X** tab (as shown in [Figure 556](#)).

Figure 556 The Paid Transactions X tab



EasyPass > test5						
Configuration Sessions Paid Transactions X						
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 557](#)).

Figure 557 The Users X tab

EasyPass > Google-New

ConfigurationSessionsUsers X

Delete

<input type="checkbox"/> Email	Group	Registered Devices	
<input type="checkbox"/> [REDACTED]		0	<div><div></div><div></div></div>
<input type="checkbox"/> [REDACTED]		0	<div><div></div><div></div></div>
<input type="checkbox"/> [REDACTED]		0	<div><div></div><div></div></div>

Showing 1 - 3 Total: 3 10 < Previous1Next >



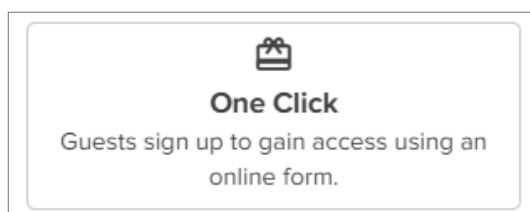
Note

The **Users X** tab appears only for the **Microsoft Azure X**, **Google Login X**, and **Onboarding 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 558 The One Click option



Note

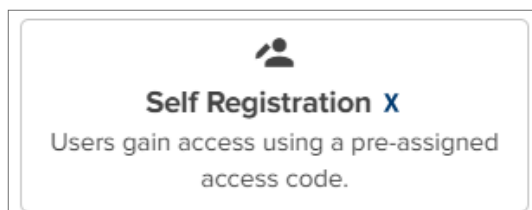
To create a One Click portal, complete the initial steps described in [Creating a portal](#) and continue with the next steps to configure the parameters of the **Basic** screen, **Limits** screen, **Design** screen, and **WLANs** screen.

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 559 *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. Click the **Self Registration** tab.

The **Self Registration** screen appears.

Figure 560 *The Self Registration screen*

A screenshot of the "Self Registration" configuration screen in the EasyPass interface. The left sidebar shows tabs: Basic, Self Registration (selected), Limits, Design, and WLANs. The main area contains the following settings: "Guests must provide their own email and their sponsor's email to request Internet access" (checked), "Approval required" (checkbox), "Approver Emails*" (text input field with placeholder "Type and press Enter"), "Mode" (radio buttons for "Manual" and "Auto", with "Manual" selected), "Receive password via text" (checkbox), "Enable" (checkbox), and "SMS Gateway Provider" (dropdown menu showing "Twilio"). At the bottom are "Save" and "Close" buttons.

2. Configure the parameters described in [Table 143](#).

Table 143 *The Self Registration screen parameters*

Parameter	Description
Approval required	Enable or disable this option. By default, this option is disabled. When this parameter is enabled, you must provide the approver email ID in the Approver Emails field. When this parameter is enabled, you have an option to select the required mode.
Approver Emails	This parameter is applicable when the Approval required checkbox is selected. Indicates the approver email ID that must be provided.

Table 143 *The Self Registration screen parameters*

Parameter	Description
	This parameter is mandatory.
Mode	<p>This parameter is applicable when the Approval required checkbox 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 checkbox. This parameter is disabled by default.</p> <p>When you select the Enable checkbox, the SMS Gateway Provider option is enabled.</p>
SMS Gateway Provider	<p>Select the required SMS gateway option to be used to send the OTP to the guest's mobile device.</p> <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 561](#) displays the parameters available for the **Twilio** option.

Figure 561 Twilio option

Receive password via text

Enable

SMS Gateway Provider

Twilio

Auth Token

Account SID

From

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 **Twilio** option, you must configure the parameters described in [Table 144](#).

Table 144 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 dropdown list and enter the mobile number.
OTP Template	OTP template. Enter the password in the OTP Template field. This parameter is mandatory.

[Figure 562](#) displays the parameters available for the **Generic SMS API** option.

Figure 562 *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*

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 **Generic SMS API** option, you must configure the parameters described in [Table 145](#).

Table 145 *Parameters of Generic SMS API*

Parameter	Description
SMS Gateway Provider Name	<p>SMS gateway provider name.</p> <p>Enter a name for the SMS gateway provider.</p> <p>Enter the user name.</p>
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	HTTP request header key value

Table 145 *Parameters of Generic SMS API*

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

Table 145 *Parameters of Generic SMS API*

Parameter	Description
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 dropdown list. For example, United States (+1)
OTP Template	OTP template. Enter the password in the OTP Template field. This parameter is mandatory.

[Figure 563](#) displays the parameters available for the **Fast SMS** option.

Figure 563 *Fast SMS option*


☐ Receive password via text

☒ Enable

SMS Gateway Provider
Fast SMS

Username

Sender ID
nsm.suthansanam@cambiumnetworks.com

API Key
[Redacted] Show

Account Type
Transaction

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

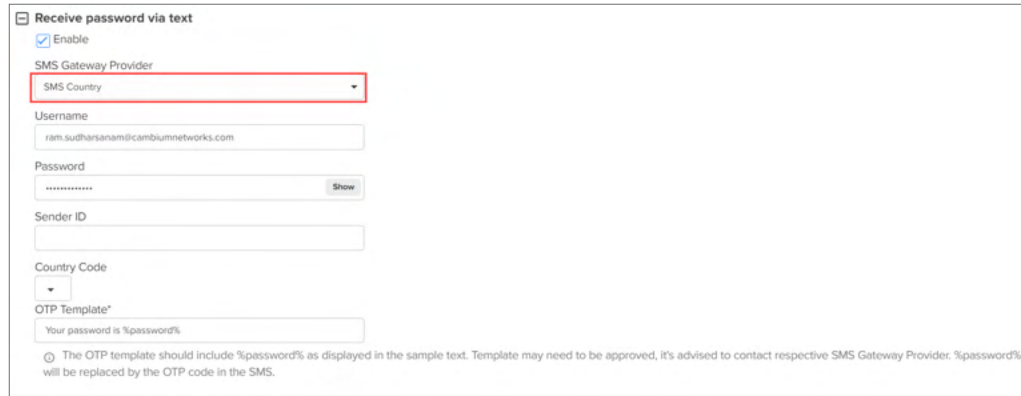
Table 146 *Parameters of Fast SMS*

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 dropdown list. The following options are supported: <ul style="list-style-type: none"> Transaction Promotional International OTP Other

Table 146 *Parameters of Fast SMS*

Parameter	Description
OTP Template	<p>OTP template.</p> <p>Enter the password in the OTP Template field.</p> <p>This parameter is mandatory.</p>

[Figure 564](#) displays the parameters available for the **SMS Country** option.

Figure 564 *SMS Country option*


☐ Receive password via text

☒ Enable

SMS Gateway Provider

SMS Country

Username

ram.sudhansami@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 147](#).

Table 147 *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 dropdown 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 565](#) displays the parameters available for the **SMS Gupshup** option.

Figure 565 SMS Gupshup option

☐ Receive password via text

☒ Enable

SMS Gateway Provider
SMS Gupshup

Username
ram.sudhansam@cambiumnetworks.com

Password
[Masked] Show

Sender ID
[Empty]

Country Code
[Dropdown]

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 Gupshup** option, you must configure the parameters described in [Table 148](#).

Table 148 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 dropdown list. For example, United States (+1)
OTP Template	OTP template. Enter the password in the OTP Template field. This parameter is mandatory.

[Figure 566](#) displays the parameters available for the **SMS API** option.

Figure 566 SMS API option

☐ Receive password via text

☒ Enable

SMS Gateway Provider
SMSAPI

Access Token
[Empty]

Sender Name
[Empty]

☐ Fast Delivery

Template Name
[Empty] ⓘ

Country Code
[Dropdown]

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 API** option, you must configure the parameters described in [Table 149](#).

Table 149 Parameters of SMS API

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

Table 149 *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 checkbox. By default, the checkbox is disabled.
Template Name	Template name. Enter the template name.
Country Code	Country code. Select the required country code from the dropdown list. For example, United States (+1)
OTP Template	OTP template. Enter the password in the OTP Template field. This parameter is mandatory.

[Figure 567](#) displays the parameters available for the **Victory Link SMS** option.

Figure 567 *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 150](#).

Table 150 *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.



Note

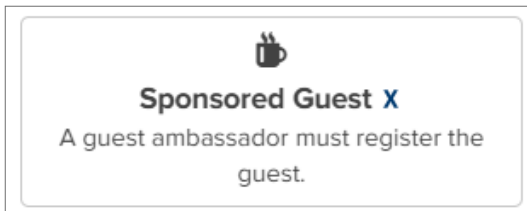
After configuring the parameters in the Self-Registration window, continue to [step 8](#) to configure the parameters in the **Limits**, **Design**, and **WLANS** screens.

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 568 *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. Click the **Sponsored Domains** tab.

The **Sponsored Domains** screen appears.

Figure 569 *The Sponsored Domains screen*

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

Table 151 *The Sponsored Domains screen parameters*

Parameter	Description
Sponsor Validation	Type of validation to be used for this portal. The following options are available: <ul style="list-style-type: none"> • Domain—Specify sponsor's domains • Email—Specify sponsor's email IDs
Sponsor Email Domains	This parameter is applicable only when you select the Domain option in the Sponsor Validation parameter.

Table 151 *The Sponsored Domains screen parameters*

Parameter	Description
	Specify multiple sponsor email domains. This parameter is mandatory.
Sponsor Emails	This parameter is applicable only when you select the Email option in the Sponsor Validation parameter. Specify multiple sponsor email IDs. This parameter is mandatory.



Note

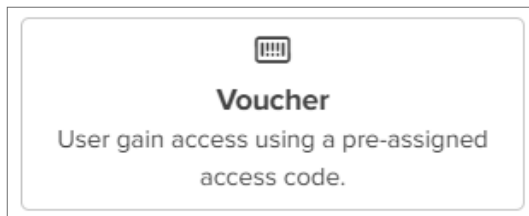
After configuring the parameters in the **Sponsored Domains** window, continue to [step 8](#) to configure parameters in the **Limits**, **Design**, and **WLANS** screens.

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 570 *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. Click the **Voucher** tab.
The **Voucher** screen appears.

Figure 571 *The Voucher screen*

EasyPass > test4

Basic

Voucher

Design

WLANs

Voucher Plan Name*

Quantity*

0

Voucher Message

Enjoy Internet Services. Here is your access code.

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.

Voucher Expiry*

1 Day

Client Rate Limit*

Unlimited

Client Quota Limit*

Unlimited

Device Limit

☐ Unlimited

1

☐ Bind Voucher to Device

Save Close

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



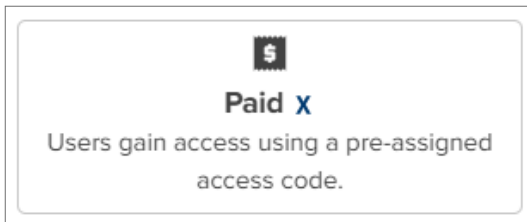
Note

After configuring the parameters in the **Voucher** screen, continue to [step 9](#) to configure the parameters in the **Design** and **WLANs** screens.

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 572 *The Paid X option*



Note

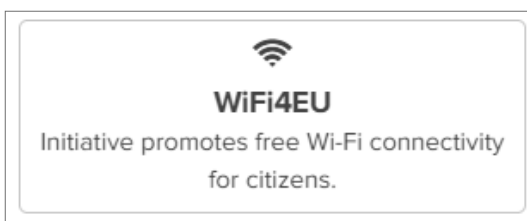
To create a Paid X portal, complete the initial steps described in [Creating a portal](#) and continue with the steps to configure the parameters of the **Basic** screen, **Plans** screen, **Design** screen, and **WLANs** screen.

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 573 *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. Click the **WiFi4EU** tab.

The **WiFi4EU** screen appears.

Figure 574 General parameters

2. Configure the parameters described in [Table 152](#).

Table 152 General parameters - WiFi4EU

Parameter	Description
Language	Select the preferred language from the dropdown 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.



Note

After configuring the parameters in the WiFi4EU window, continue to [step 8](#) to configure the parameters in the **Limits**, **Design**, and **WLANS** screens.

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 575 *The Microsoft Azure X option*



Note

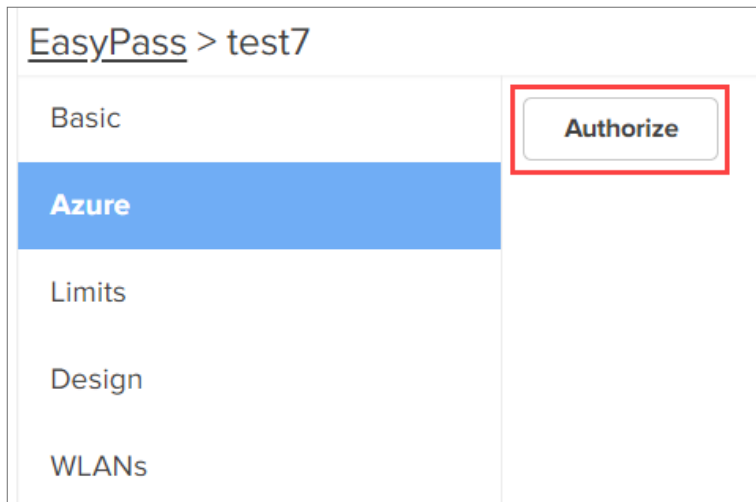
To create a Microsoft Azure X portal, complete the initial steps described in [Creating a portal](#) and continue with the next steps to configure the parameters of the **Basic** screen, **Azure** screen, **Limits** screen, **Design** screen, and **WLANs** screen.

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

1. Click the **Azure** tab.

The **Azure** screen appears.

Figure 576 *The Azure screen*



Note

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

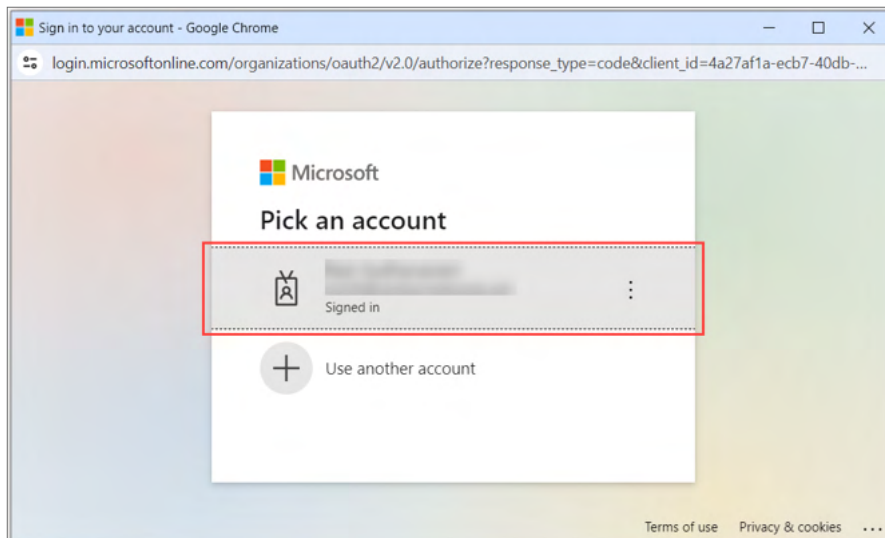
The **Authorize** step allows the EasyPass Azure application to:

- 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 **Authorize**.

The following screen appears, as shown [Figure 577](#).

Figure 577 Sign in to your account page



Note

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



Note

After configuring the parameters in the **Azure** window, continue to [step 8](#) to configure the parameters in the **Limits**, **Design**, and **WLANs** screens.

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.

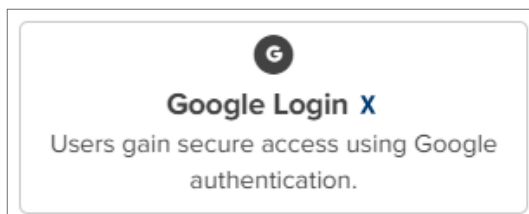


Note

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 578 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. Click the **Google** tab.

The **Google** screen appears.

Figure 579 *The Google screen*

2. Configure the parameters described in [Table 153](#).

Table 153 *The Google screen parameters*

Parameter	Description
Enable Directory Synchronization	<p>Select the checkbox to enable the directory synchronization.</p> <p>When you select the Enable Directory Synchronization checkbox, 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> <div> <p>Note</p> <p>For information on how to integrate Active Directory with Google Workspace, see the Google Workspace AD Integration document.</p> </div> <p>When you clear the Enable Directory Synchronization checkbox, you must configure the Allowed Domains parameter.</p>
Allowed Domains	<p>Enter the required domains.</p> <p>This is a mandatory parameter.</p>



Note

After configuring the parameters in the **Google** window, continue to [step 8](#) to configure the parameters in the **Limits**, **Design**, and **WLANs** screens.

Creating Onboarding X portal



Note

Onboarding **X** is supported only on Wi-Fi 6 and 6E APs running firmware version 6.6.2 or later.

Creating an Onboarding X portal enables clients to register on an open SSID with their email, Google Workspace, or Microsoft Azure (Office 365) credentials to receive an enhanced pre-shared key (ePSK), which can be used to connect to a secure network SSID.

For a non self-onboarding scenario, the administrator provides a passphrase to the users from the **Users X** page. The users can use the passphrase to connect to a network SSID. If ePSK is configured, the administrator can send an email to users containing the passphrase.

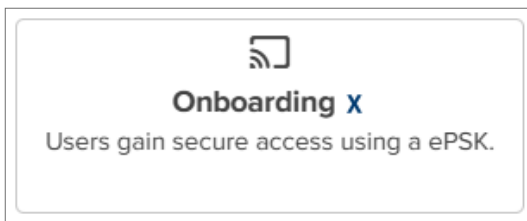


Note

After signing in with Google Workspace or Azure accounts, the ePSK is displayed as part of successful registration and is also emailed to the user for future use.

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

Figure 580 *The Onboarding X option*



Note

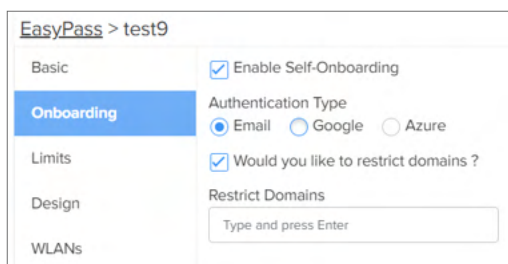
To create an Onboarding X portal, complete the initial steps described in [Creating a portal](#) and continue with the next steps to configure the parameters of the **Basic**, **Onboarding**, **Limits**, **Design**, and **WLANs** screens.

Follow these additional steps to create an Onboarding X portal:

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


The **Onboarding** screen appears.

Figure 581 *The Onboarding screen*



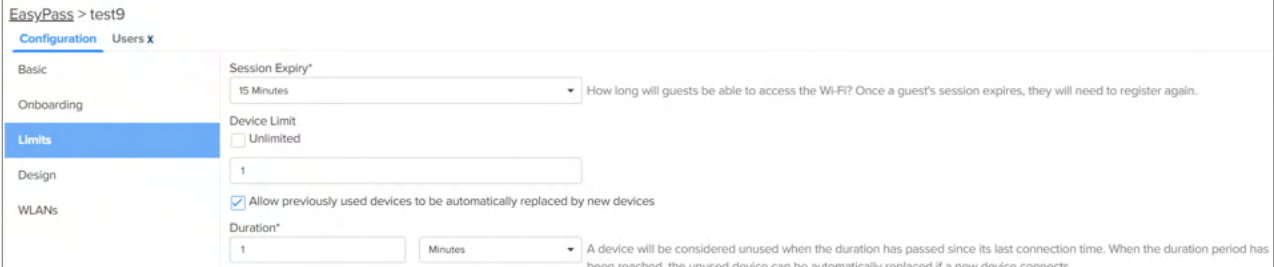
2. Configure the parameters described in [Table 154](#).

Table 154 *The Onboarding screen parameters*

Parameter	Description
Enable Self-Onboarding	<p>Select the Enable Self-Onboarding checkbox to enable self-onboarding.</p> <p>This parameter is disabled by default.</p> <p>When this parameter is enabled, you must select the required authentication type.</p> <p>When this parameter is disabled, users are notified about device limits only if the device limit is enabled and exceeded.</p> <div><div>Note<ul style="list-style-type: none">When this parameter is enabled, the WLANs screen displays the Network SSID and Registration SSID sections (as shown in Figure 583).Users can still use ePSK without self-onboarding.</div></div>
Authentication Type	<p>Select the required authentication type.</p> <p>The following options are supported:</p> <ul style="list-style-type: none">EmailGoogleAzure
Would you like to restrict domains	<p>Select the checkbox to restrict the email domains for the user.</p> <p>When you select the Would you like to restrict domains checkbox, enter the email domains that you want to restrict.</p>
Restrict Domains	<p>Enter the allowed email domains.</p>

3. Click the **Limits** tab.

The **Limits** screen appears.

Figure 582 *The Limits screen*

EasyPass > test9

Configuration Users X

Basic

Onboarding

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.

Device Limit

☐ Unlimited

1

☒ Allow previously used devices to be automatically replaced by new devices

Duration*

1 Minutes

A device will be considered unused when the duration has passed since its last connection time. When the duration period has been reached, the unused device can be automatically replaced if a new device connects.

4. Configure the parameters described in [Table 155](#).

Table 155 *The Limits screen parameters of Onboarding portal type*




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 dropdown list.</p> <div>  <div> <p>Note</p> <p>When you select the Custom option, you can configure the minimum duration value to 1 for Days, Hours, and Minutes.</p> </div> </div>
Device Limit	<p>Specifies the number of devices that the guest can connect to the wireless network.</p> <p>Minimum value: 1</p> <p>Maximum value: 200</p>
Unlimited	Device limit is unlimited.
Allow previously used devices to be automatically replaced by new devices	<p>Select the checkbox to enable the parameter.</p> <div>  <div> <p>Note</p> <ul style="list-style-type: none"> • When this parameter is enabled, it automatically replaces previously used devices with new devices according to the configured device limit. • When this parameter is disabled, previously used devices will remain in the system and will not be automatically replaced by new devices, even if the duration since their last connection has passed. </div> </div>
Duration	<p>This parameter is applicable only when Allow previously used devices to be automatically replaced by new devices checkbox is selected.</p> <div>  <div> <p>Note</p> <p>A device is considered unused when the duration has</p> </div> </div>

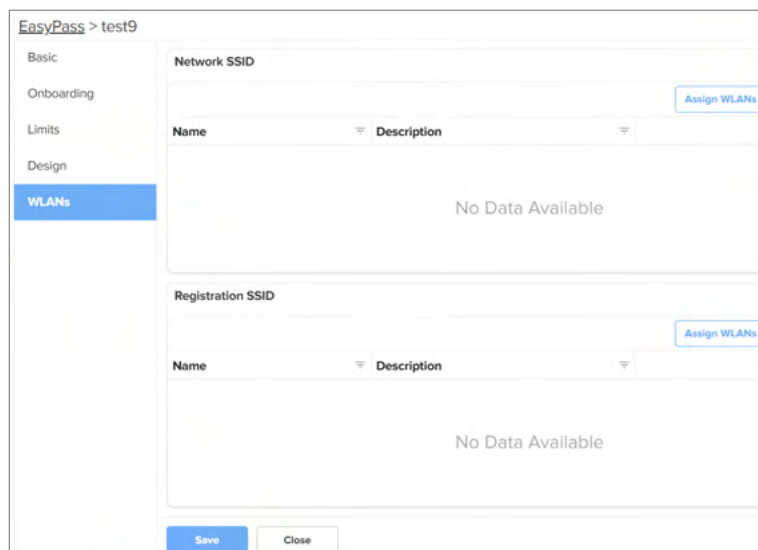
Table 155 *The Limits screen parameters of Onboarding portal type*

Parameter	Description
	<p>passed since its last connection time. When the duration period is reached, the unused device is automatically replaced if a new device connects.</p> <p>Minimum value: 1</p> <p>You can select the required option from the dropdown list. The following options are supported:</p> <ul style="list-style-type: none">• Minutes• Hours• Days

5. Click the **WLANs** tab.

The **WLANs** screen appears.

Figure 583 *The WLANs screen*



Note

The **WLANs** screen displays the **Network SSID** and **Registration SSID** sections (as shown in [Figure 583](#)).

- Network SSID is a secure SSID that users connect to after successfully registering and authenticating using the Registration SSID. It requires a ePSK for authentication to ensure users have secured access to the network after registration.
- Registration SSID is an open SSID that is used for onboarding users. It does not require a password for authentication. It allows users to authenticate using Email, Google, or Azure to register their device. After registration, users are emailed a unique password and SSID information to connect to the network.

Adding a new user

You can add a new user from the **Users X** page of the **Onboarding X** portal type.

Self-onboarding supports a dual SSID configuration, which includes an open SSID for self-onboarding and a secure network SSID for users who connect with a password. The registration SSID supports various authentication

methods such as email, Google Workspace, and Azure. Alternatively, users can skip self-onboarding and connect directly to the secure network SSID. In this case, the users are manually added to the **Users X** table and managed by the administrator.



Note

- The policy settings are managed using the user group. The user group is associated with an access control configuration, specifically through the RADIUS Filter-ID. The user group is managed through **Configuration > Wi-Fi Profiles > AP Groups > Add New > Access Control > User Group Policy > Add New > RADIUS Filter-ID**. The **RADIUS Filter-ID** is used to apply specific policies to users based on the group membership when they connect to the network.
- The maximum supported characters for **RADIUS Filter-ID** in user group policy is 32.

Complete the following steps to add a new user:

1. On the **Users** page of Onboarding X portal type, click **Add New**.

The **Add New User** window appears.

Figure 584 *The Add New User window*

2. On the **Add New User** window, complete the following steps:
 - a. In the **Name** field, enter the name of a user. This field is optional.
 - b. In the **User ID** field, enter the user ID. This field is mandatory.



Note

Only alphanumeric, underscore (_), dashes (-), period (.), plus (+), and @ characters are supported.

- c. In the **Email** field, enter an email ID of the user. This field is optional.
 - d. In the **Group** field, enter the group name.
3. In the **Advanced** section, complete the following steps:

a. From the **ePSK** dropdown list, select the required option. The following options are supported:

- i. **Auto Generate**
- ii. **Manual**

By default, the **Auto Generate** option is selected.

b. In the **Device Limit** field, enter a value.

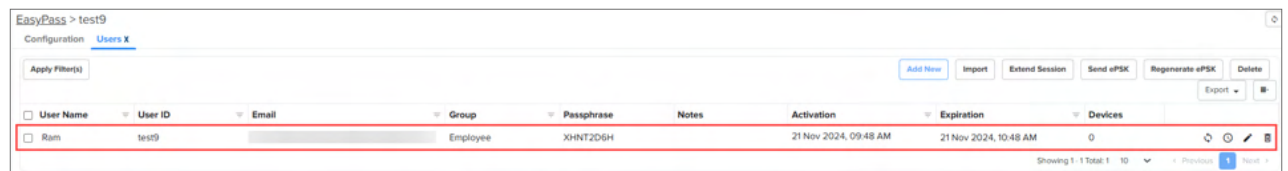
c. In the **Notes** field, enter the description for creating a new user. This field is optional.

d. Select the **Customize the activation and expiration times for this user** checkbox to customize the activation and expiration times for the user.

4. Click **Add**.

A new user is added (as shown in [Figure 585](#)).

Figure 585 *The new user details*



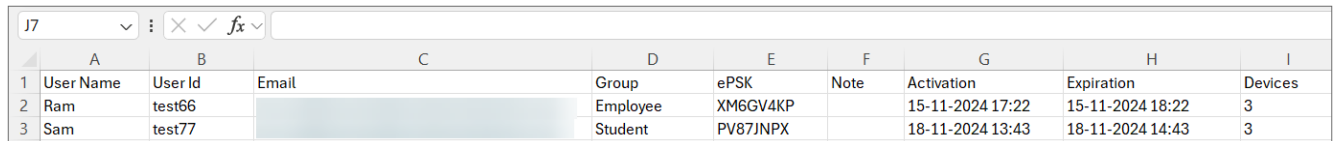
The screenshot shows the 'EasyPass > test9' configuration page. The 'Users' tab is active. A table lists user details. The first row is highlighted with a red border.

User Name	User ID	Email	Group	Passphrase	Notes	Activation	Expiration	Devices
Ram	test9		Employee	XHNT2DGH		21 Nov 2024, 09:48 AM	21 Nov 2024, 10:48 AM	0

Importing user data using a CSV file

You can import a list of users with their associated data such as User Name, User ID, Email, Group, Passphrase, and other relevant information using a CSV file as shown in the following figure.

Figure 586 *List of users with their associated data*



The screenshot shows a CSV file with the following data:

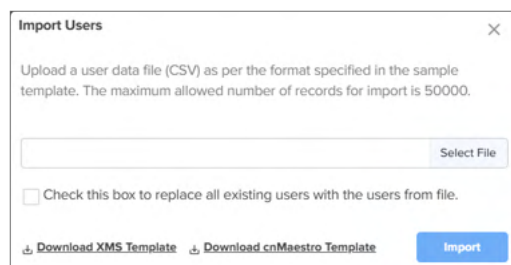
	A	B	C	D	E	F	G	H	I
1	User Name	User Id	Email	Group	ePSK	Note	Activation	Expiration	Devices
2	Ram	test66		Employee	XM6GV4KP		15-11-2024 17:22	15-11-2024 18:22	3
3	Sam	test77		Student	PV87JNPX		18-11-2024 13:43	18-11-2024 14:43	3

Complete the following steps to import user data using a CSV file:

1. Click the **Import** button (as shown in [Figure 585](#)).

The **Import Users** page appears.

Figure 587 *The Import Users page*



The screenshot shows the 'Import Users' dialog box. It contains a text area for instructions, a 'Select File' button, a checkbox for replacing existing users, and links to download templates. An 'Import' button is at the bottom right.

2. Select a CSV file from the **Select File** option.

3. Click **Import**.

The CSV file is imported.



Note

- When you select the **Check this box to replace all existing users with the users from file** checkbox, the system removes all existing users from the user list and replaces them with users included in the uploaded CSV file.
- You also have **Download XMS Template** and **Download cnMaestro Template** options.

- Click the **Export** button to export user data to a CSV file. The following options are supported:
 - **Export page as CSV**
 - **Export all as CSV**
- Click the **Regenerate ePSK** button to regenerate a new enhanced pre-shared key (ePSK) for selected users. A confirmation dialog box appears.

Figure 588 Confirmation dialog box to regenerate ePSKs for selected users



When you click **Yes** (as shown in [Figure 588](#)), a new ePSK is generated for selected users.



Note

A new passphrase is generated when **Auto Generate** or **Manual** ePSK option is selected.

You can also use the Regenerate ePSK (🔄) icon to generate a new ePSK for selected users.



Note

New or regenerated ePSKs are not automatically emailed to users. You must use the **Send ePSKs** button to send the ePSKs for selected users.

- Click the **Send ePSKs** button to send the ePSK for selected users. A confirmation dialog box appears.

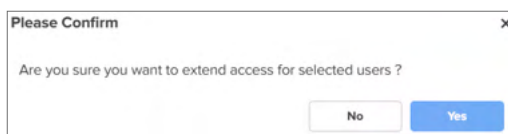
Figure 589 Confirmation dialog box to send ePSKs for selected users



When you click **Yes** (as shown in [Figure 589](#)), ePSKs are sent for selected users.

- Click the **Extend session** button to extend a session for selected users. A confirmation dialog box appears.

Figure 590 Confirmation dialog box to extend session for selected users



When you click **Yes** (as shown in [Figure 590](#)), the session is extended for selected users.

You can also use the Extend session (🕒) icon to extend the session for a selected user.



Note

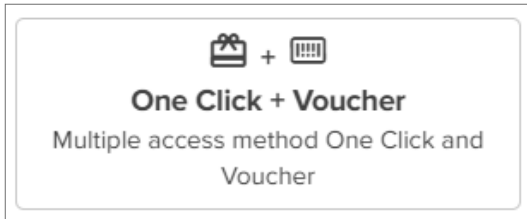
The session is extended based on the **Session Expiry** duration set in the **Limits** screen.

- Use the edit (✎) icon to edit the user details. Use the delete (🗑) icon to delete a user.

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 591 *The One Click + Voucher option*



Note

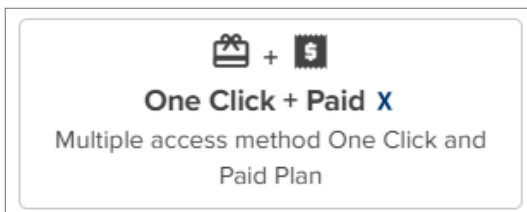
To create a One Click + Voucher portal, complete the initial steps described in [Creating a portal](#) and continue with the next steps to configure the parameters of the **Basic** screen, **Voucher** screen, **One Click** screen, **Design** screen, and **WLANs** screen.

For information on parameters in the **Voucher** and **One Click** screens, see [The Voucher screen parameters](#) and [The One Click screen parameters](#).

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 592 *The One Click + Paid X option*



Note

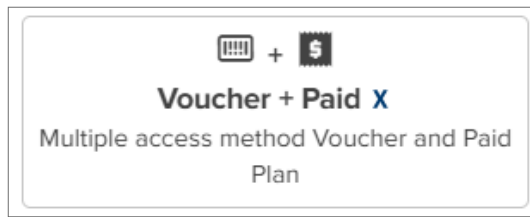
To create a One Click + Paid X portal, complete the initial steps described in [Creating a portal](#) and continue with the next steps to configure the parameters of the **Basic** screen, **Plans** screen, **One Click** screen, **Design** screen, and **WLANs** screen.

For information on parameters in the **Plans** and **One Click** screens, see [The Plans screen parameters](#) and [The One Click screen parameters](#).

Creating Voucher + Paid X portal

Creating a Voucher + Paid X portal combines the benefits of voucher-based promotions and paid access to services.

Figure 593 *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.

For information on parameters in the **Voucher** and **Plans** screens, see [The Voucher screen parameters](#) and [The Plans screen parameters](#).

MarketApps^X

This section includes the following topics:

- [MarketApps X](#)
- [Adding a new MarketApps App](#)
- [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](#)
 - [Units managed in the Managed Wi-Fi app](#)
 - [Units managed in Self-Service Personal Wi-Fi App](#)
- [Installer App](#)



Note

- MarketApps is available only in cnMaestro Cloud (version 5.1.0 and above) and is not supported on cnMaestro On-Premises.
- Only APs supporting Wi-Fi 6 (firmware version 6.6.1 and above) and Wi-Fi 7 (firmware version 7.1) are compatible with MarketApps.

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 three applications for the Multi-Dwelling Unit (MDU) market:

- **Managed Wi-Fi**
- **Self-Service Personal Wi-Fi**
- **Installer App**

These applications simplify the management and deployment of Wi-Fi services for property managers, residents, field installers, and service providers through an intuitive and streamlined workflow. The Installer App supports on-site device provisioning by guiding installers through configuration and deployment steps with minimal backend coordination. It helps ensure faster and more accurate installations across properties.

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.
- **Managed Service Providers (MSPs)**—MarketApps helps the MSPs 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.

Prerequisites

- APs must be onboarded to cnMaestro.
- WLANs and AP groups must be created and mapped to the AP.
- A valid license is required to enable MarketApps in cnMaestro.

Key features

- **Unit Assignment**—Property managers assign APs to residents and customize SSIDs and passwords.
- **QR Code Access**—Residents can scan a QR code to access the resident app and configure their Wi-Fi settings.
- **Resident Options**—Depending on the configuration, residents can either modify their SSID and password or receive a fixed SSID if changes are restricted by the MSPs.

To access MarketApps, navigate to **Network Services > MarketApps** in cnMaestro.

Figure 594 *MarketApps*

Name	Description	Managed Account	Type
Larry_suites	Residential cottages	Base Infrastructure	Self Service Personal Wi-Fi
Lakeshore_Condomoniums	Luxury apartment complex	Base Infrastructure	Managed Wi-Fi

Adding a new MarketApps App

To add a new MarketApps app, 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.

Installer
Users onboard Enterprise APs and Switches to cnMaestro

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** dropdown box.
6. Select the required app.
7. Click **Save and Continue**.

The respective app screens appear 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 595 *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.

Installer
Users onboard Enterprise APs and Switches to cnMaestro

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 596 *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**.

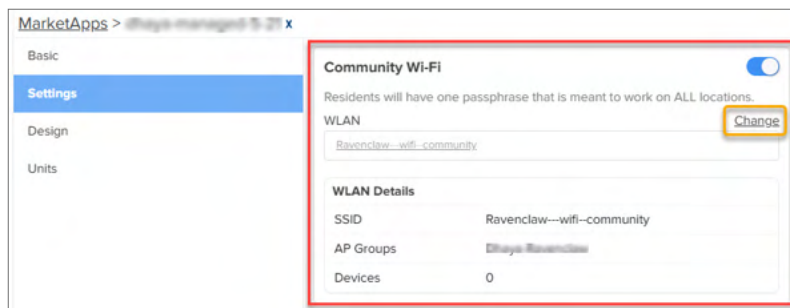
Settings tab

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 597 Community Wi-Fi settings

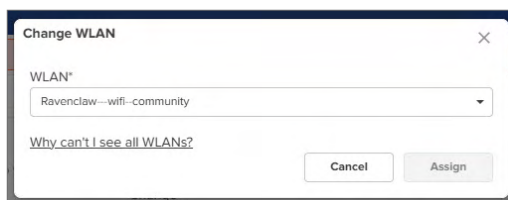


To configure **Community Wi-Fi** under the Settings tab in Managed Wi-Fi app, complete the following steps:

1. Select the **WLAN** for the community-wide Wi-Fi network.
2. Review the WLAN details, which include:
 - SSID** – Displays the configured network name.
 - APGroups** – Lists the associated AP groups.
 - Devices** – Shows the number of devices assigned to this WLAN.
3. If a different WLAN needs to be assigned, click **Change**. A confirmation window appears and click **Yes**.



4. A new **Change WLAN** window appears. Select the required WLAN from the dropdown list and click **Assign**.



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.

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. Residents can create and manage multiple personal SSIDs, with a maximum of 4 personal WLANs allowed per unit.

Figure 598 *Personal Wi-Fi settings*

To configure Personal Wi-Fi under the Settings tab in Managed Wi-Fi app, complete the following steps:

1. Enable the Personal WLAN option.
2. Select the WLAN for the personal Wi-Fi network.



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.

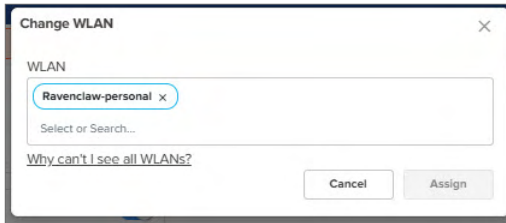
- WLAN should not be mapped to any existing MarketApps or EasyPass.

3. To assign a different WLAN, click **Change**.

Click **Yes** in the confirmation window.



4. A new **Change WLAN** window appears. Select the required WLAN from the dropdown list and click **Assign**.



5. **Allow Resident to Change Wi-Fi Settings**—MSPs can enable or disable the option for residents to configure their personalized settings.
6. **Allow Property Manager to Suspend and Terminate Internet Service**—MSPs can enable or disable the option for property managers to suspend or terminate Internet service.
7. 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.



Note

A maximum of 10 property manager email addresses can be added per MarketApps app.

8. Select the **Time Zone** from the dropdown list. This sets the local time zone of the property where the MarketApps app is running, ensuring the application operates according to the specific time zone of the city or location.
9. Define the **Password Pattern** by specifying a mix of capitalized/lowercase letters, nouns, verbs, adjectives, random letter words, and digits.
10. Define the **Password Pattern**.

Specify a password pattern using a combination of the following elements:

- Capitalized/lowercase nouns
- Capitalized/lowercase adjectives
- Capitalized/lowercase verbs
- Random letter words
- Digits (0–9)

Use the following pattern keys:

- N – Capitalized noun
- n – Lowercase noun
- A – Capitalized adjective

- a – Lowercase adjective
- V – Capitalized verb
- v – Lowercase verb
- D or d – Digit
- R or r – Random letter word

Arrange the keys in any order to define your desired password structure.

For example, the pattern **AnDvr** might generate a password like **Happytree7runxy**.

11. Select the **Language** for the manager and resident portal.



Note

Currently, only English and Spanish are supported.

12. Click **Save**.



Note

MSPs can select Community Wi-Fi, Personal Wi-Fi, or both options, depending on their requirements.

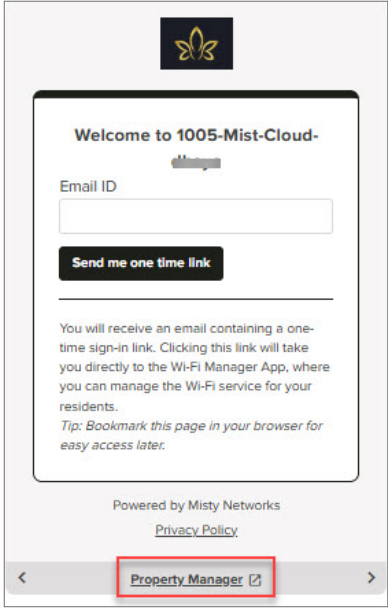
Design tab

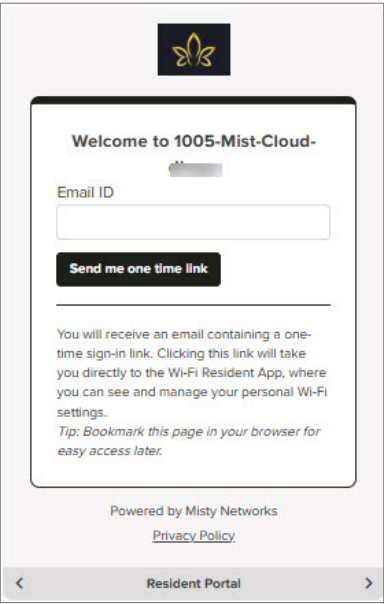
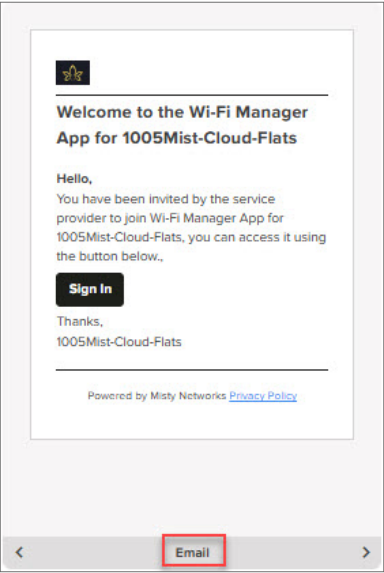
The Design tab in MarketApps allows you to customize the branding and appearance of the property manager and resident portals, ensuring a cohesive and professional user experience.

Figure 599 *Design tab parameters*

Table 156 *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.

Parameter	Description
Logo	Upload a logo file (PNG recommended) cropped to the edges and sized up to 200x200 pixels.
Color Theme	Customize the Installer App's color scheme with a chosen accent color.
Privacy URL	Provide the URL to your Privacy Policy.
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"> 1. Property Manager—Displays the Property Manager interface where users can enter their Email and request a one-time link for access.  <p>Click Property Manager or the icon to open the Manager Portal, allowing MSP admins to manage property settings. From the portal, admins can perform actions such as Assign, Suspend, Extend, and Terminate units.</p> <p>Note: Only Super Admin, Admin, and Operator users can utilize this functionality.</p> <ol style="list-style-type: none"> 2. Resident Portal—This shows the Resident Portal interface where users can input their email to receive a one-time link for accessing their personal Wi-Fi settings.

Parameter	Description
	 <p>3. Email—Provides a view of the email format that users receive, which contains a link to access the Wi-Fi Manager App.</p> 
Save	Click Save to apply the changes after configuring the Design tab.

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 600 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.

Installer
Users onboard Enterprise APs and Switches to cnMaestro

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 601 Personal Wi-Fi settings

MarketApps > [redacted] x

Basic
Settings
Design
Units

Personal Wi-Fi
Residents can create personalized SSID for their unit.

[Text Input Field]

Maximum 4 WLANs allowed. [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*
[Dropdown Menu]

[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** dropdown 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 owners can enable or disable the option for residents to configure their 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** dropdown 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 section contains the following topics:

- [Units managed in the Managed Wi-Fi app](#)
 - [Assign Unit](#)
 - [Send Portal Link](#)
 - [Extend](#)
 - [Move](#)
 - [Suspend](#)
 - [Terminate](#)
 - [Bulk Assign Residents](#)
 - [Settings](#)
 - [Theme settings](#)
 - [AP Health](#)
 - [MarketApps app selector](#)
 - [Refresh button](#)
 - [Refresh button](#)
- [Units managed in Self-Service Personal Wi-Fi App](#)

Units managed in the Managed Wi-Fi app

Managed Wi-Fi app 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:

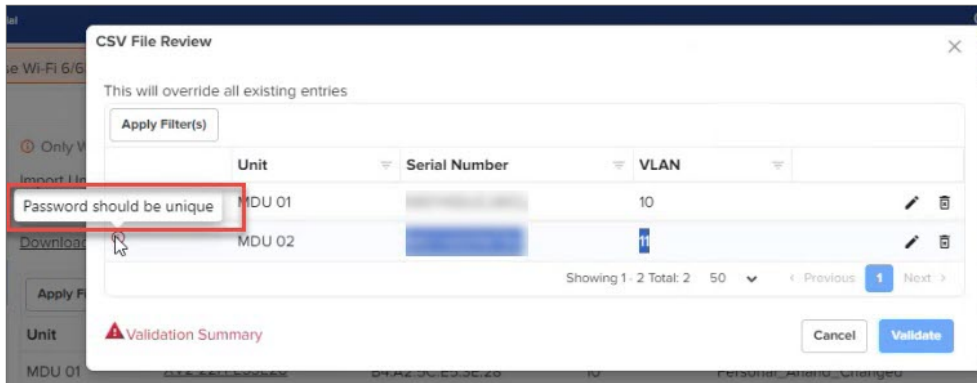
1. Navigate to the **Unit** tab and click on the **Download Sample Template** option to get the sample file.

2. An example of the sample template and parameters is shown below:

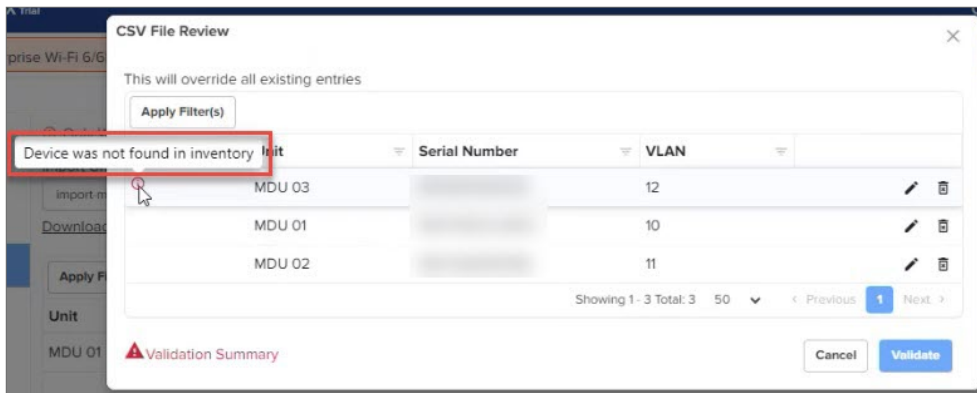
Serial Number	Unit	MAC Address	VLAN	Personal SSID	Password
Serial number of the device	Unit name	MAC Address of the device	VLAN(1 - 4094)	SSID for the personal Wi-Fi	Password for Wi-Fi
B1000D000000	MDU 01	B1:00:0D:00:00:00	10	SSID 01	Pa\$\$Word123
B1000D000001	MDU 02	B1:00:0D:00:00:01	13	SSID 02	Pa\$\$Word123
B1000D000003	MDU 03	B1:00:0D:00:00:03	11	SSID 03	Pa\$\$Word123

Parameter	Description
Serial Number	Enter the serial number of the device.
Unit	Enter the name or number of the unit (for example, MDU 01, MDU 02, and MDU 03 are apartments numbers).
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.

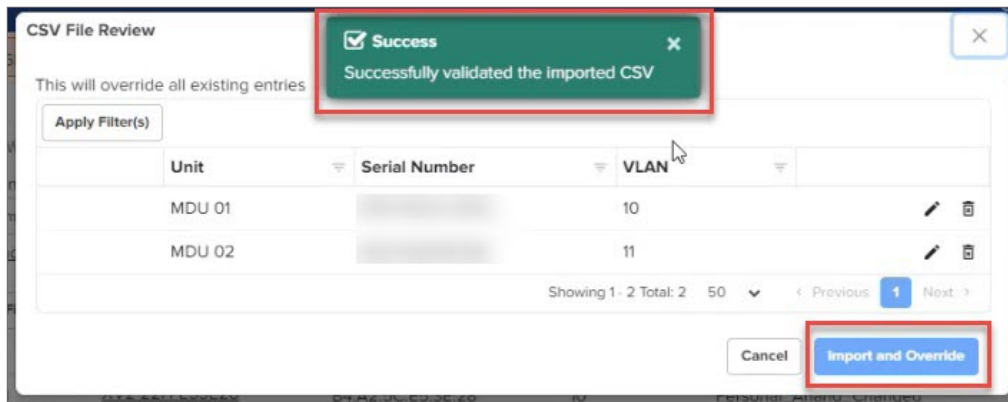
3. After entering the details, save the Excel file with a new name to ensure you have a copy of the filled template and import it to cnMaestro. Note this step is crucial to avoid overwriting the original template.
4. During the import, you might encounter validation error messages. Here are some common 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 all mapped WLANs to the app**—Ensure the device has an AP group linked with all the mapped personal and community WLANs.
 - 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.

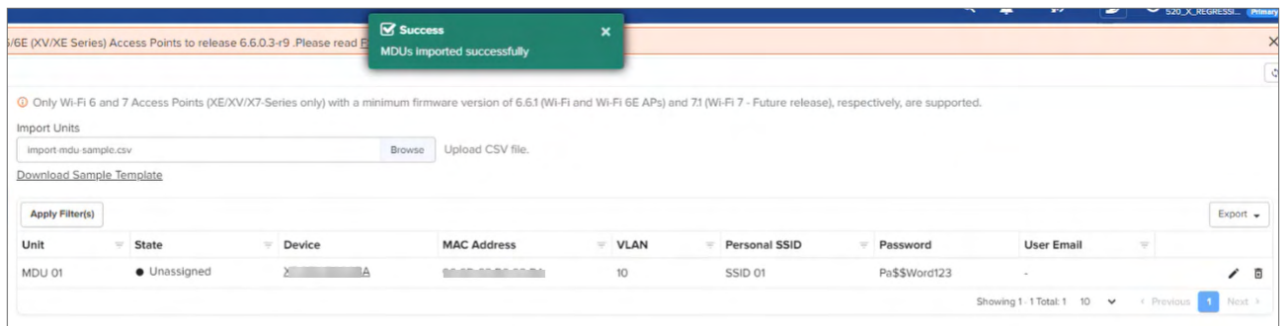


Note

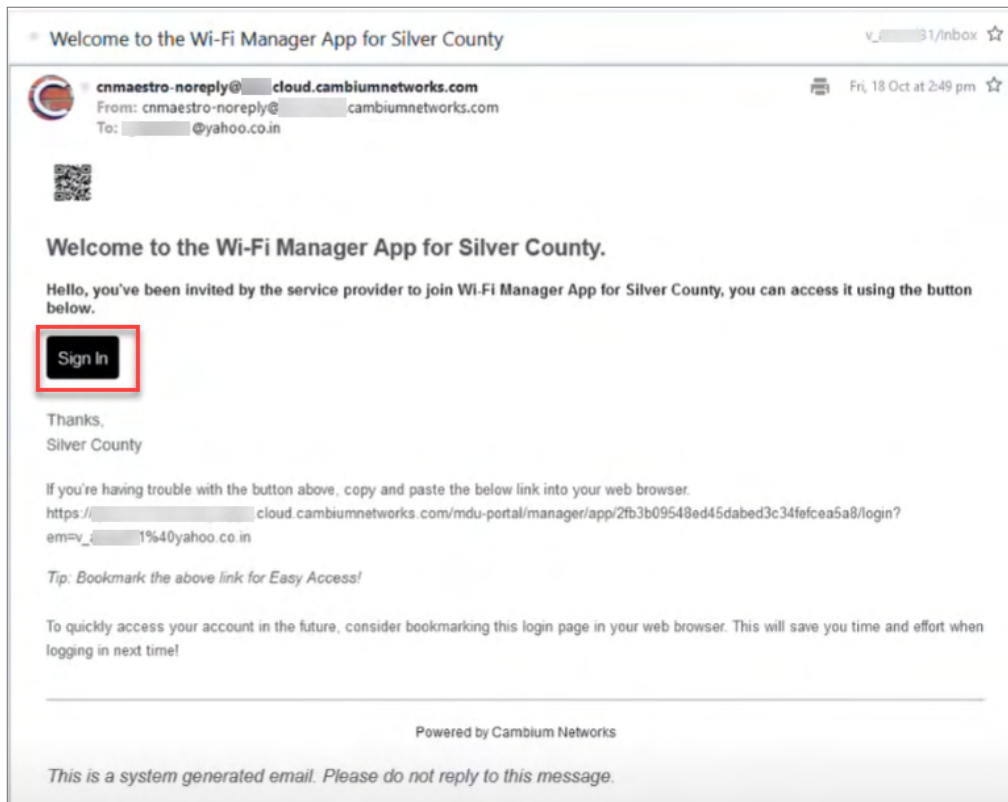
After importing, note the following points:

- 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 598) is enabled, residents can change their SSID and password settings, and these changes do not get overwritten later.

7. Once the devices are successfully added, a pop-up message displays: **MDU imported successfully.**



8. The property manager receives an email titled **Welcome to the Wi-Fi Manager APP for Silver County** and can **Sign In**.



9. The property manager enters the same email ID provided in the Managed Wi-Fi app settings.

Welcome to ManagedWi-Fi

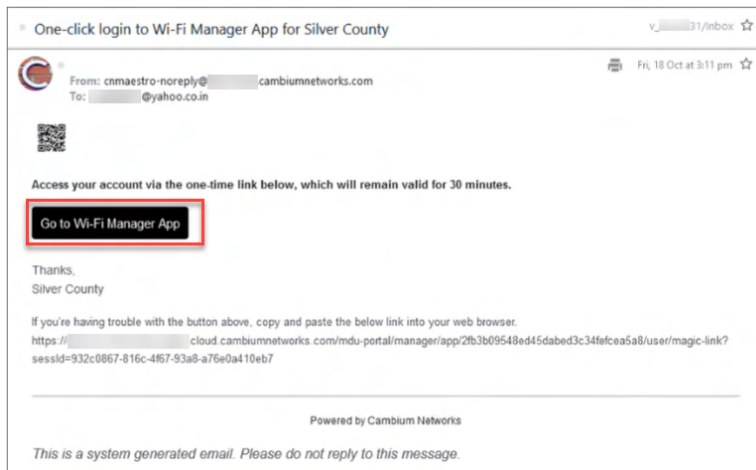
Email ID

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 Manager App, where you can manage the Wi-Fi service for your residents.

Tip: Bookmark this page in your browser for easy access later.

10. Click **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.

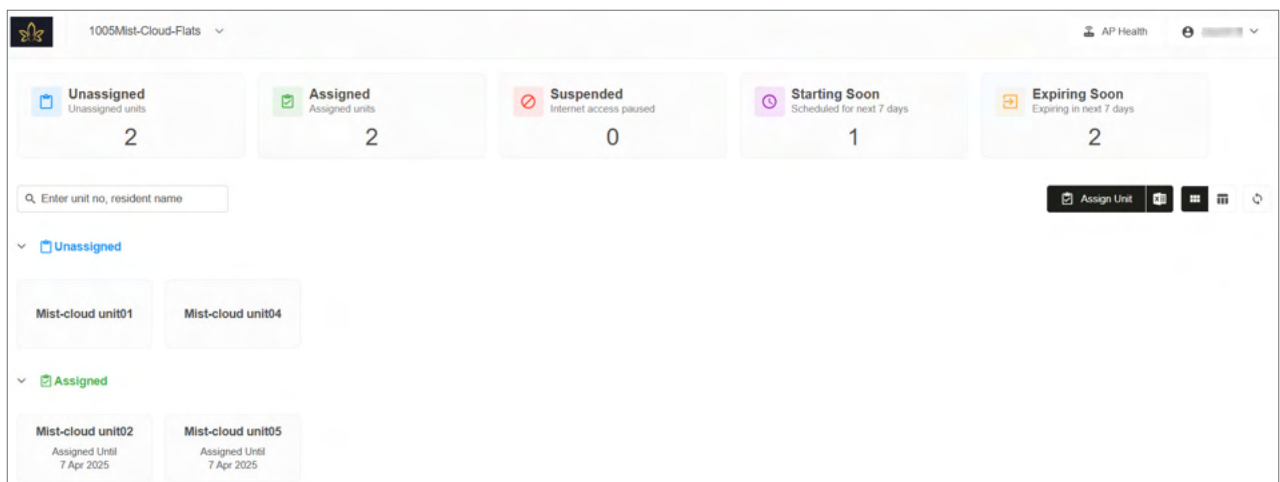


Table 157 *Wi-Fi Manager App Interface*

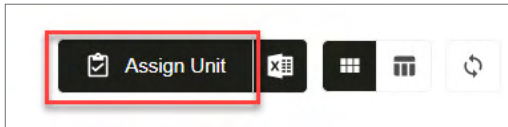
Options	Description
Unassigned	Displays the total number of units that are yet to be assigned. Click this widget to filter the view and show only unassigned units.
Assigned	Shows units that have been successfully assigned. Click this widget to filter the view and show only assigned units.
Suspended	Lists units with temporarily paused internet access. Click this widget to filter the view and show only suspended units.
Starting Soon	Indicates assignments that are scheduled to begin soon (within 7 days). Click this widget to filter the view and show only those upcoming assignments.
Expiring Soon	Highlights units whose assignments are nearing expiration (within 7 days). Click this widget to filter the view and show only expiring units.
Search	Allows searching for units or residents by entering the unit number or resident name.
Assign Unit	Assign a unit to a resident. Includes the option Bulk Assign Residents to assign multiple residents simultaneously.

Assign Unit

The **Assign Unit** option allows property managers to allocate specific units to residents. This feature simplifies resident management and facilitates communication between managers and residents.

To assign a unit, follow the below steps:

- a. Click on **Assign Unit** in the Property Manager App.



- b. A new window titled **Assign Unit** appears.

A screenshot of a web application window titled 'Assign Unit'. The window contains several input fields: a dropdown menu for 'Unit*' with 'cloud unit' selected; text boxes for 'First Name*' and 'Last Name'; a text box for 'Email ID' with 'works.com' entered; a text box for 'Description' with 'Home' entered; date pickers for 'Start Date' (01 Apr 2025) and 'End Date' (08 May 2025); and a 'Duration' field showing '37 Day(s)'. At the bottom right, there are two buttons: 'Cancel' and 'Assign Unit', with the latter highlighted by a red box.

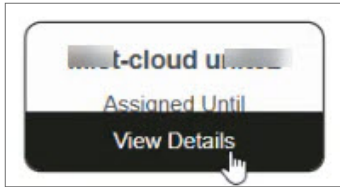
- c. Select the unit from the **Unit** dropdown menu.
- d. Enter the resident's **First Name**.
- e. Enter the resident's **Last Name**.
- f. Enter the resident's **Email ID** (optional).
- g. Provide a **Description**.
- h. Set the **Start Date** for the assignment.
- i. Set the **End Date** for the assignment.



Note

Minimum duration is one day.

- j. Review the **Duration** displayed in days.
- k. Click **Assign Unit** to finalize the assignment.
- l. A message confirms **Assign Unit action completed successfully**.
- m. After assigning a unit, hover the cursor over the assigned unit. A **View Details** option appears.



- n. Click **View Details** to open a window on the right-hand side that displays the resident's information and recent change history.

Unit Details "Unit-cloud un..."

Resident Information
Edit

Status

● Assigned

Name

Email

Start Date

1 Apr 2025, 11:02AM

End Date

7 Apr 2025, 11:59PM

Description

Recent Change History

Last 7 days

Time	Change	User
01 Apr 2025, 11:02 AM	Assigned to	
25 Mar 2025, 04:16 PM	Moved resident f	
25 Mar 2025, 04:13 PM	Updated WLAN c	
25 Mar 2025, 04:12 PM	Login successful	
25 Mar 2025, 02:03 PM	Assigned to t	

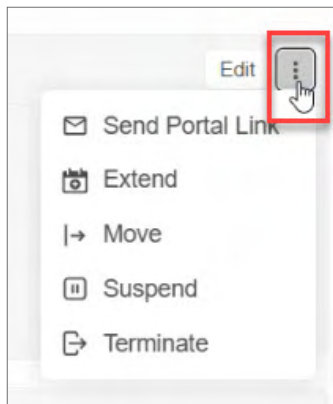
Showing 1 - 5 Total: 5
1
10

The view includes key details for the selected unit—such as unit name, status, email, start date, end date, and description.

It also shows the audit logs of all actions performed in the last 7 days, including email updates, resident logins, suspensions, and terminations, along with the time and user who performed each action.

- o. Click the **Edit** button on the top right corner of the window. A new window titled **Update** appears.

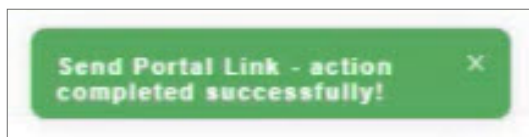
- p. The property manager can modify the resident's information such as name, email, start and end dates, and description associated with the unit, and then click **Update**.
- q. Next to the Edit button, click the three-dot icon to view more options. This menu allows you to perform actions such as sending the portal link, extending the assignment period, moving the resident to another unit, suspending access, or terminating the assignment.



Send Portal Link

This option allows property managers to send a one-time login link to the resident via email. The resident can use the link to access the Wi-Fi configuration portal and complete their setup or make necessary changes.

After the action is completed, a confirmation message appears stating: **Send Portal Link – action completed successfully** as shown in the figure below.



Extend

The Extend option allows property managers to update the end date of a unit's assignment.

When selected, a window appears with the current end date. Update it to the desired date using the calendar icon, then select **Extend** to apply the changes.

Move

The Move option allows property managers to reassign a resident to another unit. When selected, a window titled **Move Resident to other unit** appears.

To move a unit, complete the following steps:

1. Select the new unit from the **Unit** field.
2. Enter a Description (optional).
3. Select **Move** to complete the reassignment.

Suspend

The Suspend option temporarily disables internet access for a unit. When selected, a confirmation window appears.

Select **Suspend** to pause the resident's internet service. The system sends an email update to the resident when you suspend the service.

Terminate

The Terminate option permanently ends the resident's assignment and releases the unit for reassignment. When selected, a confirmation window appears.

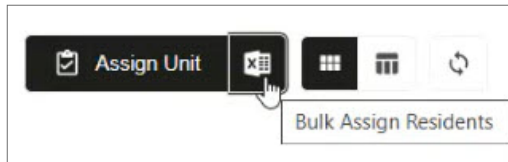
Select **Terminate** to remove the resident's access and complete the process. The system sends an email update to the resident when you terminate the service.

Bulk Assign Residents

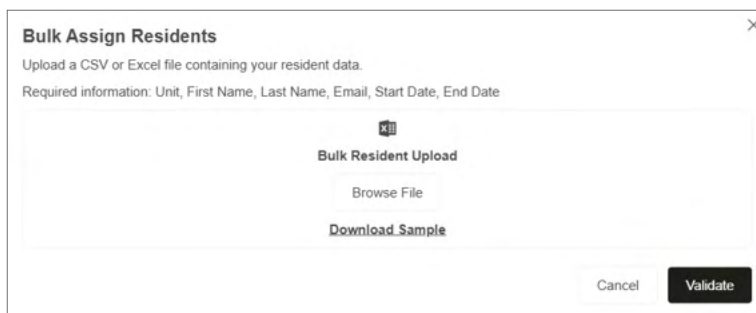
The Bulk Assign Residents option enables property managers to efficiently assign multiple units to residents at once by uploading a CSV or Excel file containing resident data.

To bulk assign units, follow the below steps:

1. Click on **Bulk Assign Residents** in the Assign Unit window.



2. A new window titled **Bulk Assign Residents** appears.



3. Click **Browse File** to select and upload your CSV or Excel file.
4. Click **Download Sample** to download a sample file format for reference.
5. When uploading, ensure that the Unit is entered as specified below:

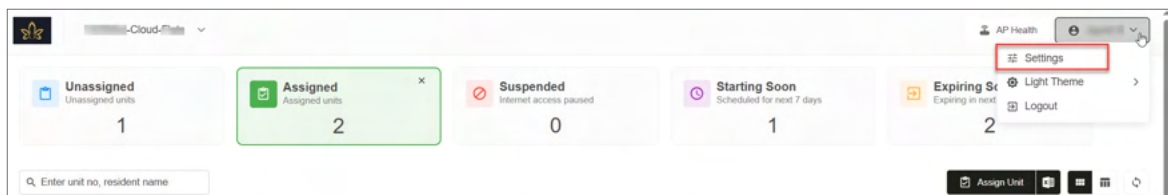
Unit	First Name	Last Name	Email	Start Date	End Date
Unit name	Resident first name	Resident last name	Resident email id	Internet access start date in format (MMM DD YYYY)	Internet access end date in format (MMM DD YYYY)
MDU 01	John Doe	A	johndl@yopmail.com	Dec 20 2024	Jan 21 2025
MDU 02	John Doe	B	johndl@yopmail.com	Dec 21 2024	Jan 30 2025

6. Click on **Validate** to finalize the bulk assignment.

Settings

The Settings option allows you to configure system preferences within the Property Manager App. To access the Settings, complete the following steps:

1. Click on **Settings** in the top right-hand corner of the app, near the email ID.



2. A new window titled **Settings** appears.

- **System Time Zone:**

Displays the property's time zone along with the date and time. This field is read-only and cannot be modified from the UI.

- **Checkout Time:**

Allows you to define the default checkout time for residents. Use the time picker to select the hour, minutes, and AM/PM. The time is displayed in a 12-hour format as shown in the figure below.

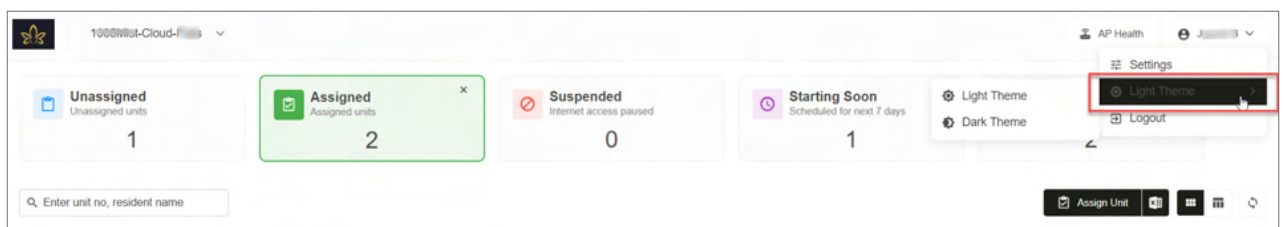
3. Click **Save** to confirm your changes.

Theme settings

The **Light Theme** option in the Property Manager App allows you to switch between Light and Dark modes to suit your viewing preference.

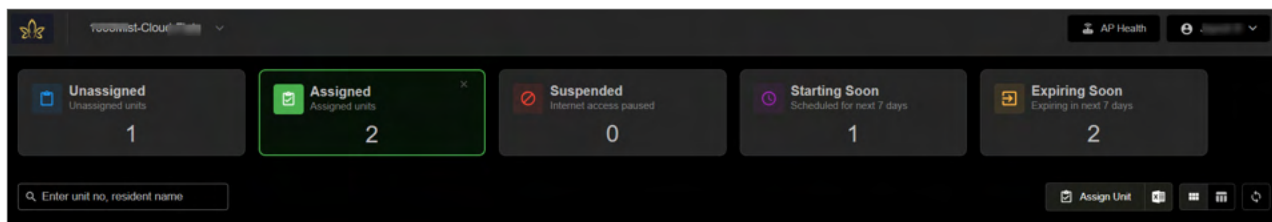
To change the theme, follow the steps below:

1. Click the **Light Theme** icon in the top-right corner of the app, below the **Settings** option.



2. A side panel appears with two theme options:

- **Light Theme:** This is the default setting. Select it to keep the app in a bright, standard mode.
- **Dark Theme:** Select this to switch to a dark interface, which is easier on the eyes in low-light environments.



3. The theme is applied instantly across the app.

AP Health

The AP Health feature in MarketApps provides real-time visibility into the operational status of APs associated with each property.

When property managers import APs using a CSV file, the system begins tracking their health automatically. The AP Health section displays the number of APs that are online, offline, and the total number of clients connected across all APs.

If any AP that was previously online in cnMaestro goes offline, the AP Health data reflects this change in real-time. These updates are also visible in the Property Manager Portal, ensuring that managers always have access to the latest device status.

To view the most recent data, click the [Refresh button](#). This updates the AP Health Stats, including AP status and client count.

Figure 602 AP Health interface

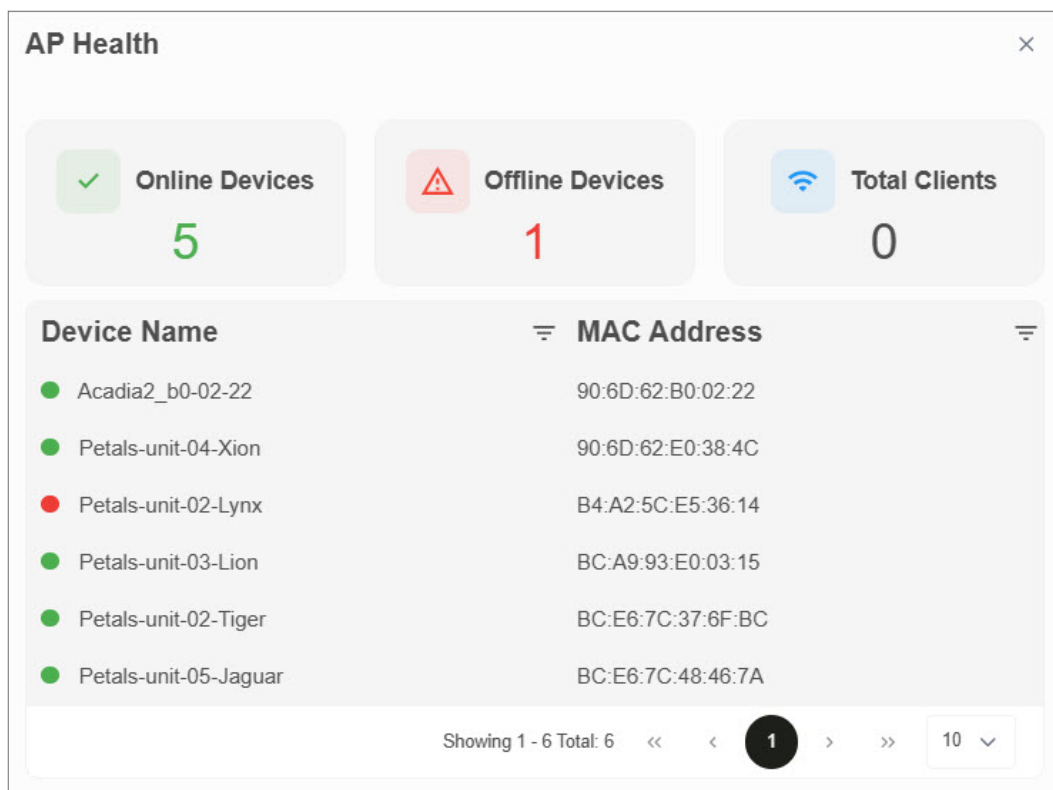


Table 158 AP Health parameters and descriptions

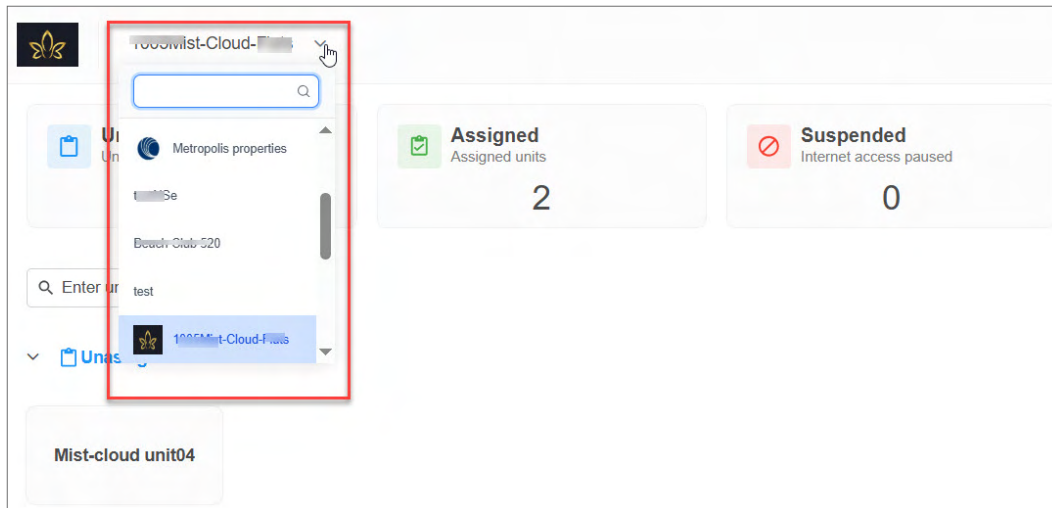
Element	Description
Online Devices	Shows the number of APs currently active and connected.

Element	Description
Offline Devices	Shows the number of APs that are currently offline or unreachable.
Total Clients	Displays the total number of client devices connected across all online APs.
Device Name	Lists the names of APs as configured during CSV import. A green indicator next to the name means the AP is online; a red indicator next to the name means the AP is offline. The filter option is available for quick searching, as shown in the figure below. <div data-bbox="440 373 873 499" data-label="Image"> </div>
MAC Address	Shows the unique hardware (MAC) address for each AP. The filter option is available for quick searching, as shown in the figure below. <div data-bbox="440 604 873 762" data-label="Image"> </div>

MarketApps app selector

The MarketApps app selector is a dropdown located at the top of the Property Manager page, next to the property name as shown in [Figure 603](#).

Figure 603 MarketApps app selector



This dropdown allows property managers to easily switch between multiple MarketApps apps that are associated with the same admin email or manager profile.

When a property manager account is linked to more than one MarketApps app, all the corresponding apps appear in this dropdown. Selecting an app from the list updates the view to show data specific to that MarketApps app—such as units, settings, and assignments—without needing to log out or switch sessions.

By default, the most recently accessed MarketApps app is shown when the user logs in. Switching between MarketApps apps instantly refreshes the interface to reflect the selected property's details, including resident data, AP status, and other configurations.

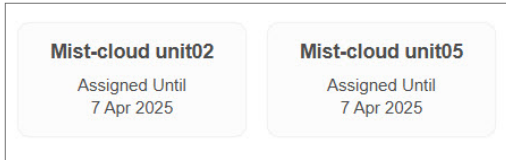
View options in the Property Manager App

In the Property Manager App, there are two 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 604](#).

Figure 604 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, as shown in the figure below.



2. **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, as shown in the figure below.

Unit	Status	Name	Email	Start Date	End Date
Mist-cloud unit02	Assigned	Arjun...	...	1 Apr 2025, 11:02AM	7 Apr 2025, 11:59PM
Mist-cloud unit04	Unassigned				
Mist-cloud unit05	Assigned	Riya...	...	2 Apr 2025, 12:00AM	7 Apr 2025, 11:59PM

At the end of each row, a three-dot menu provides quick access to actions such as Edit, Send Portal Link, Extend, Move, Suspend, and Terminate.

Action tab

When the Table view is active, an additional **Action** tab appears for performing bulk actions. You can select multiple units using the checkboxes located to the left of each Unit name as shown in [Figure 605](#). Once selected, the Action tab displays bulk operation options such as Send Portal Link, Resume, Suspend, and Terminate. This tab streamlines the process of managing multiple units at once, while individual changes can still be made using the three-dot menu in each row.

Figure 605 Action tab

Unit	Status	Name	Email	Start Date	End Date
<input checked="" type="checkbox"/> Mist-cloud unit02	Assigned	Arjun...	...	1 Apr 2025, 11:02AM	7 Apr 2025, 11:59PM
<input checked="" type="checkbox"/> Mist-cloud unit04	Unassigned				
<input checked="" type="checkbox"/> Mist-cloud unit05	Assigned	Riya...	...	2 Apr 2025, 12:00AM	7 Apr 2025, 11:59PM

Refresh button

If the portal is open in multiple browser tabs or windows, changes made in one session may not immediately reflect in the others. Click the Refresh button to update the view with the latest information.

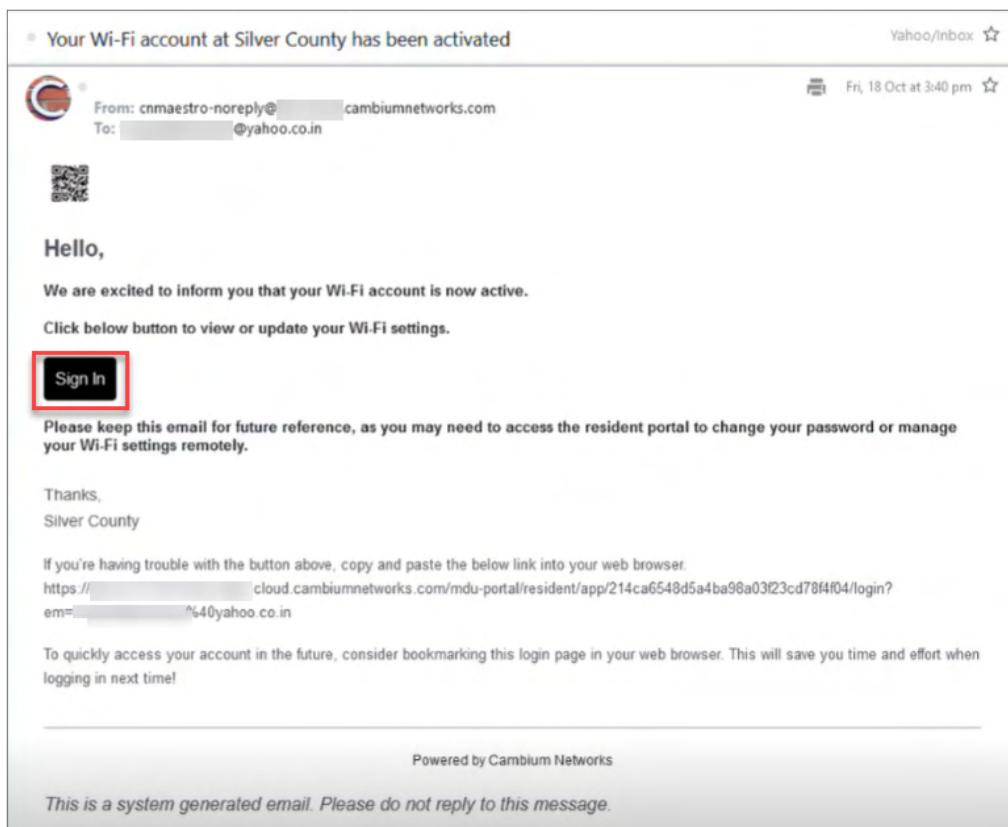
In the AP Health section, the Refresh button also updates the AP status data, ensuring that the displayed online/offline status and client count are current.

Figure 606 Refresh option



View options in the Resident App

1. Once the property manager assigns the unit, residents receive an email titled **Your Wi-Fi account Silver County has been activated** and can **sign in**.



2. Click **Send me one time link**.

Welcome to ManagedWi-Fi

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.

- The resident receives an email containing a one-time link for logging into the Resident App. Click **Go to Wi-Fi Resident App**.

One-click login to Wi-Fi Resident App for Silver County Yahoo/inbox ☆

 From: cnmaestro-noreply@cloud.cambiumnetworks.com
 To: v.arnavdutta@gmail.com@yahoo.co.in Fri, 18 Oct at 3:47 pm ☆



Access your account via the one-time link below, which will remain valid for 30 minutes.

Go to Wi-Fi Resident App

Please keep this email for future reference, as you may need to access the resident portal to change your password or manage your Wi-Fi settings remotely.

Thanks,
 Silver County

If you're having trouble with the button above, copy and paste the below link into your web browser.
<https://cloud.cambiumnetworks.com/mdu-portal/resident/app/214ca6548d5a4ba98a03f23cd78f4f04/user/magic-link?sessionId=12eda700-6b47-4641-9df8-ab885484d9f7>

Powered by Cambium Networks

This is a system generated email. Please do not reply to this message.

- You see a page titled **Welcome to Silver County**. Click on **Change**. Below the QR code, two options appear: **Community Wi-Fi** and **Personal Wi-Fi**. You can scan to connect to either network and use the arrow to switch between them.



5. A new window titled **Change Wi-Fi Settings** appears. Change your Personal Wi-Fi Network Name and Wi-Fi password in the respective fields.



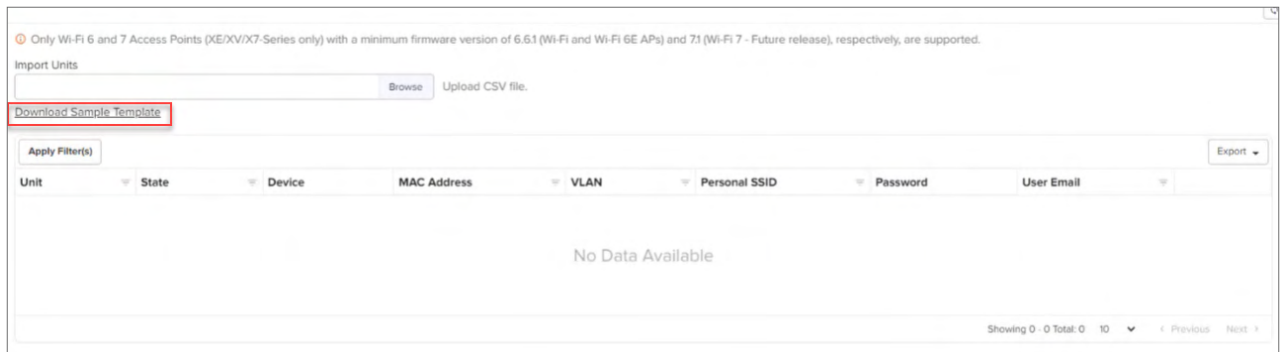
6. Click **Update** to save the changes.

Units managed in Self-Service Personal Wi-Fi App

The 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.

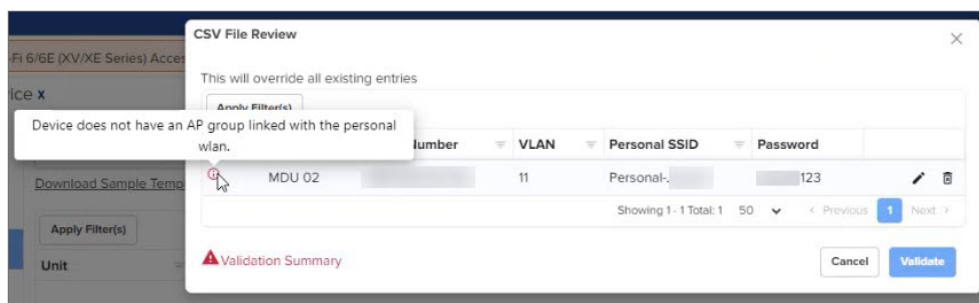


2. An example of the sample template and parameters is shown below:

Serial Number	Unit	MAC Address	VLAN	Personal SSID	Password
Serial number of the device	Unit name	MAC Address of the device	VLAN(1 - 4094)	SSID for the personal Wi-Fi	Password for Wi-Fi
B1000D000000	MDU 01	B1:00:0D:00:00:00		10 SSID 01	Pa\$\$Word123
B1000D000001	MDU 02	B1:00:0D:00:00:01		13 SSID 02	Pa\$\$Word123
B1000D000003	MDU 03	B1:00:0D:00:00:03		11 SSID 03	Pa\$\$Word123

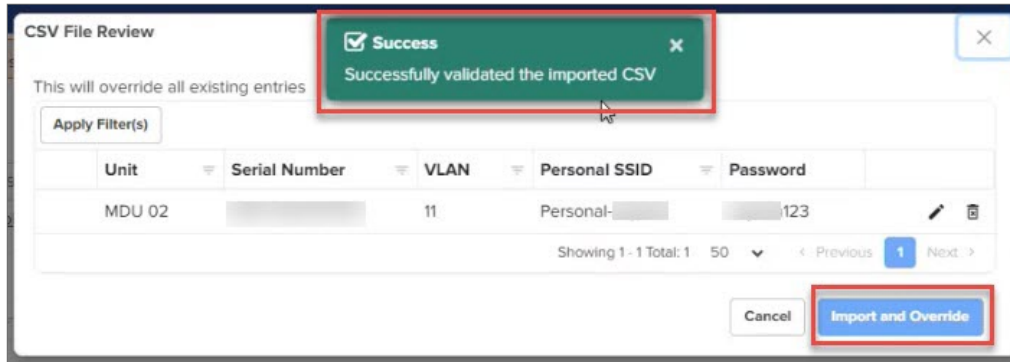
Parameter	Description
Serial Number	Enter the serial number of the device.
Unit	Enter the name or number of the unit (for example, MDU 01, MDU 02, and MDU 03 are apartment numbers).
VLAN	Enter the VLAN ID assigned to the unit.
Personal SSID	Enter the SSID for the personal WiFi network.
Password	Enter 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.

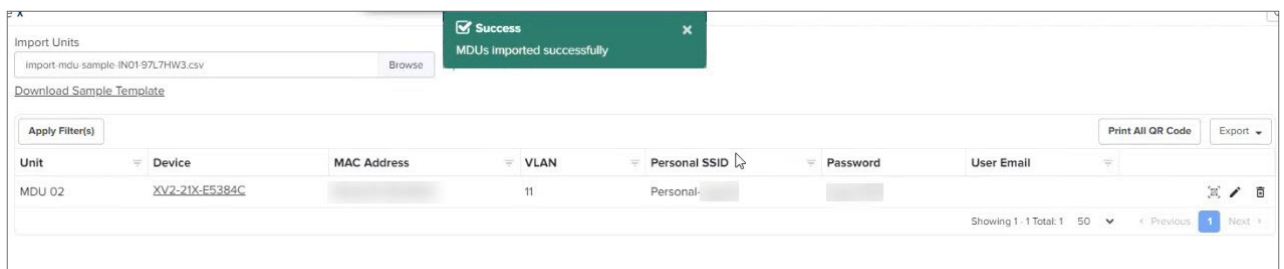


All the error messages are similar to those described in the [Units managed in Managed Wi-Fi app](#) sections.

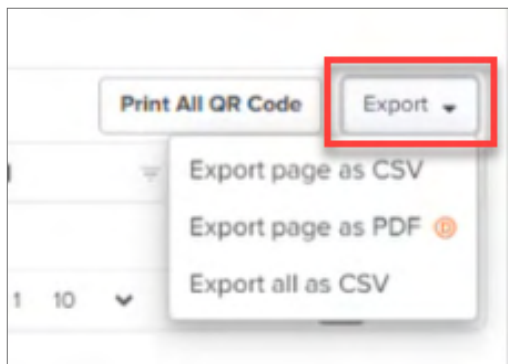
5. Once the file imports correctly, you can see the **Successfully validated the imported CSV** message as shown in the below figure.



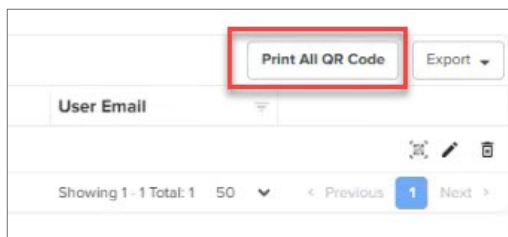
6. Click **Import and Override** to finalize the import process.
7. Once the devices are successfully added, a pop-up message displays: **MDU imported successfully**.



8. To export the data, select the required option from the **Export** dropdown list.



9. Click the **Print All QR Code** option on the right side to open a QR scan page.



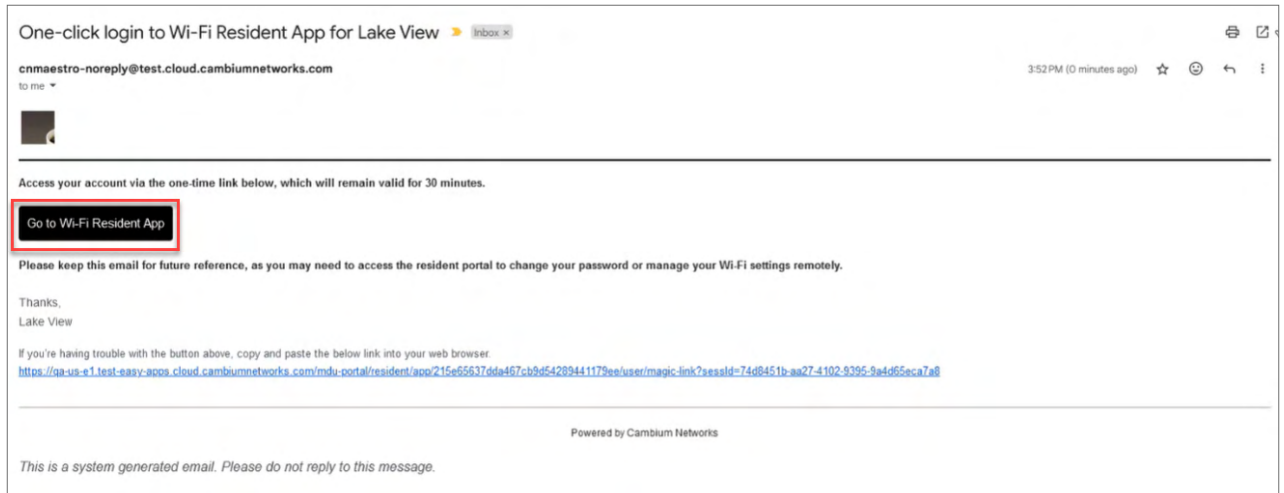
10. Scan the QR code using your mobile device to get a link.



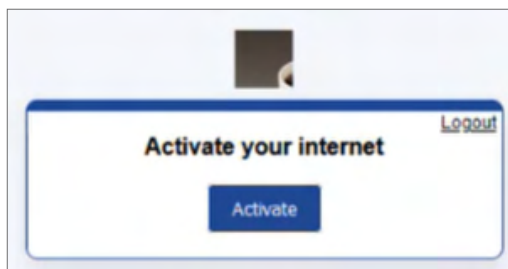
11. Enter your email ID and click **Send me a one time link**.

A screenshot of a web page titled "Welcome to Test-XXXX-SelfService". At the top left is a QR code. Below it is a text input field labeled "Email ID" containing the text "testuser@cam.ac.uk". A blue button labeled "Send me one time link" is positioned below the input field. The page contains the following text: "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." and a tip: "Tip: Bookmark this page in your browser for easy access later."A screenshot of a web page titled "Check your inbox.". The text on the page reads: "If the information you entered matches our records, you'll soon receive an email containing a one time sign-in link." Below this is a grey rectangular placeholder. Further down, it says "Don't see your email?" and "Check your spam folder or [resend](#) the link."

12. Open the email and click **Go to the Wi-Fi Resident App**.



13. Click **Activate** to initiate the internet activation process.



14. A new window titled **Change Wi-Fi Settings** appears. Change your Personal Wi-Fi Network Name and Wi-Fi password in the respective fields.



15. Click **Update** to save the changes.
16. You receive a message that says **Wi-Fi settings updated successfully**. Below the QR code, the option **Personal Wi-Fi** appears. You can scan to connect to this network.



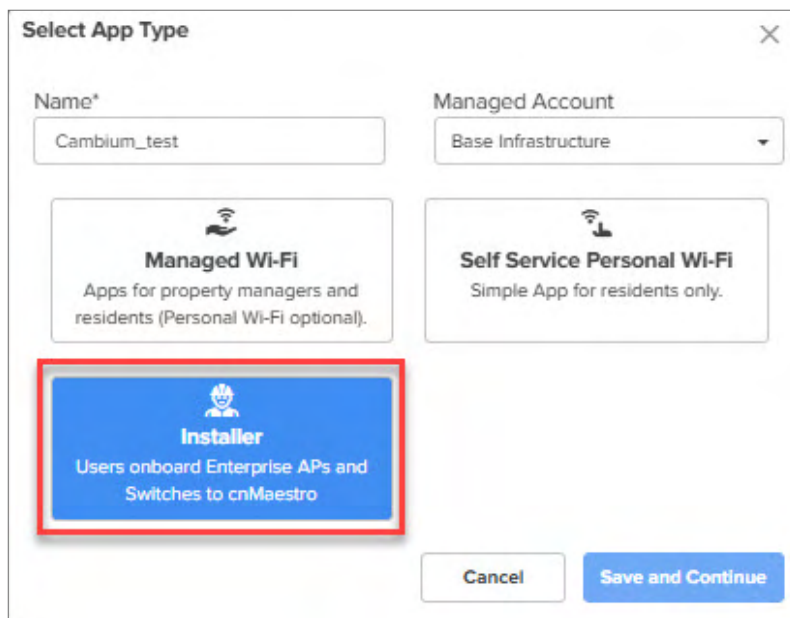
17. Scan the QR code to verify that your Personal Wi-Fi Network Name and Wi-Fi password have been updated.

Installer App

The Installer App supports ISPs and MSPs during on-site device installation. It streamlines the setup process by allowing installers to log in, record installation details (like placement, photos, and height), and automatically provision the device to the correct site with the required configuration. This removes manual coordination between field staff and backend teams, ensuring faster and more accurate onboarding.

Installers receive invitations via email, which they can use to access the app. Once logged in, installers select the site, attach the necessary AP or Switch Group, and complete the provisioning with minimal effort.

Figure 607 *App type*



Basic tab

The configuration steps for the Basic tab are the same as those detailed earlier in the documentation. For information on setting the app name, managed account, and description, refer to the [Basic tab](#) configuration steps.

Settings tab

The Settings tab in the Installer App allows you to configure installation-specific settings. You can enable options to attach AP Groups or Switch Groups during installation, based on the device type and location. These settings help ensure the correct configuration is applied when provisioning devices in the field.

Figure 608 *Installer settings tab*

The screenshot shows the 'Settings' tab in the MarketApps installer configuration interface. On the left, a sidebar contains 'Basic', 'Settings' (selected), and 'Design' tabs. The main area is titled 'Site*' and shows 'Building20' selected from a dropdown. Below this, there are two sections: 'Allowed to attach AP Group' and 'Allowed to attach Switch Group'. Both sections have a toggle switch set to 'On'. The 'AP Groups' section shows 'Community-APGroup' selected in a dropdown, with a 'Select or Search' button below it. The 'Switch Groups' section shows 'Default Switch' selected in a dropdown, also with a 'Select or Search' button. Below these, the 'Invite Installer' section shows five email addresses entered in a row: 'example.com', 'example.com', 'example.com', 'example.com', and 'example.com'. A 'Type and press Enter' instruction is below the emails. At the bottom, there is a 'Resend Invite' link and 'Save' and 'Close' buttons.

To configure settings options in the Installer app, complete the following steps:

1. Map one site to the app where all devices get onboarded. The **Site** field lists all sites available for selection in the Installer App for the specified Managed Account. This field is read-only and can be configured only once.
2. Use the **Allow to Attach AP Group** option to let installers select an AP Group during installation.

This option is disabled by default. When enabled, a searchable dropdown labeled **Select or Search** appears, allowing the MSP to choose from the available AP Groups based on location, device type, or customer category.



Note

- If **Allow to Attach AP Group** is disabled, no base configuration is applied to the AP during installation.
- If multiple groups are configured, a dropdown appears for the installer to select the appropriate group.

3. Use the **Allow to Attach Switch Group** option to let installers select a Switch Group when provisioning switches.

This option is also disabled by default. When enabled, a **Select or Search** dropdown appears, where the installer can choose the appropriate Switch Group to apply the correct base configuration.

4. Configure one or more AP or Switch Groups that the installer can select during the installation process.
5. In the **Invite Installer** field, type the installer's email address and press Enter to add it.

You can add multiple installers by entering one email ID at a time. You can add up to 10 unique email IDs.

6. Click **Save** to apply the settings.

Design tab

The Design tab lets you brand the Installer App interface and customize the fields shown during device setup. It works similarly to the Design tab in the Managed Wi-Fi app.

Figure 609 Design tab parameters

MarketApps > [App Name] InstallerApp x

Basic

Settings

Design

Display Name*

[Text Field: Installer App]

Name will be used in email communication and displayed to the installer.

Service Provider Name*

[Text Field: Cambium Networks]

The name of the entity providing the service.

Logo

[Text Field]

Select File

We recommend uploading a transparent PNG cropped to the edges of your logo. Image maximum size should be 200x200 pixels.

Theme Color

[Color Picker: #25478d]

Choose a custom accent color for the portal page.

Privacy URL

[Text Field: https://example.com/privacy-policy/]

Privacy Policy that accounts has to acknowledge on their first access to the service.

Terms and Conditions URL

[Text Field: https://example.com/terms-conditions/]

Terms and Conditions that accounts has to acknowledge on their first access to the service.

☒ Show "Powered by"

Powered by*

[Text Field: Cambium Networks]

Save Close

Sign In

Email ID

[Text Field]

Send me one time link

You will receive an email containing a one-time sign-in link. Clicking this link will take you directly to the Installer App.
Tip: Bookmark this page in your browser for easy access later.

Powered by Cambium Networks

Privacy Policy | Terms of Service

< Application >

Table 159 Installer design tab parameters

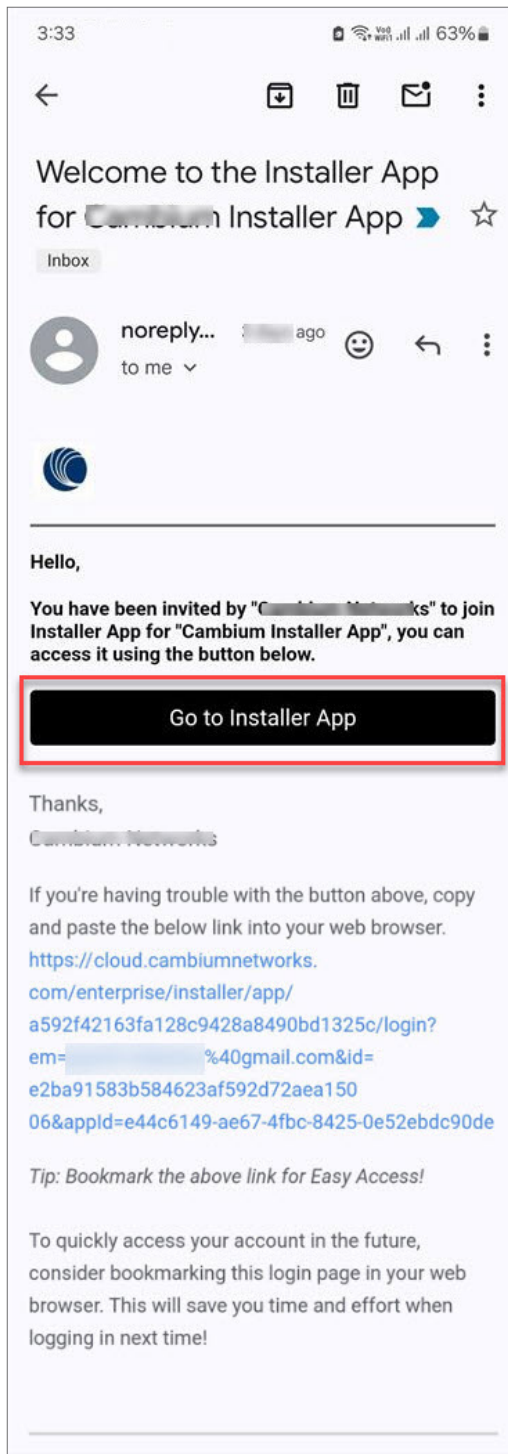
Parameter	Description
Display Name*	Specifies the name shown for the MarketApps app in the Installer App interface.
Service Provider Name*	Specifies the name of the service provider or property. This name appears only in the invitation email sent to the installer and does not appear in the Installer App interface.
Logo	Upload a logo file (PNG recommended) cropped to the edges and sized up to 200x200 pixels.
Theme Color	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"	Enable this option to display the Powered by message.

Parameter	Description
by"	
Sample screen	<p>The sample screen section includes two views:</p> <ol style="list-style-type: none"> 1. Application—Provides a view of the sign-in interface that installers use to access the Installer app. 2. Email—Provides a view of the email format that installers receive, which contains a link to access the Installer app.
Save	Click Save to apply the changes after configuring the Design tab.

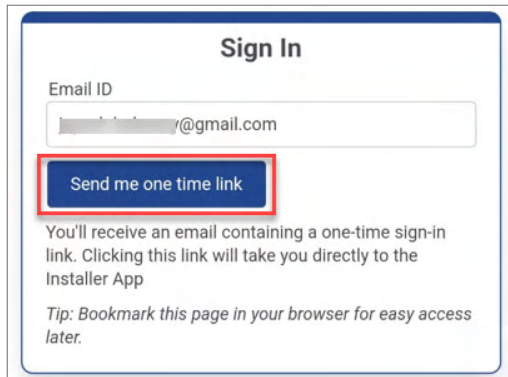
Accessing the Installer App interface

After configuring the MarketApps Installer App and inviting installers, the following steps explain how an installer accesses the Installer App interface:

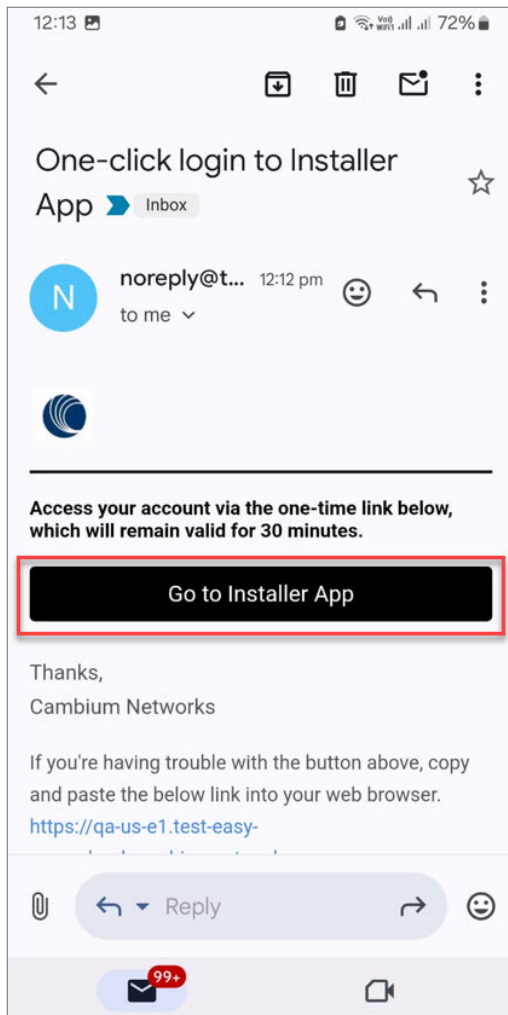
1. The installer receives a customized email titled **Welcome to the Installer App for <Display name>** as shown in the figure below.



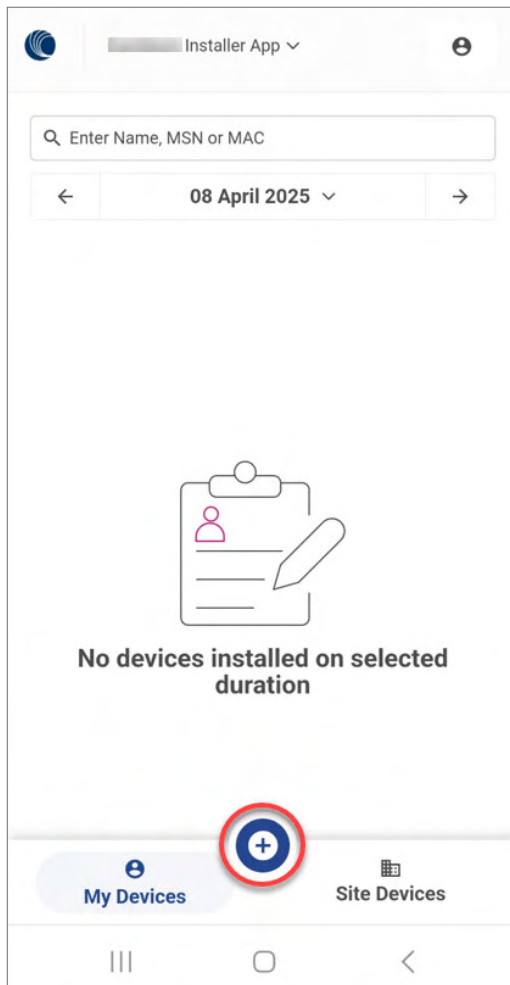
2. Installer clicks **Go to Installer App** in the email. The **Sign In** screen appears if not already logged in.



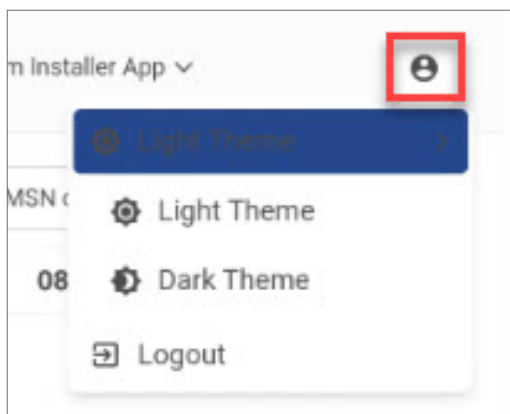
3. The installer enters their email ID and clicks **Send me one time link**.
4. The installer receives another email titled **One-Click Login to Installer App**. It includes a one-time login link that expires after 30 minutes.



5. Installer clicks **Go to Installer App** in the second email to access the app interface.
6. The app opens with a customized login screen that shows the configured display name, logo, and theme.

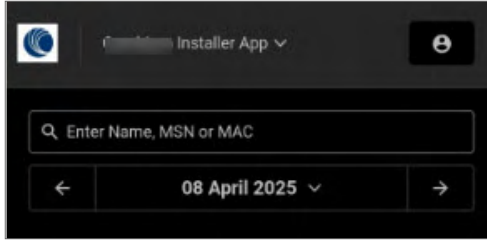


7. The app automatically displays any previous installations. The installer selects an existing entry to view its details if needed.
8. A search bar appears at the top, which allows the installer to search using a device name, MSN, or MAC address.
9. The current date appears below the search bar.
10. To change the theme or log out, the installer taps the profile icon in the top-right corner.



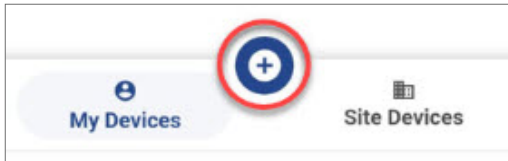
A menu appears with the following options:

- **Light Theme:** Displays the app in a bright, standard view.
- **Dark Theme:** Switches the app to a dark background for better visibility in low light.



- **Logout:** Logs the installer out of the app.

- To start a new installation, the installer taps the **+** (plus) icon located between **My Devices** and the **Site Devices** as shown in the below figure.



- A new window **Add Device** appears.



- The installer enters the Serial Number (MSN) manually or taps **Scan MSN** to scan the QR code using the device camera, then click **Add** to proceed. The **Update Device** screen appears.

Update Device

×

Serial Number (MSN)

/J4

MAC Address

e8

Device Name*

RockAP

AP Group

Default Enterprise

Address

Get Location

Height

5

Unit in feet and inch

Azimuth

10

Degrees from North (0° to 360°)

Tilt

8

Degrees from Horizon (-90° to 90°)

Description

Premium customer

Installer Comments

All good

Add Image

Add Image

Add Image

Add Image

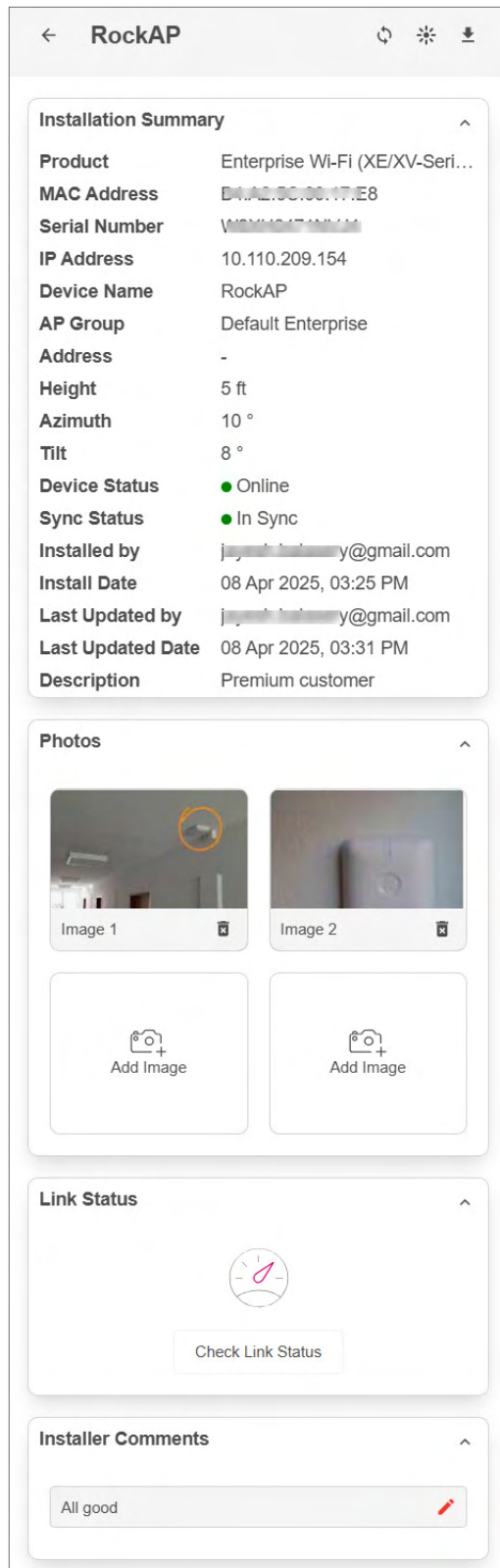
Save

Table 160 *Update Device screen parameters*

Parameter	Description
Serial Number (MSN)	Displays the device's serial number. This field is pre-filled and not editable.
MAC Address	Displays the device's MAC address. This field is pre-filled and not editable.
Device Name	The installer enters a custom name for the device.
AP Group	The installer chooses the appropriate AP Group for the device during installation.
Location	The installer taps to update the current location.
Height	The installer enters the height in feet and inches.
Azimuth	The installer enters the azimuth angle in degrees (0° to 360°).
Tilt	The installer enters the tilt angle from horizontal (-90° to 90°).

Parameter	Description
Description	The installer adds relevant notes, such as customer details or site information.
Installer Comments	The installer enters any additional observations or remarks.
Add Images	The installer can upload up to four images related to the installation.

14. Installer taps **Save** to apply the changes and complete the device installation.
15. The app redirects to a new page displaying the Installation Summary for the installed device.



The summary page includes the following sections:

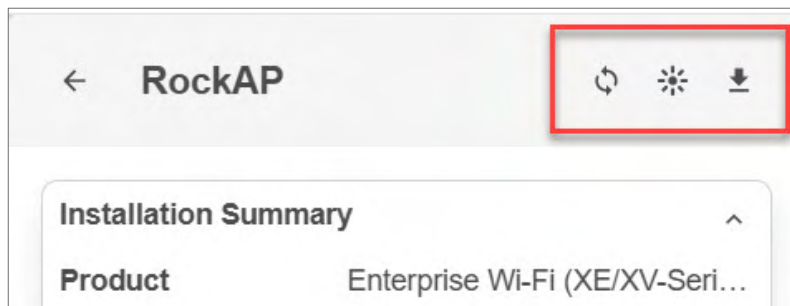
- **Installation Summary:** Shows key details such as product name, MAC address, serial number, IP address, device name, AP group, address, height, azimuth, tilt, device status, sync status, installer details, and timestamps for install and last updated.

- **Photos:** Displays uploaded installation images. The installer can tap Add Image to upload more photos if required.
- **Link Status:** Allows the installer to tap **Check Link Status** to view the Ethernet speed and validate connectivity.
- **Installer Comments:** Displays any comments entered earlier. The installer can edit or update the comment from this screen.

Additional options on the summary page

The top-right corner of the summary page includes three options that help installers perform additional actions based on their needs as shown in [Figure 610](#).

Figure 610 Additional options on the summary page



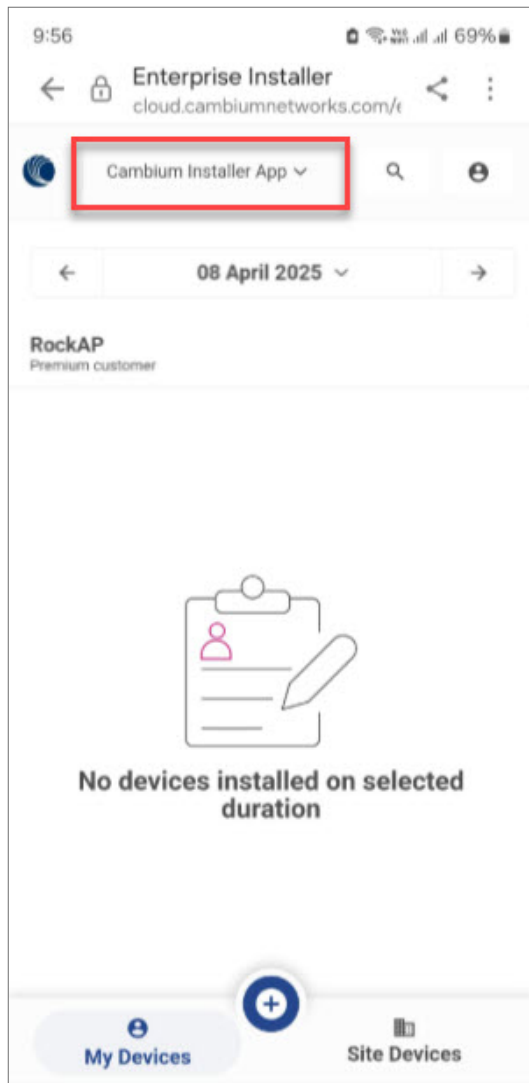
- **Refresh** – Updates the page with the latest device information pulled from the server.
- **Flash LED** – Triggers the selected device's LED to blink for 30 seconds, helping the installer identify the correct unit on-site.
- **Download Report** –Generates and downloads a PDF report containing all installation details shown on the screen. This report can be saved or shared with the Internet Service Provider (ISP).

To return to the main device list, the installer taps the back arrow located at the top-left corner next to the device name.

Viewing installed devices and switching between apps

1. The main screen displays a list of devices installed by the logged-in installer under **My Devices**. Devices installed by other installers for the same MarketApps app appear under **Site Devices**.
2. The installer can view the installation history for the past 10 days using the date field at the top to filter and navigate by date.
3. If the installer has access to multiple MarketApps Installer Apps, they can use the dropdown ([Figure 611](#)) at the top to switch between apps—there is no need to go through the invitation email flow again.

Figure 611 *Viewing installed devices*



Locating installed devices in cnMaestro

Once a device is installed through the Installer App, it appears in the Onboarding section of cnMaestro under the site selected during installation. From there, the device follows the standard onboarding workflow based on its configuration and assigned groups.

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)** dropdown list.

Figure 612 *Network Services > CBRS > Account tab*

The screenshot shows the 'Network Services > CBRS' page. It contains the following elements:

- A header bar with the text 'Network Services > CBRS' and a close icon.
- A paragraph: 'Enable Citizens Broadband Radio Service subscription for the CBRS-compliant devices in 3.6 GHz band (3550 MHz to 3700 MHz). [Learn more](#)'
- A label: 'Spectrum Access System (SAS)' with a red information icon.
- A dropdown menu with the placeholder text 'Please select a SAS vendor'.
- Two checkboxes with labels:
- ☐ I accept the [CAMBIUM NETWORKS, LTD. "CBRS" TERMS OF SERVICE](#)
- ☐ I accept the [CBRS Service payment terms](#)
- An 'Enable' button at the bottom.

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' window with the following sections:

- Business Contact** (checkbox):
 - First Name:
 - Last Name:
 - Email:
 - Phone:
 - Street Address:
 - City:
 - Zip Code/Postal Code:
 - State:
 - Country:
- Technical Contact** (checkbox):
 - ☐ Same as Business Contact
 - First Name:
 - Last Name:
 - Email:
- SAS Portal Contact** (checkbox):
 - Text: '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.'
 - Radio buttons: ☒ Business Contact, ☐ Technical Contact, ☐ Other
 - Email (if not Business Contact or Technical Contact):
- Buttons: 'Save' and 'Cancel' at the bottom.

- **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

XXXXXXXXXXXX1111 Expiration 1/2020

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

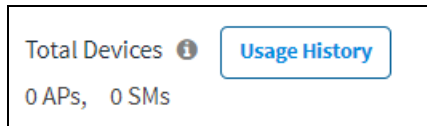
When the SAS ID allocation is pending or unavailable in the server,

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

1004 | Citizens Broadband Radio Service (CBRS)

Cambium cnMaestro Cloud | User Guide

- **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

- Select One

Bank Name

Account Holder Name

Required Field

submit

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

Search

Add AP/SH/RRH

Import Sector

Relinquish Grant

Export

Device Name	Device Type	Health	User ID	Tool Frequency (MHz)	Operating Frequency (M...	Grant Type	Sector ID	Spectrum Reuse ID	Include User ID
88	PMP 450 Connectorized	Offline		3570 - 3590	N/A	Multigrant		N/A	N/A
shd	PMP 450 Connectorized	Offline		3560 - 3580	N/A	Multigrant		N/A	N/A
tool-88	PMP 450 Connectorized	Offline		3570 - 3590	N/A	Multigrant		N/A	N/A

Showing 1 - 3 Total 3 10 Previous 1 Next

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 Search

Add AP/BHM/RRH Import Sector Relinquish Grant Export

Device Name	Device Type	Health	User ID	Tool Frequency (MHz)	Operating Frequency (M...	Grant Type	Sector ID	Spectrum Reuse ID	Include User ID
ib	PMP 450 Connectorized	Offline		3570 - 3590	N/A	Multigrant		N/A	N/A
ibd	PMP 450 Connectorized	Offline		3560 - 3580	N/A	Multigrant		N/A	N/A
toolat	PMP 450 Connectorized	Offline		3570 - 3590	N/A	Multigrant		N/A	N/A

Showing 1 - 3 Total: 3 10 Previous 1 Next

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 Search

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
ib	PMP 450 Connectorized	Offline	SITMGABLAZ9	3570 - 3590	N/A	Multigrant	34-89-23-09-12-27	N/A	N/A
ibd	PMP 450 Connectorized	Offline	SITMGABLAZ9	3560 - 3580	N/A	Multigrant	12-90-34-90-34-67	N/A	N/A
toolat	PMP 450 Connectorized	Offline	SITMGABLAZ9	3570 - 3590	N/A	Multigrant	12-45-67-34-79-21	N/A	N/A

Showing 1 - 3 Total: 3 10 Previous 1 Next



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
19	Relinquish	Base Infrastructure	System	Now		Nov 07, 2022 11:44	Nov 07, 2022 11:44	Completed
18	Reboot	Base Infrastructure	Ext E2E-101	Schedule		Nov 04, 2022 15:43	Nov 04, 2022 15:54	Completed
17	Reboot	Base Infrastructure	Ext E2E-102	Schedule		Nov 04, 2022 11:48	Nov 04, 2022 16:53	Completed
16	Reboot	Base Infrastructure	Onboard-79	Schedule		Nov 03, 2022 19:10	Nov 04, 2022 10:15	Completed
15	Reboot	Base Infrastructure	rseries_site	Schedule		Nov 03, 2022 18:27	Nov 04, 2022 09:32	Completed
14	Reboot	Base Infrastructure	umatrix_site	Schedule		Nov 03, 2022 15:52	Nov 04, 2022 12:57	Completed
13	Reboot	Base Infrastructure	System	Schedule		Nov 03, 2022 15:52	Nov 04, 2022 12:56	Completed
12	Reboot	All Accounts	System	Schedule		Nov 03, 2022 11:44	Nov 04, 2022 11:49	Completed
11	Reboot	All Accounts	System	Now		Nov 03, 2022 11:38	Nov 03, 2022 11:38	Completed
10	Reboot	Base Infrastructure	System	Schedule		Oct 29, 2022 17:28	Oct 29, 2022 17:33	Completed

Showing 1-10 Total: 18 10 Previous 1 2 Next

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.

Add AP-Bandwidth

☐ Common parameters

Device Name:

Model:

Device Type:

Private ID:

NAC Address:

MSDN:

User ID:

☐ Location related parameters

Latitude:

Longitude:

Height:

Height Type:

Horizontal Accuracy:

Vertical Accuracy:

☐ Antenna related Parameters

Integrated Antenna Gain (dBi):

External Antenna Gain (dBi):

Beamwidth(degrees):

Azimuth (degrees):

Down Tilt (degrees):

☐ ECGI related Parameters

PLMN ID:

ECI (whole ID + PCI):

ECID:

☐ Co-Existence related parameters

Sector ID:

Spectrum Reuse ID:

Add CPI Certificate
CPI information is written stored on client not on the server. It protects against any misuse of CPI certificate and its password.

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.

Import Sector Data

Excel File
cbrs_template_06.xlsx Import Spreadsheet Download Template ▼

CPI information is neither stored on client nor on the server. It protects against any misuse of CPI certificate and its password.

Certificate File* Import Certificate

File Password*

User ID* ⓘ
7A45Y9

CPIR Name*
Impena V T

Sector ID
0e-00-3e-42-9f-d6 Edit

Spectrum Reuse ID
Select Reuse ID Add Delete

Include User ID
Yes

Import

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 dropdown list.
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**.

✓ Success: 2Device(s) have been claimed. ▼

✗ Invalid: 1 Device(s) are not valid. ▼

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 Add AP/SHM/RRH Import Sector Relinquish Grant Export

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 10 Previous Next

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

MAC Address

Device Name

Device Type	Health
PMP 450b High Gain	Online



Note

- If an AP device is entered into Search, it displays both AP devices and the related SM


devices.

- If an SM devices is entered into Search, it displays only SM devices.

Mac

Q 0B

Device Name	Device Type	User ID
450i-AP Integrated	PMP 450i Integrated	SF5W5D
Lab-setup-AP	PMP 450 Connectorized	SF5W5D
ak-1	PMP 450i Connectorized	SF5W5D





1. Filter AP or sectors can be cleared by clicking  or **Clear** button.

Sector View

1. Click a sector from the Sector AP column to get the list of devices.





Sector AP	Device Type
"208.41"	PMP 450 Integrated

2. All devices of the sector are displayed.

Management Tool > Mibank-5G												
Tool Frequency (MHz): 3550 - 3580 Operating Frequency (MHz): N/A												
Search												
Add SM/BHS Reinquish 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		25.768	-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 >												

Sector Details View

- The Sector Details view displays the following fields by default:
 - Device Name, Device Type, Mode, Health, MSN, Latitude, Longitude, Sync Expiry Time, Height, Registered, Sync State, Actions.

Management Tool > Mibank-5G												
Tool Frequency (MHz): 3550 - 3580 Operating Frequency (MHz): N/A												
Search												
Add SM/BHS Reinquish 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		25.768	-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 >												



Note

If the device is **Config_Synced**, the CBSD state of the device will be updated from the device in real-time.

- SM can be added in the sector by manually entering all parameters using **Add SM** button or uploading a file containing all SM details using **Import SMs** button.
- Action column can edit or delete any device in the sector. **Edit** and **Delete** buttons are available depending upon the device state. Refer to [Edit device](#) and [Delete device](#) for more details.
- To include additional fields to be displayed in the **Sector Details** view, select required fields in the column

selector().

☐ **General**

☒ Device Name
 ☒ MAC Address
 ☒ Device Type
 ☒ Mode
 ☒ Health
 ☒ Serial Number
 ☐ CBSID ID
 ☒ Sync Expiry Time
 ☐ Horizontal Accuracy
 ☐ Vertical Accuracy
 ☐ ECGI (E-UTRAN Cell Global Identifier)
 ☒ Grant Status
 ☒ Sync State

☐ **Location**

☒ Latitude
 ☒ Longitude
 ☒ Height
 ☐ Height Type

☐ **Antenna**

☐ Integrated Antenna Gain (dBi)
 ☐ External Antenna Gain (dBi)
 ☐ Beamwidth (degree)
 ☐ Azimuth (degrees)
 ☐ Down Tilt (degrees)
 ☐ Max EIRP (dBm)
 ☐ Requested EIRP (dBm)
 ☐ Granted 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

Search

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

- Navigate to **Services > CBRS > Management Tool** > select a sector.
- 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 ▼.

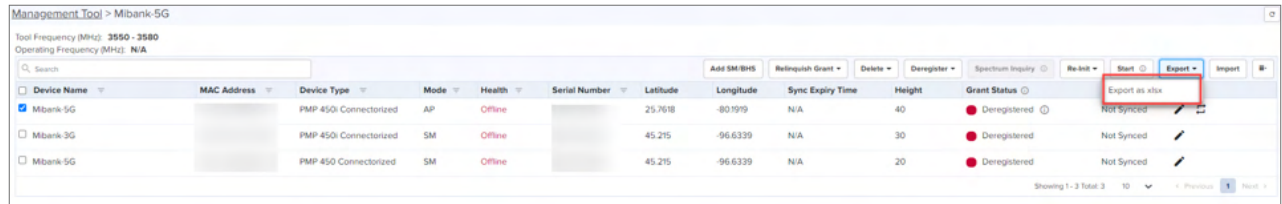
MAC	Error
0a-00-3e-45-11-e4	Serial Number is invalid

9. If the devices is already claimed, it can be onboarded by clicking the **onboard** link.

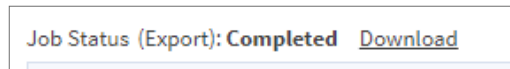
10. Once the user clicks **Import**, a job is scheduled.

Export Sector

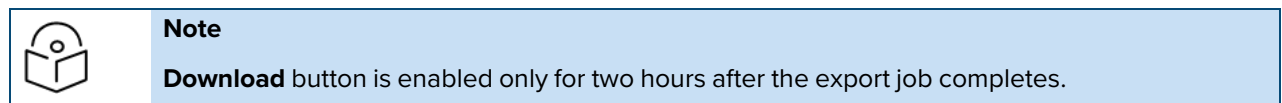
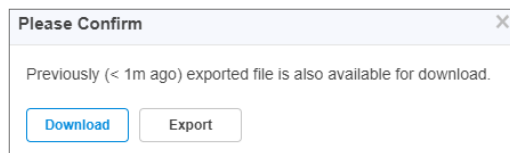
1. Navigate to **Services > CBRS > Management Tool** and then select a sector.
2. Click **Export** button to export the sector (export as xlsx).



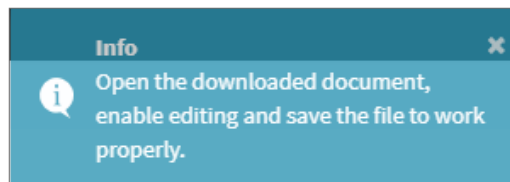
3. Once the user clicks **Export**, a job is scheduled.



4. Once the Job status is Completed, **Download** the Sector xlxs.



5. User can use the .xlxs 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 is selected, choose the appropriate option from the **Delete** dropdown list:
 - **All**: Deletes all registered SM devices.
 - **Selected**: Deletes the selected SM 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.

The following confirmation message is displayed when you select the **Selected** option from the **Delete** dropdown list.

Please Confirm

This action will delete 1 device(s) under current sector. Do you want to continue?


☐  The device will be deregistered from the SAS, if it is registered.

If the device is no longer in use, it is strongly recommended to delete the CPI data from the device to prevent accidental reregistration, which may result in recurring charges.

For PMP devices running Release 24.2 or later:

- In the device UI, go to the Configuration > CBRS tab and click Delete CPI Data.
- Return to this message and click Yes to proceed.

For PMP devices running a version earlier than Release 24.2:

- In the device UI, go to the Configuration > CBRS tab and click Delete CPI Data.
- Click Reboot.
- Immediately return to this message and click Yes to proceed.
-  **Important:** The final step must be completed before the device finishes restarting. Otherwise, the device may reregister, even if it has been deleted from cnMaestro.

6. After confirmation, a job is scheduled.

Job Status (Delete): **Completed with device(s) failure**

7. 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.

8. Select the AP of the sector to delete.

9. 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 dropdown list.
 - All:** Unblocks all registered devices.
 - Selected:** Unblocks the selected devices.

Management Tool > RRH

Device Name	Device Type	Mode	Health	MSIN	Latitude	Longitude	Sync Expiry Time	Registered	Sync State	Actions
<input checked="" type="checkbox"/> RRH	Third Party	RRH	Offline		90	90	N/A	N/A	Not Synced	 
<input type="checkbox"/> SM-1	3GPP eUICC 201 SM	SM	Offline		44.5678	-110.98765	N/A	20	DEREGISTERED	Not Synced 
<input type="checkbox"/> SM-2	Tyndall 201	SM	Offline		44.56789	-110.987654	N/A	20	 DEREGISTERED	Not Synced 

Showing 1 - 3 Total: 3

4. 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

5. 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.

Spectrum Inquiry (Wed Mar 31 2021 22:42:13 UTC +0530)

Editing the co-existence parameter will reset the SAS timer. Edit only if really needed

☒ SAS provided spectrum availability view

Sorted By Ranking

Sorted By Frequency

☒ Co-Existence Configuration

Sector ID: 0a-00-3a-45-4a-06 Spectrum Reuse ID: Balaji

☒ Spectrum Reuse ID Statistics

Spectrum Reuse IDs already defined in your Network

Spectrum Reuse ID	Center Frequency (MHz)/Channel Bandwidth (MHz) [Sector Count]
Balaji	3585.00 / 3585.00 - 3585.00 / 3585.00 [1]

☒ EIRP computation

Devices are listed with calculated maxEIRP and requested EIRP based on the selected center frequency and channel bandwidth. Click Save to update the EIRP of devices and continue the procedure

☐ I understand, SAS may take up to 5h 40m to fully process the co-ex parameters and the Spectrum Inquiry response may not be updated yet

Center Frequency (MHz)*: Please Select Channel BW (MHz)*: Please Select SAS Allowed Total MaxEIRP (dBm):

Calculate Max EIRP



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

Search

Add SM/BHS Revoke 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
<input type="checkbox"/> Mibank-5G		PMP 450i Connected	AP	Offline		25.7618	-80.1919	N/A	40	● Deregistered	Not Synced
<input type="checkbox"/> Mibank-3G		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 10 Previous 1 Next



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).

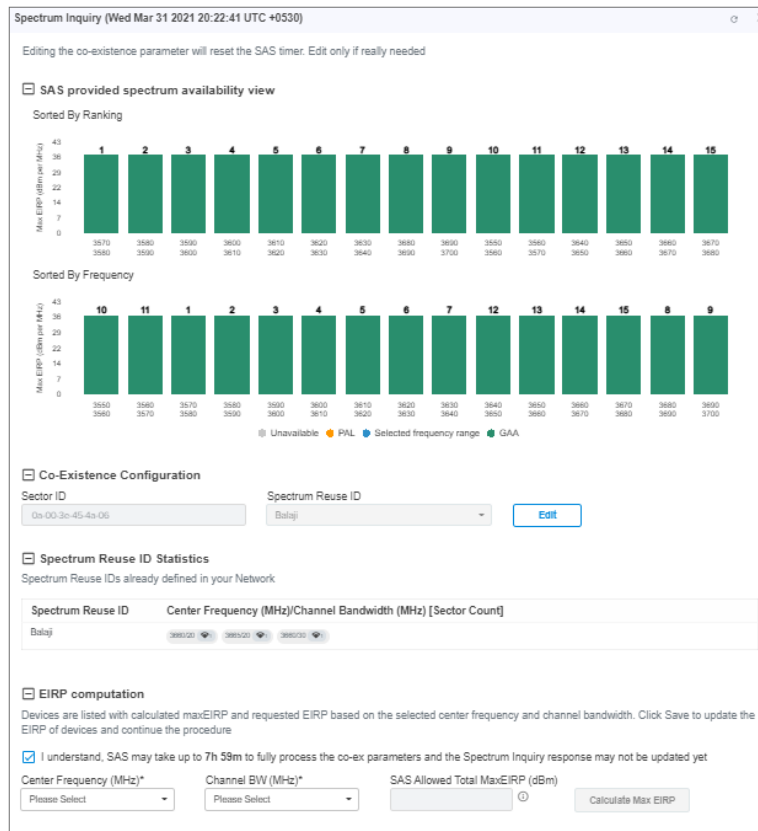
Multi-Grant

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.

4. 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.

5. 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.

6. Once the Spectrum Inquiry is verified, click **Save**.

A Sector created with Multiple Grants will be displayed as shown below:

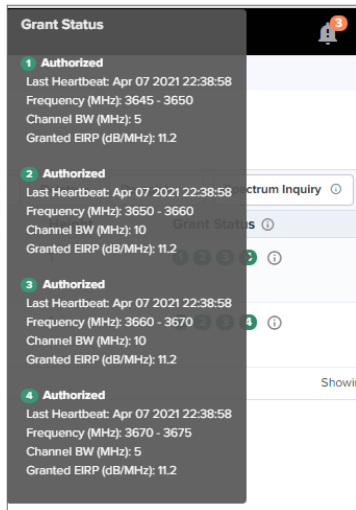
Management Tool > devicesno

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 ⓘ	Not Synced	Edit Refresh
devicesdev	PMP 450 Conn...	SM	Offline		44.444	-110.444	2d 2h 32m	1	1 2 3 4 ⓘ	Not Synced	Edit

Showing 1 - 2 Total 2 Previous 1 Next >

7. To view the Grant Status click the info (ⓘ) icon.



Relinquish Grant

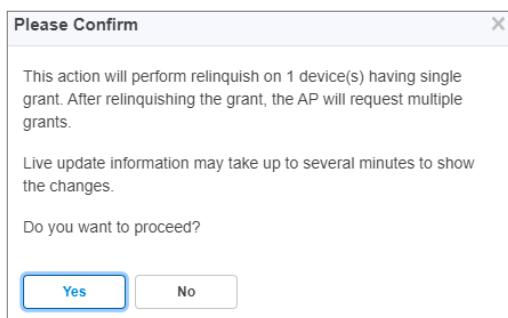
Relinquish Grant relinquishes all grants of selected sector. This will make devices enter the Registered state. The device will start Multi-Grant procedure if Multi-Grant feature is enabled on it.

To Relinquish Grant Perform as follows:

1. Navigate to **Services > CBRS > Management Tool** and select a sector with Single Grant.
2. 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.



3. Click **Yes** to confirm the action.



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

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"/> devicesmdev	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 10 < Previous 1 Next >

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).

- Navigate to **Services > CBRS > Management Tool** and select a sector.
- Click **Stop** if the CBRS procedure is already running.
- 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.

- Click **Re-init** to start the reinitialization procedure
- Confirmation window pops up:
 - Click **Continue** or
 - Select **Spectrum Inquiry** to edit the **EIRP values** as shown in [Start procedure](#).

Please Confirm

Do you want to proceed with saved sector details ?

Continue
Spectrum Inquiry



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.

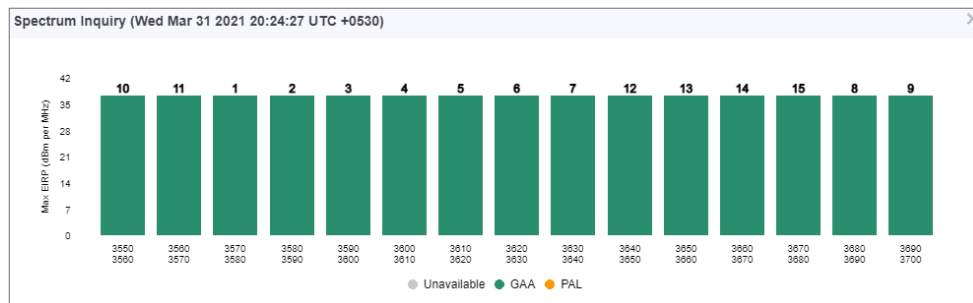
Once the user clicks **Deregister**, a job is scheduled.

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 users 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.

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 450i Integr...	SM	Online		45.114385	-96.642474	N/A	22	Authorized	Config Synced	

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

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

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 dropdown 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.

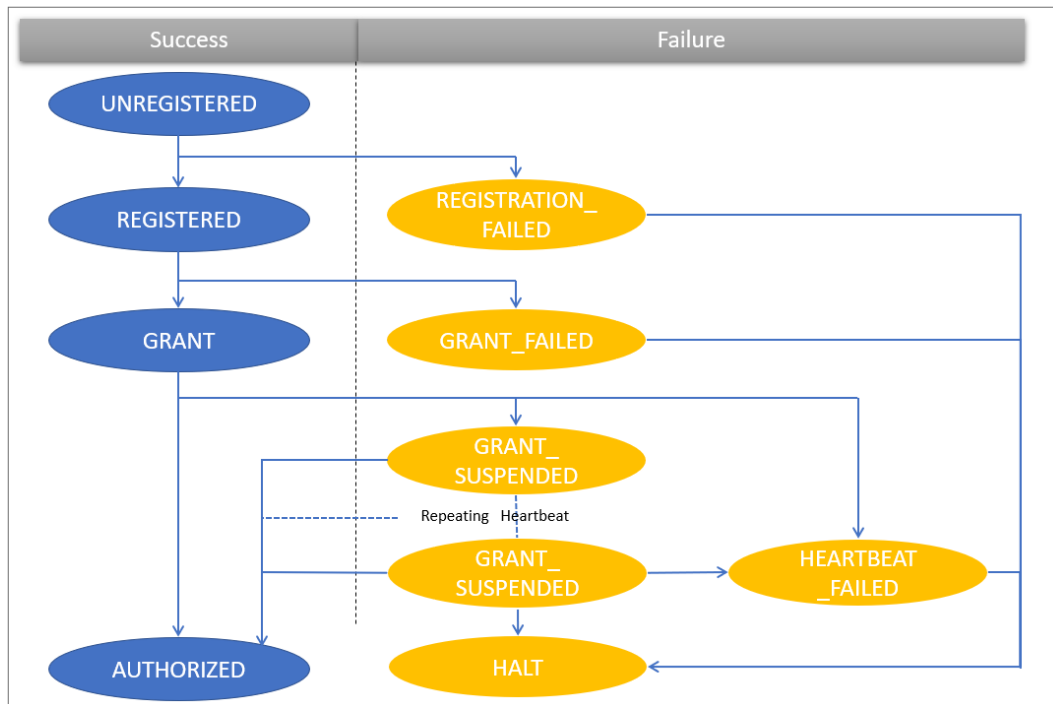
cnMaestro checks the heartbeat status of a CBRS device every 12 hours. The following statuses are updated in the **Heartbeat Status** column, based on whether the device is online or offline:

- **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

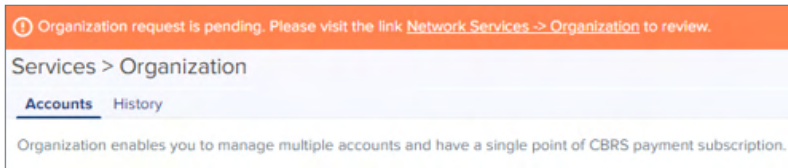
Category	Parameter	Details
Common	Channel BandWidth (MHz)	Channel Bandwidth of AP or BHM in MHz.
	Center Frequency (MHz)	Center frequency of AP or BHM in MHz.
	Device Name	Name given to device on SAS Admin (A maximum of 120 characters are supported. However, this name is not copied to the device when synchronized.)
	Device Type	Type of device.
	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.

Category	Parameter	Details
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.
Antenna Parameters	Azimuth (degrees)	Boresight direction of the horizontal plane of the antenna in degrees with respect to True North.
	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

☐ **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

☐ I authorize Cambium Networks to make changes to the selected account

[Request Support](#)

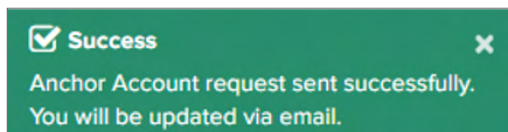
2. Select **Anchor Account** from the dropdown list.



Note

Users are allowed to select only one Anchor account from the dropdown 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 > 1 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

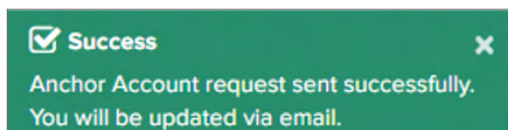
2. Select **Convert this Account to Anchor Account**.



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:

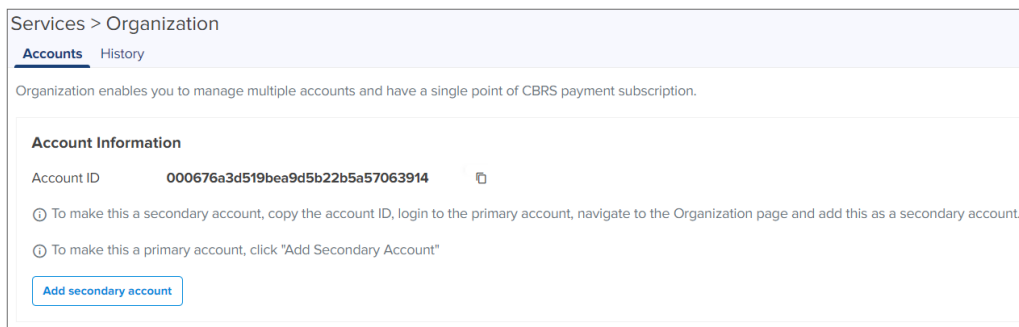
- [Create an Organization](#)
- [Remove Accounts](#)
- [Disable Secondary Account Services](#)
- [Edit Services](#)
- [Share CBRS Configuration with the On-Premises Instance](#)
- [Organization History](#)

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

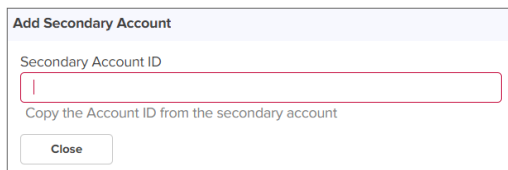
Account ID **000676a3d519bea9d5b22b5a57063914**

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

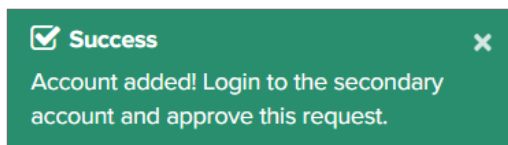
☒ Enable Unified Payments

ⓘ 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

Secondary Accounts

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

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	250c38b22c5526c73dcb6b615b5bf90	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	b8740772e97516dd935b6c415ddc1f	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 the delete () icon.

Network Services > Organization

[Accounts](#) [History](#)



Organization enables you to manage multiple accounts and have a single point of CBRS payment subscription. [Learn more](#)

Account Information - Primary Account

Account ID 

Account Type **Network Management System**

Secondary Accounts

Cambium ID	Account ID	Account Type	Approval Status	Enabled Services	
521_ESS	<input style="background-color: #f0f0f0;" type="text" value="521_ESS"/>	NMS	● Approved	Shared SAS ID, Unified Payments	 

[Add New](#)

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

DOCUMENTATION2

Reason

test

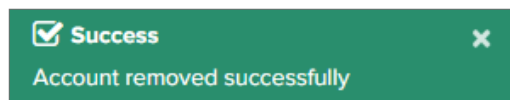
Proceed

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

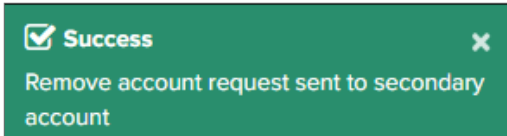
- If services such as **Shared SAS ID** or **Unified Payments** are active in the Secondary Account, the services need to be disabled from the Secondary Account, and the request must be approved by the Secondary Account administrator.



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.

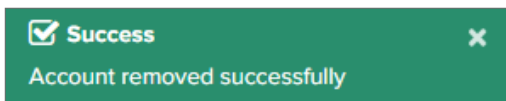
Please confirm

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.



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 ID7972ccc4d7dd0da4af1617c8c85a4d01
Account TypeNetwork Management System

Primary Account


The following Primary account wants to add you to its organization.

Cambium IDQA_SANDBOX_SB2
Approval StatusApproved

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.

Network Services > Organization

Accounts
History

Organization enables you to manage multiple accounts and have a single point of CBRS payment subscription. [Learn more](#)

Account Information - Primary Account

Account ID

Account Type
Network Management System

Secondary Accounts

Cambium ID	Account ID	Account Type	Approval Status	Enabled Services	
521_ESS	<div></div>	NMS	Approved	Shared SAS ID, Unified Payments	<div> <div></div> <div></div> </div>

Add New

- 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

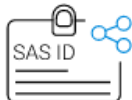
Secondary Account ID
7972ccc4d7dd0da4af1617c8c85a4d01

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

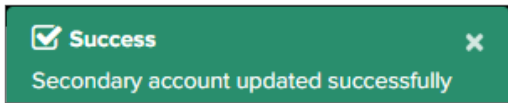
Please Note: Enabling Shared SAS ID will also enable Unified Payments

Update
Close

1046 | Organizations for CBRS

Cambium cnMaestro Cloud | User Guide

5. The following message displays if successful.

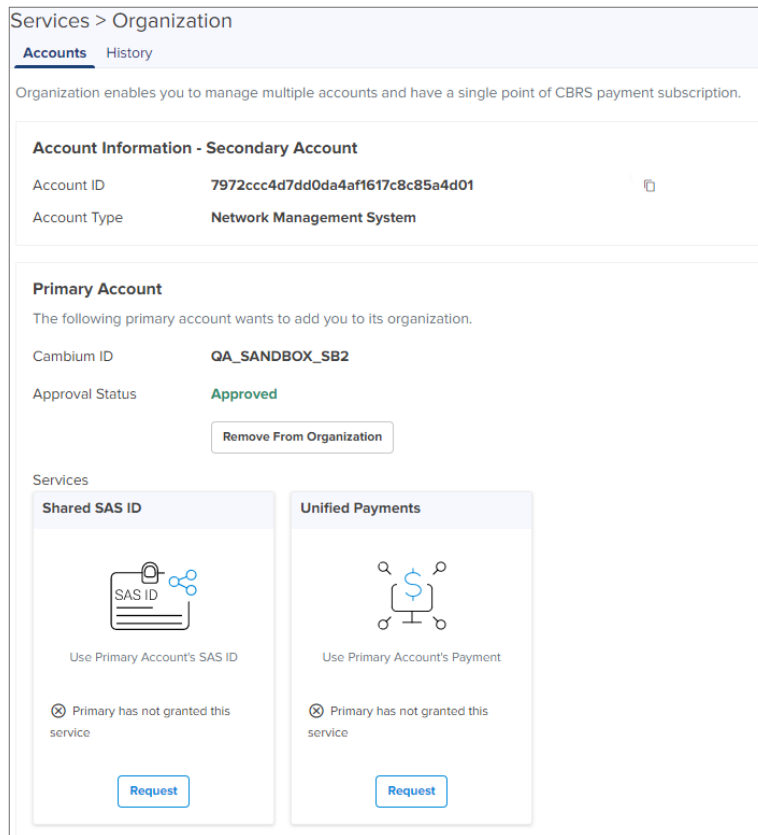


Request services from Secondary Account

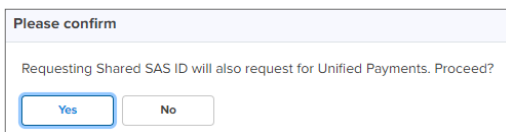
If the services are disabled, the Secondary Account needs to make a request to the Primary Account to activate them.

To request activation, perform the following on the Secondary Account:

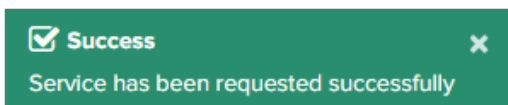
1. Navigate to **Network Services > Organization > Accounts**.
2. Click **Request**.



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.

Manage Instances						
Onboarding On-Premises Instances						
<input type="text" value="Search"/>						
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	<div> <div>Sync Now</div> <div></div> </div>
Showing 1 - 1 Total: 1 10 < Previous 1 Next >						

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

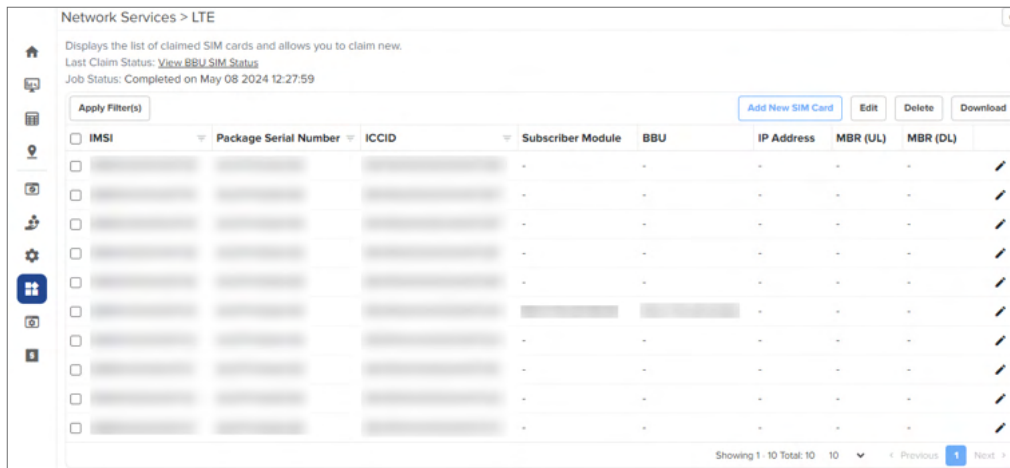
cnMaestro supports LTE as part of its cnMaestro deployment. LTE allows customers to onboard the SM with IMSI into cnMaestro.

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

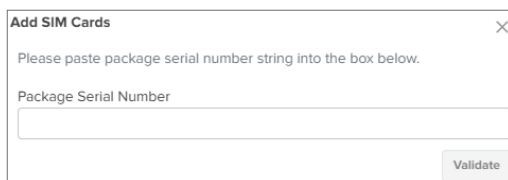
To add a SIM card, complete the following steps:

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 buttons for 'Add New SIM Card', 'Edit', 'Delete', and 'Download'. A table lists SIM cards with columns: IMSI, Package Serial Number, ICCID, Subscriber Module, BBU, IP Address, MBR (UL), and MBR (DL). The table shows 10 rows of data. At the bottom, there is a pagination bar indicating 'Showing 1 - 10 Total: 10' and navigation buttons for 'Previous' and 'Next'.

2. Click **Add New SIM Card**. The following window appears.



The 'Add SIM Cards' dialog box is shown. It contains a text input field for 'Package Serial Number' and a 'Validate' button. The text inside the dialog says: 'Please paste package serial number string into the box below.'

3. Enter appropriate **Serial Number** of SIM package and click **Validate**.
4. After successful validation of the serial number, click **Add**.

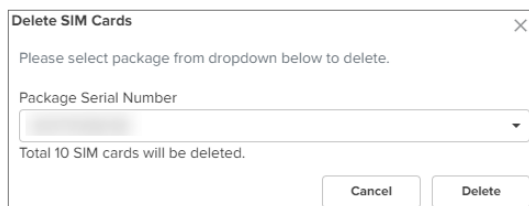


Note

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 is shown. It contains a dropdown menu for 'Package Serial Number' and a 'Delete' button. The text inside the dialog says: 'Please select package from dropdown below to delete.' Below the dropdown, it says: 'Total 10 SIM cards will be deleted.'



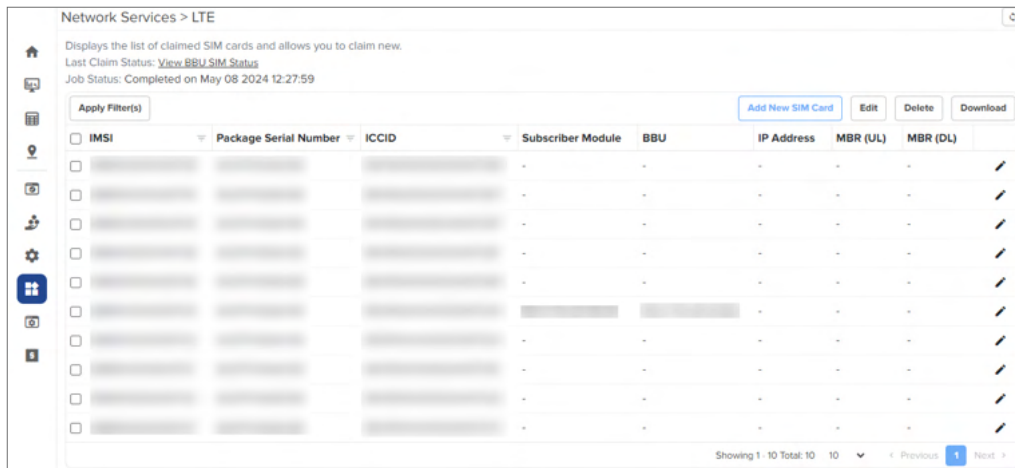
Note

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**.

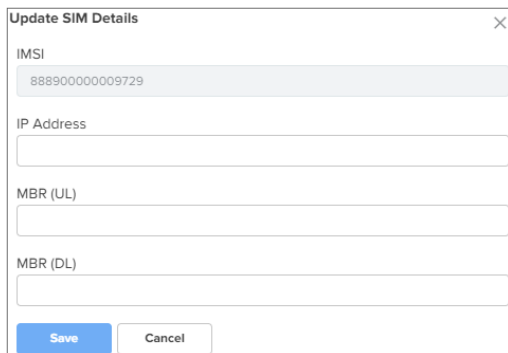


The screenshot shows the 'Network Services > LTE' interface. It includes a sidebar with navigation icons, a header with a home icon and a description: 'Displays the list of claimed SIM cards and allows you to claim new. Last Claim Status: View BBU SIM Status Job Status: Completed on May 08 2024 12:27:59'. Below the header is a table with columns: IMSI, Package Serial Number, ICCID, Subscriber Module, BBU, IP Address, MBR (UL), and MBR (DL). The table contains 10 rows of data. At the bottom right, it says 'Showing 1 - 10 Total: 10' and has pagination controls for 'Previous', '1', and 'Next'.

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 with a close button (X) in the top right corner. It contains the following fields: IMSI (with the value 888900000009729), IP Address, MBR (UL), and MBR (DL). At the bottom, there are 'Save' and 'Cancel' buttons.

Update SIM Details X

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 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 10 < 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 613](#).

Figure 613 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)
Centos-8	10.110.221.34	Online (7h 36m ago)	Base Infrastructure	1.0.0-b39	9h 57m ago	Success (< 1m ago)

Showing 1 - 2 Total: 2 10 < 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](#)

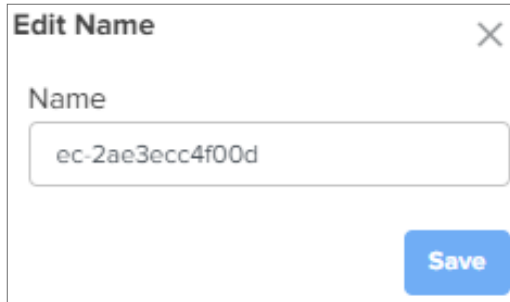
Topology Sync

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.



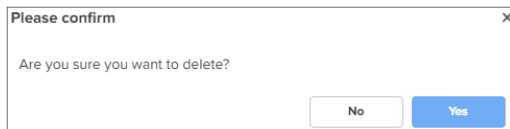
The 'Edit Name' dialog box has a title bar with 'Edit Name' and a close button (X). Inside, there is a label 'Name' above a text input field containing the text 'ec-2ae3ecc4f00d'. At the bottom right of the dialog is a blue button labeled 'Save'.

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'.

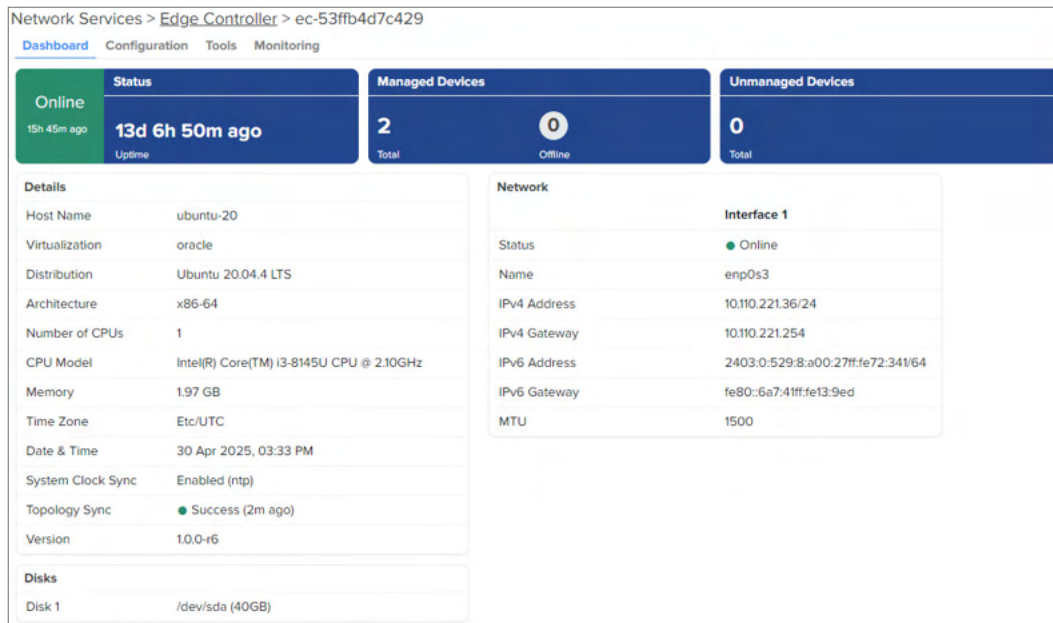
2. Click **Yes**.

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 614](#).

Figure 614 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 161](#).

Figure 615 Edge Controller and PTP 820/850 devices status

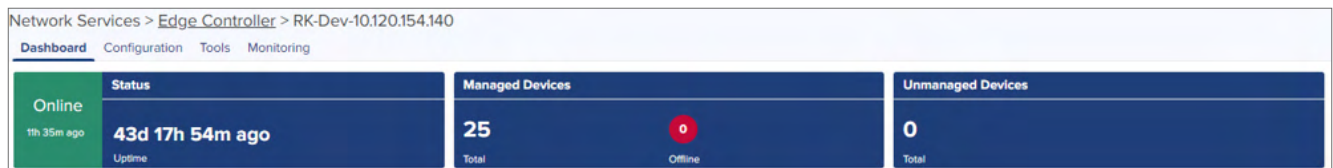


Table 161 Fields in the Edge Controller dashboard

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.
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.

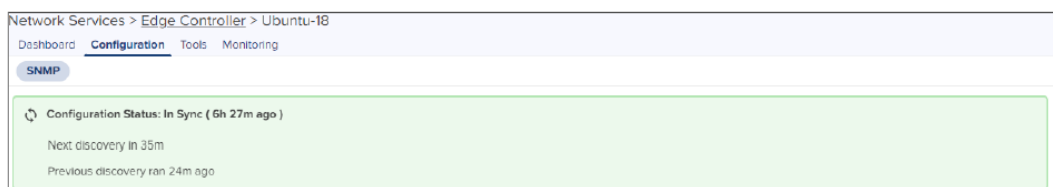
Table 161 Fields in the Edge Controller dashboard

Field	Description
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 616](#).

Figure 616 Configuration Status



Rules

To add a new rule, perform the following steps:

1. Click **Add New**.



The **Add New Network Discovery Rule** window appears.

Add New Network Discovery Rule

Subnet*

Allowed IPv4 subnets are /24 or smaller. Eg. 10.0.0.0/25

Network Address Range

Port

161

Versions

☒ v2c ☐ v3

Read-Write Community

Show

Add

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.

Versions

☐ v2c ☒ v3

Username*

Context Name

Authentication Protocol

☒ None ☐ SHA ☐ MD5

Authentication Password*

Show

Privacy Protocol

☒ None ☐ AES 128 ☐ DES

Privacy Password*

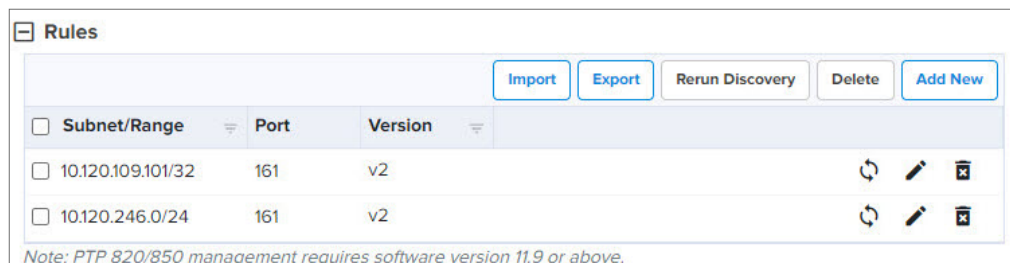
Show

Add

- 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**.

Subnet/Range	Port	Version
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				
1	10.120.109.101/32	161	2	private										
2	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**.



Blacklist

IP Address

No Data Available

Note: Devices with matching IP will be unclaimed if already managed.

Add Blacklist IP Address window appears.



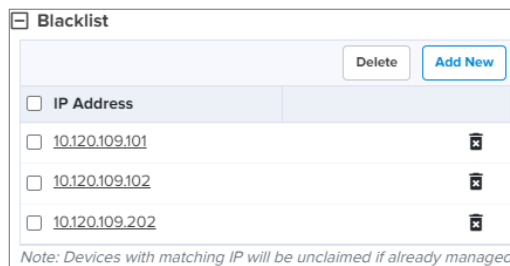
Add Blacklist IP Address

IP Address*

Save

2. Type **IP Address**.
3. Click **Save**.

Blacklisted IP Addresses are displayed in the table.



Blacklist

IP Address

10.120.109.101

10.120.109.102

10.120.109.202

Note: Devices with matching IP will be unclaimed if already managed.

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 dropdown.
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

4. 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

[Show Logs](#)

Output

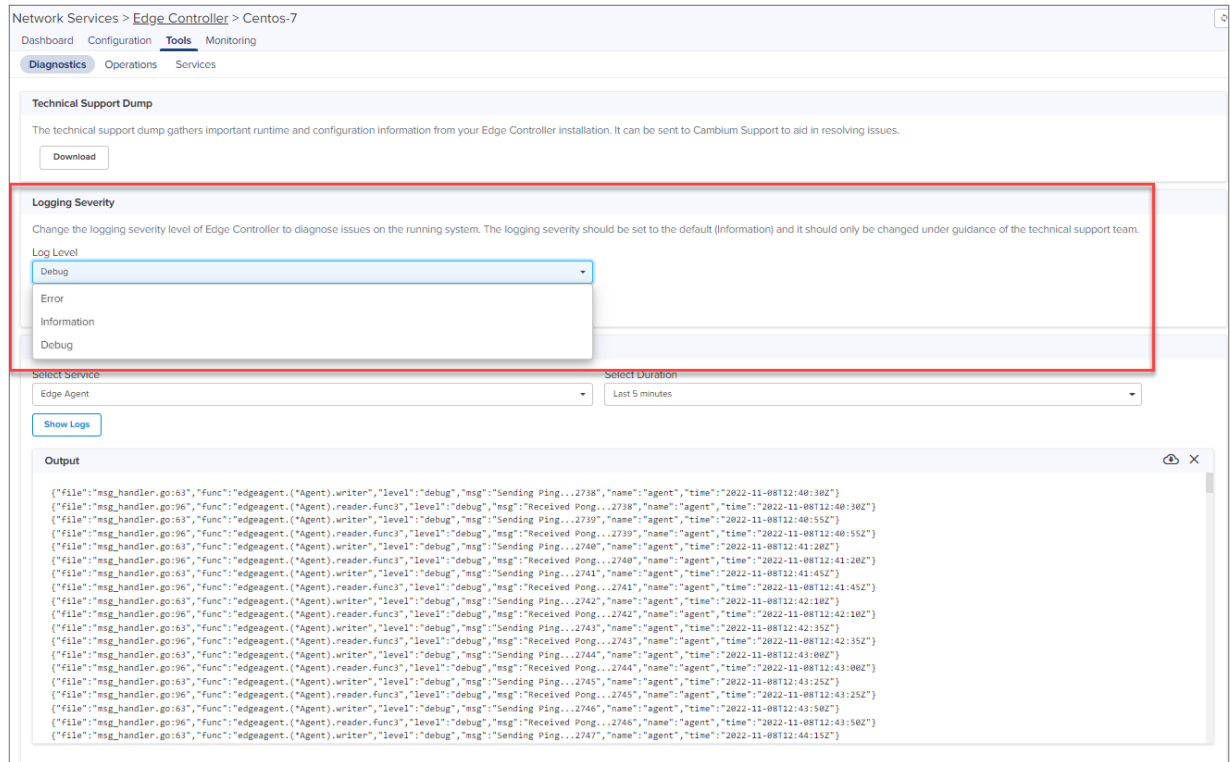
```
{
  "file": "msg_handler.go:63",
  "func": "edgeagent.(*Agent).writer",
  "level": "debug",
  "msg": "Sending Ping...4743",
  "name": "agent",
  "time": "2024-05-09T20:46:28Z"
}
{
  "file": "msg_handler.go:96",
  "func": "edgeagent.(*Agent).reader.func3",
  "level": "debug",
  "msg": "Received Pong...4743",
  "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** dropdown.
 - 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.

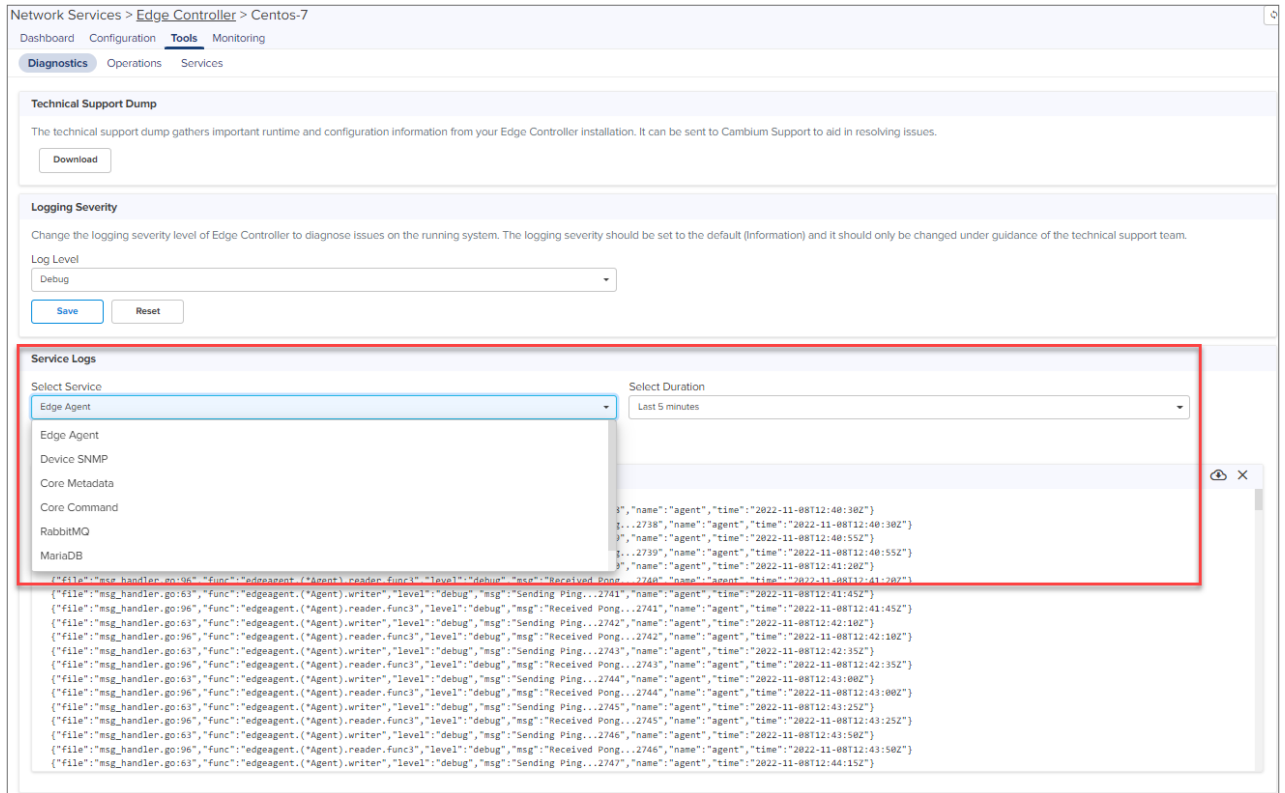
1. Select **Service** and **Duration** from the dropdown.

The following list of service and duration (5 minutes, 15 minutes, 30 minutes and last 1 hour) are available from the dropdown:

- Edge Agent
- Device SNMP
- Core Metadata
- Core Command
- RabbitMQ
- MariaDB
- SFTP

2. Click **Show Logs**.

The output for the selected criteria appears as shown:

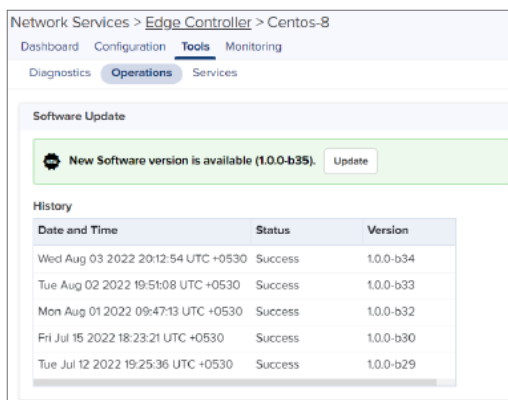


3. Click download (📄) icon to download the generated output.
4. Click clear (✕) icon to clear the output.

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. 1. Navigate to **Tools > Operations**.
2. 2. Click **Check for new software update**, checks for any new available software update.



Services

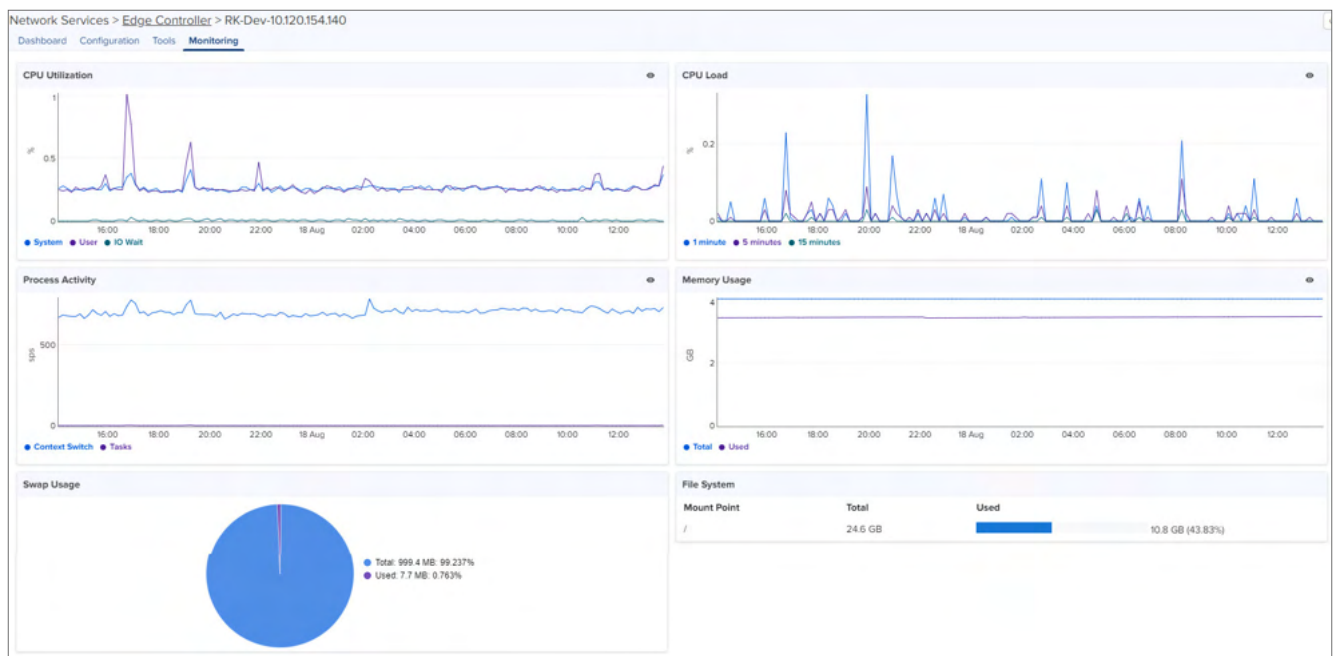
In **Services** page you can view the services running in the Edge Controller.

Figure 617 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.



Installation Summary

Cambium Networks Installer 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 Cambium Networks Installer during the installation process.



Note

- Installation Summary is a cnMaestro X feature.
- Installation summary of PMP SM is available for users in cnMaestro Cloud and OnPremises from 3.1.0 release.
- 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 Installation Summary.

To view the installation summary:

1. Navigate to **Network Services > Installation Summary**.

The **Installation Summary** page appears.

2. You can **Search** Installation Summary details by using **MAC Address**, **Name at Installation**, **Date and Time**, **Added By**, and **Comments**.

MAC Address	Name at Installation	Date and Time	Installation Duration	Added By	Comments	State
	cbrs-sm-185-179	30 Oct 2023, 03:36 PM	0h 4m		pmp cnarcher installation summary	Deleted

Table 162 *Fields in 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.

- Click **View Details**  icon to view detailed Installation Summary.

Installation Summary : cbrs-sm -185-179 on 30 Oct 2023, 03:36 PM

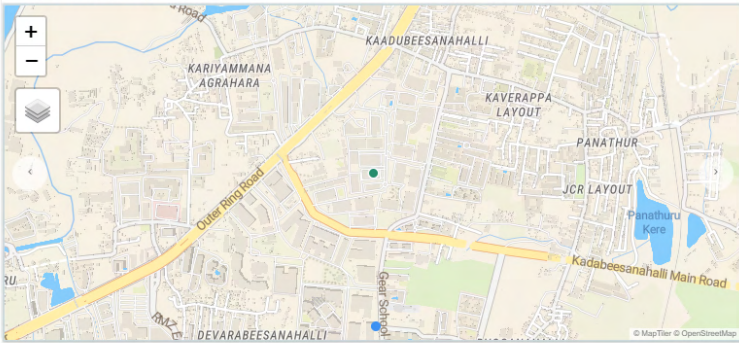
Summary

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 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 163 Summary fields in Installation Summary

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.

1067 | Installation Summary

Cambium cnMaestro Cloud | User Guide

Configuration

Table 164 Configuration fields in Installation Summary

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 165 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 166 Fields in AP Scan Result

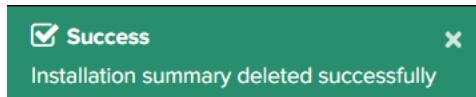
Field	Description
AP MAC	MAC address of the AP.
AP Bandwidth	Bandwidth of the AP.
AP Frequency	Frequency of the AP.
Registered	Details of the registered SM.

1. Click the delete (🗑️) icon to delete single or multiple entries from the **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

The Cambium Networks Installer mobile application uploads the installation summary to cnMaestro when Internet connection is available on the user's mobile device.

This feature is supported only on Android devices.

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](#)

ID	Name	Status	Type	Sector Count	Start Time	End Time	
30	sa	Scheduled	Daily	3	10 May 2024, 12:12 PM	-	
29	dw	Completed	Now	1	06 May 2024, 12:50 P...	06 May 2024, 12:57 PM	
28	DP	Completed	Now	3	06 May 2024, 12:22 P...	06 May 2024, 12:31 PM	
26	cfew	Completed	Now	2	06 May 2024, 11:54 AM	06 May 2024, 12:08 P...	
25	safari	Scheduled	Daily	1	10 May 2024, 03:17 PM	-	
24	check sa	Completed	Now	7	12 Apr 2024, 10:24 AM	12 Apr 2024, 10:38 AM	
23	12sa	Completed	Daily	9	09 Apr 2024, 03:14 PM	10 Apr 2024, 04:55 PM	
22	SA	Completed	Now	8	27 Mar 2024, 12:12 PM	27 Mar 2024, 12:26 PM	
21	alarm	Completed	Now	5	19 Mar 2024, 10:48 AM	19 Mar 2024, 11:02 AM	
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 167 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.

- Click **View Result** icon on top right corner to view the detailed Spectrum Analyzer summary.

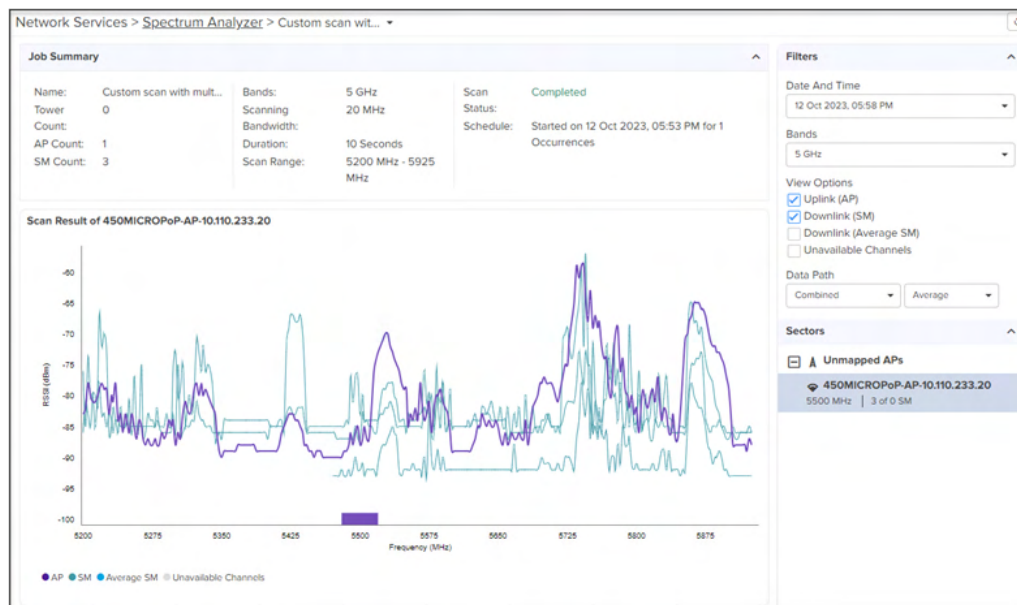


Table 168 *Job Summary parameters*

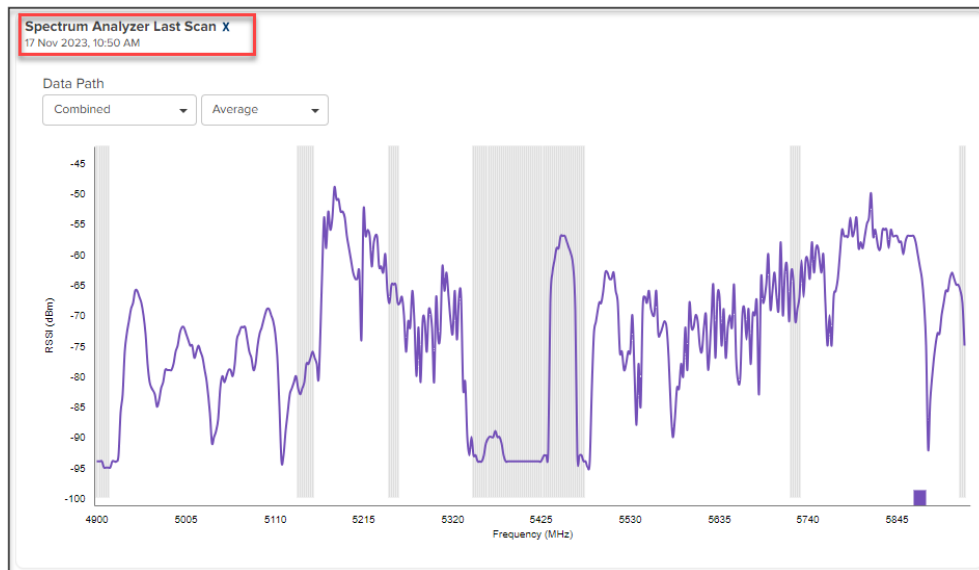
Field	Description
Name	The user-assigned name for the analysis job.
Tower Count	The number of towers included in the analysis.
AP Count	The number of APs in the analysis.
SM Count	The number of SMs in the analysis.
Bands	The frequency bands under analysis.
Scanning Bandwidth	The width of the frequency 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 169 *Filters parameters*

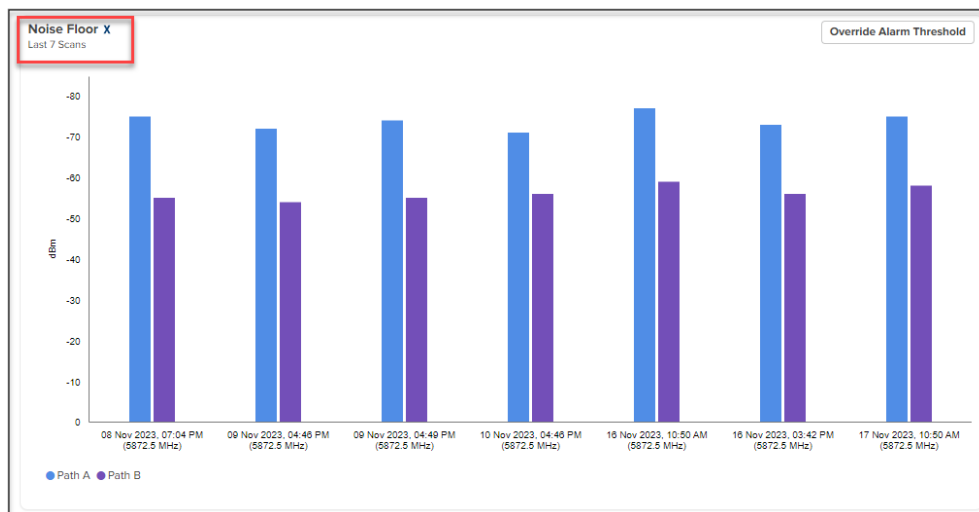
Field	Description
Date and Time	The specific date and time when the spectrum analysis is conducted.
Bands	The frequency bands included in the analysis.
View Options	<p>The viewing options for analyzing the spectrum.</p> <ul style="list-style-type: none"> • Uplink (AP) • Downlink (SM) • Downlink (Average 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**.



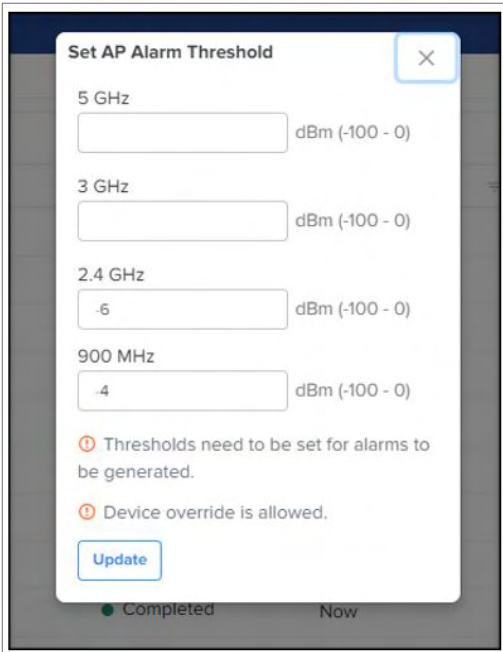
- b. The dashboard automatically generates the appropriate graph for AP and SM based on the device type.
- c. The default data path for displayed graphs is **Combined**, and users can customize it to their preferences.
- d. The dashboard displays **Noise Floor**, which provides noise floor information 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)

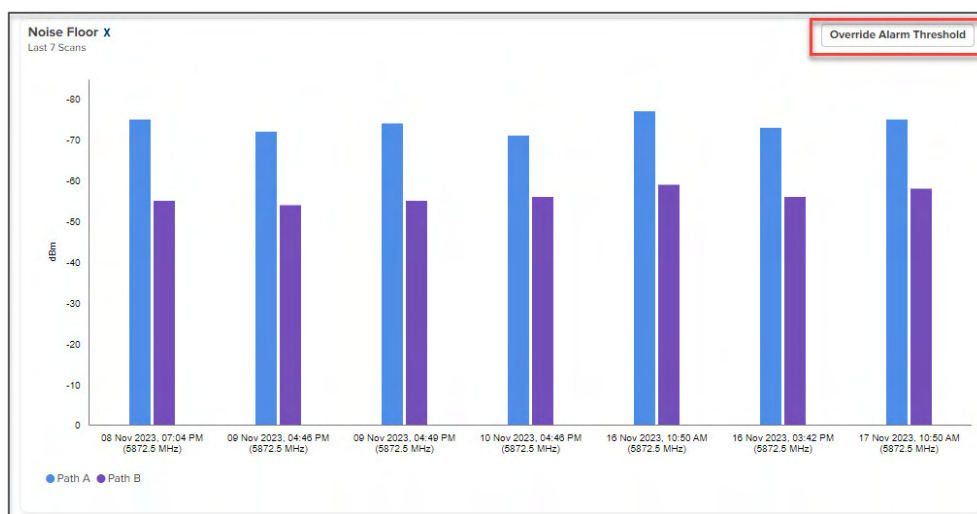
ⓘ Thresholds need to be set for alarms to be generated.

ⓘ Device override is allowed.

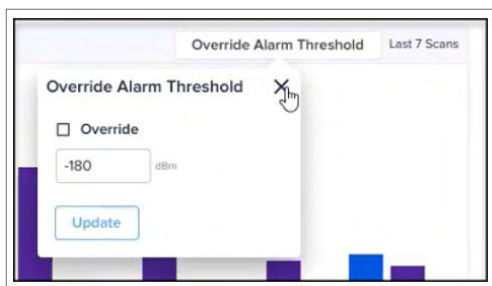
[Update](#)

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 X** page.
2. Click **Add New**.

Add Spectrum Scan

Name*

Select Sector

Spectrum Analysis is supported by devices running software version 22.1.0 and above.

AP Name	Network	Tower	Band	Frequency	Channel Width
<input type="checkbox"/> CBRS-187	default	@CBRS_Tower_DND	3 GHz	3612.5 MHz	15 MHz
<input type="checkbox"/> PMP 450i RVI	JP-Wi-Fi-SIT		5 GHz	5240 MHz	20 MHz
<input type="checkbox"/> PMP 450i-BBC827	_Network	New_PMP_	5 GHz	5735 MHz	20 MHz

0 AP Selected Showing 1 - 3 Total: 3 10 < Previous 1 Next >

Schedule

☒ Now
 ☐ Daily
 ☐ Weekly
 ☐ Monthly (30 days)

Scan Range

Custom Scan

Min Frequency

0

Max Frequency

0

(MHz)

Scanning Bandwidth*

Not Applicable for PMP 450m AP. AP will scan using its current configuration bandwidth

Duration*

10

Seconds (10 - 1000)


Cancel

Add

Table 170 *Add Spectrum Scan parameters*

Field	Description
Name	Job name to distinguish the analysis job within the Spectrum Analyzer.
Schedule	Scheduling options, including: <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 dropdown with two options: <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.

Table 170 *Add Spectrum Scan parameters*

Field	Description
Scanning Bandwidth	<div>The specific scanning bandwidth from the available options to adjust the spectrum analysis.</div> <div><div>Note Scanning Bandwidth is not applicable for PMP 450m AP.</div></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](#)
- [Audit Logs](#)
- [Settings](#)
- [Updating Company Information](#)

Users

This chapter provides the following details:

- [Managing Users](#)
- [Assigning roles for IdP-based domain 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 618 Adding Users

Administration > Users

[Manage Users](#) [IdP Role-Mappings X](#) [Session Management X](#)

Invite others to manage this account. Up to 200 users can manage an account. [Learn more](#)

[Apply Filter\(s\)](#) [Add User](#) [Allowed Domains](#) [Invite Cambium Support](#) [Delete](#)

<input type="checkbox"/> Username	<input type="checkbox"/> Invited Email	<input type="checkbox"/> Role	<input type="checkbox"/> Email	<input type="checkbox"/> Status	
<input type="checkbox"/> [redacted]	[redacted]	Super Administrator	[redacted]	Active	Edit Delete
<input type="checkbox"/> -	[redacted]	Administrator	-	Invited	Edit Delete
<input type="checkbox"/> -	[redacted]	Super Administrator	-	Invited	Edit Delete
<input type="checkbox"/> -	[redacted]	Super Administrator	-	Invited	Edit Delete
<input type="checkbox"/> -	[redacted]	Super Administrator	-	Invited	Edit Delete
<input type="checkbox"/> -	[redacted]	Super Administrator	-	Invited	Edit Delete
<input type="checkbox"/> -	[redacted]	Super Administrator	-	Invited	Edit Delete
<input type="checkbox"/> -	[redacted]	Super Administrator	-	Invited	Edit Delete
<input type="checkbox"/> -	[redacted]	Monitor	-	Invited	Edit Delete
<input type="checkbox"/> [redacted]	[redacted]	Super Administrator	[redacted]	Active	Edit Delete
<input type="checkbox"/> -	[redacted]	Super Administrator	-	Invited	Edit Delete

Showing 1 - 10 Total: 371 10 < Previous 1 2 3 4 5 ... 38 Next >

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 171 *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 171 *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
Installation Summary	<p>View installation summary of PMP and ePMP SMs, Enterprise Wi-Fi APs, and cnMatrix devices installed using the Cambium Networks Installer 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 171 *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
LTE	<p>Manage cnRanger LTE devices.</p>

Table 171 *Role-Mappings*

Feature	Description
	<ul style="list-style-type: none"> • Super Administrator - All • Administrator - All • Operator - View and Edit SIM credentials only • Monitor - None • CPI - None
Managed Service Provider (MSP)	<p>MSP operations such as modification of branded service, managed account and user invitations.</p> <ul style="list-style-type: none"> • Super Administrator - All • Administrator - View • Operator - None • Monitor – None • CPI - None <p>Note: Operator/Monitor users are not permitted to move devices across managed accounts.</p>
Monitoring	<p>Display of monitoring data at all levels.</p> <ul style="list-style-type: none"> • Super Administrator - All • Administrator - All • Operator - All • Monitor - View • CPI - View
Notifications	<p>Alarms and Events management.</p> <ul style="list-style-type: none"> • Super Administrator - All • Administrator - All • Operator - All • Monitor - View • CPI - View
Onboarding	<p>Device approval, modifying individual device configuration, and performing software update.</p> <ul style="list-style-type: none"> • Super Administrator - All • Administrator - All • Operator - All • Monitor - None • CPI - All
Reporting	<p>Report generation.</p> <ul style="list-style-type: none"> • Super Administrator - All

Table 171 *Role-Mappings*

Feature	Description
	<ul style="list-style-type: none"> • Administrator - All • Operator - All • Monitor - All • CPI - All
Session Management	<p>Capability to view and logout other users sessions.</p> <ul style="list-style-type: none"> • Super Administrator - All • Administrator - All • Operator - None • Monitor - None • CPI - None
Software Upgrade	<p>Upgrade the device with the latest software.</p> <ul style="list-style-type: none"> • Super Administrator - All • Administrator - All • Operator - All • Monitor - None • CPI - None
Spectrum Analyzer	<p>Analyze and monitor wireless spectrum for optimizing network performance on PMP devices.</p> <ul style="list-style-type: none"> • Super Administrator - All • Administrator - All • Operator - All • Monitor - None • CPI - None
User Management	<p>User management operations such as manage users and roles.</p> <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:



Note

You can invite multiple users simultaneously by entering their email IDs in the Email text box or Copy and paste the multiple email IDs as a comma-separated input.

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** dropdown 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.

Administration > Users

[Manage Users](#) [IdP Role-Mappings X](#) [Session Management X](#)

Invite others to manage this account. Up to 200 users can manage an account. [Learn more](#)

[Apply Filter\(s\)](#) [Add User](#) [Allowed Domains](#) [Invite Cambium Support](#) [Delete](#)

<input type="checkbox"/>	Username	Invited Email	Role	Email	Status	
<input type="checkbox"/>			Super Administrator		Active	✎ 🗑
<input type="checkbox"/>	-		Administrator	-	Invited	✎ 🗑
<input type="checkbox"/>	-		Super Administrator	-	Invited	✎ 🗑
<input type="checkbox"/>	-		Super Administrator	-	Invited	✎ 🗑
<input type="checkbox"/>	-		Super Administrator	-	Invited	✎ 🗑
<input type="checkbox"/>	-		Super Administrator	-	Invited	✎ 🗑
<input type="checkbox"/>	-		Super Administrator	-	Invited	✎ 🗑
<input type="checkbox"/>	-		Monitor	-	Invited	✎ 🗑
<input type="checkbox"/>			Super Administrator		Active	✎ 🗑
<input type="checkbox"/>	-		Super Administrator	-	Invited	✎ 🗑

Showing 1 - 10 Total: 371 10 [Previous](#) [1](#) [2](#) [3](#) [4](#) [5](#) [...](#) [38](#) [Next](#)



Note

You can invite multiple users simultaneously by entering their email IDs in the Email text box or Copy and paste the multiple email IDs as a comma-separated input.

- To add a new domain (for example, a gmail ID), click **Add User**.

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*

user123@icloud.com

✕

Type and press Enter

Role

Monitor

Following are the list of new domains:

☐ Allow users in "icloud.com" domain.

[Learn more](#)

Cancel

Send

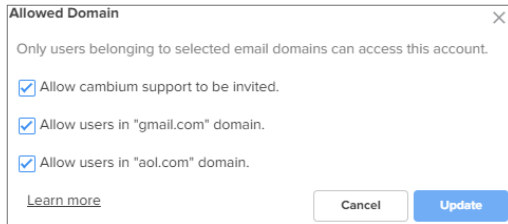
- Select the **Allow users in "gmail.com" domain** checkbox (the domain name varies based on the email ID you add).

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 "gmailail.com" domain** checkbox is available only when you are adding a new domain.

- 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.



5. Clear the required domain checkbox to blacklist that specific domain.
6. 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 checkbox on the **Allowed Domain** window.

Assigning roles for IdP-based domain users

A group mapping is a link between cnMaestro roles and IdP roles or groups. When signing in to cnMaestro, roles can be automatically assigned based on roles in the IdP. This can be used to maintain roles in Active Directory or a similar central identity provider.

Create a group mapping for each set of roles that you want to assign to a user based on the user's IdP group memberships. Your organization might have groups with different sets of permissions based on teams, Cloud environments, or read/write/admin access. You can create a group mapping for each set of permissions. For example, you might create a group mapping that assigns the roles `DeveloperWrite` and `ResourceOwner` to a user who is a member of the data-science group in your IdP server.



Note

The IdP role mapping configuration is applicable only to cnMaestro X accounts.

To set up IdP role mapping, contact [Cambium Support](#) who will ask for some information and generate an IdP role mapping key.

With the IdP role mapping key, IdP groups or roles can be mapped to a role in cnMaestro for the IdP domain users. For example, with an Active Directory group called `app-cnmaestro-superadmin` mapped to the "Super Administrator" role in cnMaestro, members of this Active Directory group will be assigned the Super Administrator role automatically when logging in.

Advantages

The advantages of IdP-based domain user role configuration are:

- Authentication can be centralized and users can access multiple accounts with the same login.
- Security policies, such as password or authentication requirements, can be managed through a single policy.
- User experience improves as there is no need for multiple passwords and logins, making access seamless across all platforms.

Using the **Administration > Users > IdP Role-Mappings** UI page in cnMaestro, a new IdP role-mapping can be added and roles can be assigned to the IdP domain users.

Prerequisite tasks

Before adding IdP role-mappings and assigning roles in cnMaestro, make sure to complete the following prerequisite tasks:

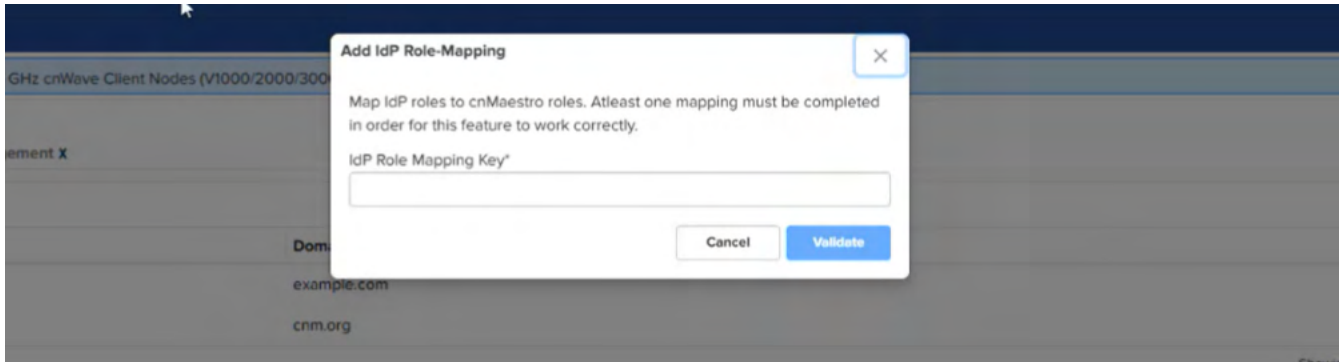
- An IdP must be registered by the [Cambium Support](#) team.
- The IdP must have the IdP Role Mapping Key, which is generated and provided by the Cambium Support team.

Assigning roles for IdP-based domain users

To add a new role-mapping and assign a role for the IdP-based domain users, complete the following steps:

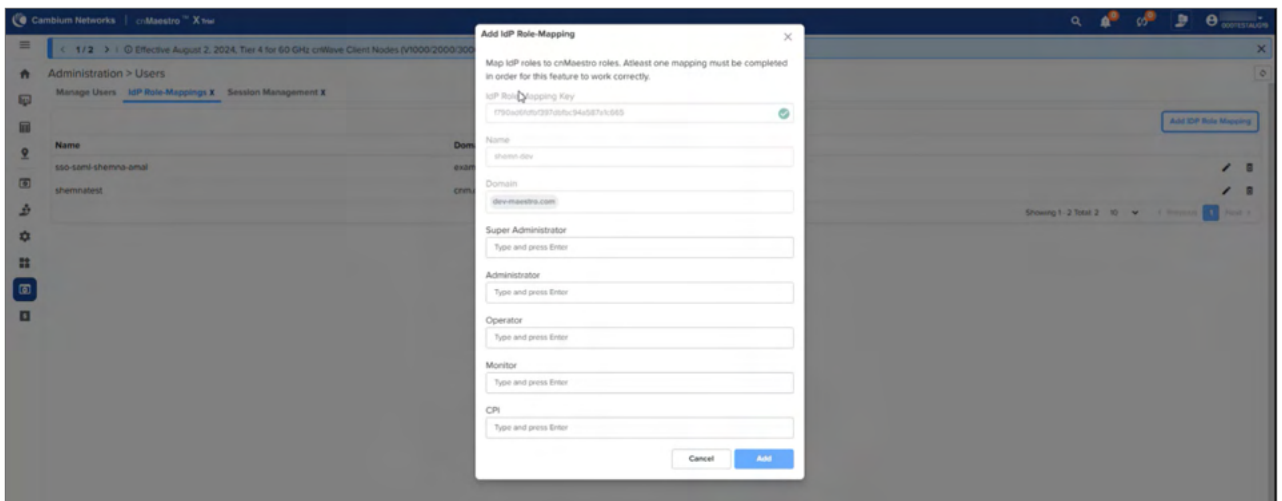
1. Navigate to **Administration > Users > IdP Role-Mappings**.
2. Click **Add IdP Role Mapping**.

The **Add IdP Role-Mapping** box appears.



3. In the **IdP Role Mapping Key** text box, enter the key provided by the [Cambium Support](#) team.
4. Click **Validate**.

On successful validation of the IdP, you can view the IdP details configured on the Support site. For example, IdP name and domain.



5. In the **Add IdP Role-Mapping** box, assign the required roles to the user groups.
6. Click **Add**.

When domain users log in to the cnMaestro UI, they can access multiple accounts with a single log-in.

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 roles can logout Operator and Monitor accounts.

Sessions

Displays the detailed information on the user sessions.

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](#)

Search

Managed Account: All Accounts

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	49.37155.5	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]
T...	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 10

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 an On-Premises customer accounts to Cloud is addressed by this feature. This allows the user to synchronize inventory and other configuration details between the On-Premises instances and the Cloud account.

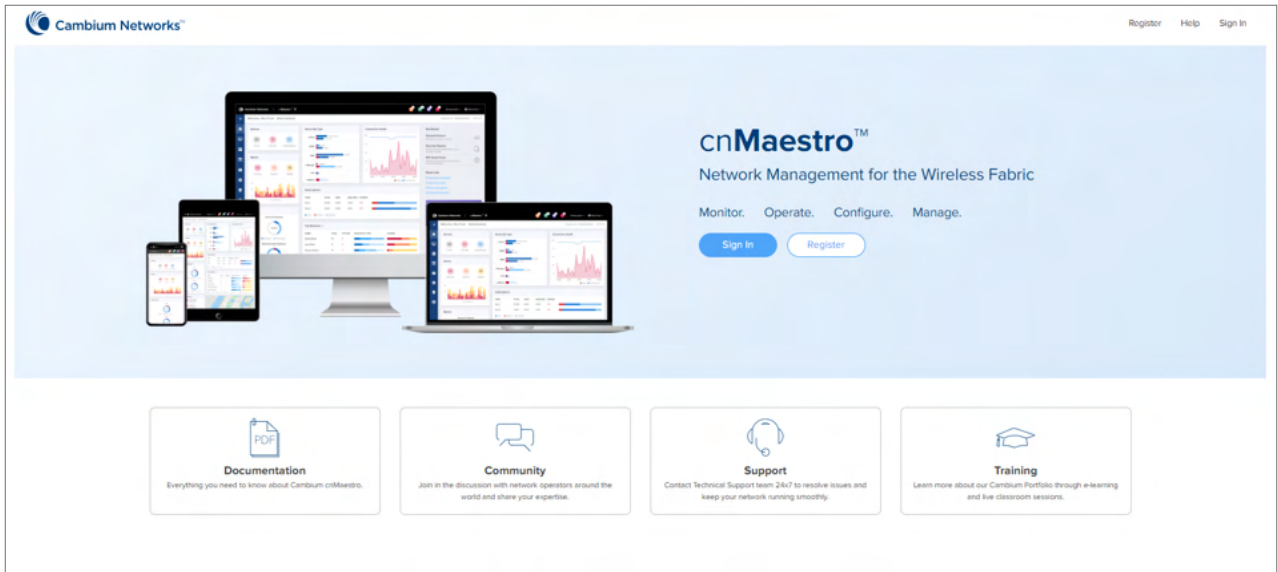
Manage Instances describes the following topics:

- [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:

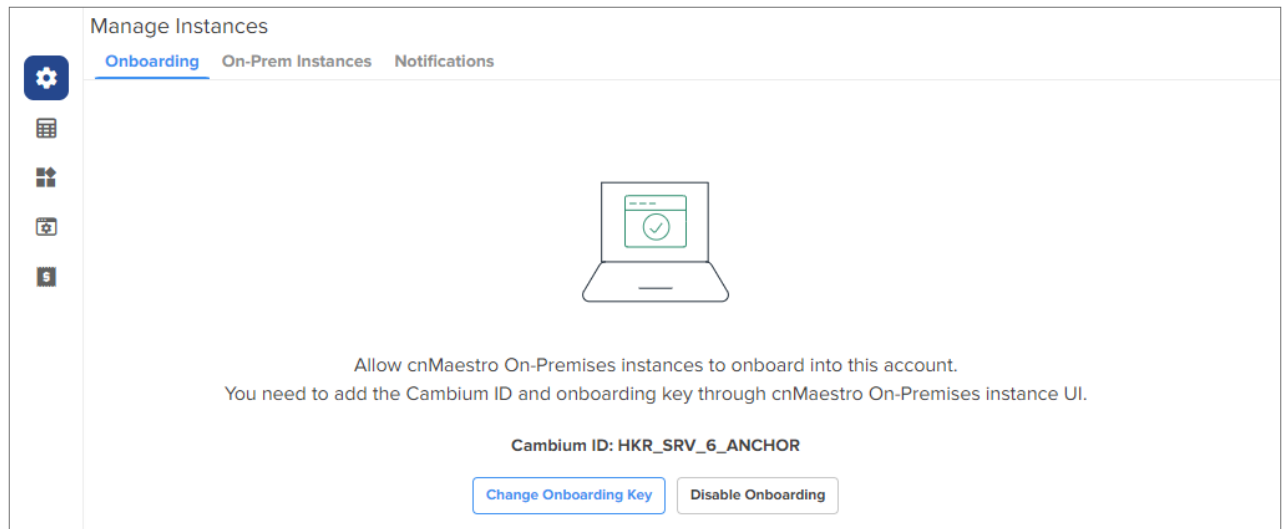
1. Log in to the cnMaestro UI, <https://cloud.cambiumnetworks.com>.



2. In **Account Type**, select **Anchor**.

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.



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.

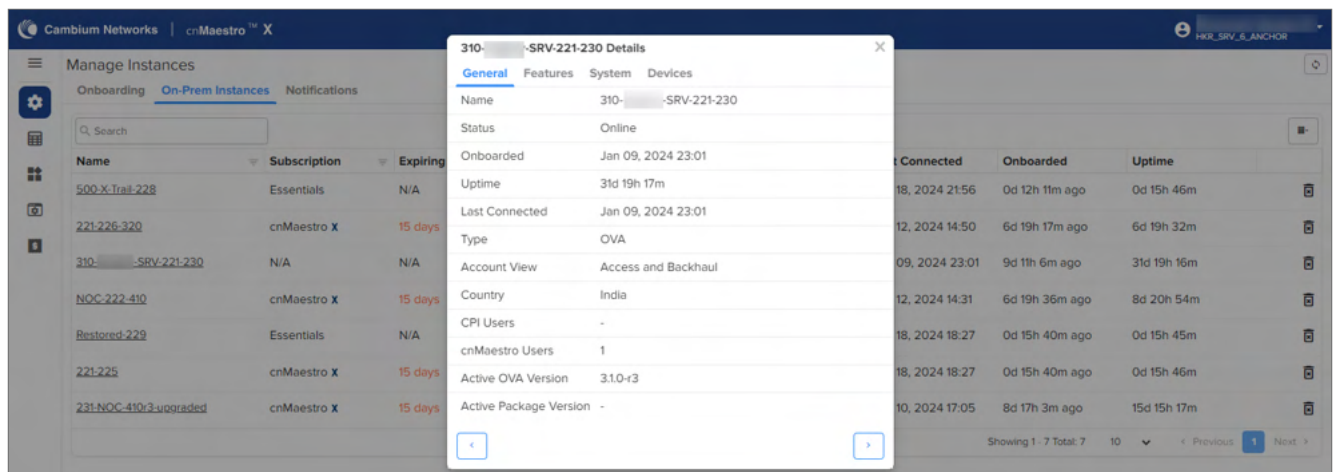
Manage Instances

Onboarding **On-Prem Instances** Notifications

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:



Notifications

Notification page displays the history of the most recent events notification of On-Premises instances with **Severity**, **Source**, **Name**, **Raised Time**, and **Message**.

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

Click View Details to view the Event Details as shown below:

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.

Device	MAC Address	Managed Account	Type	IPv4 Add...	IPv6 Address	Status	Serial Number	Description	Onboard Duration	Active S/W Version
PMP 450i RV		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:5bb1:8000:1	Online (2d 3h 30m)			0d 10h 34m	1.3.3
V5K DN 3040		MSP	60 GHz crWave V5000 DN	-	fd18:10f:5bb1:8003:1	Online (2d 3h 30m)			0d 10h 34m	1.3.3
PoP 300C		MSP	60 GHz crWave V5000 DN (PoP)	-	fd18:10f:5bb1:8002:1	Online (2d 3h 30m)			0d 10h 34m	1.3.3
V5K DN 3130		MSP	60 GHz crWave V5000 DN	-	fd18:10f:5bb1:8001:1	Online (2d 3h 30m)			0d 10h 34m	1.3.3
V3K d		MSP	60 GHz crWave V3000 DN	-	fd18:10f:5bb1:4:1	Online (2d 3h 30m)			0d 10h 34m	1.3.3
PoP V5K		MSP	60 GHz crWave V5000 DN (PoP)	-	fd18:10f:5bb1:1:1	Online (1d 2h 59m)			0d 10h 34m	1.3.3
CN V3K		MSP	60 GHz crWave V1000 CN	-	fd18:10f:5bb1:1:1	Online (1d 7h 36m)			0d 10h 34m	1.3.3
V5K CN 042		MSP	60 GHz crWave V1000 CN	-	fd18:10f:5bb1:2:1	Online (2d 3h 30m)			0d 10h 34m	1.3.3

Administration

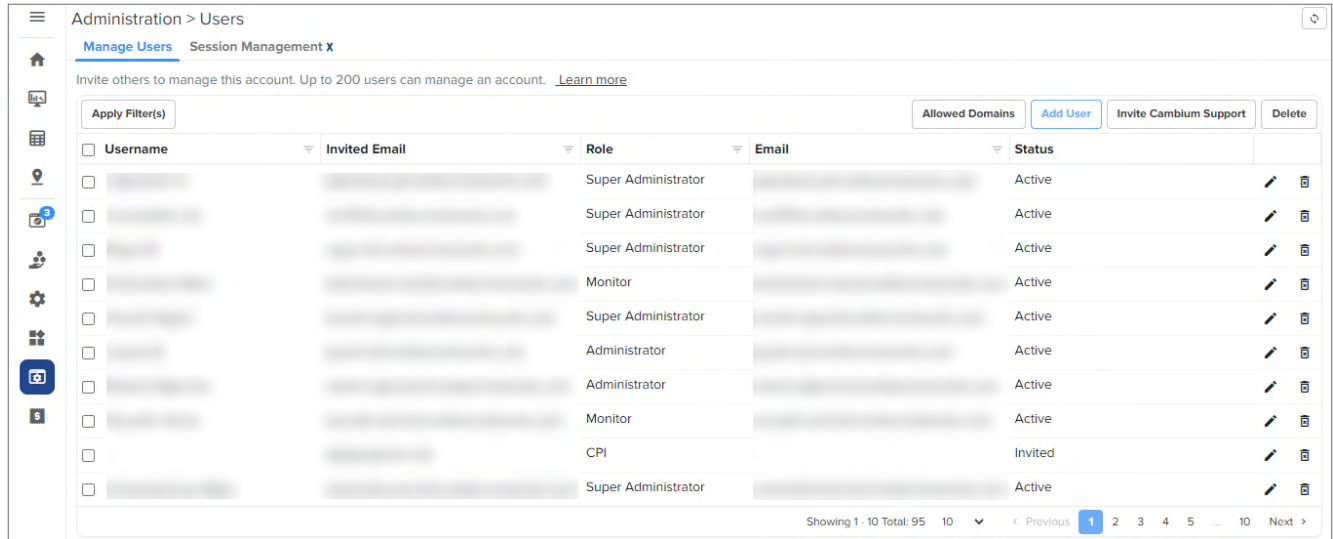
Administration provides the following details:

- 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 619 Adding Users



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:

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](#)

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](#).

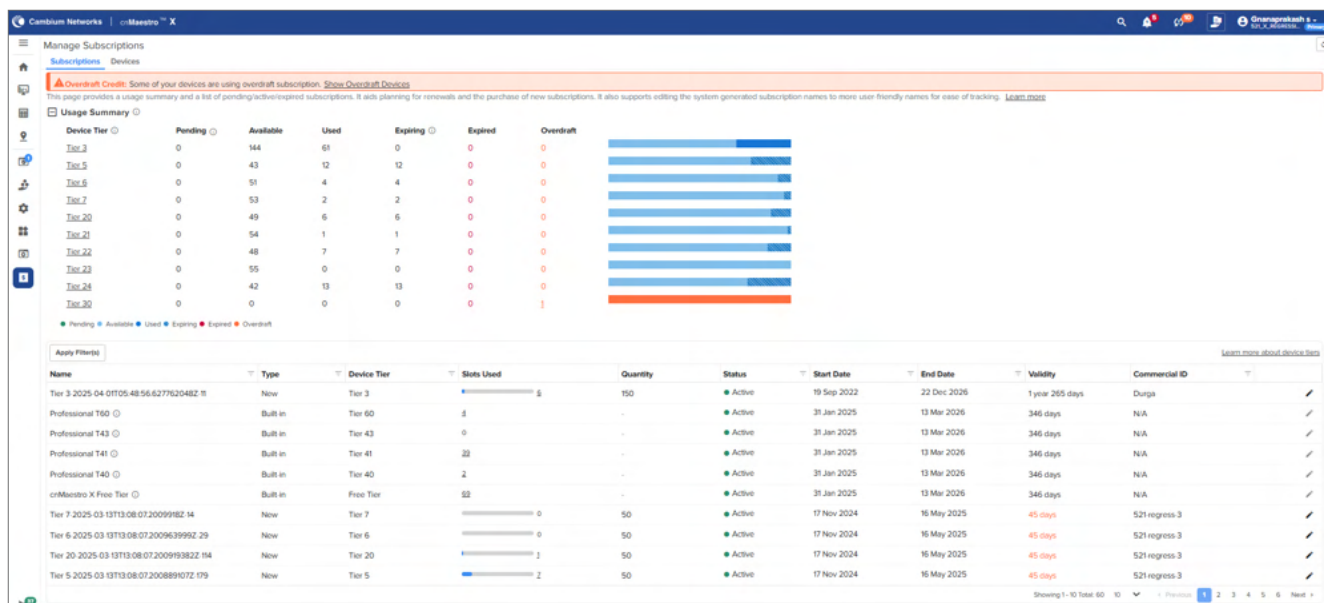
Manage Subscriptions

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.

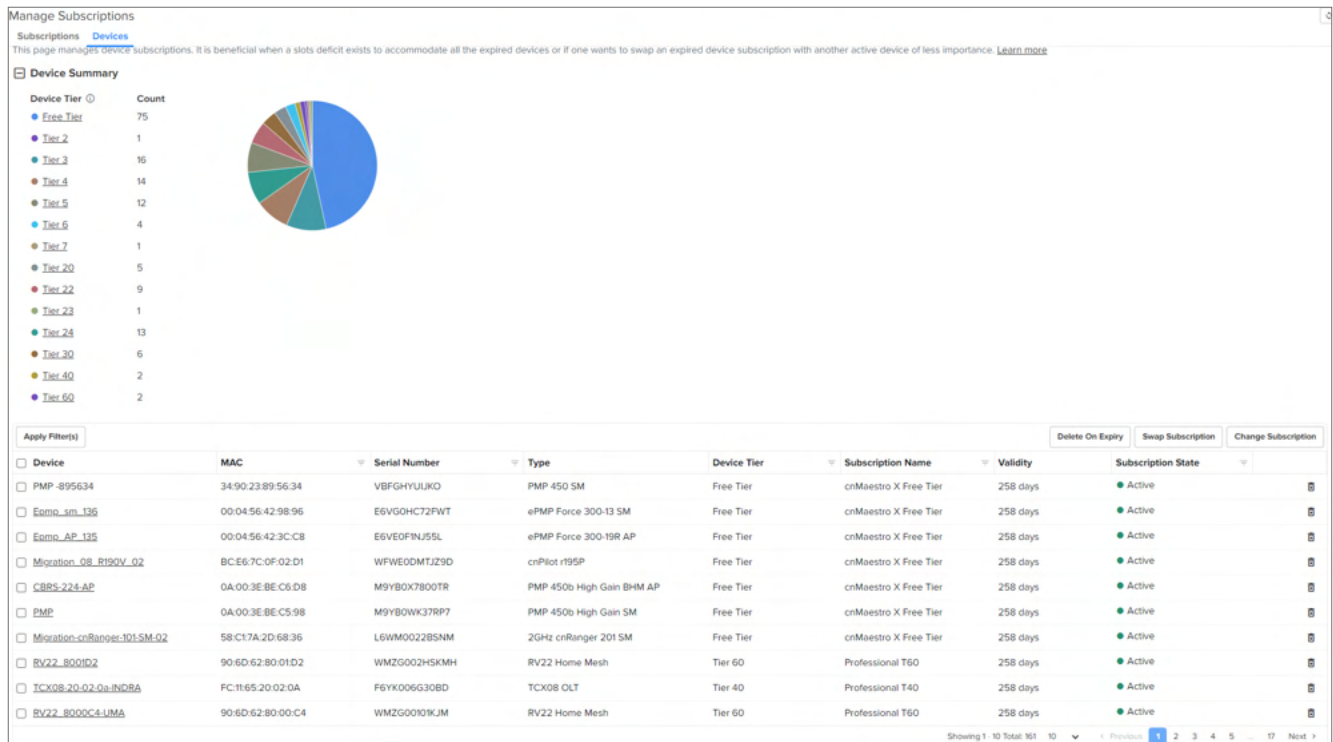
Edit window pops up as shown below.

The screenshot shows the 'Edit' window for a subscription. It has a title bar 'Edit' with a close button. The form contains a 'Name' field with the value 'Tier 1-2022-09-27T06:06:28Z-490' and a 'Description' field which is empty. At the bottom are 'Save' and 'Cancel' buttons.

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 620 Audit Logs

<

The following table describes the Audit Logs parameters and their descriptions.

Table 172 *Audit Log Parameters*

Parameter	Description
Action	Displays the action performed by the user (create, delete, download, etc).
Description	Textual description of the task.
Export	Export the audit log data in the CSV format. <div data-bbox="451 346 521 422"></div> <div data-bbox="586 338 654 367">Note</div> <div data-bbox="586 386 1529 455">The Export page as PDF option is deprecated from cnMaestro release 5.2.0 onwards. This option will be completely removed from the UI from release 5.3.0.</div> <div data-bbox="586 470 930 695"></div>
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 are supported for individual Audit Log entries. Each activity performed on the server is detailed in the following table.

Table 173 *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.
Device-Troubleshoot	Device troubleshooting actions performed from the respective device Tools page.
Downgrade	Downgrade a 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.

Table 173 Log Action Parameters

Parameter	Description
Reboot	Reboot a device.
Reset	To reset a device
Upgrade	Upgrade a device.
Upload	Upload a file on the server.
User-Domain-Whitelist	Details of user domain allow listing.
Company-Info-Update	Update company information.
XMSC-Migration	Information about device migration from XMS to cnMaestro.

Audit Modules

Auditing activity is mapped to individual modules within cnMaestro. A breakdown of the available modules is listed below.

Module	Types	Description
ACL	Provisioning	Adding, editing, and removing the ACL entries.
Administrator	Provisioning Operations Security	User Management: Login, Users, Roles, Email.
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 Cloud and On-Premises instances.
Configuration	Provisioning Operations	Details of configuration actions.
Data-Tunnel	Provisioning	Data Tunneling.
Device	Provisioning Operations	Device management.
Email-Notifications	Operations	Add or edit email notifications.
Guest-Portal	Provisioning	Guest portal.
Infrastructure	Provisioning	Site, Network, Tower Management.
Jobs	Provisioning Operations	Jobs infrastructure.
License	Licensing	Update license details.
MarketApps	Operations	MarketApps configuration details.
MSP	Operations	Operations covering Managed Services and Managed Account.
Onboard	Provisioning Operations	Onboarding Queue.

Module	Types	Description
Profile	Provisioning	Create or update a profile.
Report	Provisioning Operations	Data Reports.
SIM	Provisioning	SIM claim and delete.
Subscription	Operations	Subscription details.
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 621 *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	PMP SM Offline, cnPilot Home Offline, ePMP ...
	json	Minor	Active	@MSP	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 ...
	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 622 *Adding Subscribers*

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	PMP SM Offline, cnPilot Home Offline, ePMP ...
	json	Minor	Active	@MSP	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 ...
	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 >

2. Click **Add Recipient**.

The following window is displayed:

Add Email Subscriber

☒ Active

Severity

Major

All alarms of chosen severity or greater will be sent.

Email

Enter Email ID

Content Type

☒ HTML ☐ JSON

Managed Account

All Accounts

Ignore Notification

☒ cnPilot Home Offline

☒ ePMP SM Offline

☒ PMP SM Offline

Cancel

Add

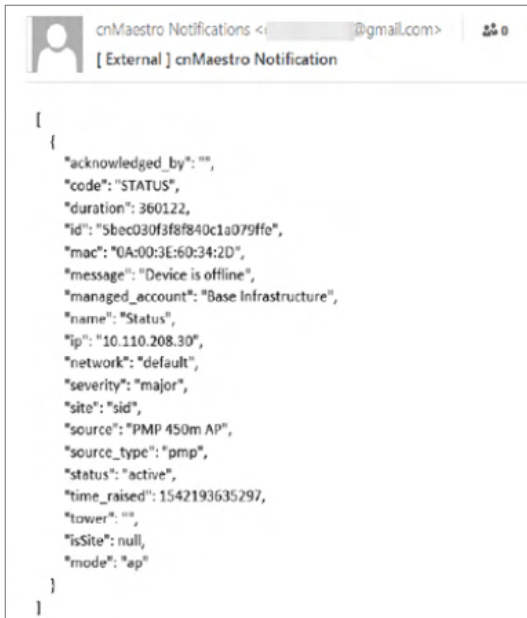
3. Enter the Email ID of the subscriber in the **Email** textbox.
4. Select the severity level from the **Severity** list.
5. Select the Managed Account type from the **Managed Account** list.
6. Choose **HTML** or **JSON** radio button for the **Content Type**.
7. Select the appropriate option (s) for **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

JSON Email Example



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 623 *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)	4.2.31-r9	<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

Updating Company Information



Note

Company information is applicable only on cnMaestro Cloud and Anchor Accounts from release version 5.2.0 and later.

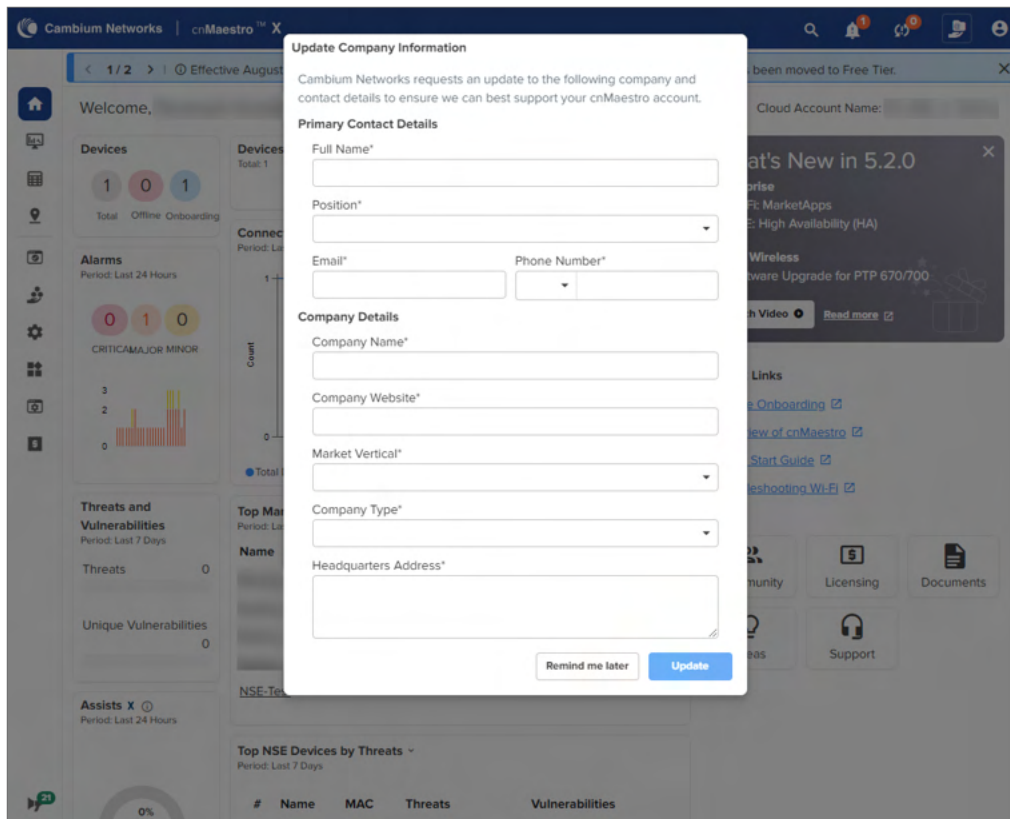
Users must provide certain personal and company contact details so that Cambium can provide better support for their cnMaestro accounts. Users must provide the following details in cnMaestro:

- Primary contact details, such as user's name, user's email ID, and their role or the designation in the company to which the cnMaestro account belongs.
- Company details, such as company name, address, website URL, company type, and market vertical.

From cnMaestro release 5.2.0, the **Company Information** page appears in the following instances:

- **Logging into cnMaestro 5.2.0 for the first time**—When the users log in to their existing cnMaestro accounts for the first time after the 5.2.0 upgrade, the **Update Company Information** pop-up window is displayed.

Figure 624 Update Company Information window



For information on the parameters on this screen, see [Table 174](#).

If you click **Remind me later**, you can still update the information by one of the following ways:

- Navigate to the **Administration > Company Information** page directly and update the required information. See [Updating information through the Company Information page](#).

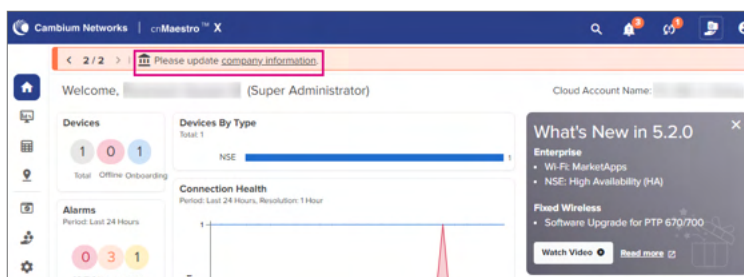
OR

- Click the **update information** link in the banner.



Note

- The banner remains until you complete updating the company information.
- cnMaestro displays the pop-up window again when either the session ends or when the user logs out and logs back into the account.



- Creating a new Cloud account—When creating a new cnMaestro Cloud account.

Figure 625 *Creating a new Cloud account*

The screenshot shows a web form titled "Create a New Cloud Account". It includes a header with the Cambium Networks logo and a sub-header "Create a New Cloud Account". Below this, there is a "Company ID" field with a dropdown menu. A "Next" button is visible. The form also contains sections for "Primary Contact Details" and "Company Details", each with several input fields and a "Next" button at the bottom.

- As a standalone page that users can access through the **Administration > Company Information** page.

Figure 626 *Administration > Company Information page*

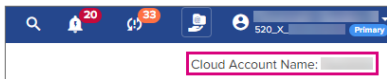
The screenshot displays the "Administration > Company Information" page. At the top, a message states: "Cambium Networks requests an update to the following company and contact details to ensure we can best support your cnMaestro account." Below this, the "Primary Contact Details" section includes fields for "Full Name*" (containing "1211234432"), "Position*" (a dropdown menu with "Business Analyst" selected), "Email*" (containing "test@gmail.co"), and "Phone Number*" (a dropdown menu with "AF (+93)" selected and a text field with "123456"). The "Company Details" section includes fields for "Company Name*" (containing "Test1234"), "Company Website*" (containing "www.testw"), "Market Vertical*" (a dropdown menu with "Federal Civilian" selected), "Company Type*" (a dropdown menu with "Distributor" selected), and "Headquarters Address*" (containing "test"). A blue "Update" button is located at the bottom of the form.

Updating information through the Company Information page

To update company information through the **Company Information** page, complete the following steps:

1. Navigate to **Administration > Company Information** page.
2. Enter the details described in the following table:

Table 174 *Company Information details*

Parameter	Description
Primary Contact Details	
Full Name	Name of the user in the cnMaestro account.
Position	Role or the designation of the user in the company. Select from the dropdown list.
Email	Email ID of the user.
Phone Number	Phone number of the user. Select the country code from the dropdown list and provide a valid phone number.
Company Details	
Company Name	Name of the company. This name will appear as the Cloud Account Name in the cnMaestro home page. 
Company Website	URL of the company website.
Market Vertical	Type of market or industry the company caters to. For example, Government, Defense, Education. Select from the dropdown list.
Company Type	Nature of work that the company does. For example, Defense, Manufacturer, Distributor. Select from the dropdown list.
Headquarters Address	Address of the company headquarters.

3. Click **Update**.



Note

After updating the information, cnMaestro displays the **Update Company Information** pop-up window and the banner again after six months.

Appendix

This section includes the following topics:

- [Guest Access](#)
- [Network Port Requirements](#)
- [XMS-Enterprise to cnMaestro X](#)
- [Converting Tier 2 Unused Slots](#)

Guest Access

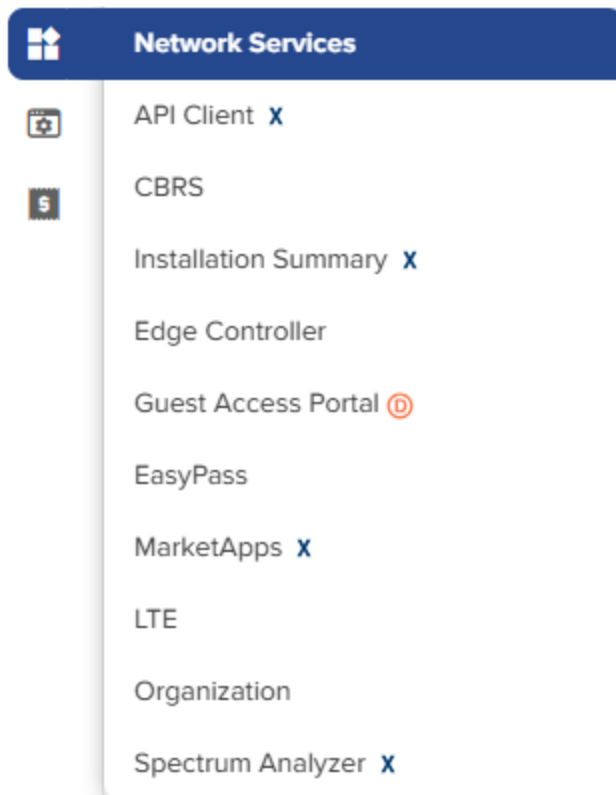
This section describes how to configure Guest Access using cnMaestro. This feature allows the clients to connect to the internet through Free Tier, Vouchers, or Paid Access types.



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 627](#). To create captive portals on cnMaestro, use EasyPass. For information, see [EasyPass](#).

Figure 627 Network Services



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

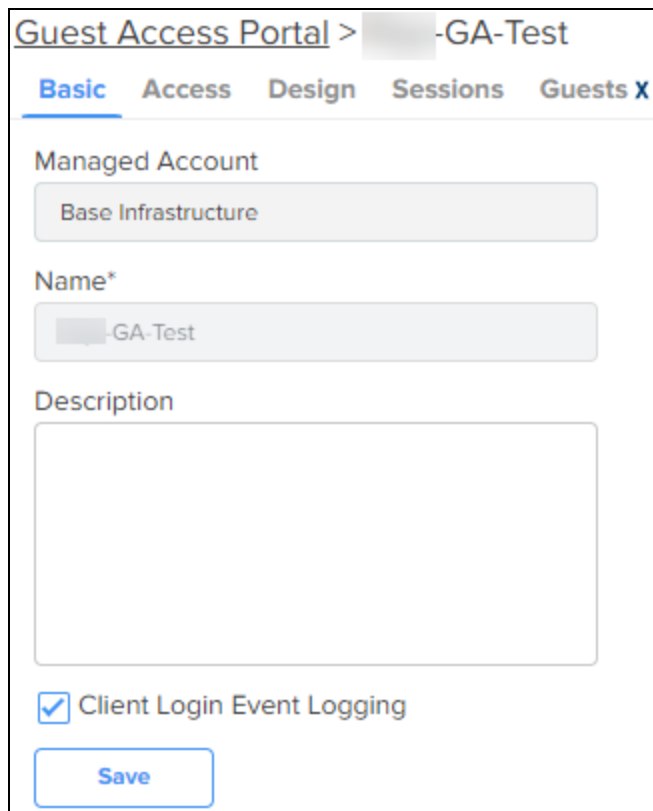
- Create the Guest Access Portal in cnMaestro
- Map the device to cnMaestro

Creating the Guest Access Portal in cnMaestro

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

Basic Details

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



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](#) > -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

 Valid range is 1-43800 hour(s)

Session Duration

 Valid range is 1-43800 hour(s)

☒ **Client Rate Limit**

☒ **Client Quota Limit**

☒ **Social Login**

☒ **SMS Authentication**

☒ **Add Whitelist**

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 175 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.
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

Table 175 *Free Access Type Parameters*

Parameter	Description
	<p>https://developers.facebook.com/apps/.</p> <ul style="list-style-type: none"> • 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 > i-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 x teachers x

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

Kbps

Uplink

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 > -GA-Test

Basic

Access

Design

Sessions

Guests X

Free

Enterprise X

Paid X

Vouchers

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.

Table 176 *Self Registration Parameters*

Parameter	Description
Enable Self Registration	Select the checkbox to enable self registration feature and configure the following parameters.
Sponsor Guest Settings 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.	
Require Sponsor	Select the checkbox if you want the self registration to be approved by a sponsor. The guests must enter the sponsor email address when registering for access to the SSID.
Sponsor Type	Specifies whether the sponsor approval for guest internet access must be automatic or manual. The following options are available: <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.

Table 176 *Self Registration Parameters*

Parameter	Description
Sponsor Email List	Configure the list of sponsor email addresses for approving access requests.
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 checkbox 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 dropdown list). This field is available only when you select Directional in the Quota

Table 176 Self Registration Parameters

Parameter	Description
	Type field.
Uplink	Specifies the uplink data usage limit (in either MB or GB, selected from the dropdown 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 dropdown 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 for 'Enterprise X' under the 'Access' tab. The 'Google' sub-tab is selected. The configuration options include:

- Microsoft Azure:** ☒ Enable Google Login
- Google Login:**
 - ☐ Enable Directory Synchronization
 - Allowed Domains*:**
- Device Limit:**
- Client Session:**
 - Session Duration*:** Min(s) Valid range is 1-2628000 min(s)
- Client Rate Limit:**
 - Downlink:** Kbps
 - Uplink:** Kbps
- Client Quota Limit:**
 - Quota Type:**

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

Table 177 Google Parameters

Parameter	Description
Enable Google Login	Select the checkbox to enable Google-based Wi-Fi access and configure the following

Table 177 *Google Parameters*

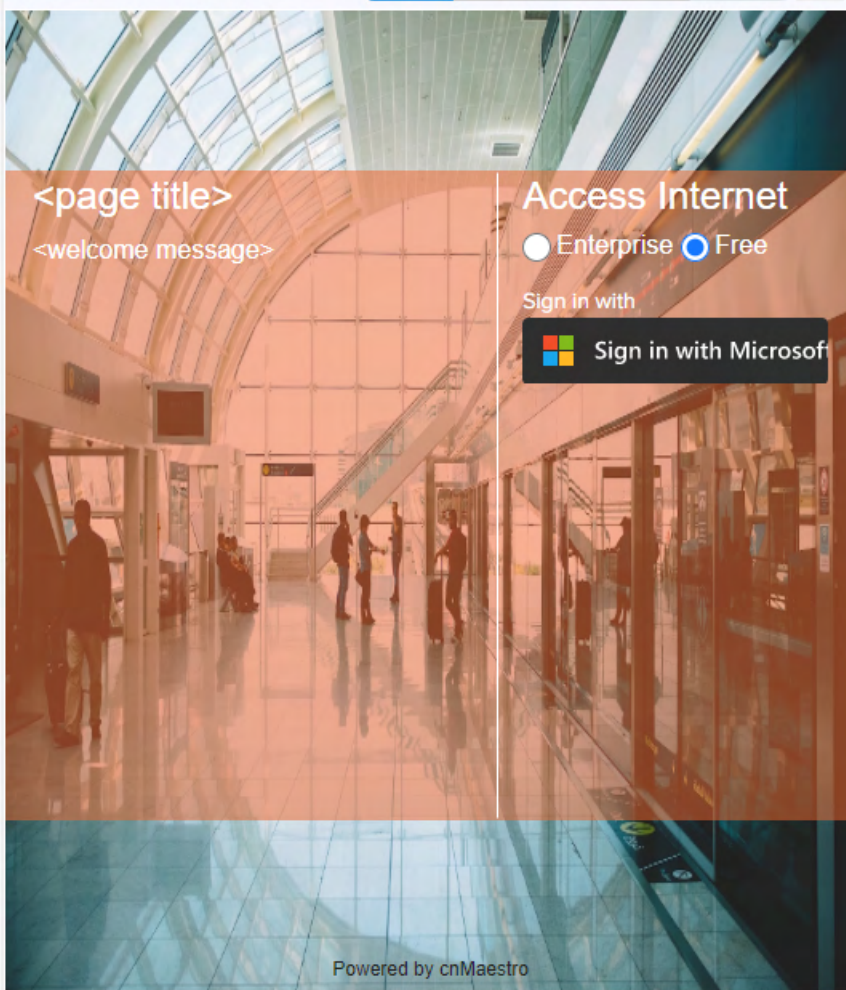
Parameter	Description
	parameters.
Device Limit	Specifies the number of devices that the guest can connect to the wireless network. Default: 5.
Google Login	
Enable Directory Synchronization	Select the checkbox to enable synchronization of Google Apps Domain Directory. This functions requires authorization. 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 dropdown 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 dropdown 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 dropdown 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**:

Preview

Airport Beach Coffee Hotel WiFi4EU



Logo

Logo ⓘ



Logo Background

Background



Background

Background Image ⓘ

☐ 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 > GP

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

[Add New](#)

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 178 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 limit s 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.
- The maximum number of vouchers that users are allowed to create per Voucher portal is as follows:
 - cnMaestro X—30,000
However, users are allowed to create a maximum of 2,000 vouchers at a single time.
 - cnMaestro Essentials—4,000
However, users are allowed to create a maximum of 1,000 vouchers at a single time.
- Total number of generated Vouchers = Vouchers Unclaimed + Vouchers Claimed + Vouchers Expired.
- The admin can export all, valid, or current page Voucher codes as a PDF or in the CSV format.

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 > Guest Access Portal > <portal-name>** page and select the **Access > Vouchers** tab.
- Select the **Enable Voucher Access** checkbox.

The screenshot shows the 'Guest Access Portal > GP' interface. The 'Access' tab is selected, and the 'Vouchers' sub-tab is active. The 'Enable Voucher Access' checkbox is checked. Below this, there are buttons for 'Add New', 'Card Preview', 'Export', 'Add Vouchers', 'Delete Selected', and 'Delete Expired'. A table with columns 'Voucher ID', 'Status', 'Creation Time', 'Claimed Time', and 'Expiry Time' is shown, but it contains no data, displaying 'No Generated Vouchers' instead. At the bottom, there is a 'Save' button and a note: 'Note: Splash page needs to be saved to reflect any changes in Access portal settings.'

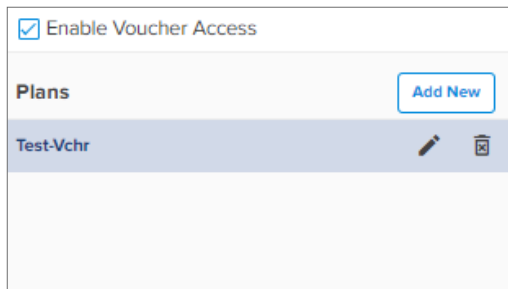
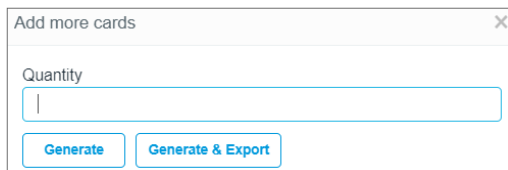
- Click **Add New**. The window with general and design parameters for the plan is displayed.

The 'Add New plan' dialog box is shown. It has two main sections: 'Plan Details' and 'Vouchers Design'. The 'Plan Details' section includes fields for 'Name', 'Session Duration' (with a dropdown menu), 'Voucher Expiry' (with a dropdown menu), 'Discount Rate Limit' (with a text input), 'Uplink Rate Limit' (with a text input), 'Quota Type' (with a dropdown menu), 'Voucher Device Limit' (with a text input), and a checkbox for 'Bind Voucher to Device'. The 'Vouchers Design' section includes a 'Background Image' field with a 'Browse' button, a 'Title' field, a 'Message' field, and an 'Access Code Message' field. At the bottom, there is a preview of the voucher design, which shows 'Internet Access Voucher' and a placeholder for the access code. The dialog box has 'Save' and 'Cancel' buttons at the bottom.

Table 179 *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.

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

Figure 628 *Select a plan***Figure 629** *Add Vouchers*

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 Add New Card Preview Export Add Vouchers Delete Selected Delete Expired

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

Showing 1 - 5 Total 5 10 Previous Next

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

Figure 630 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.

Guest Access Portal > GAP-Test-NOV25

Basic Access **Splash** Sessions

Preview

Airport Beach Coffee Hotel WiFi4EU ...

<page title>

<welcome message>

Access Internet

☒ Voucher ☐ Free

Voucher Code

Login

Save

Logo
Background
Text Design
Content
Advanced
Custom Fields
WiFi4EU **Beta**

Table 180 *Design Page Parameters*

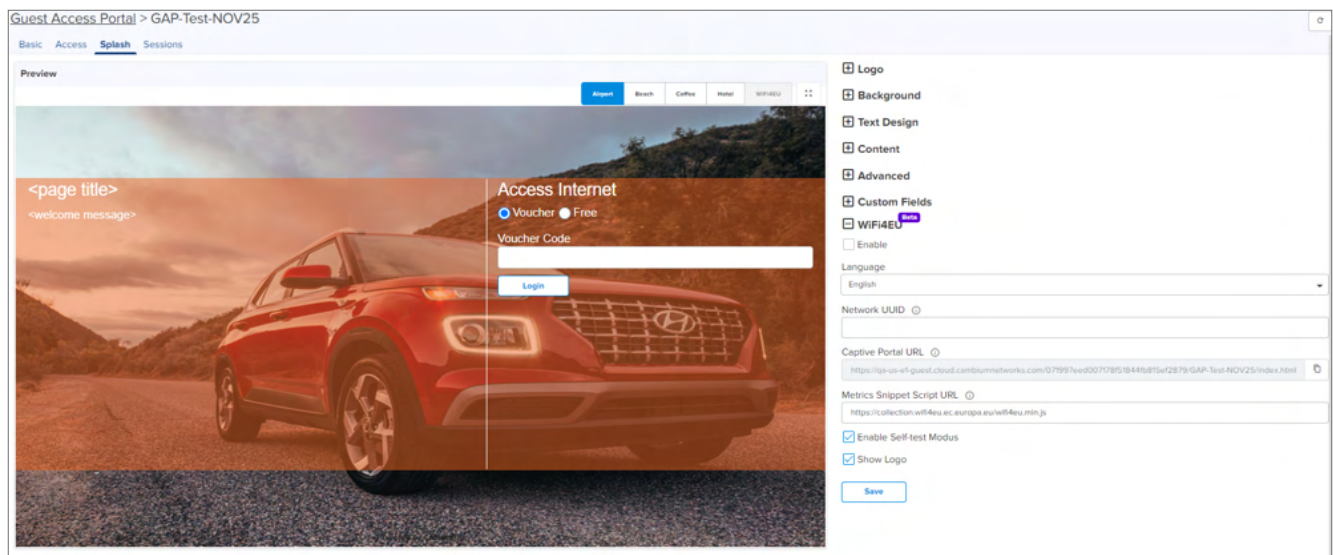
Parameter	Description
Accept Terms Message	Text to appear as the accept terms message.
Advanced	Expand Advanced option. Browse and select the advanced fields.
Background	Browse and select the image that needs to be displayed as the background. <ul style="list-style-type: none"> Recommended image resolution—1024 pixels × 800 pixels Maximum supported image file size—5 MB Supported file formats—JPEG, JPG, PNG, and GIF
Background Placement	Choose the option from the dropdown 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 checkbox 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.

Table 180 *Design Page Parameters*

Parameter	Description
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 Button	Text to appear in the terms agree 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 181** *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.

Parameter	Description
	<ul style="list-style-type: none"> • 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.

The screenshot shows the 'Guest Access Portal' interface with the 'Sessions' tab selected. The 'Client Session' table is currently empty, displaying 'No Data Available'. Below it, the 'Client Login Events' table shows a list of login events with columns for Client MAC, Portal, Access Type, SSID, Access Point, Voucher Code, Login Time, Email, and Mobile Number. The events are sorted by Login Time in descending order.

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		

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 data in the CSV format.



Note

The **Export page as PDF** option is deprecated from cnMaestro release version 5.2.0 onwards. This option will be completely removed from the UI in release version 5.3.0.

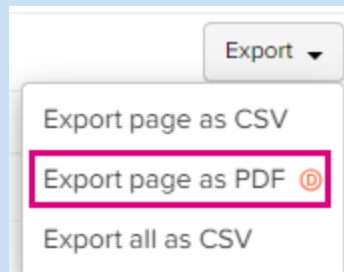


Table 182 *Sessions Parameters*

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 > -GA-Test		
Basic	Access	Design
Sessions		
Guests X		
Sessions and Login Events		
Paid Transactions		
Users X		
<input type="checkbox"/> Email	Group	Registered Devices
No Data Available		
Showing 0 - 0 Total: 0 10 < Previous Next >		

Table 183 *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

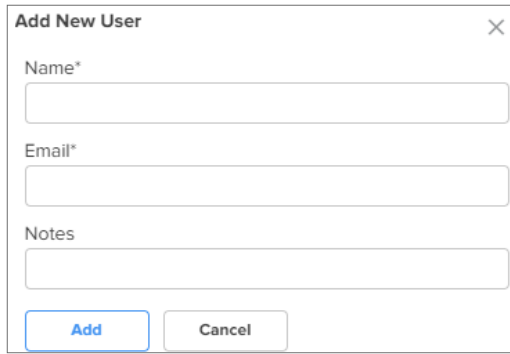
The Guests page allows you to view details of self registered guests connecting to the wireless network. However, to view this page, you must first enable and configure self registration under **Network Services > Guest Access Portal > Access > Enterprise X > Self Registration**.

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*

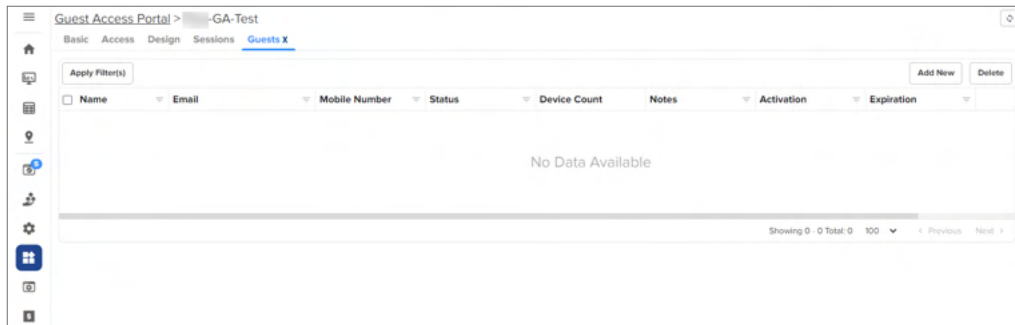
Email*

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 the 'Guest Access Portal' interface for a device named 'GA-Test'. The 'Guests' tab is selected, displaying a table with columns: Name, Email, Mobile Number, Status, Device Count, Notes, Activation, and Expiration. The table is currently empty, showing 'No Data Available'. There are 'Add New' and 'Delete' buttons at the top right of the table area. The bottom of the interface shows pagination: 'Showing 0 - 0 Total 0 100' and navigation arrows for 'Previous' and 'Next'.

Table 184 *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

Background Image

Background image to be displayed on the splash page

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** checkbox.
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:

Session Timeout: Session time in seconds (60 to 66400)

Inactivity Timeout: 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 Gateway	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

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

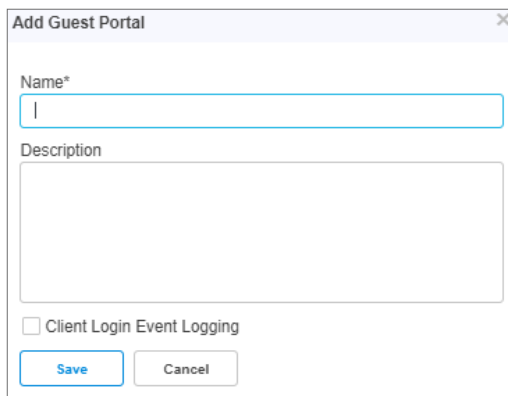
Guest Access using Social Login

Configuration

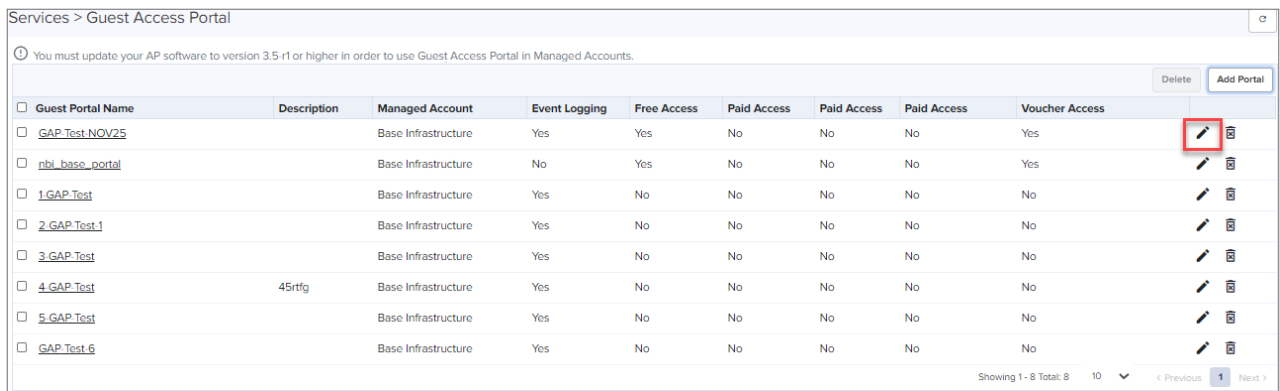
To achieve cnMaestro Guest Access using Social Logins like Google, Twitter, Facebook, and Office 365, perform the following steps:









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**.



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



<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"/>	nbl_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	

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

Guest Access Portal > GP

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 > GP

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
[Empty field]

☒ Twitter

Consumer API Key
[Empty field]

Consumer API Secret Key
[Empty field]

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

☒ Facebook

Id
[Empty field]

Secret
[Empty field] Show

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

☒ 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
[Empty field]

SMS Authentication

Add Whitelist

Save

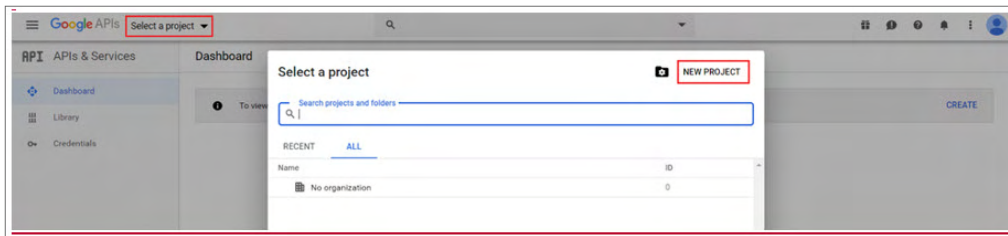
API Key Generation

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

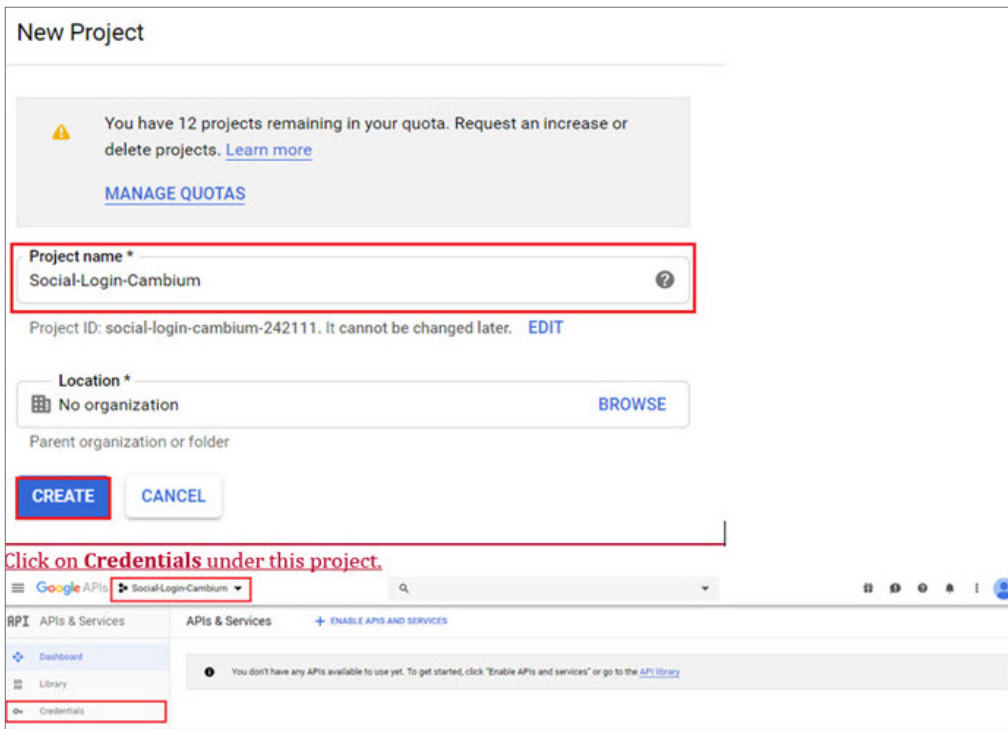
- [Google](#)
- [Twitter](#)
- [Facebook](#)
- [Office 365](#)

Google

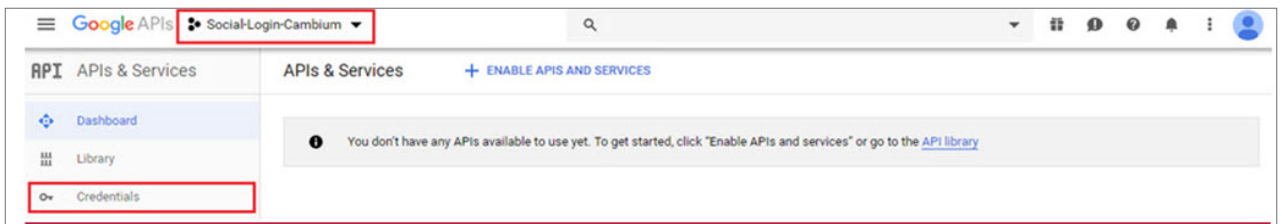
1. Login to Google Account and navigate to <https://console.cloud.google.com/>.
2. Click **Select a Project** and create a **New Project**.



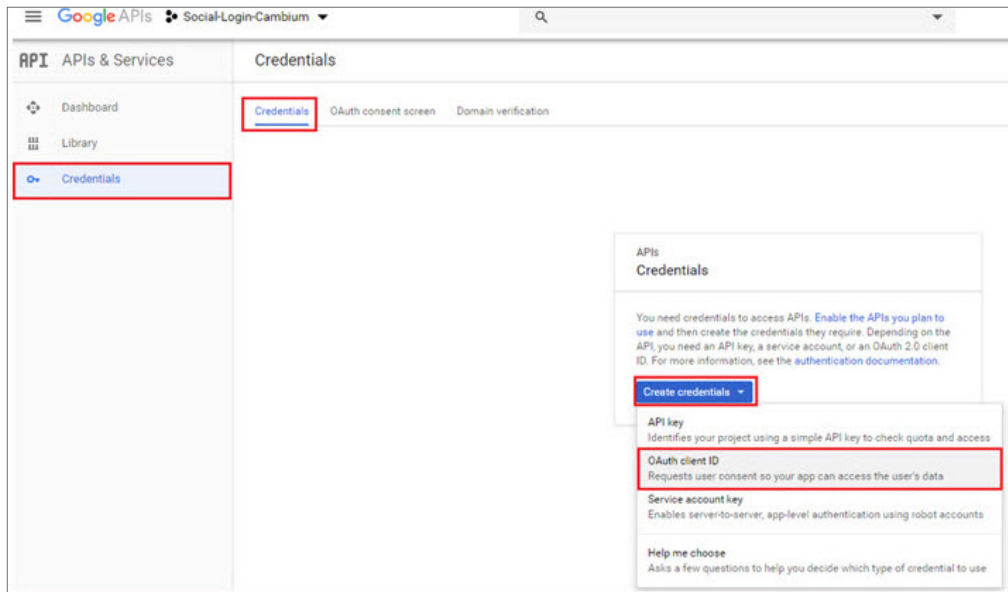
3. Give a name to the Project and click **CREATE**..



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

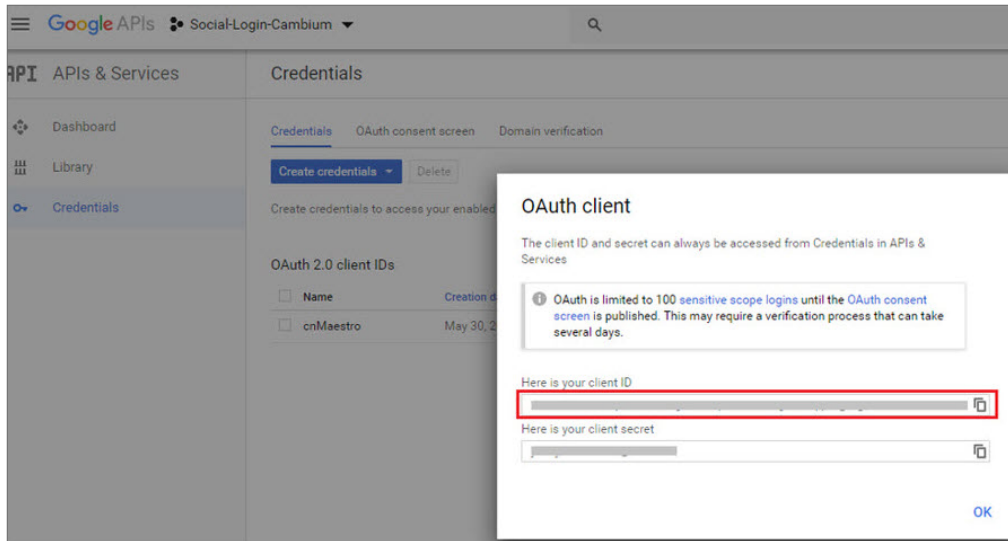
cnMaestro GUI

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.

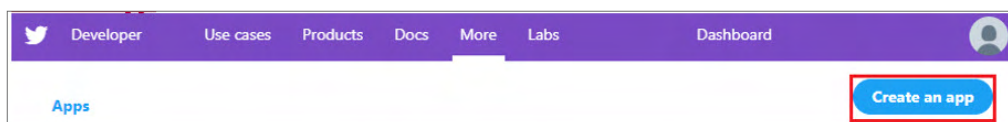


11. Copy the Client ID and paste it to the cnMaestro enabling Google under Social Logins and click **Save**.

The screenshot shows the 'Social Login' configuration page. The 'Guest Portal Hostname / IP' field is filled with 'qk-us-el-guest.cloud.cambiumnetworks.com'. Below this, there is a note about captive portal bypass. The 'Google' checkbox is checked, and the 'Id' field is empty. Other social login options like Twitter, Facebook, and Office 365 are listed but not selected. There are also sections for 'SMS Authentication' and 'Add Whitelist'. A 'Save' button is at the bottom.

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-s1-5pkodub@un.cloud.cambiumnetworks.com

Privacy policy URL
https://ap-s1-s1-5pkodub@un.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.

[Cancel](#) [Save](#)

cnMaestro GUI

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

- 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
Consumer API key (API key)
Consumer API secret key (API secret key)
[Regenerate](#)

- Paste them to cnMaestro GUI for Twitter social login.

Social Login

Guest Portal Hostname / IP
 qa-us-ef-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
☒ Twitter

Consumer API Key

Consumer API Secret Key

Callback URL

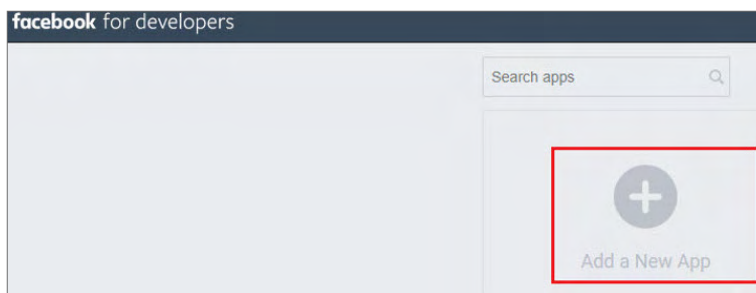
☐ Facebook
☐ Office 365

SMS Authentication
☐ Add Whitelist

[Save](#)

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.

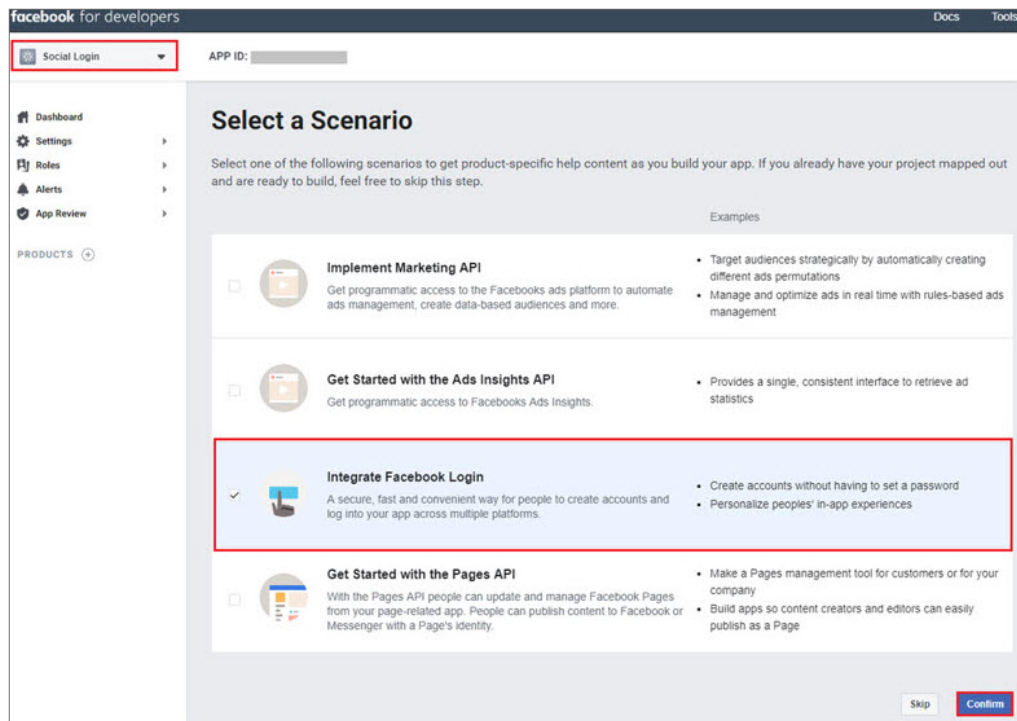
Display Name

Contact Email

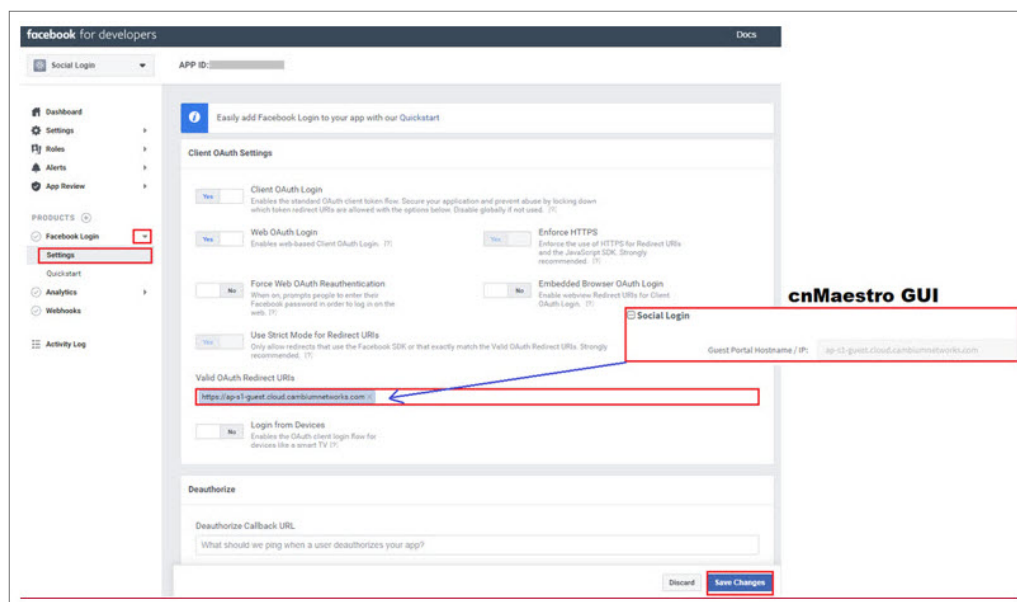
By proceeding, you agree to the Facebook Platform Policies

[Cancel](#) [Create App ID](#)

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:

App Domains: Contact Email: @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
qa-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
☐ Twitter
☒ Facebook

Id: [redacted]
 Secret: [redacted] Show

Reply URL: https://qa-us-el-guest.cloud.cambiumnetworks.com/cn-ctrl/guest/071997i

☐ 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: XXXXXXX-12345-4565-aabbcc ① → Copy and paste it to cnMaestro →

Application Secrets

Generate New Password ② 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

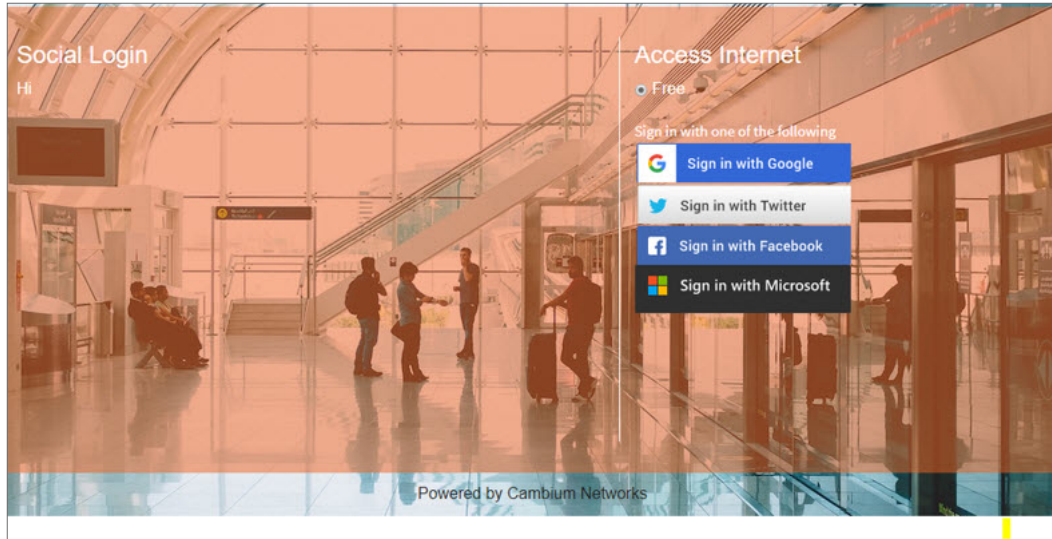
SMS Authentication

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** checkbox.
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 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 XML reply failure element field.

Sample configuration in the cnMaestro

Figure 631 : Guest Access Portal

Guest Access Portal > SASI_GAP

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: 1000 Min(s) Valid range is 1-2628000 min(s)

Session Duration: 1000 Min(s) Valid range is 1-2628000 min(s)

Client Rate Limit

Client Quota Limit

Social Login

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

Network Port Requirements

Network Port Requirements for Outbound Access

The following table provides information about network port requirements for APs to have outbound access to various services and applications:

Table 185 Outbound Port Details

Port Number	Port Type	Purpose
443	TCP	HTTPS Web access and device communication for the following URLs: <ul style="list-style-type: none">*.cambiumnetworks.com (for connecting to cnRouter and cnMaestro)*.xirrus.com (for activation and license keys)*.cloud.xirrus.com (for general communication with XMS-Cloud)*.cloudfront.net (for software downloads)*.amazonaws.com (for diagnostics)

Table 185 *Outbound Port Details*

Port Number	Port Type	Purpose
53	TCP / UDP	For DNS resolution of the following URLs: <ul style="list-style-type: none">• *.cambiumnetworks.com (for connecting to cnRouter and cnMaestro)• *.xirrus.com (for activation and license keys)• *.cloud.xirrus.com (for general communication with XMS-Cloud)• *.cloudfront.net (for software downloads)• *.amazonaws.com (for diagnostics)
123	UDP	For accessing the time servers.

**Note**

There must not be any proxy or other devices blocking WAN access to the APs.

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:

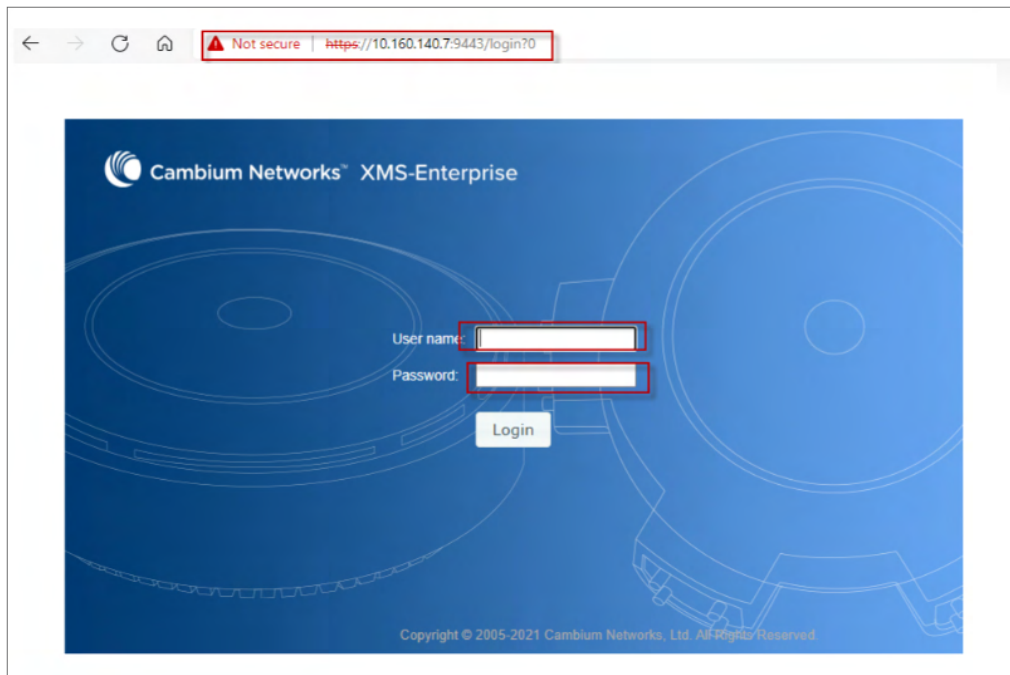
1. In XMS-E, perform the following actions:
 - [Export Golden Configuration](#)
 - [Migrate to cnMaestro X](#)
2. In cnMaestro X, perform the following actions:
 - [Create Wi-Fi AP Group](#)
 - [Approve APs into Wi-Fi AP Group](#)
 - [Import and Apply AP configuration](#)

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**.

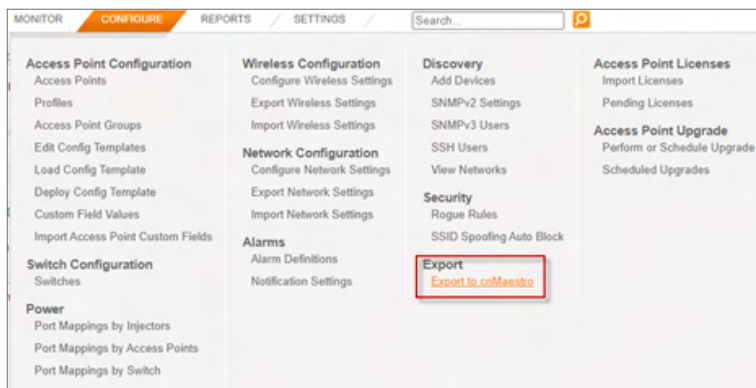


Export Golden Configuration

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**.

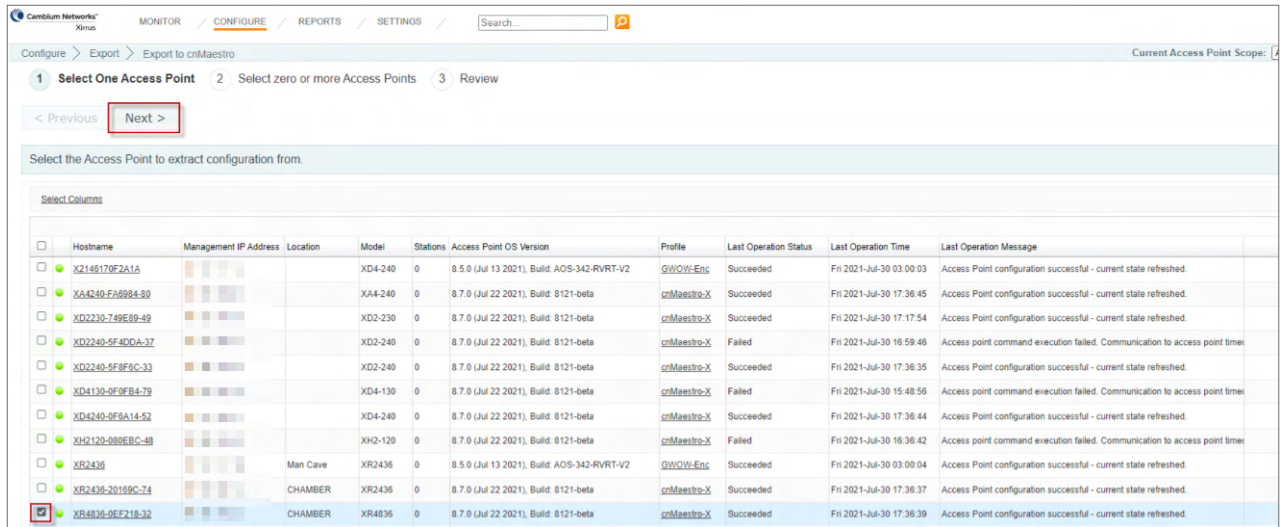


2. Select the AP to create the golden configuration for a group of APs and click **Next**.

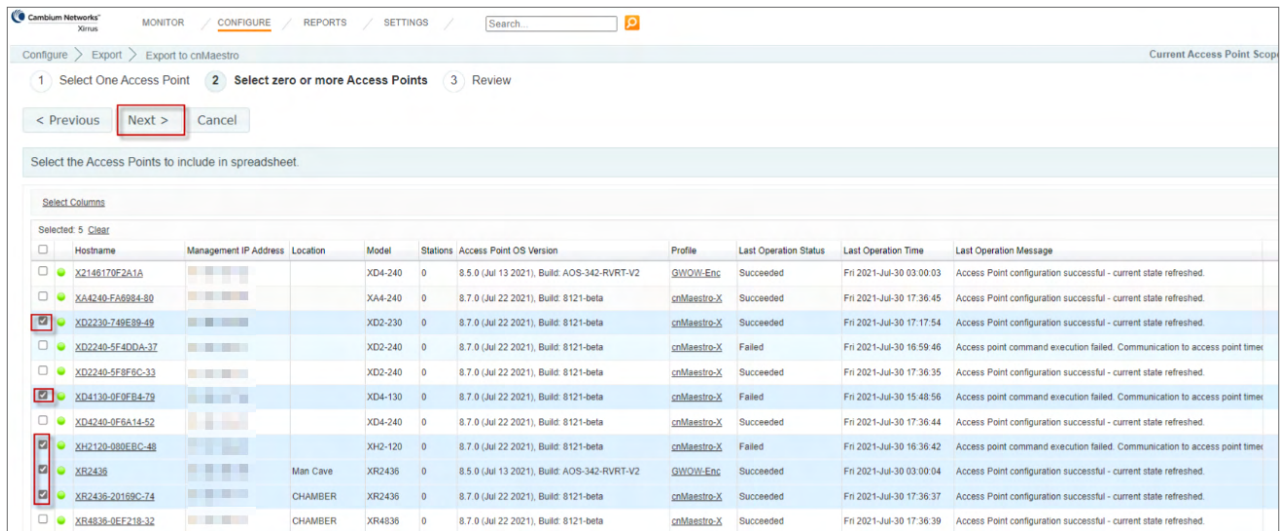


Note

- 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.



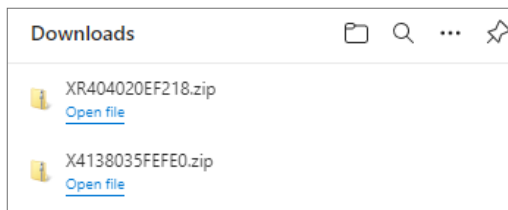
3. Select group of APs to be added to the spreadsheet and click **Next**.



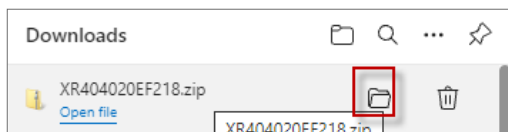
4. Click **Export**.

In Local System unzip the directory and files to local directory.

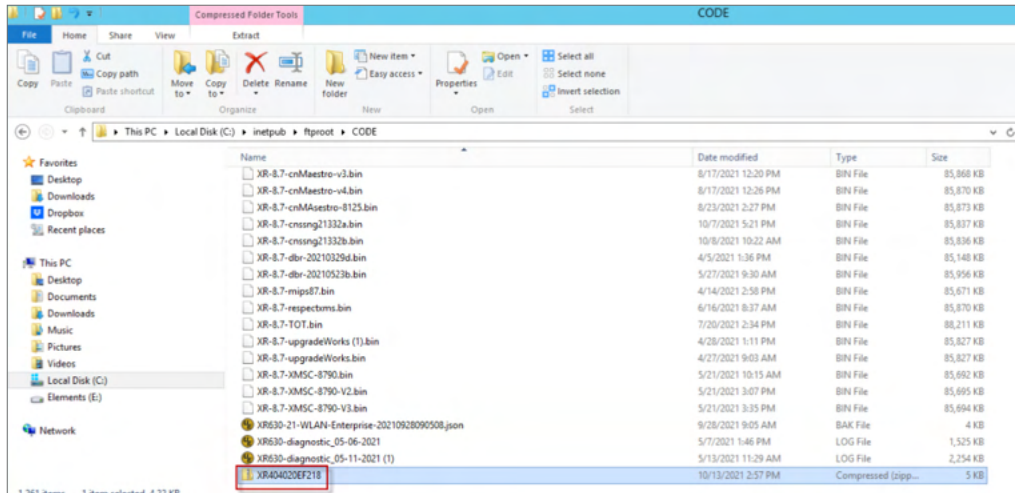
5. Download the zip files from the browser window.



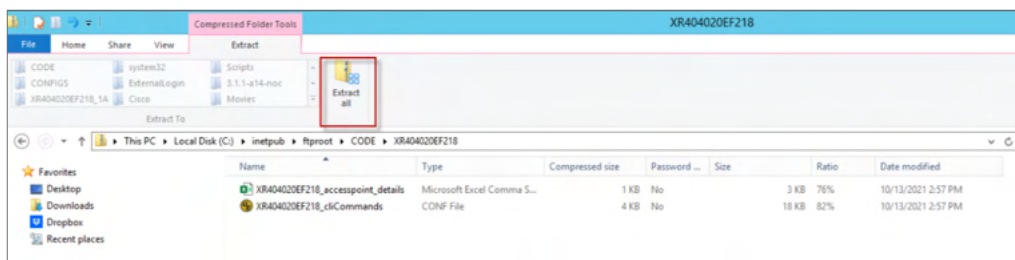
6. Go to the folder where the zipped files are saved and extract the contents to a folder.



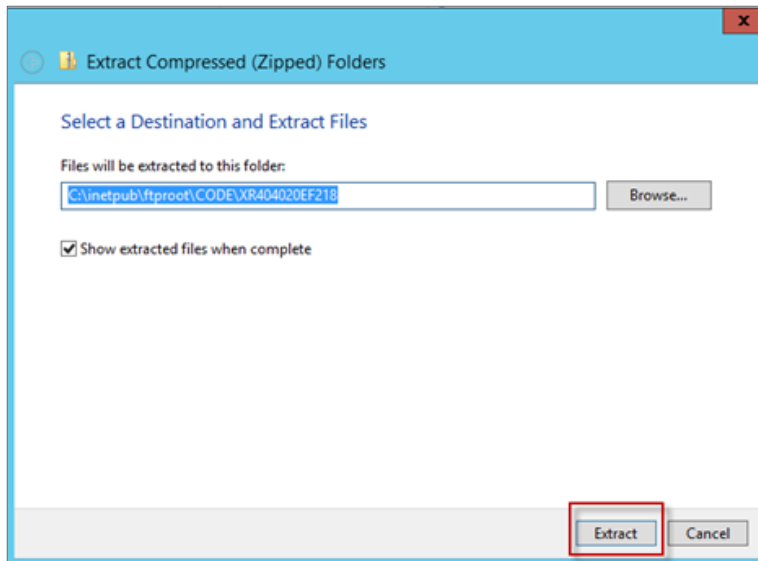
7. Open the directory path where the file has been stored and double-click on the zipped file.



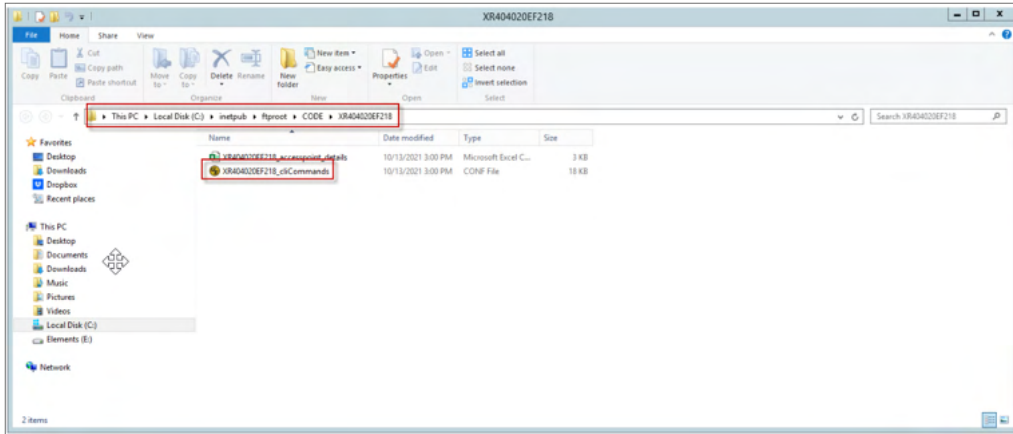
8. Click **Extract all**.



9. Extract the folder to the path.



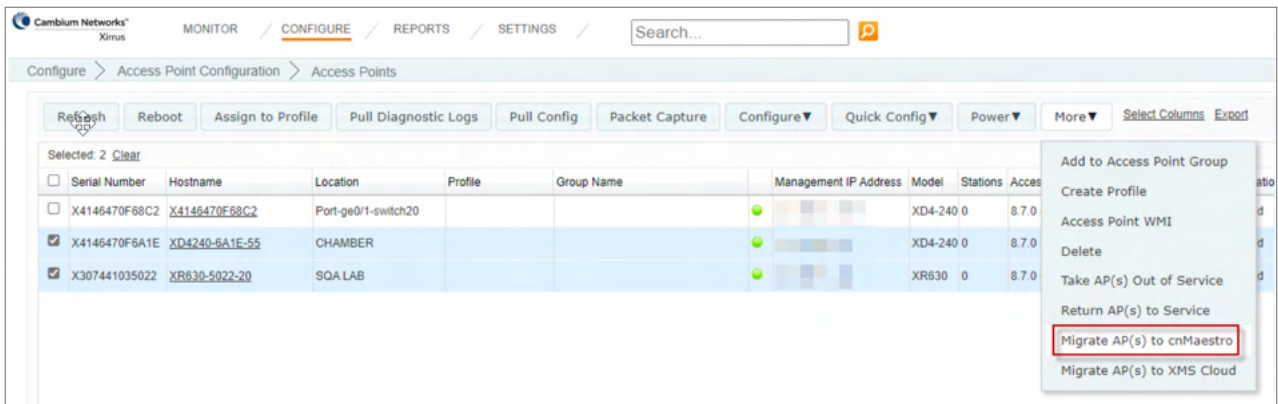
10. Make a note of the folder or file location as you will require this file later.



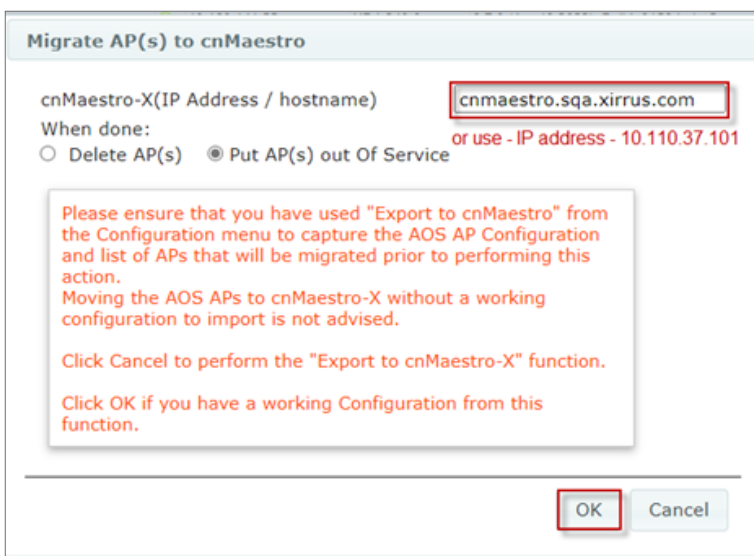
Migrate to cnMaestro X

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**.



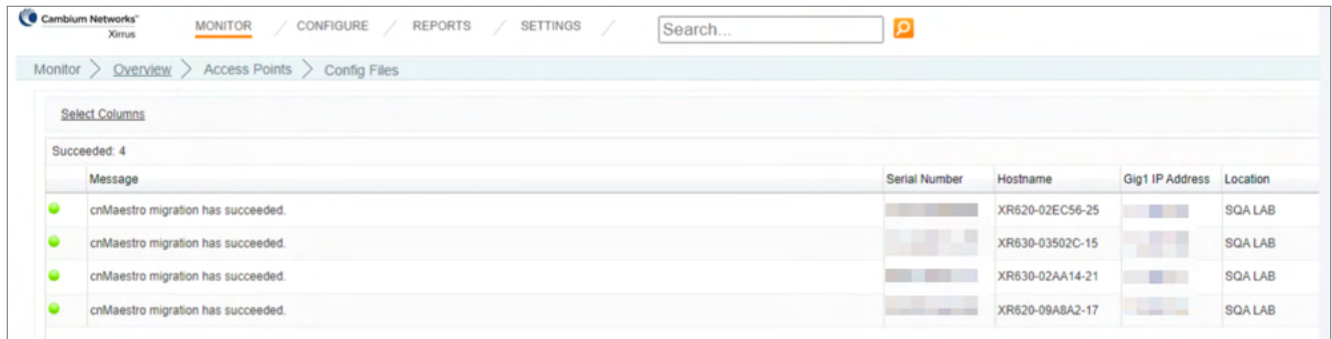
Note

- 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.



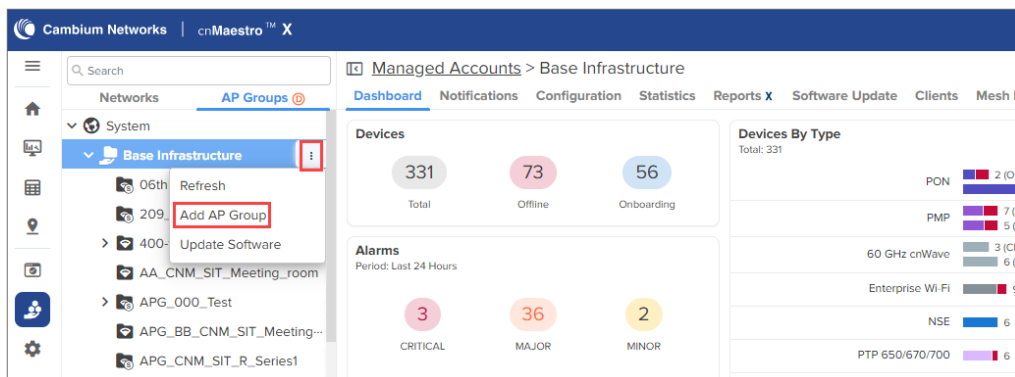
The screenshot shows the 'Monitor > Overview > Access Points > Config Files' page. A 'Succeeded: 4' message is displayed above a table with the following columns: Message, Serial Number, Hostname, Gig1 IP Address, and Location. The table contains four rows, each with a green success icon and the message 'cnMaestro migration has succeeded.'.

Message	Serial Number	Hostname	Gig1 IP Address	Location
cnMaestro migration has succeeded.		XR620-02EC56-25		SQA LAB
cnMaestro migration has succeeded.		XR630-03502C-15		SQA LAB
cnMaestro migration has succeeded.		XR630-02AA14-21		SQA LAB
cnMaestro migration has succeeded.		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 dropdown.
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

5. In the **Full Configuration** page, click the **Import** option.

AP Groups > Add New

Basic

Full Configuration

Import Config

Configuration file
Import.conf

Import

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 Export

Save Close

6. Select the CLI command file from the unzipped directory.

Open

This PC > Local Disk (C:) > inetpub > ftproot > CODE > XD4240_GoldenConf

Name	Date modified	Type	Size
X4146470F6A1E_accesspoint_details	4/22/2022 11:48 AM	Microsoft Excel C...	3 KB
X4146470F6A1E_cliCommands	4/22/2022 11:48 AM	CONF File	43 KB

7. Click **Import**.



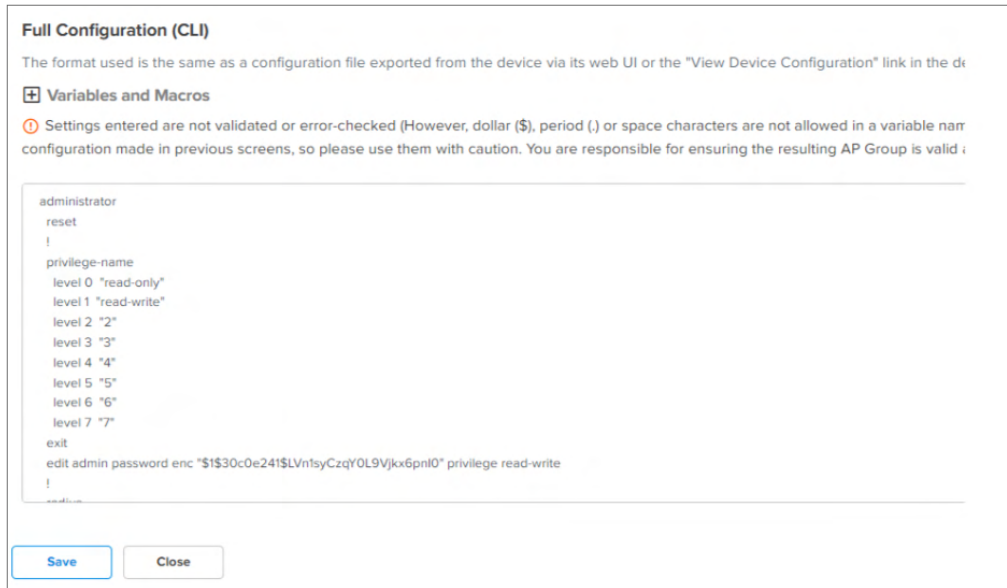
Import Config

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**

- Click **Save**.

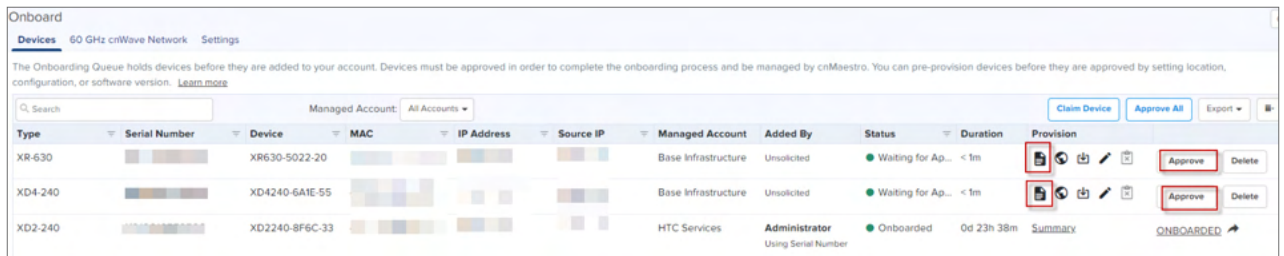
Approve APs into Wi-Fi AP Group

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.

- 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

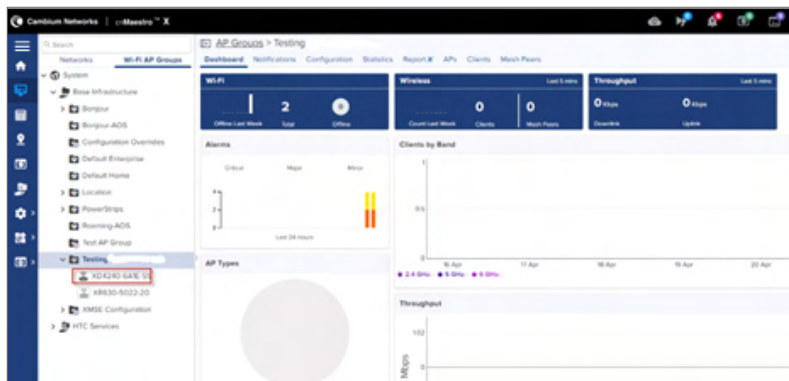
Type	Serial Number	Device	MAC	IP Address	Source IP	Managed Account	Added By	Status	Duration	Provision	Actions
XR-630		XR630-5022-20				Base Infrastructure	Unsolicted	Waiting for Ap...	< 1m		Approve Delete
XD4-240		XD4240-6A1E-55				Base Infrastructure	Unsolicted	Waiting for Ap...	< 1m		Approve Delete
XD2-240		XD2240-8F6C-33				HTC Services	Administrator	Onboarded	0d 23h 38m	Summary	ONBOARDED

- Enter the required details, provision the device for location, and assign to an AP Group.

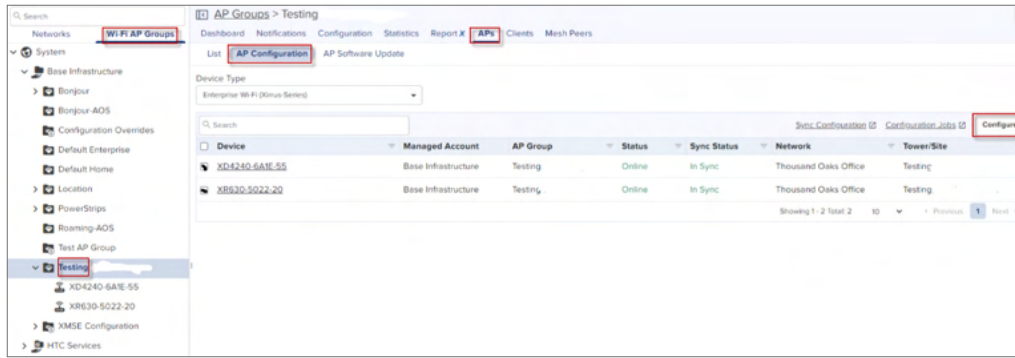
3. Click **Save**.
4. In the **Onboard > Devices** page, select **Approval All** (to approve all devices at once) or **Approve** (to approve devices individually.)

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**.

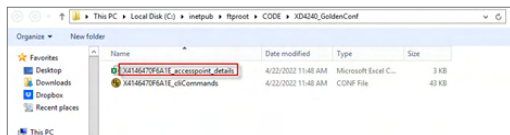


Note

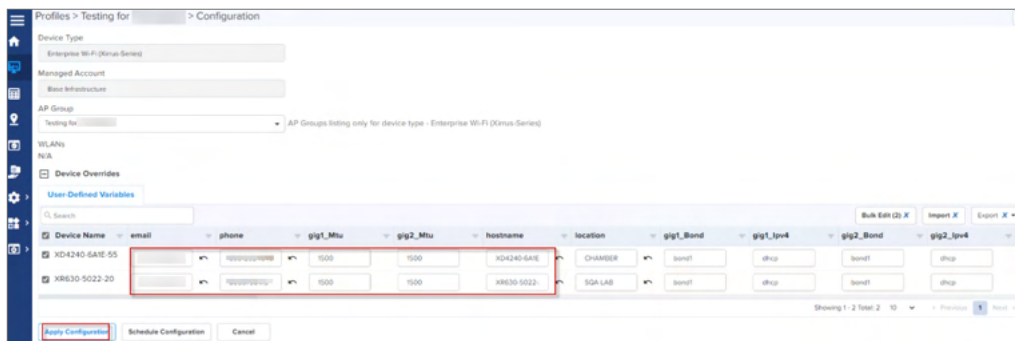
Email and Phone fields are auto populated from the .csv file.



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 186](#).

Table 186 Example of converting unused Tier 2 slots

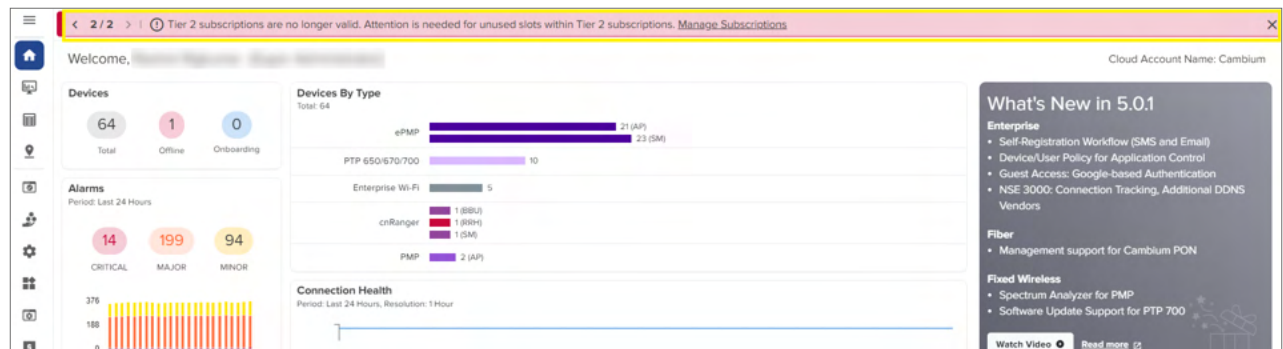
New Tier	Device Family and Type	
Tier 21	cnVision	FLEXr, HUB360
	ePMP	All AP Models
Tier 22	PMP	All AP Models except 450m and 450mv
Tier 23	PMP	450m
Tier 24	cnRanger	All BBU Models
	cnReach	All cnReach Models
	PTP	All PTP Models

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 632](#).

Figure 632 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 633](#)), displaying the same banner and details of tiers.

Figure 633 The Manage Subscriptions page with tier information

Manage Subscriptions


This page provides a usage summary and a list of pending/active/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. [Learn more](#) [Upgrade to X-NFR](#)

Not enough slots

To upgrade to cnMaestro X, you must have an active subscription for every device in your account. [Learn more](#)

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


Name	Type	Device Tier	Slots Used	Status	Start Date	End Date	Validity	Commercial ID
Professional T60	Built-in	Tier 60	0	Active	20 Dec 2023	28 Jan 2025	342 days	N/A
Professional T43	Built-in	Tier 43	0	Active	20 Dec 2023	28 Jan 2025	342 days	N/A
Professional T41	Built-in	Tier 41	0	Active	20 Dec 2023	28 Jan 2025	342 days	N/A
Professional T40	Built-in	Tier 40	0	Active	20 Dec 2023	28 Jan 2025	342 days	N/A
cnMaestro X Free Tier	Built-in	Free Tier	31	Active	20 Dec 2023	28 Jan 2025	342 days	N/A
Tier 2-2024-02-20T13:05:45.99997899Z-408	New	Tier 2	0 / 100	Pending	02 Mar 2024	16 May 2024	76 days	Future_Subscription_T2
Tier 30	Trial	Tier 30	0	Active	30 Jan 2024	28 Apr 2024	67 days	
Tier 20	Trial	Tier 20	0	Active	30 Jan 2024	28 Apr 2024	67 days	
Tier 7-2	Trial	Tier 7	0	Active	30 Jan 2024	28 Apr 2024	67 days	
Tier 6-2	Trial	Tier 6	0	Active	30 Jan 2024	28 Apr 2024	67 days	

3. Select the Tier 2 subscription and click the corresponding  icon (as shown in [Figure 633](#)).

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 634 The Convert Tier 2 window

Convert Tier 2-2024-02-26T07:40:38.788211254Z-323

 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

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 634](#)) 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 © 2025 Cambium Networks, Ltd. All rights reserved.