Cambium Networks™

USER GUIDE

cnMaestro On-Premises

6.0.0

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.

© 2026 Cambium Networks Limited. All Rights Reserved

Contents

Contents ***3***

Introduction ***27***

Supported Devices and Features **27**

Supported Virtualization Infrastructures 27

Hardware requirements 28

Devices and minimum software versions 28

Supported browsers 32

cnMaestro features 32

On-Premises Quick Start **39**

Installation 39

Virtualization 39

Desktop virtualization 39

Bare metal hypervisor 39

cnMaestro deployment 40

Cloud Synchronization **47**

Cloud Anchor account 47

Creating Cloud Anchor account 47

Cloud Anchor account cnMaestro X activation 51

Cloud Anchor account features 54

Cloud Connectivity **66**

Connecting cnMaestro On-Premises to Cloud Anchor account 66

Disconnect cnMaestro On-Premises from Cloud Anchor account 68

Cloud connectivity disconnected State 70

On-Premises Subscription Management **70**

Upgrade to cnMaestro X 70

Downgrade to Essentials 72

Delete On-Premises instances 73

Slot Deficit 76

Manage Subscriptions 77

Subscriptions 77

Devices 78

Expiry Notification 81

Data retention period 82

cnMaestro X features behavior state **82**
Navigating the cnMaestro UI **90**
Basic 90
Account View 91
Access and Backhaul view 92
Enterprise view 92
Home page 93
Page structure 93
Searching for cnMaestro resources using the Search bar 95
Page navigation 95
Access and Backhaul View 96
Overview 96
Enterprise Account view 103
Overview 103
System 103
Devices 103
AP Groups 104
WLANs 105
Sites 105
Side menu 105
Section tabs 106
System status 106
Data Tables and Chart UI Controls 107
Logout 107
Architecture **107**
Networking 108
High Availability (HA) **109**
Overview 109
Primary vs Secondary 109
Shared (Floating) IP Address 109
Network Ports 109
Recommendations 110
Dual Interfaces 110
Add eth1 Network Adapter 111
HA Cluster Setup 113
Bootstrap (Primary) 113
Accept (Primary) 113

Join (Secondary) ... 113
Basic HA Cluster Creation Flow ... 114
HA Menu ... 116
High Availability Cluster Menu (Pre-Bootstrap) ... 117
High Availability Menu (Post-Bootstrap) ... 117
New Cluster ... 117
Accept Join Requests ... 118
Join Existing Cluster ... 118
Validate SSH Fingerprints ... 119
HA Cluster Status ... 119
Delete Node ... 120
Leave Cluster ... 121
Information ... 122
Behaviour of cnMaestro features when HA is Enabled ... 122
Device Onboarding ... 123
Onboarding Status ... 124
Claiming Devices ... 125
Claiming Devices with Cambium ID ... 127
Claiming the Wi-Fi Devices from AP Group ... 127
Claiming Wi-Fi devices from the Site dashboard ... 128
Claiming multiple Enterprise devices using CSV import ... 130
Points to consider when importing enterprise devices using CSV import option ... 132
Reclaim ... 132
Grace period ... 132
Deleting Devices ... 135
Device-Specific UI Onboarding ... 135
Static URL ... 135
cnMatrix ... 136
Enterprise Wi-Fi ... 136
cnPilot Home ... 136
cnRanger ... 136
cnReach ... 137
cnVision Client ... 138
cnVision Hub ... 138
ePMP 1000 AP/SM ... 138
ePMP 1000 Hotspot ... 139
PMP ... 139

PTP 650/670/700 140
Onboarding Xirrus device 140
Onboarding through CLI for cnMaestro X 141
Onboarding Xirrus AP to cloud using Cambium ID and Onboarding Key 142
Onboarding through DHCP options for cnMaestro X 143
Onboarding a cnWave 5G Fixed BTS device 144
Claiming the cnWave 5G Fixed BTS device 144
Claiming the cnWave 5G Fixed BTS device with a Serial Number 147
Onboarding Edge Controller 149
Onboarding PTP 820/850 devices 149
DHCP Options (Linux) 150
Onboarding PON devices 152
Onboarding 60 GHz cnWave devices 154
60 GHz E2E Controller Onboarding 155
External E2E Controller Onboarding 155
Device E2E Controller (Running Onboard) Onboarding 157
60 GHz E2E Controller Onboarding devices 158
Deleting Devices in Bulk 159
Device-specific restrictions 160
Deleting devices in bulk 161
Viewing the status of device deletion and retrying 162
Export All as CSV 163
Exporting and downloading all data in the CSV format 164
Monitoring 166
Network Monitoring 166
Assists X 166
Exporting assists information 169
Assists filter 169
Assists Status 170
Device filter 172
Enable Assist 173
Assists X fix now 173
Dashboard 175
KPI (Key Performance Indicators) 175
Application History X and Applications X 176
Device Health 177

Connection Health 177
Charts and Graphs 177
Site dashboard 178
Enterprise Site dashboard 179
Devices widget (Total, Offline, Out of Sync) 180
Throughput 181
Client Connection Health X 181
Wi-Fi Client Analytics X 181
Assists X 182
Alarms 182
Top Active Alarms 182
AP Types 182
Channel Distribution by Band 183
Clients Performance by Band (Enterprise Wi-Fi) 183
Clients SNR by Band (Enterprise Wi-Fi) 183
Connected 6 GHz Client Capability 184
Application History X (Category History X) 184
Client Capability History 185
Radio Distribution by Band 185
WLAN Distribution by Band 185
Throughput Graph 186
Top Wi-Fi APs by Throughput or Clients 186
Top Clients by Session 186
Top Clients by Usage 186
60 GHz cnWave Site Dashboard 187
PON Site Dashboard 187
Notifications 188
Event/Alarm Source 191
Aggregation 191
Storage 191
Events 191
Event Severity 191
Event Export 191
Alarms 200
Alarm History 203
Wi-Fi Events 205
Configuration 205

Statistics and Details 208
Statistics page 209
Details page 218
PON (OLT) 244
PTP 650/670/700 245
PTP 820/850 Details 246
Performance **250**
Map **263**
Geolocation Map Settings 265
Map Navigation 266
Mode 267
Embedded Maps 267
Sector Visualization 267
Tools **272**
60 GHz cnWave Tools 272
cnMatrix Tools 272
Cable Diagnostic 274
Port Enable or Port Disable 274
PoE Toggle 275
PoE Enable or PoE Disable 276
Remote CLI 278
cnPilot Home Tools 280
cnRanger Tools 282
cnRanger BBU 283
cnRanger SM 283
cnReach Tools 283
cnVision Tools 284
Edge Controller Tools 285
Enterprise Wi-Fi Tools 285
Packet Capture 287
Wi-Fi Performance Test 291
ePMP Tools 293
PMP Tools 294
cnWave 5G Fixed Tools 296
Status 296
Link Test 297
Ping Test 298

Wireless Intrusion Detection System (WIDS) 300
Neighboring APs 301
Rogue APs 303
Honeypot APs 304
Wired Devices 304
Ad Hoc Networks 305
Allowlist APs 306
Configuring WIDS 307
Configuring Wired Neighbor Discovery 308
Wireless Flood Detection 308
Wireless Intrusion Prevention System (WIPS) 309
Off Channel Scan (OCS) 310
PMP Dashboard 311
Multiple Component Carrier (CC) Support in PMP 450v 311
PMP 450v 4×4 AP/BHM dashboard 312
PMP 450v 4×4 SM/BHS and PMP 450v 2×2 SM/BHS dashboard 312
PMP 450v 4×4 AP/BHM Map View 313
Wireless LAN Dashboards 314
Wi-Fi Monitoring 314
Dashboard 314
Clients 317
Details 326
Mesh Peers 329
Site Dashboard 330
Client Connection Health X 331
Assists X 331
Alarms 332
Top Active Alarms 332
AP Types 332
Channel Distribution by Band 332
Clients Performance by Band (Enterprise Wi-Fi) 333
Clients SNR by Band (Enterprise Wi-Fi) 333
Connected 6 GHz Client Capability 333
Application History X (Category History X) 334
Client Capability History 334
Radio Distribution by Band 335
WLAN Distribution by Band 335

Throughput 335
Throughput Graph 336
Top Wi-Fi APs by Throughput or Clients 336
Wi-Fi devices widget (Total, Offline, Out of Sync) 336
Top Clients by Session 336
Top Clients by Usage 337
Floor Plan 337
Statistics 342
Wireless Clients 343
WLANs Dashboard 344
Fiber OLT and ONU 348
Dashboard 349
Alarms 350
Port Status 350
ONU by Signal Level 350
ONU by Signal Level per Port 351
ONUs 351
PON Downlink Utilization 351
PON Downlink Throughput 352
PON Uplink Throughput 352
Ethernet Downlink Throughput 352
Ethernet Uplink Throughput 353
Notifications 353
Configuration 354
Details 355
Performance 356
ONUs 356
Export ONUs 357
Rename ONUs 357
Ports 358
Software Update 360
OLT Software Update 360
ONU Software Update 361
Tools 362
ONU Dashboard 362
Inventory 366
Inventory Export 366

Bulk Delete 366
Bulk Reboot 367
Schedule Reboot 368
Import Device Configuration 368
Sample Configuration File 369
Sample Configuration File (60 GHz cnWave) 369
Uploading a Configuration File 370
Reports 372
Data Reports 373
Devices Report 374
Audit Logs Report 382
Performance Report 383
Active Alarms Report 389
Alarm History Report 389
Events Report 390
Wireless Clients Report 391
Wi-Fi Events Report 392
Mesh Peers Report 393
Guest Access Login Events 394
Remote Upload 395
Reports jobs 396
Graphical Reports 397
Create Graphical Report Templates 399
Generate Reports Based on Templates 402
Provisioning 405
Software Update 405
Software Update Overview 405
Create Software Update Job 406
Device Selection 406
Device Type 406
Software Update Dashboard 406
Scheduling Software Update Job 411
Software Update while Onboarding 412
Software Update through Managed Devices 412
Device Table 413
Retry Software Update 414

Options 414
Upgrade steps 415
Software Update Jobs and Parameters 415
Abort Software Job 416
Viewing Running Jobs in header 417
cnReach Bulk Software Upgrade 417
Firmware versions (OS and Radio) 417
Bulk Upgrade 417
Upgrade Tracking 418
Fixed Wireless Configuration 419
Overview 419
Configuration Templates 419
Sample ePMP Template 419
Configuration Variables 420
Variable Usage 420
Macros 420
Variable Caching 420
Device Type-Specific Configurations 420
Device Mode restrictions 421
Variable validation 421
Sample Templates 421
Template file creation 421
Template 421
BTS and CPE Configuration 423
Configuration Template for PTP 820/850 424
NTP Configuration 426
Time Services 426
SNMP 427
Security 427
Configuration Update 428
Device Selection 428
Device Type 428
Device Table 428
Options 429
Configuration Update Steps 430
Configuration Backup 430
System level 430

Device level 432
Import Configuration Backup 433
Restore from Backup 433
Configuration Jobs 435
Configuration Update at Onboarding 436
Wi-Fi Configuration 437
Enterprise Wi-Fi AP 437
Configuring Enterprise Wi-Fi APs using Wi-Fi Profiles 438
Create an AP Group 438
Configuring 802.1X port-based authentication 456
IPv6 Support 457
Map WLANs to AP Groups 459
Lock device Configuration 460
Retrying configuration 460
Apply AP Group to Device 461
AP Group and WLAN Import/Export 462
Creating a WLAN 464
Creating an ePSK WLAN 473
Configuring Wi-Fi offloading and Passpoint 479
Access Control 483
Services 486
Pre-Defined Overrides 487
User-Defined Overrides 488
User-Defined Variables 489
Bulk Overrides 490
Management 491
Radios 491
User-Defined Variables 492
Location 495
Management VLAN 496
Radios 496
WLANs 497
Ethernet VLAN 498
User-Defined Variables 499
Synchronize (Sync) Configuration 500
Manual synchronization 500
Configuration Job Status 502

Factory Reset 502
Association ACL **504**
Overview 505
Configuring Association ACL 505
Custom Applications **506**
cnMatrix Switch Profiles **508**
Switch Groups 508
Basic 510
Management 511
Network 513
Security 517
Ports 518
User-Defined Overrides 522
Switch Group Operations 522
Auto Sync Configuration 523
Create a Configuration Job 523
Synchronize (Sync) Configuration 524
Policy Based Automation (PBA) 527
Devices 529
Port Stack 530
Port Templates 534
Port Templates Operations 536
Configuration 538
Factory Reset 542
Device Details 542
Details Overview 543
Topology 544
Port Statistics 544
Clients 545
60 GHz cnWave Network Configuration **546**
Managing E2E Network 546
Dashboard 547
Notifications 553
Configuration 553
E2E Controller 559
High Availability X 560
Links 563

Statistics 573
Reports 574
Software Update 574
Map 578
Troubleshooting 588
Changing channel or Golay for specific 60 GHz cnWave links 599
Setting the Last Resort Metric (LRM) for a cnWave 60 GHz link 602
Tools 604
Site Configuration 616
Site Dashboard 619
Node Configuration 619
PoP Node configuration 621
DN/CN Node configuration 622
PoP Node 625
Dashboard 625
Configuration 626
Links 639
Details 643
Tools 644
DN/CN Node 647
Dashboard 647
Configuration 648
JSON 651
Links 653
Tools 655
Configuring Advanced Features 658
Lock Device Configuration 658
Strict Device Password Policy 658
Auto-Provisioning 659
Creating Auto-Provisioning Rule 659
Managed Services 661
Managed Accounts 661
Overview 661
Managed Accounts 661
Accounts 662
Scope 662

Access Points 662
Managed Account Service 663
Account UI 663
Account Service Users (Administrators) 664
Account Service Users (Administrators) Roles 664
Configuring Managed Account Services 666
Enable Managed Accounts 666
Additions in the cnMaestro UI when Managed Accounts is Enabled 667
Creating Managed Account Services 668
Creating Account 669
Validating Account Users 671
Check Email for Invite 672
Create Account in Account Service 672
Login to the Accounts UI 672
Managed Account Administration 673
Overview 673
Important Points to Remember 673
System View 674
Account View 674
Account Administrator (User) View 675
Users View 675
System Dashboard 676
Account Administration 677
Device Management 677
System Onboarding 677
Device Onboarding 677
Moving a Device Between Accounts 677
Account Deletion 678
Swap 60 GHz cnWave Accounts 679
Disabling the Managed Accounts feature 680
Network Services 681
API Client 682
Overview 682
API Clients 682
RESTful API Specification 682
Authentication 682

Establish a Session 683
API Access 683
Session Expiration 683
Concurrent Access 683
Rate Limiter 684
Swagger API **686**
Introduction 686
API Session **688**
Retrieving access token 688
Renewing access tokens 689
Access resources 690
API Details **691**
HTTP Protocol 691
HTTP Response codes 691
HTTP Response codes 691
REST Protocol 691
Resource URLs 691
Responses 693
Parameters 694
Field selection 694
Filtering 695
Time Filtering 696
Sorting 696
Pagination 696
Internal Response limits 697
Access API **698**
Token (basic request) 698
Request 698
Response 698
Example 699
Token (alternate request) 699
Request 699
Response 699
Example 700
Validate Token 700
Request 700
Response 700

Example 701
API Changes **701**
Devices, Statistics, and Performance APIs **701**
Overview 701
cnMaestro v2 API 701
Devices API Response (v2 Format) 702
Supported values for onboarding state 704
Supported values for device type 705
Device onboarding failure error codes 705
Statistics API Response (v2 Format) 706
60 GHz cnWave 706
cnMatrix 707
cnReach 708
Fixed Wireless (cnVision, ePMP and PMP) 709
PTP 650/670/700 712
PTP 820/850 713
Wi-Fi 714
cnWave 5G Fixed 716
Performance API Response (v2 Format) **719**
60 GHz cnWave 719
cnMatrix 720
cnReach 721
Fixed Wireless (cnVision, ePMP and PMP) 722
PTP 650/670/700 723
PTP 820/850 724
Wi-Fi 725
cnWave 5G Fixed 726
Client API Response (v2 Format) **727**
External Guest Access Login API **728**
60 GHz cnWave RESTful API **729**
E2E Network 730
Device (Node) Configuration 731
E2E Controller 732
EasyPass **733**
Guest/Public Access 734
Combined 735
Implementation of EasyPass portals for various types of users 736

EasyPass configuration **736**
Creating a portal 737
Configuring common parameters 741
The Basic screen parameters 741
The Limits screen parameters 742
The Design screen parameters 744
The Voucher screen parameters 749
The One Click screen parameters 750
The Plans screen parameters 752
Accessing the common tabs 757
Sessions 757
Guests 758
Vouchers 759
Paid Transactions X 760
Creating One Click portal 761
Creating Self Registration X portal 761
SMS Gateway Providers 763
Creating Sponsored Guest X portal 770
Creating Voucher portal 771
Creating Paid X portal 772
Creating WiFi4EU portal 772
Importing user data using a CSV file 773
Creating One Click + Voucher portal 775
Creating One Click + Paid X portal 775
Creating Voucher + Paid X portal 776
Creating a Third-Party Integration portal 776
Creating a portal and secret key 777
Revoking and generating the secret key 778
Using the Secret Key in API Requests 779
SNMP Configuration **779**
Overview **779**
Enable SNMP **779**
Configure SNMP parameters **779**
cnMaestro MIB (Management Information Base) **780**
RADIUS Proxy **780**
Overview **781**
RADIUS Proxy Configuration 781

Citizens Broadband Radio Service (CBRS) **782**
Enabling CBRS in On-Premises 782
Share CBRS configuration to the On-Premises Instance 783
Management Tool **784**
Export 785
Relinquish Grant 785
Creating a Management Tool Sector 786
Domain Proxy View **803**
Searching a Domain Proxy Sector 804
Domain Proxy Sector view 804
Searching a Domain Proxy in Non Sector View 804
Configuring HTTP Proxy Server for CBRS and AFC Connectivity **807**
External Proxy Requirements 808
Squid as an External Proxy 808
High Availability for Squid External Proxy 809
Configuring HTTP Proxy for CBRS and AFC 809
LTE **810**
Adding SIM Cards **810**
Delete SIM Cards 811
Update SIM Details 811
Viewing BBU SIM Status 812
Managing Edge Controller **813**
Topology Sync 813
Edit 813
Delete 814
Dashboard **815**
Configuration **815**
Rules 816
Import 817
Export 818
Delete 818
Edit 818
Blacklist 819
Advanced Settings 819
Tools **820**
Diagnostics 820
Technical Support Dump 820

Logging Severity 821
Service Logs 822
Operations 823
Services 823
Monitoring 824
Installation Summary **824**
Configuration **827**
Photos and Location **827**
Link Test Result **827**
AP Scan Result **827**
Spectrum Analyzer X **828**
Administration ***834***
User Management **834**
Local Users 834
Role-Based Access 835
Role-Mappings 835
Creating Users and Configuring User Roles 837
Changing Password 838
Authentication 839
Authentication Server 839
Viewing Authentication Servers 839
Authentication Priority 840
Create New Authentication Server Configuration 841
Verifying the Role of the User 843
Show User Groups for Active Directory 844
OpenID Connect 845
SAML 846
Session Management 848
Sessions 848
Cloud Anchor Account **848**
Manage Instances **848**
Onboarding 849
On-Premises Instances 851
Notifications 851
Inventory **852**
Administration **852**

Users 853
Role-Based Access 853
Creating Users and Configuring User Roles 853
Session Management 854
Network Services 854
CBRS 854
Manage Subscriptions 854
Subscriptions 855
Devices 857
On-Prem Instances 857
Server Management 858
Monitoring 859
Settings 859
Basic 860
Configure NTP Server 860
Configure Email Server 860
Notifications 862
Login Security Banner 862
Operations 863
Reboot Virtual Machine 863
Update cnMaestro Software 863
Package Types 863
System Backup 863
Restore Backup 864
OVA Update Process 868
In-System Upgrade 868
Software Update 869
Diagnostics 870
Server Technical Support Dump 870
Logging Severity 871
Services 871
Network Tools 872
Certificate Management 872
View Certificate 873
Generate a Certificate Signing Request (CSR) 873
Import a Certificate 874
Backup Management 875

Reset 875
Managing Software Images **875**
Overview 875
Add Images 876
Delete Images 877
Update Recommended Version 878
Automatically Update Device Software 879
Webhooks X **880**
Configuring Webhooks template **880**
Supported variables 883
Error and retransmission 885
Notifications **885**
Adding a notification 886
HTML email example 889
JSON email example 889
Supported source types 889
Audit Logs **890**
Syslog **893**
Event Syslog 894
Audit Syslog 895
Firewall **896**
Enabling Firewall 896
Configuring Firewall 896
Default state 898
Appendix ***899***
Guest Access **899**
Configuration **900**
Creating the Guest Access Portal in cnMaestro 900
Basic Details 900
Access Portal 901
Configuring Additional Parameters for Guest Access Portal 909
Design Page 917
Mapping the device to Guest Access Portal in cnMaestro 922
Configuration at device level 922
Configuration at cnMaestro side 923
Access Types **924**

Guest Access using Social Login 925
Configuration 925
API Key Generation 927
Creating Google Service Account 936
Sample Template 939
Guest Access Portal Logout 939
SMS Authentication 940
Generic SMS Gateway configuration 940
Sample configuration in the cnMaestro 947
Maintenance 947
Command Line alternatives 947
Enabling TLS 1.0/TLS 1.1 948
Export cnMaestro Data 948
Import cnMaestro Data 948
Technical Support Dump 948
Apply OVA Upgrade 948
Apply Package Upgrade 949
SSH Access 949
Enabling SSH Access 949
Data Backup 951
Overview 951
cnMaestro backups 951
Full Backups 951
Virtualization System Backup Methods 952
Extending the Data Disk 953
VMware Workstation Disk Expansion 953
VirtualBox Disk Expansion 954
Partition and File System Updates 954
Account Recovery 955
Virtual Machine (Console) Account Recovery 955
cnMaestro Application Account Recovery 956
Application Account Recovery 956
Configure Network Time Protocol (NTP) 957
Disabling NTP Support 957
Anchor Account and Benefits 958
Creating a Cloud Anchor Account 958
Benefits of a Cloud Anchor Account 959

Data Security and Privacy 960
Information that is synced with the Cloud Anchor account 960
On-Premises instance information 961
Registration information 961
Onboarded device information 962
Upgrade of On-Premises from 3.1.x to 3.2.0 962
Deployments 966
VMware ESXi Installation 966
cnMaestro VM Deployment 967
Oracle VirtualBox 5 Installation 969
Deployment 969
VMWare Workstation 971
KVM Installation 972
Deployment 972
Windows DHCP 974
Configuring Option 60 975
Windows DHCP Server Configuration 975
Configuring Option 43 976
Windows DHCP Server Configuration 976
Configuring Option 15 976
Windows DHCP Server Configuration 976
Configuring Vendor Class Identifiers 977
Using DHCP Option 15 979
Configuring the Policies at the SCOPE Level 979
Citrix Hypervisor Installation 981
Resources 982
Import using Citrix Hypervisor 982
Access cnMaestro 987
SSH Access 987
HTTPS Access 988
Advanced Options 989
Expand the Data Disk 989
Expand the volume through Citrix Hypervisor 989
Expand the file system within cnMaestro 990
Network Port Requirements 991
Inbound Ports 991
Outbound Ports 991

Custom Network Scripts 992
Xirrus Migration using Tool **992**
XMS-E system 992
Export Golden Configuration 993
Claiming the Wi-Fi Devices 995
Migrate to cnMaestro X 996
Create Wi-Fi AP Group 998
Import and Apply AP configuration 999
Cambium Networks ***1002***

Introduction

cnMaestro On-Premises is a standalone network management platform that can be installed in a data center. It is distributed as a virtual machine. The on-premises functionality is nearly identical to the cloud version.

cnMaestro operates based on the subscription modes such as:

- Essentials - It is free and supports basic management functionality.
- cnMaestro X - It is paid and requires a subscription allows you to access the X features and management capabilities.

Note

Users can request a 90-day free cnMaestro X trial through the link available on the cnMaestro home page or https://www.cambiumnetworks.com/cnmaestro-x/.

This section covers the following topics:

- Supported Devices and Features
- Quick Start
- Cloud Synchronization
- UI Navigation
- Architecture
- Device Onboarding
- High Availability

Supported Devices and Features

Supported Virtualization Infrastructures

Cambium cnMaestro On-Premises is released as an Open Virtualization Archive (OVA) file.

Note

Cambium cnMaestro On-Premises is also available as an Amazon Machine Image (AMI) that can be accessed through the AWS Marketplace. For more details, visit https://aws.amazon.com/marketplace/pp/prodview-tfe6lkwozpdho.

The following table lists the platforms supported by cnMaestro:

Table 1 *Supported virtualization infrastructures*

Platform	Version
VMware ESXi	Version 6.5 Update 3 (Build 7967664) or higher (this is the preferred platform)
VMware Workstation/Player	Version 17

Hardware requirements

cnMaestro On-Premises is preconfigured with two virtual drives of approximately 120 GB total size. The image supports up to 10,000 devices including all Cambium devices listed in the Devices and minimum software versions section.

Note

- Virtual hardware is different than physical hardware.
  - Virtual hardware executes the cnMaestro application.
  - Physical hardware executes the VMware virtualization infrastructure and the cnMaestro application (and other independent applications).
- Cambium Networks recommends using a recent Intel Core i7 or Xeon CPU with the following Geekbench multi-core score:
  - 4,500 for 100 devices
  - 8,000 for 4,000 devices
  - 13,400 for 10,000 devices
  - 34,306 for 20,000 devices
  - 41,779 for 25,000 devices
- cnMaestro backend databases require CPUs which support the SSE instruction set.
- Cambium Networks recommends using an SSD drive to improve performance.
- System resources, such as vCPU and RAM must be more than the hardware requirements listed in Table 2, if the following features are used:
  - RADIUS proxy is enabled—Double the hardware requirements.
  - NBI APIs are enabled and generates multiple performance reports—1.5 times the hardware requirements.
  - cnMaestro X is enabled and includes enterprise devices (cnMatrix, Enterprise Wi-Fi)—1.5 times the hardware requirements.

The following table lists the hardware requirements supported by cnMaestro:

Table 2 *Hardware Requirements*

Number of Devices	Wireless Clients	Number of vCPUs	RAM Size (GB)	Hard Disk (GB)
1 - 100	Up to 1500	3	6	144
101 - 1,000	Up to 15,000	5	10	144
1,001 - 5,000	Up to 60,000	6	12	200
5,001 - 10,000	Up to 150,000	12	24	350
10,001 - 20,000	Up to 300,000	18	36	500
20,001 - 25,000	Up to 375,000	24	48	650

Devices and minimum software versions

Note

By default, Cambium Networks does not update device builds during OVA or package upgrades. The

user must upload device software by clicking the **Add** button in **Administration** > **Server** > **Software Images** > **Manage Software Images**. Software can also be downloaded through a cnMaestro Anchor Account.

For further information, refer to Managing Software Images.

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

Table 3 *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 (All series except the below two switches)	5.0.2-r4
cnMatrix EX3030RM-P	6.2
cnMatrix EX3052RM-P	6.2
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
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
E2E Controller	1.0.1-r2
Edge Controller	1.0.0-r1
ePMP 1000	4.5.0
ePMP 1000 Hotspot	3.3.1.2-r1
ePMP 2000	4.5.0
ePMP 3000	4.5.0
ePMP 3000L	4.5.0

Table 3 *Supported devices and minimum software versions*

Device	Minimum Software Version
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
ePMP MP 3000	4.5.0
ePMP PTP 550	4.5.0
ePMP PTP 550E	4.5.0
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

Table 3 *Supported devices and minimum software versions*

Device	Minimum Software Version
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
X7-53X	7.1.1
X7-55X	7.1.1

Table 4 *Supported Xirrus device models*

Device Model	Minimum Software Version
Wave 2 APs: • XA4-240 • XD2-230 • XD2-240 • XD4-240 • XH2-240	8.7.0
Wave 1 APs: • XD4-130 • XH2-120 • XR-630 • XR-620	8.7.0
Wave 1/2 Modular 4-radio: • XR-2436/Wave 2 • XR-2426 • XR-4436 • XR-4426 • XR-2226 • XR-2236 • XR-2247 • XR-2447 • XR-4447	8.7.0

Table 4 *Supported Xirrus device models*

Device Model	Minimum Software Version
Wave 1 Modular 8-radio: • XR-4836/Wave 2 • XR-4826	8.7.0

Supported browsers

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

Table 5 *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

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 6 *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: • 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	✔	✔

Table 6 *Features supported by cnMaestro*

Feature	Description	Cloud	On-Premises
	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).	✔	✔
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**	View the best route from a CN or 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:	✔	✔

Table 6 *Features supported by cnMaestro*

Feature	Description	Cloud	On-Premises
	• Golay • SNR • MCS • RSSI • Throughput (Mbps) • Airtime (%) • Link Fade Margin (LFM) Applicable only to 60 GHz cnWave devices.		
Custom Applications X	Configure applications with a specific IP address or a domain name, and apply filter rules.	✔	✔
Deployment—cnMaestro	The Cloud version is fully hosted and maintained by Cambium Networks at https://cloud.cambiumnetworks.com. The cnMaestro On-Premises version is released as an OVA (Open Virtualization Archive) file that needs to be installed on either VMware or VirtualBox.		✔
Device Auto Refresh X	Device Auto Refresh allows to refresh data automatically in the E2E Network.		✔
Device Connectivity	In the Cloud version, all devices can be accessed through https://cloud.cambiumnetworks.com. 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.	✔	✔
Device Image Management	In the Cloud, device images are automatically available. 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.	✔	✔
EasyPass	Create captive portal to allow clients to access the network through the following portal types: • One Click • Self Registration X • Sponsored Guest X • Voucher • Paid X	✔	✔

Table 6 *Features supported by cnMaestro*

Feature	Description	Cloud	On-Premises
	• WiFi4EU—Available only in the European Union • Third-Party Integration		
EasyPass: Combined - One-click + Voucher, One-click + PaidX, Voucher + PaidX	Create captive portal to allow clients to access the network through the following portals: • One-click + Voucher • One-click + Paid X • Voucher + Paid X	✔	✔
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: • PMP SMs • ePMP SMs • cnMatrix • Enterprise Wi-Fi APs	✔	✔
Interference Scan X	Applicable only to 60 GHz cnWave devices. 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).	✔	✔
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.	✔	✔
Link Throughput Test X	Test the throughput between the link end points. Applicable only to 60 GHz cnWave devices.	✔	✔
Local and Authentication Server Administrators	Multiple types of administration access for local administrators (with a username and password maintained by cnMaestro) or authentication services (including TACACS+ X, RADIUS X, LDAP X, Active Directory X, OpenID Connect X, and SAML X).		✔
Long Term Historical Data X	Display long-term performance graphs for the following: • Fixed Wireless Broadband up to 2 years. • Wi-Fi APs, IIoT, and cnMatrix up to 1 year.	✔	✔

Table 6 *Features supported by cnMaestro*

Feature	Description	Cloud	On-Premises
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	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:: • Managed Wi-Fi • 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	Support the following tailored account views in the cnMaestro UI: **Access and Backhaul**: Used for managing Fixed Wireless and Wi-Fi deployments, including the following: • 60 GHz cnWave • cnMatrix • 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 (ePMP 1000 Hotspot) • Enterprise Wi-Fi (Xirrus-Series) • ePMP • PMP • PON • PTP 650/670/700 • PTP 820/850	✔	✔

Table 6 *Features supported by cnMaestro*

Feature	Description	Cloud	On-Premises
	Enterprise: Used for managing Wi-Fi deployments, including the following: • cnMatrix • Enterprise Wi-Fi (E-Series and XE/XV/X7-Series) and cnPilot Enterprise APs (ePMP 1000 Hotspot) • Enterprise Wi-Fi (Xirrus-Series)		
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.	✔	✔
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.		✔
Reports **X** (Data, Graphical, and Graphical Report Template)	• Export Active Alarms, Alarm History, Audit Logs, Devices, Events, Guest Access Login Events, Mesh Peers, 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: • Super Administrator • Administrator • Operator	✔	✔

Table 6 *Features supported by cnMaestro*

Feature	Description	Cloud	On-Premises
	• 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: • **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.		✔
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.	✔	✔

Table 6 *Features supported by cnMaestro*

Feature	Description	Cloud	On-Premises
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.	✔	✔

On-Premises Quick Start

Installation

The default passwords for cnMaestro are:

Table 7 *Default passwords*

Component	Username/Password
cnMaestro UI	admin/admin
Virtual Machine Console	cambium/cnmaestro

Note

Please change your passwords after logging in for the first time.

Virtualization

On-Premises supports two types of virtualization:

- Desktop virtualization
- Bare metal hypervisor

Desktop virtualization

Desktop virtualization executes within an existing operating system environment (Windows, Mac, or Linux). The virtualization software (such as VMware Workstation or Oracle VirtualBox) executes in tandem with other desktop applications. cnMaestro can be installed as a virtual machine on one of these platforms.

The desktop environment is the easiest way to get cnMaestro up-and-running quickly. You can download a trial version of VMware Workstation Player from VMware.

Bare metal hypervisor

A bare metal hypervisor takes over the entire physical machine and uses it to host virtual instances. This type of virtualization is best for production environments, but takes time to set up correctly. VMware vSphere Hypervisor (ESXi) is an example of this type of virtualization, and it is discussed in detail in Deployments. More information on vSphere is available at https://www.vmware.com/products/cloud-infrastructure/vsphere.

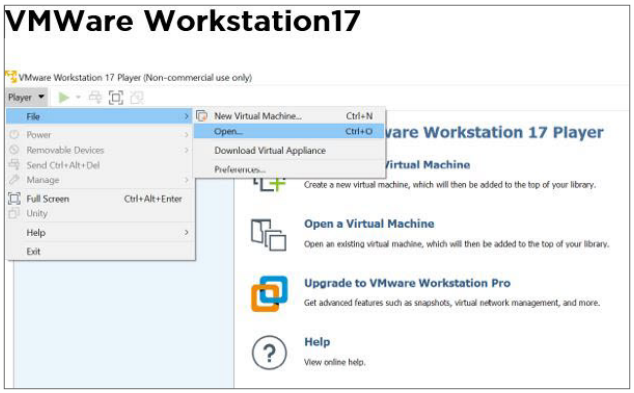
cnMaestro deployment

This document describes cnMaestro deployment using VMware Workstation Player. Directions for VMware vSphere ESXi and VirtualBox are found in Deployments. VMware Workstation Player (and Oracle VirtualBox) are the easiest to install and evaluate, and ESXi is preferred for production.

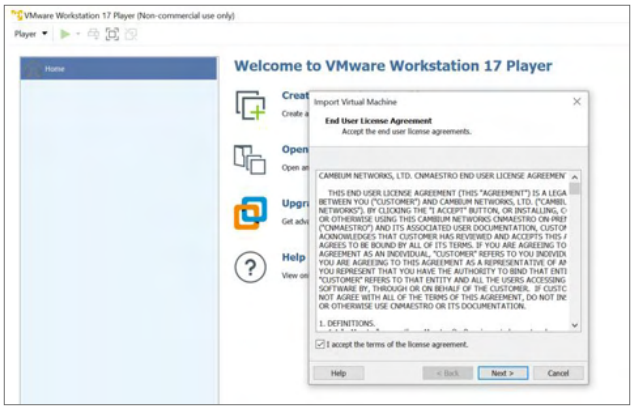
VMware Workstation Player

Follow the steps below to import cnMaestro On-Premises into VMware Workstation Player:

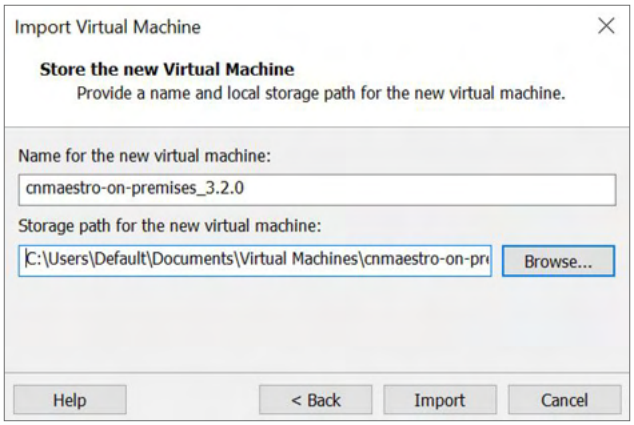
1. Download the cnMaestro On-Premises OVA file from Cambium Support Center.
2. Open VMware Workstation Player and navigate to **Player** > **File** > **Open**. Import the cnMaestro OVA.



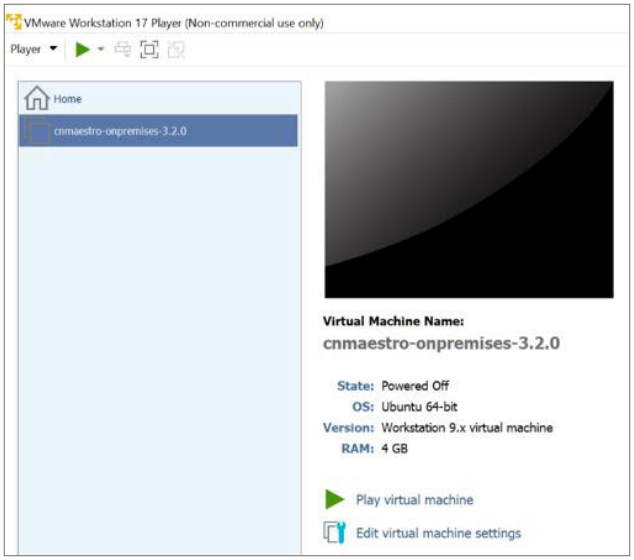
3. Accept the cnMaestro EULA.



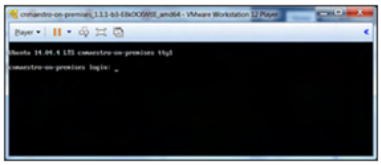
4. Click **Import** to start the deployment. This process could take a couple of minutes.



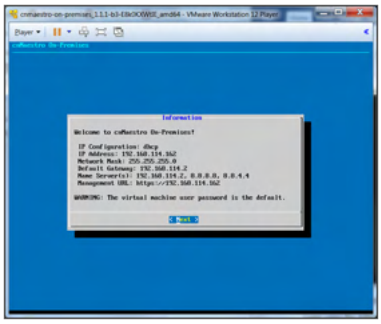
5. Click **Play** to start the Virtual Machine.



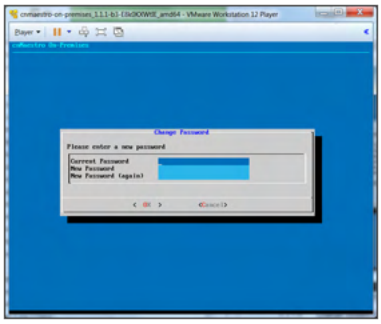
6. Login to the cnMaestro Console using the default username and password (cambium/cnmaestro). The Console is the primary way to access the cnMaestro CLI (Command Line Interface).



7. The **Information** page displays the current network settings.



8. Click **Next** and navigate to the **Password** page to update the password.

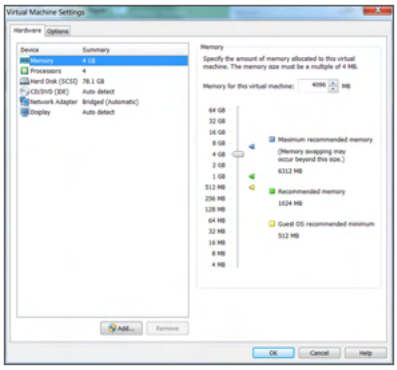


Update virtual machine hardware

cnMaestro by default is configured to use 2 CPUs, 4 GB memory, and NAT. To change these parameters, you should stop the virtual machine, update the virtual machine settings in VMware, and then restart. Click **Edit Virtual Machine Settings** from the VMware home screen. From there you can update the virtual hardware.

Note

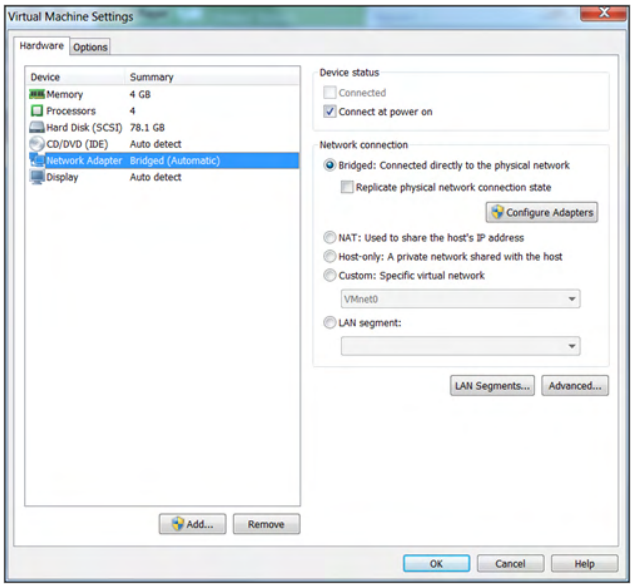
If you are evaluating more than 100 devices, we recommend to use at least 4 GB of memory and 4 processors.



Configure network adapter

By default, cnMaestro acquires its IP address from a DHCP Server. With desktop virtualization, the DHCP server is in a private network localized in the host device, and therefore the IP address of cnMaestro will not be accessible from the external LAN. VMware should instead be configured so the virtual machine network interface is shared with the device.

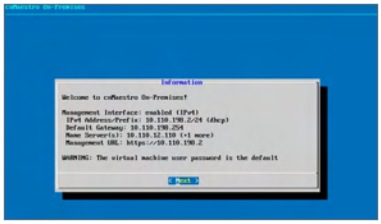
1. In the VMware settings, select **Bridged** for the Network Adapter state and select the **Network Adapter** > **Configure Adapter** to choose the external LAN adapter**.**



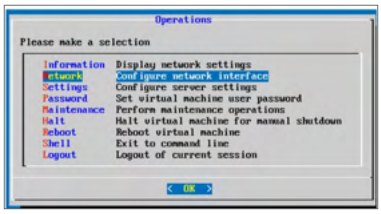
2. Restart cnMaestro.

Configure cnMaestro networking

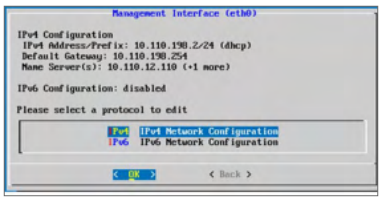
1. After logging back in, the **Information** page displays the IP address from the LAN instead of the private network.



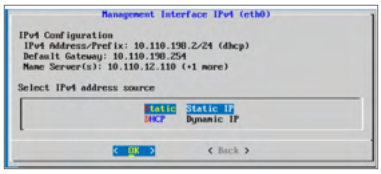
2. Click **Next** to view the **Operations** menu and select **Network.**



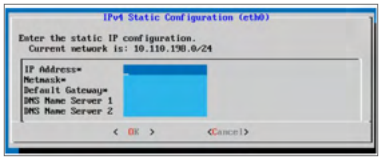
3. The **Management Interface (eth0)** window appears.



4. Select **IPv4** then **Static** to configure a static IP address.



5. Set **IPv4 Static Configuration** parameters.



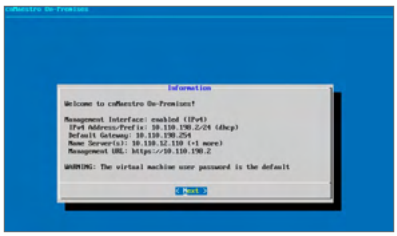
Network configuration

By default, cnMaestro is configured with a single eth0 interface. You can extend this to support a second eth1 interface for control (device) traffic. Details for configuring two interfaces are specified later in this document.

Single interface (eth0)

Name	Interface	Details
Management/Cluster/Device	eth0	User interface, cluster, API, device controller traffic.

Validate the changes. You can validate your update by navigating back to the **Information** page and viewing the current network configuration.



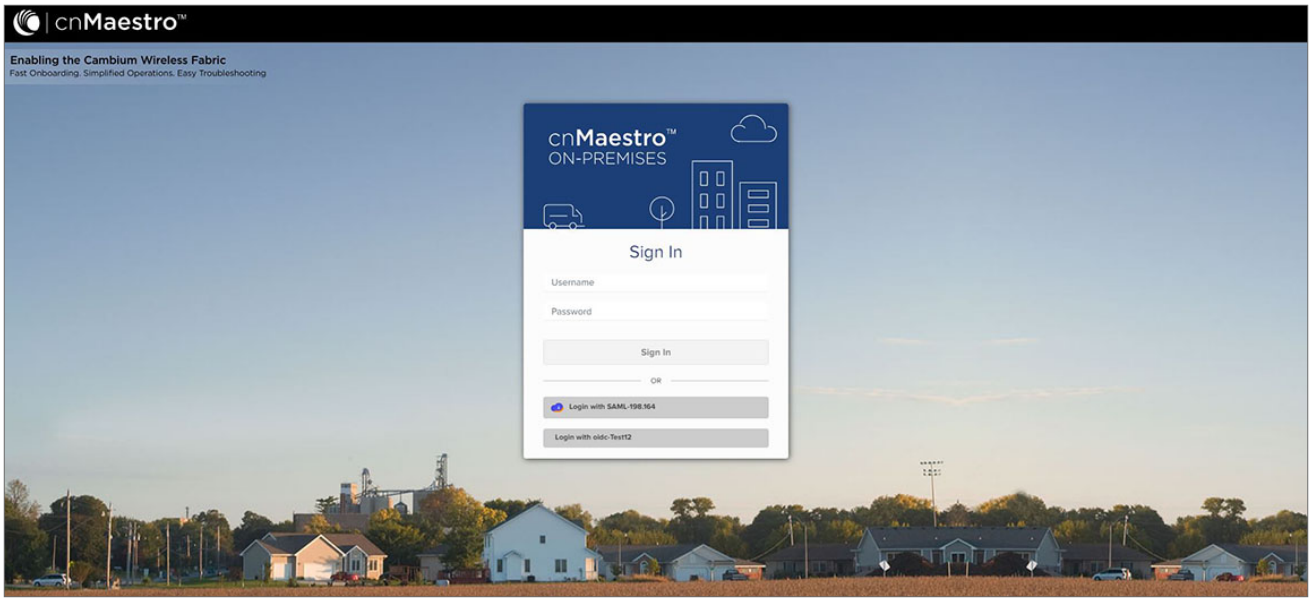
cnMaestro UI access

Access the UI using the **Management URL** specified in the **Information** page.

The default username and password is admin/admin.

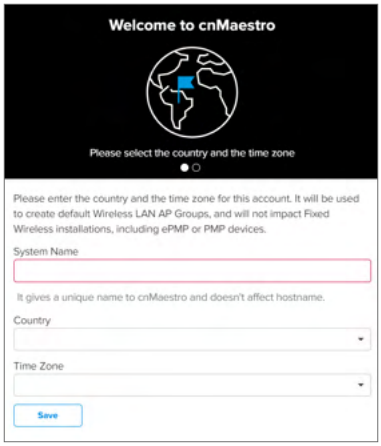
Note

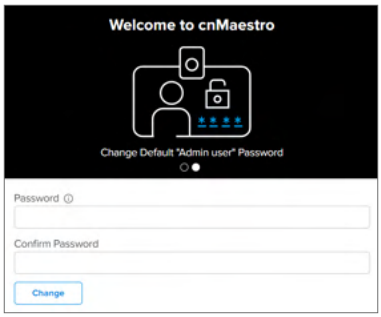
The browser displays an untrusted certificate error when you access Cambium cnMaestro On-Premises. This is because it uses a self-signed certificate. You can upload your own Root CA and Signed Certificates to suppress the error.



First login

1. Upon first login, cnMaestro will request initial configuration and require changing the default password.



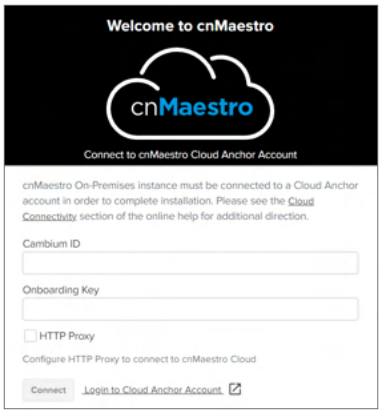


User should connect the On-Premises instance to a cnMaestro Cloud account using an Anchor account. For more details, refer to Cloud Connectivity.

Perform the following steps to connect to the Cloud account:

1. Enter the **Cambium ID** and **Onboarding Key**.

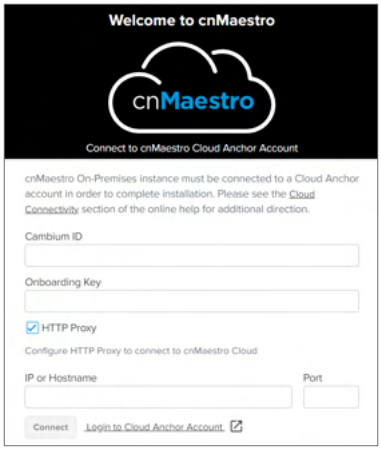
   To obtain the Cambium ID and the onboarding key, refer to Cloud Connectivity.



2. Select **HTTP Proxy.**

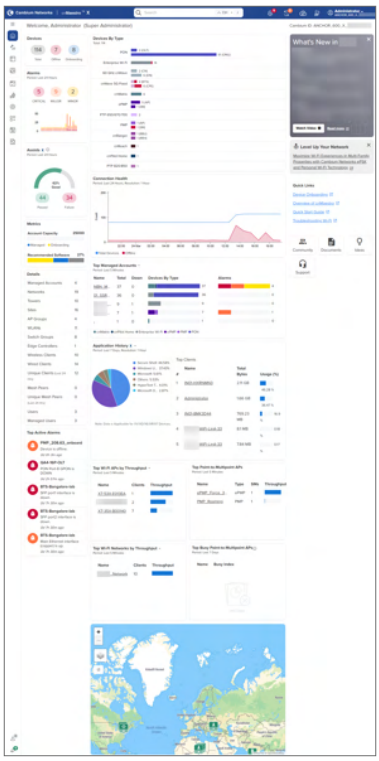
   Configure HTTP Proxy to connect to cnMaestro Cloud.

3. Enter **IP** or **Hostname.**
4. Enter **Port** number.
5. Click **Connect.**



After the Cloud Connectivity of On-Premises with Cloud Anchor account, it displays the home page as shown in Figure 1.

Figure 1 *Home page*



Cloud Synchronization

Cloud synchronization allows the user to connect On-Premise instances to a Cloud Anchor account to manage and monitor the On-Premises instances.

Cloud Anchor account

Cloud Anchor accounts manage On-Premises cnMaestro X subscriptions and Inventory details. They also simplify CBRS provisioning and billing by aggregating multiple On-Premises instances and automatically push announcements of new device firmware and cnMaestro software images.

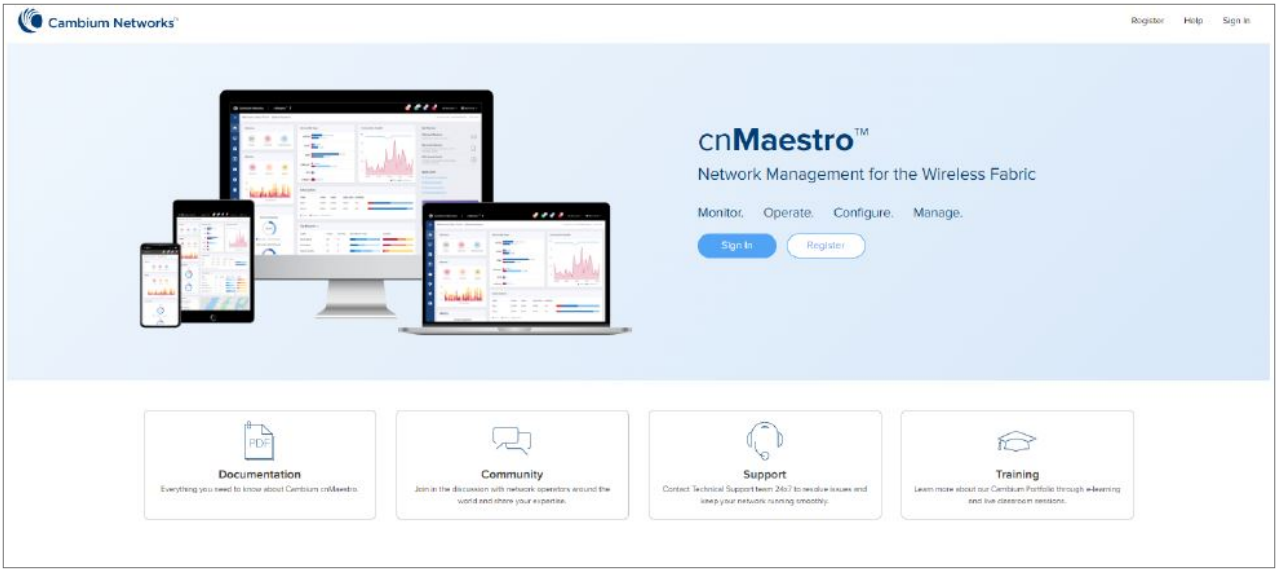
This topic contains the following sections:

- Creating Cloud Anchor account
- Cloud Anchor account cnMaestro X activation
- Cloud Anchor account features

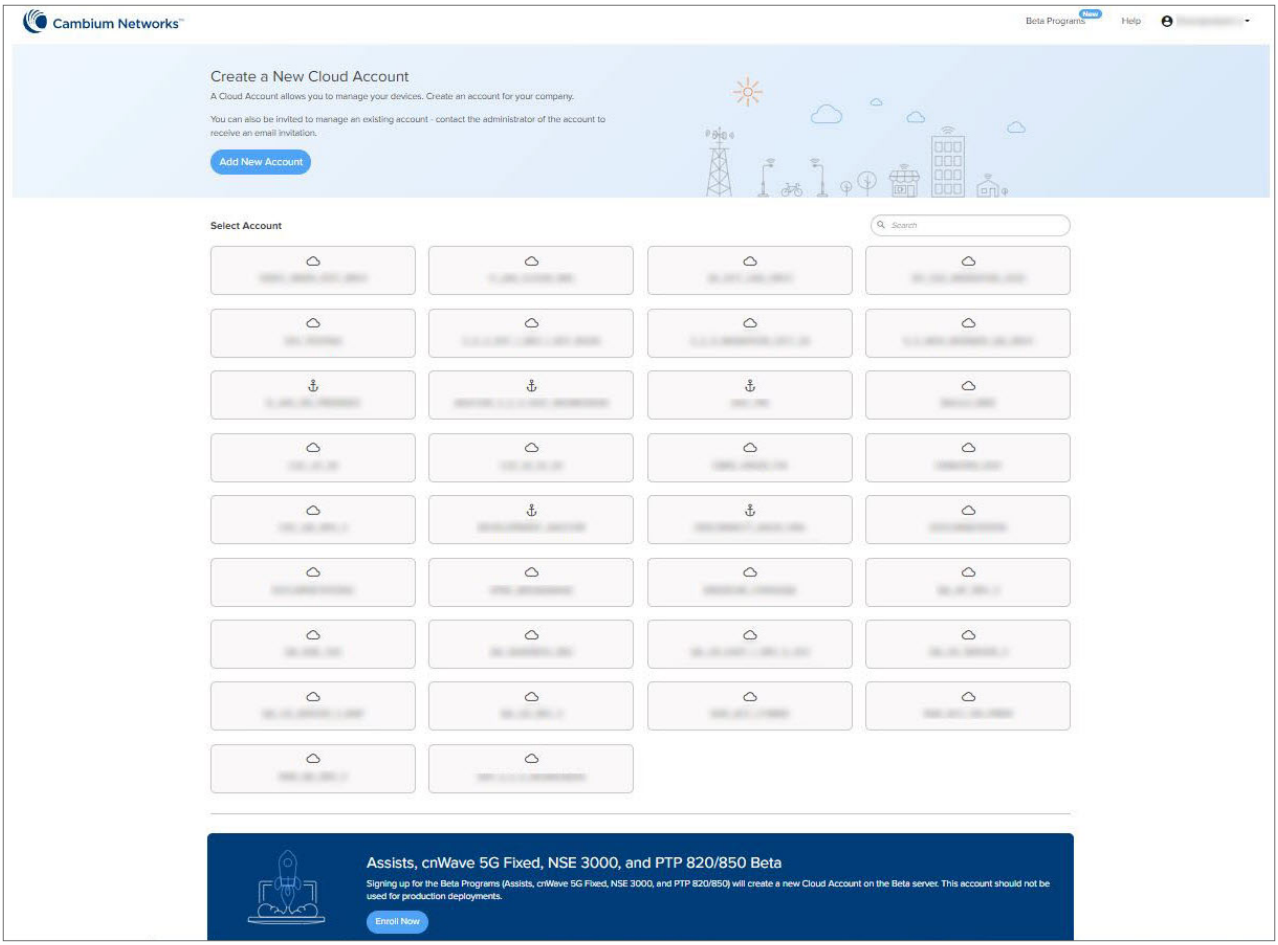
Creating Cloud Anchor account

You must create a Cloud Anchor account before connecting the On-Premises Instance, as shown below:

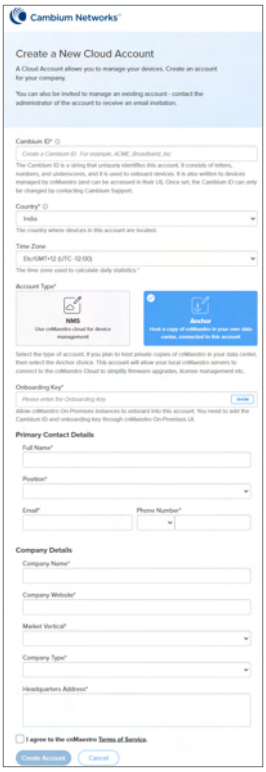
1. Navigate to https://cloud.cambiumnetworks.com and click **Sign In**.



2. Enter the **Email address** and **Password**.
3. Click **Sign In.**
4. Click **Add New Account**.



5. **Create a New Cloud Account** page pops up.

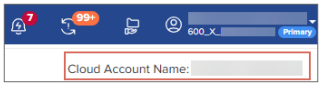


6. Enter the required details as described below:

Table 8 *Anchor account type 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 **Anchor** to install cnMaestro On-Premises.
Onboarding Key	Key required to onboard cnMaestro On-Premises instances in to this Cloud Anchor account. You must enter this key and the Cambium ID in the respective cnMaestro On-Premises instances UI to onboard to this Cloud Anchor account.
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.

Table 8 *Anchor account type fields*

Parameter	Description
	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.

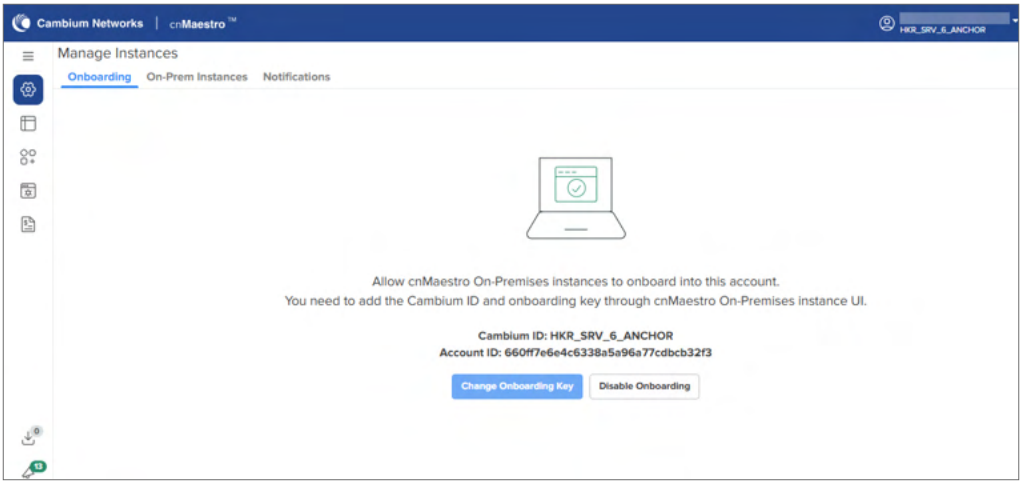
Note

The **Cambium ID** is the primary identifier of the account. It may optionally be used to onboard devices.

7. Enter details such as **Cambium ID**, **Friendly Name**, **Country**, and **Time Zone.**
8. Select the **Account Type** as **Anchor**.
9. Enter the **Onboarding key**.
10. Enable **I agree to the cnMaestro Terms of Service**.
11. Click **Create Account**.

    A new Cloud Anchor account will be created with Essentials as shown in Figure 2.

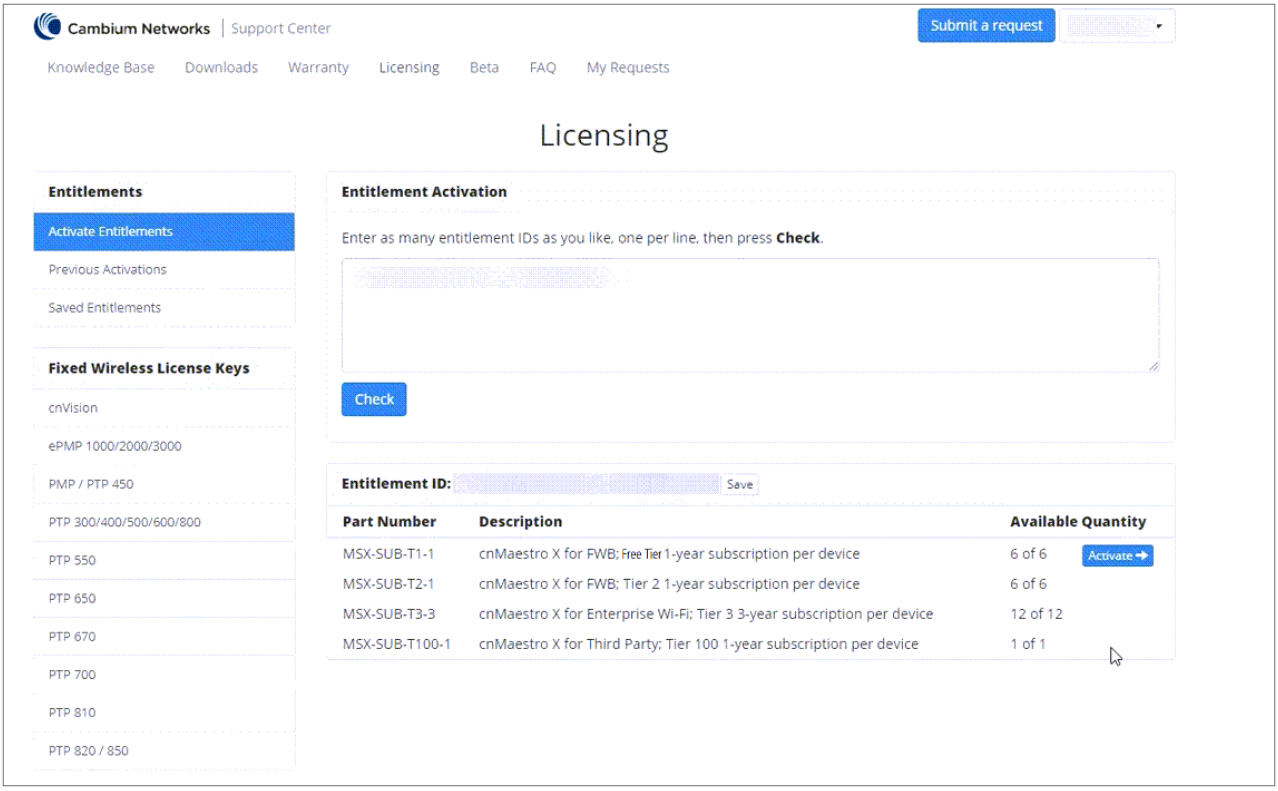
Figure 2 : *Cloud Anchor account*



Cloud Anchor account cnMaestro X activation

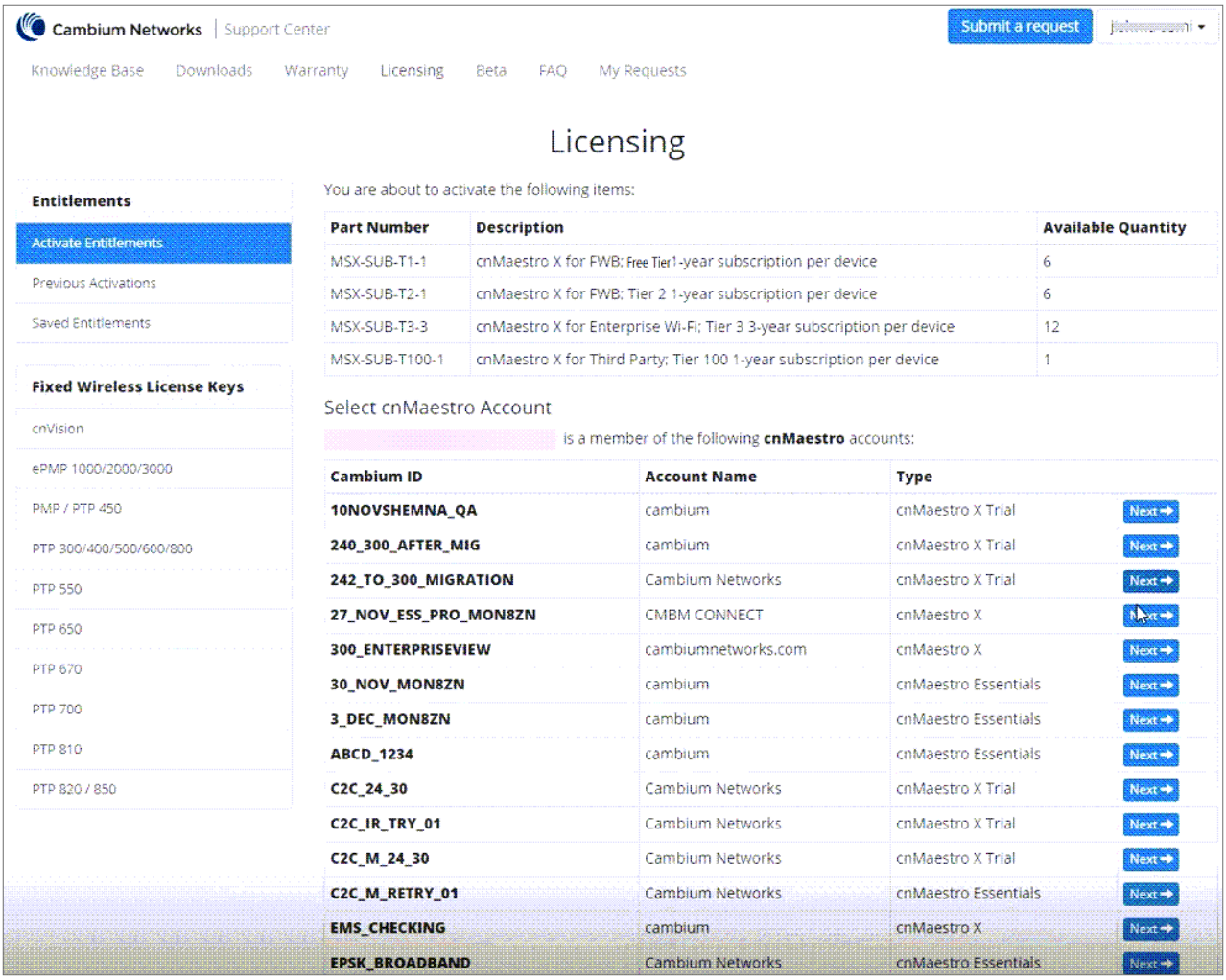
To activate the cnMaestro X account for Cloud Anchor account, perform the steps below:

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.**

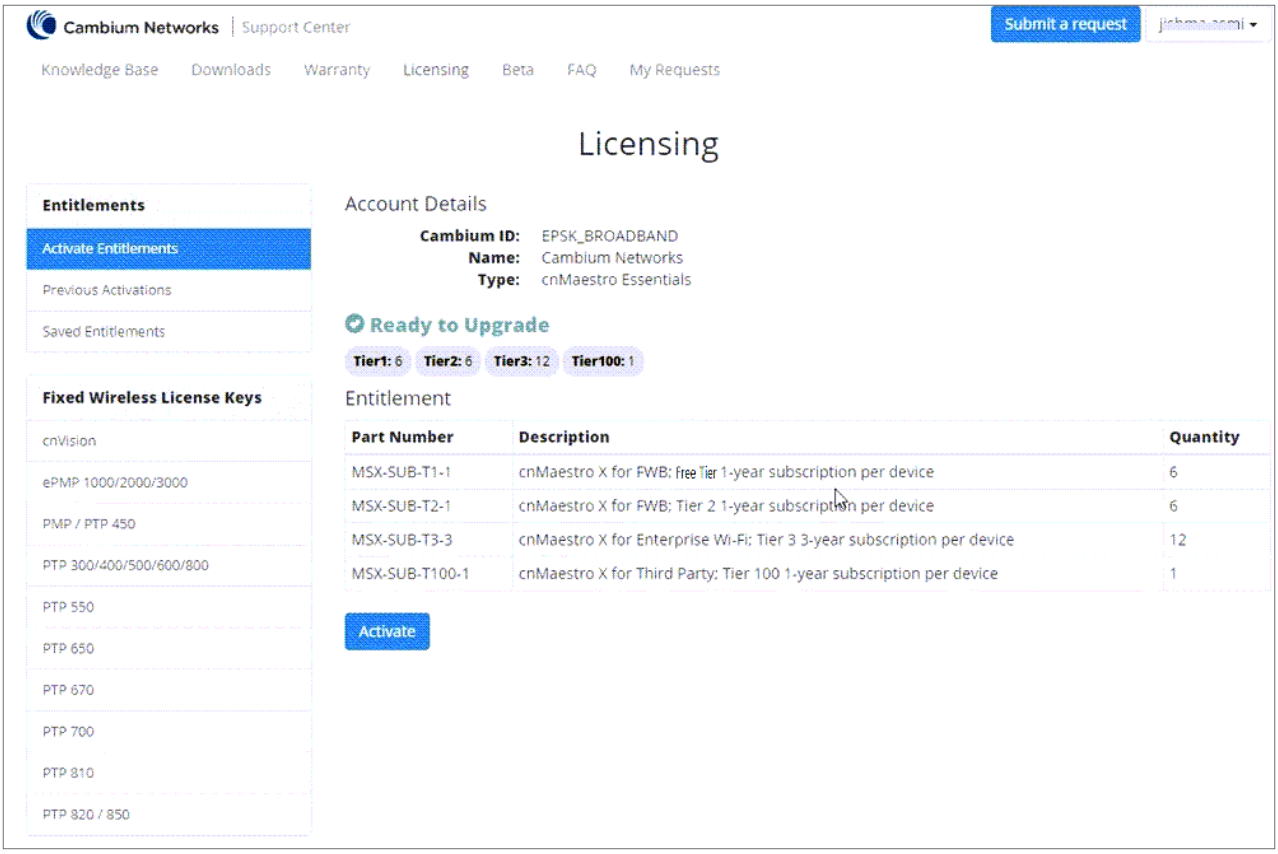


5. Once the **Entitlement ID** is validated, the **Activate** button is enabled.

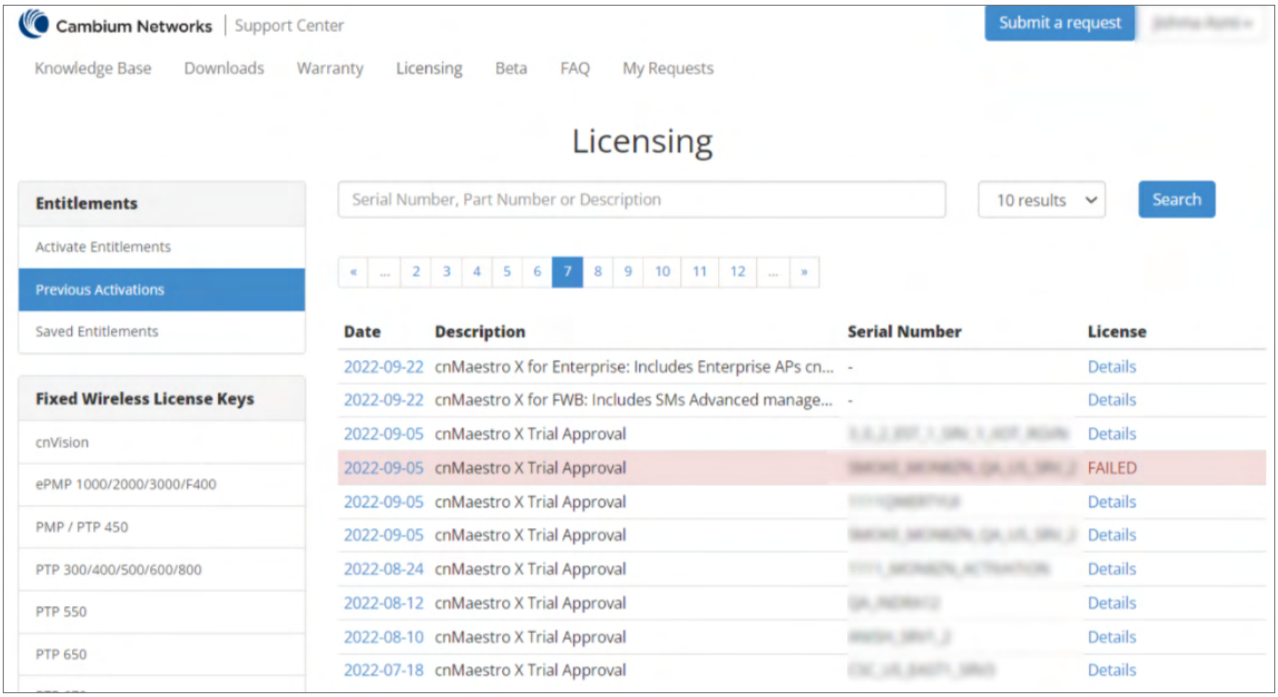
6. Click **Activate**.
7. Select the Cambium ID from the list and click **Next.**



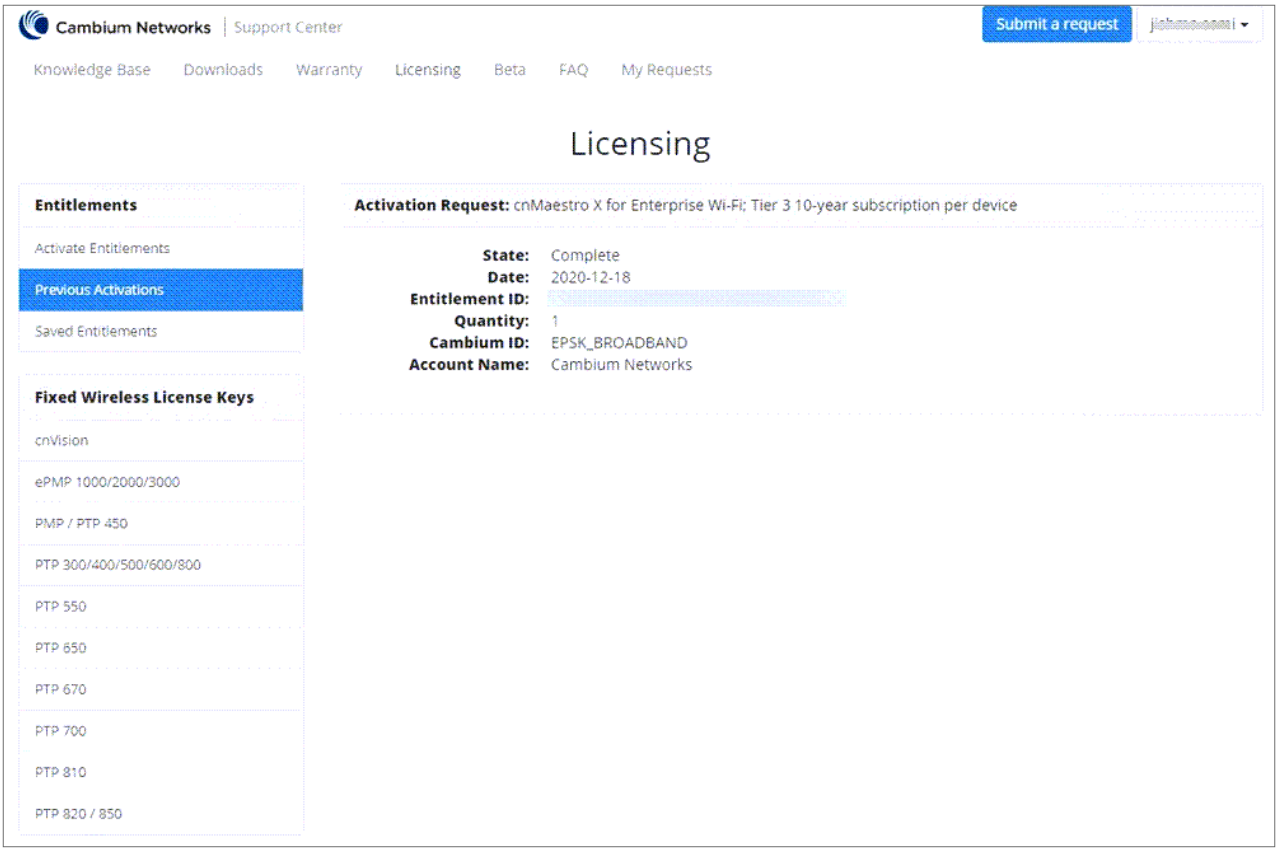
8. The **Ready to Upgrade** page displays.



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



11. Click **Details** to view the license description.



The Subscription is activated with the number of requested slots.

On the Cloud Anchor account page, a notification banner will be displayed after a successful upgrade, and the user needs to wait for 15 minutes.

Cloud Anchor account features

Table 9 lists the Cloud Anchor account features supported between the Essentials and cnMaestro X.

Table 9 *Primary features supported by Cloud Anchor account*

Feature	Description	cnMaestro Essentials	cnMaestro X
Administration	Allows to invite others to manage this account.	✔	✔
Audit Logs	Displays the audit logs.		✔
Manage Instances	Displays the monitoring details of the devices connected to On-Premises.	✔	✔
Manage Subscriptions	Provides usage summary and break-up of slots usage of On-Premises instances.		✔
Network Services	Enables CBRS management.		✔
Notifications	Provides Cloud Anchor account events and On-Premises connectivity details.	✔	✔
Session Management	Supports viewing and termination of cnMaestro administrator sessions.		✔
Jobs	View delete status of devices and On-Premises instances.	✔	✔

When the On-Premises account is connected with Cloud Anchor account, it collects limited On-Premises statistics and automatically pushes announcements of new device firmware and software images.

Following are the Cloud Anchor account features:

- Manage Instances
- Notifications
- Inventory
- Administration
- Network Services
- Manage Subscriptions

Manage Instances

This section describes:

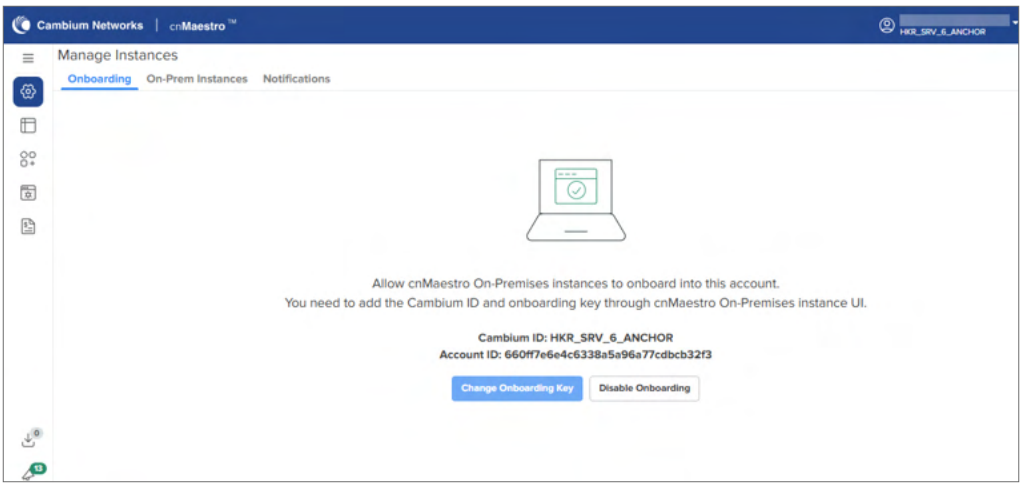
- Onboarding
- On-Premises instances
- Disable Onboarding

Onboarding

Onboarding page allows the user to modify the onboarding key and disable/enable a fresh On-Premise connections.

To edit the Onboarding Key, perform the following steps:

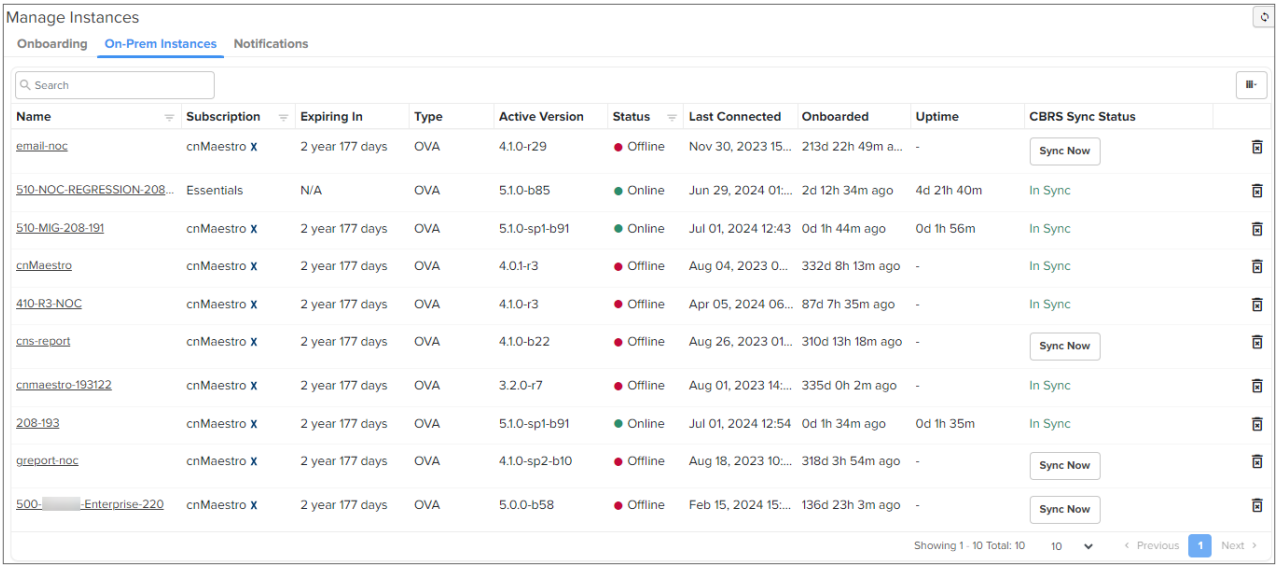
1. Navigate to the **Manage Instances** page and click **Change Onboarding Key**.



2. The **Change Onboarding Key** window is displayed.

3. Enter **Onboarding Key** and click **Save**.

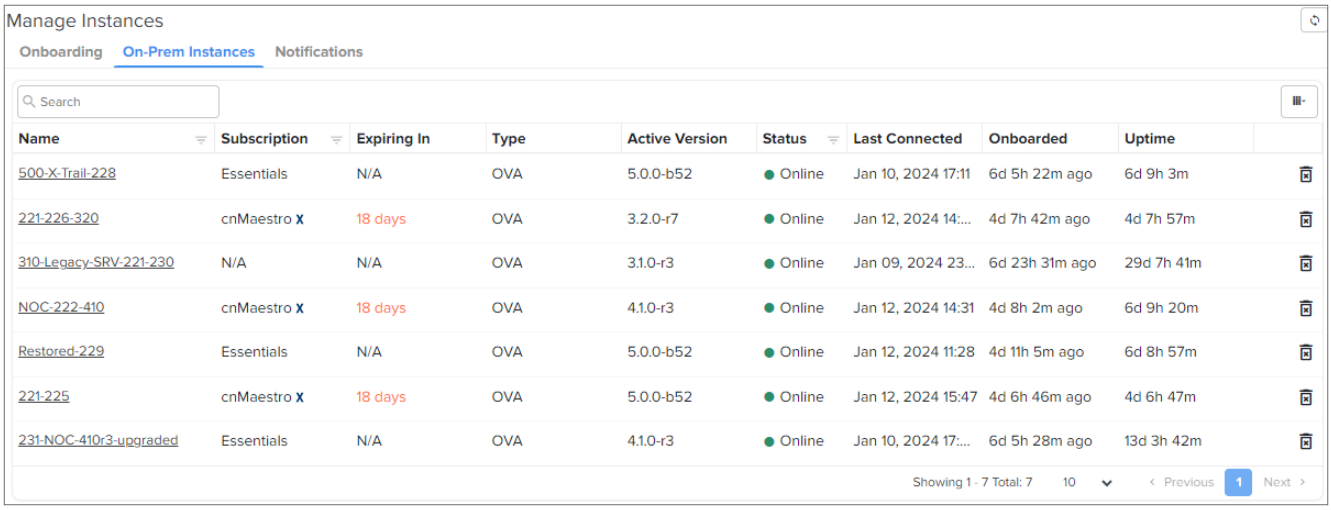
4. Once the On-Premises instances onboards, the **On-Premises Instances** page lists all the connected On-Premises instances in the account.



Name	Subscription	Expiring In	Type	Active Version	Status	Last Connected	Onboarded	Uptime	CBRS Sync Status
email-noc	cnMaestro X	2 year 177 days	OVA	4.1.0-r29	Offline	Nov 30, 2023 15...	213d 22h 49m a...	-	Sync Now
510-NOC-REGRESSION-208...	Essentials	N/A	OVA	5.1.0-b85	Online	Jun 29, 2024 01:...	2d 12h 34m ago	4d 21h 40m	In Sync
510-MIG-208-191	cnMaestro X	2 year 177 days	OVA	5.1.0-sp1-b91	Online	Jul 01, 2024 12:43	0d 1h 44m ago	0d 1h 56m	In Sync
cnMaestro	cnMaestro X	2 year 177 days	OVA	4.0.1-r3	Offline	Aug 04, 2023 0...	332d 8h 13m ago	-	In Sync
410-R3-NOC	cnMaestro X	2 year 177 days	OVA	4.1.0-r3	Offline	Apr 05, 2024 06...	87d 7h 35m ago	-	In Sync
cns-report	cnMaestro X	2 year 177 days	OVA	4.1.0-b22	Offline	Aug 26, 2023 01...	310d 13h 18m ago	-	Sync Now
cnmaestro-193122	cnMaestro X	2 year 177 days	OVA	3.2.0-r7	Offline	Aug 01, 2023 14:...	335d 0h 2m ago	-	In Sync
208-193	cnMaestro X	2 year 177 days	OVA	5.1.0-sp1-b91	Online	Jul 01, 2024 12:54	0d 1h 34m ago	0d 1h 35m	In Sync
greport-noc	cnMaestro X	2 year 177 days	OVA	4.1.0-sp2-b10	Offline	Aug 18, 2023 10:...	318d 3h 54m ago	-	Sync Now
500-[redacted]-Enterprise-220	cnMaestro X	2 year 177 days	OVA	5.0.0-b58	Offline	Feb 15, 2024 15:...	136d 23h 3m ago	-	Sync Now

On-Premises instances

Once the On-Premises instances have been onboarded with the Key, they will be included in the **On-Prem Instances** page. Multiple On-Premises installations can be managed through a single Cloud Anchor account.



Name	Subscription	Expiring In	Type	Active Version	Status	Last Connected	Onboarded	Uptime
500-X-Trail-228	Essentials	N/A	OVA	5.0.0-b52	Online	Jan 10, 2024 17:11	6d 5h 22m ago	6d 9h 3m
221-226-320	cnMaestro X	18 days	OVA	3.2.0-r7	Online	Jan 12, 2024 14:...	4d 7h 42m ago	4d 7h 57m
310-Legacy-SRV-221-230	N/A	N/A	OVA	3.1.0-r3	Online	Jan 09, 2024 23...	6d 23h 31m ago	29d 7h 41m
NOC-222-410	cnMaestro X	18 days	OVA	4.1.0-r3	Online	Jan 12, 2024 14:31	4d 8h 2m ago	6d 9h 20m
Restored-229	Essentials	N/A	OVA	5.0.0-b52	Online	Jan 12, 2024 11:28	4d 11h 5m ago	6d 8h 57m
221-225	cnMaestro X	18 days	OVA	5.0.0-b52	Online	Jan 12, 2024 15:47	4d 6h 46m ago	4d 6h 47m
231-NOC-410r3-upgraded	Essentials	N/A	OVA	4.1.0-r3	Online	Jan 10, 2024 17:...	6d 5h 28m ago	13d 3h 42m

By clicking the On-Premises instance host name, you can see the details of the On-Premises instances such as **General, Features**, **System**, and **CBRS** as shown in Figure 3.

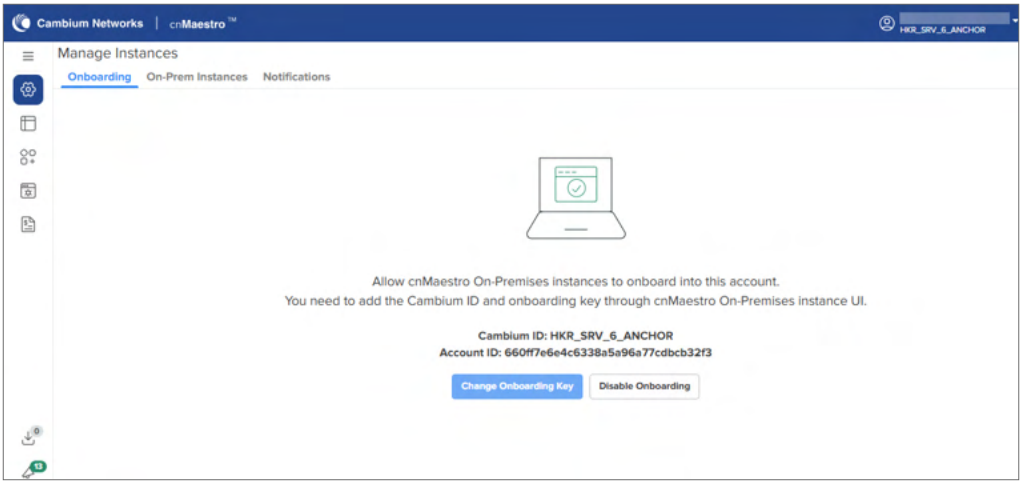
Figure 3 : *On-Premises Instances details*

Disable Onboarding

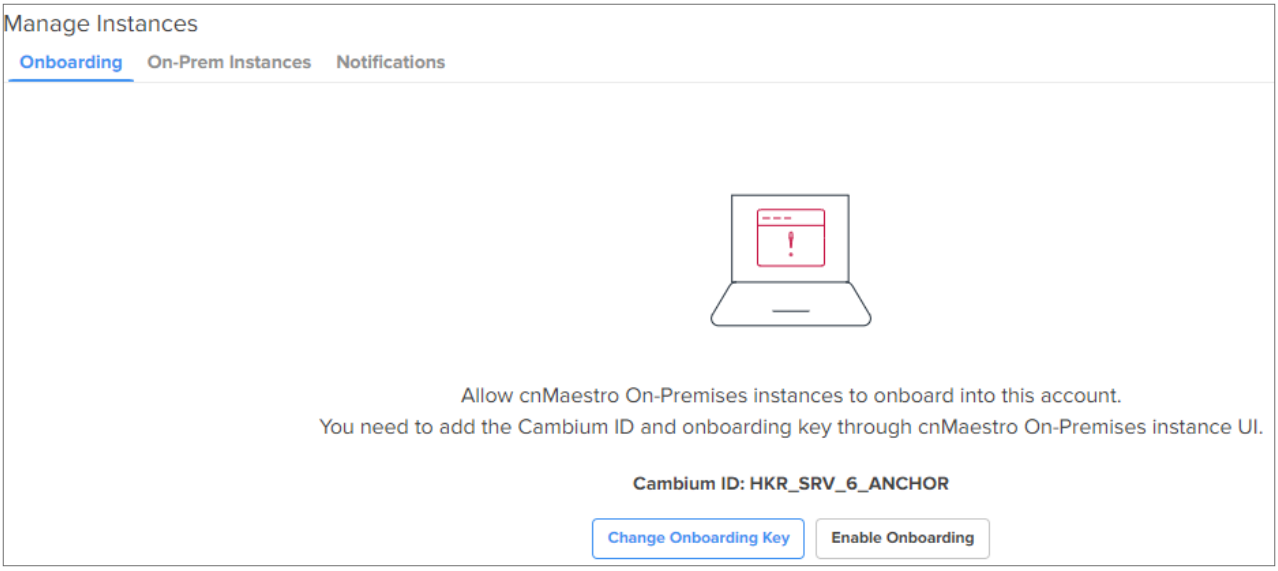
When the user do not want to onboard any extra On-Premises instances can configure the disable onboarding. It will not impact any existing onboarded On-Premises instances.

To disable the Onboarding Key, perform the following steps:

1. Navigate to the **Manage Instances** page > **Onboarding** tab and click **Disable Onboarding**.



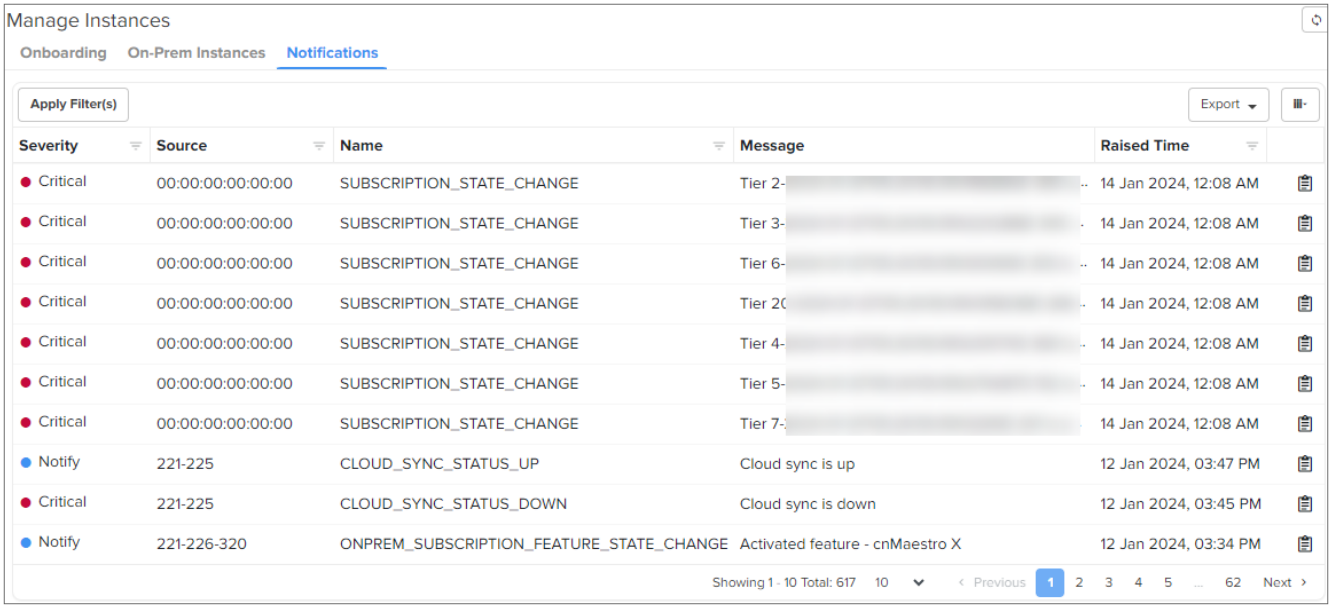
1. On-Premises instances onboarding will be disabled.



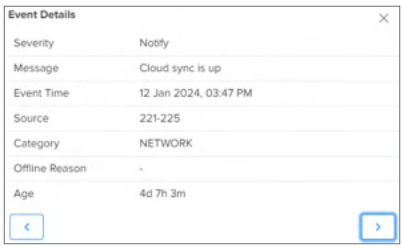
1. Click **Enable Onboarding** to onboard the On-Premises instances when required.

Notifications

Notification page displays the history of the most recent events of Cloud synchronization and subscriptions with **Severity**, **Source**, **Name**, **Raised Time**, and **Message**.

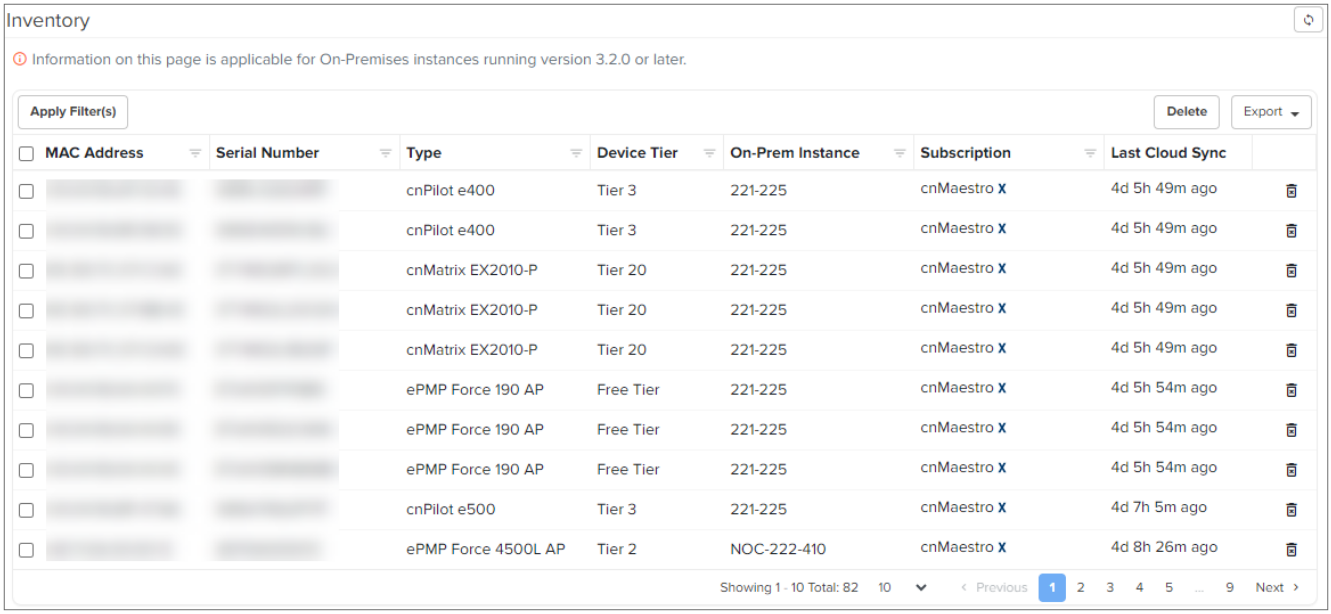


Click the view details icon to view the Event Details as shown below:



Inventory

The **Inventory** page displays a list of devices of On-Premises instances 3.2.0 or above under the selected Cloud Anchor account with tier and subscription details.



Administration

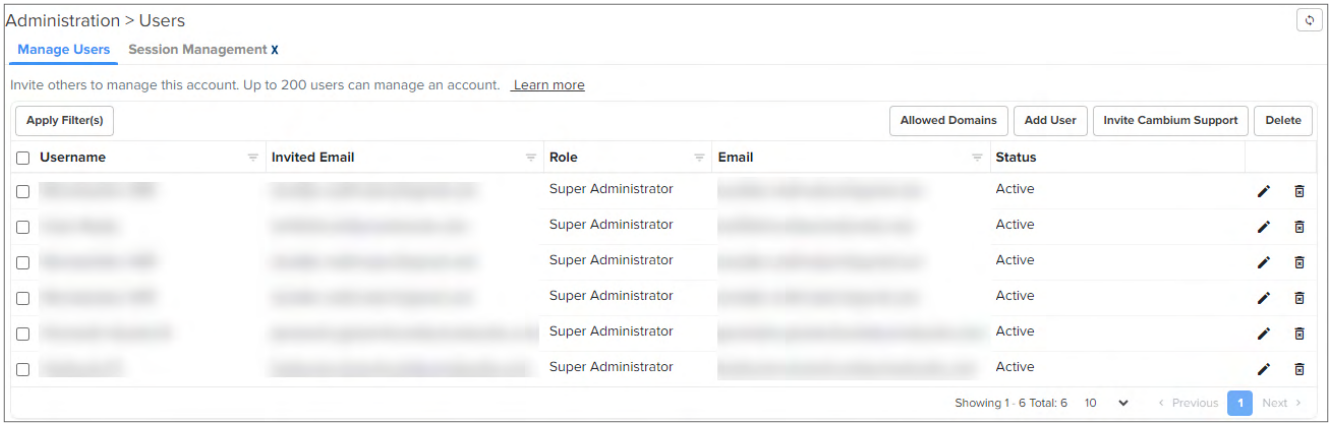
Administration provides the following details:

- Users
- Settings
- Audit Logs

Users

Cloud Anchor account allows to add Users using the **Administration** > **Users** page.

Figure 4 *Adding Users*

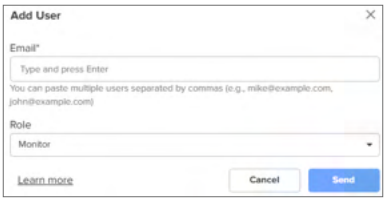


On successful authentication of every request from the user and an E-mail invitation will be sent to the users.

Creating Users and Configuring User Roles

To add an administrator:

1. Navigate to **Administration > Users** page.
2. Click **Add User** button. The Add User window is displayed.



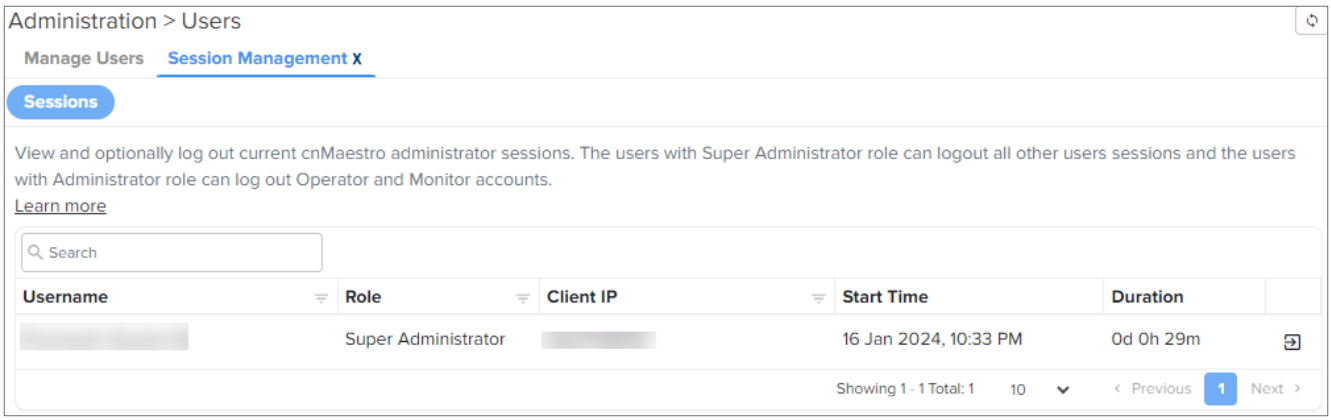
3. Enter the email address in the **Email** box.

   You can invite multiple users simultaneously either by individually entering the email IDs in the text box and pressing Enter after each entry, or by copying and pasting the email IDs as a comma-separated list.

4. Click **Send**.

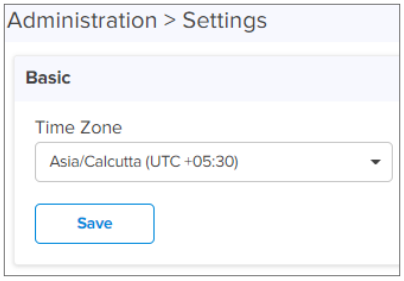
Session Management

Session Management lists the current cnMaestro administrator sessions. The users with the Super Administrator role can log out of all other users sessions.



Settings

The **Basic Settings** page allows you to select the time zone from the dropdown. Based on the selected time zone all the time based subscription activities are configured accordingly.



Audit Logs

Audit Logs records the user activities. Users can access Audit Logs in the **Administration** > **Audit Logs** page.

Administration > Audit Logs x

Export

Result	Time	Type	Module	Acti...	Source	IP Address	Description
Success	16 Jan 2024, 10:45 PM	Provisioning	Onboard	Edit			On-Prem onboarding enabled
Success	16 Jan 2024, 10:44 PM	Provisioning	Onboard	Edit			On-Prem onboarding disabled
Success	16 Jan 2024, 10:33 PM	Security	Administrator	Login			logged in successfully
Success	13 Jan 2024, 03:26 PM	Security	Administrator	Logout			session logout operation performed by succe...
Success	13 Jan 2024, 03:26 PM	Security	Administrator	Logout			logged out
Success	13 Jan 2024, 10:57 AM	Security	Administrator	Logout			logged out
Success	13 Jan 2024, 10:57 AM	Security	Administrator	Logout			session logout operation performed by successful
Success	12 Jan 2024, 05:07 PM	Operations	Device	Delete	On-prem Administrator	N/A	Device deletion succeeded for MAC -
Success	12 Jan 2024, 05:07 PM	Operations	Device	Delete	On-prem Administrator	N/A	Device deletion succeeded for MAC -
Success	12 Jan 2024, 05:07 PM	Operations	Device	Delete	On-prem Administrator	N/A	Device deletion succeeded for MAC -

Showing 1 - 10 Total: 666 10 ‹ Previous 1 2 3 4 5 ... 67 Next ›

Network Services

Network Services provide the following details:

- CBRS
- Organization

Citizens Broadband Radio Service (CBRS)

CBRS subscription for the CBRS-compliant devices in 3.6 GHz band (3550 MHz to 3700 MHz).

For further information, refer to Configuring HTTP Proxy Server for CBRS and AFC Connectivity.

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.

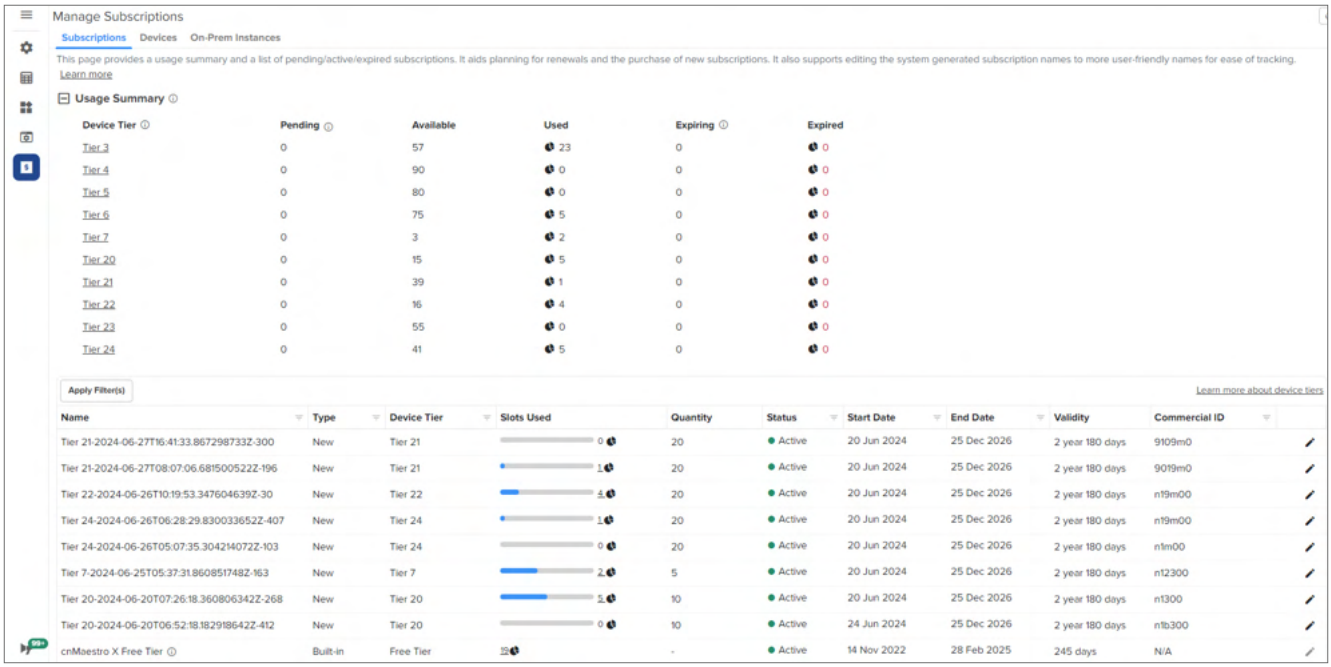
Manage Subscriptions

Manage Subscriptions provide the following details:

- Subscriptions
- Devices
- On-Prem Instances

Subscriptions

Subscriptions page describes the usage summary and a list of pending, active, and expired subscriptions and On-Premises instances allotted. It aids in planning for renewals and the purchase of new subscriptions.

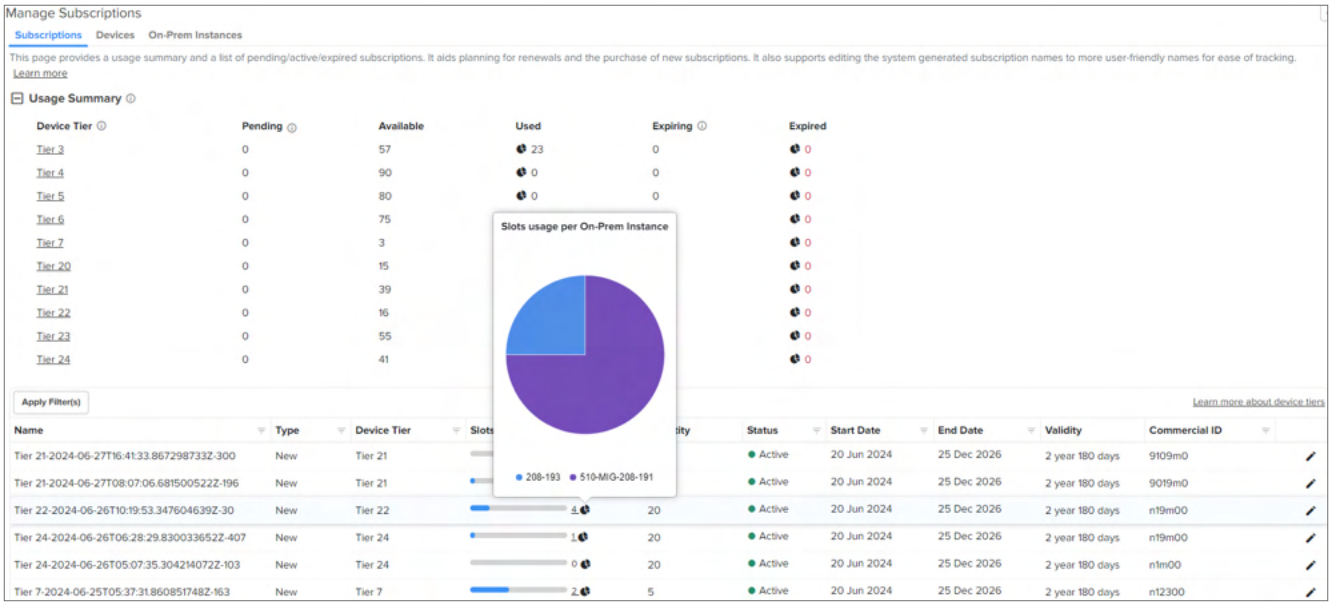


The **Manage Subscriptions** page displays the following parameters:

Table 10 *Subscription parameters*

Parameters	Description
Name	Device tier name.
Type	Displays the subscriptions type such as: • Built-in • Evergreen • New • Renewal • Trial
Device Tier	Type of device tier.
Slots Used	Number of slots used in usage per On-Premises instances.
Status	Displays the status such as: • Active • Expired • Pending • Terminated Click on the status device number to view the particular devices list.
Start Date	Displays the start date of the subscriptions.
End Date	Displays the end date of the subscriptions.
Validity	Displays the total validity of the subscriptions from the current date in year and days.
Commercial ID	Commercial ID used for the subscriptions.

To view the slot usage per On-Premises instance, click the view slot usage ( ) icon:

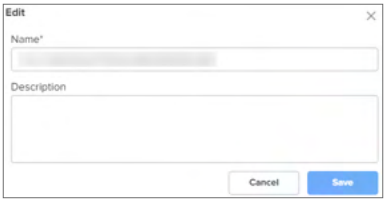


It also supports editing the system generated subscription names to more user-friendly names for ease of tracking.

To edit the **Subscriptions**, perform the following steps:

1. Click the edit (✎) icon.

   The **Edit** window is displayed.

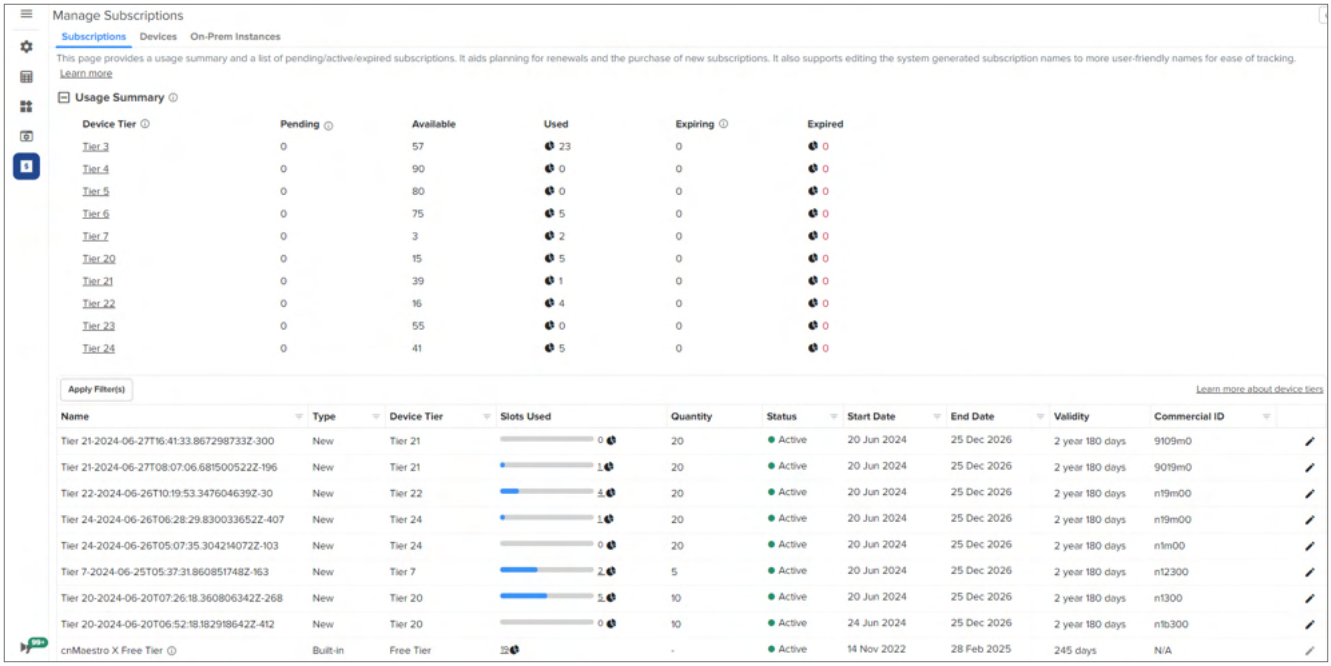


2. Enter **Name** and **Description**.
3. Click **Save**.

Usage Summary

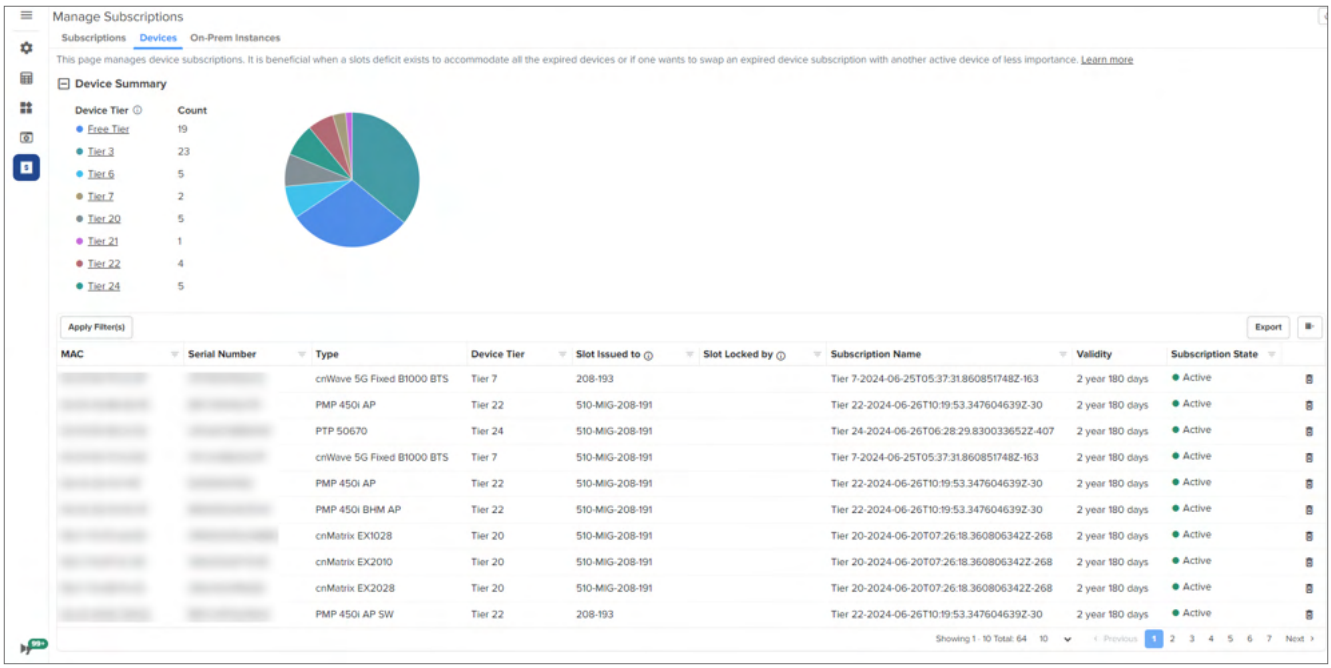
Usage summary displays the number of slots that are Pending, Available, Used, Expiring, and Expired, and click the **Device Tier** to view the particular list of devices as shown in Figure 5.

Figure 5 *: Usage summary*



Devices

The **Devices** page displays devices mapped to the subscription.



The **Device** page displays the following parameters:

Table 11 *Device parameters*

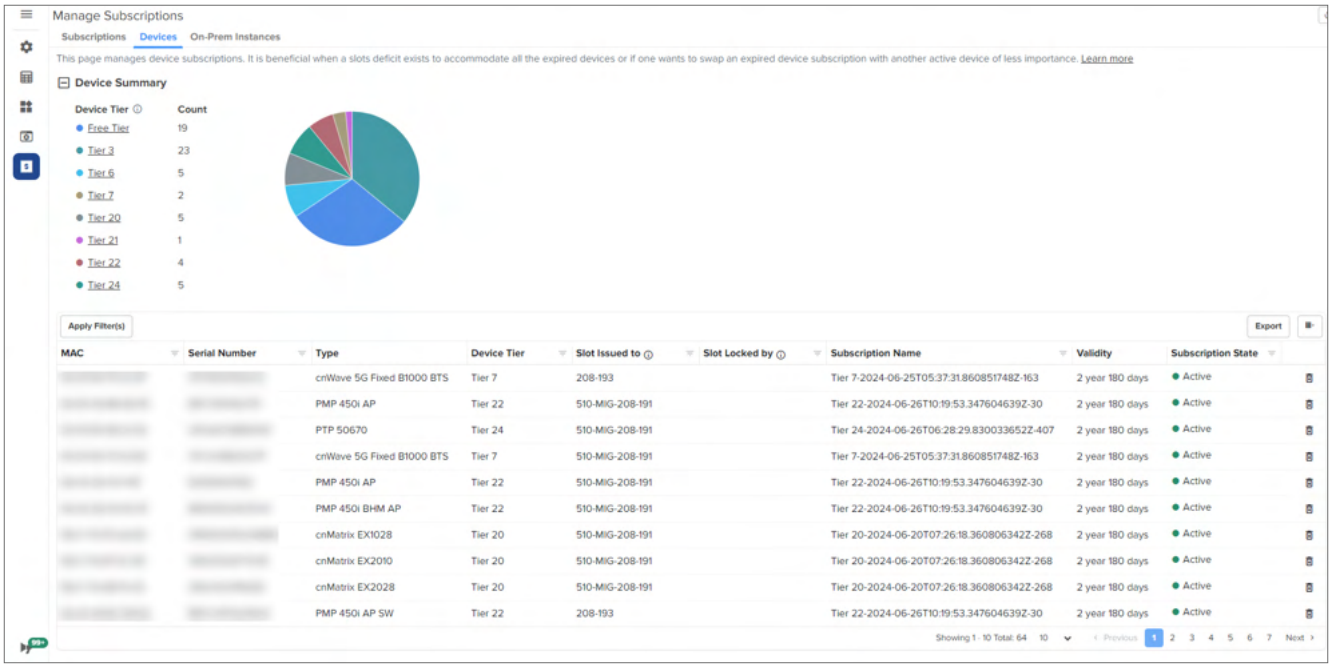
Parameters	Description
MAC	MAC address of the device.
Serial Number	Serial Number of the device.

Parameters	Description
Type	Type of the device.
Device Tier	Device tier type.
Slot Issued to	On-Premises instance to which the device slot is currently issued.
Slot Locked By	On-Premises instance to which the device slot was originally issued.
Subscription Name	Name of the subscription.
Validity	Displays the total validity of the subscriptions from the current date in year and days.
Subscription State	Type of subscription state, such as: • Active • Expired • Delete on Expiry

Device Summary

Device summary displays the available tiers and the device count according to the tiers. By clicking on the Device Tires in the device summary you can view the particular device list as shown in Figure 6.

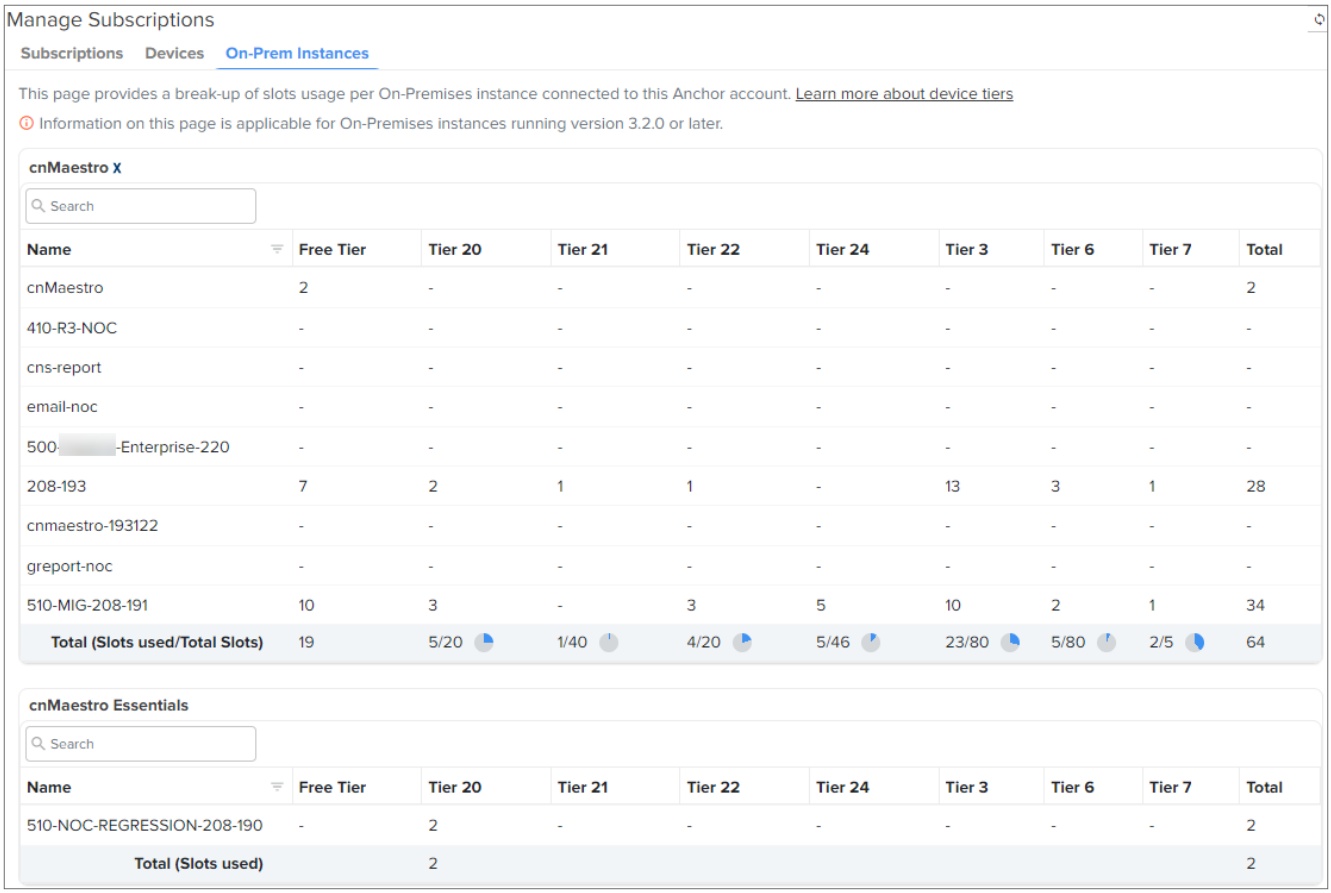
Figure 6 *: Device summary*



On-Prem Instances

> **Note**
>
> The **On-Premises Instances** page is applicable only for subscribed On-Premises instances running OVA version 3.2.0 and above.

On-Premises instances page provides a break-up of slots usage per On-Premises instance connected to this Cloud Anchor account such as cnMaestro X, Onboarding, and Essentials.



Manage Subscriptions

Subscriptions | Devices | On-Prem Instances

This page provides a break-up of slots usage per On-Premises instance connected to this Anchor account. Learn more about device tiers

Information on this page is applicable for On-Premises instances running version 3.2.0 or later.

cnMaestro X

Search

Name	Free Tier	Tier 20	Tier 21	Tier 22	Tier 24	Tier 3	Tier 6	Tier 7	Total
cnMaestro	2	-	-	-	-	-	-	-	2
410-R3-NOC	-	-	-	-	-	-	-	-	-
cns-report	-	-	-	-	-	-	-	-	-
email-noc	-	-	-	-	-	-	-	-	-
500[redacted]-Enterprise-220	-	-	-	-	-	-	-	-	-
208-193	7	2	1	1	-	13	3	1	28
cnmaestro-193122	-	-	-	-	-	-	-	-	-
greport-noc	-	-	-	-	-	-	-	-	-
510-MIG-208-191	10	3	-	3	5	10	2	1	34
Total (Slots used/Total Slots)	19	5/20	1/40	4/20	5/46	23/80	5/80	2/5	64

cnMaestro Essentials

Search

Name	Free Tier	Tier 20	Tier 21	Tier 22	Tier 24	Tier 3	Tier 6	Tier 7	Total
510-NOC-REGRESSION-208-190	-	2	-	-	-	-	-	-	2
Total (Slots used)		2							2

- **cnMaestro X**—Lists the cnMaestro X On-Premises instances and devices that are subscribed along with slots by usage and availibility.
- **Onboarding**—Lists the cnMaestro trial version of On-Premises instances which are upgraded from On-Premises 3.1.x and devices count that are used.
- **Essentials**—Lists the cnMaestro Essentials On-Premises instances and devices that are managed along with slot device count.

Cloud Connectivity

Cloud Connectivity allows the user synchronize the On-Premises instances with the Cloud Anchor account. This provides the announcements and licensing of new device device software of cnMaestro.

All new On-Premises instances must be connected to a Cloud Anchor account during the initial setup of configuration. The existing On-Premises instances must be connected to a Cloud Anchor account to avail the managed subscriptions. To create and manage a Cloud Anchor account, refer to Cloud Anchor account.

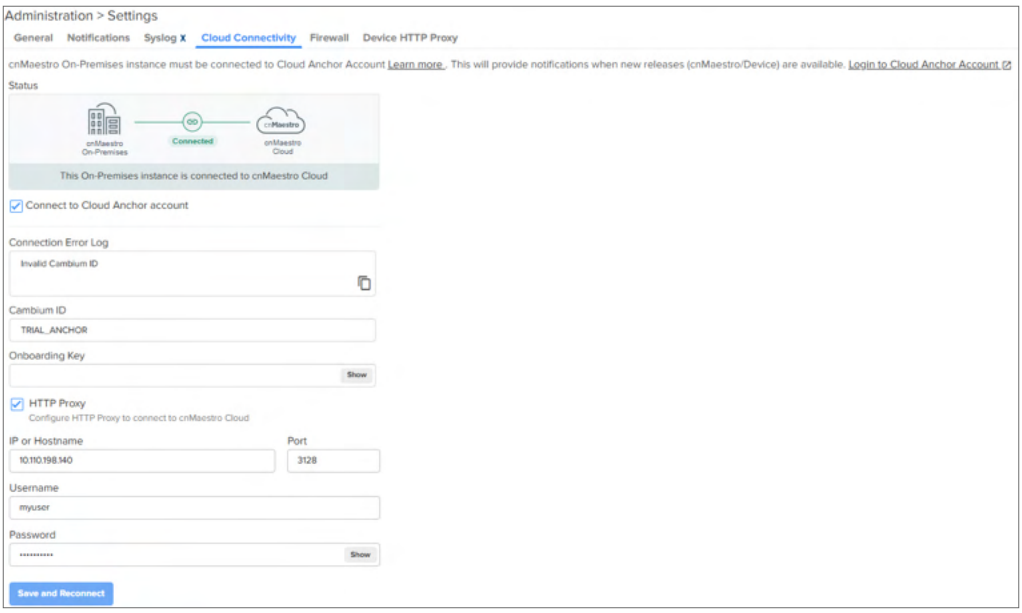
Connecting cnMaestro On-Premises to Cloud Anchor account

Perform the following steps to connect the cnMaestro On-Premise Instance with the Cloud Anchor Account:

1. Navigate to the **Administration > Settings > Cloud Connectivity** in the cnMaestro On-Premises UI.
2. Enter the **Cambium ID** for the Cloud Anchor account.
3. Enter the **Onboarding Key** created in the section above.
4. Enable **HTTP Proxy**, if required, by configuring the IP address or the hostname and Port number.

> **Note**
>
> Enable **HTTP Proxy** only when On-Premise Instances need to connect with a public network through proxy.

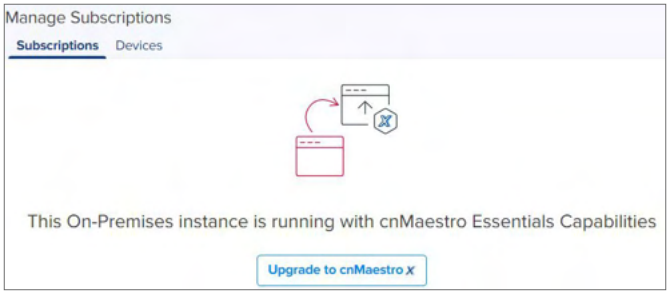
5. Click **Save and Connect**.



> **Note**
>
> - During the retry, it may take up to 15 minutes to connect the On-Premises instance with the Cloud Anchor account.
> - The On-Premises instance periodically updates the status of its inventory to the Cloud Anchor account every one hour.

On successful connectivity of the On-Premises instance with Cloud Anchor account, it displays the **Manage Subscription** page as shown in Figure 7. Refer to On-Premises Subscription Management.

Figure 7 *Manage Subscriptions*

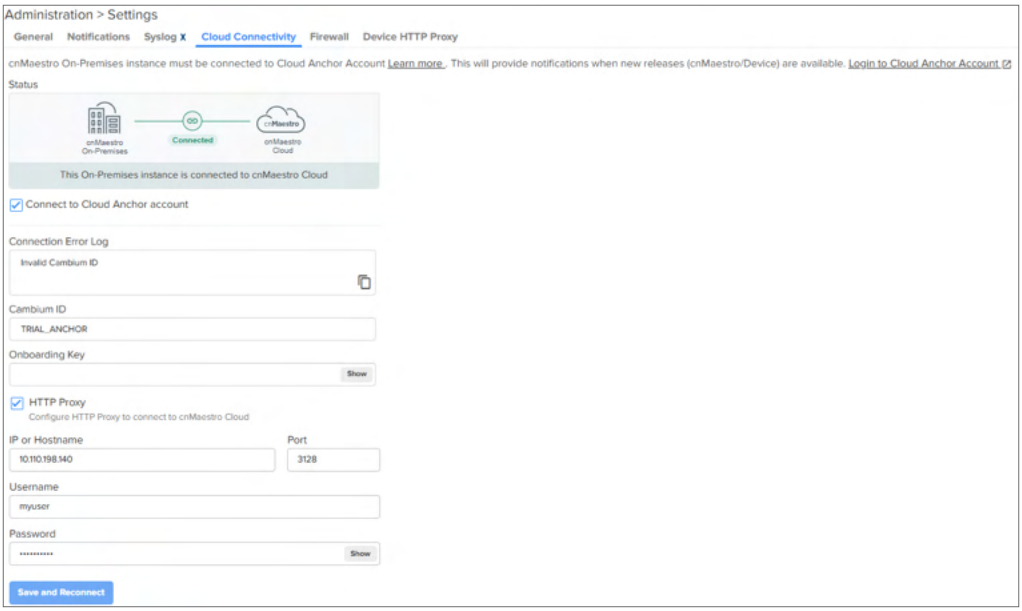


Disconnect cnMaestro On-Premises from Cloud Anchor account

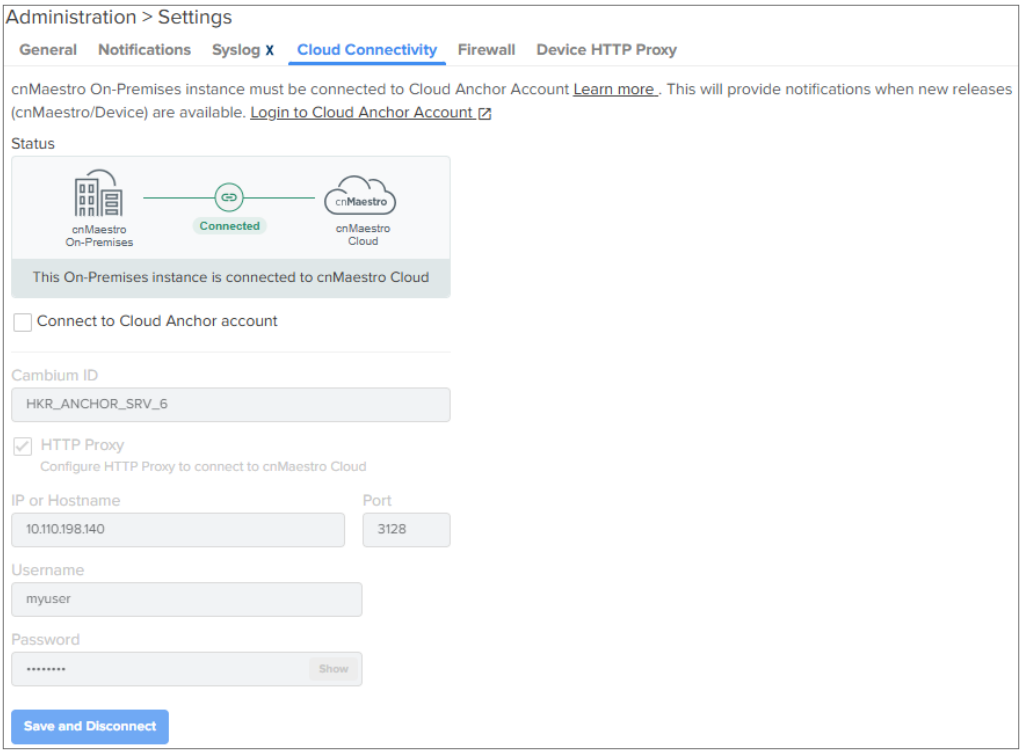
On-Premises instances can be disconnected from the Cloud Anchor account by disabling the **Connect to cloud anchor account** which allows you to keep the devices in unmanaged state.

To disconnect the On-Premises instances, perform the following steps:

1. Navigate to **Administration** > **Settings** > **Cloud Connectivity.**



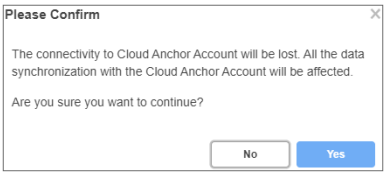
2. Clear the **Connect to cloud anchor account** checkbox.



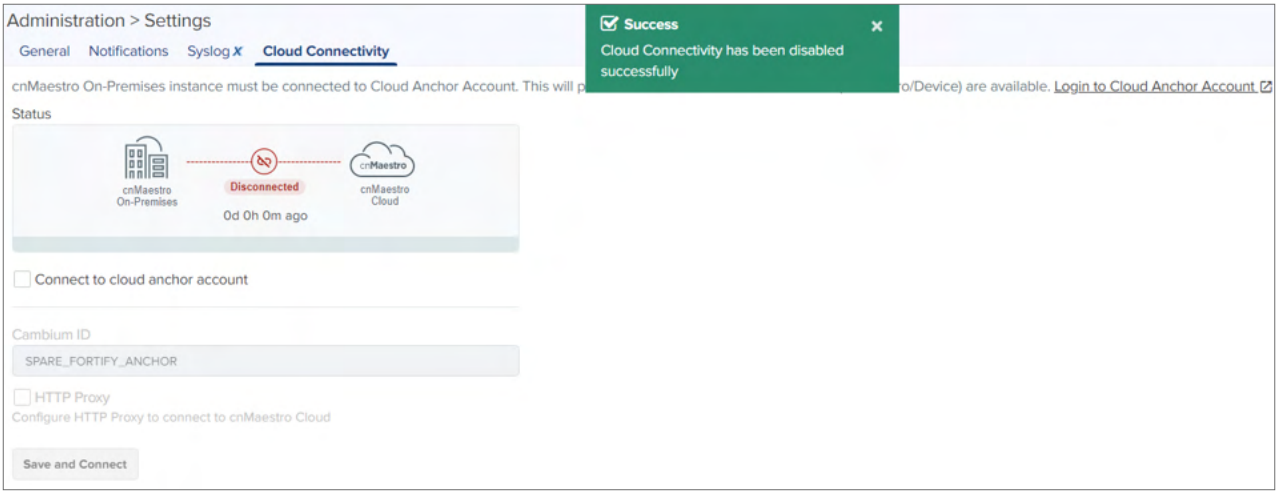
3. Click **Save and Disconnect**.

   A confirmation window appears.

4. Click **Yes** to continue.

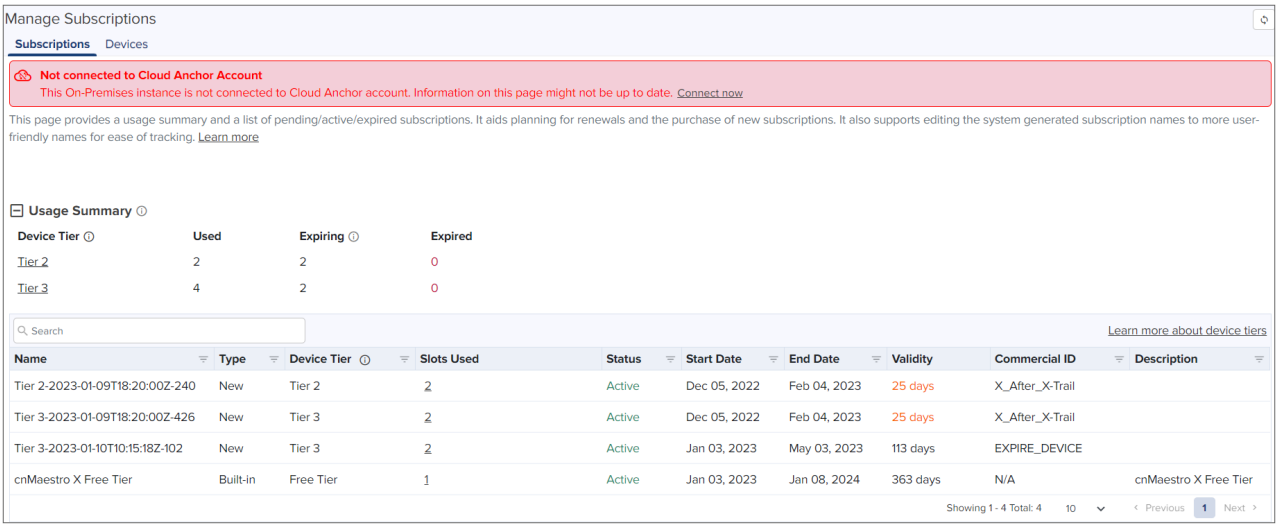


5. A success message is displayed.

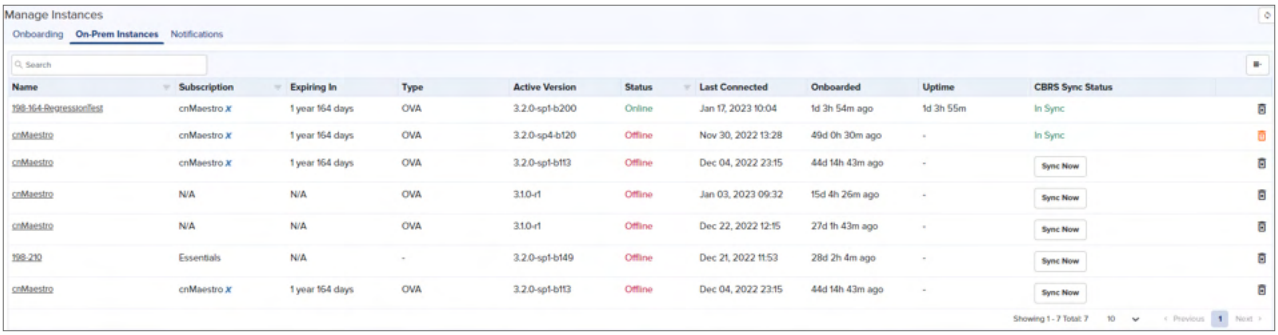


A notification banner will be displayed on the Subscription page as shown in Figure 8.

Figure 8 *Not connected to Cloud Anchor account banner*



The connectivity to Cloud Anchor account will be disconnected and the On-Premises instance displays as offline.



Cloud connectivity disconnected State

If an On-Premises instance disconnects from the Cloud Anchor account, its status becomes offline, and it does not allow the following actions:

- Onboarding and deleting devices.

  Deletions must be performed once connectivity is restored.
- Deleting the On-Premises instance.
- Restoring the device data.
- Managing the subscriptions.

On-Premises Subscription Management

On-Premises subscription management allows you to upgrade or downgrade to cnMaestro X, manage the device slots and subscriptions. Users can mange the On-Premises Instances only when the Cloud Anchor account is created and connected to it using Cloud Connectivity.

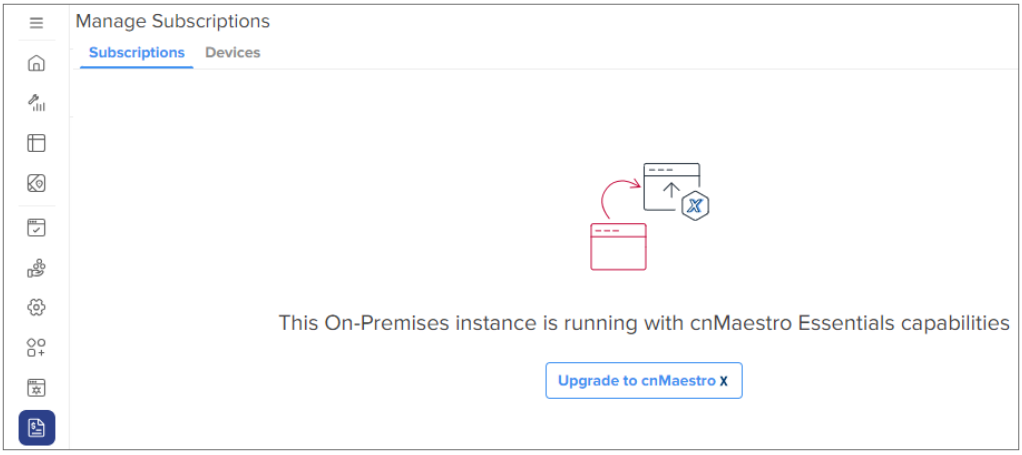
This section describes the following topics:

- Upgrade to cnMaestro X
- Downgrade to Essentials
- Delete On-Premises instances
- Slot Deficit
- Manage Subscriptions
- Expiry Notification
- Data retention period

Upgrade to cnMaestro X

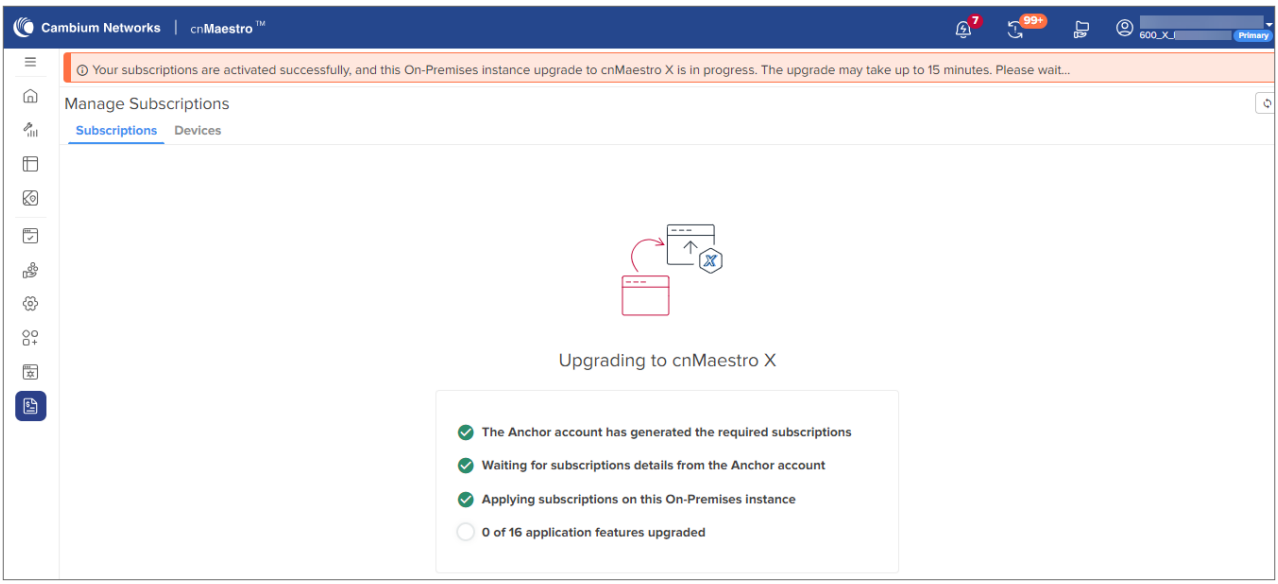
To upgrade to cnMaestro X after connecting to Cloud Anchor account, perform the following:

1. Navigate to **Manage Subscriptions** > **Subscriptions**.

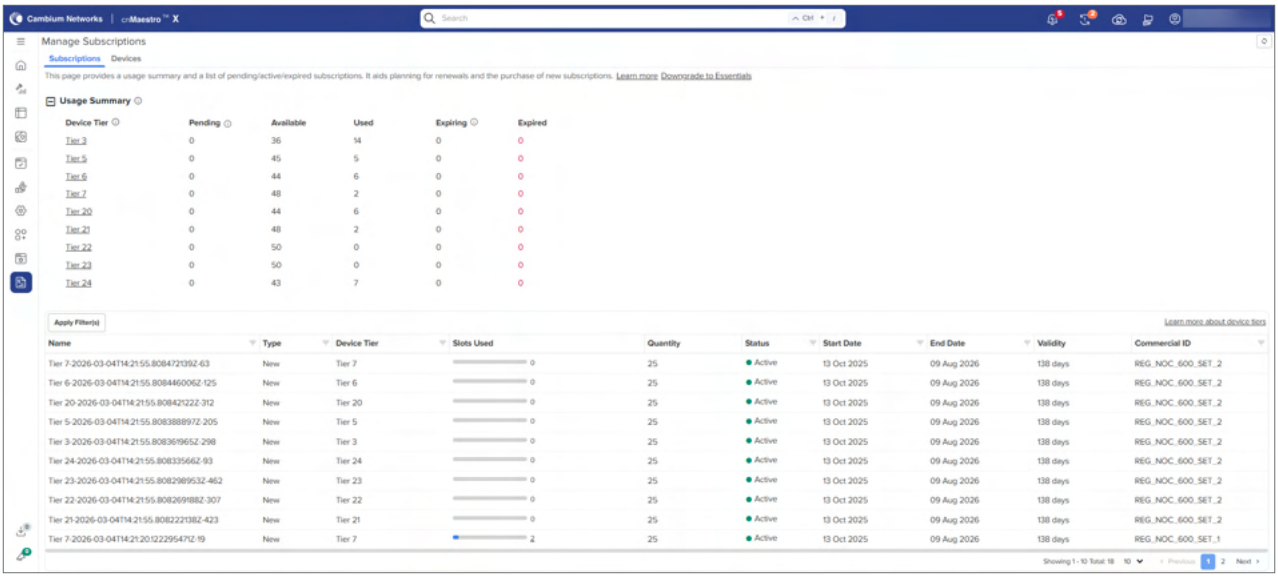


2. Click **Upgrade to cnMaestro X**.

   It performs the steps to upgrade to cnMaestro X as shown.



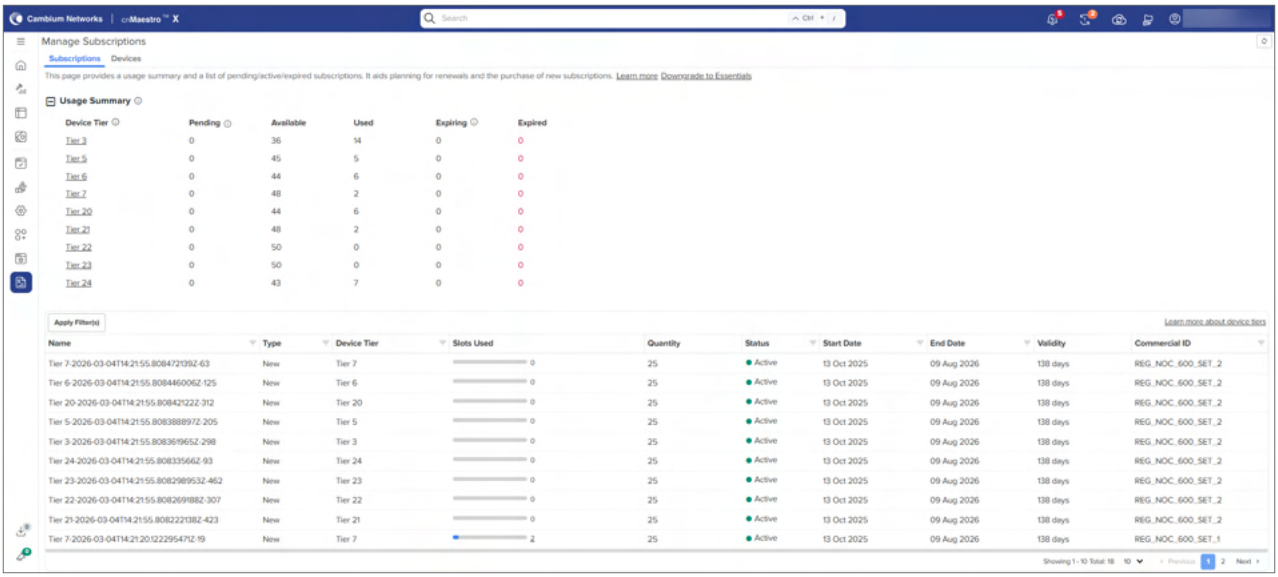
3. On the successful upgrade cnMaestro X label will be displayed and the Usage Summary and Device list on the **Subscriptions** page as shown below:



Downgrade to Essentials

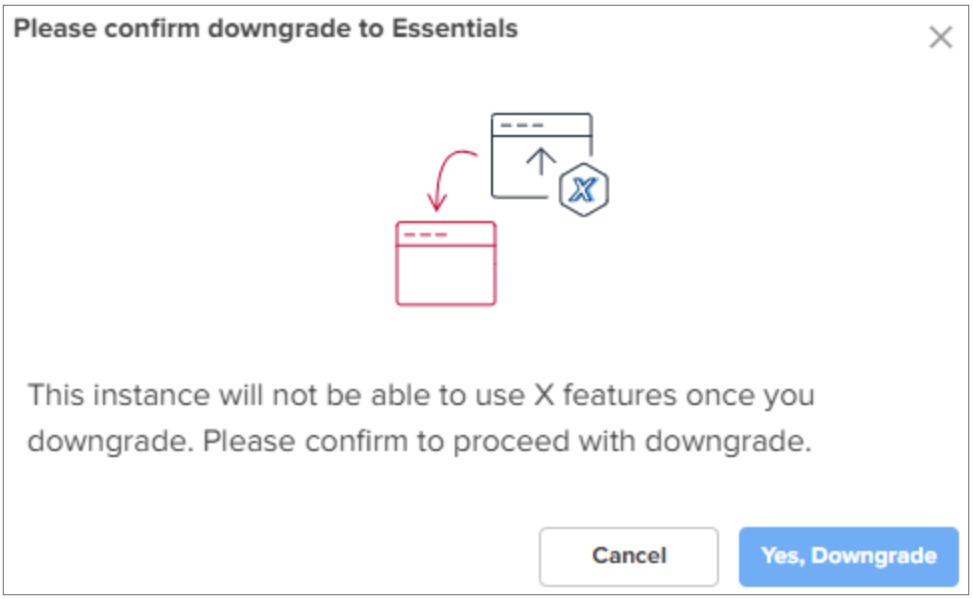
To downgrade to essentials perform the following:

1. Navigate to **Manage Subscriptions** > **Subscriptions**.



2. Click the **Downgrade to Essentials** link at the top of the page.

   The downgrade confirmation window pops up.



3. Click **Yes, Downgrade**.

Delete On-Premises instances

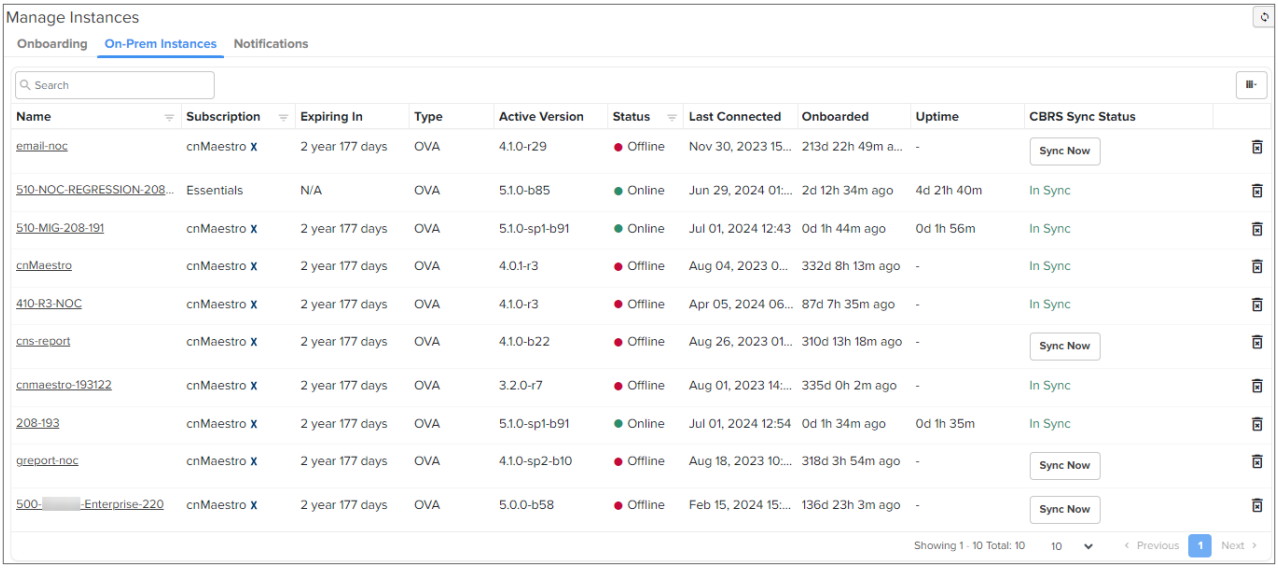
To stop managing the On-Premises instances from the subscription page you must initiate the process from the linked Cloud Anchor account. Once the deletion process is initiated from the Cloud Anchor account it displays the notification banner on the On-Premises account.

Note

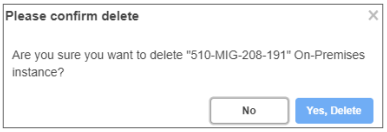
- If the On-Premises instance has a cnMaestro X subscription and is online, it automatically downgrades the On-Premises instance to Essentials and deletes the On-Premises instance.
- On-Premises instance deletion is not allowed if it is in cnMaestro X and offline. You must bring back the On-Premises instance to the online state or contact Cambium Networks support to delete the offline X instances.
- The deleted instance releases the slots to the Anchor account, but it continues with the same set of devices. and allows the On-Premises instance to continue with the same set of devices in the Essentials mode.

To delete the On-Premises instances, perform the following:

1. Navigate to **Cloud Anchor Account** > **Manage Instances** > **On-Premises instances**.



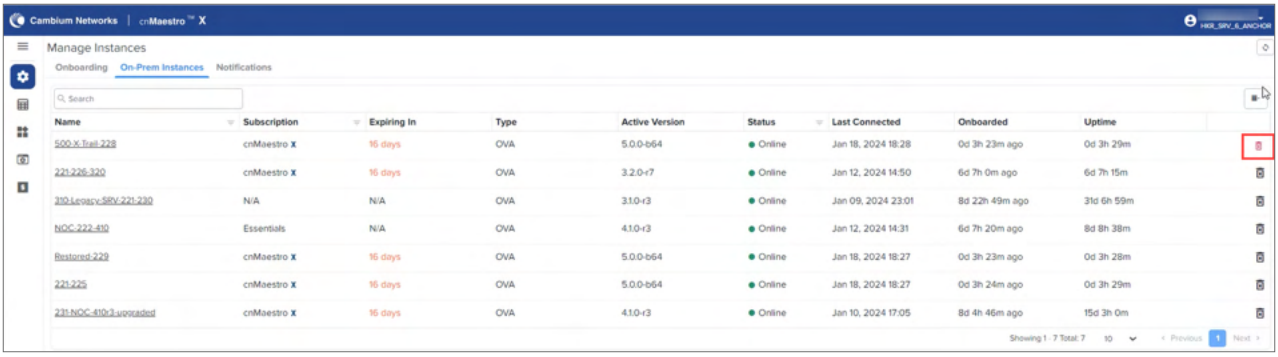
2. Click the **Delete On-Premises instance** (🗑) icon.
3. A confirmation window pops up.



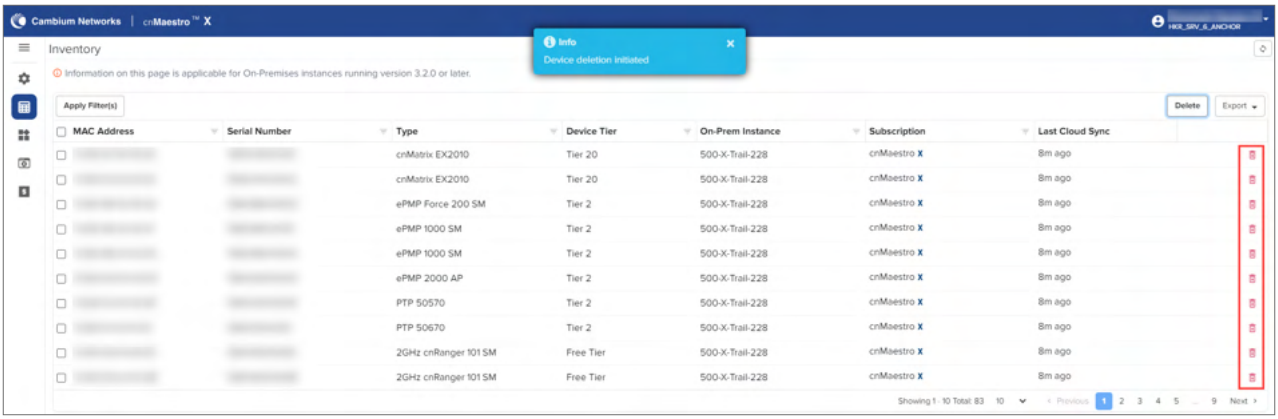
4. Click **Yes, Delete**.

> **Note**
>
> On Cloud Anchor account to delete the On-Premises instances, may take 10 minutes.

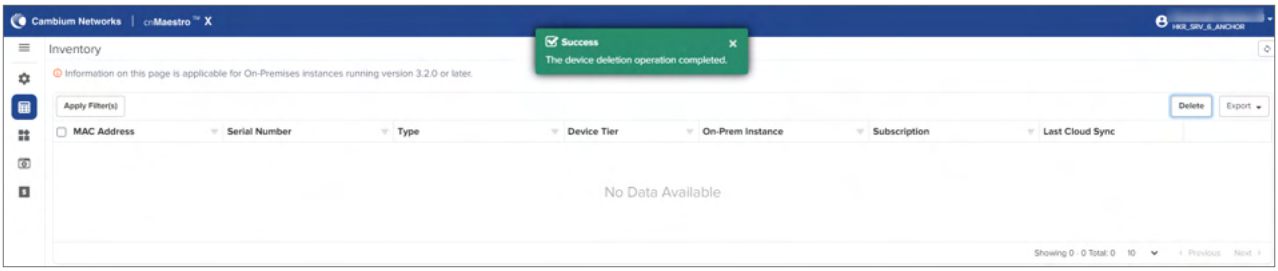
5. Deletion of On-Premises instances will be initiated (the delete icon turns red in color) and it also deletes the devices from the **Inventory** tab.



> **Note**
>
> Following are the different colors that appear during the deletion process and their indications:
>
> - Red indicates that the deletion is in progress.
> - Orange indicates that a failure has occurred in the deletion process, and the failure message is displayed as a tool tip.

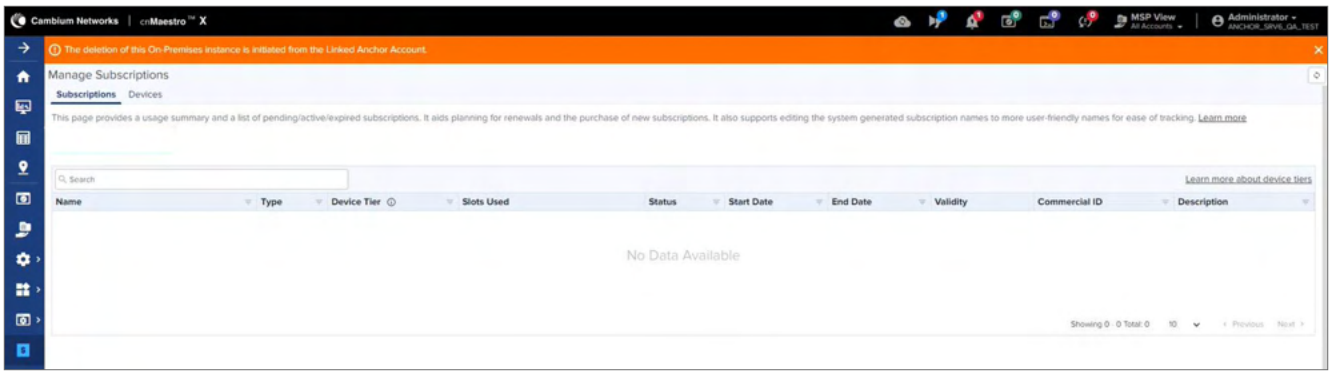


6. **Success** window pops up.

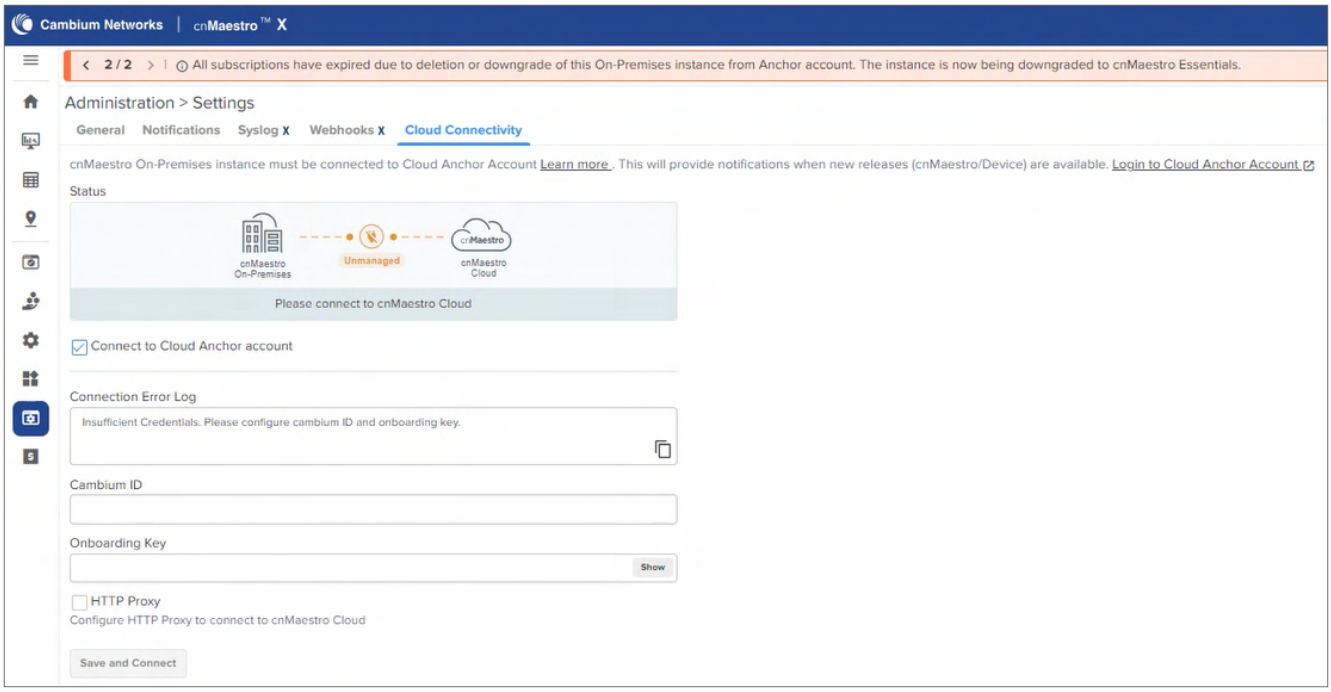


If the deletion of On-Premises instance is initiated from the linked Cloud Anchor account, it displays a banner on the On-Premises account as shown in Figure 9. It also creates the notification and logs on the **Audit Logs** page.

Figure 9 *Deletion initiated*

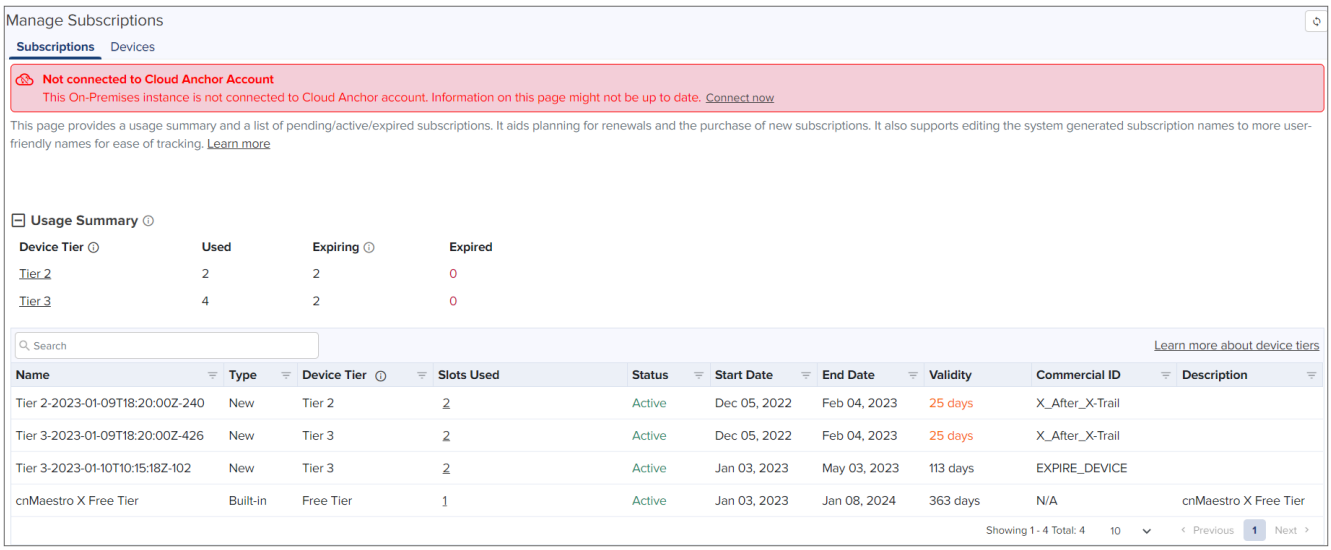


On the successful deletion of On-Premises instances and devices from the linked Cloud Anchor account. On-Premises instances will be disconnected from the Cloud Anchor account.



It also displays the notification banner on the **Subscription** page as shown in Figure 10.

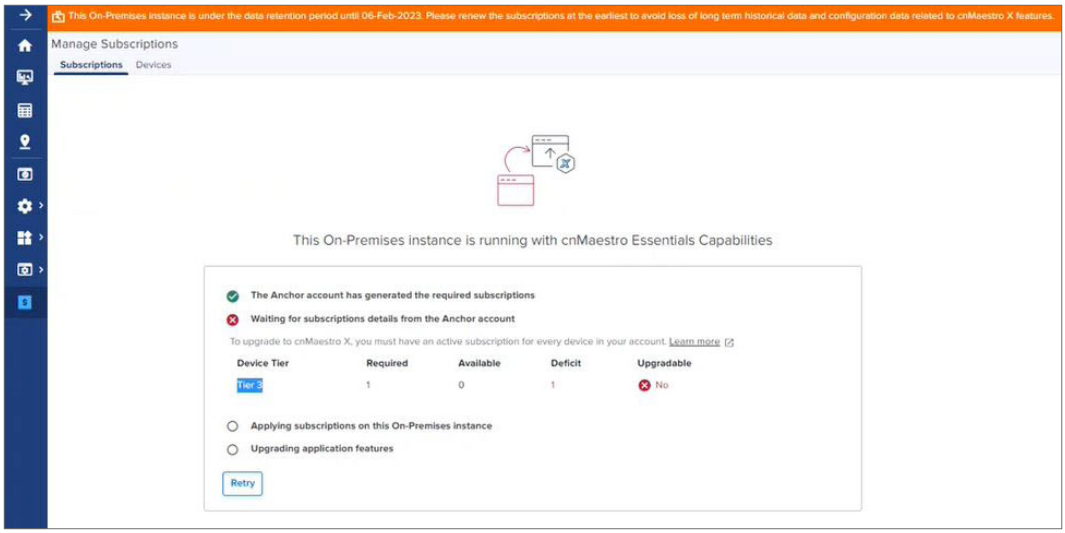
Figure 10 *Downgraded account*



Slot Deficit

A Slot Deficit occurs during the upgradate to cnMaestro X when the number of active subscriptions for each device slot is less than the required slots to upgrade.

Upgrading to cnMaestro X will not be processed until the devices are removed or added to match the available subscription slots that are less than the slot required for the instance.



Manage Subscriptions

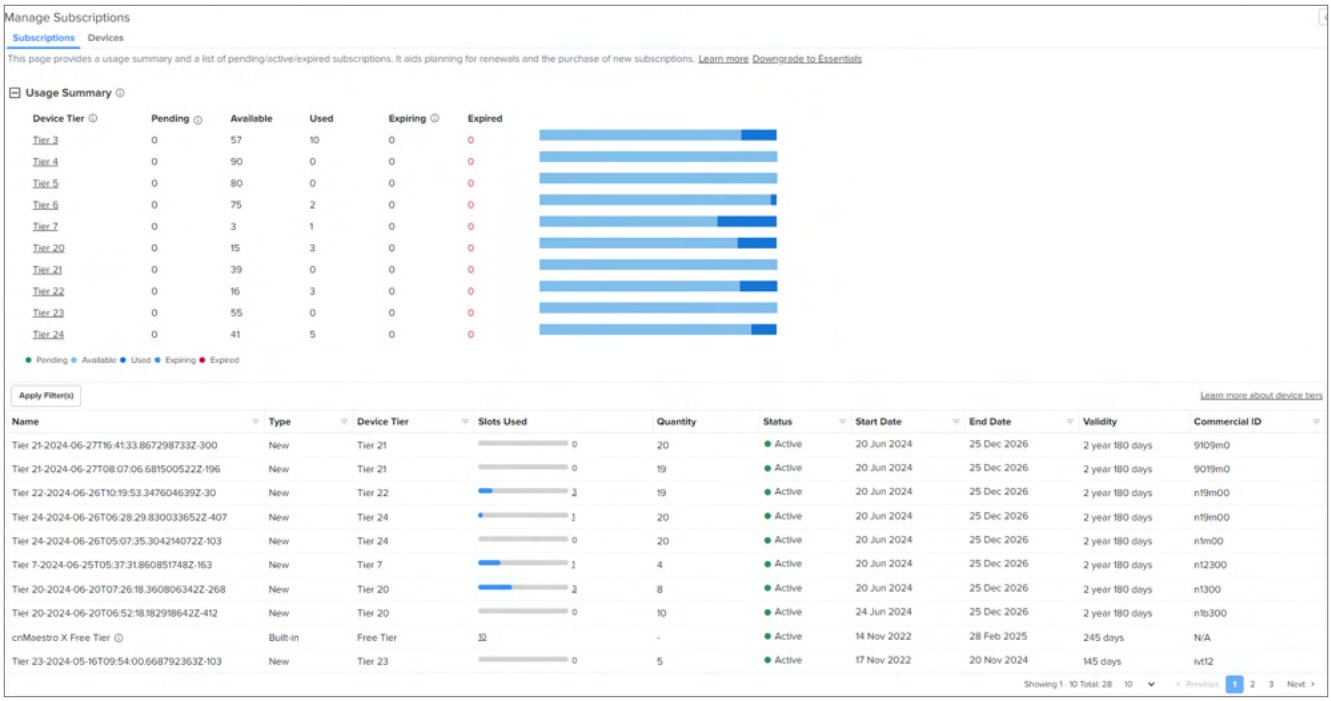
Manage Subscriptions page provides the usage summary and aids in planning for renewals and the purchase of new subscriptions.

This section provides the details about:

- Subscriptions
- Devices

Subscriptions

Subscriptions page provides the usage summary of **Device Tier** list of Pending, Available, Used, Expiring, and Expired. It also allows the user to upgrade and downgrade the cnMaestro X after connecting the On-Premises instance to Cloud Anchor account. It displays the usage details of the corresponding On-Premises and if the On-Premises is in a connected state, then it pulls the availability from the anchor.

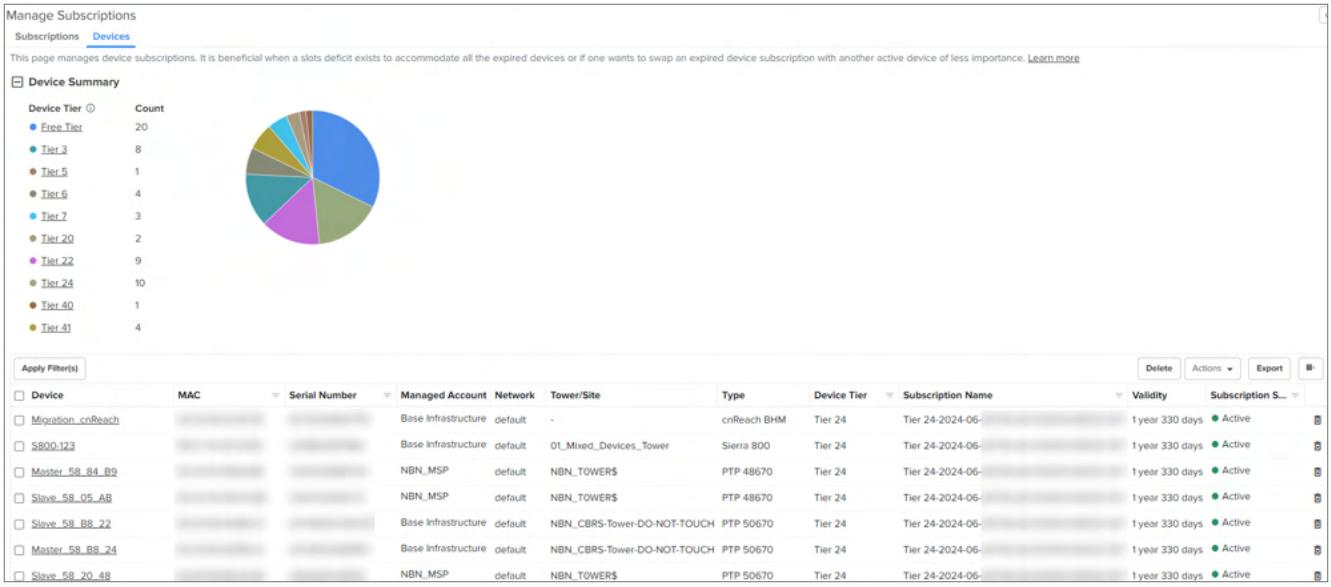


Note

Subscriptions page provides the usage summary of the corresponding instance.

Devices

Device page manages device subscriptions. It is beneficial when a slot 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. It also displays the device summary by accumulating the tier based device count in a list and pie chart format.

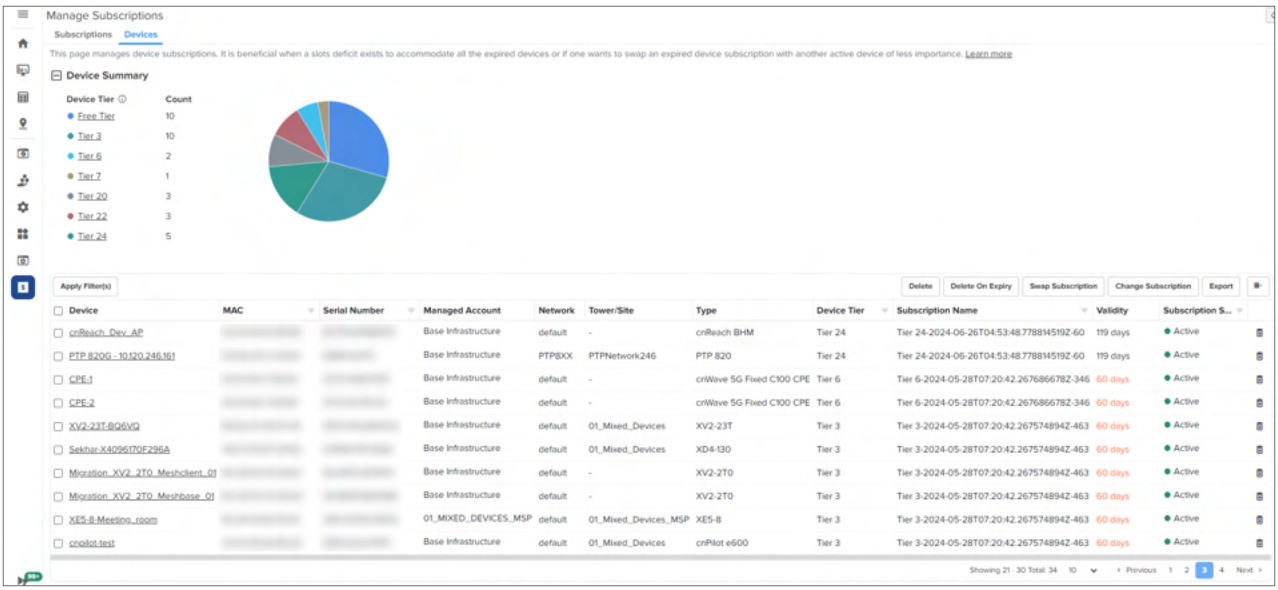


Swap Subscription

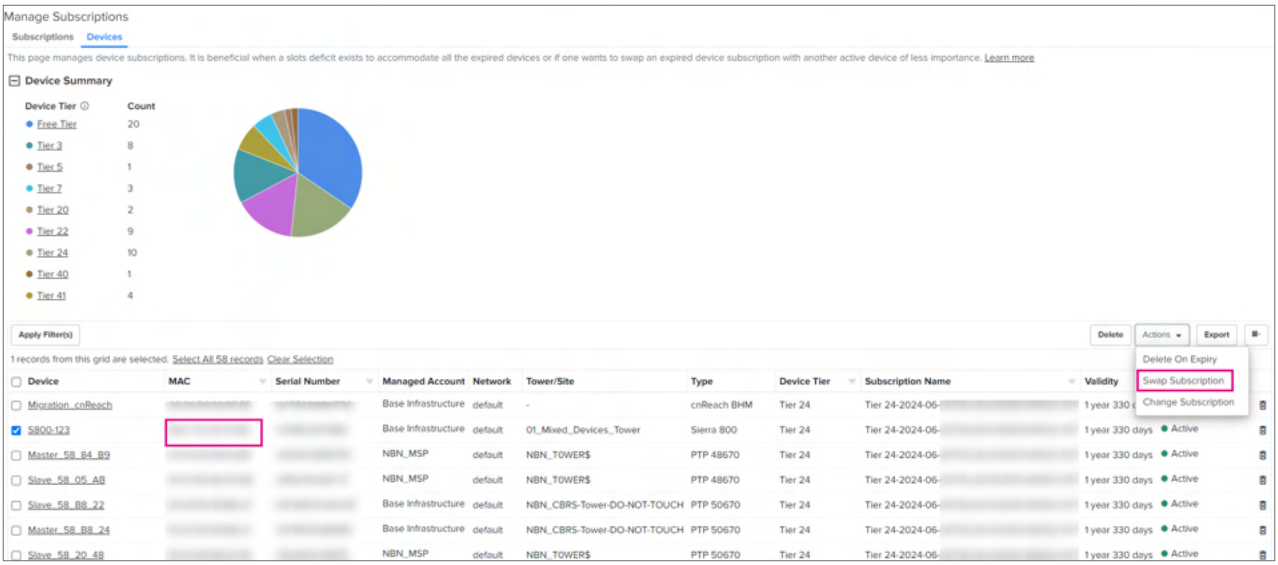
Swap Subscription allows the user to swap one device subscription with another device of the same tier on the same On-Premises instances. It can be performed at any time.

To swap subscriptions, perform the following steps:

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



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



3. Click **Actions** > **Swap Subscription.** Enter the **MAC Address** of the targeted device and click **Swap.**

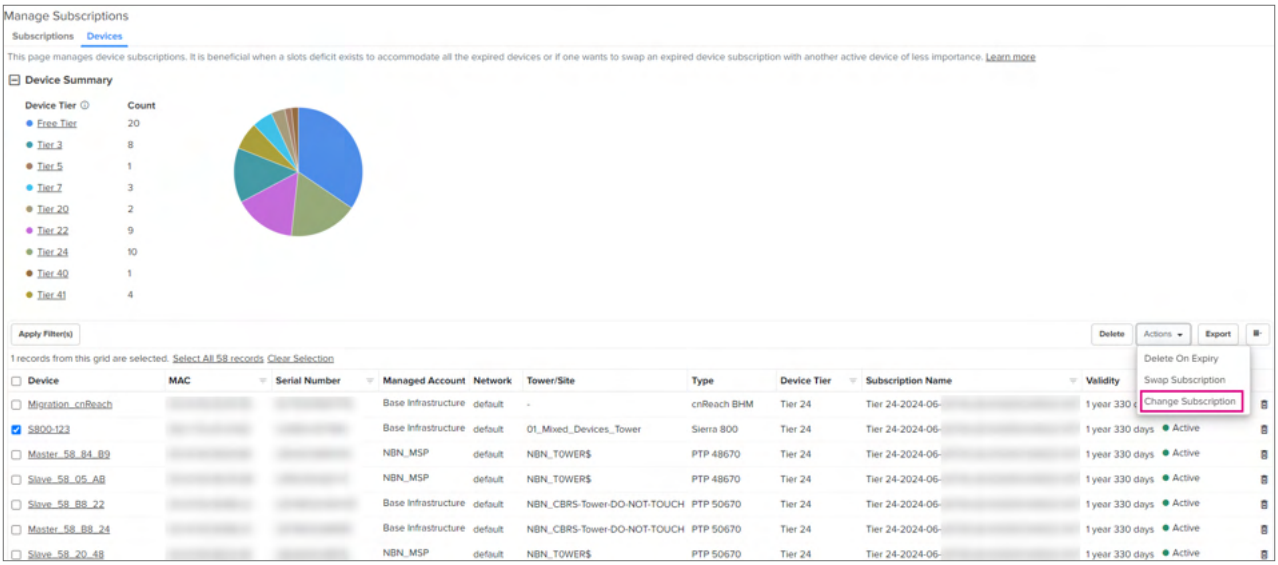
Device updated successfully message displays on success.

Change Subscription

Change Subscription allows to changes the device from one subscription to another of the same tier across multiple On-Premises instances that are connected to the same Cloud Anchor account when slots are available.

To change subscription, perform the following steps:

1. Navigate to the **Subscriptions** > **Devices.**



2. Select the device from the list and click **Actions** > **Change Subscription.**
3. **Change Subscription** window pops up.

   Select the **Subscription** from the dropdown.

4. Click **Change**.

   Success window appears.

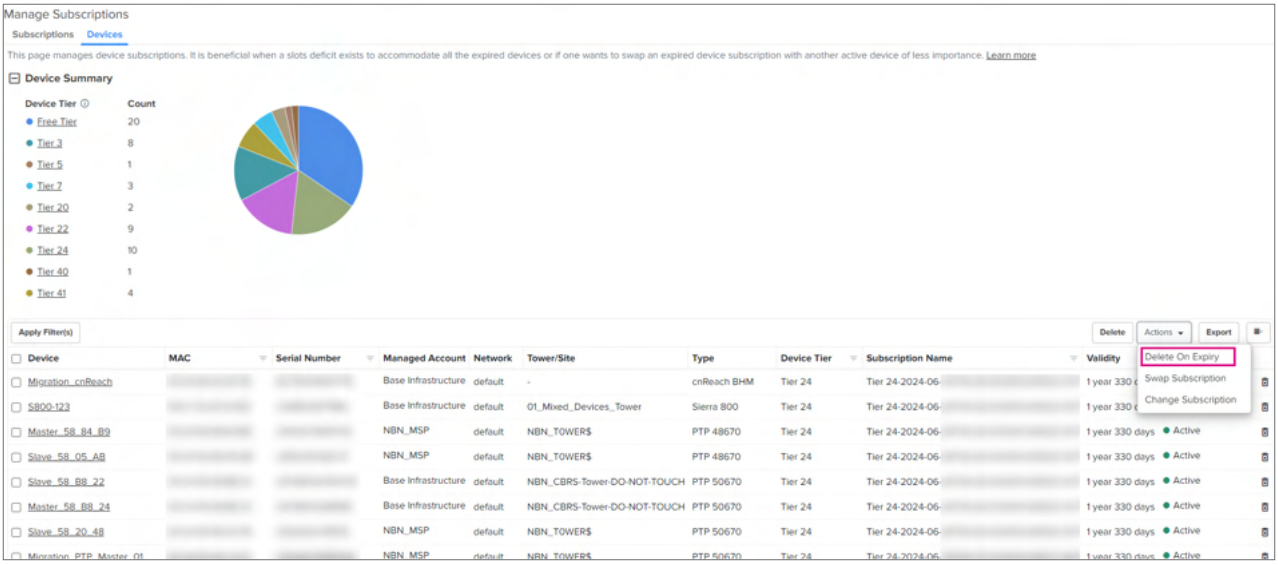
Delete on Expiry

> **Note**
>
> When the device state is changed to **Delete on Expiry**, this action cannot be undone.

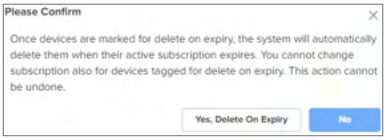
User can select the device and set the subscription state to **Delete on Expiry**, once the subscription is expired, then the device will be automatically deleted from the On-Premises instances.

To set the Delete on Expiry, perform the following steps:

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



2. Click **Actions** > **Delete on Expiry.**
3. **Please Confirm** window pops up.

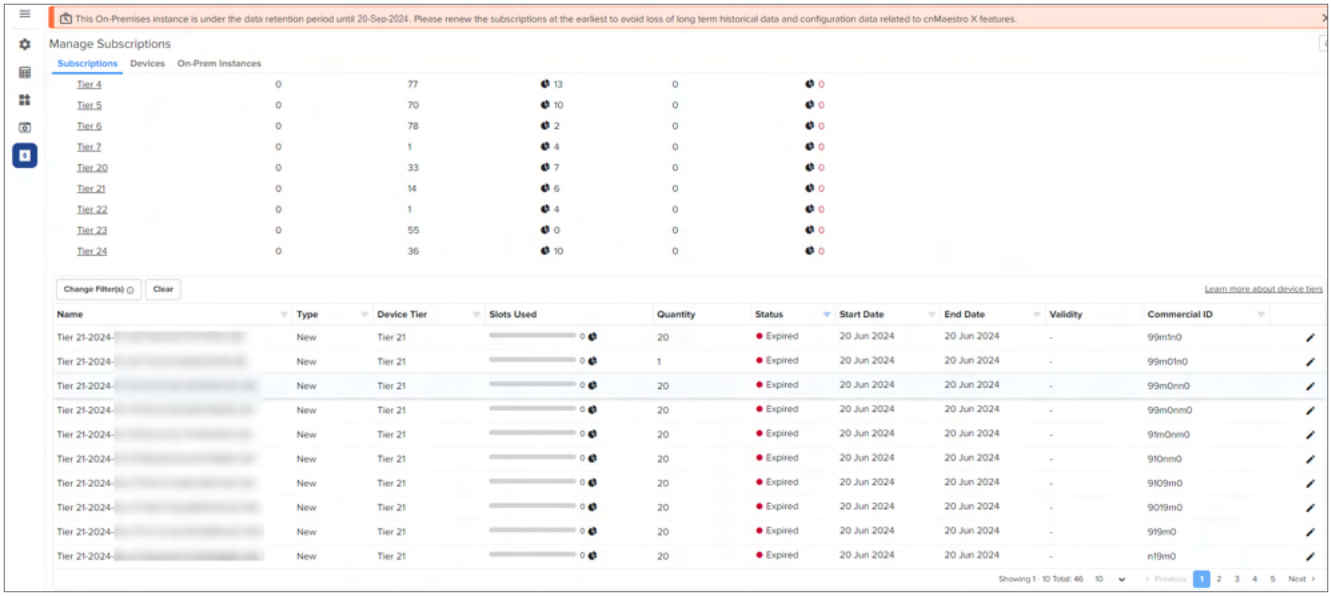


4. Click **Yes Delete On Expiry**.
5. Subscription state changes to **Delete on Expiry** from **Active**.

Expiry Notification

If the subscription validity is less than 90 days, in the Validity column the number of days left will be highlighted in red color. Also, a notification banner will be displayed as shown Figure 11.

Figure 11 *Expiry notification banner*



If the number of expired subscription slots is equal to or less than the number of available subscription slots, automatically moves the devices to the available active subscription of the same tier.

Data retention period

If the device is downgraded from the current version, then data retention is enabled. During this data retention period cnMaestro allows users to manage the devices with minimal data (for example, configuration and statistics) and without disruption, so that the user can renew later. If the subscriptions are not renewed, then all the retained data will be deleted at the end of data retention period.

When the account is in the data retention period, it displays the notification banner as shown in Figure 12.

Figure 12 *Data retention banner*

cnMaestro X features behavior state

cnMaestro X subscriptions can be purchased for a duration of 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.

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 12 *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	**Link Events** • Maintains link events data up to 30 days. **Maps** • 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 **High Availability** • Allows configuring a secondary (backup or passive) E2E Controller from cnMaestro	**Link Events** • Only 7 days link events data is exposed • Data will still be collected in retention period **Maps** • Status and Sectors in Device Overlay	**Link Events** • Not accessible **Maps** • Status in Link Overlay • Status and Sectors in Device Overlay
AAA	Allows to configure the authentication server.	Configuration will be retained, but the feature will no longer be available.	Not accessible
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.	• Enterprise Wi-Fi—Not accessible	• Enterprise Wi-Fi—Not accessible

Feature	cnMaestro X	On Downgrading cnMaestro X to Essentials and Data Retention Period	After Data Retention Period
	This is available for Enterprise Wi-Fi devices.		
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	• 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
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	Allows user to configure personal SSID, password, and VLAN. This disables the local	Not accessible	Not accessible

Feature	cnMaestro X	On Downgrading cnMaestro X to Essentials and Data Retention Period	After Data Retention Period
(Part of **WLANs** > **ePSK** configuration)	ePSK and the WLAN SSID.		
Bulk Edit	• 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	• Displays Wi-Fi Client application and network statistics.	Not accessible	Not accessible
Configuration Lock	Allows to push the configuration changes even if the device is updated directly.	Not accessible	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** • Self Registration • Sponsored Guest • Paid **Employee/Student Access** • Microsoft Azure • Google Login • Onboarding **Combined** • One Click + Paid • Voucher + Paid	Configuration will be retained, but the cnMaestro X portal types will no longer be available.	cnMaestro X portal types will no longer be available.
Email Notifications	Maximum of 10 email recipients can be added per	• All the configured email recipients are retained	Only the 2 earliest added recipients are retained. The

Feature	cnMaestro X	On Downgrading cnMaestro X to Essentials and Data Retention Period	After Data Retention Period
	Managed Account (All Accounts, Base Infra and per MSP)	• None of the email recipients are deleted. • Only the 2 earliest added subscribers per Managed Account would receive email notifications.	remaining email recipients are deleted automatically.
ePSK Limit	ePSK entry limit can be 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:
	• Paid access
	• Enterprise:
	  ◦ Sponsored Guests
	  ◦ Self Registration
	• 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 confirmation and password for enterprise self registration and sponsored guests.	Configuration will be retained, but the feature will no longer be available.	Not accessible
Guest Portal	Allows 500 guest portals, 10,000 sessions, and 20,000 login event session records for a maximum of 1 year.	• If the count is more than 4 then, all portals are read-only and allows to delete. • All existing client sessions will continue without any disruption.	Only 4 portals will be retained and rest will be deleted.
Graphical Reports Template	• **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	Not accessible.	Not accessible.

Feature	cnMaestro X	On Downgrading cnMaestro X to Essentials and Data Retention Period	After Data Retention Period
	Client Types by Failure Count • **Access Points**—Top Access Points by Traffic Usage • **Clients**—6 GHz 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 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. • Validate IdP role mapping key • View existing role mappings • Add, edit, delete role mappings.	Not accessible	Not accessible
Installation Summary	Displays the installation summary of devices installed using the cnArcher Mobile Application.	Not accessible	Not accessible
Layer 7	Filter individual applications	Not accessible	Not accessible

Feature	cnMaestro X	On Downgrading cnMaestro X to Essentials and Data Retention Period	After Data Retention Period
(Application Filtering) (Part of **Wi-Fi Profiles** > **Access Control Policies** > **IP and Application Filtering Rules**)	or applications belonging to a category.		
Long term Historical Data	Displays the devices performance graph: • 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 months.	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.
Managed Services	Allows to manage each accounts with independent administration and configuration.	• 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	Allows to create 50 floor plan	• All floor plans are	• Additional floor plans is

Feature	cnMaestro X	On Downgrading cnMaestro X to Essentials and Data Retention Period	After Data Retention Period
Plan	per site.	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.	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
SNMP	SNMP track and monitor the cnMaestro.	Not accessible	Not accessible
Spectrum Analyzer	Analyzes and monitors the wireless spectrum for optimizing network performance on PMP devices.	Not accessible	Not accessible
Stanley-AeroScout	Delivers accurate and reliable location data for assets and customers with the STANLEY Healthcare Wi-Fi tags.	Not accessible	Not accessible
Syslog	Allows to generate Event logs and Audit logs.	Not accessible	Not accessible
Terrain View	It allows to view maps in Terrain view.	Not accessible	Not accessible
Webhooks	Webhooks provide real-time streaming for alarms using a push notification.	Not accessible	Not accessible
Wireless Intrusion Detection System (WIPS)	Protect wireless networks from unauthorized access and potential security threats.	Statistics is not available through API	Not accessible

Feature	cnMaestro X	On Downgrading cnMaestro X to Essentials and Data Retention Period	After Data Retention Period
	• WIDS data is processed • APIs are supported		
Wireless Intrusion Prevention System (WIPS)	Enhances security of wireless networks by deauthenticating rogue APs and clients. • 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

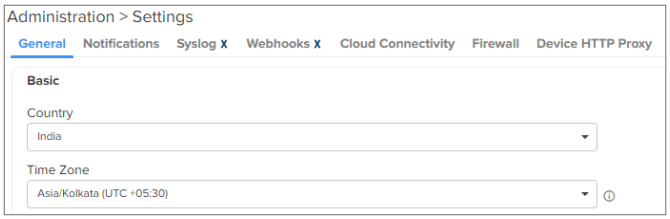
cnMaestro provides a number of ways to navigate the UI.

This section includes the following topics:

- Basic
- 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

Basic

cnMaestro supports the **Time Zone** of all countries, which can be selected based upon the composition during devices installed.



Note

- Only Super Administrator and Administrator can change the Time Zone.
- The Time Zone setting is applicable only for Email Notifications, Webhooks, and RESTful APIs only.

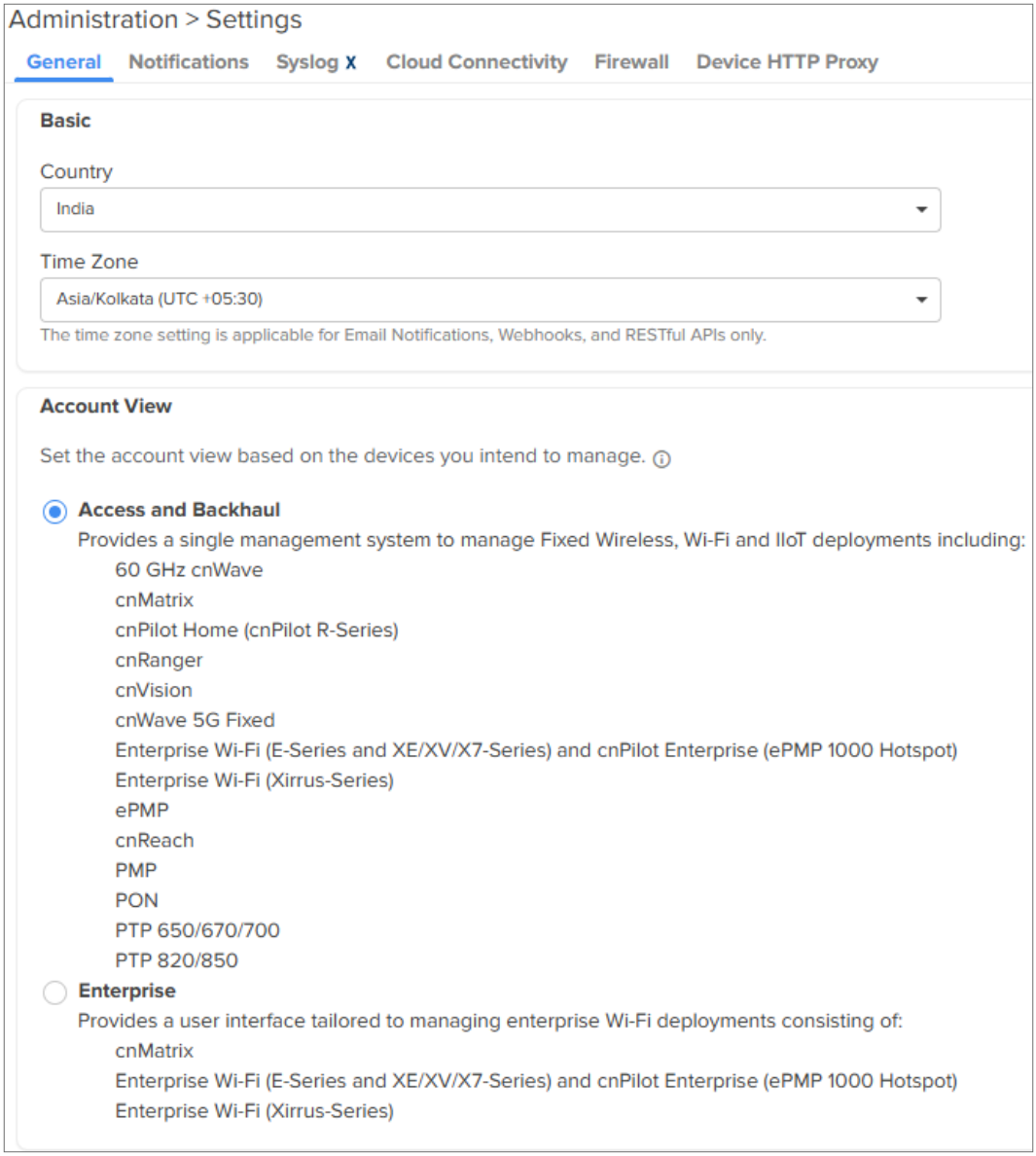
Account View

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

- Access and Backhaul view
- Enterprise view

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

Figure 13 *Account View*



Access and Backhaul view

The Access and Backhaul View supports all Fixed Wireless and Wi-Fi devices. 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) and cnPilot Enterprise (ePMP 1000 Hotspot), Enterprise Wi-Fi (Xirrus-Series), ePMP, PMP, PTP 650/670/700, PTP 820/850, and PON.

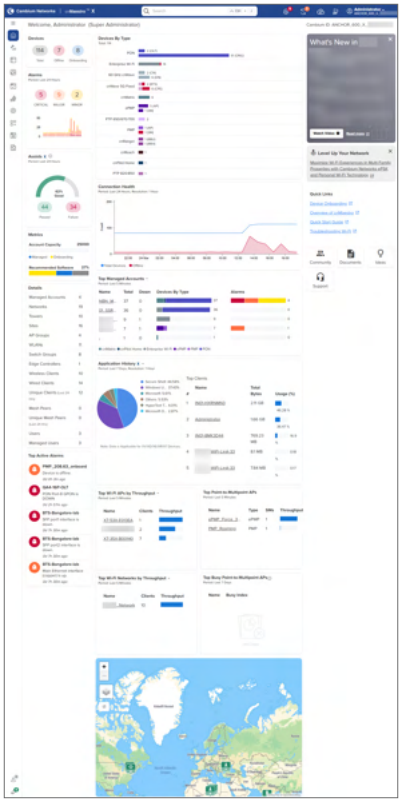
Enterprise view

The Enterprise View supports the Enterprise Wi-Fi portfolio, which includes the cnPilot Enterprise APs (ePMP 1000 Hotspot), cnMatrix, and Enterprise Wi-Fi APs (E-Series, and XE/XV/X7-Series), and Enterprise Wi-Fi (Xirrus-Series). It provides a simplified UI for Wi-Fi components (hiding fixed wireless features such as Towers).

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 14 *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 15 *cnMaestro page structure*

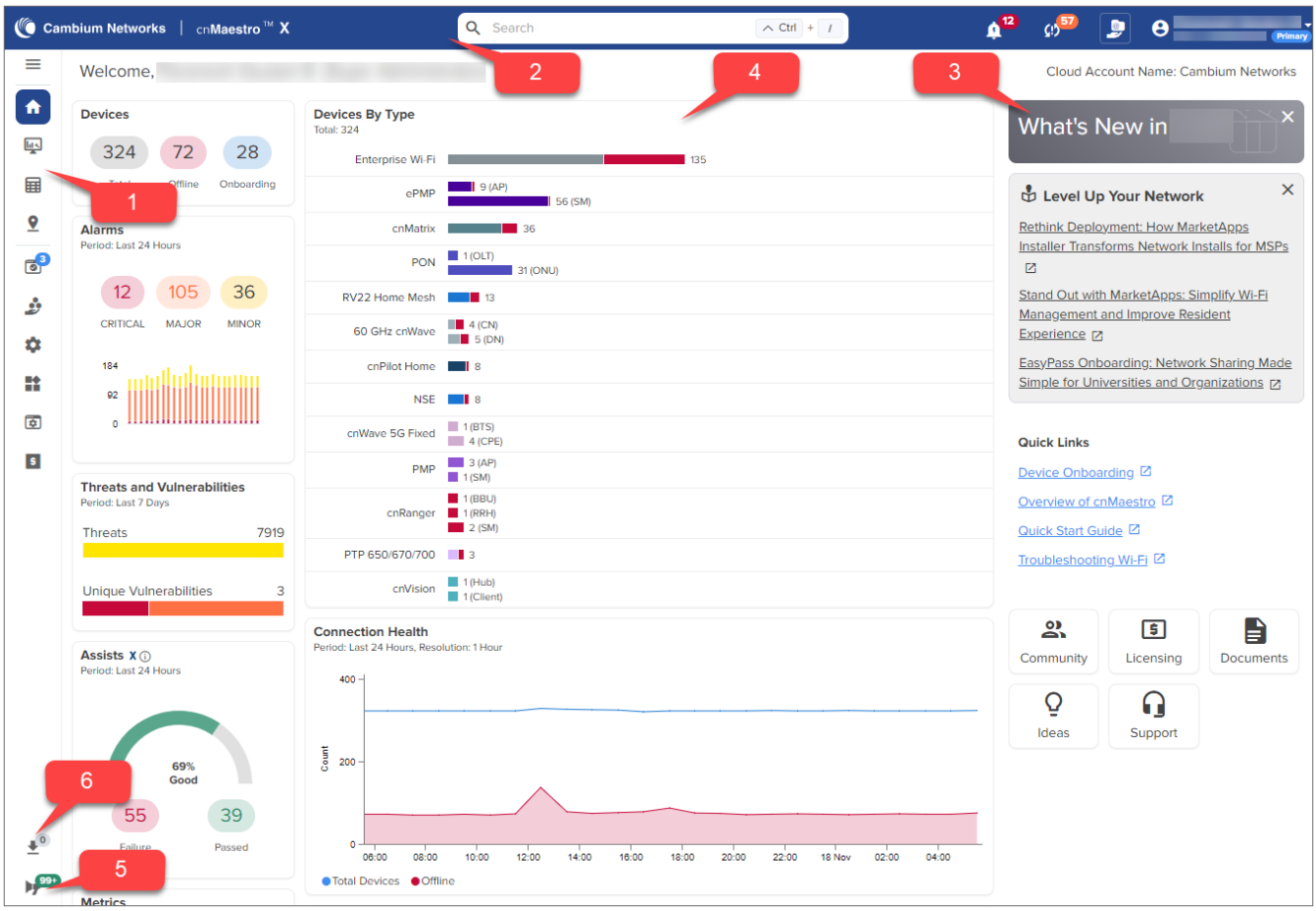
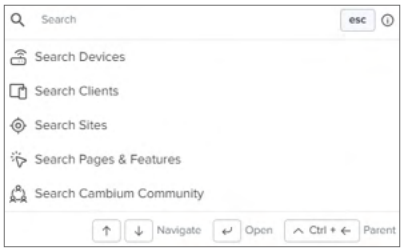


Table 13 *UI description*

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**,**Cloud connectivity status**, and **Out of Sync Devices**, and **Search**. For information on the **Search** bar, refer to Searching for cnMaestro resources using the Search bar.
3	Right menu	Provides links to Cambium **Ideas**, **Support**, **Community**, **Documents**, and **Licensing**. It also displays the current release version of cnMaestro and lists the new features and enhancements in that version.
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.
6	Download Manager	Displays the status of the download process when initiated by the **Export All as CSV** option. For more information, refer to Export All as CSV.

Searching for cnMaestro resources using the Search bar

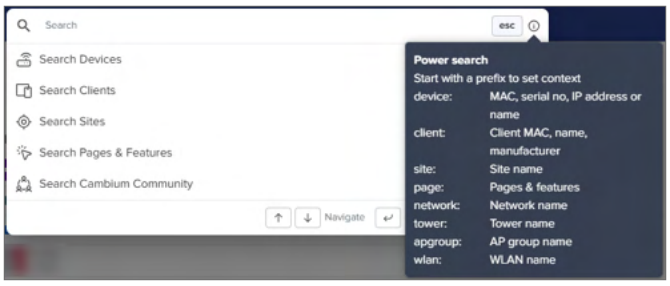
The Search bar at the top of the cnMaestro homepage allows users to easily search for and access cnMaestro resources, such as, onboarded devices, unmanaged devices, clients, sites, pages or features, and community posts. You can also search for towers, networks, WLANs, and AP groups.



- **Search Devices**—Search devices that are present in your cnMaestro account. You can search for devices by using the name, MAC address, serial number or the IP address.
- **Search Clients**—Search for clients connected to the Cambium devices with the help of the name, MAC address, or the manufacturer name.
- **Search Sites**—Search for sites using the site name.
- **Search Pages and Features**—Search for pages or feature names to directly access those pages.
- **Search Cambium Community**—Search for support pages from Cambium Networks community.

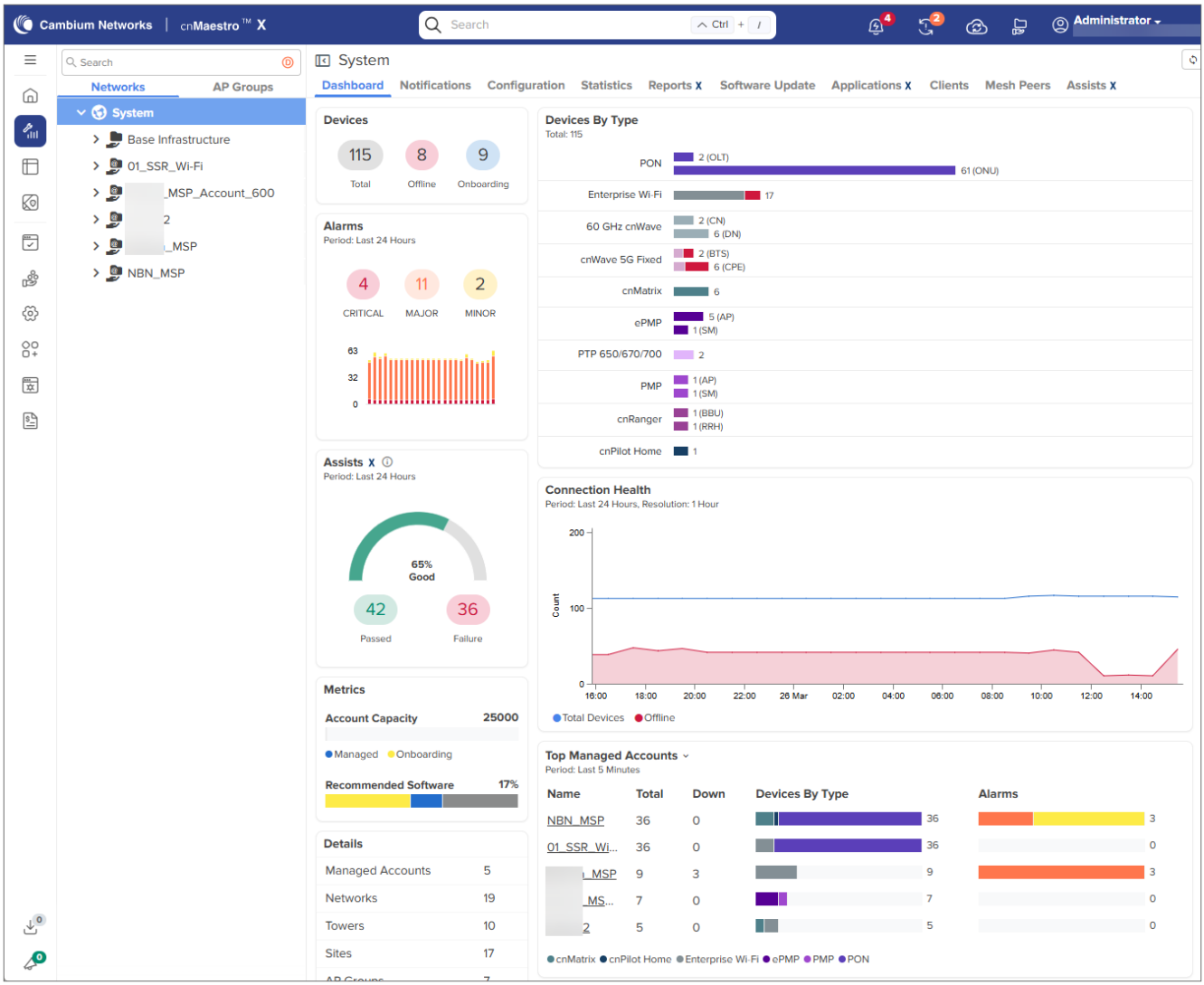
Users can also perform a power search by using certain predefined prefixes so, so as to set the context of the search, as shown below:

For example, to search for any network in your account, type `network:` <network-name> and press Enter.



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 16.



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.

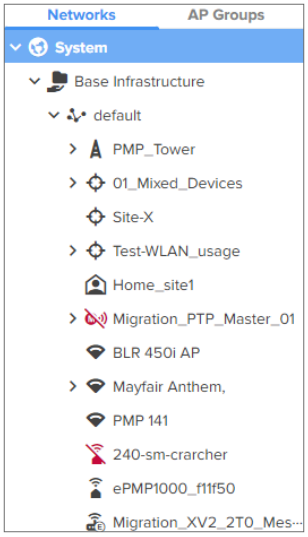
Note

- 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 the Access and Backhaul view.

- 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 16 *Networks*



The structured hierarchy has the following nodes:

Table 14 *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.

Table 14 *Structured hierarchy nodes*

Icon	Name	Description
	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.
	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**.
	Home Site	Home sites are located within networks and contain cnPilot Home Router (r-series) APs.
	Network	All devices are placed within **Networks**. Networks represens 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).
	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.

Table 14 *Structured hierarchy nodes*

Icon	Name	Description
	PTP Master	Point-to-Point (PTP) Master device located in a network and optionally mapped to a Tower.
	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.
	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 15 *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 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.

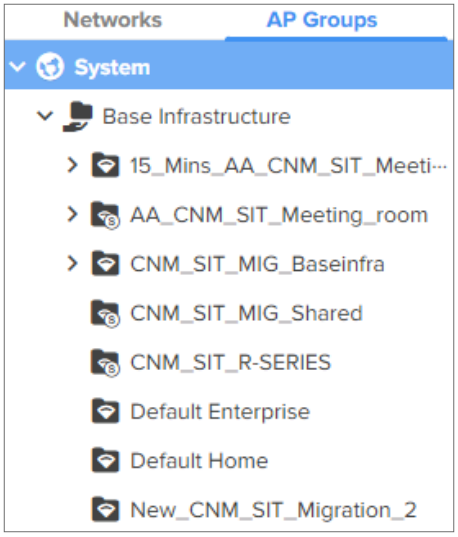
Table 15 *Tree menu*

Action	Node	Description
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.
Download PoP(s) Onboarding Config	Network and PoP Nodes	Download PoP(s) Onboarding Configuration data.
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.
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 17 *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.

On the **System** > **Dashboard** page, click the map view ( ) icon to access the expanded view of the MAP.

Note

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

Figure 18 *Map navigation*

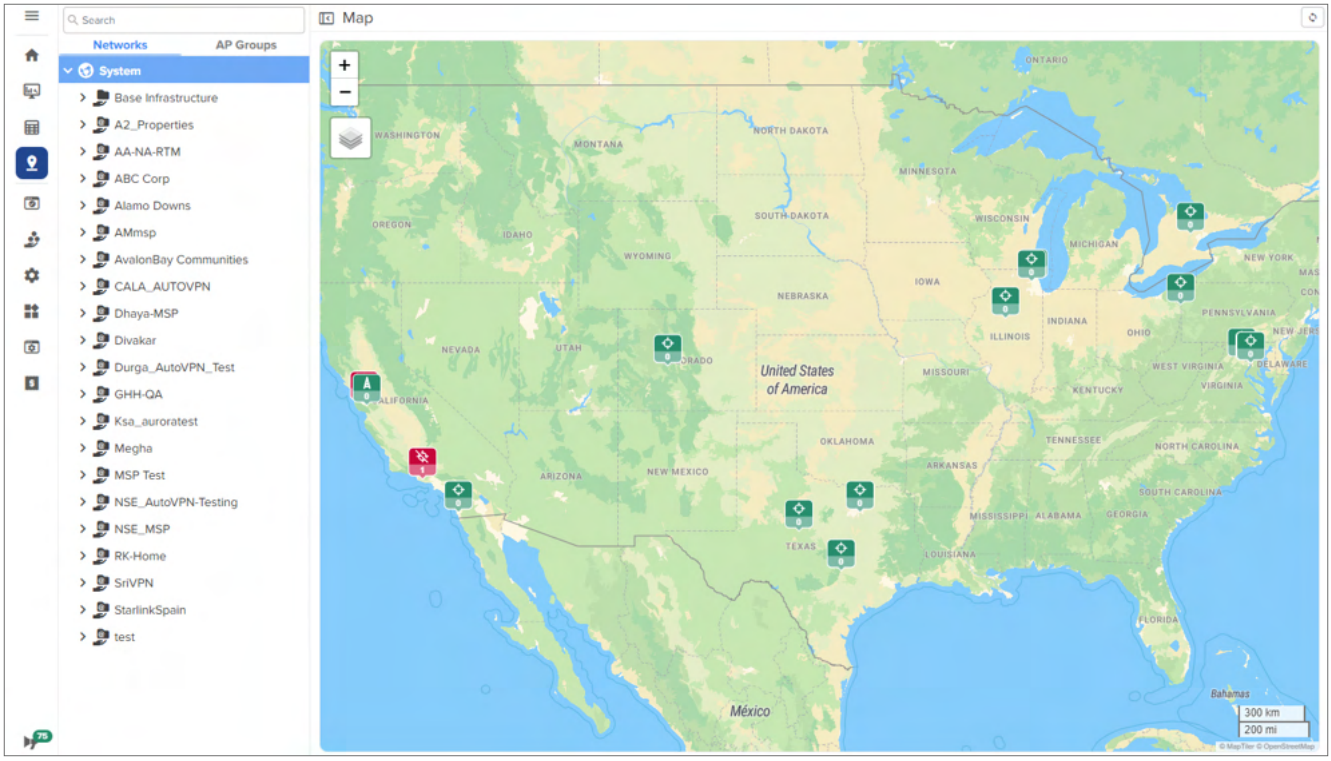


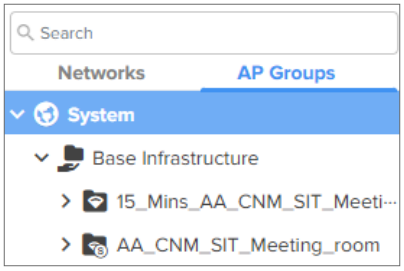
Table navigation

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 19 *Node search*



Enterprise Account view

Overview

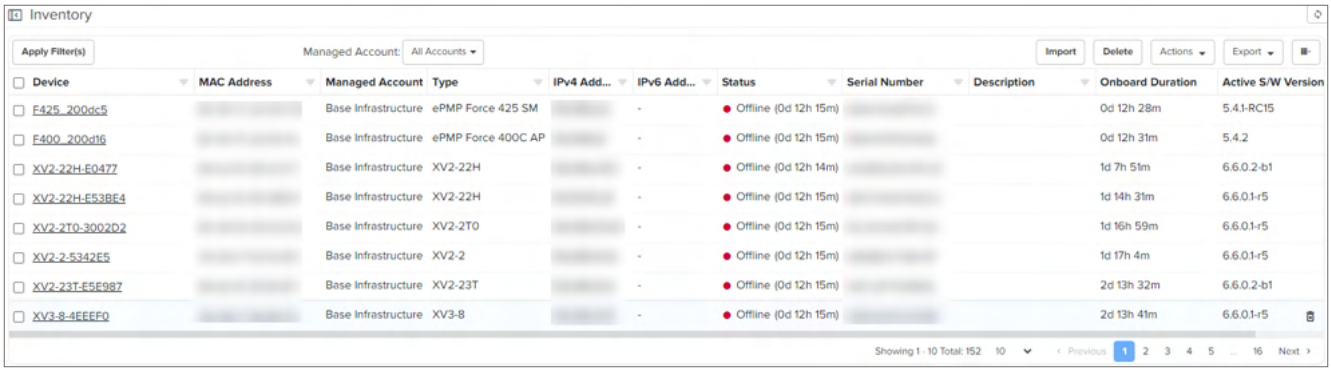
The Enterprise account differs from Access and Backhaul in that it is largely table-driven. It does not have the Quick Buttons or the Device Tree, instead, it has direct navigation for Devices, AP Groups, WLANs, Switch Groups, and Sites. Each of these is presented in tabular form.

System

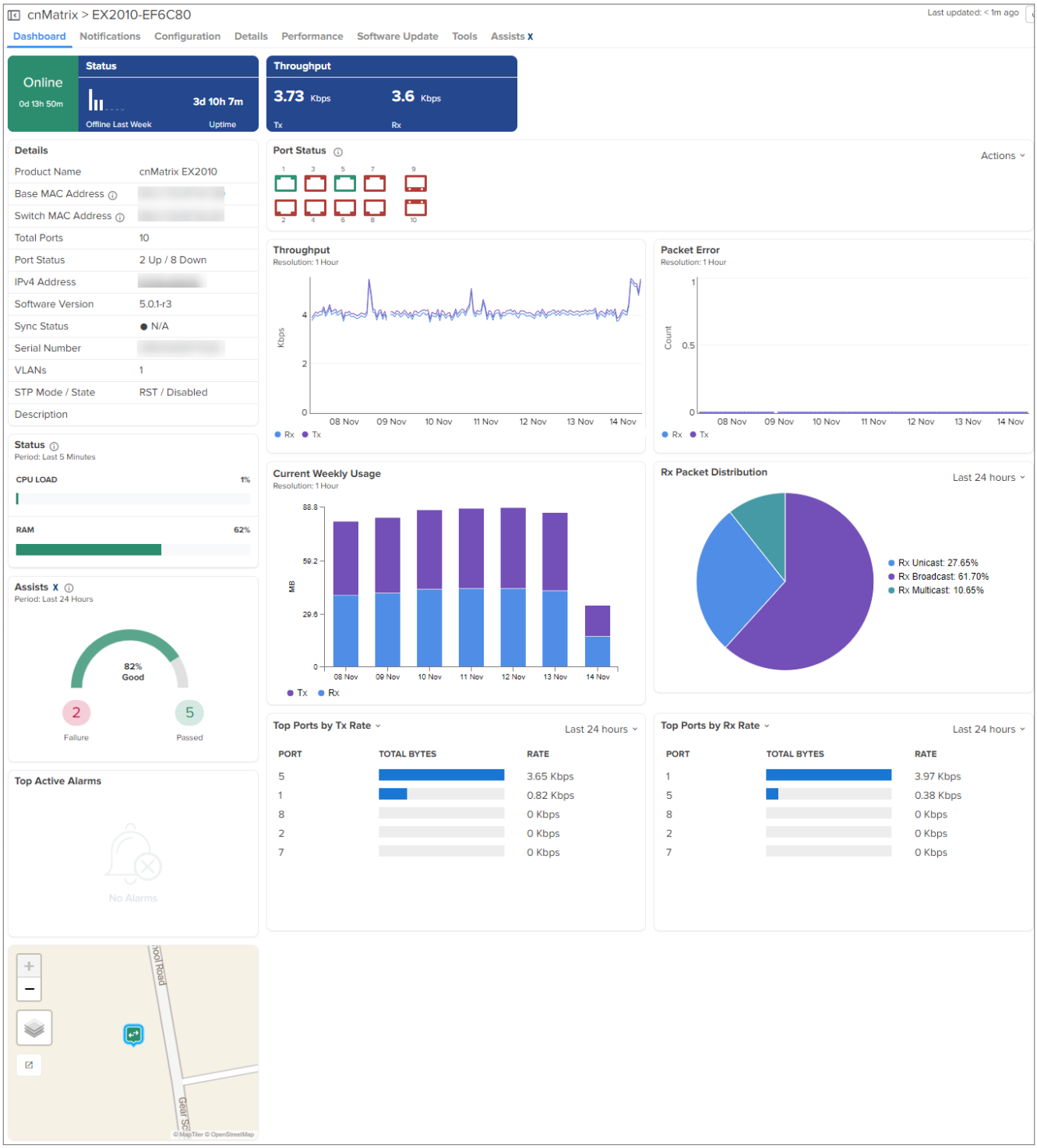
Global functionality is presented in the System menu. It aggregates data across the entire installation.

Devices

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



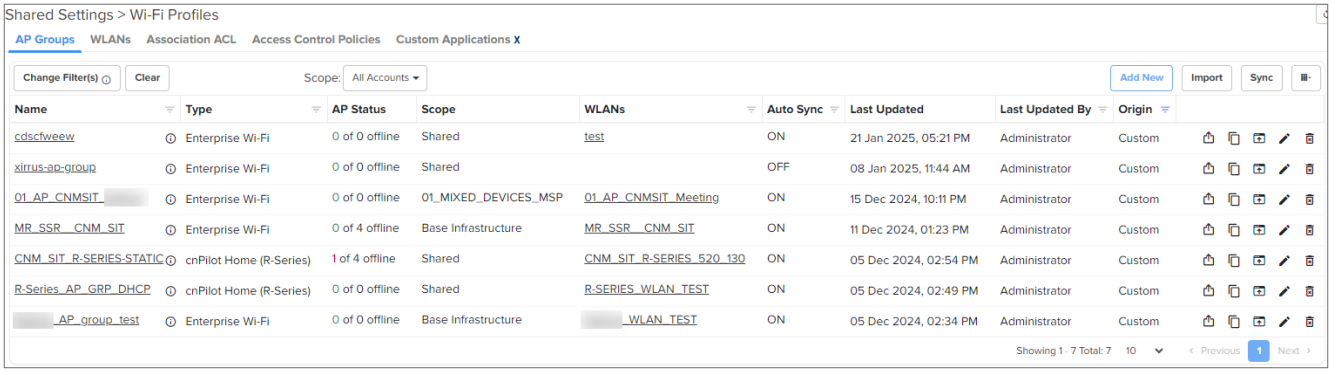
Selecting a device launches its management page.



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 20 *AP Groups*

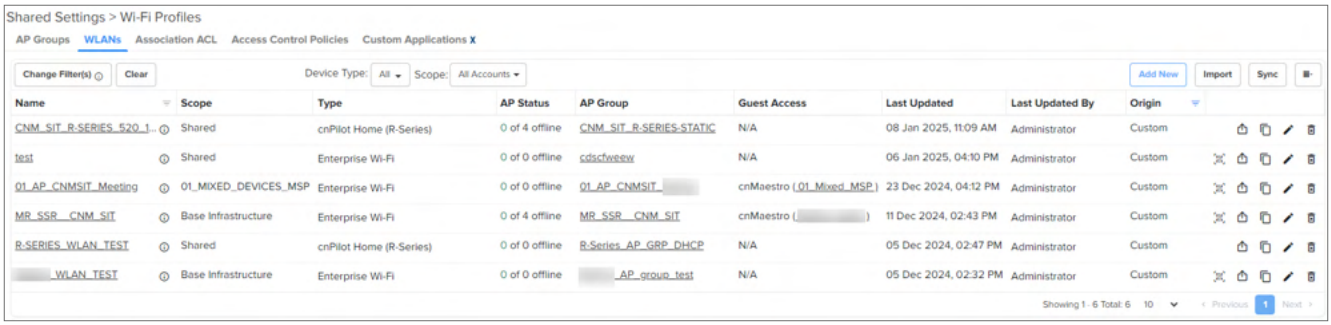


WLANs

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 21 *WLANs*



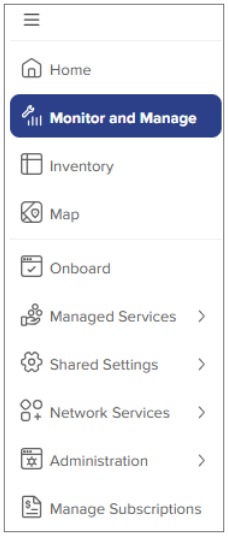
Sites

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 22 *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 16 *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
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.

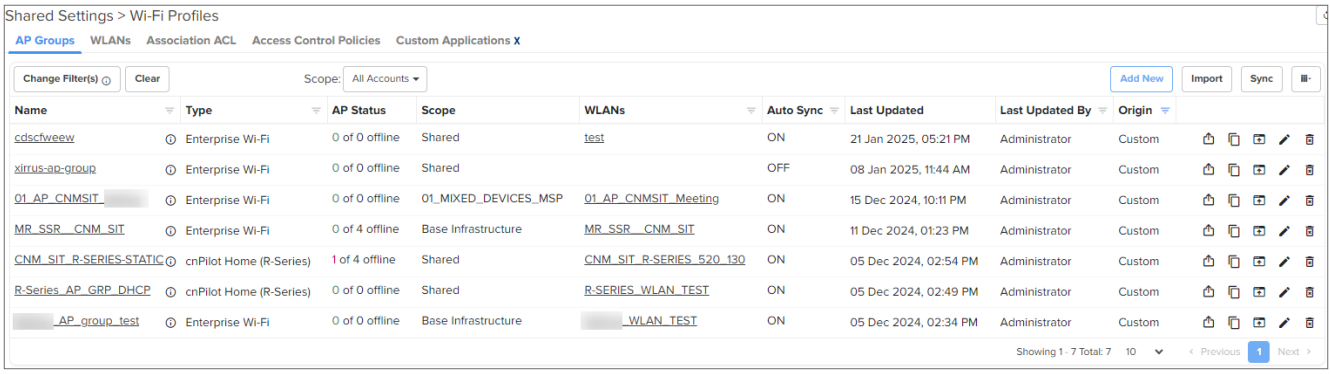
Table 17 *System status icons*

Icon	Name	Description
	Announcements	Notifies the latest Device Software images, Package, or OVA to upload from Cloud.
	Cloud Connectivity Status	It notifies that cnMaestro Cloud is Synced or not with the On-Premises.
	Major Alarms	The count of critical and major alarms raised in the system.
	Out-of-Sync Devices	The number of Wi-Fi and cnMatrix devices with unsynchronized configuration (which can occur when automatic synchronization is disabled in the respective group configuration or if 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:

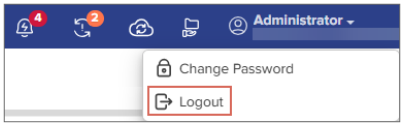


Note

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**.

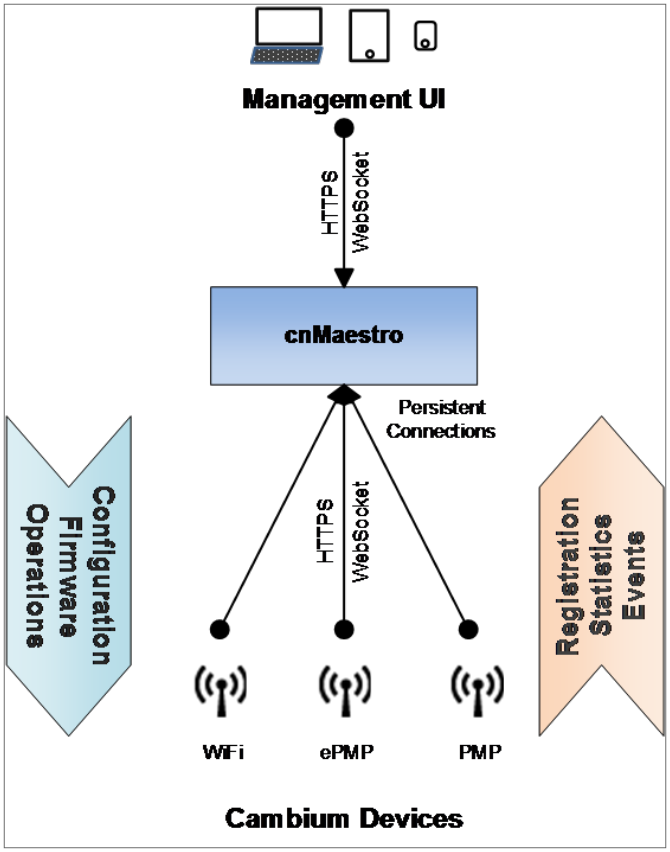


Architecture

The diagram below presents a simplified view of the cnMaestro architecture. Both devices and users contact cnMaestro over a secure HTTPS connection. The device connection uses WebSockets and is persistent. The device periodically sends data to cnMaestro (such as metrics and events), and cnMaestro directs the device to update configuration and software (among other operations).

In cnMaestro On-Premises, devices must be configured to contact the cnMaestro instance (by default, they access https://cloud.cambiumnetworks.com). This can be done either by configuring the device through its UI, or by setting the DHCP options, as described in the Windows DHCP topic.

Figure 23 *On-Premises architecture*



Networking

Most connection issues occur because the device is unable to contact cnMaestro. If devices do not enter the Onboarding Queue it may not be able to reach cnMaestro. Use the Ping and Traceroute tools on the device to troubleshoot.

Note

- Devices must have a route to the cnMaestro On-Premises server.
- A static IP address or hostname for cnMaestro server, so it will persist over time.
- An outbound connection from the device must be allowed for port 443.
- An outbound connection will also be required for port 80 for legacy software on some devices. If your devices are running an image older than the one listed below, outbound connectivity over port 80 is needed for software update. The versions listed (and later) support port 443.
  - 60 GHz cnWave (External Controller) 1.0.1
  - 60 GHz cnWave (Onboard Controller) 1.0.1
  - cnPilot E-Series / ePMP 1000 Hotspot: 3.2.1-r6
  - cnPilot R-Series: 4.4.2-R2
  - cnRanger 1.0.1.0-r1
  - cnReach: All versions
  - Enterprises Wi-Fi 6 APs: 6.0

- ePMP: 3.2
- PMP: 15.0.1
- PTP: All versions

High Availability (HA)

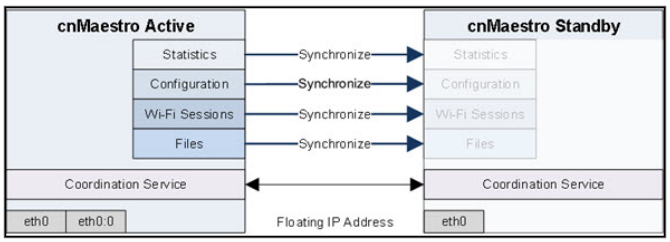
This section includes the following topics:

- Overview
- HA Cluster Setup
- HA Menu

Overview

cnMaestro On-Premises supports Layer 2 HA through an active-standby (1+1) architecture. The default HA installation has a single management interface (eth0) and a shared (floating) management IP address. The basic deployment is highlighted below:

Figure 24 *Overview of High Availability*



Primary vs Secondary

The Primary server always has up-to-date configuration and data, and it hosts the cnMaestro application. The Secondary replicates data from the Primary and enters standby state when fully synchronized.

Shared (Floating) IP Address

A Shared IP address is used onboard the devices apart from cnMaestro access. It is configured in devices for onboarding purpose or typed into a Web browser to launch the cnMaestro UI. Since the shared IP migrates between the two installations, it must be on the same subnet as both static IPs.

Network Ports

The following ports/protocols must be accessible between the two systems:

Ports	IP Type	Details
22	TCP	Data Replication
8300	TCP	Distributed Synchronization
8301	TCP, UDP	Distributed Synchronization

Recommendations

Cambium Networks recommends backing up virtual machines prior to starting HA. To take daily automated backups of cnMaestro configuration, navigate to **Administration** > **Server** > **Operations** > **System Backup and Restore**. For larger installations, and to backup statistics, refer to the section on backing up the data disk.

Note

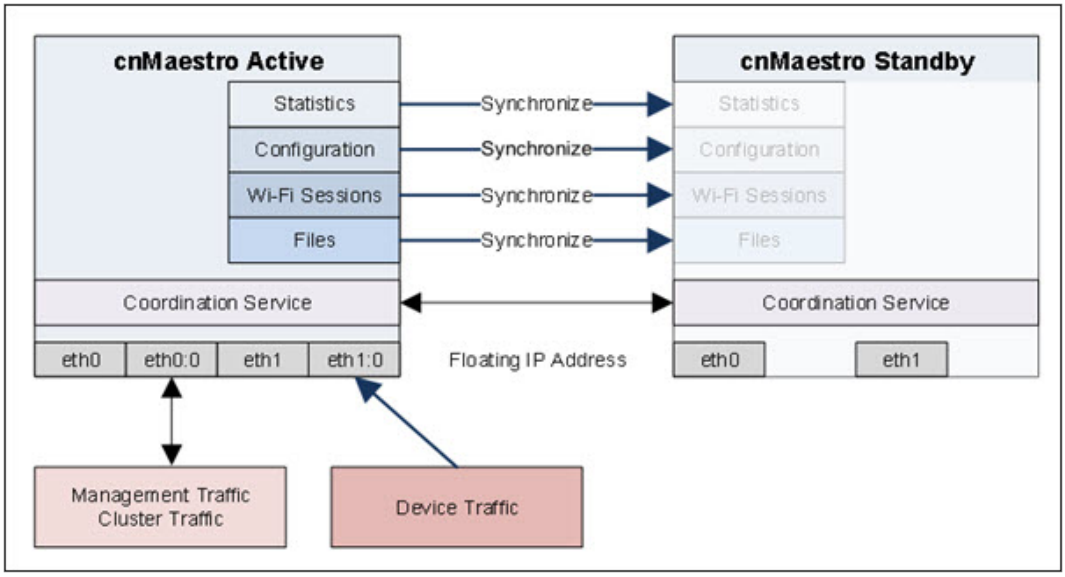
1. Both the primary and the secondary cnMaestro instances must be up and running all the time.
2. Both the primary and the secondary cnMaestro instances must be having the same software version always.
3. Each instance must be configured with a static IP address. A shared floating IP address is hosted by the primary server.
4. Both the primary and standby cnMaestro instances need to be on the same VLAN.
5. HA Cluster traffic uses TCP ports 22, 8300, and 8301, which must not be blocked.
6. HA enabled servers share the same Serial Number when they are in a cluster. When resetting or deleting a peer, both the standalone servers attempt to connect to the Anchor account every 15 minutes. To resolve this conflict, you need to either poweroff or delete one of the instances.

Dual Interfaces

cnMaestro can be provisioned with two interfaces, eth0 and eth1, or when hosted on Hypervisors such as ESXI, KVM and so on. These allows traffic to be segmented into Management/Cluster and Device/Control. Starting with 3.1.0 release, this traffic separation will be strictly enforced. The implementation allows deployments with separate management and control subnets to integrate more easily with cnMaestro.

Traffic Type	Interface	Details
Management/Cluster	eth0	User interface, Cluster, API, outbound traffic to Internet
Device/Control	eth1	Device control traffic

A high-level overview of the separation is below:



> **Note**
>
> Overriding the management/control traffic separation is possible with a dual interface installation by applying a network override.

Perform the following steps to apply a network override:

Override the Management (eth0) Interface to Accept Control Traffic

1. Manually edit /srv/files/etc/cnmaestro-network.overrides to include the following:

```
iptables -t nat -D PREROUTING -i eth0 -p tcp --dport 443 -j REDIRECT --to-ports
1443
iptables -A INPUT -i eth0 -p tcp -m tcp --dport 443 -j ACCEPT
```

2. Restart the system (or type sudo /srv/bin/cnmaestro-network)

Override the Control (eth1) Interface to Accept Management Traffic

1. Manually edit /srv/files/etc/cnmaestro-network.overrides to include the following:

```
iptables -t nat -D PREROUTING -i eth1 -p tcp --dport 443 -j REDIRECT --to-ports
1444
iptables -A INPUT -i eth1 -p tcp -m tcp --dport 443 -j ACCEPT
```

2. Restart the system (or type sudo /srv/bin/cnmaestro-network)

High Availability Deployment Considerations

In a High Availability deployment, if the overrides file is edited on the Primary instance, it is automatically replicated to the Secondary. However the Secondary will still need to be manually restarted in order for the update to take effect.

Add eth1 Network Adapter

To add eth1, the virtual machine needs to be stopped, and a second Network Adapter added manually. Adding multiple adapters to a virtual machine leads to issues with PCI ordering, which determines how eth0 and eth1 are mapped to the running VM: the PCI ordering does not necessarily follow the order of interface addition. The section below details how to make sure the PCI ordering is correct.

Network Interface PCI Ordering

In a two-interface configuration, VMware may apply Network Interfaces in an order different than that presented in the UI. This may result in a second interface mapped to eth0 instead of eth1. In order to resolve this, you may need to update VMware configuration.

VMware Workstation

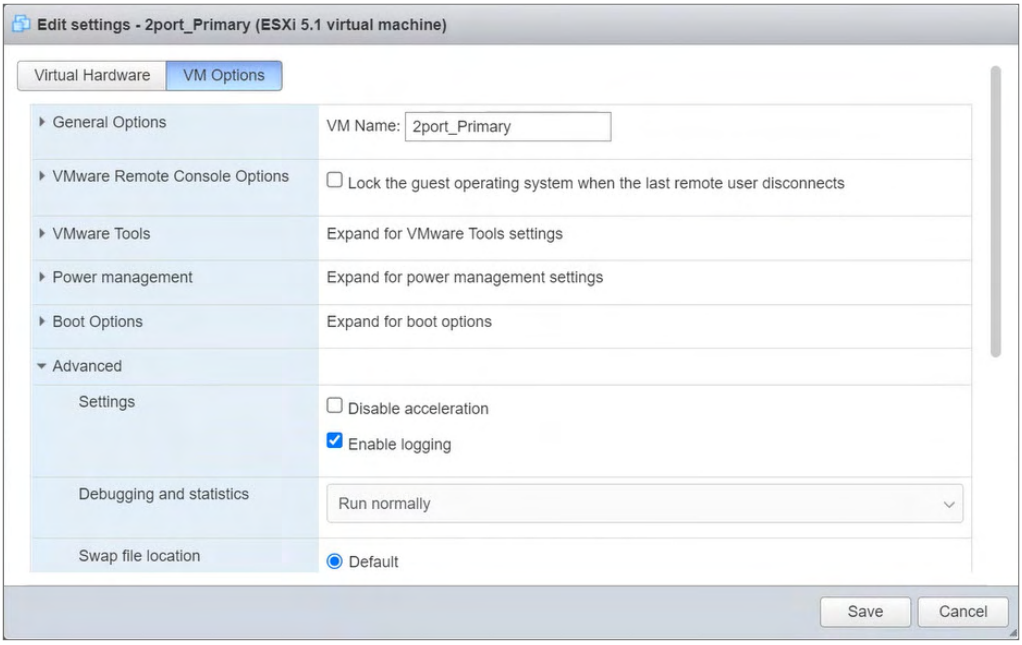
In VMware Workstation, edit the configuration file (ending in .vmx) in the virtual machine home directory. After shutting down the VM, change the following two entries, so the eth0 PCI number is lower than eth1.

```
ethernet0.pciSlotNumber = "33"
ethernet1.pciSlotNumber = "34"
```

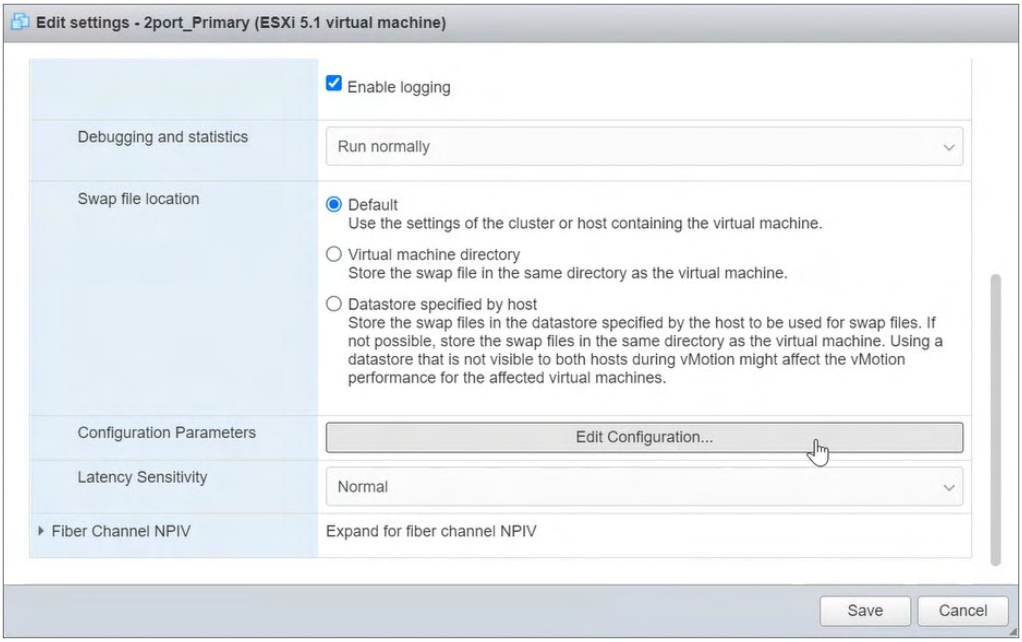
VMware ESXi

The same operation is required for VMware ESXi, but it can be performed through the UI.

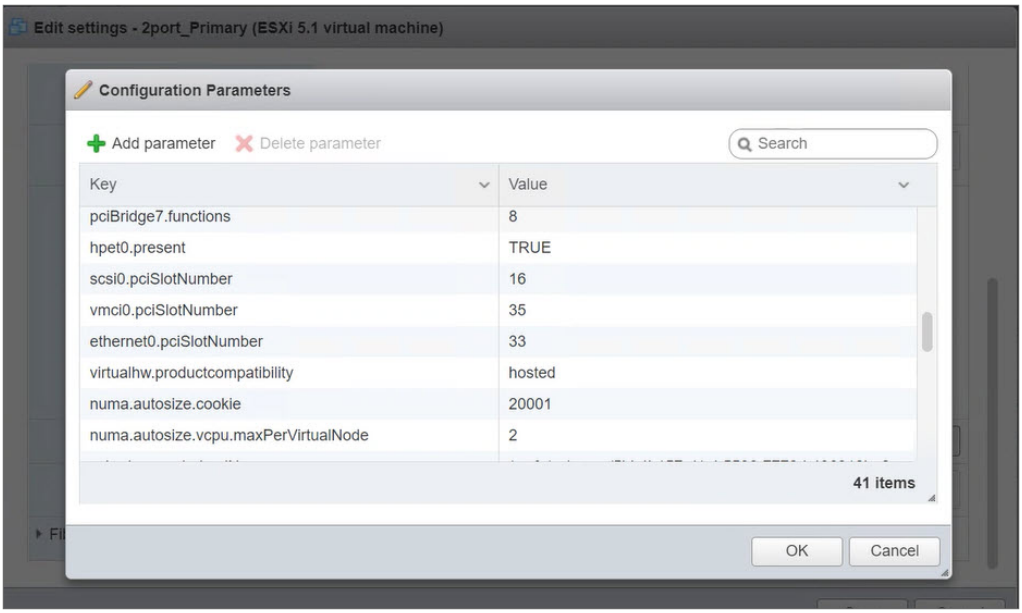
1. Select **Edit Settings** of the VM and choose **VM Options** > **Advanced**.



2. Scroll down and select **Edit Configuration**.



This launches a screen that allows updating the PCI numbers.



HA Cluster Setup

HA Cluster Setup requires bootstrapping the Primary system and then adding the Secondary. The high-level steps are defined below. All cluster operations are performed through the cnMaestro Console.

Bootstrap (Primary)

The first step is to enable high availability on a cnMaestro instance – effectively creating a HA cluster and initializing high availability processes. The bootstrapped instance is called the Primary, and it hosts the shared IP address.

Accept (Primary)

The Primary server then configures a shared secret to allow a Secondary system to join the cluster. The secret is used for authentication, and it is valid for 30 minutes.

Join (Secondary)

The Secondary joins the Primary using the shared secret, and extends the Cluster. At this point, the Secondary begins replicating data (which could take many minutes). Once fully replicated, the Secondary becomes standby and is able to fail-over.

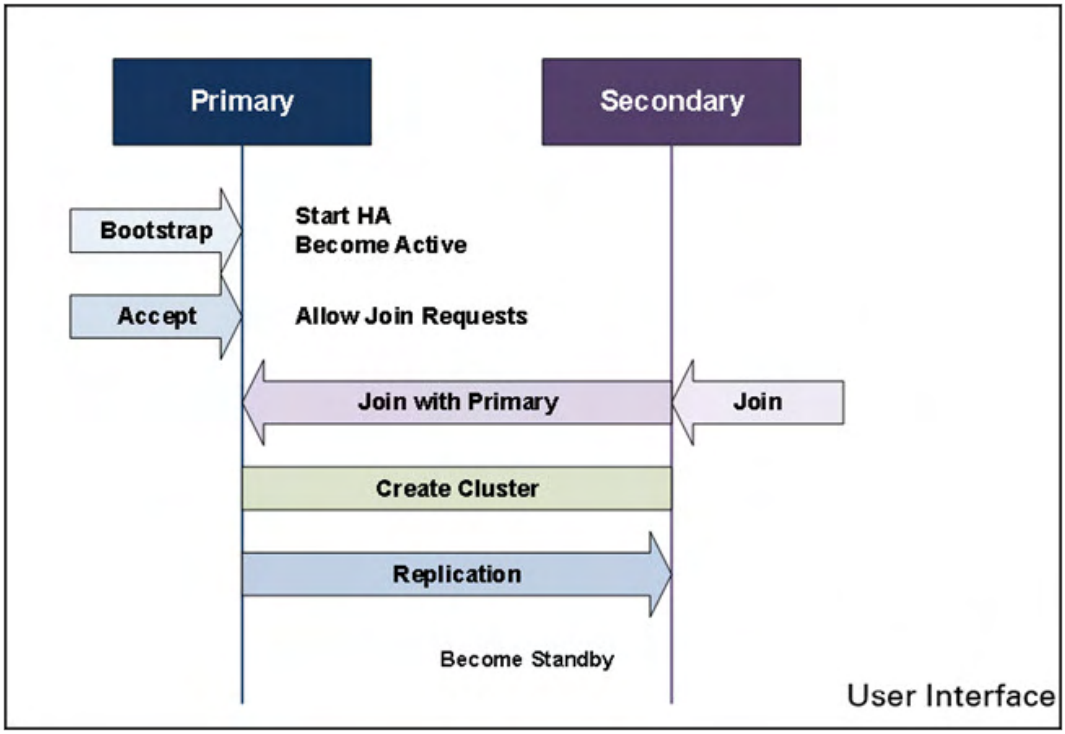
Note

The Join process uses SSH (port 22) to connect to the Primary. It is important to review the fingerprint displayed during the Accept and Join operations, to make sure they are the same (and protect against man-in-the-middle attacks).

Warning

All data on the Secondary will be overwritten during the operation.

Figure 25 *Accept Join*

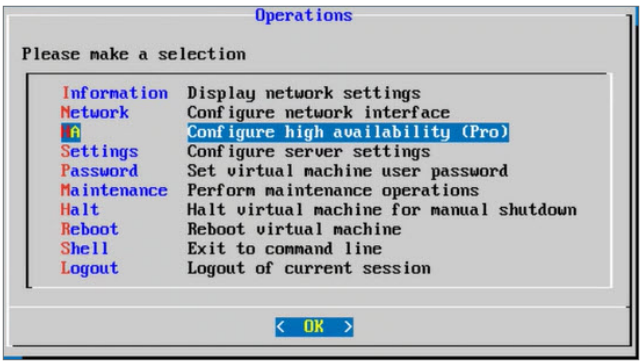


Basic HA Cluster Creation Flow

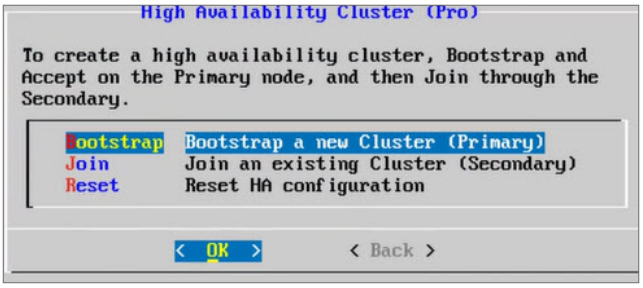
A general HA configuration flow is presented below. Each page will be discussed independently in later sections.

Primary Server

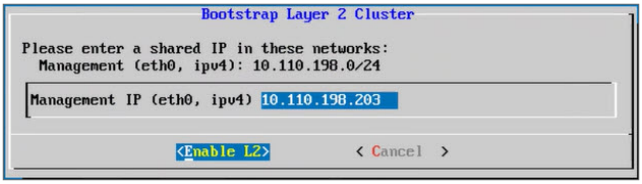
1. After logging into cnMaestro console, from **Operations** tab, select **HA** and click **OK**.



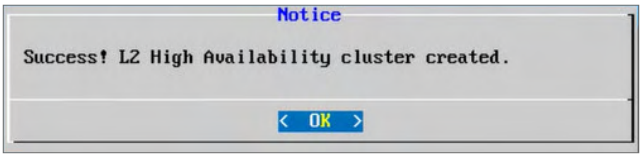
2. From **High Availability Cluster** tab, select **Bootstrap** and click **OK**.



3. From the **Bootstrap Layer 2 Cluster** tab, enter **Management IP** and click **Enable L2**. The Management IP must be on the same subnet as the eth0 interface.



L2 High Availability Cluster is created, success window pops up as shown below.



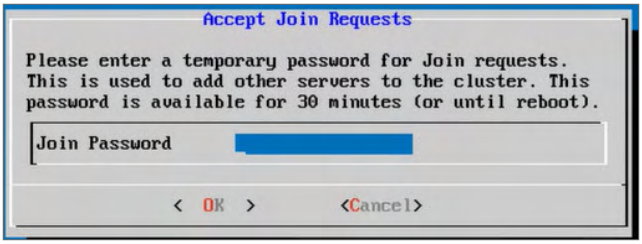
The Primary Bootstrap is successfully completed.

4. Click **OK**.

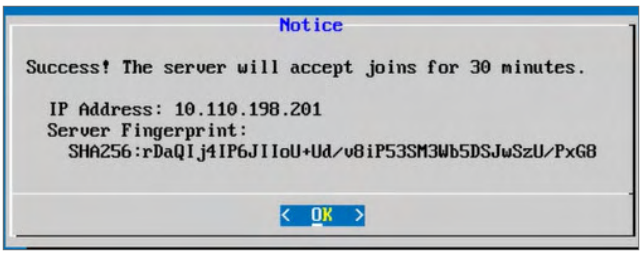
   Accept Join Requests page displays.

5. Enter a temporary password for Join requests.

   This password is used by the Secondary system to authenticate and join, the Cluster. It is valid for 30 minutes.



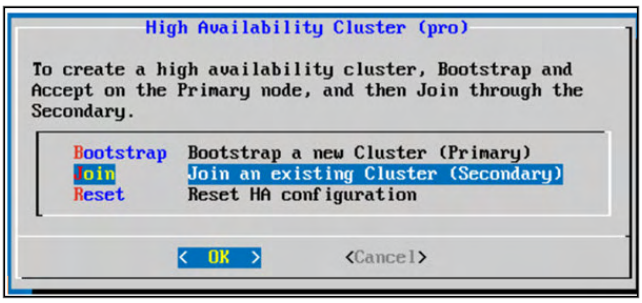
6. After the **Join Password** is set, click **OK** to initialize the system for 30 minutes.



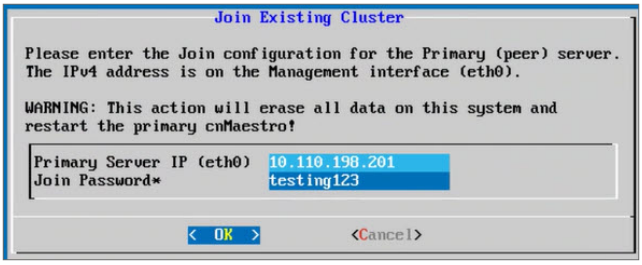
7. A SSH Fingerprint is generated. Match the fingerprint to the one displayed during the Join process.

Secondary Server

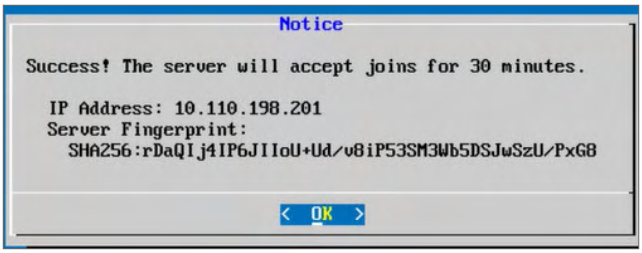
1. On the Secondary cnMaestro server, from the **High Availability Cluster** menu, select **Join** and click **OK**.



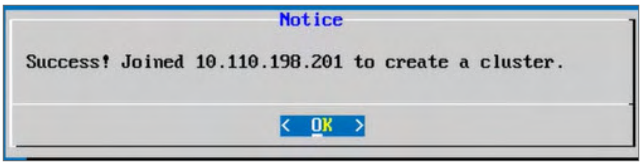
2. **Join Existing Cluster** window appears. Enter the **Primary Server IP (eth0)** and the **Join Password**, click **OK**.



A pop-up window displays the fingerprint of the Primary server. Validate the fingerprint shown on the Secondary exactly matches the fingerprint of the Primary (when it is accessed directly). If the fingerprints are different, the Primary server is incorrect, and the Join should be cancelled.



3. After verifying and continuing, the successfully joined cluster window appears.

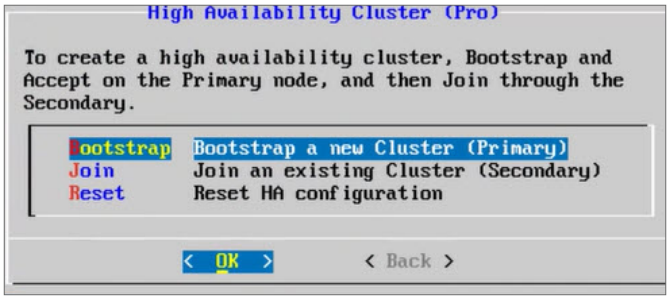


HA Menu

This section walks through the different HA tabs available in the console.

High Availability Cluster Menu (Pre-Bootstrap)

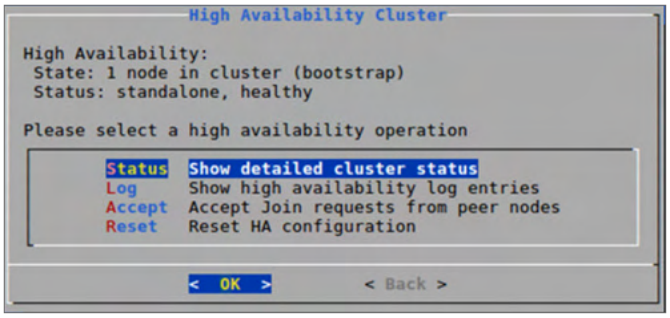
This menu is available before HA is enabled and the cluster has been created.



Field	Description
Bootstrap	Convert standalone instance into HA cluster.
Join	Join a standalone HA Cluster to create a replication Cluster.
Reset	Reset HA infrastructure to default. This option is provided as a failsafe.

High Availability Menu (Post-Bootstrap)

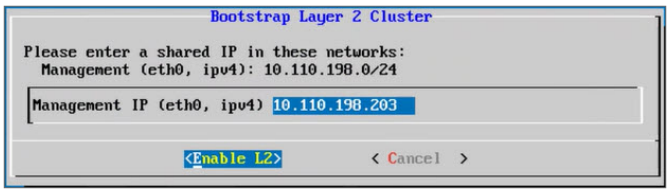
This menu is available after a successful Bootstrap.

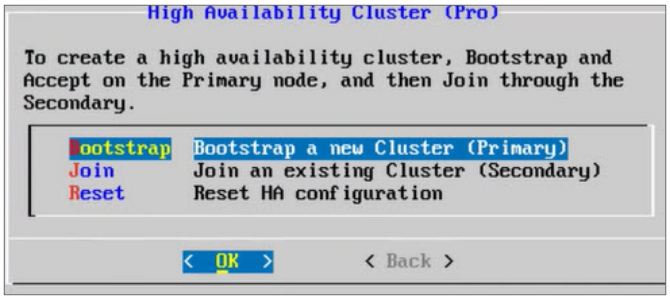


Field	Description
Accept	Join requests from the peer nodes.
Log	Log entries of High Availability.
Reset	Reset HA configuration.
Status	Overall status for the Cluster.

New Cluster

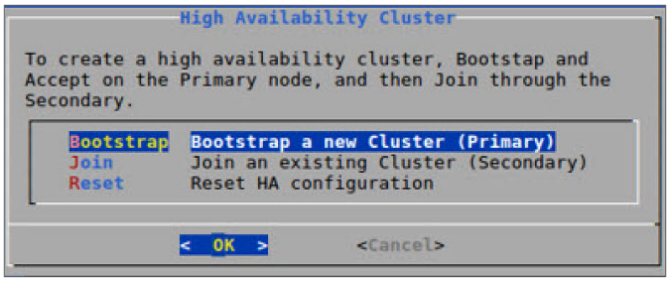
An HA Cluster requires the eth0 interface be configured with a static IP address. Once the Cluster is created, the IP address cannot be changed without dissolving the Cluster. During the bootstrap process, a shared IP address is configured in the same subnet as eth0. This address floats between the active cnMaestro system, and it should be used for cnMaestro access.





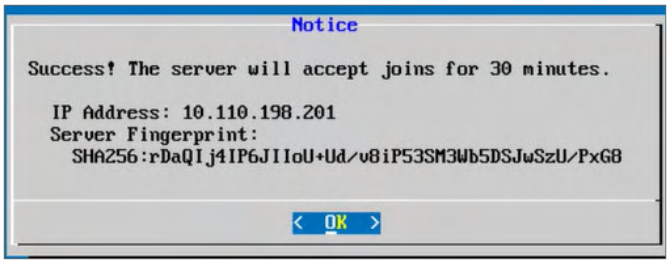
Accept Join Requests

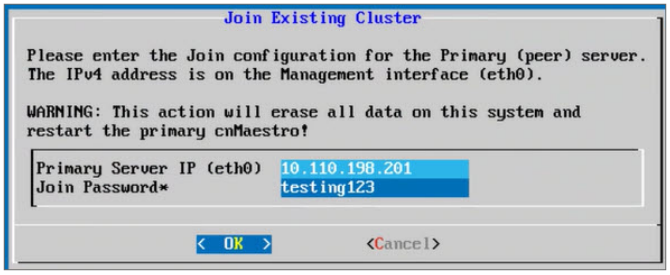
As part of the Bootstrap process, create a shared password used during the Join. The password will be available for 30 minutes after creation.



Join Existing Cluster

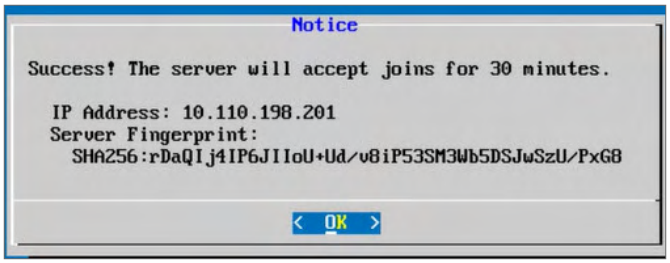
To join another system to the Cluster, select the Join option of the HA menu on the Secondary Server. The IP address is the eth0 address for the Primary server (only the eth0 IPv4 address is used to create a cluster). The Password is the same created during Accept.





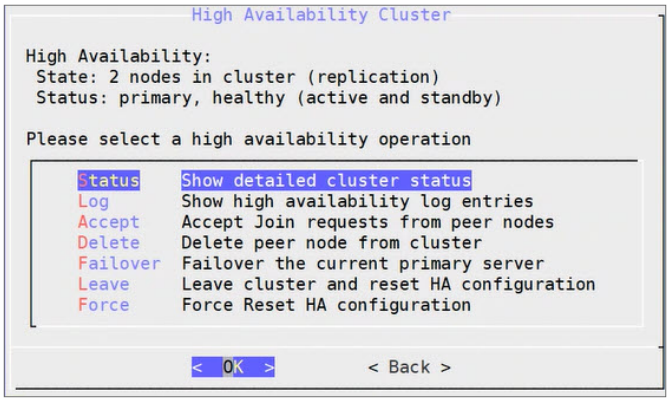
Validate SSH Fingerprints

Customers should validate the fingerprint before joining. If the fingerprint on the Primary is different than the fingerprint displayed at the Secondary, the Join should be canceled, because the Primary server is incorrect.



HA Cluster Status

The HA Cluster Status tab details the current HA state, including the replication status. After a cluster operation, it may take a few minutes for the page to show full details.



Field	Description
Accept	Set a password used by another system to join the Cluster.
Delete	Delete a node from the Cluster.
Failover	Failover to the current Standby node. This is not visible while standalone.
Force/Reset	Forcibly Reset HA configuration. This causes a non-graceful reset of the current node, and it does not delete the node from the Peer. This operation should only be used if the Leave operation fails.
Leave	Leave the Cluster. This deletes all HA configuration and puts the device into a default state.
Status	Overall status for the Cluster.

Select **Status** and click **OK**. The following window appears:

```
HA Cluster Status

State: Primary (active)
Mode: Replication (2 nodes in cluster)
Type: Layer 2
Shared IP (eth0): 10.110.198.203

Statistics: Primary, Replicating (synchronized)
Configuration: Primary, Replicating (synchronized)
Wi-Fi Sessions: Primary, Replicating (synchronized)
Files: Primary, Replicating (synchronized)

Cluster Servers:
    10.110.198.201 (alive) *self
    10.110.198.202 (alive)

<Refresh>          < Back  >
```

```
HA Cluster Status

State: Secondary (standby)
Mode: Replication (2 nodes in cluster)
Type: Layer 2
Shared IP (eth0): 10.110.198.203

Statistics: Secondary, Replicating (lag: 5 seconds)
Configuration: Secondary, Replicating (synchronized)
Wi-Fi Sessions: Secondary, Replicating (synchronized)
Files: Secondary, Replicating (synchronized)

Cluster Servers:
    10.110.198.202 (alive) *self
    10.110.198.201 (alive)

<Refresh>          < Back  >
```

Field	Description
Statistics	Status of statistics data replication (this tends to take the longest).
Configuration	Status of configuration replication.
Wi-Fi Sessions	Status of Wi-Fi session replication.
Files	Status of file system replication (including floor maps, etc.).

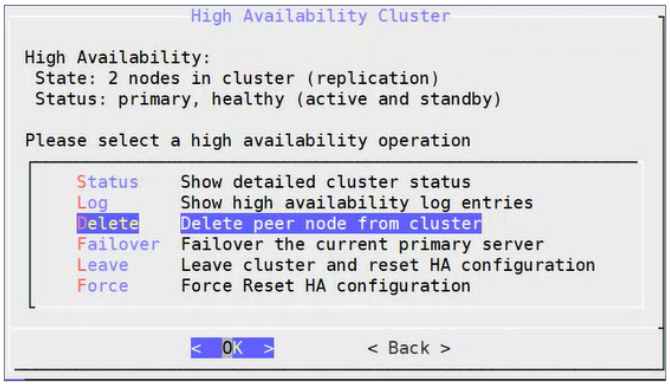
Delete Node

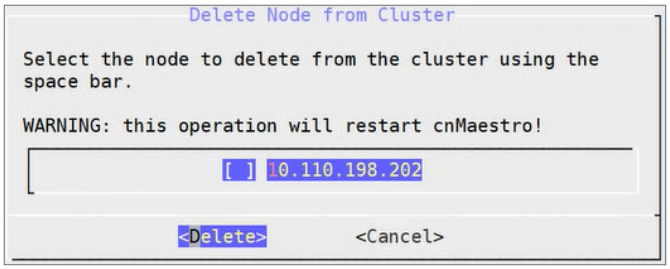
Delete from Cluster

Deleting removes the peer node from the cluster. Navigate to **Operations** > **HA**, select **Delete** and click **OK**.

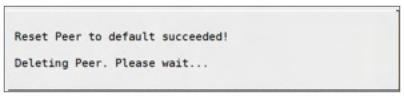
Use the space bar to select the Node and select **Delete** and click **Enter**.

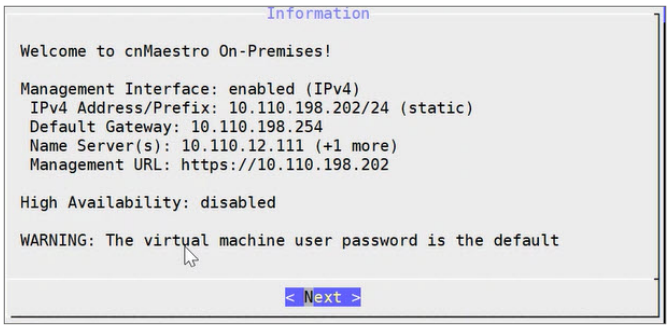
Deleting a Node Resets the HA configuration of the node and removes it from the Cluster (as long as the node is still online). If the node is down, or unresponsive, it needs to be manually removed by accessing the node itself and selecting **Leave**.

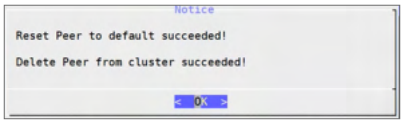




After deletion, HA has been reset on the deleted node, and the current node becomes Standalone.







Note

After node deletion, it is recommended to perform Force/Reset operation under HA menu.

Leave Cluster

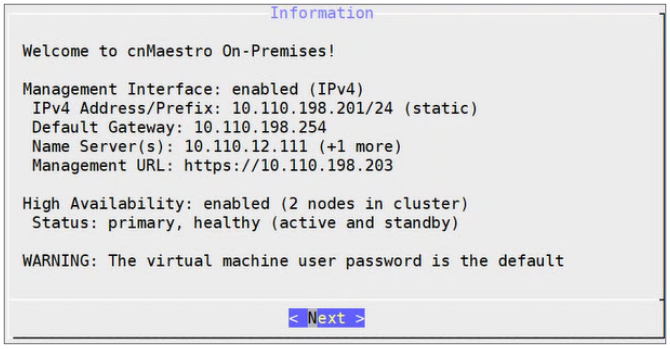
Leaving removes the current node from the cluster. It first tries to delete the node from the peer; then it resets the current node to default. If the delete fails (for example, if there is no network connectivity), it needs to also be deleted manually through the peer Console.

Note

After Leave operation, it is recommended to perform Force/Reset operation under HA menu.

Information

The Information page provides global status for the system at initial login. It has a High Availability section at the bottom.



Behaviour of cnMaestro features when HA is Enabled

This section lists the behavioral changes of cnMaestro features when HA is enabled:

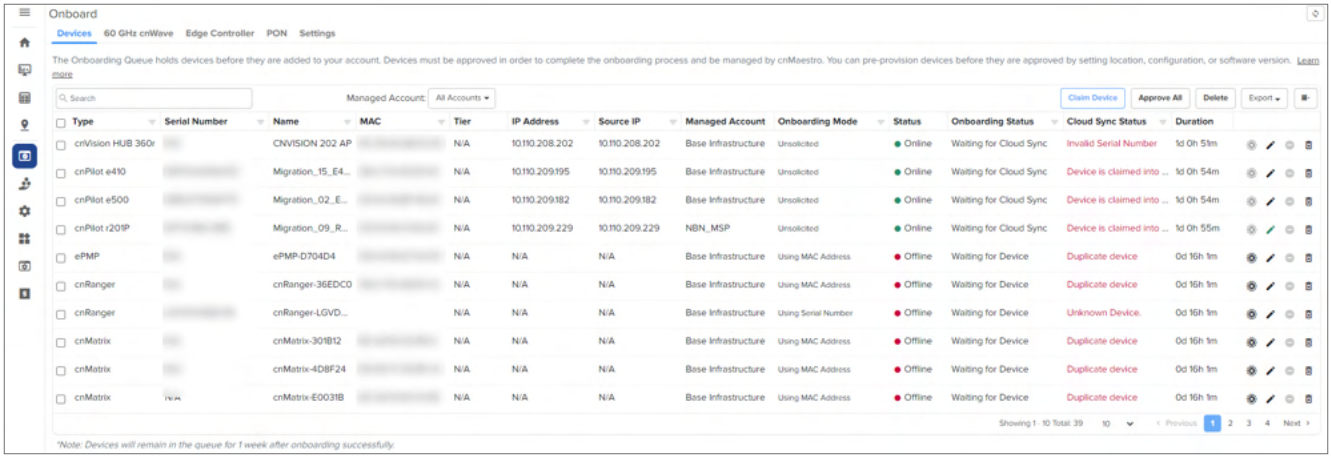
Feature	Observations	
Device Approval from Onboarding Queue	If the fail over happens when Device Approval is In-Progress, then the **Device Approval** will get struck. You have to re-initiate the **Approval All.**	
Software Update Jobs	If the fail over happens when the Software Update job is **In-Progress**, then the devices software update will be Timeout after fail over.	
	Software Update break up	**Impact after failover**
	Software update to 50 devices with **Devices to update in parallel** set as 10.	10 devices which were in parallel updated will get impacted. After failover job will get timed out after 5 minutes. You have to retrigger software update for these 10 devices.
	Software update to 50 devices with **Devices to update in parallel** set as 50.	All 50 devices which were in parallel update will get impacted. After failover job will get timed out after 5 minutes.You have to retrigger software update for 50 these devices.
Configuration push jobs in running state	If the fail over happens when the Configuration Update is **In-Progress**, then the configuration update will be Timeout.	
	Configuration update to 50 devices with **Devices to update in parallel** set to 10.	10 devices which were in parallel update will get impacted. After fail over job will get Time out after 5 minutes. You have to retrigger Config update for these 10 devices.
	Configuration update to 50 devices with **Devices to update in parallel** set to 50.	50 devices which were in parallel update will get impacted. After fail over job will get Time out after 5 minutes. You have to retrigger Config update for these 50 devices.
OVA Upgrade	If failover happens when the OVA upgrade is in progress, then you have to reintiate OVA	

Feature	Observations	
	upgrade.	
	OVA upgrade	**Impact after failover**
	Failover happens during OVA file upload.	File upload is canceled. You have to retrigger it.
	Failover happens during 10% to 100% OVA upgrade.	OVA upgrade is canceled. You have to retrigger it.
	Failover happens after 100% of OVA upgrade and before **Apply.**	File upload is canceled. You have to retrigger it.

Device Onboarding

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 configure the devices before they are approved by setting location, configuration, or software version.

Figure 26 *Onboarding devices*



While onboarding the devices using the different modes the onboarding status changes according to the changes of the Cloud Sync Status till the device gets approved and onboarded.

During onboarding the devices it starts to synchronize with the Cloud Anchor accout. If that Cloud synchronize fails displays the following erros

Table 18 displays the parameters of onboarding page.

Table 18 *Onboarding page parameters*

Parameters	Description
Type	Device type with model number.
Serial Number	Device serial number.
Name	Device name provided during the configuration.
MAC	Device MAC number.

Parameters	Description
Tier	Device tier type.
IP Address	Device IP Address.
Source IP	Source IP address of the device.
Managed Account	Selected managed account name.
Onboarding Mode	Device onboarding mode MAC Address or Serial Number.
Status	Status of the device online or offline.
Onboarding status	Onboarding status of the device. It displays the several status as shown in Table 19.
Cloud Sync Status	Cloud synchronization status of the devices. It displays the several status as shown in Table 20.
Duration	Duration of the onboarding device in days, hours, and minutes.

Onboarding Status

Table 19 describes the onboarding status of the devices.

Table 19 *Onboarding status*

Onboarding status type	Description
Updating	Approved and updating the device configuration to onboard.
Onboarded	Synchronized with Cloud Anchor account and the device is onboarded.
Waiting for Device	Devices to be onboarded.
Waiting for Approval	Approval of devices from On-Premises account.
Waiting for Cloud Sync	Device approved and synchronizing with Cloud.
Onboarding	Synchronized with Cloud Anchor account and the device is onboarding.
Authentication Failed	Authentication fails due to connection between the device and On-Premises Instances.

Table 20 describes the Cloud synchronization errors during the onboarding of devices.

Table 20 *Cloud Synchronization errors*

Cloud Sync error type	Description
Unsupported Device	Does not allow to synchronize the unsupported devices.
Unknown Device	User needs to delete the unknow MAC address of the device.
Invalid Serial Number	Enter the valid serial number and claim the devices.
Device claimed into another account	Error occurs, if On-Premises instances is claimed into multiple Cloud Anchor account. User needs to remove the instances from any one of the Cloud Anchor account.
Internal Error	Unexpected On-Premises instances error.

Cloud Sync error type	Description
Invalid MAC	Enter the valid MAC and claim the devices.
Cloud Sync not allowed	Cloud Anchor account synchronization is not supported for few devices. For example, NSE devices are not allowed to be onboarded on to cnMaestro On-Premises instances.
Device mapped to another instance	Error occurs, if the same device is mapped into multiple On-Premises instances. User needs to remove that device from any of the instances.

Claiming Devices

A device can be claimed when it is added using the Serial Number, MAC Address, or Cambium ID. All claimed devices are placed in the Onboarding Queue. The devices must be approved and cloud synced to become fully managed.

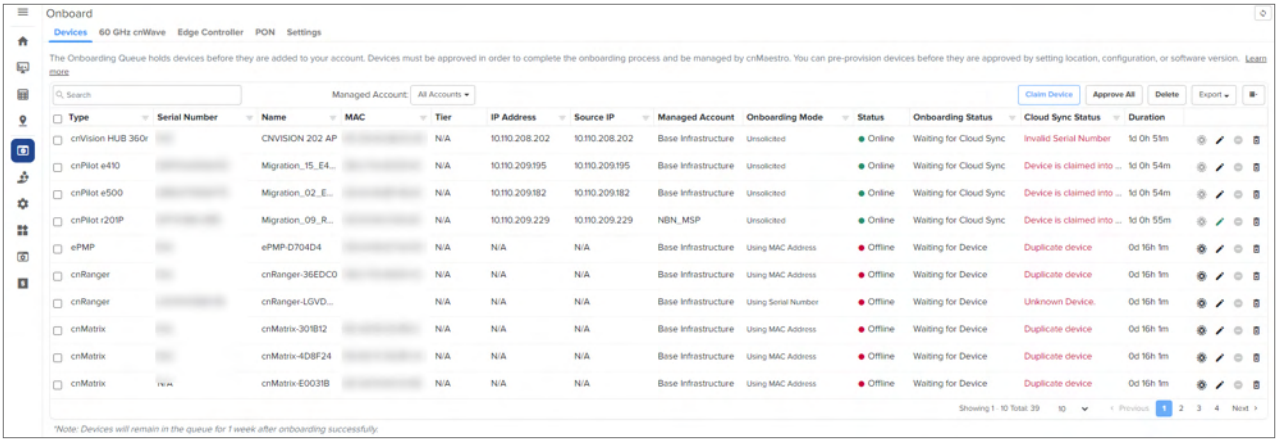
Note

- Only serial numbers with a length of 12 characters can be claimed.
- 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.

Claiming with Serial Number, MAC Address 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.

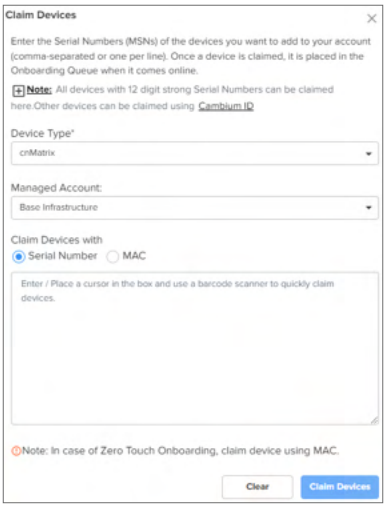
To claim a device, perform the following steps:

1. Navigate to **Onboard** page.



2. Click **Claim Device**.

   Claim Devices window appears.

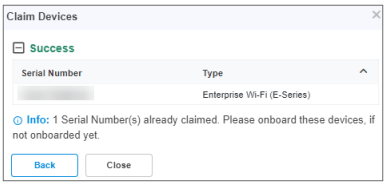


Note

In case of Zero Touch device onboarding, claim the device using the MAC address.

3. Enter the **Serial Number** or **MAC** of the device.
4. Click **Claim Devices.**

   Success window pops up.



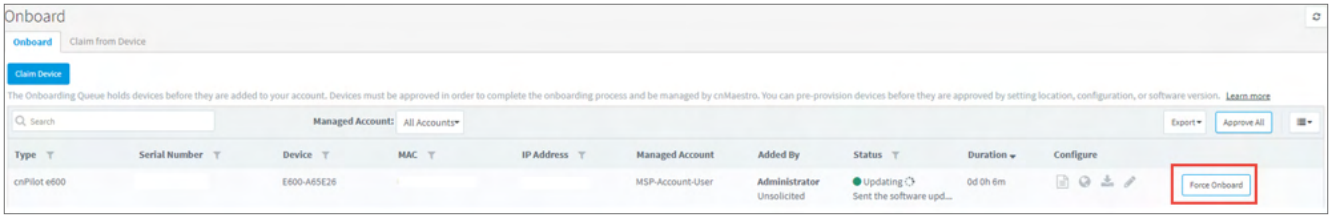
To manage the devices in On-Premises, the Onboarding Queue must be cloud synced and approved. Click the **Approve Device** ( ) button to onboard. Unapproved devices will remain in the Onboarding Queue indefinitely.

Note

- Once approved, the connected devices are onboarded and added to the account, and all configuration or software updates are applied.
- 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.

Note

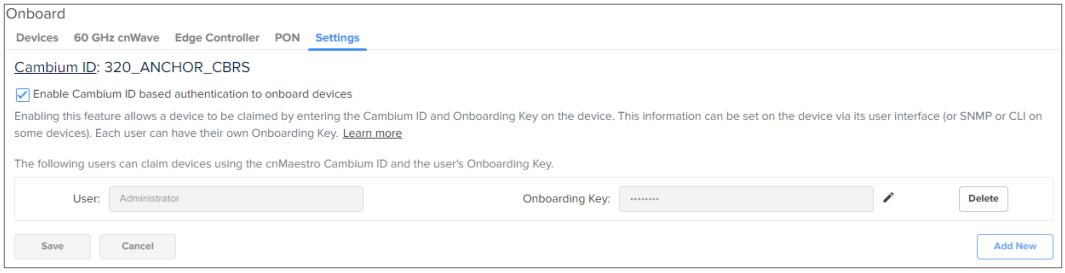
If the device gets struck in the Onboarding Queue, the **Force Onboard** button will automatically enable. Click **Force Onboard** to onboard the device.



Claiming Devices with Cambium ID

You must enable the Cambium ID based authentication to onboard devices. Enabling this feature allows a device to be claimed by entering the Cambium ID and Onboarding Key on the device.

Figure 27 *Claim devices*



The Cambium ID can be viewed from **Onboard** > **Settings**. If On-Premises is connected to Cloud, then the Cambium ID is shared by both accounts. It uniquely identifies the account. 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.

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 s shown in Table 21.

Table 21 *Types of Claiming Devices with Cambium ID*

Type	Description
Device UI	Enter the Cambium ID/Onboarding Key directly into the Device User Interface. This prompts the device to access On-Premises instances and place the devices 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 shown in Device-Specific UI Onboarding. Once devices are added to the Onboarding Queue using Cambium ID, the administrator must approve them prior to them being onboarded.

Claiming the Wi-Fi Devices from AP Group

To claim multiple devices from the AP Group, perform the following steps:

1. Navigate to the **Wi-Fi AP Groups** tree view and click the dropdown menu for the selected **AP Group**.
2. Click the **Claim Device(s)** option.
3. Select the **Device Type**, **Network** and **Site** under which these devices should be placed. By default, the devices claimed will have the configuration settings as the AP Group.

4. Specify the MAC Address of the devices line-by-line or comma-separated, or click **Import.csv** to import the MAC addresses of the devices from a 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 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 28** *Example CSV file to include the device name*

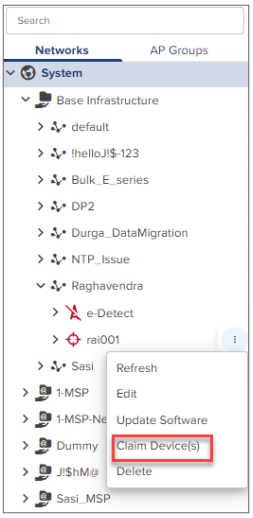
	A	B
1	MAC Address	Device Name
2	90:6D:62:B0:BC:9A	South-East-1
3	E4:C4:5C:E5:34:55	North-Pole
4	AB:04:56:C7:82:DE	Point-Nemo

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

Claiming Wi-Fi devices from the Site dashboard

To claim multiple devices from the Site dashboard, perform the following steps:

1. Navigate to **Monitor and Manage** > **Networks** tree view and select the dropdown menu for the Site.
2. Click **Claim Device(s)** from the dropdown.



3. Select the site that should be applied for Enterprise Wi-Fi (E-Series, XE/XV-Series, and Xirrus) devices. The devices claimed under the Site will have the configuration settings from the selected site.

4. Specify the MAC Address of the devices line-by-line or comma-separated, or click **Import.csv** to import the MAC addresses of the devices from a 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 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 29 *Example CSV file to include the device name*

	A	B
1	MAC Address	Device Name
2	90:6D:62:B0:BC:9A	South-East-1
3	E4:C4:5C:E5:34:55	North-Pole
4	AB:04:56:C7:82:DE	Point-Nemo

5. Click **Claim Devices** to add the devices to the selected AP Group and **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.

When claiming devices using the CSV files, by default, only the MAC address and device name is allowed. However, if you select a particular device type (cnMatrix or Enterprise Wi-Fi) and a corresponding switch group 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
MAC Address	Device Name	AP Group	ssid	channel	channel-width	switchport access vlan
		testing				

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**

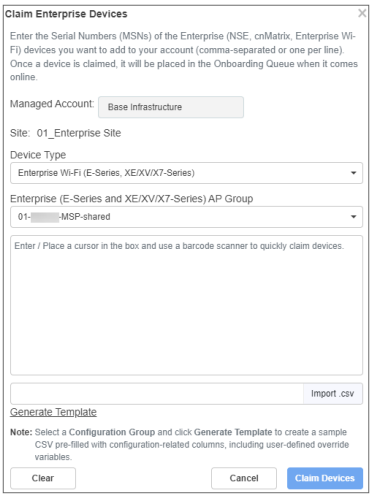
To import multiple Enterprise devices using the CSV import option, complete the following steps:

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

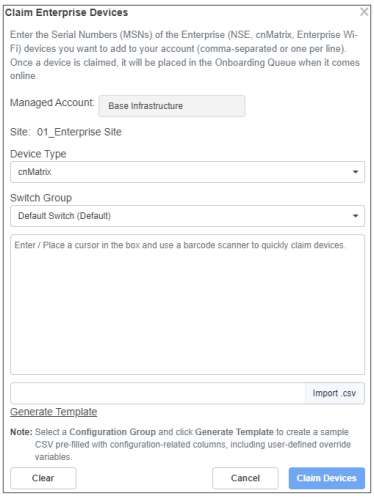
   The **Claim Enterprise Devices** window is displayed as shown in the following images.

   - At the enterprise site-level:

     Wi-FI APs



cnMatrix 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 **Mac Address** and **Device Name** columns, which are the default.

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.

Reclaim

The following scenarios explains when the devices starts to reclaim:

- If an unmaged On-Premises instances with onboarded devices tries connecting back to the Cloud Anchor account starts to reclaim the devices.
- If any On-Premises instances is upgraded from 3.1.x to 3.2.0 or above starts to reclaim the devices.
- During the Cloud synchronization, restore and backup from another On-Premises instances starts to reclaim the devices.

Grace period

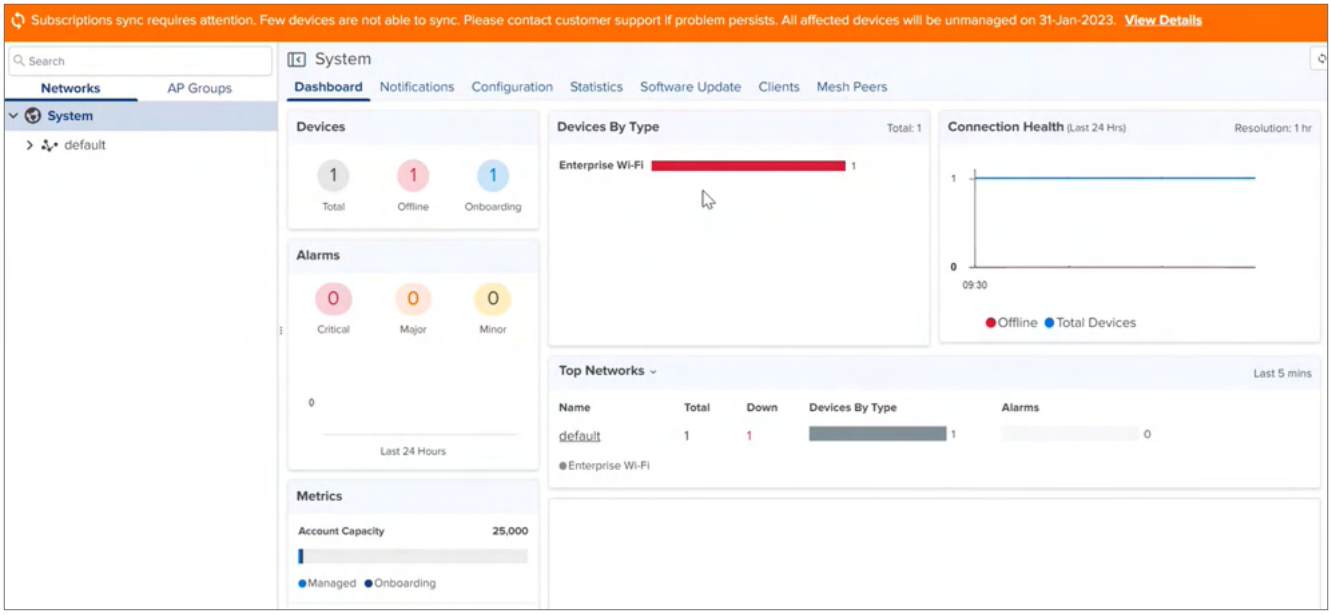
Grace period starts when there is an invalid device state and an invalid subscription state. A notification banner will be displayed and the grace period is valid only for 90 days. At the end of the grace period, cnMaestro takes the required action.

Invalid device state

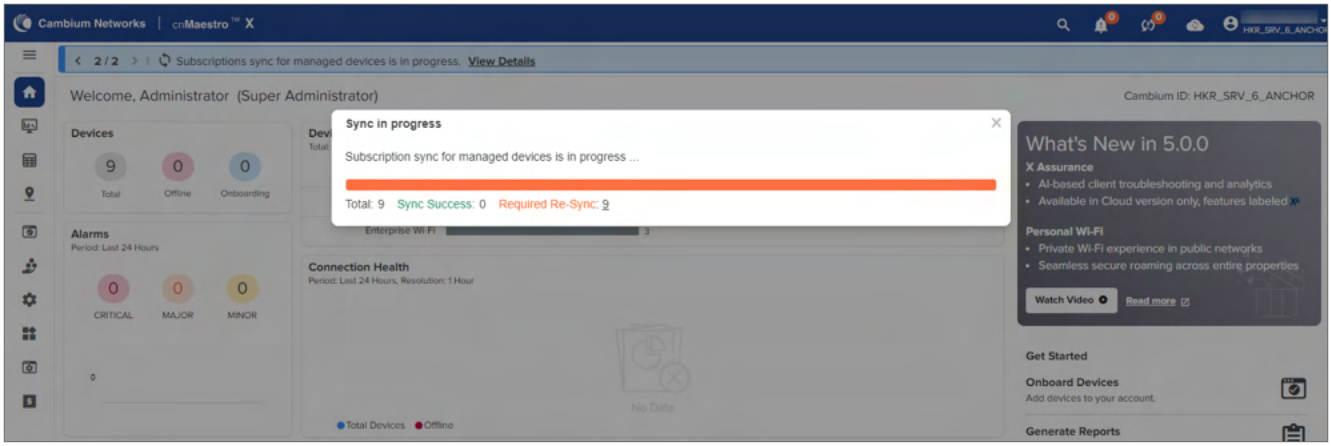
The grace period of an invalid device starts, when there is a conflict state detected during the reclaim or reconnect of the devices for a longer duration. A notification banner will be displayed as shown in Figure 30.

Users can rectify the invalid state by deleting the devices which required re-sync.

Figure 30 *Invalid device state*

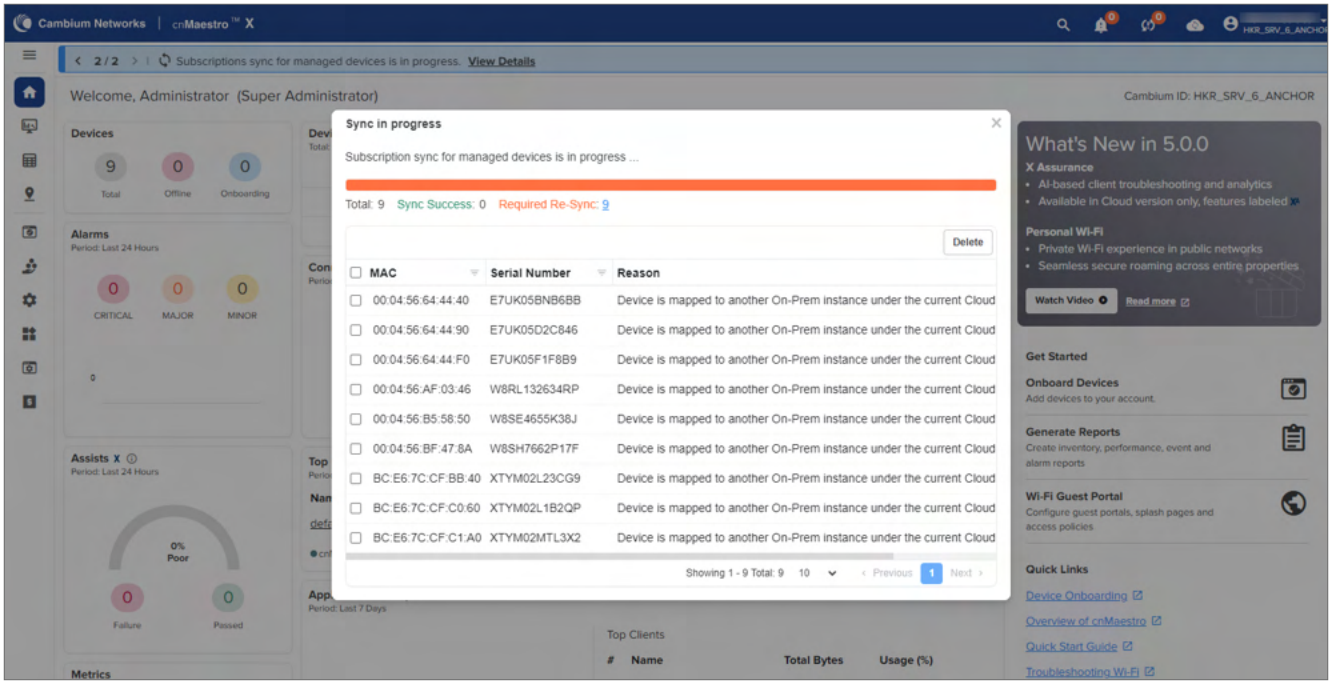


Click **View Details** to view the synchronization progress details.



Users can delete the re-sync required devices by clicking the Required Re-Sync as shown in Figure 31.

Figure 31 *Required Re-Sync*



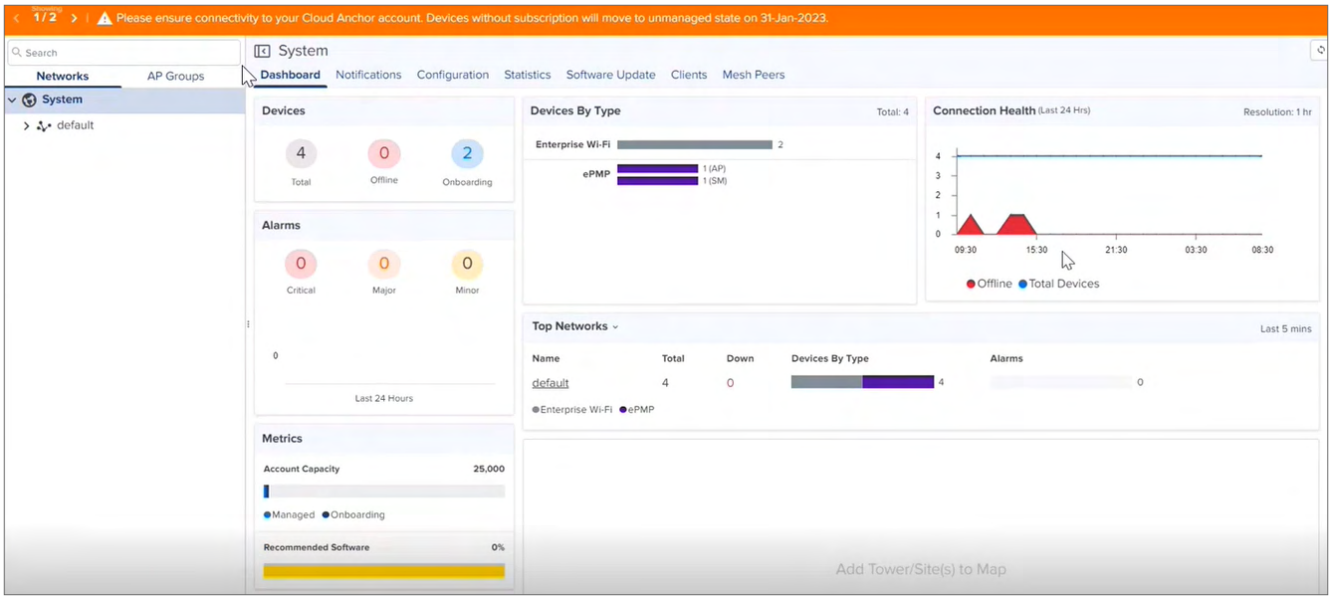
At the end of the grace period, the invalid devices will be unmanaged and moved to the onboarding queue.

Invalid subscription state

The grace period of an invalid subscription state starts because of any cloud synchronization issue or the On-Premises instances is not capable of getting their new subscription from the anchor account as shown in Figure 32.

Users can rectify the invalid state by connecting to the cloud or can contact the Cambium Networks support center.

Figure 32 *Invalid subscription state*



At the end of the grace period, all the devices will be moved to the onboarding queue, Cloud connectivity will be unmanaged, and a login prompt will be displayed to connect to the cloud.

Deleting Devices

You can delete a single or multiple unmanaged devices in bulk from the onboard page. For more details about bulk deletion, see Deleting Devices in Bulk.

Device-Specific UI Onboarding

In order to access cnMaestro, devices must be configured with the cnMaestro On-Premises URL. There are three ways to do this (listed in priority order):

1. Configure the cnMaestro URL on the device
2. Configure DHCP Option 43 on the DHCP server
3. Configure DHCP Option 15 on the DHCP server

If none of these are present, the default action on the device is to access the cnMaestro Cloud URL: https://cloud.cambiumnetworks.com.

This section contains the following topics:

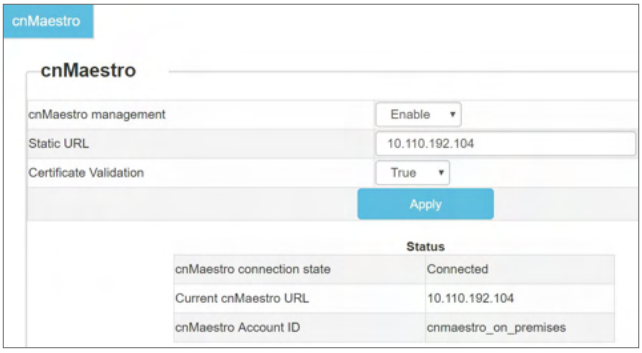
- Static URL
  - cnMatrix
  - Enterprise Wi-Fi
  - cnPilot Home
  - cnRanger
  - cnReach
  - cnVision Client
  - cnVision Hub
  - ePMP 1000 AP/SM
  - ePMP 1000 Hotspot
  - PMP
  - PTP 650/670/700
- Onboarding Xirrus device
- Onboarding a cnWave 5G Fixed BTS device
- DHCP Options (Linux)
- Onboarding PON devices
- Onboarding 60 GHz cnWave devices

Static URL

If a static URL is configured in the device UI, the device will always connect using it. The below sections details where to set the cnMaestro URL on various device types. The Cambium ID and Onboarding Key can optionally be used in some devices for added security.

cnMatrix

1. Navigate to **System** > **cnMaestro** tab.
2. Enter **Static URL**.

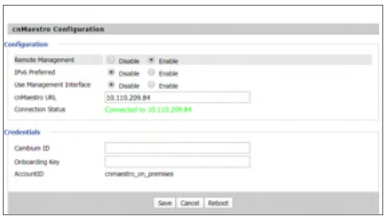


Enterprise Wi-Fi

1. Navigate to **Configure** > **System** > **Management** tab**.**
2. Enter **cnMaestro URL**.

cnPilot Home

1. Navigate to **Administrator** > **cnMaestro** tab.
2. Enter **cnMaestro URL.**

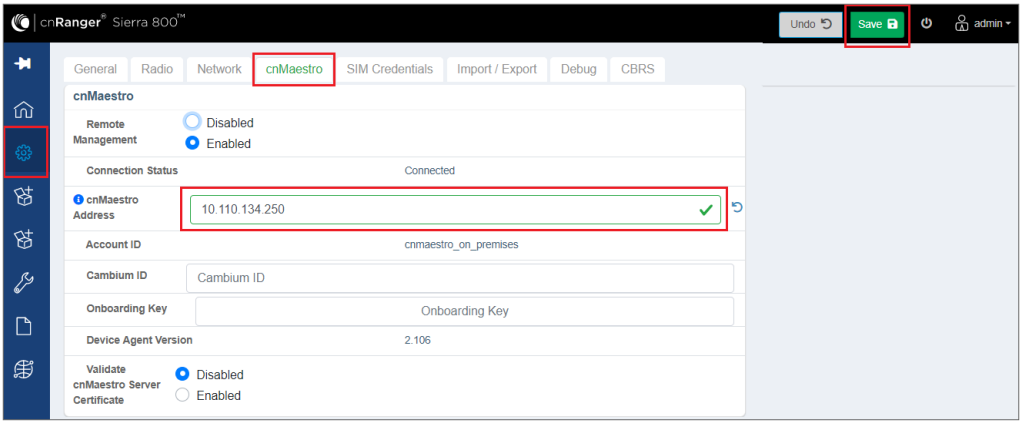


cnRanger

Setting static URL for cnMaestro on Sierra 800

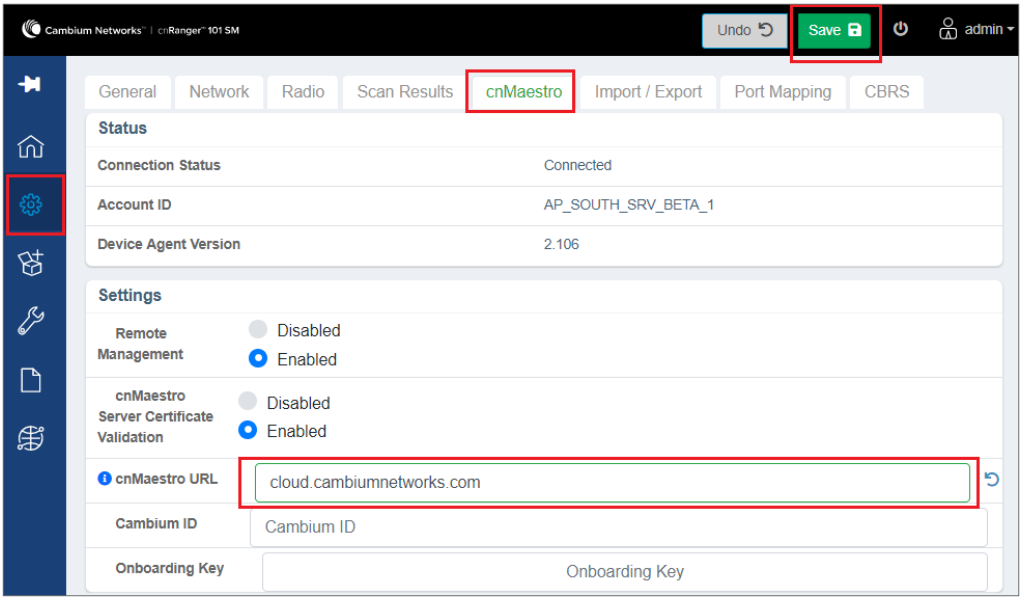
1. Navigate to **Configuration** > **cnMaestro** tab.
2. Under cnMaestro section, enter URL in the **cnMaestro Address**.

3. Click **Save**.



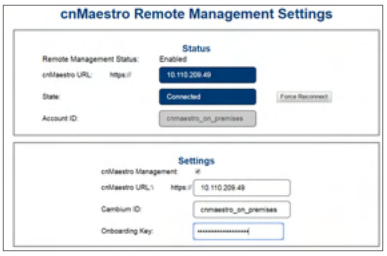
Setting static URL for cnMaestro on Tyndall 101

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



cnReach

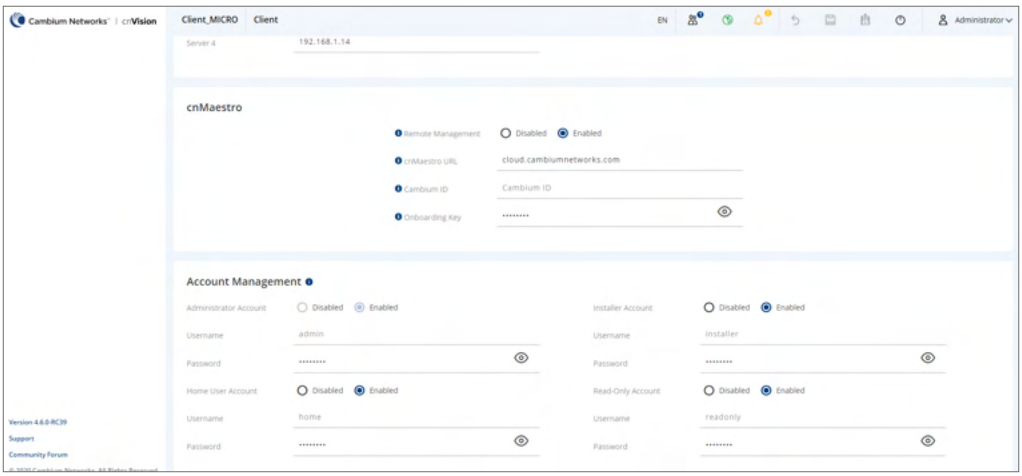
1. Navigate to **cnMaestro** > **Management Settings** > **Settings**.



2. Click **cnMaestroManagement** checkbox.
3. Enter **cnMaestro URL.**

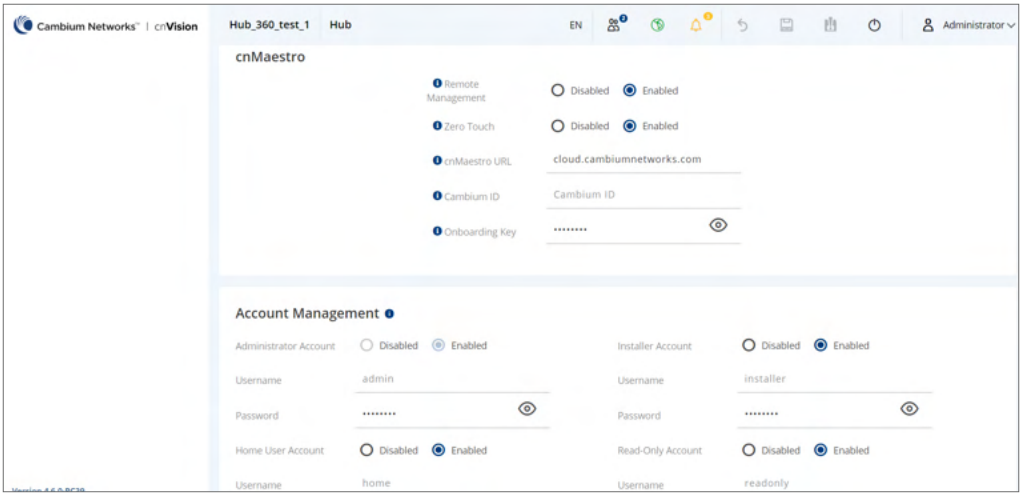
cnVision Client

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



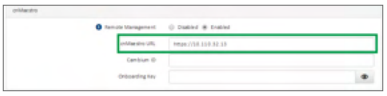
cnVision Hub

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



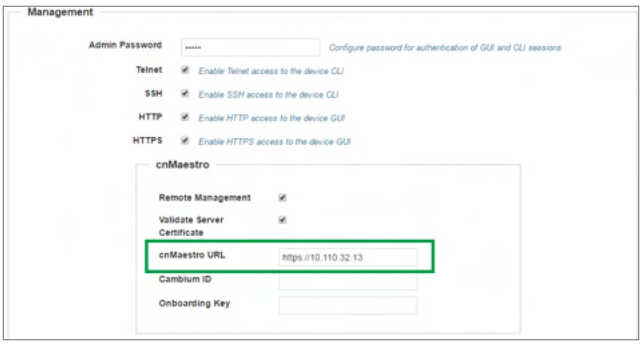
ePMP 1000 AP/SM

1. Navigate to **Configuration** > **System** > **cnMaestro** tab.
2. Enter **cnMaestro URL.**



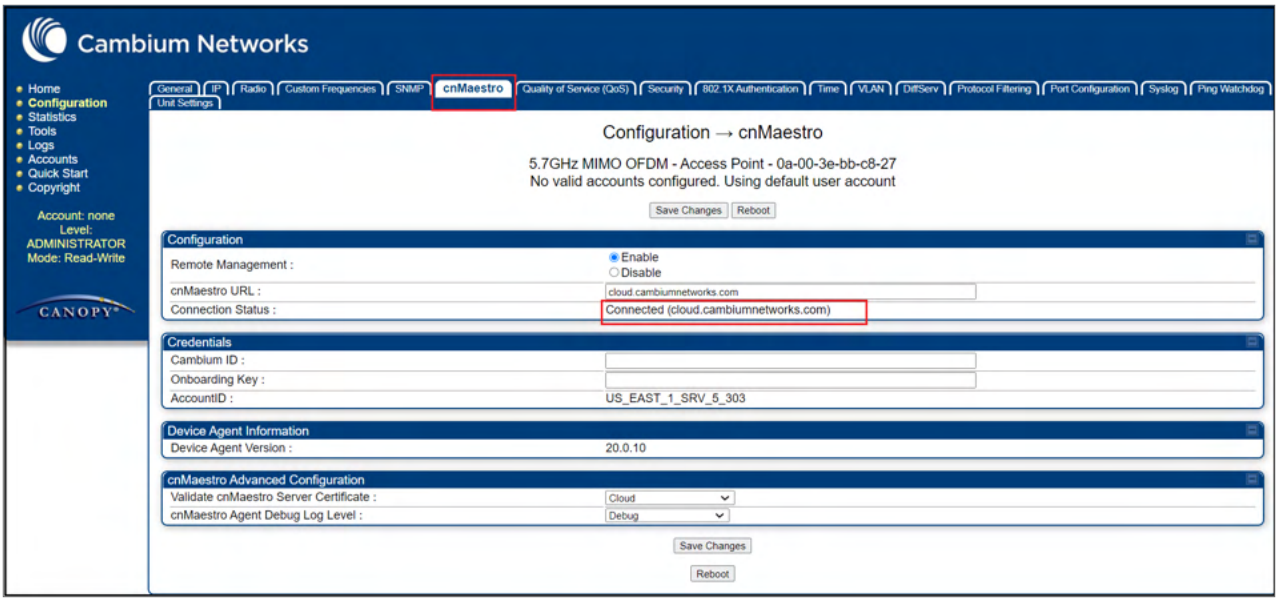
ePMP 1000 Hotspot

1. Navigate to **Configure** > **System** > **Management** tab**.**
2. Enter **cnMaestro URL.**



PMP

1. Navigate to **Configuration** > **cnMaestro** tab.
2. Enter **cnMaestro URL**.
3. To check the cnMaestro connection status, navigate to **Configuration** > **cnMaestro** > **Connection Status.**



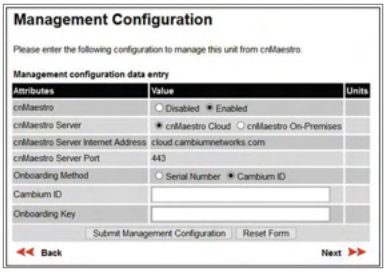
PMP configuration prerequisites

Please make sure the following configuration requirements are met in PMP before onboarding to cnMaestro.

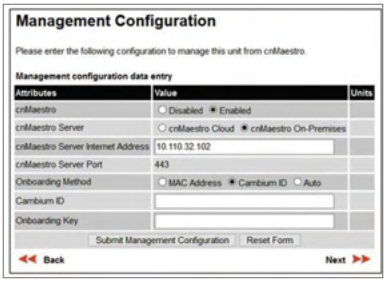
- **SM (not using NAT)**
  - LAN 1 network interface should have 'public' accessibility.
  - IP address should be public IP address: either static IP address or obtained via DHCP.
  - DNS server configuration should be filled: either static IP address or obtained via DHCP.
- **SM using NAT**
  - Remote Management interface with standalone configuration should be enabled.
  - Remote Management IP address should be public IP address.
  - DNS server should be configured.
- **AP**
  - IP address should be public.
  - DNS server should be configured.

PTP 650/670/700

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



3. Select **cnMaestro On-Premises** radio button.




```
option domain-name "mycompany.com";
```

Onboarding Xirrus device

Xirrus device can be onboarded in three ways:

1. Onboarding through CLI for cnMaestro X
   - Domain name-based
   - IP-based

2. Onboarding Xirrus AP to cloud using Cambium ID and Onboarding Key
3. Onboarding through DHCP options for cnMaestro X

Onboarding through CLI for cnMaestro X

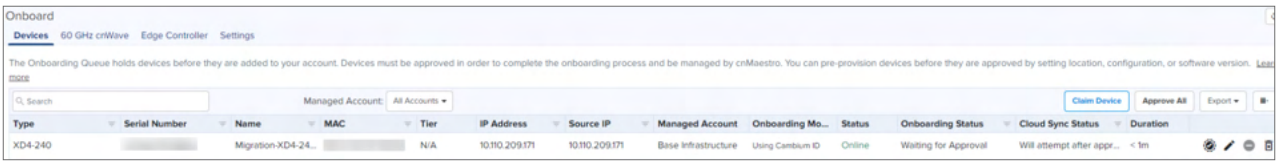
Domain name based

Perform the following steps to onboard Xirrus device through CLI:

1. Connect to the device using any SSH tool.
2. Log in 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 domain_name scheme cnmaestro enable
# save
Saving configuration .... OK
```

4. Log in to cnMaestro Instance.
5. Navigate to **Home** > **Onboard** > **Devices**.
6. In the **Devices** page, the device **Waiting for Approval** is shown as below:



   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**.

IP based

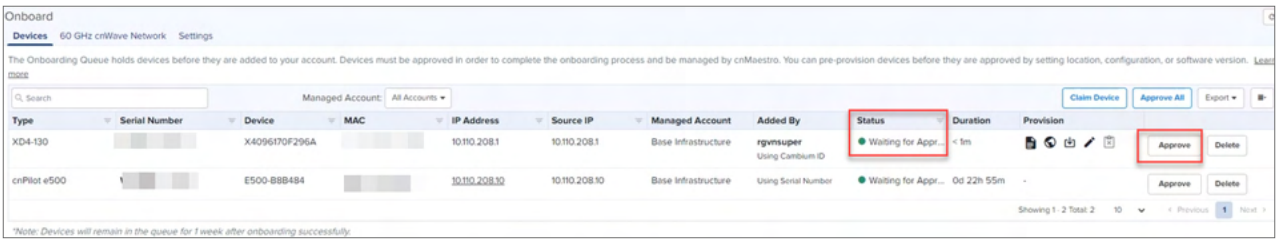
Perform the following steps to onboard Xirrus device through CLI:

1. Connect to the device using any SSH tool.
2. Log in 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 15.421.253.125 scheme cnmaestro enable
# save
```

```
Saving configuration .... OK
```

4. Log in to cnMaestro Instance.
5. Navigate to **Home** > **Onboard** > **Devices**.
6. In the **Devices** page, the device **Waiting for Approval** is shown as below:

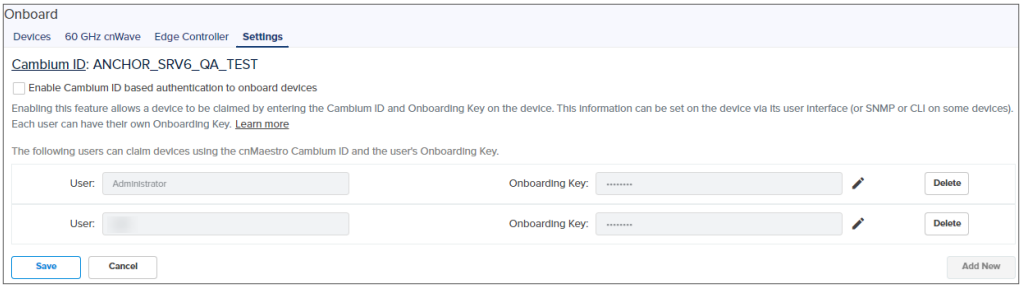


The Status field display **Waiting for Approval**. It is optional to provision the device for location, software version update, and assign to an AP Group.

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

Onboarding Xirrus AP to cloud using Cambium ID and Onboarding Key

1. Navigate to **Onboard** > **Settings.**
2. Select **Enable Cambium ID based authentication to onboard devices.**



3. Connect to the device using any SSH tool.
4. Log in as admin, the default password is admin.
5. Execute the following command in ssh console:

```
#ssh admin <device IP address>
#password <admin>
#configure
#management
#(config-mgmt)# cnMaestro-onboarding id 123456789 key cambium123
(config-mgmt)# save
Saving configuration .... OK
(config-mgmt)#
```

Onboarding through DHCP options for cnMaestro X

1. Define DHCP Option 43 (Vendor Specific) with On-Premises server URL.
2. Define DHCP Option 15 (domain name).

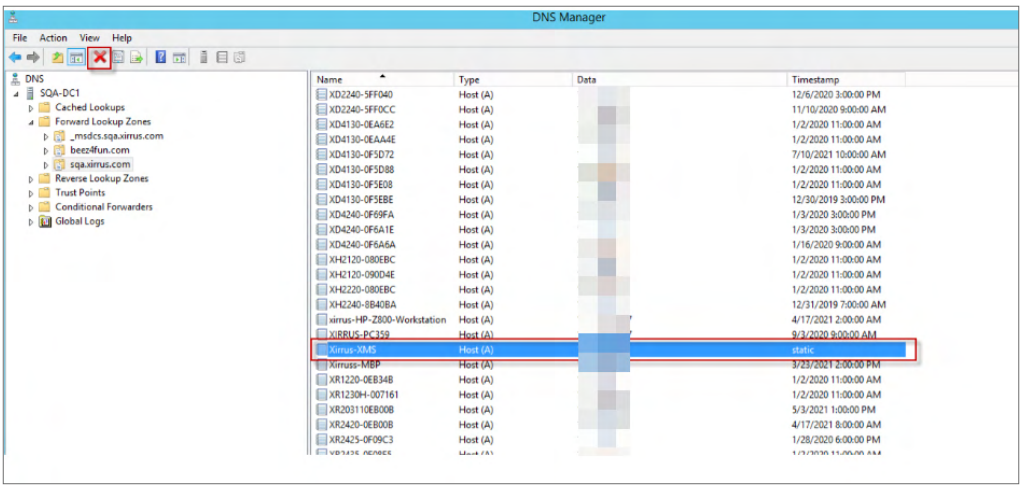
For example, DHCP is defined with option 43 and 15

Option 43 is https://cnmaestro.sqa.xirrus.com

Option 15 is sqa.xirrus.com

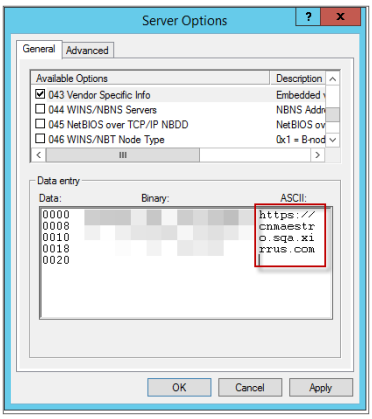
DNS Server

1. Add cnmaestro as Host (not cnmaestro X).
2. Remove the Xirrus-XMS from DNS Server. This change may take time depending on the DNS record update time.



- Add DNS Option 43 (vendor specific) if required - URL.

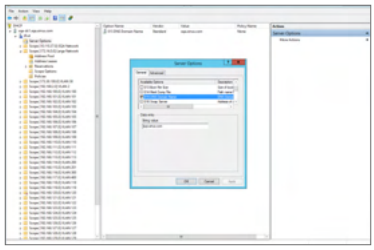
  Example: https://cnmaestro.sqa.xirrus.com - Type in the value in the ASCII section of the display.



- DHCP Sever - AP Scope.

  Ensure DNS option 15 (DNS domain name) is defined.

  Example: sqa.xirrus.com



For more details on how to configure a Microsoft Windows-based DHCP server to send DHCP Options to Cambium Networks devices, refer to Windows DHCP.

3. Check if the device is online in the cnMaestro UI page. When the device is in **Waiting for Approval** state, **Approve** the device to complete the onboarding process.

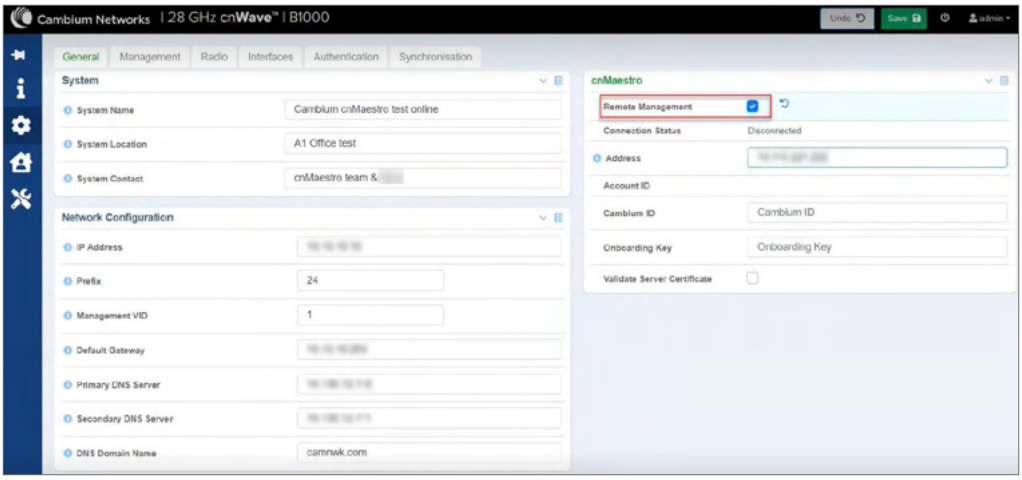
   For details to migrate Xirrus devices from XMSE to cnMaestro X using a tool, refer to XMSE to cnMaestro X.

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, perform the following steps:

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



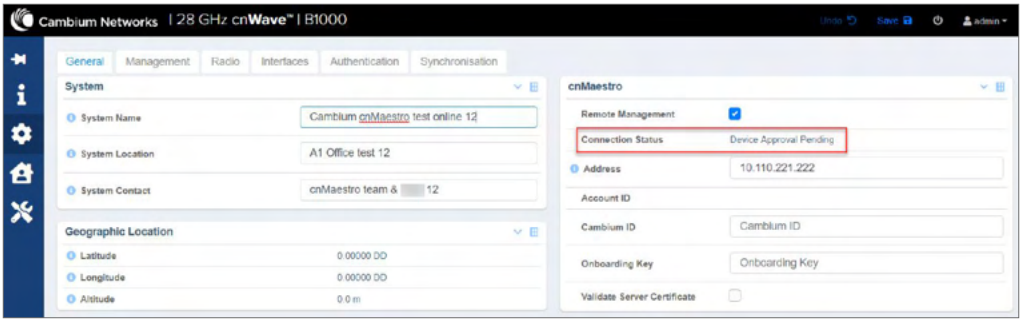
3. In the **Address** field, enter the cnMaestro URL or IP Address.
4. Enter your **Cambium ID** and **Onboarding Key**. **Validate Server Certificate** is an optional field.

> **Note**
>
> You can enter a valid **Cambium ID** and **Onboarding Key** in the cnWave 5G Fixed BTS device UI, when **Enable Cambium ID based authentication to onboard devices** option is enabled in the **Settings** section in the cnMaestro **Onboard** page.

5. Click **Save**.

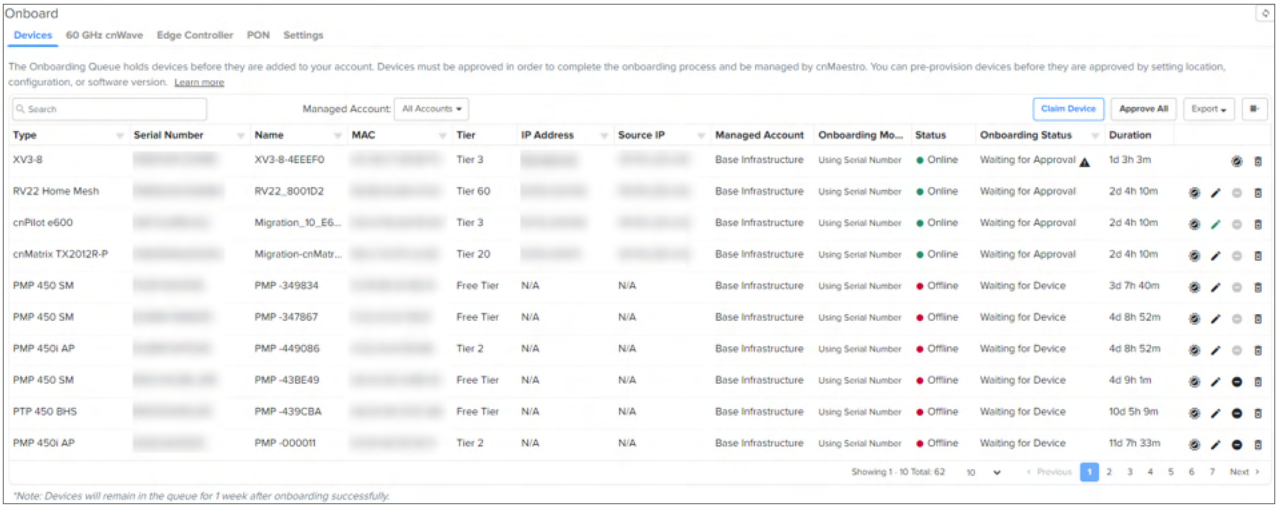
   When the cnWave 5G Fixed BTS device is onboarded to the cnMaestro for the first time, the **Connection Status** field in the cnWave 5G Fixed BTS device UI displays **Device Approval Pending** as shown in Figure 33.

Figure 33 *Device Approval Pending status in cnWave 5G Fixed BTS*



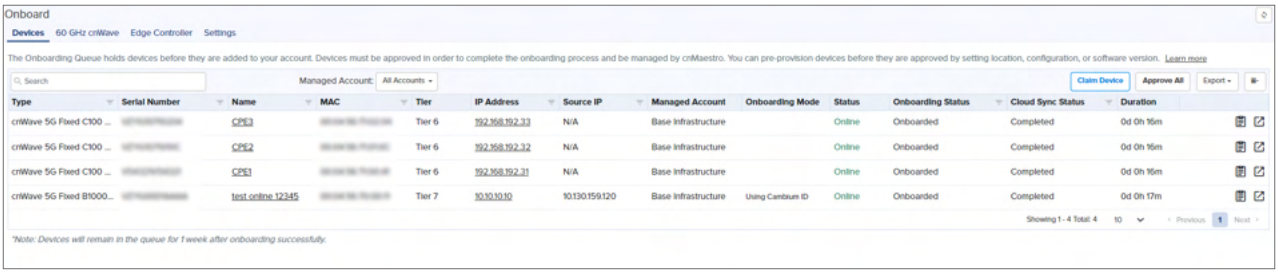
6. In the cnMaestro UI, navigate to **Onboard** > **Devices** and click **Approve**, as shown in Figure 34.

Figure 34 *Approving the cnWave 5G Fixed device using the cnMaestro UI*



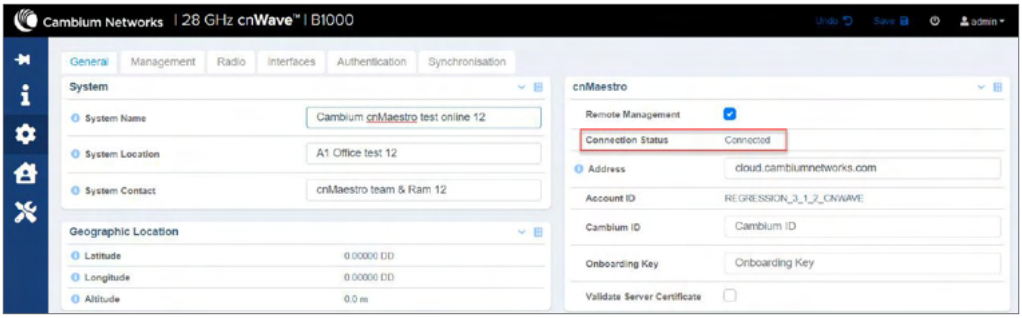
The cnWave 5G Fixed BTS device is onboarded to cnMaestro.

Figure 35 *Viewing the cnWave 5G Fixed BTS device onboarded in cnMaestro*



The **Connection Status** field in the cnWave 5G Fixed BTS device UI displays **Connected**, on approval, as shown in Figure 36.

Figure 36 *cnWave 5G Fixed BTS device Connected*

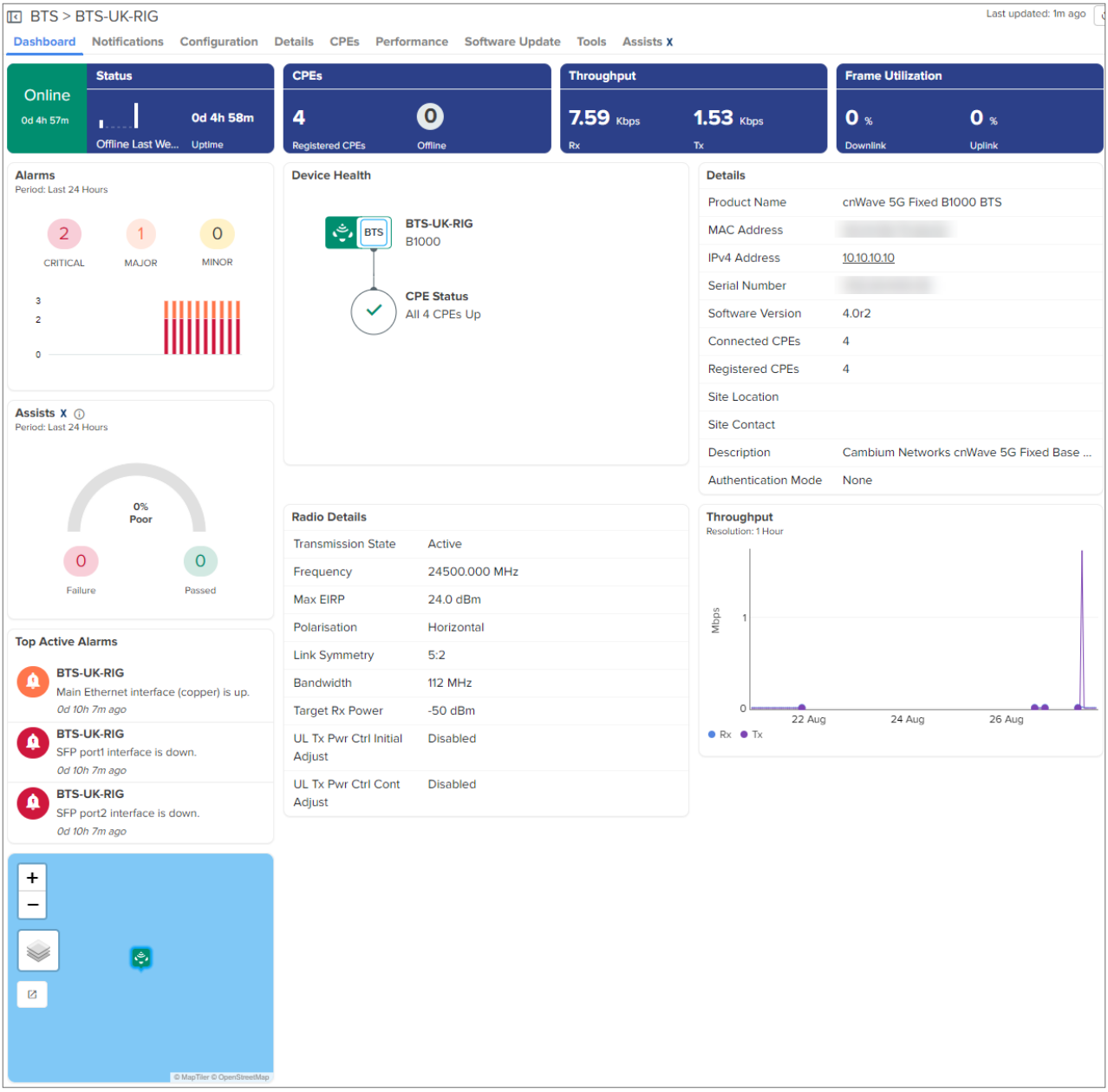


To view the cnWave 5G Fixed BTS device in cnMaestro, perform the following steps:

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.

   When onboarding the cnWave 5G Fixed BTS device the registered cnWave 5G Fixed CPE devices can also be onboarded without approval.

Figure 37 *Viewing cnWave 5G Fixed BTS device and registered CPE devices*



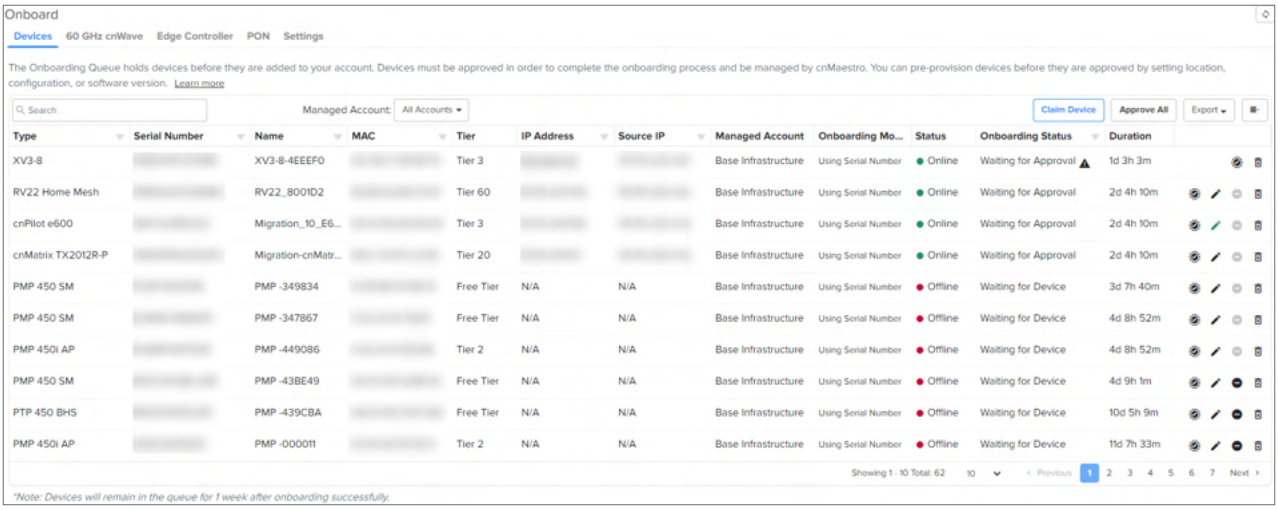
Claiming the cnWave 5G Fixed BTS device with a Serial Number

To claim and onboard the 28GHz cnWave BTS device, perform 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 .

   Onboard page



2. Click **Claim Device** located at the right side of the **Onboard** page, as shown in .

   The **Claim Devices with Serial Number** page appears, as shown in Figure 38.

3. Enter the serial number of the 28GHz cnWave BTS device in the text box, as shown in Figure 38.

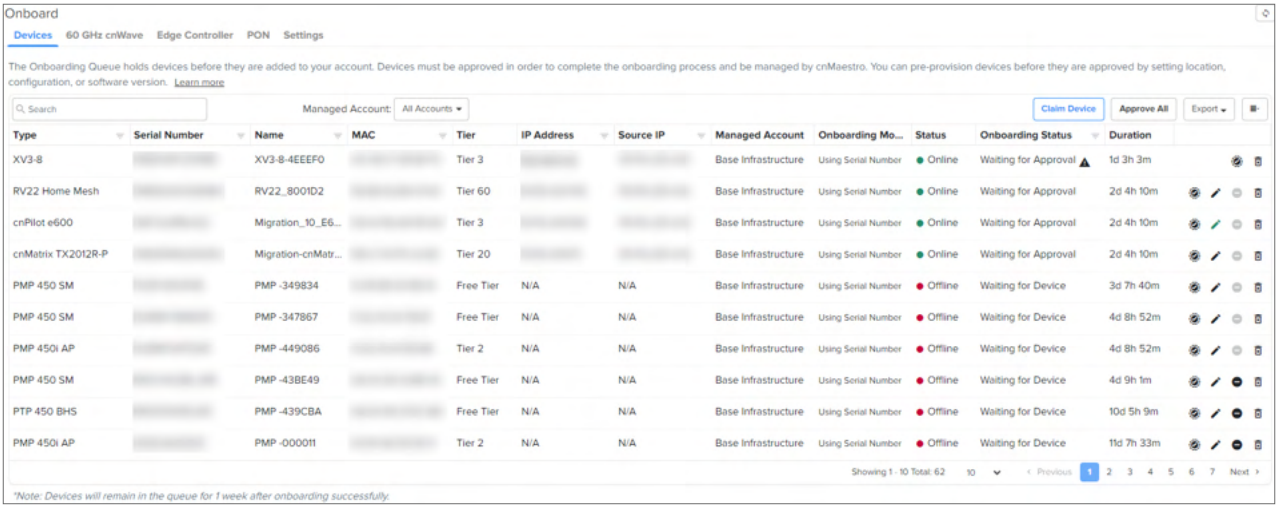
> **Note**
>
> You can also place the cursor in the text box and use a barcode scanner to quickly claim the devices.

Figure 38 *Claim Devices with Serial Number page*

4. Click **Claim Devices.**

5. To onboard the 28GHz cnWave BTS device, click **Approve** located at the right side of the **Onboard** page, as shown in Figure 39.

Figure 39 *Onboarding Queue*



Note

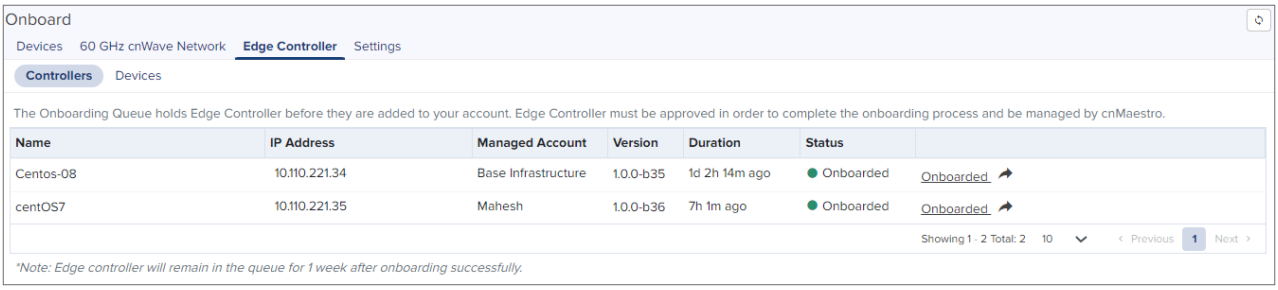
If you do not click **Approve**, the device remains in the Onboarding Queue.

Onboarding Edge Controller

To onboard Edge Controller perform 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**.

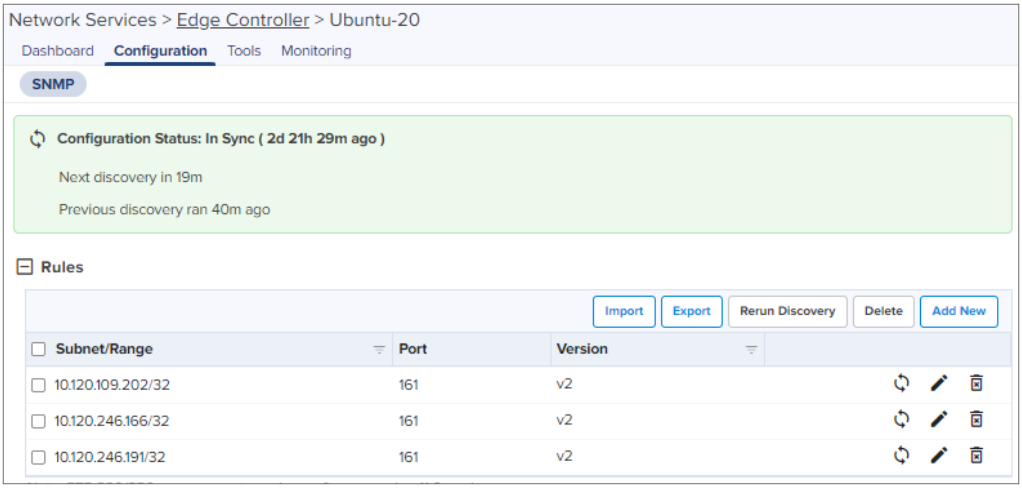
Figure 40 *Edge Controller*



Onboarding PTP 820/850 devices

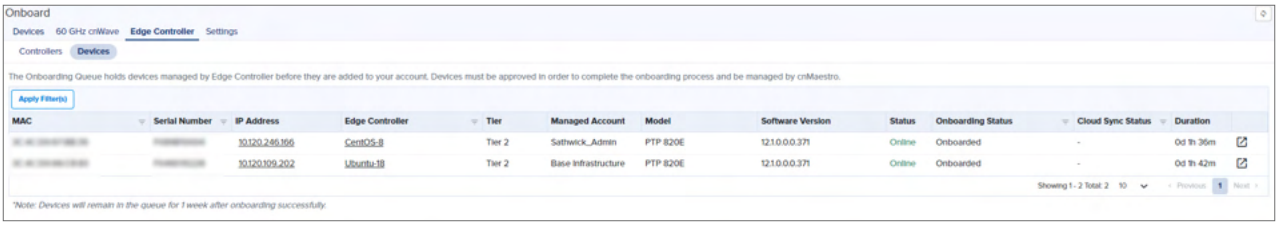
To onboard PTP 820/850 devices perform the following steps:

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



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

Figure 41 *PTP 820/850 devices*



DHCP Options (Linux)

A DHCP Server can be used to configure the IP Address, Gateway, and DNS Servers for Cambium Networks devices. If you administer the DHCP Server, you can also configure DHCP Options to direct devices how to access cnMaestro automatically (so the URL does not need to be set on each device). Cambium Networks devices support DHCP Options 43 and 15 for setting the cnMaestro Cloud URL.

The following configuration is for Linux-based systems. Refer to Windows DHCP for configuring DHCP options for Windows.

Note

DHCP Options are available from the following builds:

- cnMatrix: 2.0.4-r1
- cnPilot e400/e500/e502S/e501S: 3.2.1-r6
- cnPilot e425H/e505: 4.0
- cnPilot e430W/e410/e600: 3.5.2-r4
- cnPilot e510: 3.11.4-r9
- cnPilot e700: 3.7-r9
- cnPilot r190: 4.4.2-R2
- cnPilot r195P: 4.7
- cnPilot r195W: 4.5.2

- cnPilot r200P/r201P: 4.4.2-R2
- cnReach: 5.2.17e
- ePMP 1000, ePMP Force 180/200: 3.1
- ePMP 1000 Hotspot: 3.2.1-r6
- ePMP 2000: 3.0
- ePMP 3000: 4.5
- ePMP Elevate: 3.2
- ePMP Force 190: 3.5
- ePMP Force 300: 4.1
- ePMP PTP 550: 4.1
- PMP: 15.0.1
- PTP 650, PTP 670 (650 Emulation): 02-67

The priority order for determining the cnMaestro URL is the following:

1. Static URL manually set through the Device UI.
2. DHCP Option 15.
3. DHCP Option 43.
4. Default Cambium Cloud URL (https://cloud.cambiumnetworks.com).

Note

cnRanger, cnReach, PTP 650, PTP 670, and PTP 700 do not support DHCP Options for onboarding.

Using DHCP Option 43

DHCP Option 43 returns the Cambium cnMaestro On-Premises URL as a Vendor-Specific Option. DHCP Option 43 is returned in tandem with DHCP Option 60 (the Vendor Class Identifier, or VCI).

The VCI for the individual Cambium products is listed below:

Table 22 *VCI (DHCP Option 60)*

Product	VCI (DHCP Option 60)
cnMatrix	Cambium-cnMatrix-EX2K
cnPilot r190	Cambium-cnPilot r190
cnPilot r195	Cambium-cnPilot r195
cnPilot r200P	Cambium-cnPilot r200P
cnPilot r201P	Cambium-cnPilot r201P
cnPilot e400/e410/e430W cnPilot e425H/e505 cnPilot e500/e501S/e502S/e510 cnPilot e700/e600 XE3-4, XE3-4TN, XE5-8	Cambium-WiFi-AP

Product	VCI (DHCP Option 60)
XV2-2, XV2-2T0, XV2-2T1, XV2-22H, XV2-21X, XV2-23T, XV3-8	
ePMP	Cambium
ePMP 1000 Hotspot	Cambium-WiFi-AP
PMP 430 SM	Cambium PMP 430 SM
PMP 450 AP	Cambium PMP 450 AP
PTP 450 BHM	Cambium PTP 450 BHM
PMP 450 BHS	Cambium PTP 450 BHS
PMP 450 SM	Cambium PMP 450 SM
PMP 450b SM	Cambium PMP 450b SM
PMP 450i AP	Cambium PMP 450i AP
PMP 450i BHM	Cambium PTP 450i BHM
PTP 450i BHS	Cambium PTP 450i BHS
PMP 450i SM	Cambium PMP 450i SM
PMP 450m APs	Cambium PMP 450m AP

Typically, Option 43 is the preferred mechanism to configure the cnMaestro URL. Example configuration for the ISC DHCP Server is presented below (from the /etc/dhcp/dhcpd.conf file).

```
option option-43 code 43 = string;

# ePMP/PMP Devices
class "Cambium" {
    match if option vendor-class-identifier = "Cambium";
    # DHCP server MUST return the device's Vendor Class back, in the offer.
    option vendor-class-identifier "Cambium";
    # cnMaestro On-Premises IP is 192.168.0.100
    option option-43 "https://192.168.0.100";
}

# WiFi Devices
class "Cambium-WiFi-AP" {
    match if option vendor-class-identifier = "Cambium-WiFi-AP";
    option vendor-class-identifier "Cambium-WiFi-AP";
    option option-43 "https://192.168.0.100";
}

# cnPilot R200P Devices
class "Cambium-cnPilot R200P" {
    match if option vendor-class-identifier = "Cambium-cnPilot R200P";
    option vendor-class-identifier "Cambium-cnPilot R200P";
    option option-43 "https://192.168.0.100";
}

# cnPilot R201P Devices
class "Cambium-cnPilot R201P" {
    match if option vendor-class-identifier = "Cambium-cnPilot R201P";
    option vendor-class-identifier "Cambium-cnPilot R201P";
    option option-43 "https://192.168.0.100";
}
```

Using DHCP Option 15

DHCP Option 15 allows the device to derive the cnMaestro URL from the domain name. For example, if the domain name in DHCP Option 15 is **mycompany.com**, the device will try to access the cnMaestro server at **cnmaestro.mycompany.com** (essentially the string **cnmaestro** is prepended to the domain). The domain itself, and the IP address of cnMaestro, must be configured in the DNS server for this to work correctly.

Sample configuration for the ISC DHCP Server is presented below (from the /etc/dhcp/dhcpd.conf file).

```
option domain-name "mycompany.com";
```

Onboarding PON devices

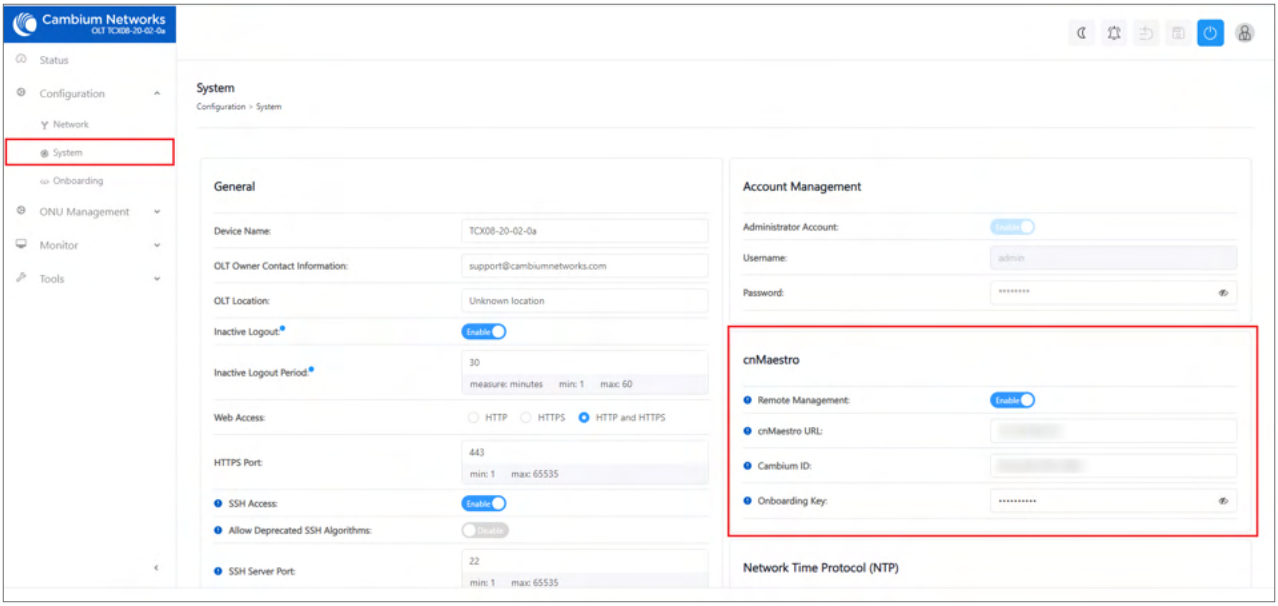
This section describes the onboarding of PON devices to the cnMaestro X account. The onboarding process requires the device Manufacturing Serial Number (MSN). The MSN of the device can be found at the bottom of the device as shown in Figure 43.

To onboard the PON devices, perform the following steps:

1. On the Home page, navigate to **Configuration** > **System**.

   The System page appears, as shown in Figure 42.

   Figure 42 *The System page*

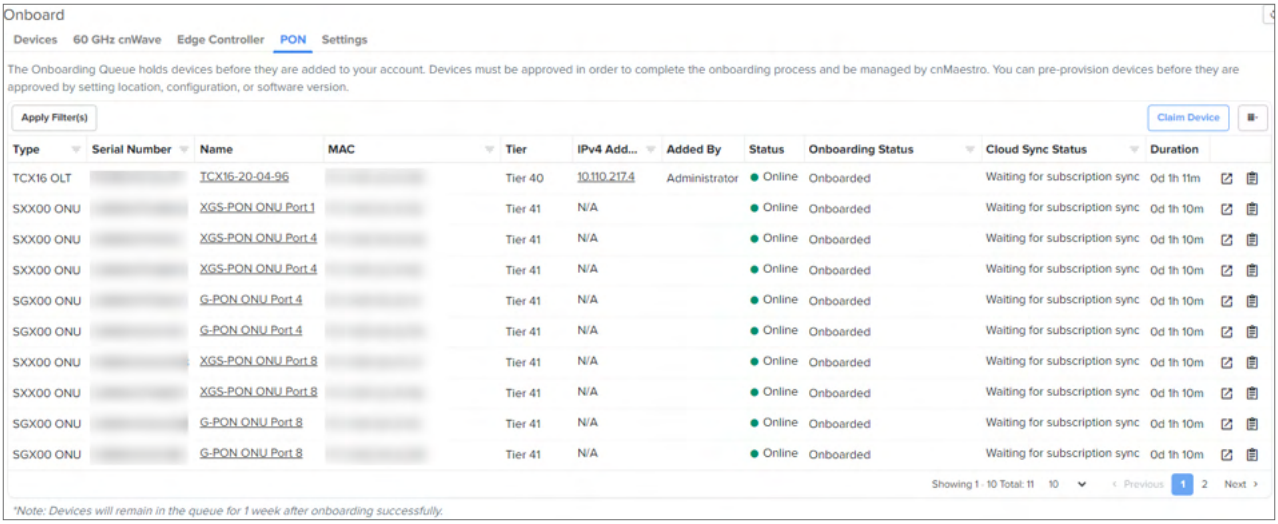


2. Under **cnMaestro** section, enable the **Remote Management** option.
3. Type the **cnMaesto URL**, **Cambium ID**, and **Onboarding Key**.
4. Save the changes.

To onboard the PON devices from cnMaestro, perform the following steps:

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

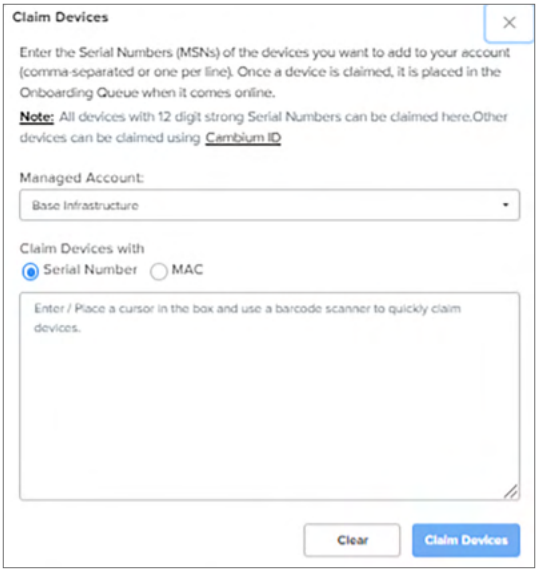
   Figure 43 *Onboard page for PON devices*



2. Click **Claim Device**.

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

Figure 44 *Claim devices with Serial Number*



3. Select the account from the **Managed Account** dropdown list .
4. Select the required option under **Claim Devices with** and enter the details.
5. Click **Claim Devices**.

   The device will be listed in the Onboarding Queue.
6. Click the **Approve Device** ( ) icon.

Onboarding 60 GHz cnWave devices

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

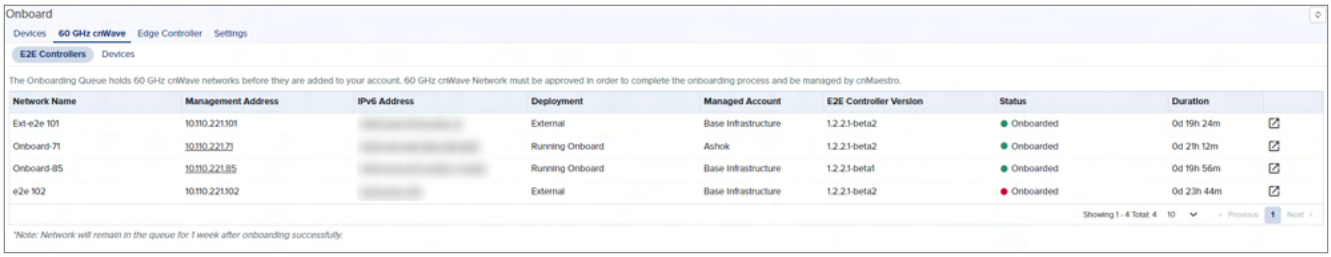
1. Ensure that the 60 GHz cnWave E2E Controller OVA file (for external) is deployed on a Linux machine or Oracle Virtualbox (which is used for device management).
2. Set the IP address of the external E2E Controller.
3. At the console, SSH into the external E2E Controller using its IP address.

   The cnWave E2E Controller Terminal UI (TUI) opens.
4. Navigate to the **cnMaestro** option.

   The Configure cnMaestro Management Server window opens.
5. Set appropriate values for the following parameters:
   - URL: Enter the cnMaestro URL that is used for management.
   - Cambium ID:
   - Onboarding Key:
6. Click **Update**.

60 GHz E2E Controller Onboarding

The Onboarding Queue has a separate tab for 60 GHz cnWave E2E Networks. They must be approved by the user before they are added to cnMaestro and can manage 60 GHz cnWave devices. This approval can be done either by accessing through the **Onboard** page or **Tree** menu.



This section covers the following topics:

- External E2E Controller Onboarding
- Device E2E Controller (Running Onboard) Onboarding
- 60 GHz E2E Controller Onboarding devices

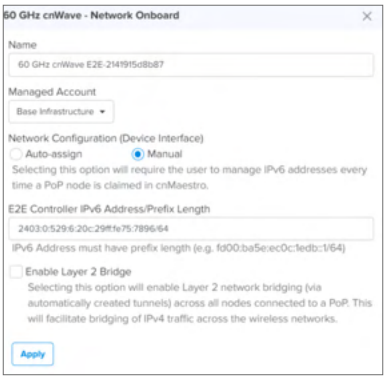
External E2E Controller Onboarding

External E2E Controller is an OVA file which can be deployed in ESXi or VMware. The External E2E Controller discovers cnMaestro after it is deployed and ready.

The E2E Controller will also be placed in the **Tree** prior to approval (in addition to the Onboarding Queue). To Onboard the E2E Controller Network through the **Tree**, perform the following steps:

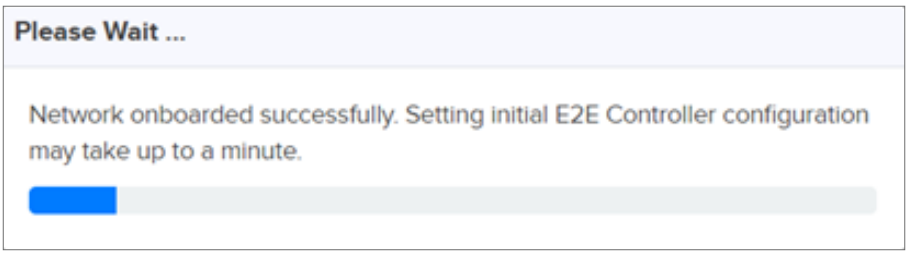
1. Navigate to the Controller in the tree and select the **Monitor and Manage** tab**.**
2. Click **Approve.**

3. **60 GHz cnWave – Network Onboard** window pops up.

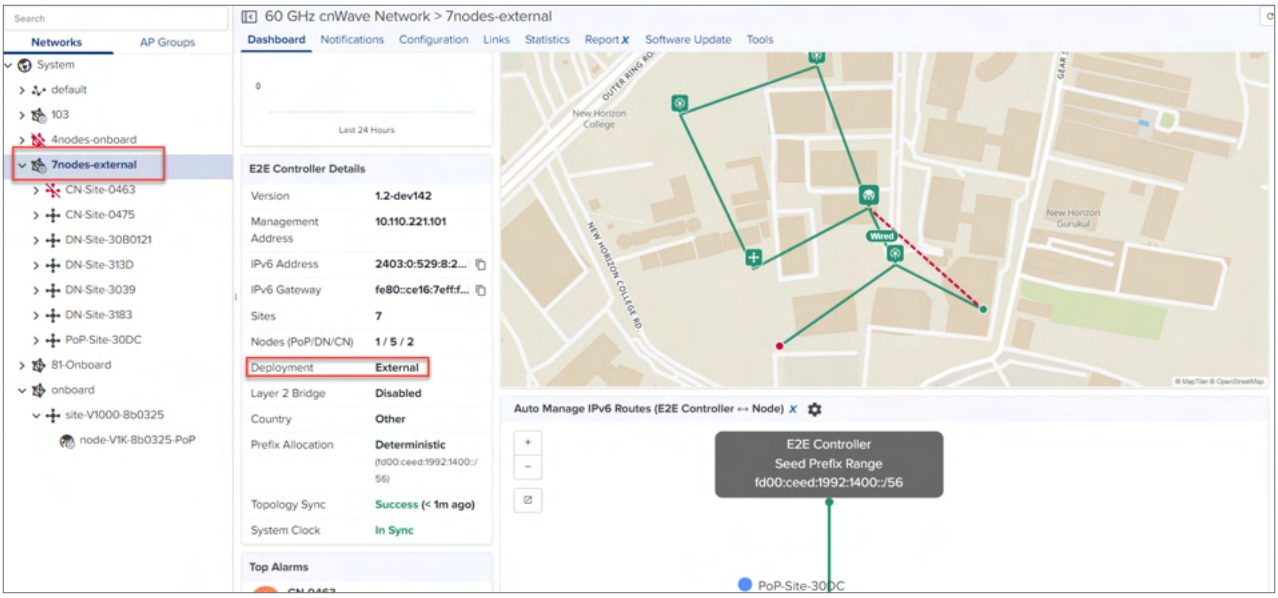


4. By default **Auto-assign** is selected however, the user can select **Auto-assign** or **Manual** to update the IPv6 address in the E2E Network. It takes a while for the IPv6 address to update (after which, the user can optionally **Enable Layer 2 Bridge**).
5. Click **Apply.**

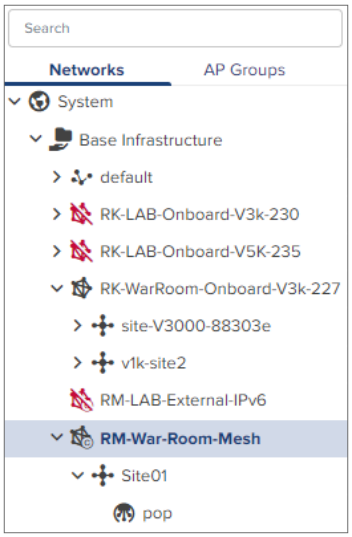
   Wait until the network onboard completes.



6. E2E Network **Dashboard** in cnMaestro is shown below:



External E2E Controller network icon will be displayed .

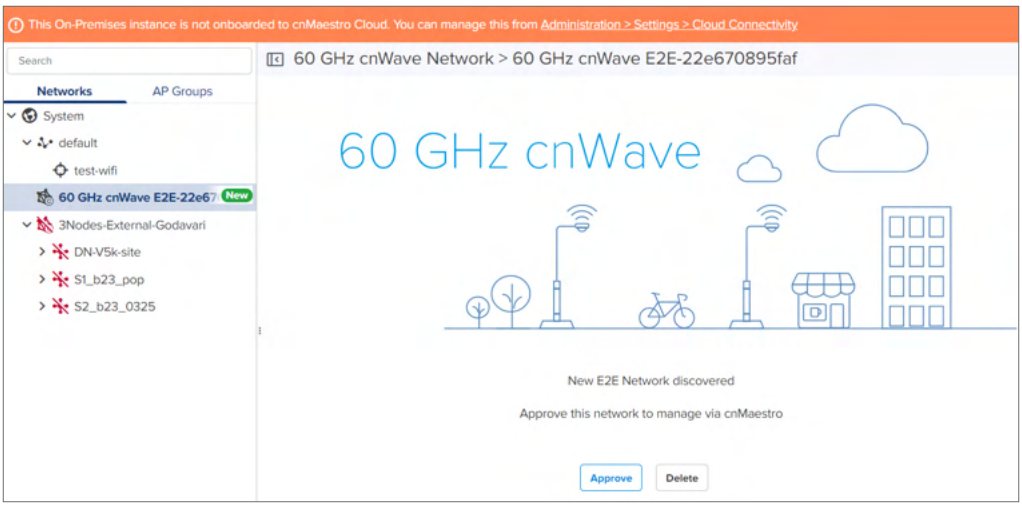


Device E2E Controller (Running Onboard) Onboarding

The Onboard E2E Controller is hosted on a 60Hz cnWave device. (E2E Controller option to be enabled in the device UI).

To approve, proceed as follows:

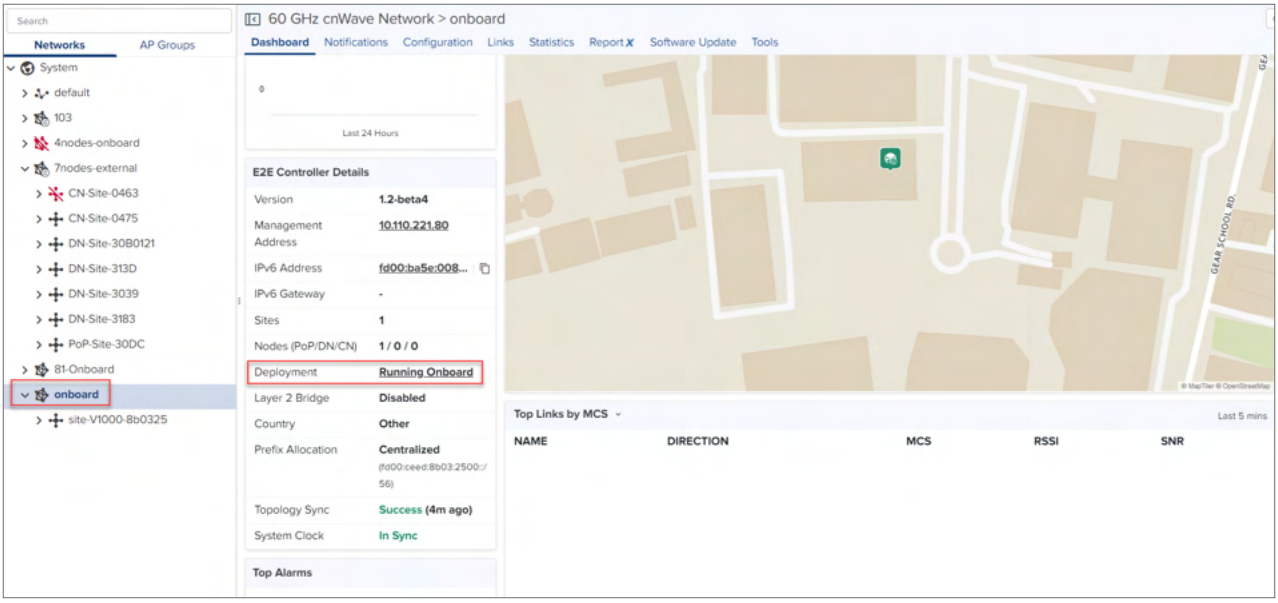
1. Navigate to **Manage** > **Network** > select **60 GHz cnWave E2E Network.**
2. Click **Approve.**



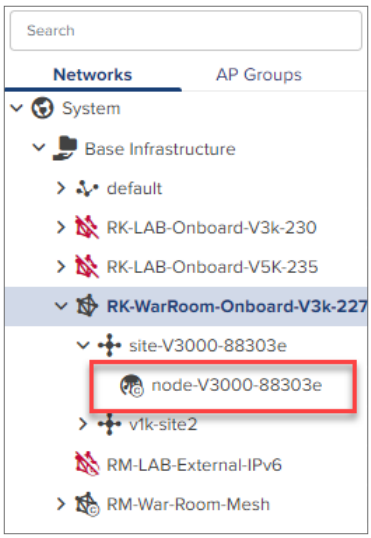
3. **60 GHz cnWave-Network Onboard** window pops up and provides option to edit Network name.
4. Click **Save**.

5. After the successful Onboard E2E Network, it can be managed through cnMaestro. The E2E Network

Dashboard for an Onboard Controller is shown below:



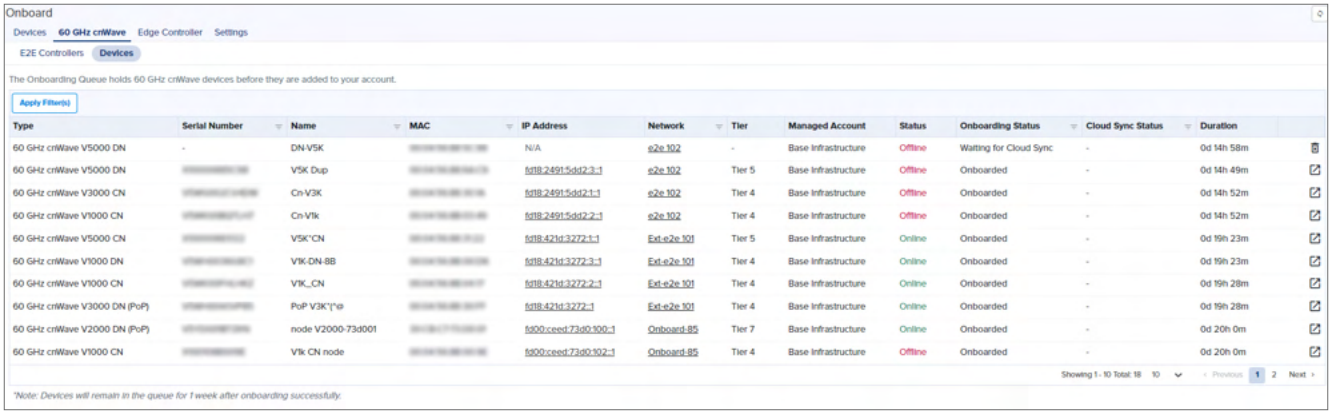
If PoP Node is running the Onboard E2E Controller then, the PoP icon will be indicated with as shown below:



60 GHz E2E Controller Onboarding devices

The Onboarding Queue holds 60 GHz cnWave devices before they are added to your account and displays the Onboarding and Cloud Sync status as shown in Figure 45.

Figure 45 *: 60 GHz cnWave devices*



Deleting Devices in Bulk

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

- From the On-Premises instance:
  - Unmanaged devices from the **Onboard** > **Devices** page.
  - Onboarded and managed devices from the **Inventory** page (both online and offline)—at the System-, Network-, Tower-, and Site-levels.
  - From the **Manage Subscriptions** > **Devices** page.
- From the Cloud Anchor account:
  - Onboarded and managed devices from the **Inventory** 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.

Note

- To delete devices in bulk from the On-Premises instance, the instance must be connected to a Cloud Anchor Account.
- Deleting cloud-synched devices from the On-Premises instance creates a job in both the On-Premises instance and the Cloud Anchor account.

  However, deleting devices from the Cloud Anchor account creates a job in the Cloud Anchor account only.

The following topics are described:

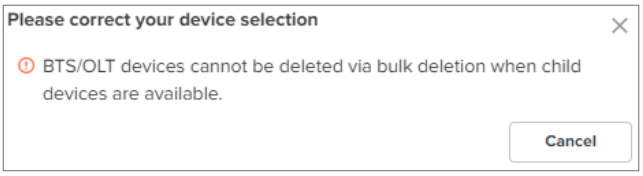
- Device-specific restrictions
- Deleting devices in bulk
- Viewing the status of device deletion and retrying

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 46 *Deleting BTS/OLT devices in bulk*

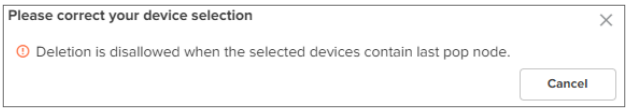
  However, you can delete a single BTS or OLT devices along with the associated devices (CPE or OLT) when you click the delete ( ) icon in the corresponding row.

  Figure 47 *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:

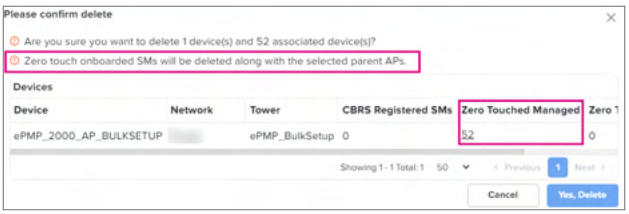
    Figure 48 *Deleting Onboard E2E Controllers with last pop node*

    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 49 *Deleting APs with SMs onboarded using zero touch method*

  - 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 50 *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.

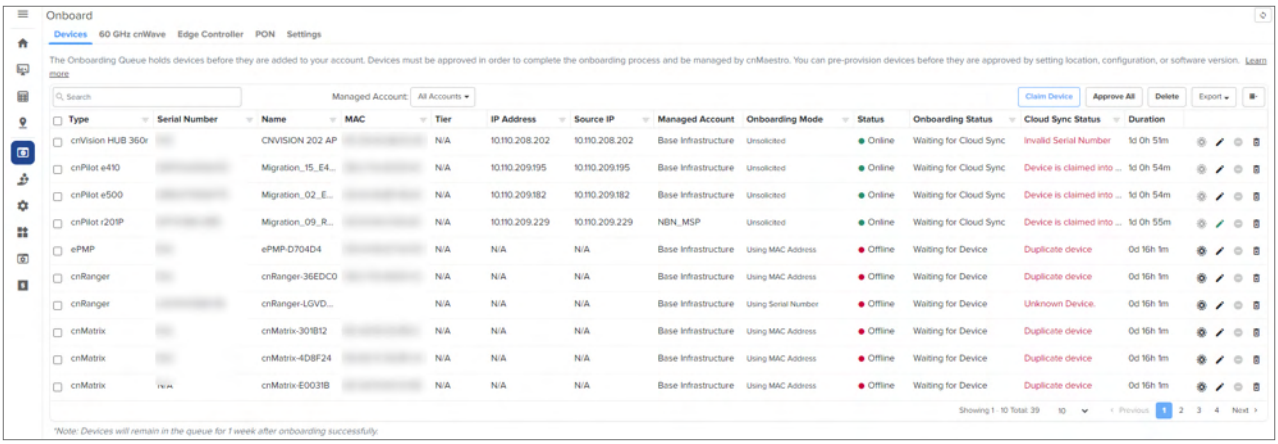
  This occurs even when CBRS-claimed SMs are not selected for bulk deletion.

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 51 *Onboard > Devices page*



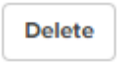
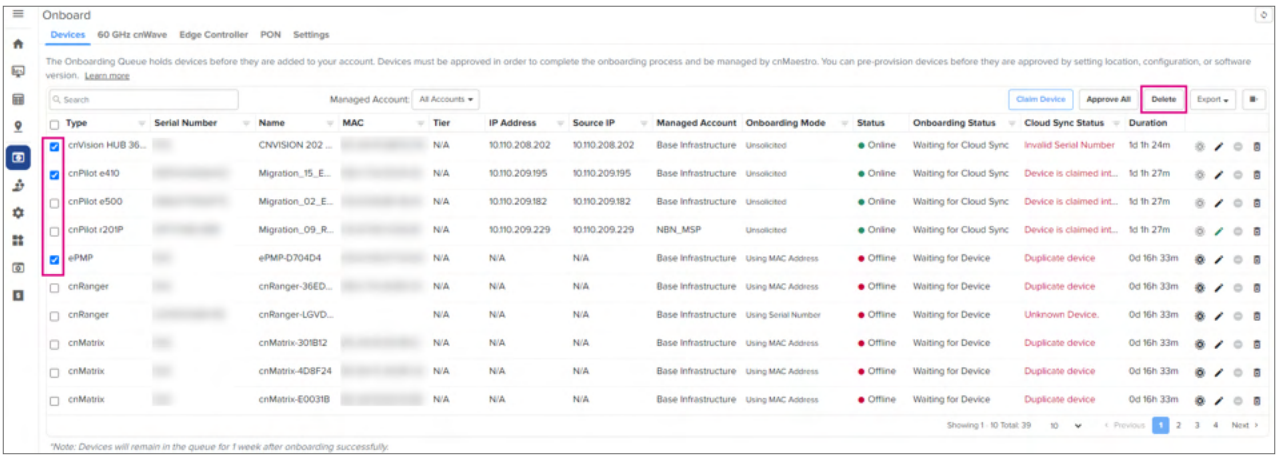
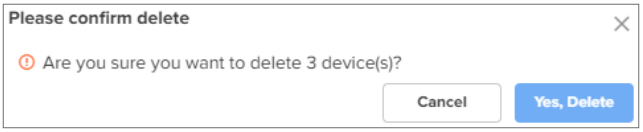
2. Select the checkboxes corresponding to the devices that you want to delete and click the **Delete** () button.

   Figure 52 *Select devices*



3. Click **Yes, Delete** in the confirmation dialog box.

Figure 53 *Confirmation*



4. The devices are removed from the page and a banner appears on the top of the page for the deletion job created.

   Figure 54 *Deletion job banner*

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

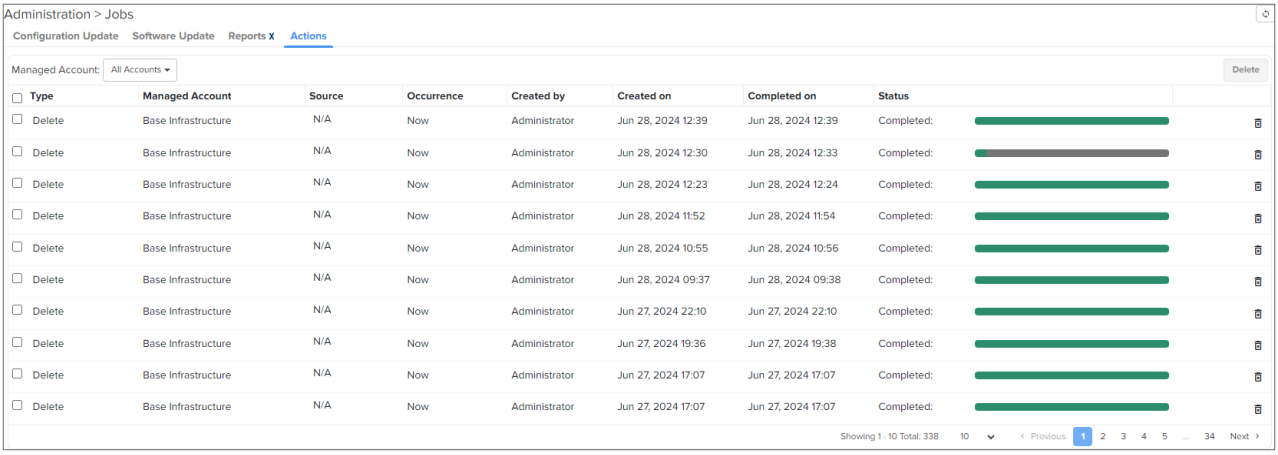
Viewing the status of device deletion and retrying

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:

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

   Figure 55 ***Administration*** > ***Jobs*** > ***Actions*** *page*



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

   The Delete Status window appears.

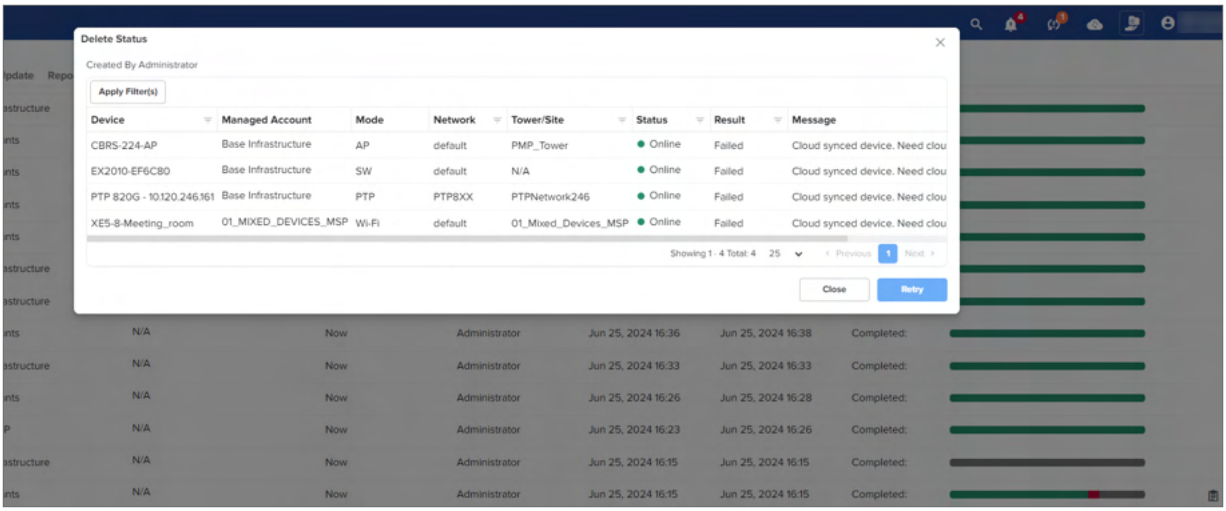
   Figure 56 *Delete Status window*

   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 57 *Delete status for failed delete*



- 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 (%).

3. 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**.

Export All as CSV

The **Export All as CSV** feature allows users to download all data records displayed in a table as a CSV file. Unlike the **Export Page as CSV** option that downloads only the currently visible page, this feature retrieves and prepares all available filtered records for download.

This feature triggers an immediate download process that is handled through a **Download Manager**.

cnMaestro supports the following limits in this feature:

Parameter	cnMaestro X	cnMaestro Essentials
Maximum number of records included in the export **Note** This limit is applicable only on some pages, such as on the **Notifications** page where the info icon is visible Export all as CSV ⓘ. For all other pages where this export option is available, there is no limit. Following are some of the pages where this limit is not applicable: • **Statistics** • **Clients** • **Inventory** • **Device Overrides**	50000	20000
Number of concurrent exports per account	5	3

Note

The generated CSV file is available for download for a duration of 24 hours only.

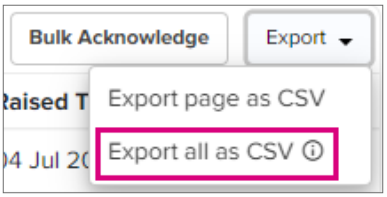
Exporting and downloading all data in the CSV format

To export and download the data in the CSV format, complete the following steps:

1. Navigate to the page where you want to export the data, for example, **System** > **Notifications** > **Alarms**.

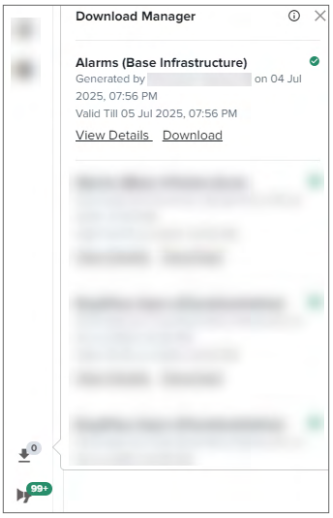
   You can either download the complete data or download a specific set of filtered data.

2. From the Export dropdown list, select **Export all as CSV**.



   A message is displayed informing the data is being populated.

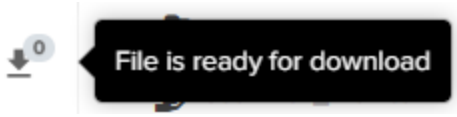
3. Click the download manager ( ) icon on the bottom left of the page.



The Download Manager displays the progress of the export with the following statuses:

- —File is successfully generated

  A successful notification message is also displayed.

- —File generation is in progress
- —File generation failed. Check details for more information.

4. Click View Details, to view the following details of the file generated:

Details of Alarms (System)	
Generated By	
Generated On	05 Sep 2025, 11:48 AM
Expired by	06 Sep 2025, 11:48 AM

5. To download the CSV file, click **Download**.

Monitoring

This section includes the following topics:

- Network Monitoring
- 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

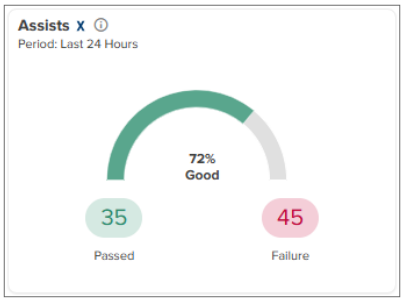
Network Monitoring

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

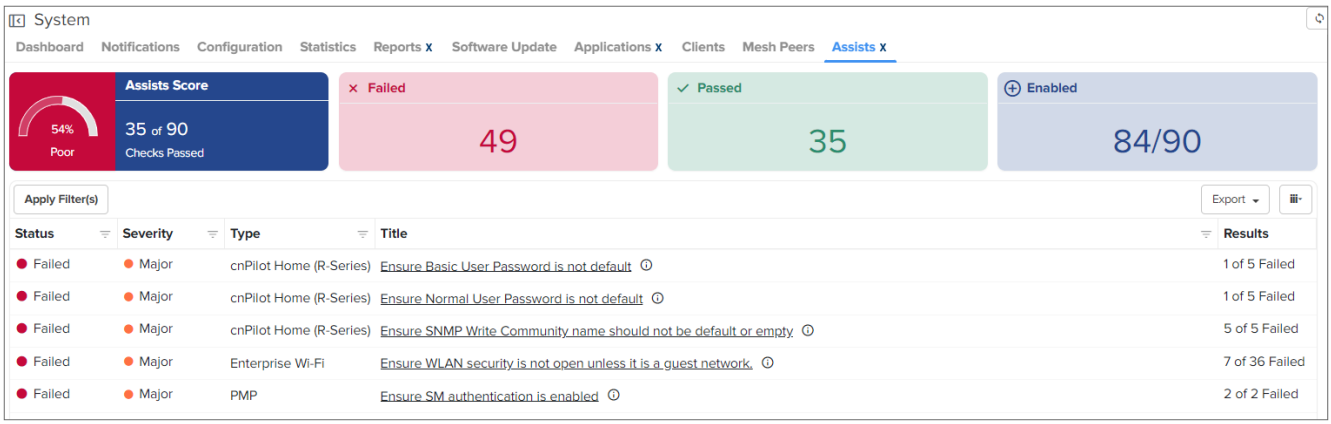
Assists X displays scanned configuration scores and results for last 24 hours.



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 58.

This enables prioritization of management traffic.

Figure 58 *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 23.

Table 23 *Assist Scores*

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

Table 24 *Assists X parameters*

Fields	Description
Status	Status of the assists are shown as follows: • Passed • Failed • Disabled
Severity	Severity level of the assists are shown as follows: • 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 59.

Hovering the cursor on the **Results** column in the Assists X home page displays a preview of the assist results as shown in Figure 59.

Figure 59 *Assists X Results*

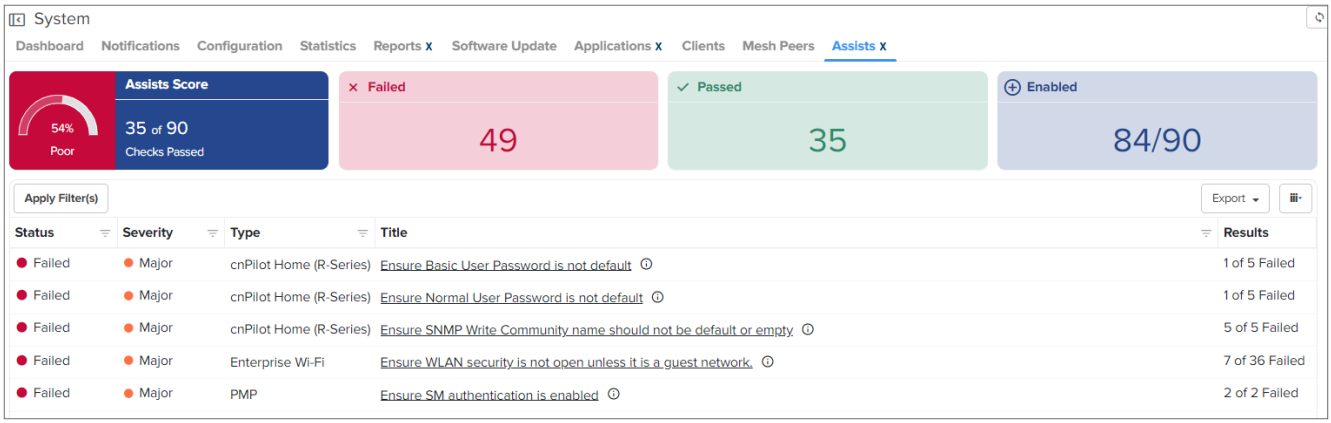


Table 25 *Assist Result Status*

Assist Result	Description
Passed	Assists recommendations are met.

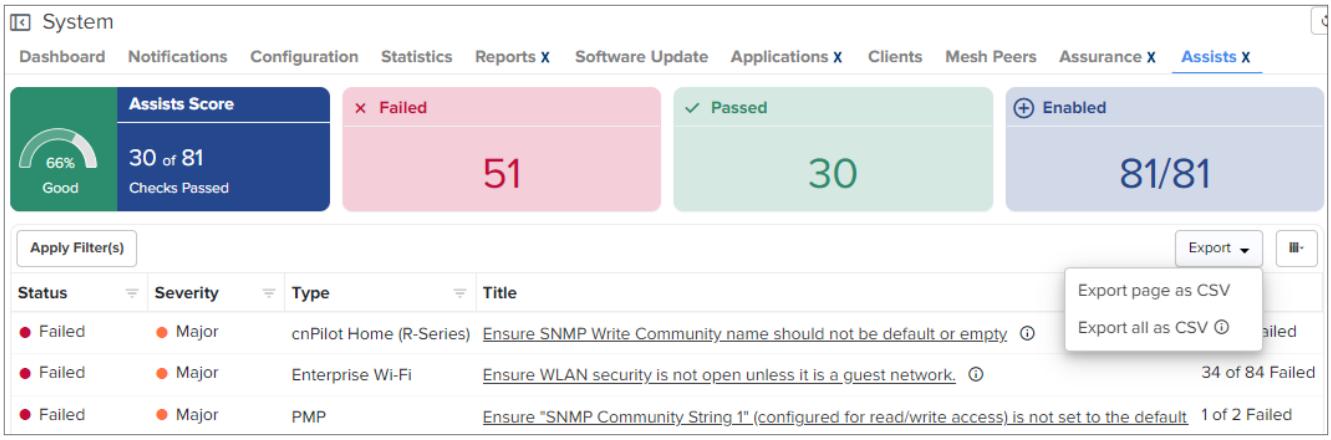
Table 25 *Assist Result Status*

Assist Result	Description
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

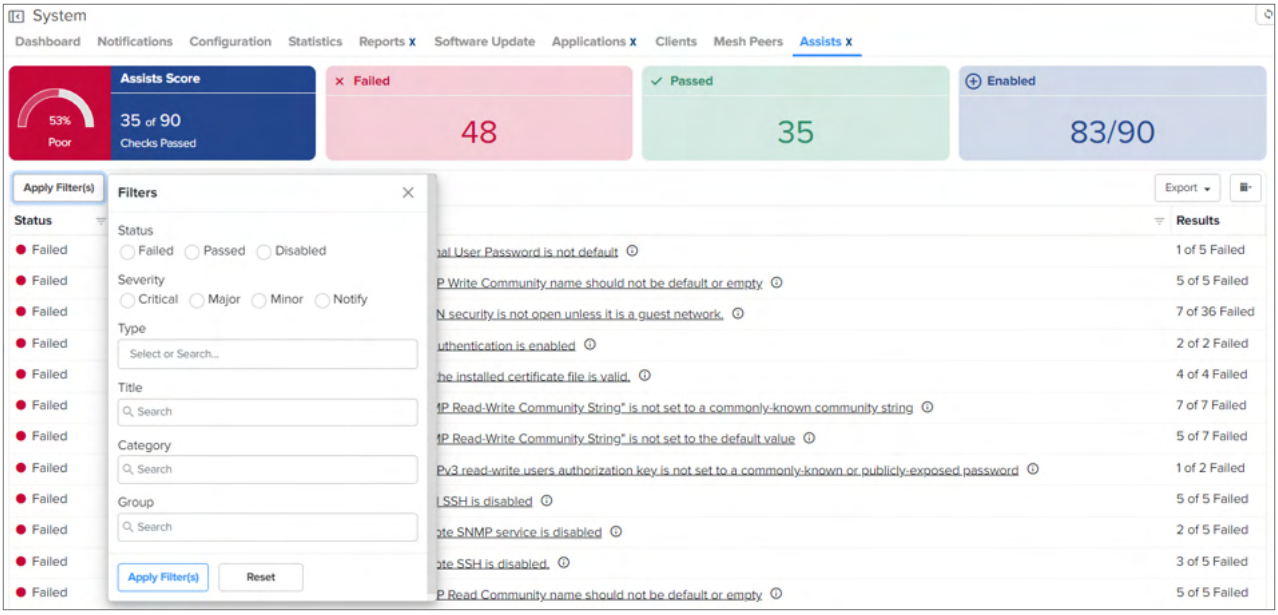


Assists filter

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 60 *Assists: New Filter*



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.

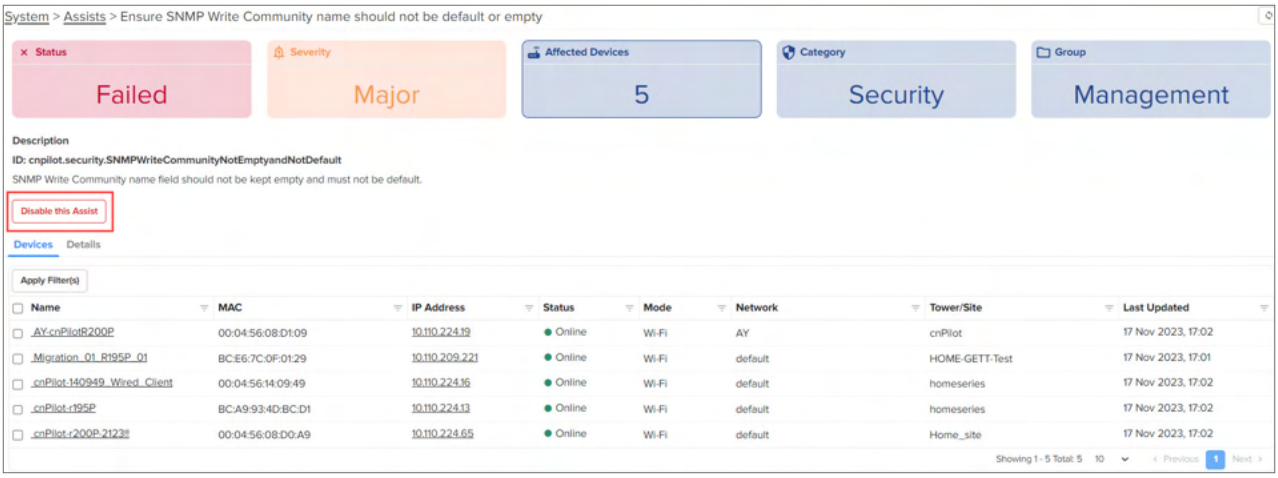
Assists Status

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 61.

To disable Assists, perform the following steps:

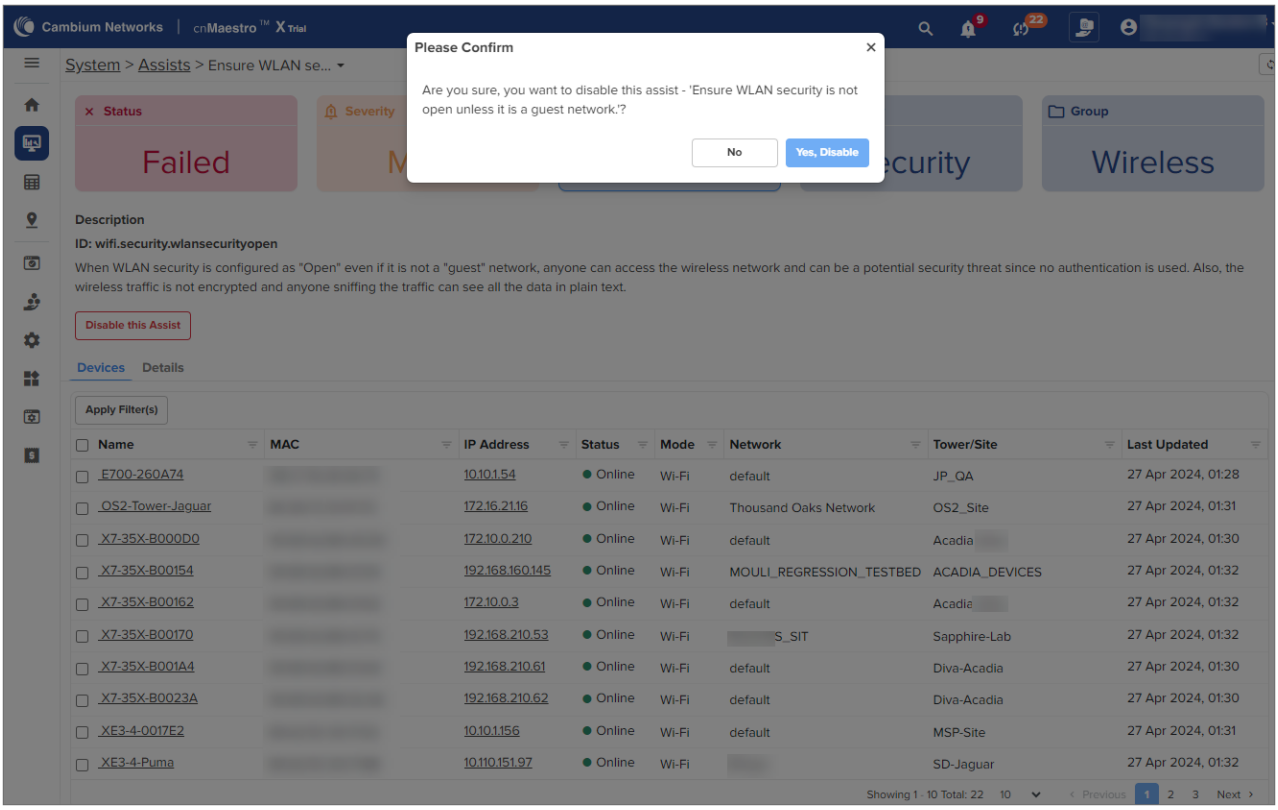
1. In the **Assist Status** page, click **Disable this Assist.**

   Figure 61 *Assist Status page*



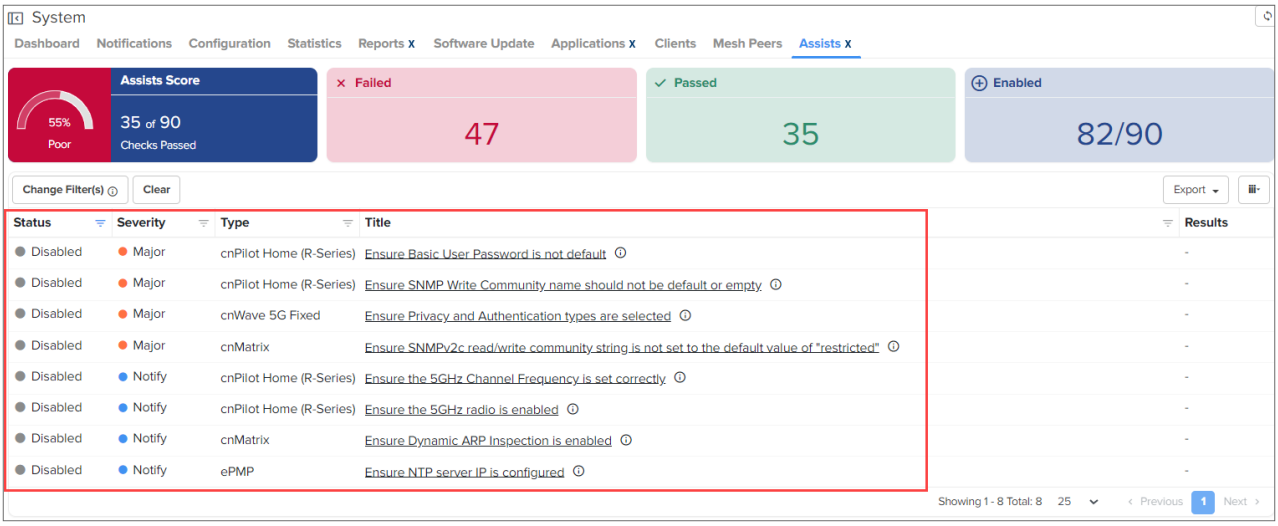
   A confirmation message appears for the assist to disable.

2. Click **Yes, Disable**.

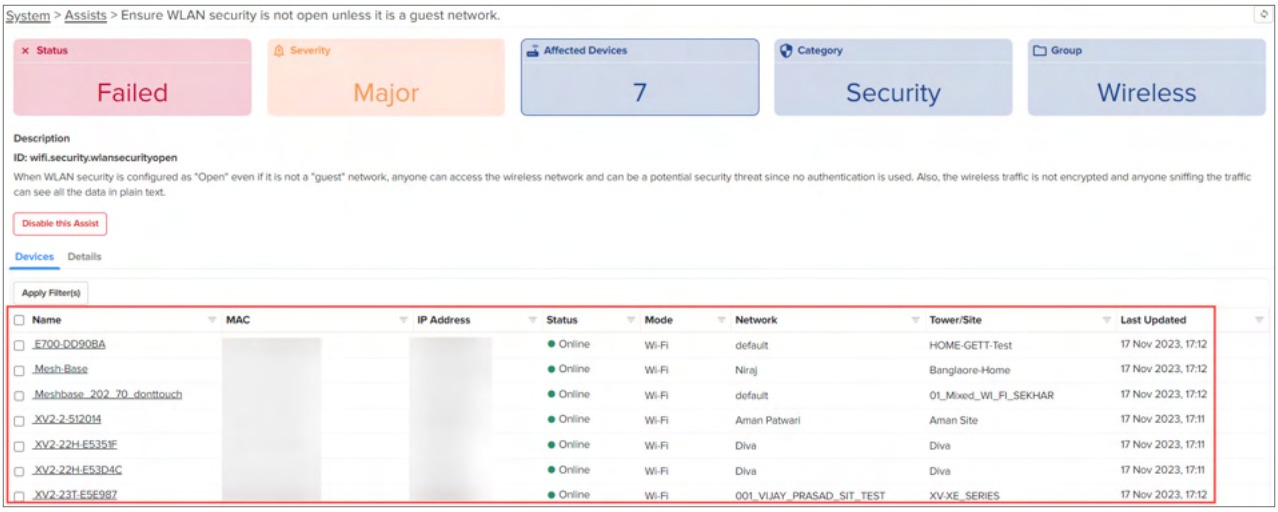


Disabled Assists are listed at the bottom of the Assists X home page. The **Results** column do not indicate the progress bar for the Assists Disabled as shown in Figure 62. The total number of enabled Assists in the home page is reduced when Assists is disabled.

Figure 62 *Assists Disabled*



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

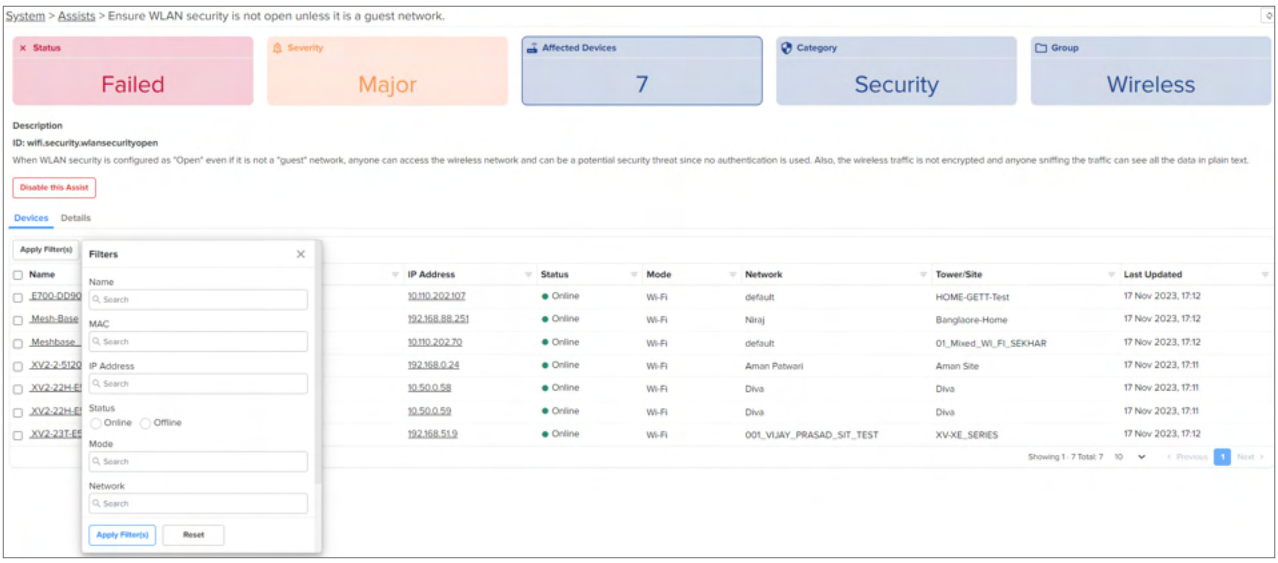


Device filter

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 63 *Assists device filter*



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

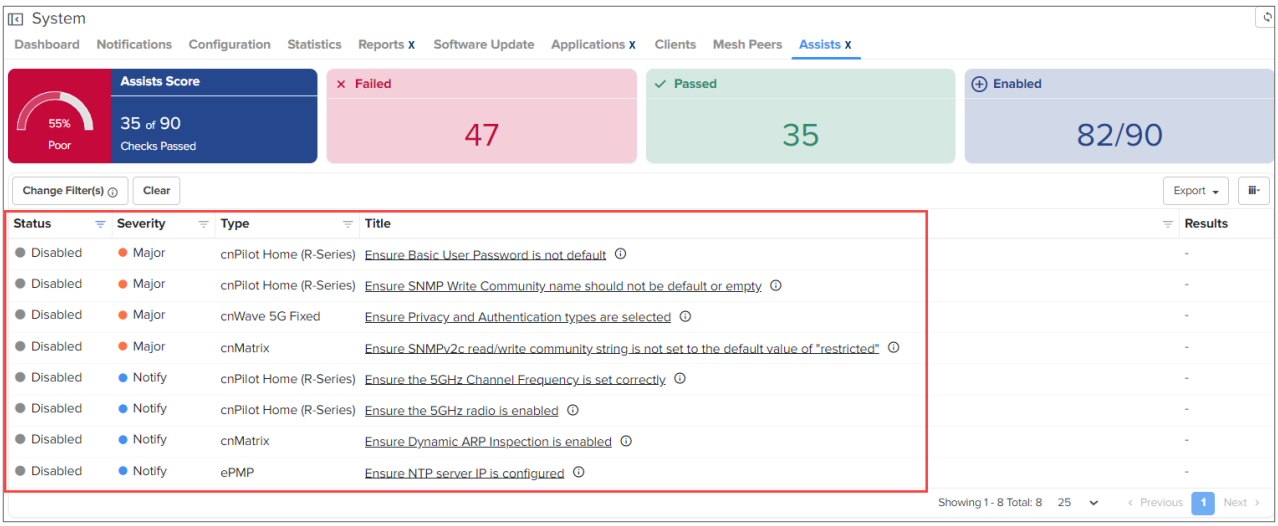
6. Click **Reset** to reset the filter option in the device table.
7. Click **Clear Filters** to clear all the filter options.

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

Enable Assist

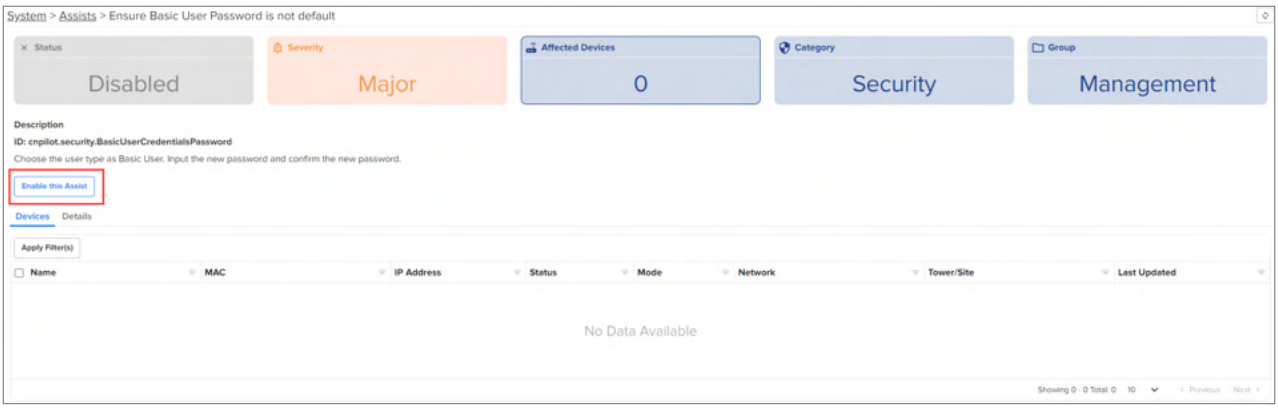
To enable assist, perform the following steps:

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



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

2. Click **Enable this Assist**.



Assists X fix now

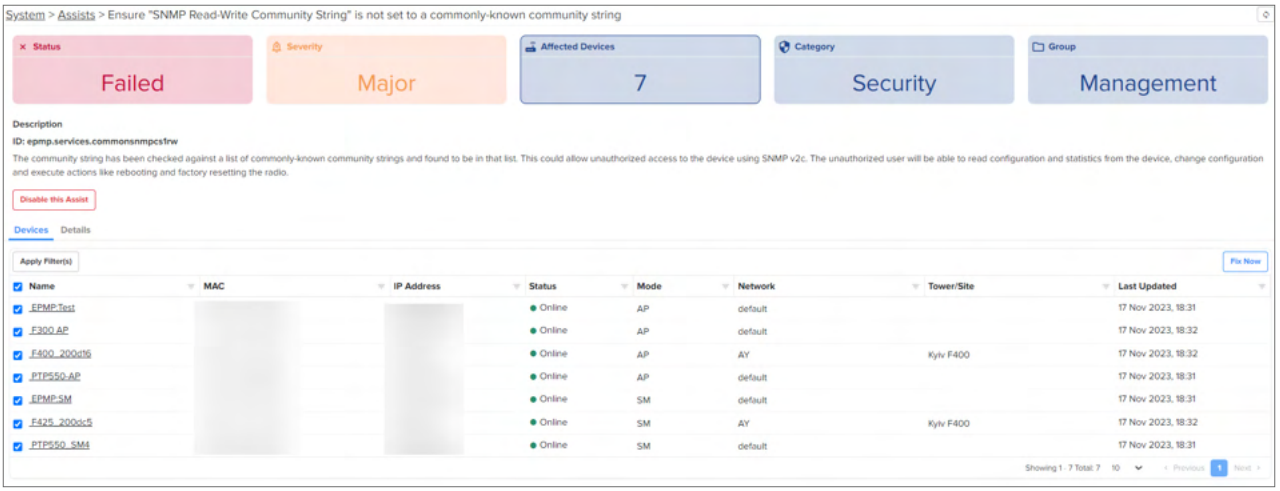
Note

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.



3. Click **Fix now**.

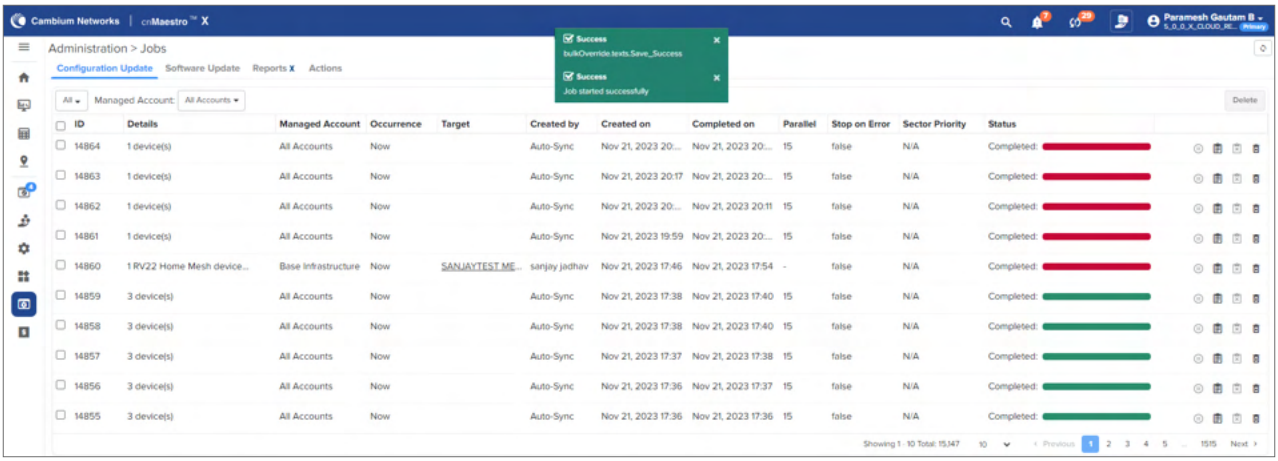
   The **Fix Now** window pops up.

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.



When the failed assists are fixed, the status is changed to **Passed** as shown in Figure 64.

Figure 64 *Passed Assists*

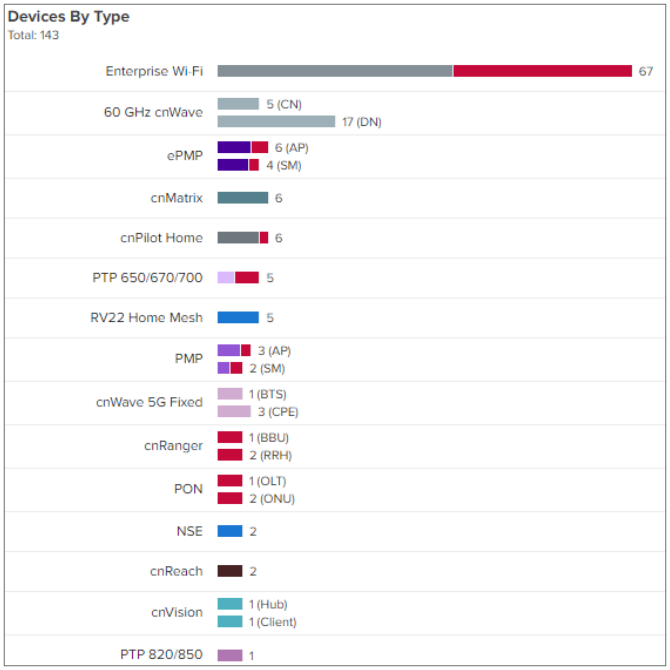
Dashboard

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 65 *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 and Applications X

The **Application History X** and the **Category History X** widgets in the **System Dashboard** page display the application-wise and category-wise usage history along with the top five client usage details for the last 7 days.

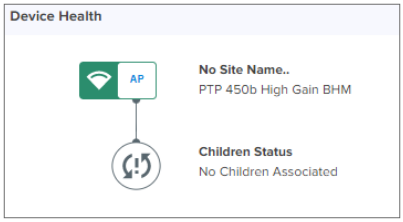
Figure 66 *Application History X*

Figure 67 *Category History X*

Device Health

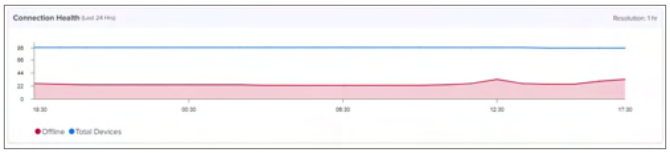
Device Health displays the health of the network from the Tower to the edge Device.

Figure 68 *Device Health*



Connection Health

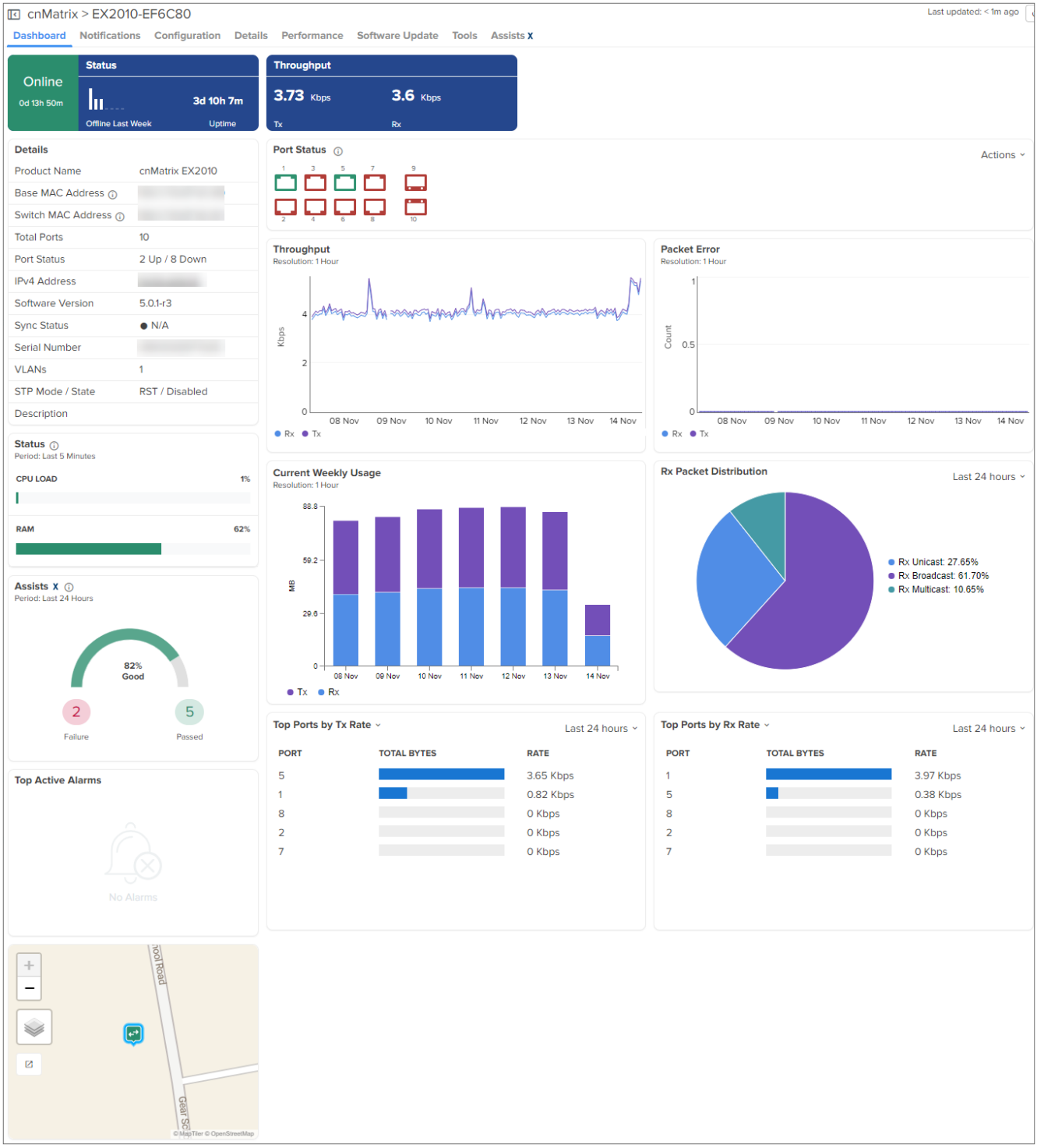
Connection Health displays the health of the devices connected to the network.



Charts and Graphs

Contextual charts and graphs provide details on important dashboard metrics.

Figure 69 *Charts and Graphs*



Site dashboard

The Site dashboard displays cumulative information about the devices present in them. cnMaestro allows you to create the following types of sites:

- Enterprise (for Enterprise Wi-Fi APs and cnMatrix switches)
- Home site (for R-series APs)

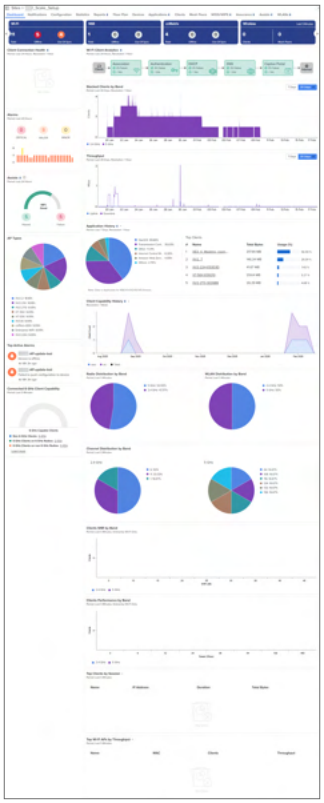
- 60 GHz cnWave site (for 60 GHz cnWave devices)
- PON site (for PON devices—OLTs, ONUs)

The information displayed on this dashboard depends on the type of site that you create.

- Enterprise Site dashboard
- 60 GHz cnWave Site Dashboard
- PON Site Dashboard

Enterprise Site dashboard

The Enterprise Site Dashboard provides the overview of site-related parameters and devices applicable to Enterprise Wi-Fi APs and cnMatrix devices.



The Enterprise Site Dashboard displays the following graphics:

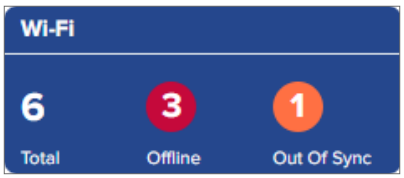
- Devices widget (Total, Offline, Out of Sync)
- Throughput
- Client Connection Health X
- Wi-Fi Client Analytics X
- Assists X
- Alarms
- Top Active Alarms
- AP Types
- Channel Distribution by Band

- Clients Performance by Band (Enterprise Wi-Fi)
- Clients SNR by Band (Enterprise Wi-Fi)
- Connected 6 GHz Client Capability
- Application History X and Applications X
- Client Capability History
- Radio Distribution by Band
- WLAN Distribution by Band
- Throughput Graph
- Top Wi-Fi APs by Throughput or Clients
- Top Clients by Session
- Top Clients by Usage

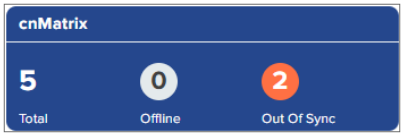
Devices widget (Total, Offline, Out of Sync)

Displays total number of APs and cnMatrix switches in the Site and the devices that are offline and out of sync in respective widgets:

Wi-Fi APs widget (Total, Offline, Out of Sync)



cnMatrix devices widget (Total, Offline, Out of Sync)



- **Total**—Click the number to display the **Sites** > **Devices** > **List** page with the device type filter applied.
- **Offline**—Click the number to display the **Sites** > **Devices** > **List** page with the **Status** filter applied as **Offline**.
- **Out Of Sync**—Click the number to display the **Sites** > **Devices** > **Configuration** page with the **Sync Status** filter applied as **Not In Sync**.

  The Out of Sync feature is applicable to Enterprise Wi-Fi APs and cnMatrix switches.

  To sync the configuration, select the required devices and click **Sync Configuration**.

Figure 70 *Devices > Configuration page for Enterprise Wi-Fi APs*

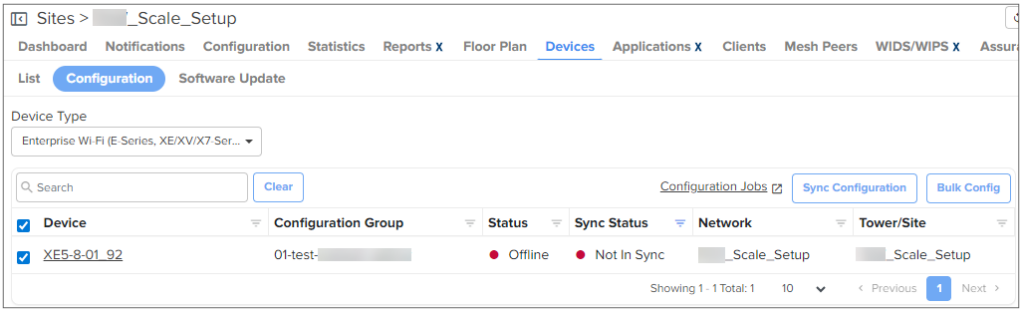
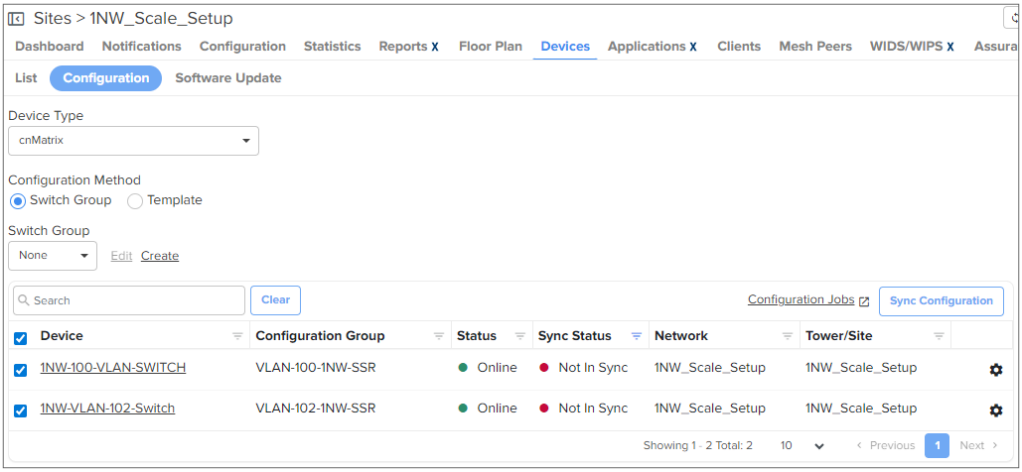


Figure 71 *Devices > Configuration page for cnMatrix switches*

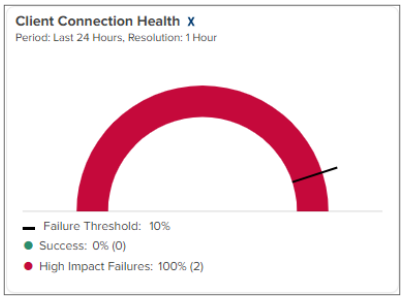


Throughput

Displays aggregated throughput for all the clients.

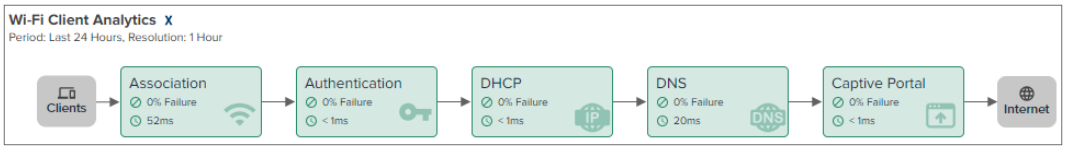
Client Connection Health X

Displays the percentage of success and failed client connections in that site.



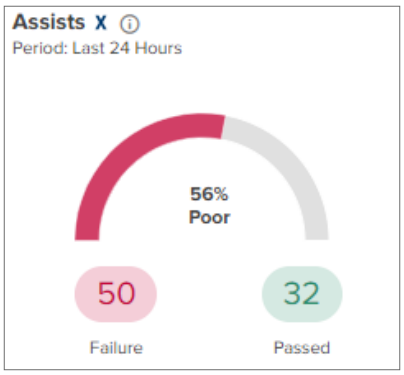
Wi-Fi Client Analytics X

Displays the failure percentage in each stage of the client connection to the AP and subsequent network access.



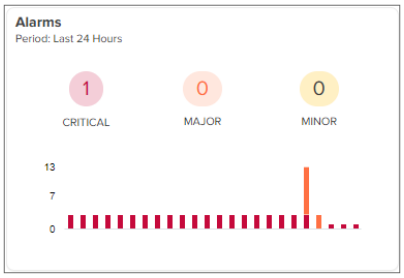
Assists X

Assists X displays scanned configuration scores and results for last 24 hours for that site. For more information, see Assists X.



Alarms

Displays the alarms raised for the devices in the Site in the last 24 hours as a bar graph. It also displays the count of critical, major and minor alarms raised. Clicking the number displays the **Site** > **Notifications** > **Alarms** page. For details about the **Alarms** page, see Alarms.

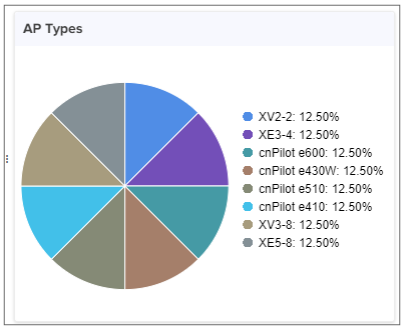


Top Active Alarms

Displays the topmost active alarms raised in that Site.

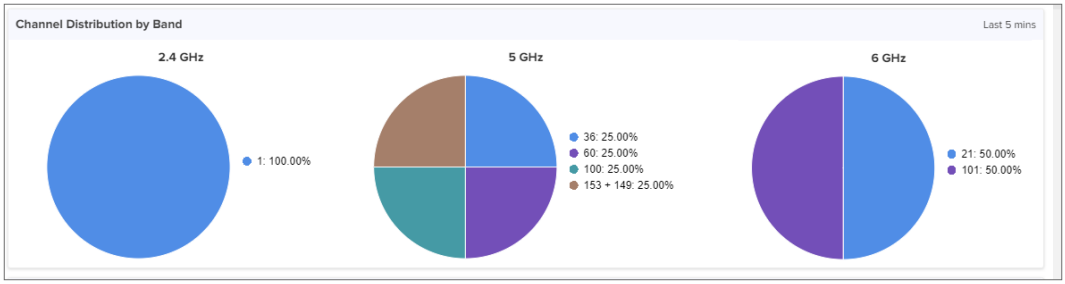
AP Types

Displays the distribution of different AP models in a pie chart.

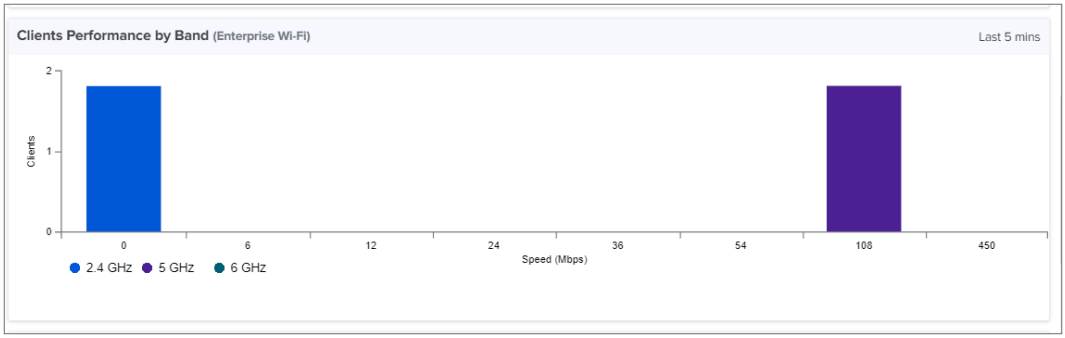


Channel Distribution by Band

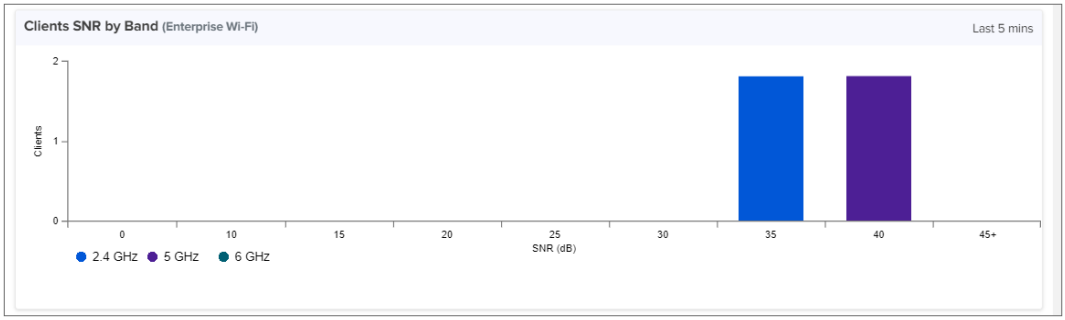
Channel distribution displays usage of channels in 2.4 GHz, 5 GHz. This helps in planning and implementing WLANs within a high-density environment. .



Clients Performance by Band (Enterprise Wi-Fi)



Clients SNR by Band (Enterprise Wi-Fi)



Connected 6 GHz Client Capability

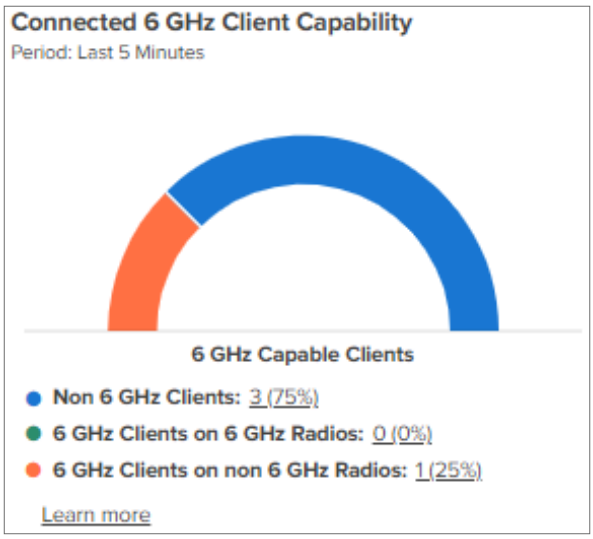
The Connected 6 GHz Client Capability widget presents a point-in-time view of Wi-Fi 6 GHz clients associating to non-6 GHz radios. These clients may experience better service if SDR radios are upgraded from 5 GHz to 6 GHz. A high percentage of 6 GHz capable clients connecting to non-6 GHz radios is an indication to upgrade radios to 6 GHz. The Connected 6 GHz Client Capability widget is represented using different colors and corresponding percentage values as described below:

- Non 6 GHz Clients: represents non 6 GHz clients connected across the devices at the Site level.
- 6 GHz Clients on 6 GHz Radios: represents 6 GHz clients connected across the devices at the Site level.
- 6 GHz Clients on non 6 GHz Radios: represents 6 GHz clients connected across the devices on non 6 GHz radios at the Site level.

Note

For best results, deploy a few radios in 6 GHz mode in high traffic areas.

Figure 72 *Connected 6 GHz Client Capability*

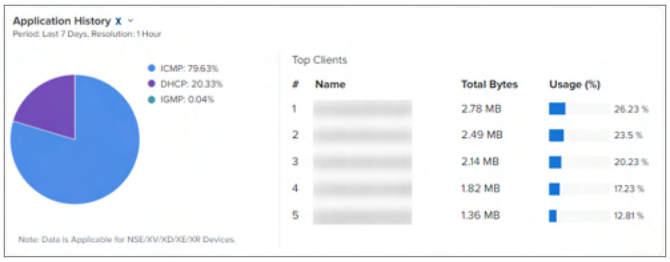


Clicking next to clients number navigates to **Wireless Clients** page.

Application History X (Category History X)

The Application History X (Category History X) section displays a pie chart with the distribution of the top protocols used by clients connected to the Enterprise devices (XV/XD/XE/XR). It also displays the details of the top five clients based on data usage.

From the section title dropdown list, select Category History X to display the pie chart with the distribution of categories.



Client Capability History

The Client Capability History graph displays the highest detected Wi-Fi protocol for Clients active at a Site on a weekly basis. Wi-Fi 6 GHz devices are grouped into a single 6 GHz category. A large number of 6 GHz Capable Clients is an indication 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 73 *Clients History in line chart*

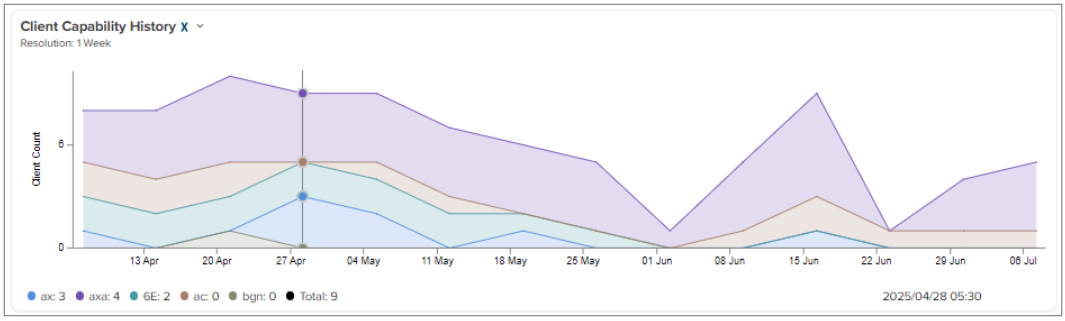
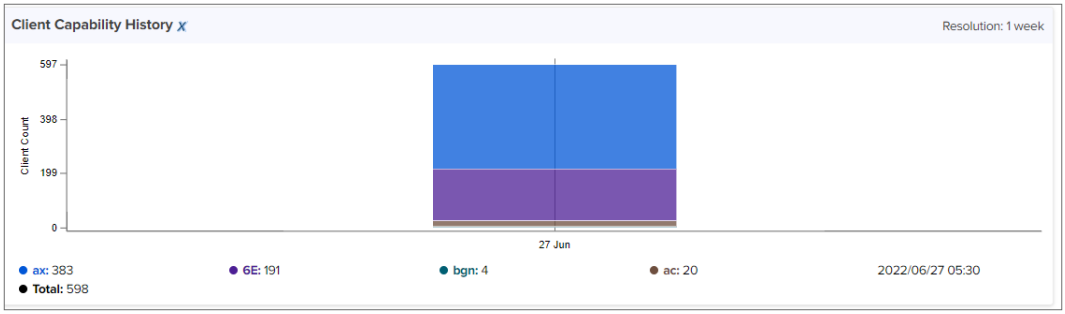
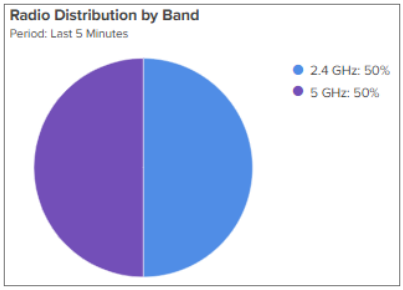


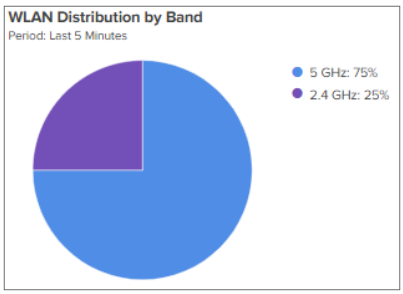
Figure 74 *Clients History in bar chart*



Radio Distribution by Band

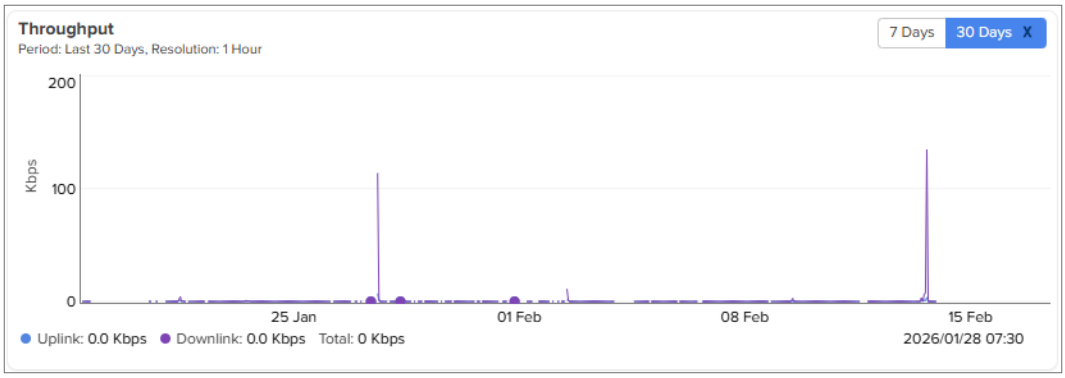


WLAN Distribution by Band



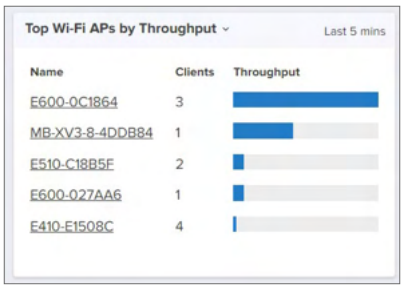
Throughput Graph

Throughput graph displays client traffic for the last 7 days or 30 days (**X**).



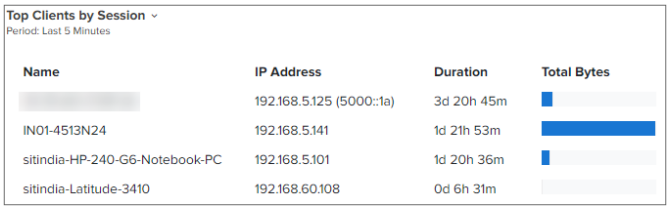
Top Wi-Fi APs by Throughput or Clients

Displays a bar graph with the top APs listed by the throughput or by the number of clients connected to them.



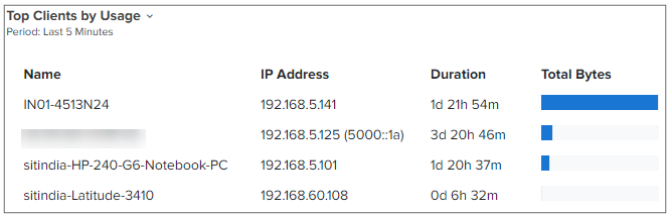
Top Clients by Session

Displays the top clients by session and the respective details.



Top Clients by Usage

Displays the top clients by usage and the respective details.



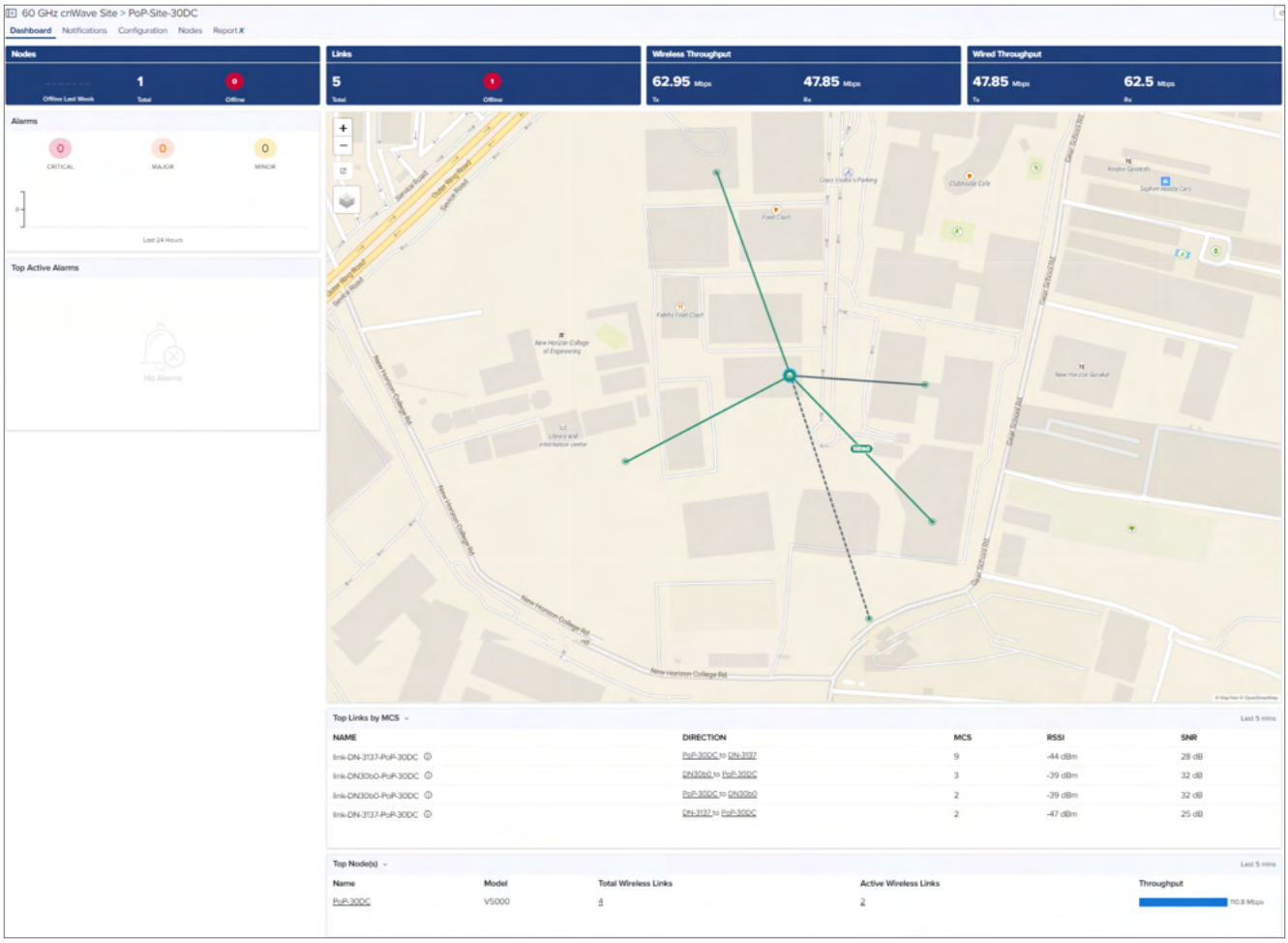
60 GHz cnWave Site Dashboard

Dashboard pages are customized for each device type and aggregation level.

The 60 GHz cnWave Site dashboard section displays the following:

- Nodes
- Links
- Wireless Throughput
- Wired Throughput
- Alarms
- Top Active Alarms
- Top Links by MCS, RSSI, and SNR
- Top Node(s), PoP(s), DN(s), and CN(s)

Figure 75 *60 GHz cnWave Site Dashboard*



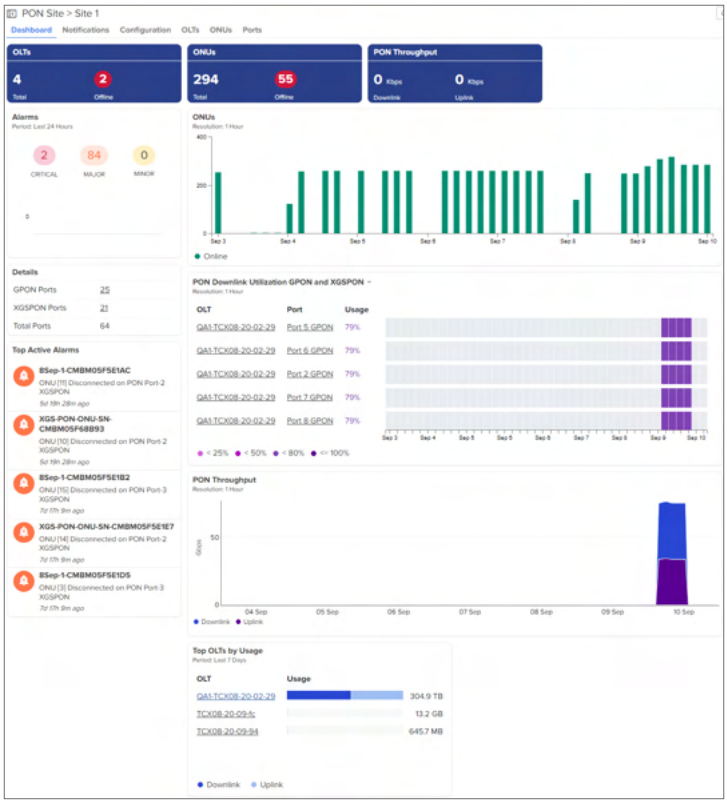
PON Site Dashboard

Dashboard pages are customized for each device type and aggregation level.

The 60 GHz cnWave Site dashboard section displays the following:

- OLTs count
- ONUs count
- PON Throughput
- Alarms
- Details
- Top Active Alarms
- ONUs graph
- PON Downlink Utilization GPON and XGSPON
- PON Throughput
- TOP OLTs by Usage

Figure 76 *PON Site Dashboard*



Notifications

The **Notifications** page displays details of alarms, alarm history, and events. These are synchronous messages that provide real-time system status.

Table 26 *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.

Table 26 *Notification overview*

Type	Description
	Note After every server reboot or restart: • cnMaestro takes up to 10 minutes to reflect the alarm count. • Email Notification subscribers status up and down major alarms are blocked for 30 minutes. • Webhooks will not send device status up and down major alarms for next 30 minutes.
Alarms History	Expired Alarms are added to the Alarm History. The Alarm History page displays historical active alarm counts. **Note** When an alarm changes to the inactive state, it is displayed for a maximum of 30 days.
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 77 and Figure 78:

- **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 77 *PTP 820/850 Device Alarms*

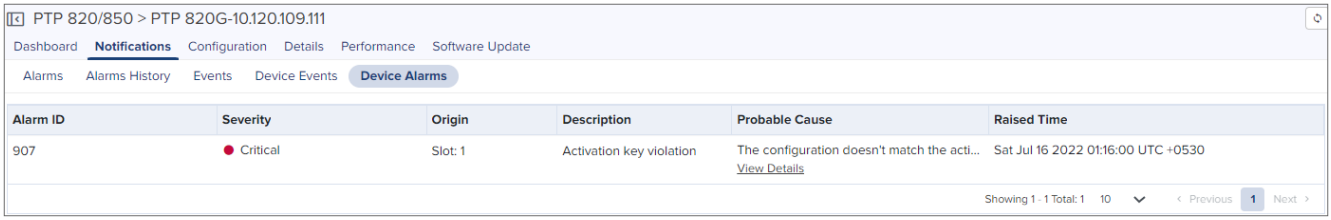
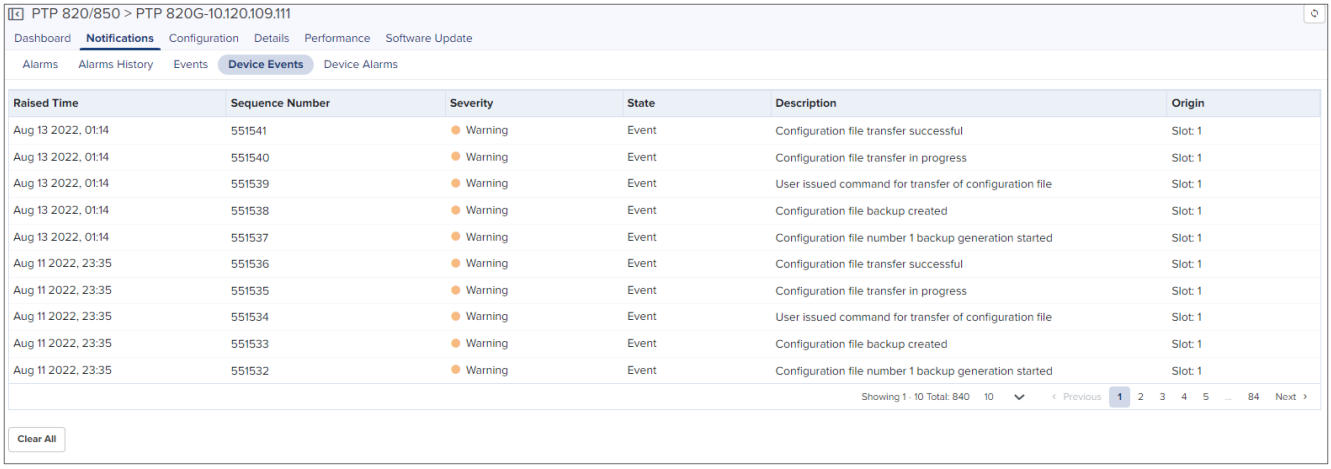


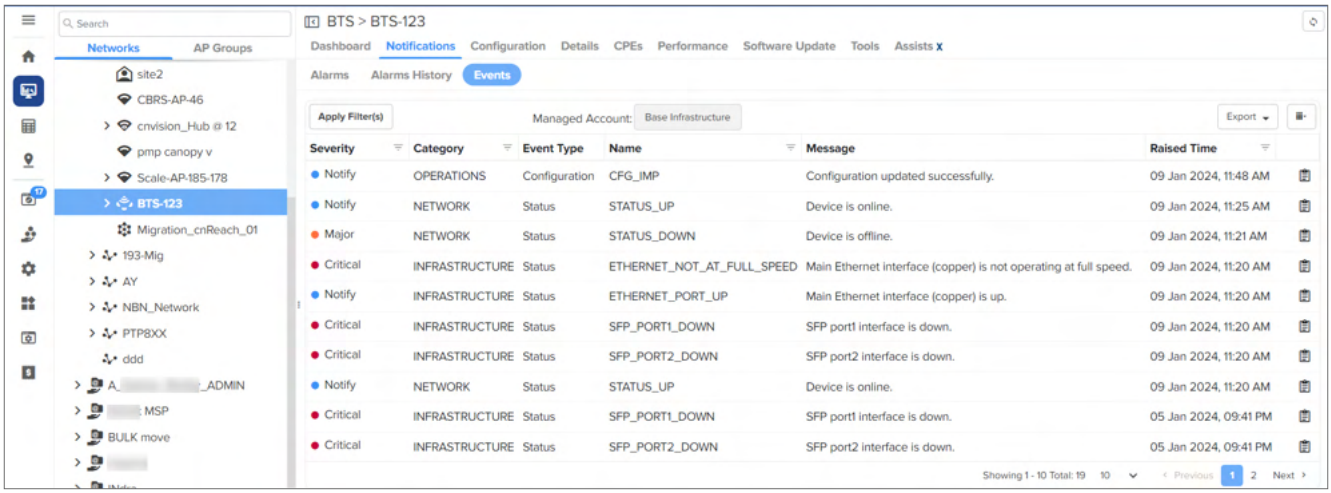
Figure 78 *PTP 820/850 Device Events*



For cnWave 5G Fixed products, the **Notifications** page contains the following tabs:

- **Alarms**: Displays the count of critical, major, and minor alarms raised for the BTS or the CPE device. The **Alarms** page also displays severity level, alarm name, message (a brief description), duration, alarm status, raised time, and the acknowledged status of alarm in a table.
- **Alarms History**: Displays details of expired alarms in graph and table format.
- **Events**: Displays information of events raised for the BTS or the CPE device. Using the **Apply Filter(s)** button, you can select and view the event related parameters such as severity, category, event type, name, message, and raised time (as shown in Figure 79). Click the **View Details** icon to view detailed information of a specific event. To export the alarm data in the CSV format, click **Export**.

Figure 79 *cnWave 5G Fixed Events*



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 27 *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

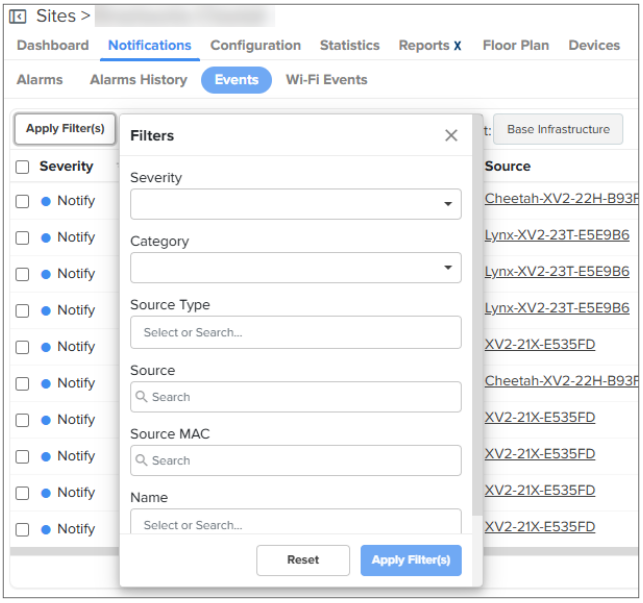
The data in the Event table is exported in a CSV file format. The following export options are available:

- Export page as CSV
- Export all as CSV

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 80 *Events: New Filter*

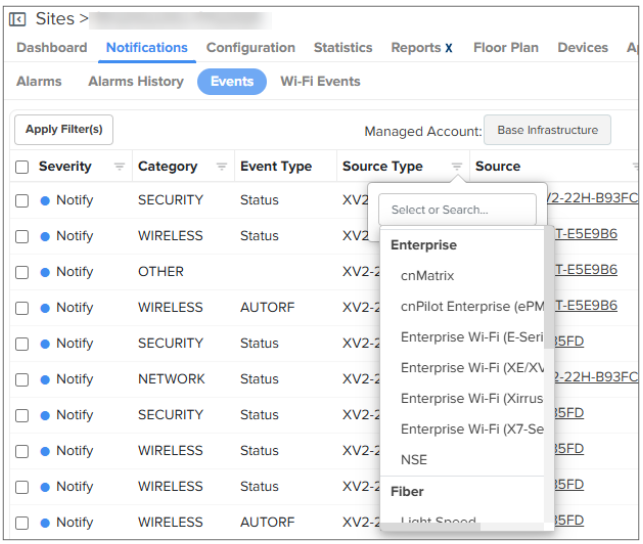


You can manually filter or search by typing parameters in the column header of the Events table.

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

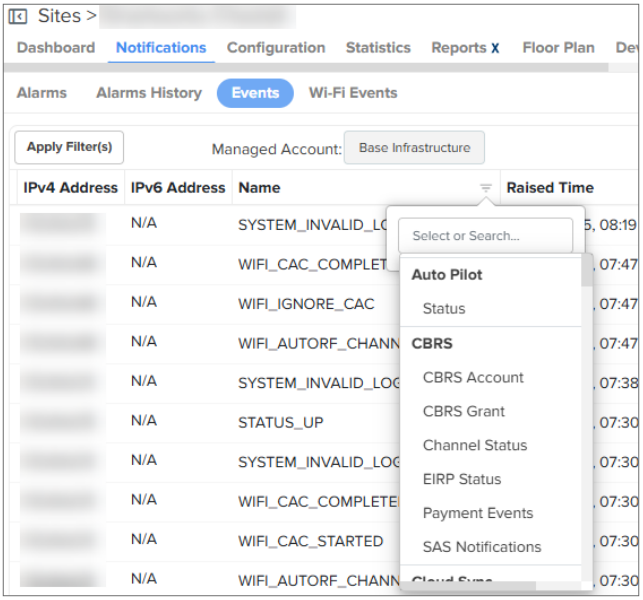
   If you do not receive expected filter details, click **Change Filter(s)** in the Events table to apply new filters.

Figure 81 *Events: Source Type filter*



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 28.

Figure 82 *Events: Name filter*



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 83 *Events: Delete event(s)*

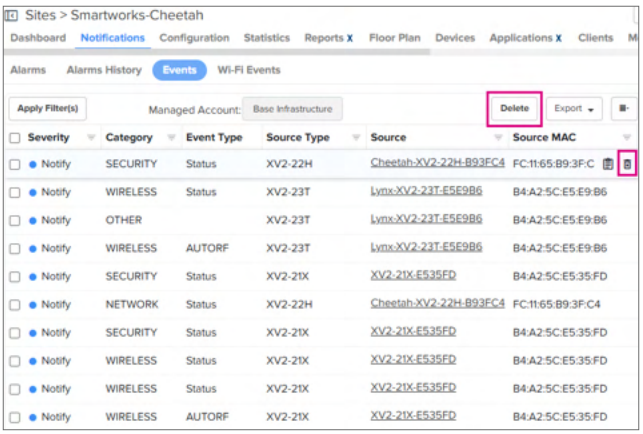


Table 28 *Category Names and Codes*

Category	Subcategory	Codes
Auto_pilot	Auto Pilot Status	AUTOPILOT_ADDED_AP
		AUTOPILOT_AP_CONNECTED
		AUTOPILOT_AP_DISCONNECTED
		AUTOPILOT_REMOVED_AP

Category	Subcategory	Codes
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
Configuration	Config Sync	CFG_IMP
		CFG_EXP
		CONFIG_SYNC
		CFG_UPD_ST
		SYSTEM_CONFIG_APPLIED

Category	Subcategory	Codes
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
E2E	E2E Events	E2E_CTLR_IMG_UPD
GPS	GPS Status	GPS_SYNC_ST
		GPS_FW_UPD_ST
		GPS_VER
		GPS_SYNC

Category	Subcategory	Codes
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
		DHCPSRVR_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
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
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

Category	Subcategory	Codes
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
	Client Dissociation	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 29 *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
Wired	Events related to issues/notifications with the wired Wi-Fi AP Clients. Source: Devices and Clients
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:

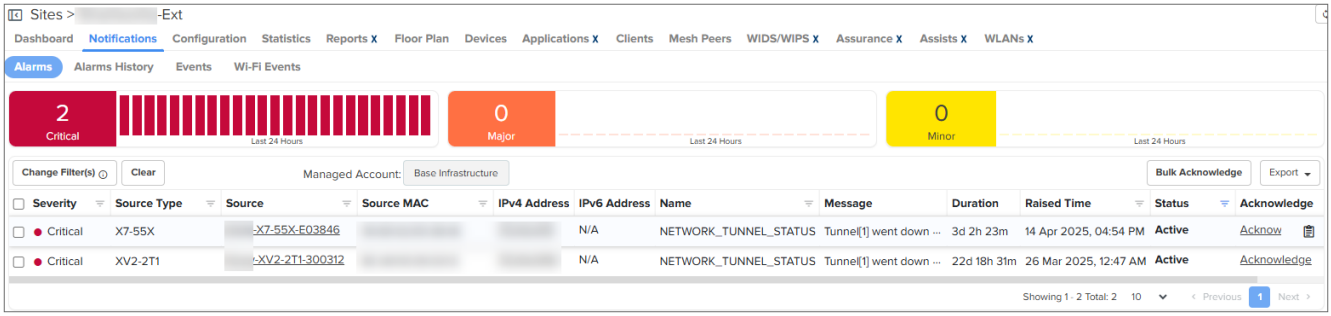


Table 30 *Alarm Life Cycle*

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.

Table 30 *Alarm Life Cycle*

State	Description
Active	The alarm remains active until the combination of inputs that generated it are cleared.
Expired	Expired Alarms are placed in the Alarm History.
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 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 31 *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

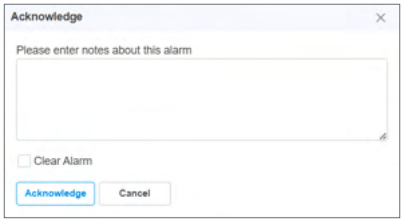
Table 32 *Alarm Types*

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 84 *Alarm Acknowledgment*

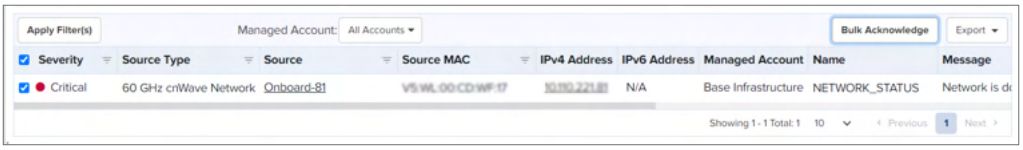


Alarm Bulk Acknowledgment

To acknowledge multiple alarms at the same time, follow these steps:

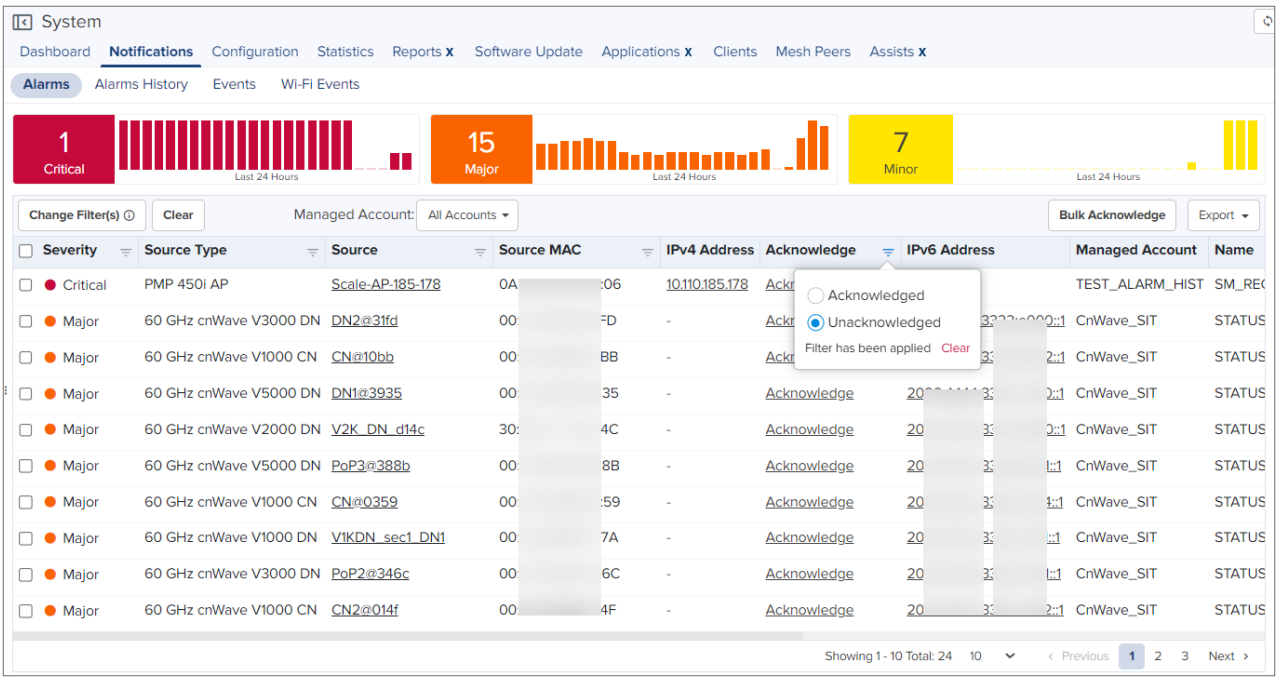
1. Navigate to the **Monitor and Manage** > **Notifications** > **Alarms** page.

   Figure 85 *Alarm Bulk Acknowledgment*



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:

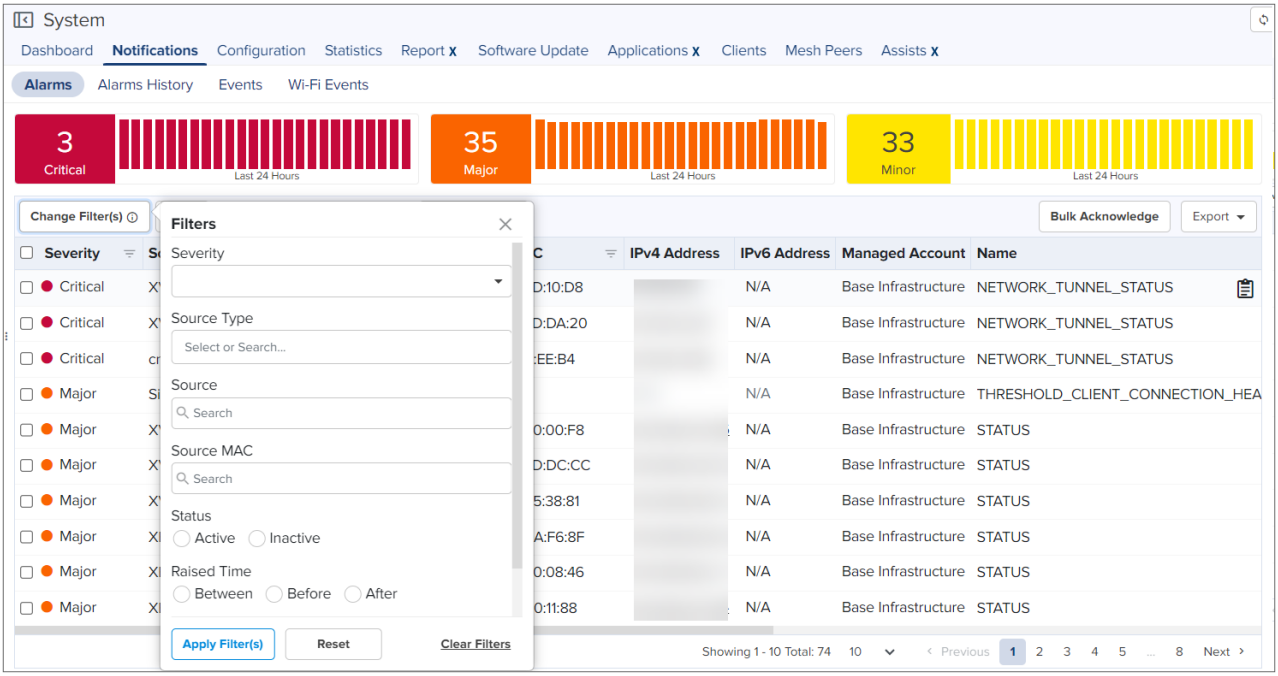


Alarm filters

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 86 *Alarms: New Filter*



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

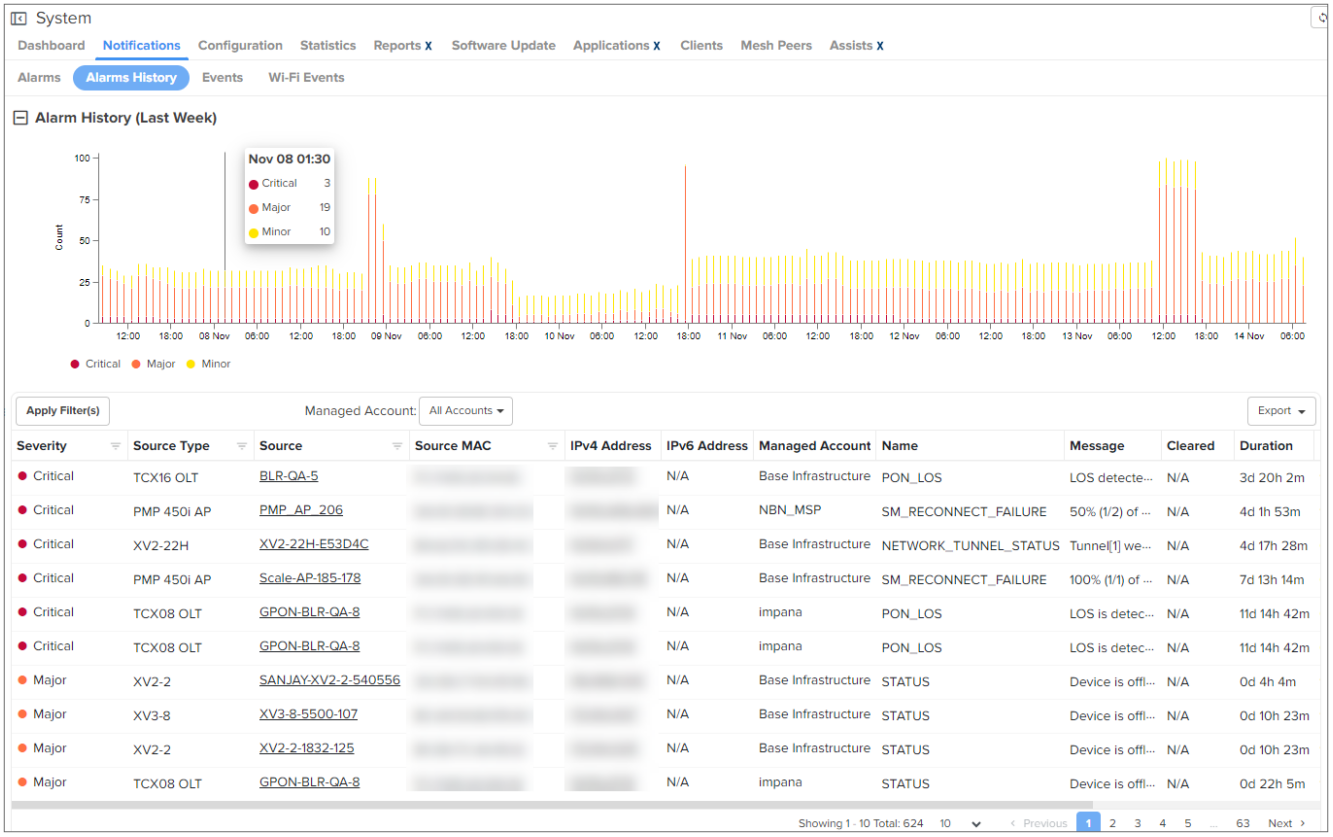
4. Click **Reset** to reset the filter option in the Alarms filter.
5. Click **Clear Filters** to clear all the filter options.

   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 87 *Alarm History*

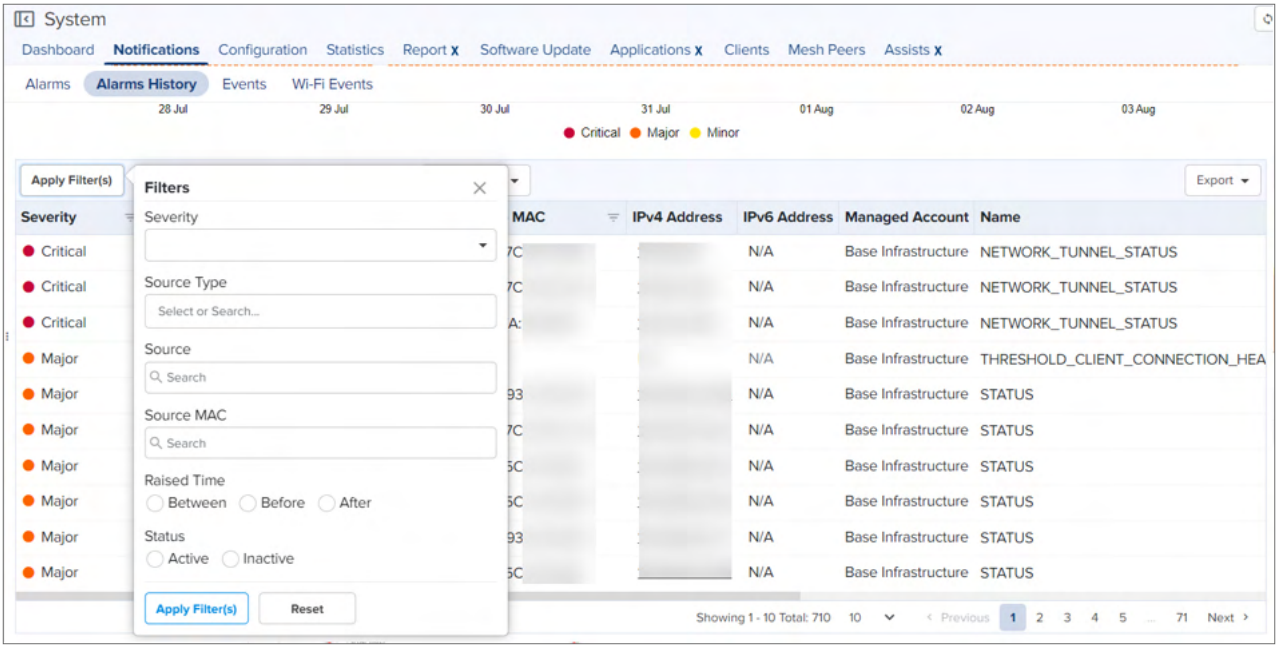


Alarm History filters

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 88 *Alarm History: New Filter*



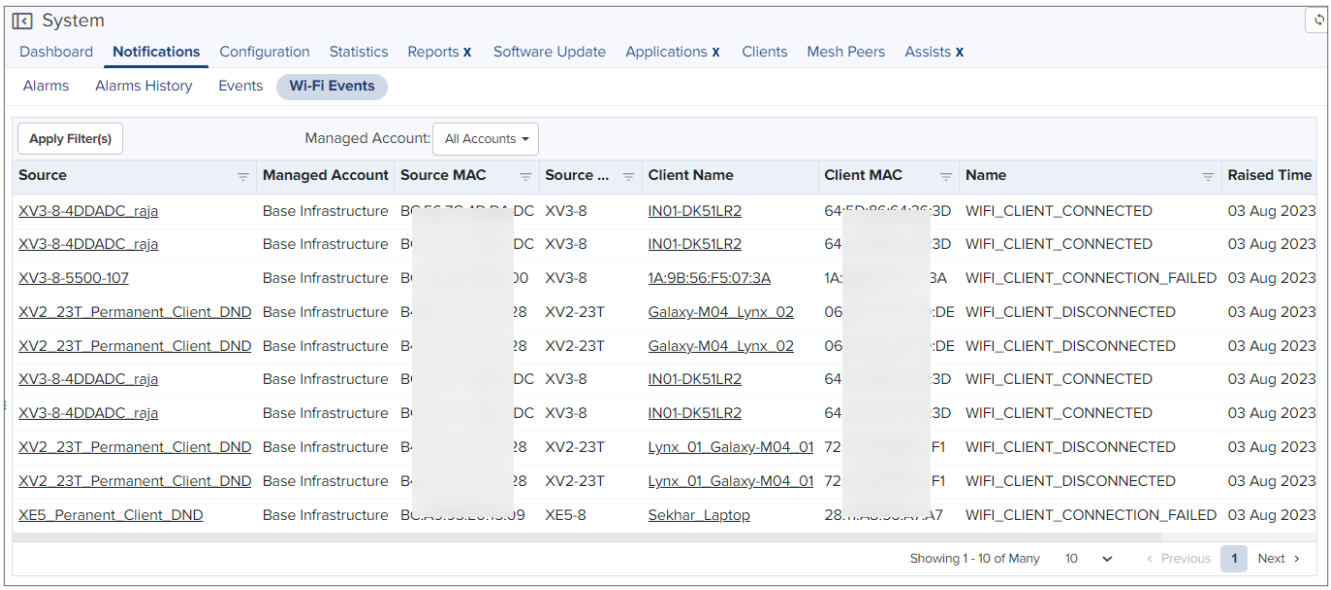
You can manually filter or search by typing parameters in the column header of the Alarm History table.

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:



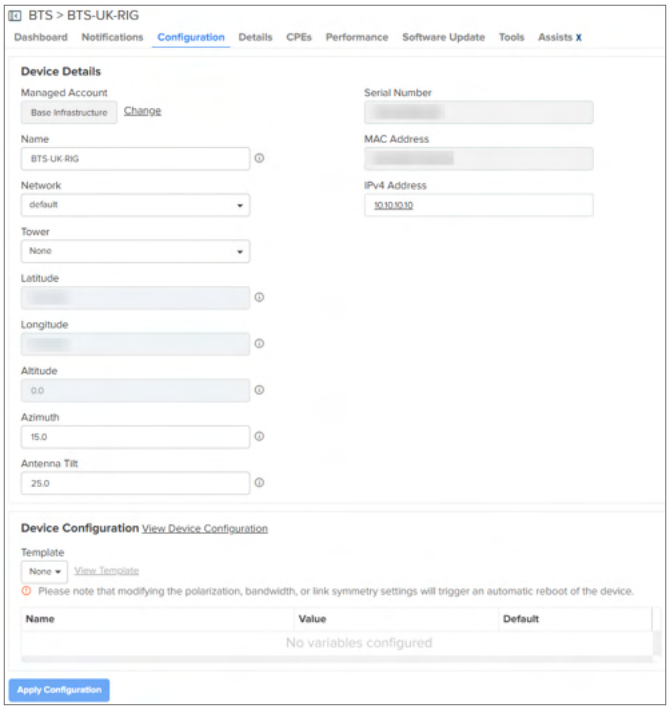
Configuration

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 89 is an example of the **Configuration** page for the cnWave 5G Fixed BTS product.

Figure 89 *The Configuration page - BTS*



You can also view the device configuration and backup the configuration.

Figure 90 *The Configuration page - View device configuration*

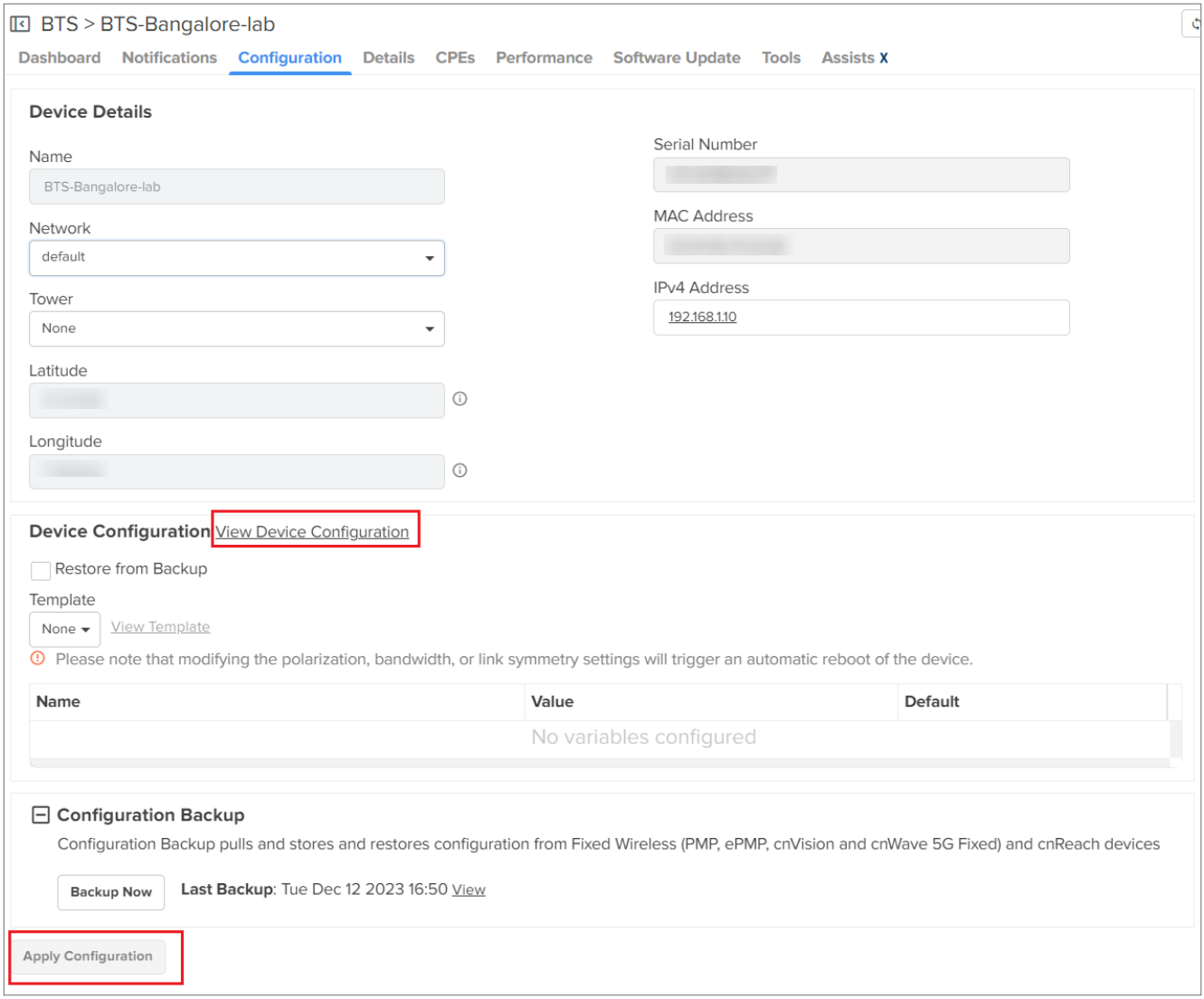


Table 33 lists and describes parameters available on the **Configuration** page for the cnWave 5G Fixed products (BTS and CPE).

Table 33 *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.

Table 33 *List of parameters on the Configuration page*

Parameter	Description
	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). 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.	
Restore from backup	An option to restore the device configuration from the backup. Select the checkbox if you want to restore the device configuration from the backup.
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.
Configuration backup	An option to back up the new configuration details and view the last backup information. Click **Backup Now** to store the new device configuration details.
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 34 *Device Statistics*

Device Type	Statistics Page Information
60 GHz cnWave Nodes	**General** • Device • IPv6 Address • MAC • Mode • Model • PoP Node • Serial Number • Site • Software Version • Status • Status Time • Network • Zone **GPS** • Fix Type • Height • Latitude • Longitude • Satellites Tracked • Sync Mode **Network** • Ethernet Throughput (Rx) • Ethernet Throughput (Tx) • Main Aux SFP • Radios • Sector Throughput (Rx) • Sector Throughput (Tx)
cnMatrix	**General** • Device Name

Table 34 *Device Statistics*

Device Type	Statistics Page Information
	• IPv4 Address • IPv6 Address • MAC Address • Network • Product Name • Serial Number • Status • Tower/Site • Uptime **Traffic** • Throughput (DL) • Throughput (Rx)
cnPilot Home	**General** • AP Group • Device Name • IPv4 Address • IPv6 Address • MAC Address • Mesh Type • Network • Product Name • Serial Number • Status • Tower/Site • Uptime **Wireless** • Radios
cnRanger BBU	**General** • Device Name • IPv4 Address • IPv6 Address • MAC Address • Network • Registered SM Count

Table 34 *Device Statistics*

Device Type	Statistics Page Information
	• Serial Number • Status • Tower/Site • Uptime **Wireless** • Radios
cnRanger SM	**General** • Device Name • IPv4 Address • IPv6 Address • MAC Address • Network • Serial Number • Status • Tower/Site • Uptime **Wireless** • Radios
cnReach	**General** • Device • IPv4 Address • IPv6 Address • MAC • Network • Radio • Status • Tower/Site
cnReach XIO	**General** • Active S/W Version • Device • IPv4 Address • IPv6 Address • MAC • Network

Table 34 *Device Statistics*

Device Type	Statistics Page Information
	• Product Name • Serial Number • Status • Tower/Site
cnVision Client	**General** • Device Name • Distance • IPv4 Address • IPv6 Address • MAC Address • Network • Serial Number • Session Time • Status • Tower/Site • Uptime **Network** • LAN Interface • LAN Interface 2 • WAN IP Address **Wireless** • Antenna Gain • Connected AP • Radios
cnVision Hub	**General** • Device Name • IPv4 Address • IPv6 Address • MAC Address • Network • Registered SM Count • Serial Number • Status • Tower/Site

Table 34 *Device Statistics*

Device Type	Statistics Page Information
	• Uptime **Network** • LAN Interface • LAN Interface 2 **Wireless** • Antenna Gain • DL/UL Ratio • Max Range • Radios
cnWave 5G Fixed BTS	**General** • Device Name • MAC • IPv4 Address • Network • Status • Tower/Site **Radio Details**: Radio status of the BTS device • 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	**General** • Device Name • CRNTI • IMSI • IPv4 Address

Table 34 *Device Statistics*

Device Type	Statistics Page Information
	• Link Uptime • MAC • Network • Registration Count • Registration State • Status • Tower/Site **Radio Details** • Alignment Active • Current EIRP (dBm) • DL Backoff (dB) • DL Channel Distortion (dB) • DL EVM (dB) • DL MCS • DL Rx Power (dBm) • DL Sounding State • DL Spatial Frequency • 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	**General** • AP Group • Device Name • IPv4 Address • IPv6 Address • MAC Address • Mesh Type • Network • Port Speed

Table 34 *Device Statistics*

Device Type	Statistics Page Information
	• Product Name • Serial Number • Status • Tower/Site • Uptime **Wireless** • Radios
ePMP AP	**General** • Device Name • IPv4 Address • IPv6 Address • MAC Address • Network • Registered SM Count • Serial Number • Status • Tower/Site • Uptime **Network** • LAN Interface • LAN Interface 2 **Wireless** • Antenna Gain • DL/UL Ratio • Max Range • Radios
ePMP SM	**General** • Device Name • Distance • IPv4 Address • IPv6 Address • MAC Address • Network

Table 34 *Device Statistics*

Device Type	Statistics Page Information
	• Serial Number • Session Time • Status • Tower/Site • Uptime **Network** • LAN Interface • LAN Interface 2 • WAN IP Address **Wireless** • Antenna Gain • Connected AP • Radios
PMP AP	**General** • Device Name • IPv4 Address • IPv6 Address • MAC Address • Network • Registered SM Count • Serial Number • Status • Tower/Site • Uptime **Network** • LAN Interface **Traffic** • Busy Index (DL) • Busy Index (UL) **Wireless** • Antenna Gain • Color Code • DL/UL Ratio

Table 34 *Device Statistics*

Device Type	Statistics Page Information
	• Max Range • Radios
PMP SM	**General** • Device Name • Distance • DFS Status • IPv4 Address • IPv6 Address • MAC Address • Network • Serial Number • Session Time • Status • Tower/Site • Uptime **Network** • LAN Interface • WAN IP Address **Wireless** • Actual Average EVM (DL) • Actual Average EVM (UL) • Antenna Gain • BER (Average) • Color Code • Connected AP • LUID • Radios
PTP 650/670/700	**System** • Device Name • IPv4 Address • IPv6 Address • MAC Address • Network • Product Name

Table 34 *Device Statistics*

Device Type	Statistics Page Information
	• Status • Tower/Site • Uptime **Network** • Aux Interface • Main PSU Interface • SFP Interface **Wireless** • Antenna Gain • Errored Seconds • Licensed Country • Radios • Severely Errored Seconds • Unavailable Seconds
PTP 820/850	**General** • Device Name • Edge Controller • IPv4 Address • IPv6 Address • MAC Address • Model • Network • Radios • Serial Number • Status • Tower/Site

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

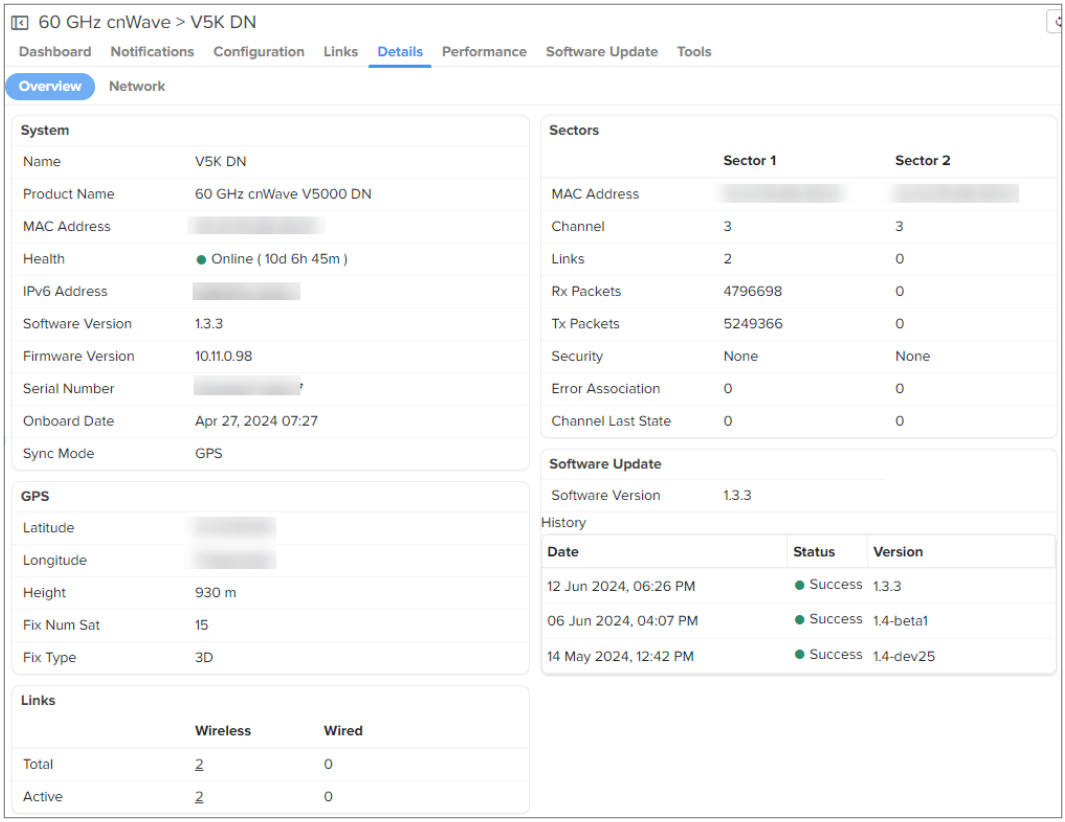
60 GHz cnWave

The **Details** section displays following tabs for 60 GHz cnWave:

- Overview
- Network Info

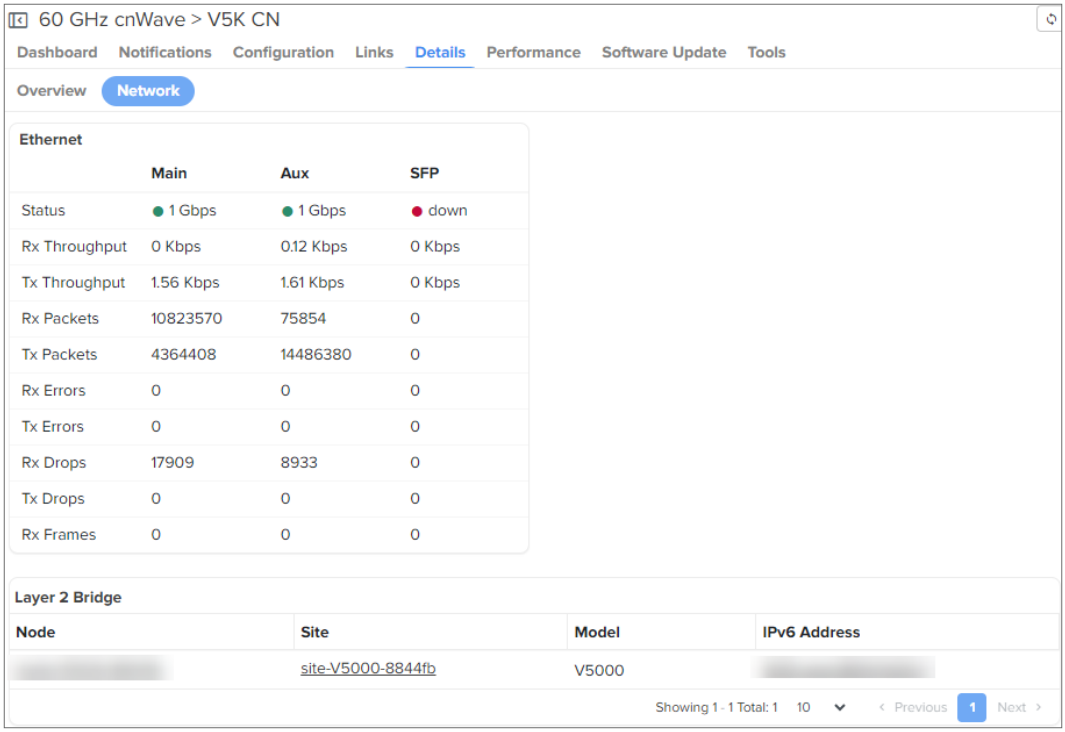
Overview

Figure 91 *60 GHz cnWave: Device > Details > Overview*



Network Info

Figure 92 *60 GHz cnWave: Device > Details > Network Info*



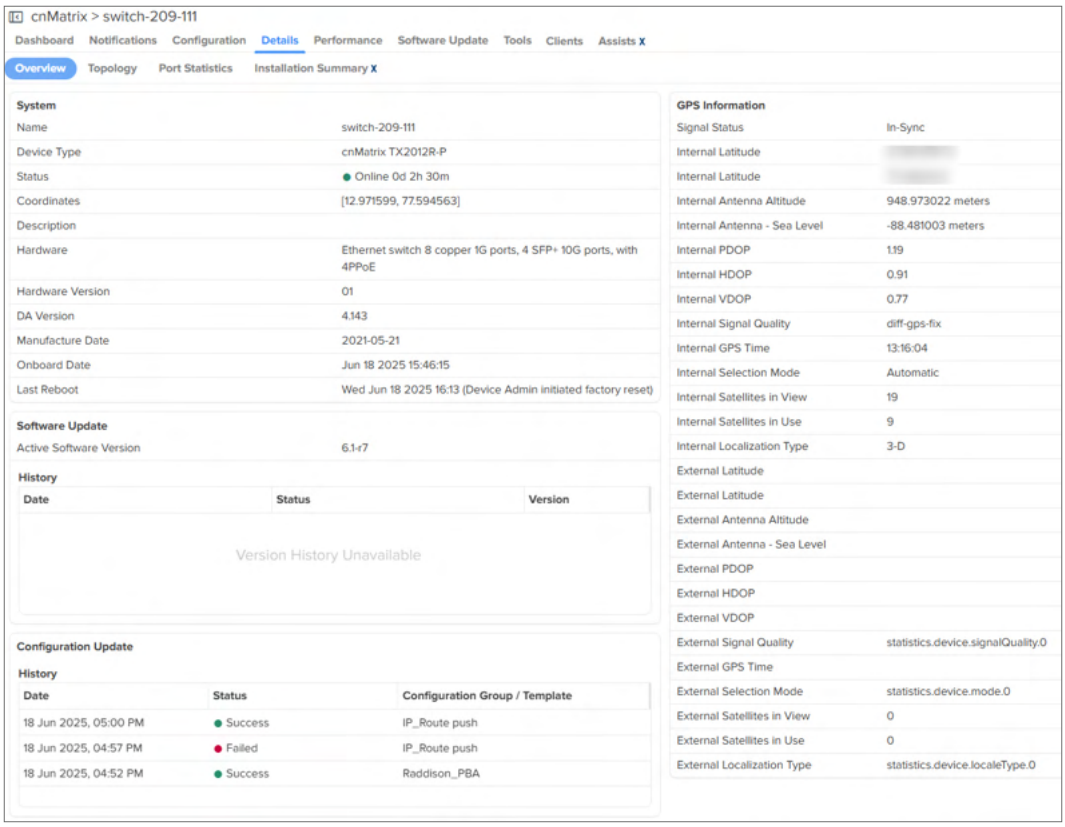
cnMatrix

The **Details** section displays following tabs for cnMatrix:

- Overview
- Topology
- Port Statistics
- Installation Summary **X**

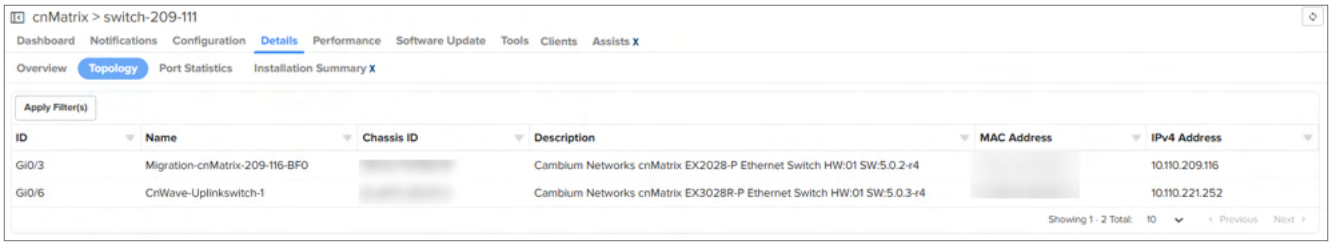
Overview

Figure 93 *cnMatrix: Device > Details > Overview*



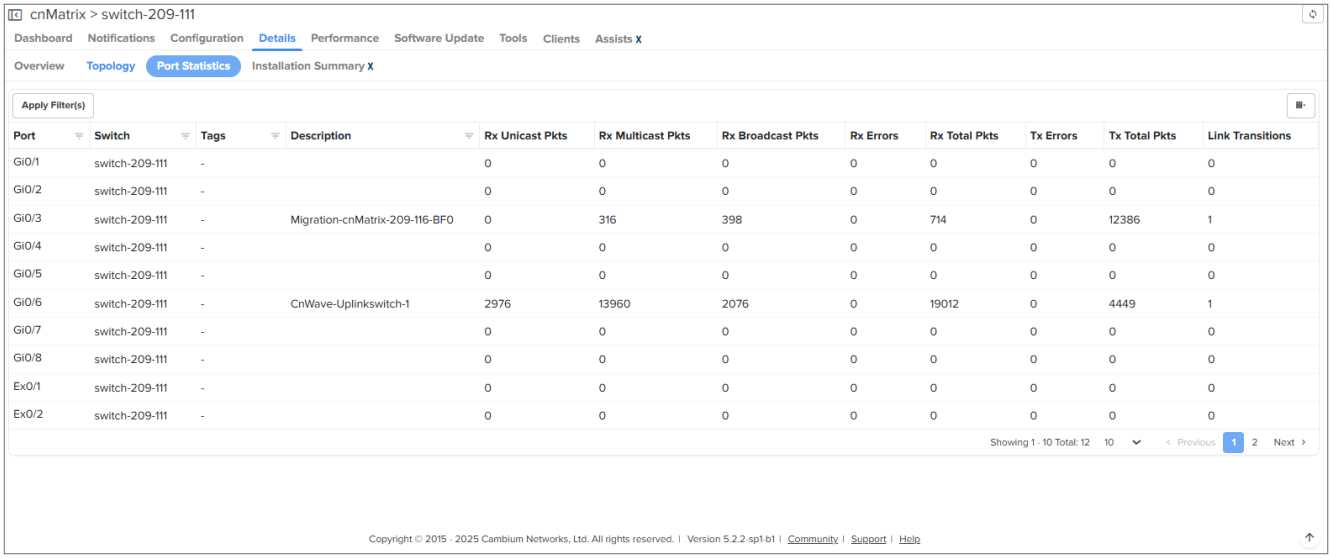
Topology

Figure 94 *cnMatrix: Device > Details > Topology*



Port Statistics

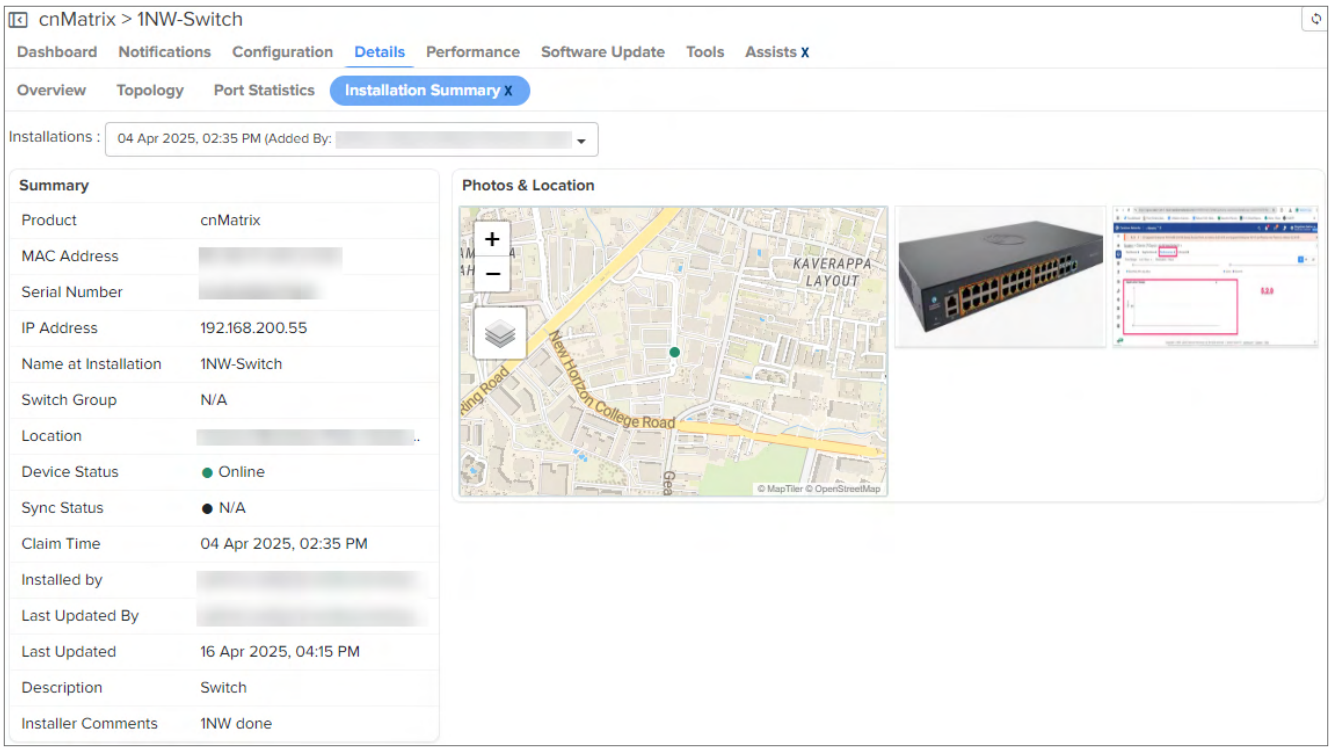
Figure 95 *cnMatrix: Device > Details > Port Statistics*



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	switch-209-111	-		0	0	0	0	0	0	0	0
Gi0/2	switch-209-111	-		0	0	0	0	0	0	0	0
Gi0/3	switch-209-111	-	Migration-cnMatrix-209-116-BF0	0	316	398	0	714	0	12386	1
Gi0/4	switch-209-111	-		0	0	0	0	0	0	0	0
Gi0/5	switch-209-111	-		0	0	0	0	0	0	0	0
Gi0/6	switch-209-111	-	CnWave-Uplinkswitch-1	2976	13960	2076	0	19012	0	4449	1
Gi0/7	switch-209-111	-		0	0	0	0	0	0	0	0
Gi0/8	switch-209-111	-		0	0	0	0	0	0	0	0
Ex0/1	switch-209-111	-		0	0	0	0	0	0	0	0
Ex0/2	switch-209-111	-		0	0	0	0	0	0	0	0

Installation Summary

Figure 96 *cnMatrix: Device > Details > Installation Summary*



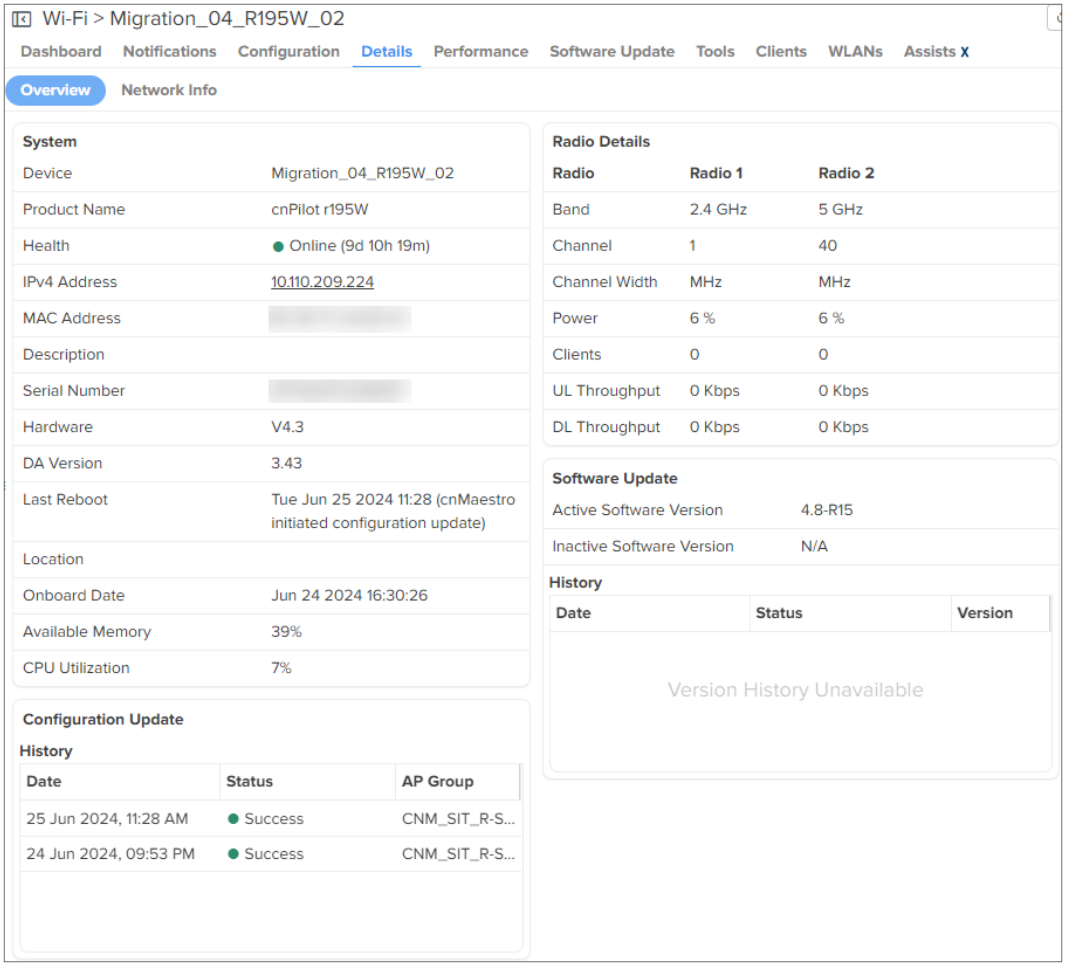
cnPilot Home

The **Details** section displays following tabs for cnPilot Home:

- Overview
- Network Info

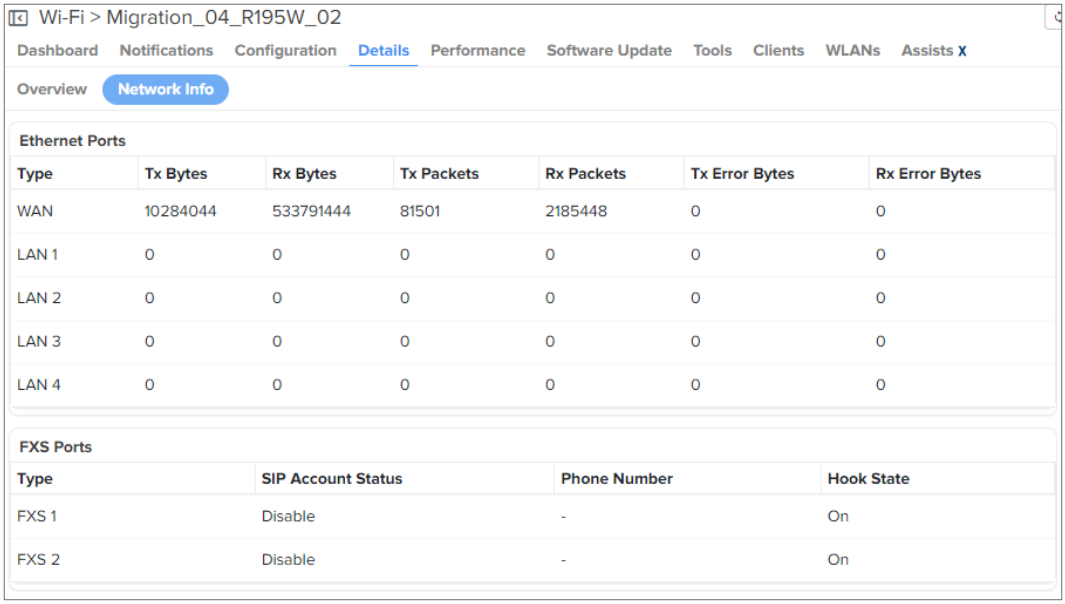
Overview

Figure 97 *cnPilot Home: Device > Details > Overview*



Network Info

Figure 98 *cnPilot Home: Device > Details > Network Info*



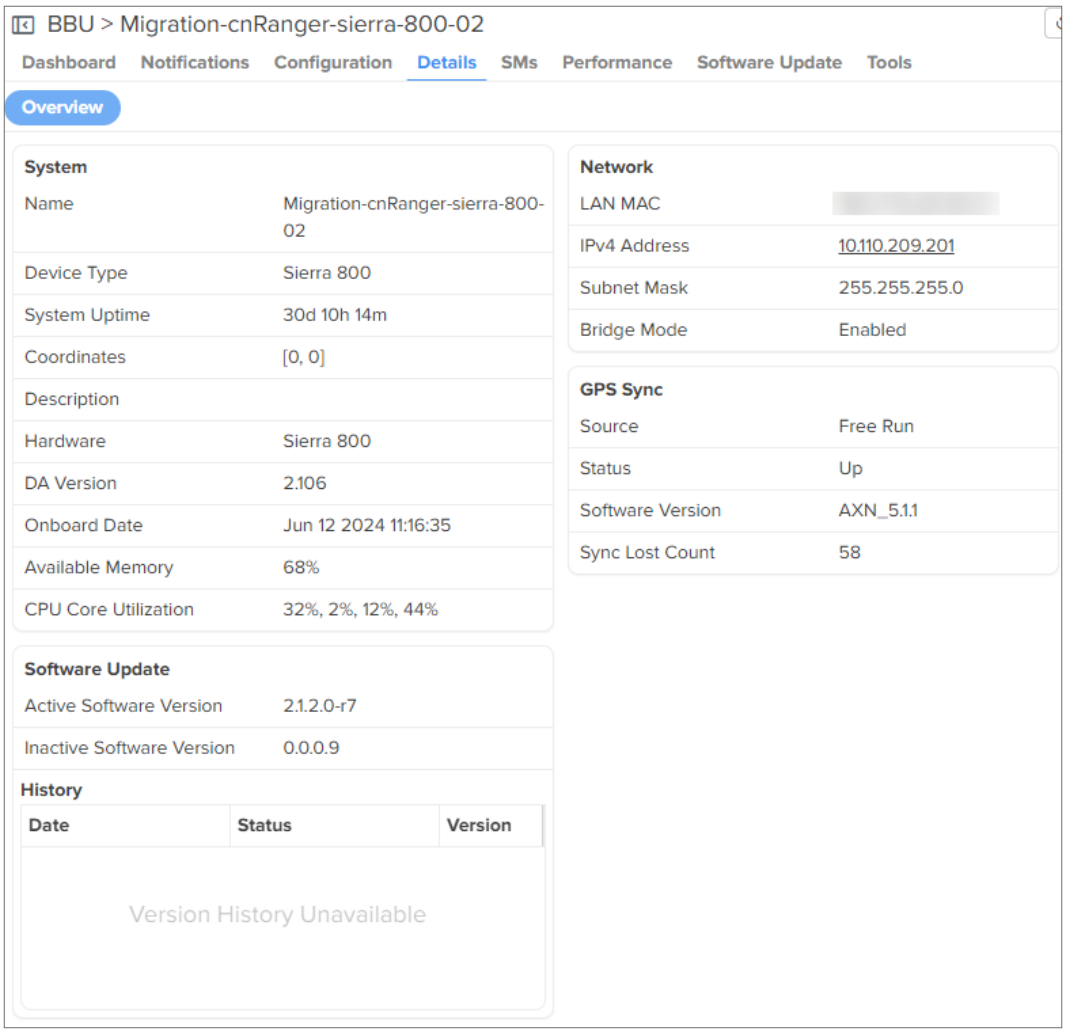
cnRanger BBU

The **Details** section displays following tabs for cnRanger BBU:

- Overview

Overview

Figure 99 *cnRanger BBU: Device > Details > Overview*



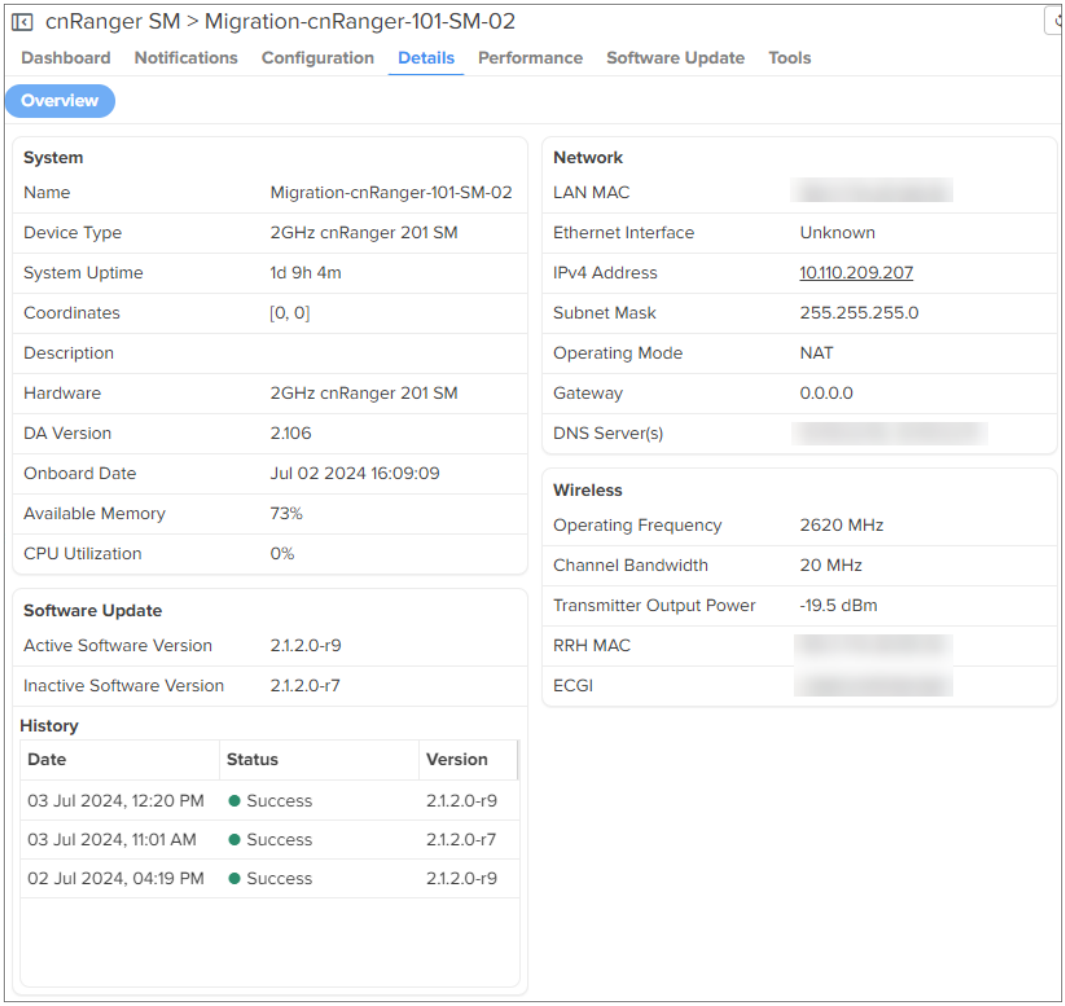
cnRanger SM

The **Details** section displays following tabs for cnRanger SM:

- Overview

Overview

Figure 100 *cnRanger SM: Device > Details > Overview*



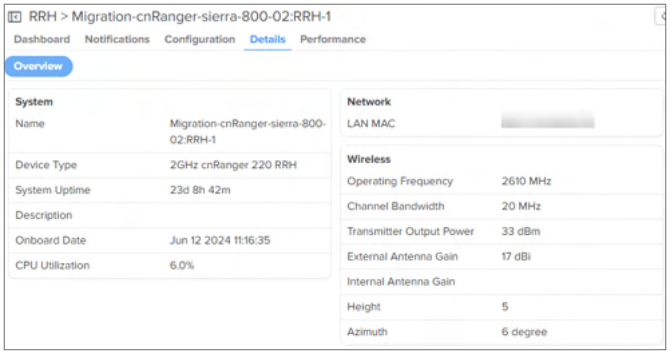
cnRanger RRH

The **Details** section displays following tabs for cnRanger RRH:

- Overview

Overview

Figure 101 *cnRanger RRH: Device > Details > Overview*



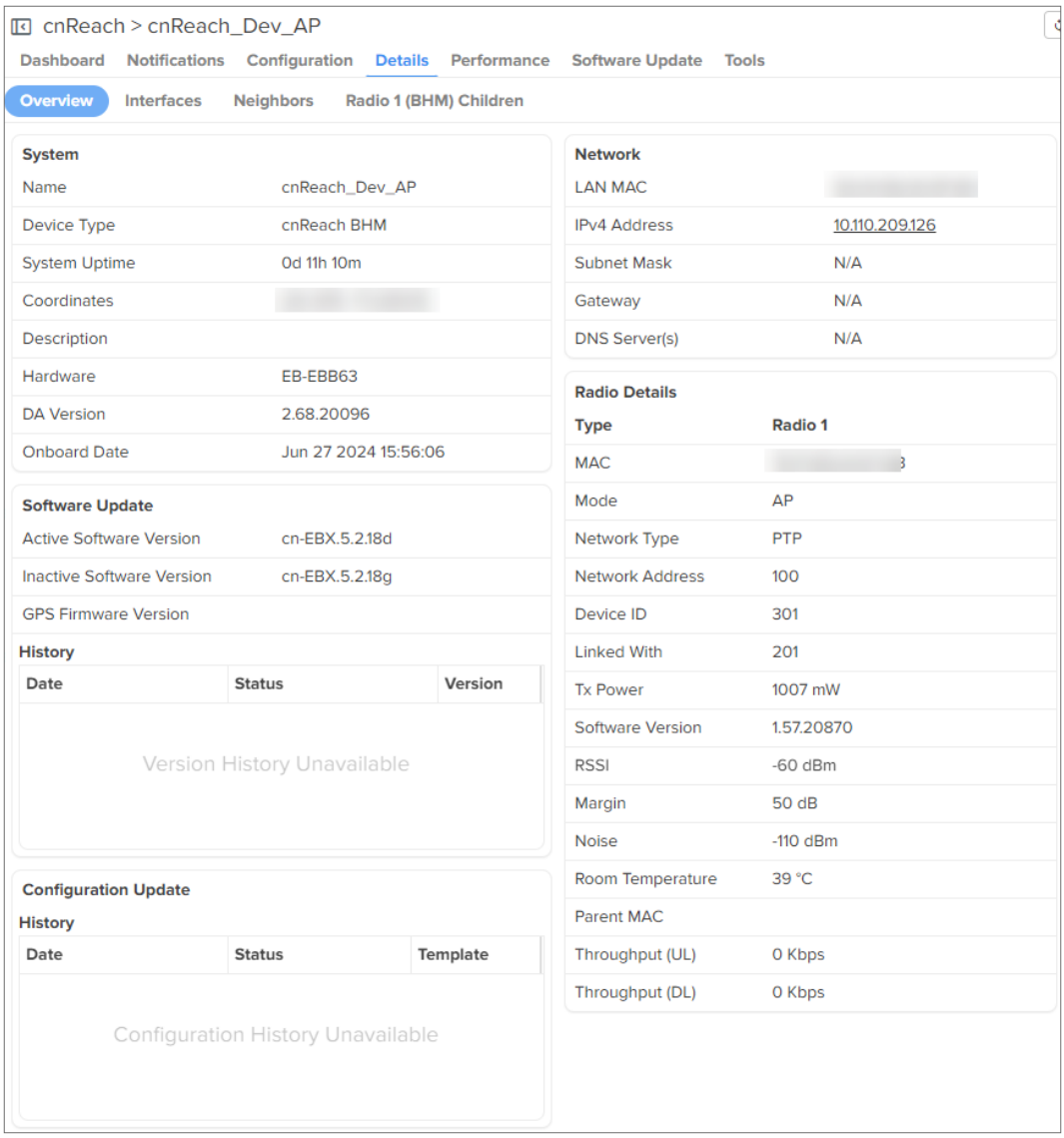
cnReach

The **Details** section displays following tabs for cnReach:

- Overview
- Interfaces
- Neighbors
- Radio 1 (BHM) Children

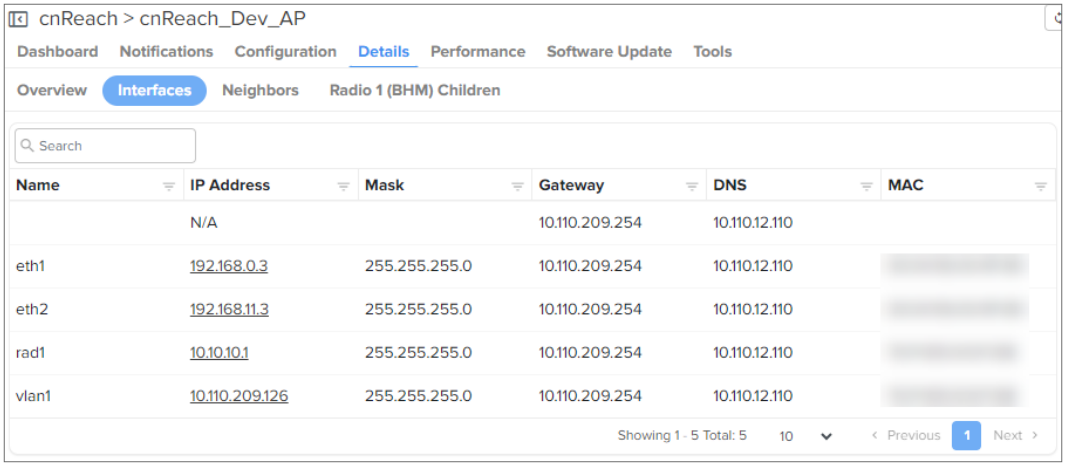
Overview

Figure 102 *cnReach: Device > Details > Overview*



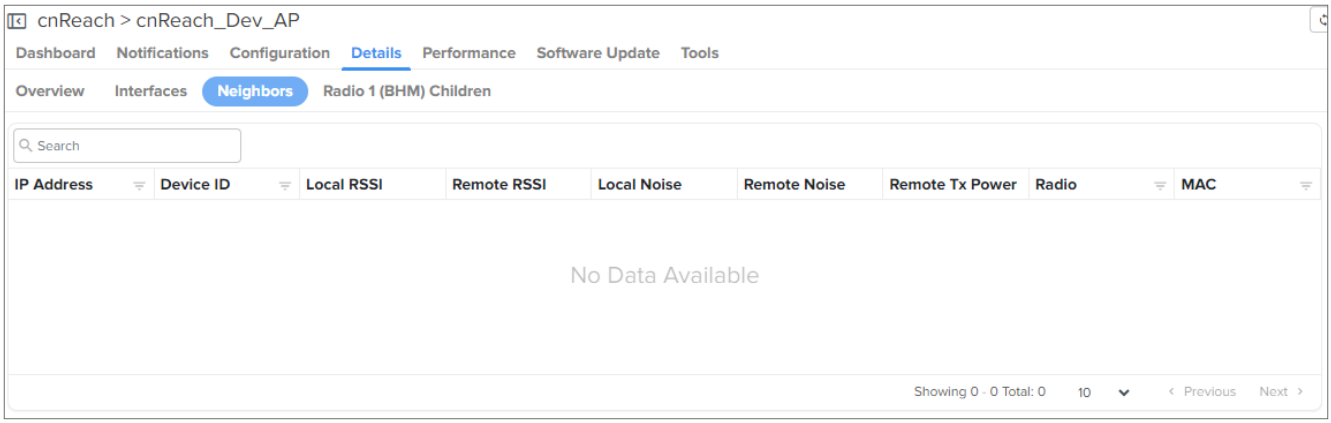
Interfaces

Figure 103 *cnReach: Device > Details > Interfaces*



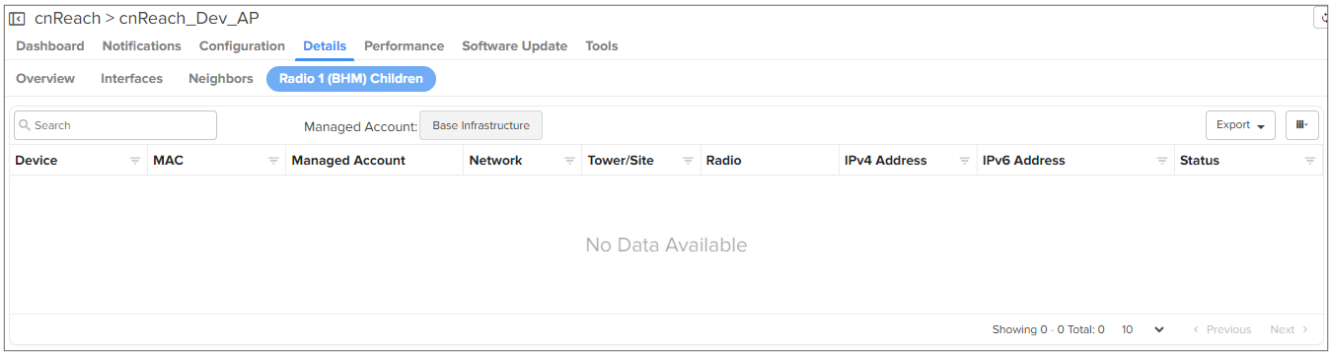
Neighbors

Figure 104 *cnReach: Device > Details > Neighbors*



Radio 1 (BHM) Children

Figure 105 *cnReach: Device > Details > Radio 1 (BHM) Children*



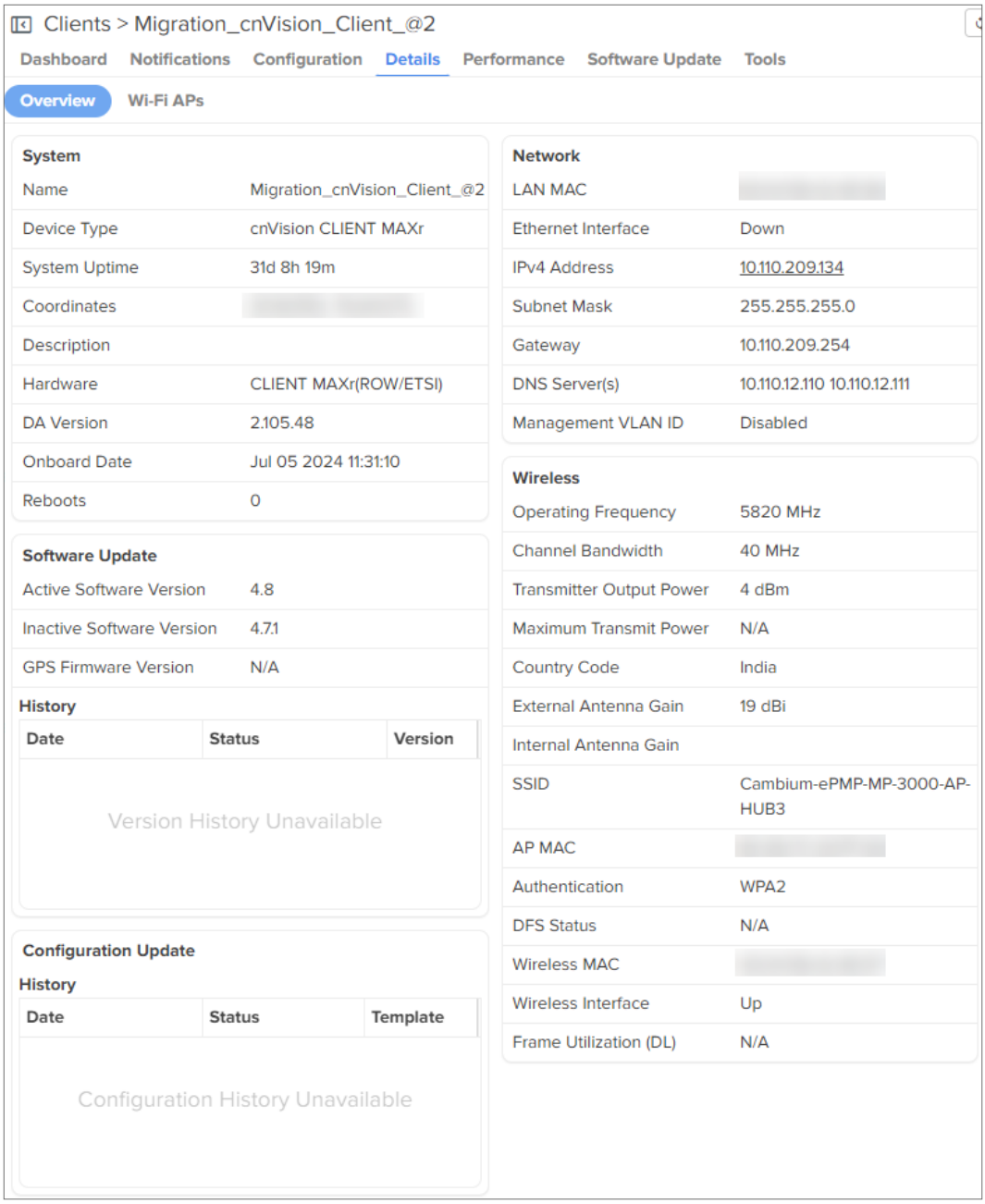
cnVision Client

The **Details** section displays following tabs for cnVision Client:

- Overview
- Wi-Fi APs

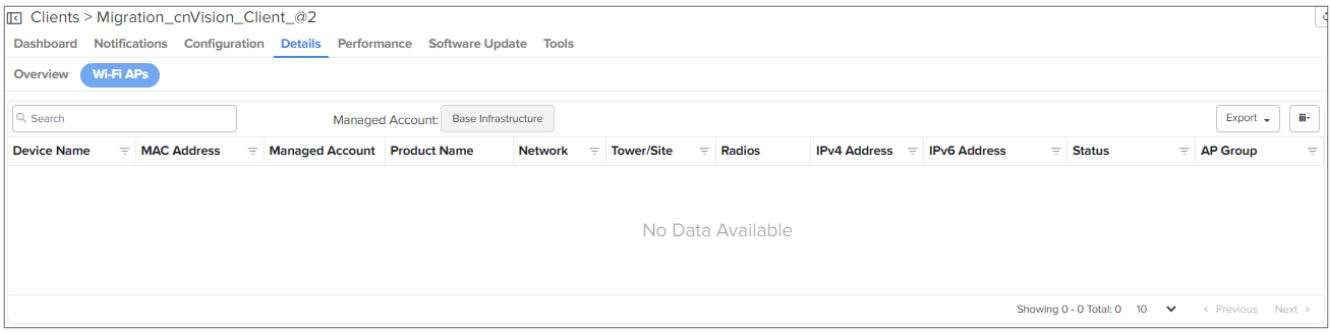
Overview

Figure 106 *cnVision Client: Device > Details > Overview*



Wi-Fi 5APs

Figure 107 *cnVision Client: Device > Details > Wi-Fi APs*



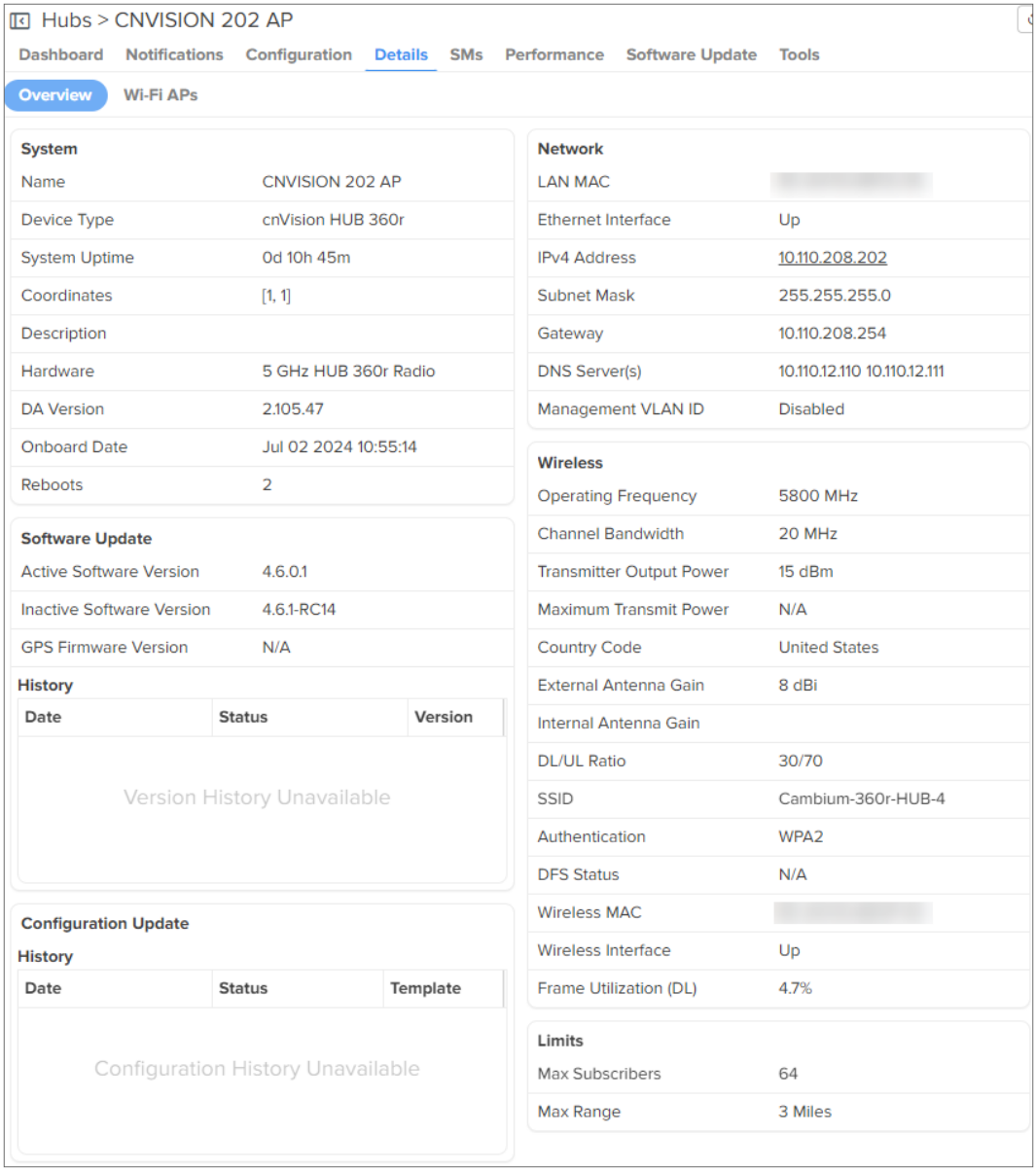
cnVision Hub

The **Details** section displays following tabs for cnVision Hub:

- Overview
- Wi-Fi APs

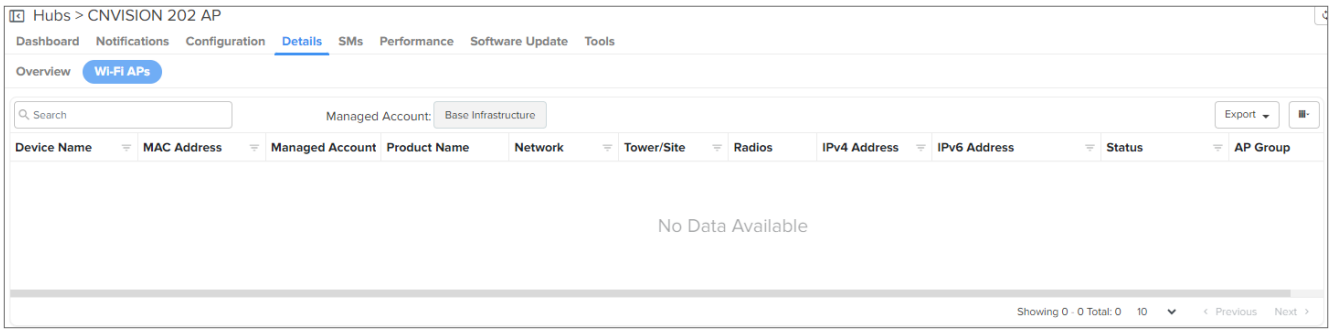
Overview

Figure 108 *cnVision Hub: Device > Details > Overview*



Wi-Fi APs

Figure 109 *cnVision Hub: Device > Details > Wi-Fi APs*



cnWave 5G Fixed Details

cnWave 5G Fixed BTS

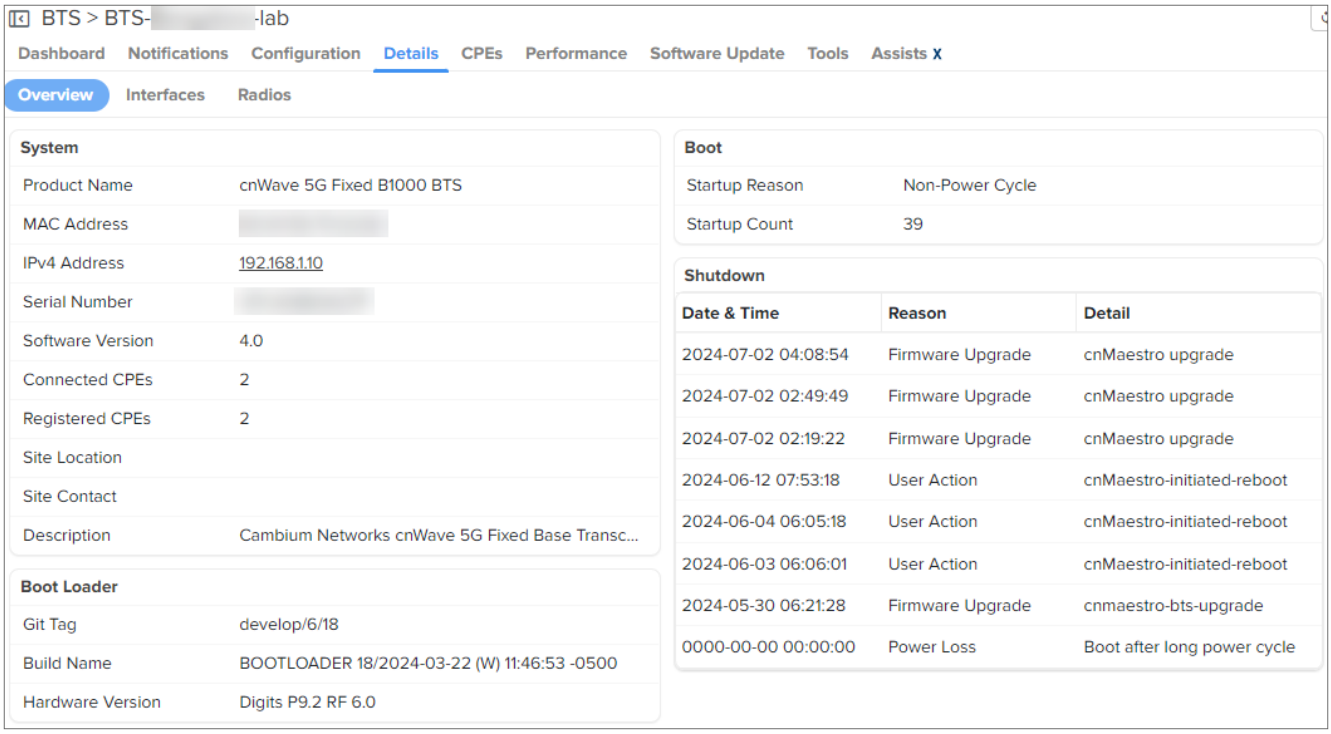
The **Details** > **Overview** section displays following tabs for cnWave 5G Fixed BTS device:

- Overview
- Interfaces
- Radios

Overview

Overview page provides the information such as Details, Boot Loader, Boot, and Shutdown.

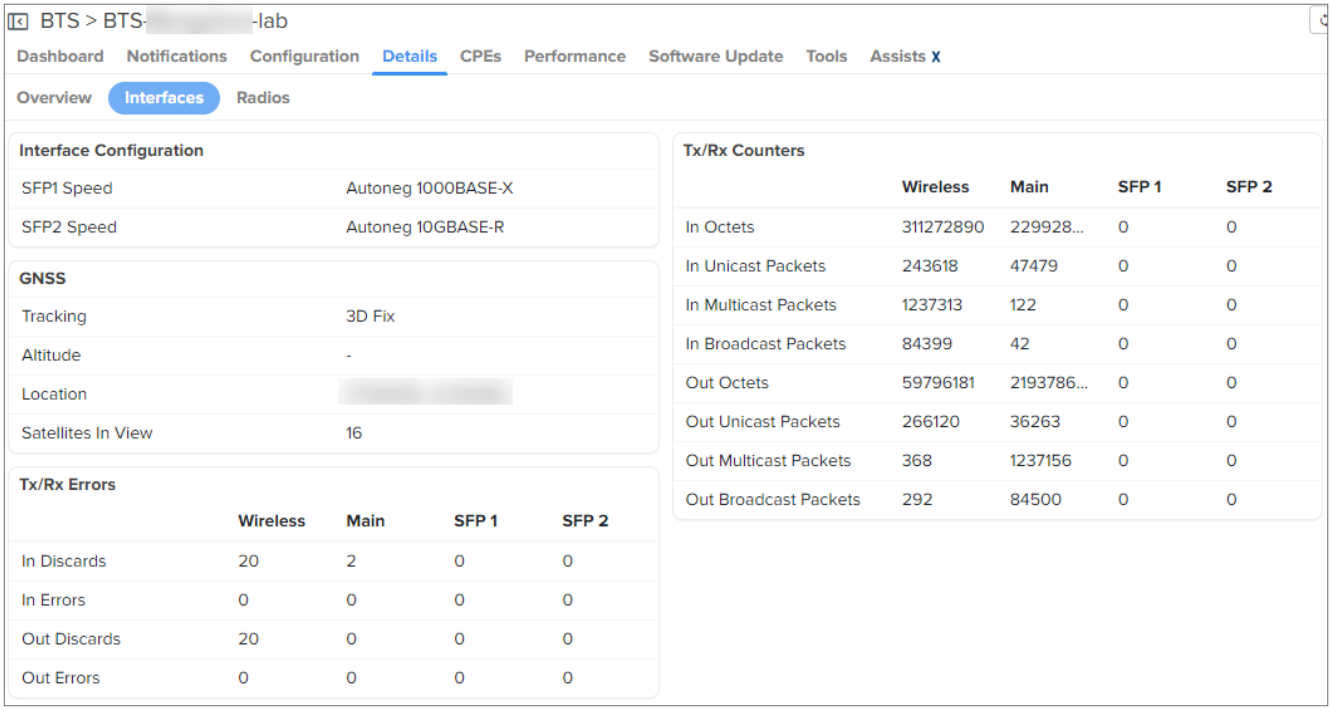
Figure 110 *cnWave 5G Fixed: Device > Details > Overview*



Interfaces

Interface page provides the information such as Interface Configuration, GNSS, Tx/Rx Errors, and Tx/Rx Counters.

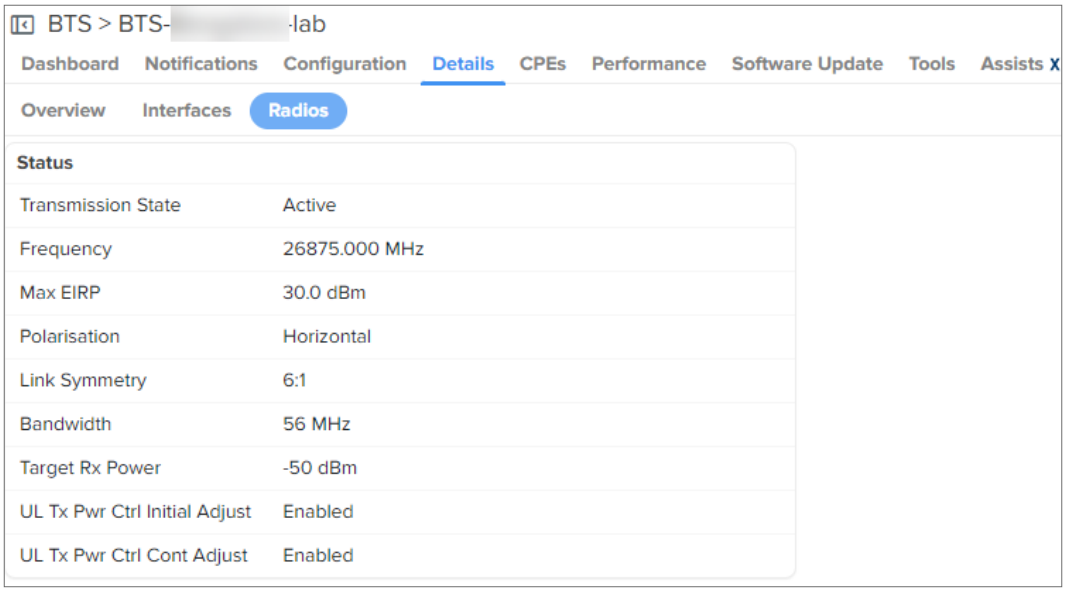
Figure 111 *cnWave 5G Fixed BTS: Device > Details > Interfaces*



Radios

Radios page provide the details of radios.

Figure 112 *cnWave 5G Fixed BTS: Device > Details > Radios*



cnWave 5G Fixed CPE

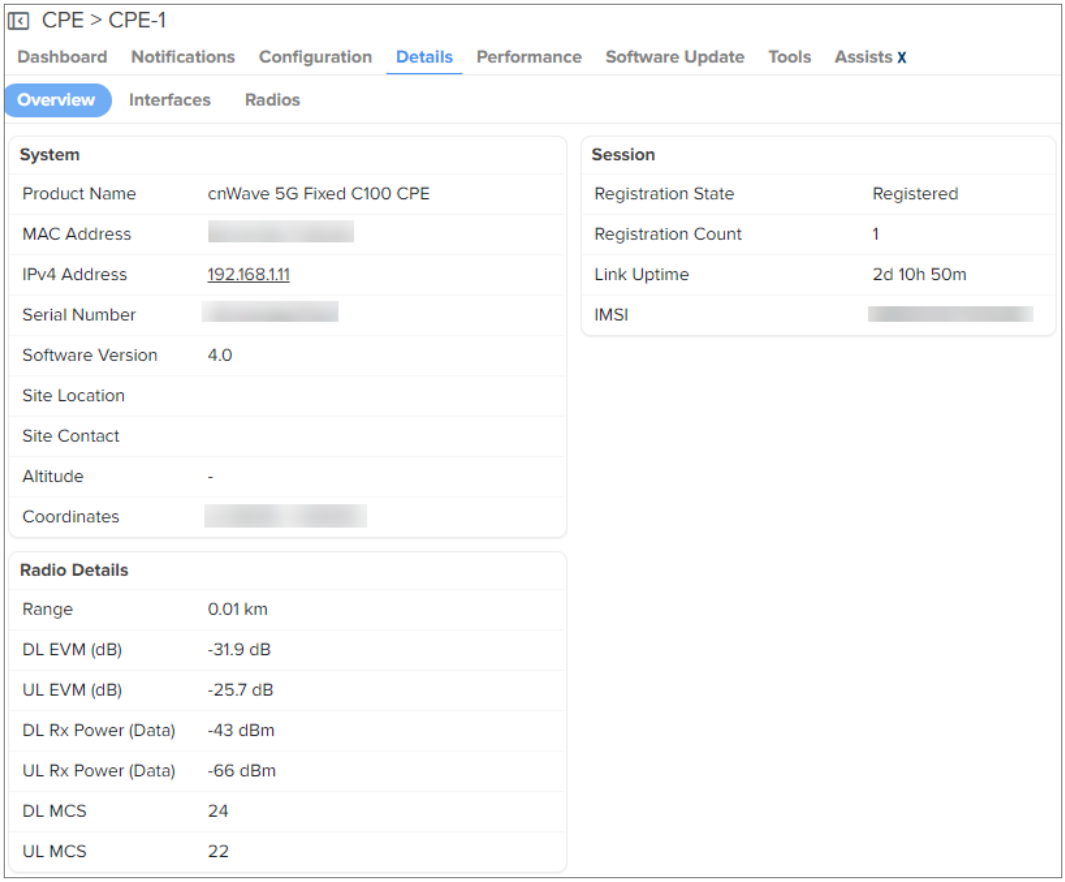
The **Details** section displays following pages for cnWave 5G Fixed CPE device:

- Overview
- Interfaces
- Radios

Overview

Overview page provides the information such as Details, Radio Details, and Sessions.

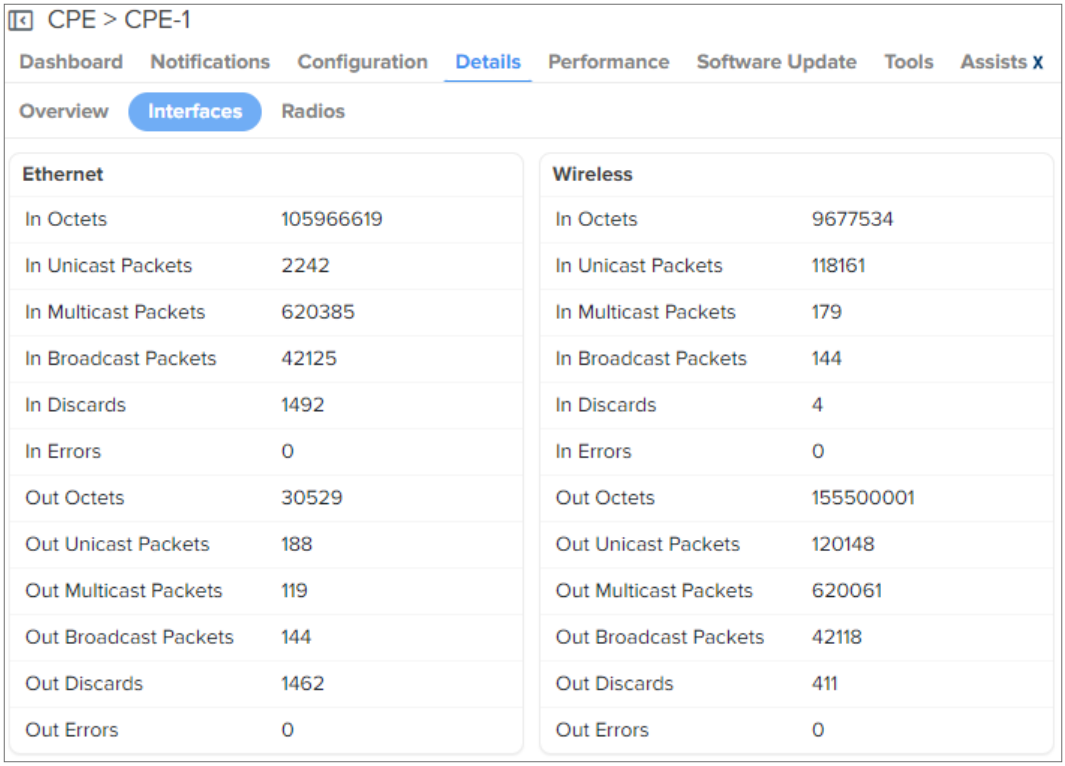
Figure 113 *cnWave 5G Fixed CPE: Device > Details > Overview*



Interfaces

Interface page provides the information such as Ethernet and Wireless.

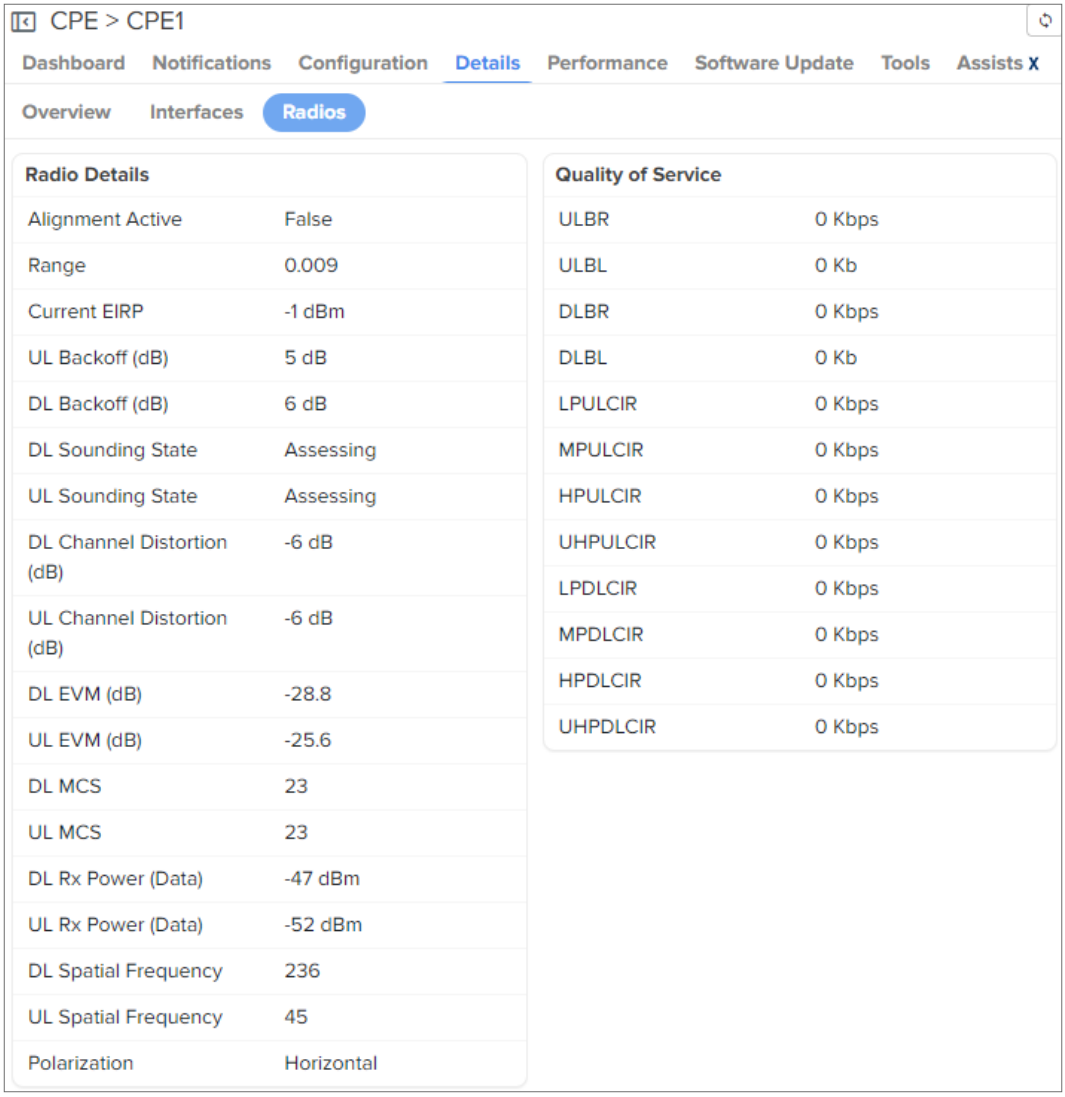
Figure 114 *cnWave 5G Fixed CPE: Device > Details > Interfaces*



Radios

Radios page provide the details of radio details.

Figure 115 *cnWave 5G Fixed CPE: Device > Details > Radios*



Enterprise Wi-Fi AP (XE-, XV-, and X7-Series)

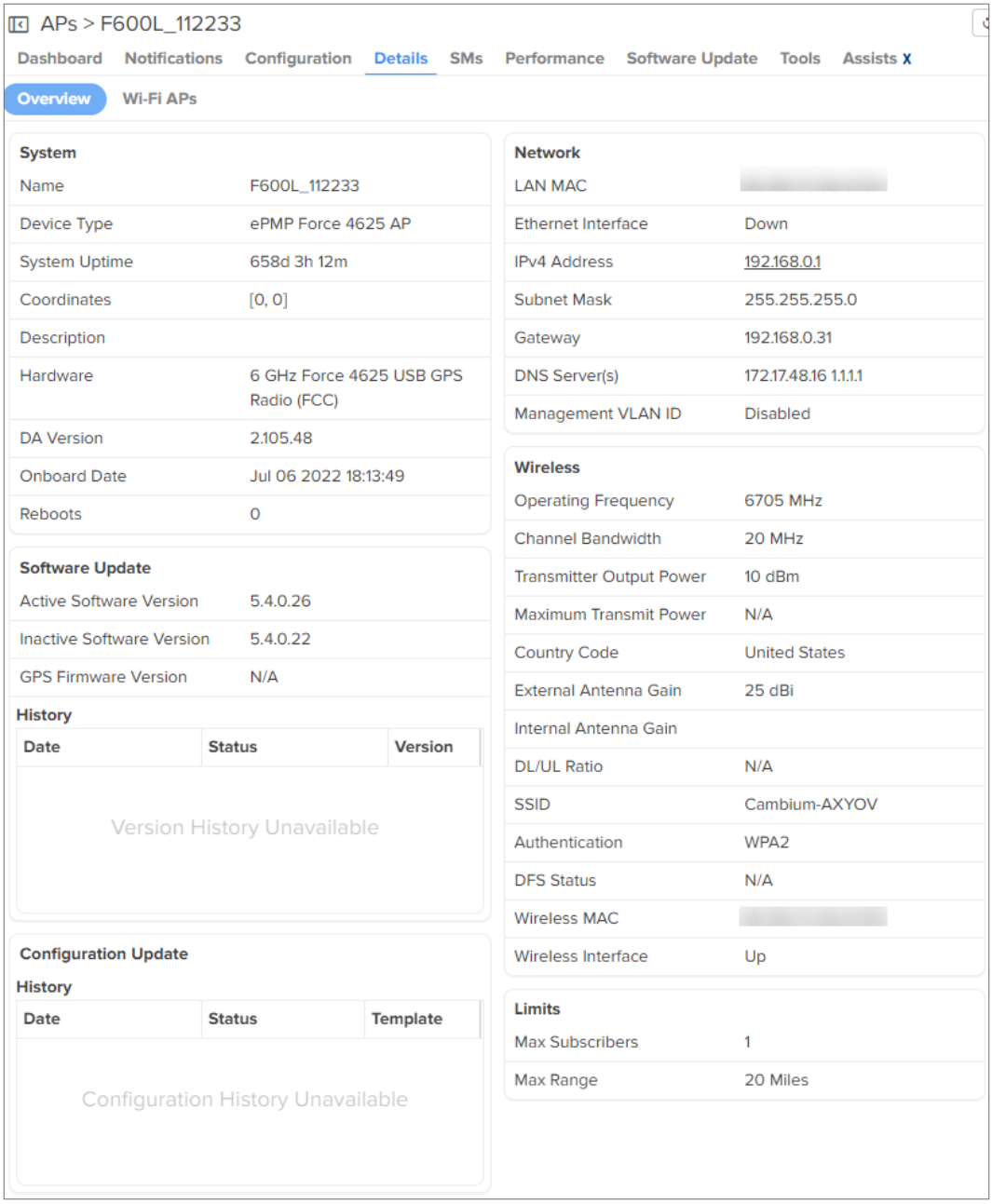
ePMP AP

The **Details** section displays following tabs for ePMP APs:

- Overview
- Wi-Fi APs

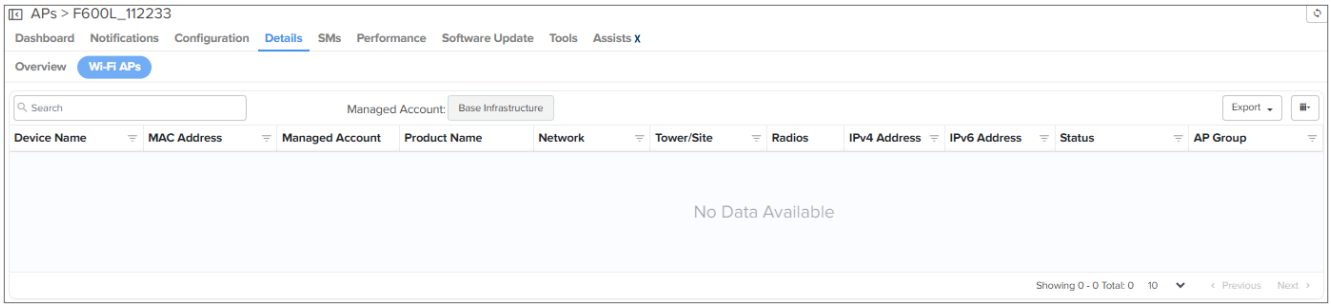
Overview

Figure 116 *ePMP AP: Device > Details > Overview*



Wi-Fi APs

Figure 117 *ePMP AP: Device > Details > Wi-Fi APs*



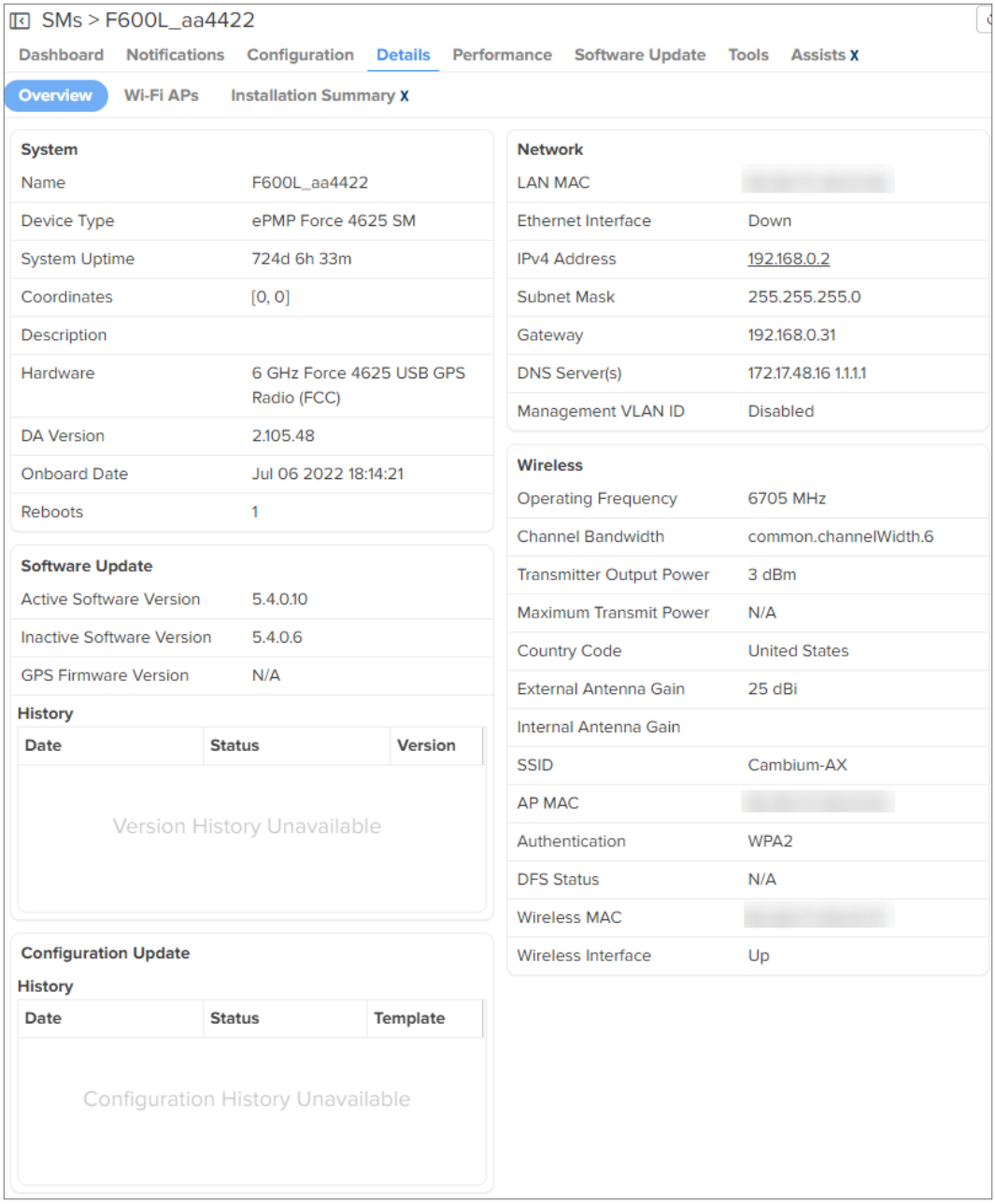
ePMP SM

The **Details** section displays following tabs for ePMP SMs:

- Overview
- Wi-Fi APs
- Installation Summary X

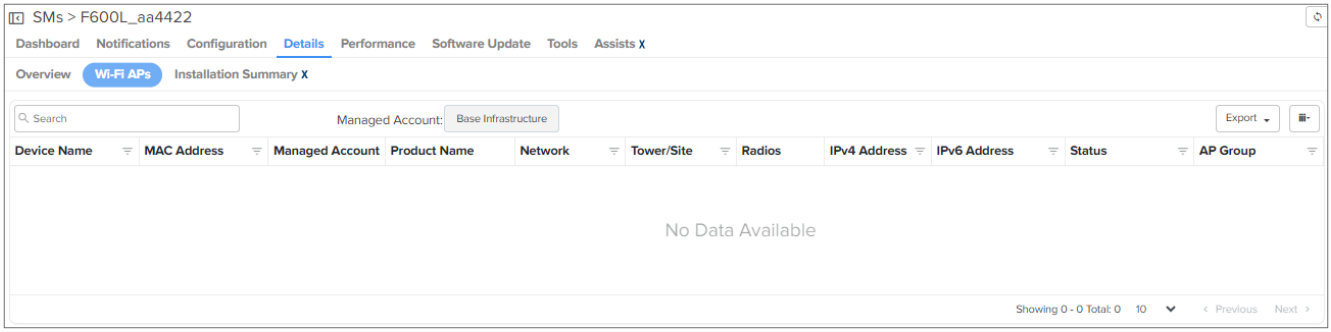
Overview

Figure 118 *ePMP SM: Device > Details > Overview*



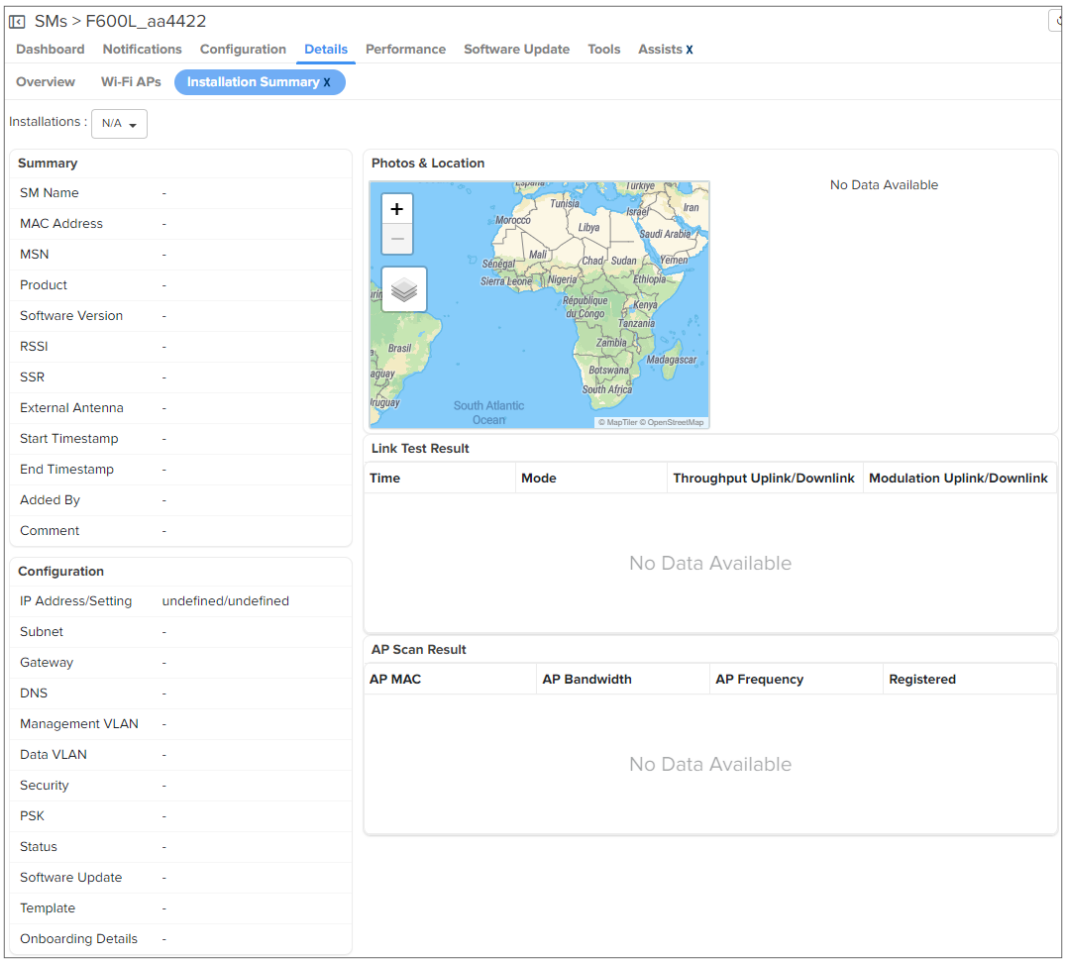
Wi-Fi APs

Figure 119 *ePMP SM: Device > Details > Wi-Fi APs*



Installation Summary X

Figure 120 *ePMP SM: Device > Details > Installation Summary* **X**



PMP AP

The **Details** section displays following tabs for PMP APs:

- Overview
- Wi-Fi APs

Overview

Figure 121 *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		

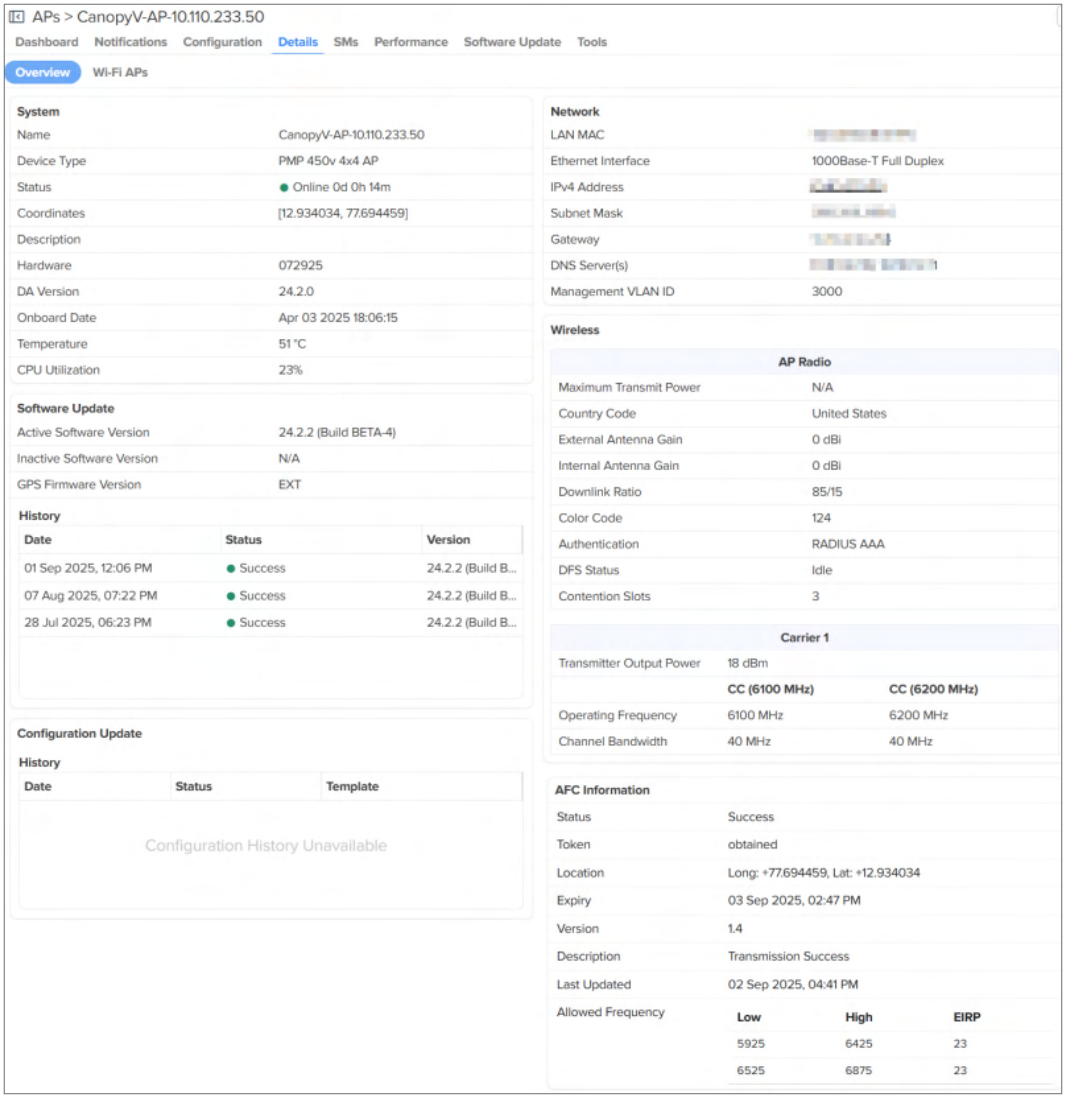
Network

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

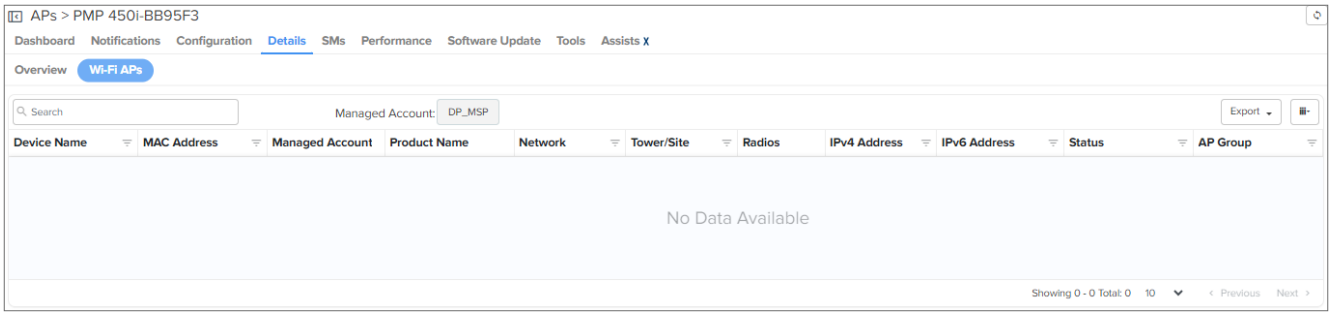
Operating Frequency	5735 MHz
Channel Bandwidth	20 MHz
Transmitter Output Power	17 dBm
Maximum Transmit Power	N/A
Country Code	FCC
External Antenna Gain	0 dBi
Internal Antenna Gain	0 dBi
Downlink Ratio	75/25
Color Code	222
Authentication	Disabled
DFS Status	Idle
Contention Slots	3

Figure 122 *PMP 450v 4 X 4 AP: Device > Details > Overview*



Wi-Fi APs

Figure 123 *PMP AP: Device > Details > Wi-Fi APs*



PMP SM

The **Details** section displays following tabs for PMP SMs:

- Overview
- Wi-Fi APs
- Installation Summary X

Overview

Figure 124 *PMP SM: Device > Details > Overview*

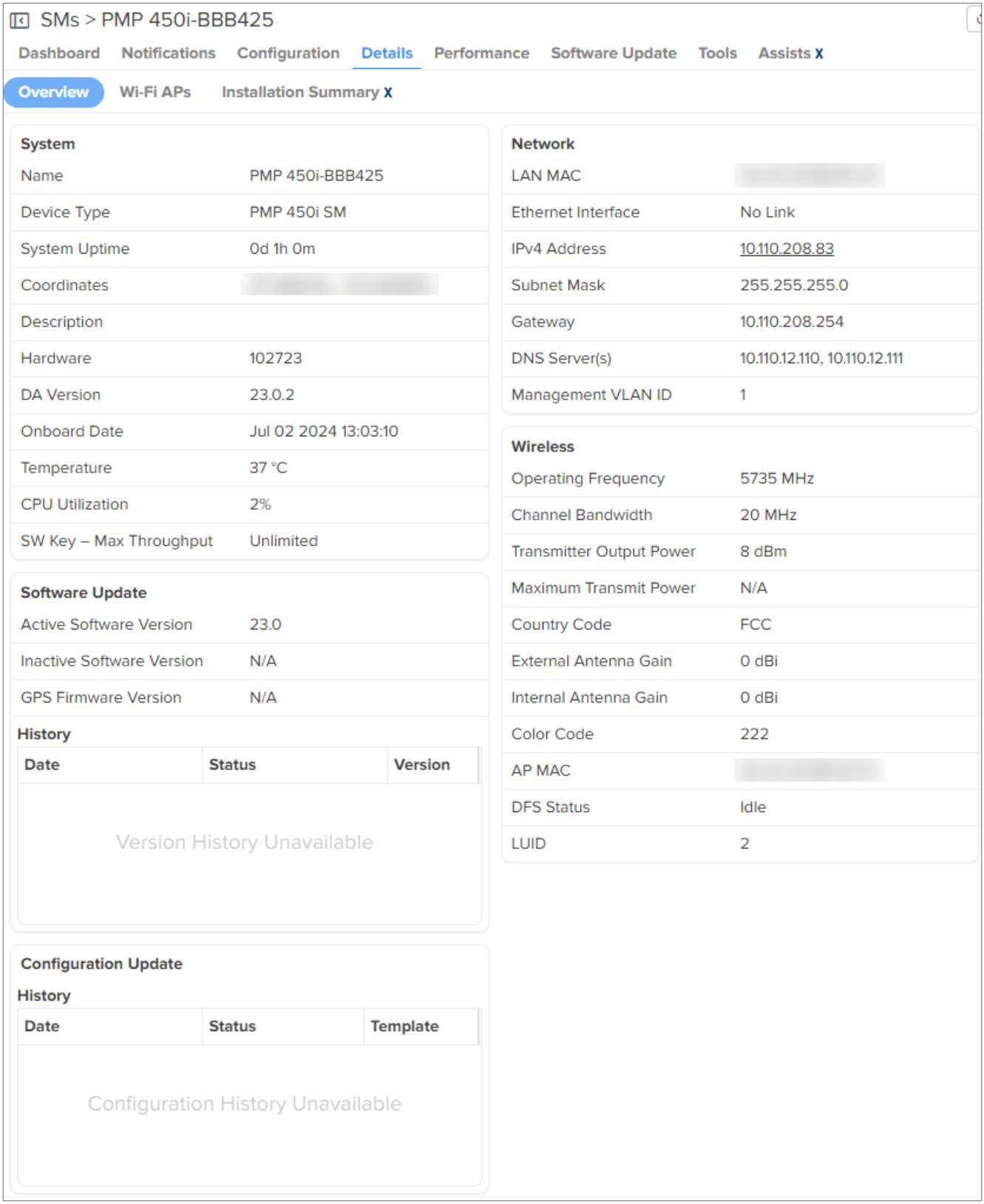
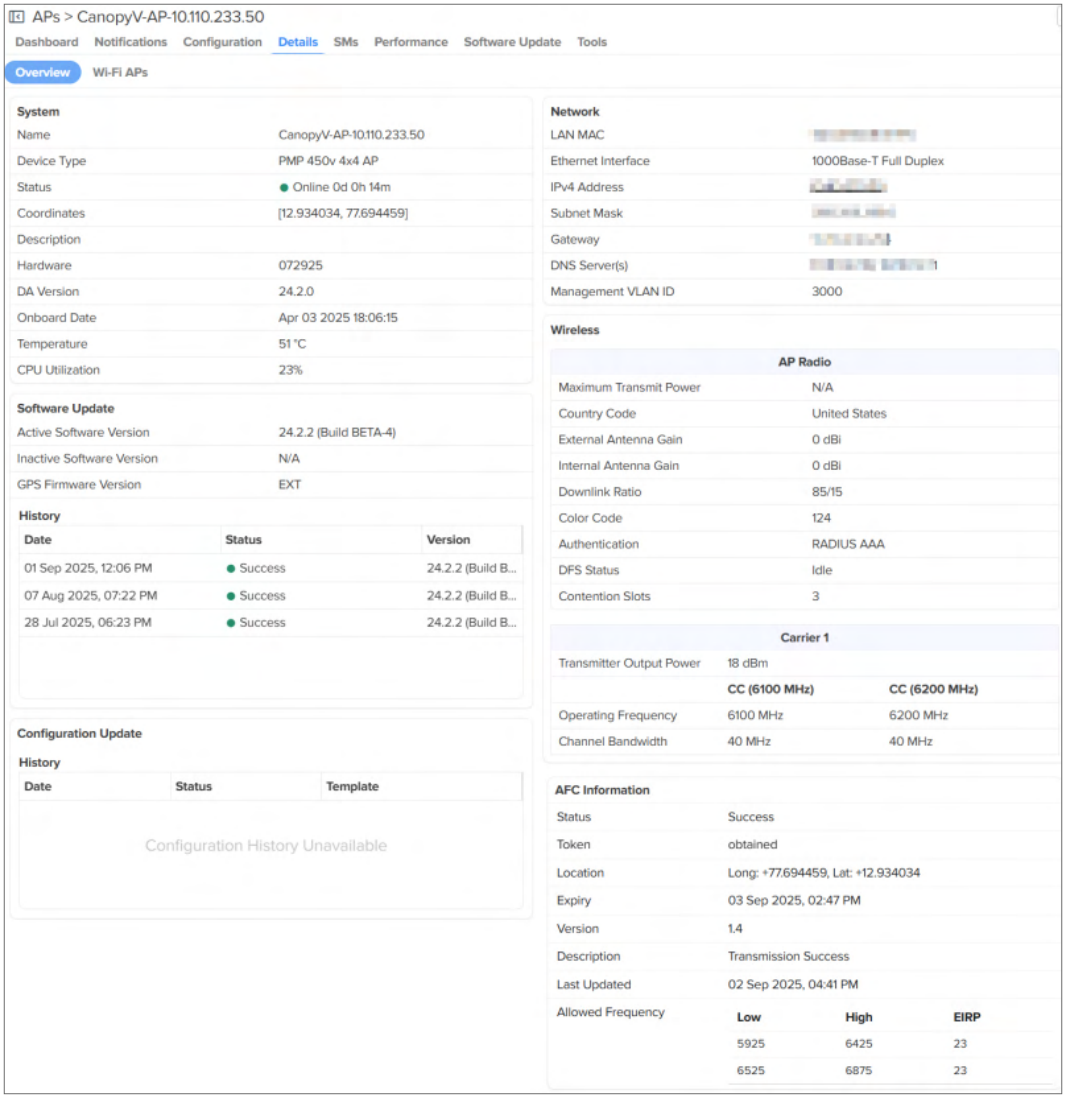
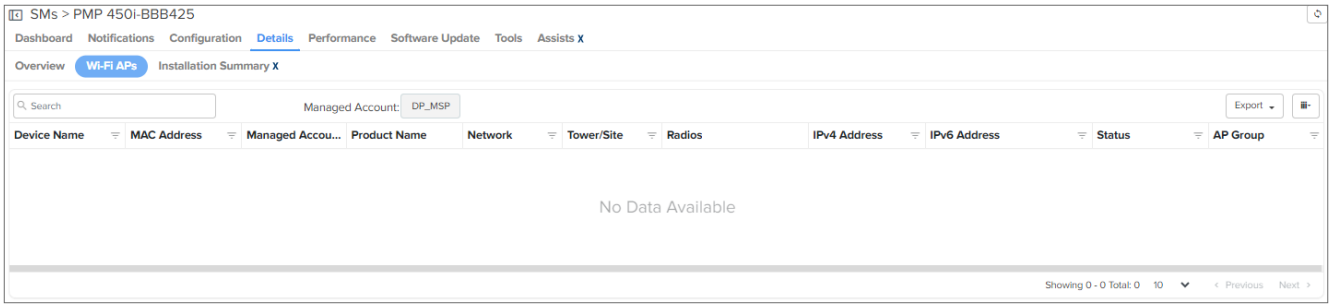


Figure 125 *PMP 450v 4 X 4 and PMP 450v 2 X 2 SMs: Device > Details > Overview*



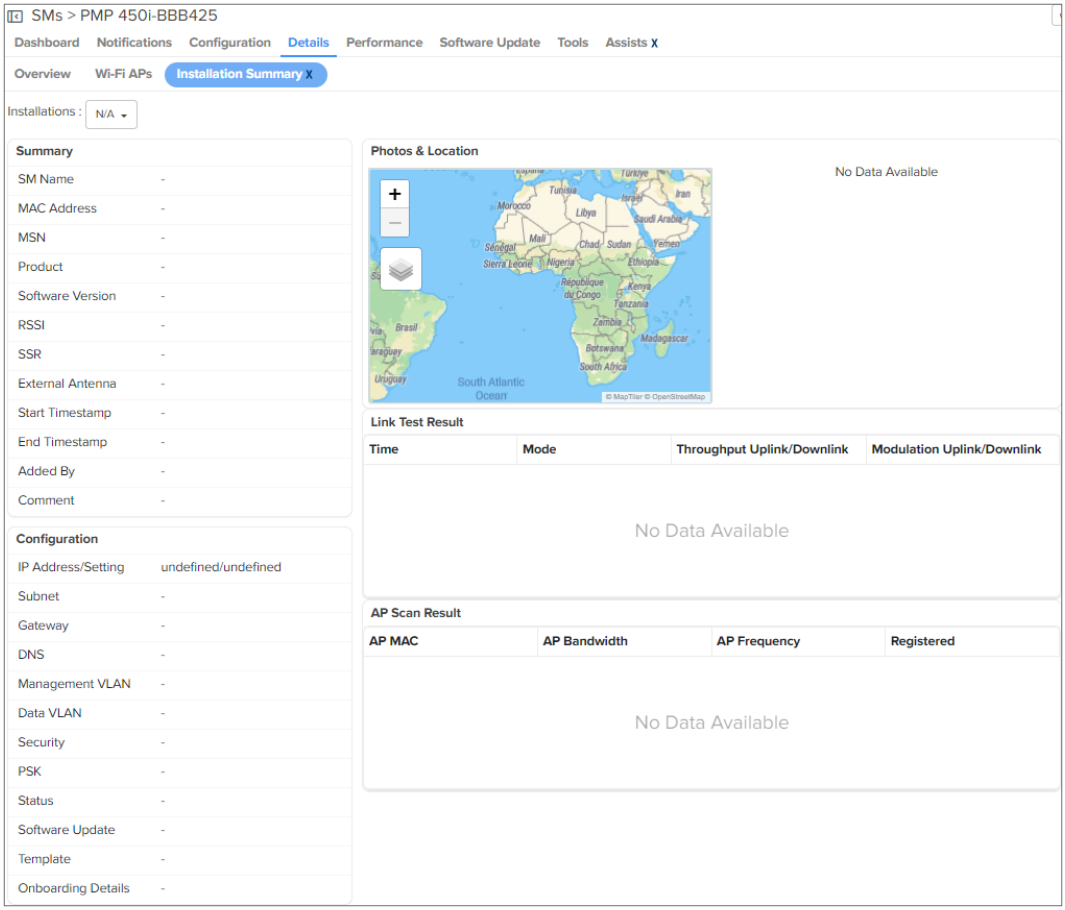
Wi-Fi APs

Figure 126 *PMP SM: Device > Details > Wi-Fi APs*



Installation Summary X

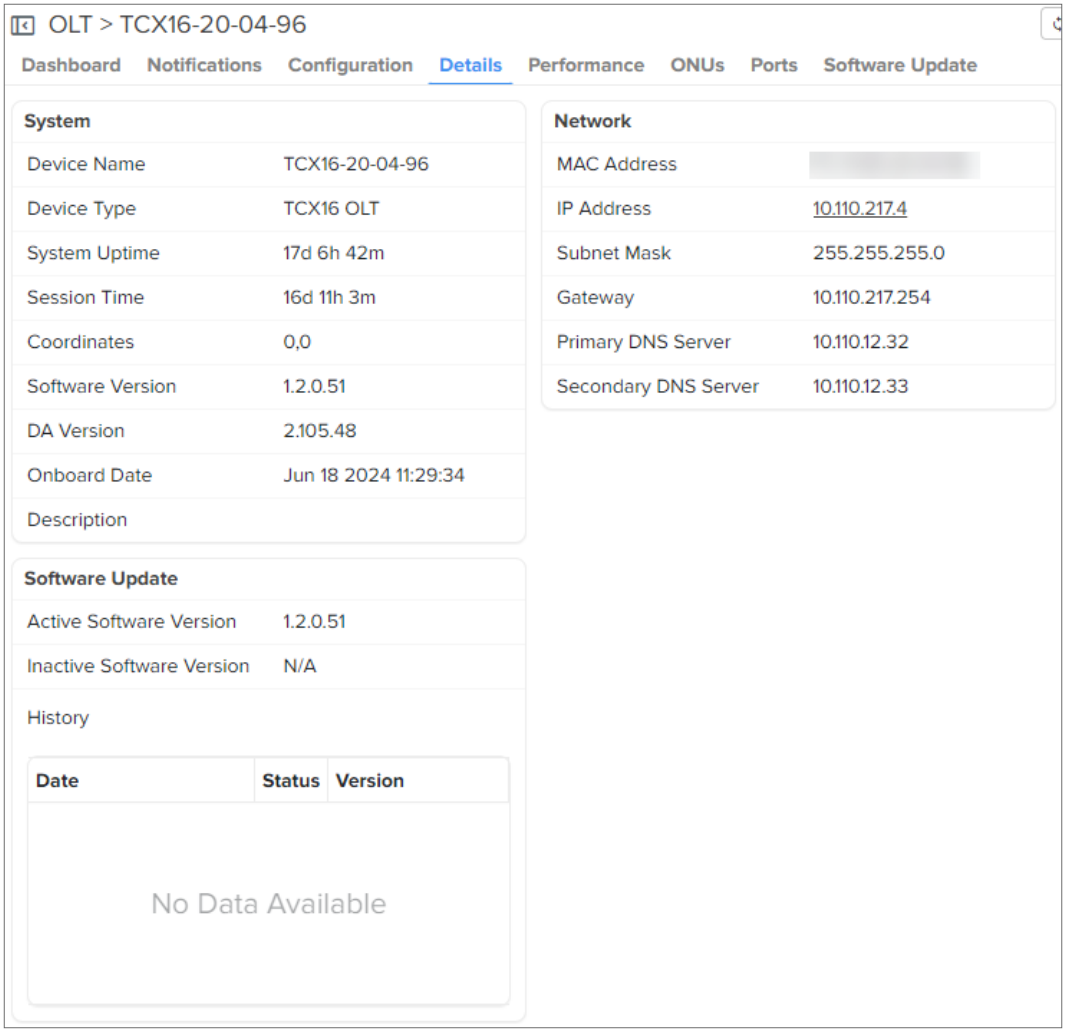
Figure 127 *PMP SM: Device > Details > Installation Summary* **X**



PON (OLT)

The **Details** section displays following information for PON (OLT) device. For more information, see Details.

Figure 128 *PON (OLT): Device > Details*



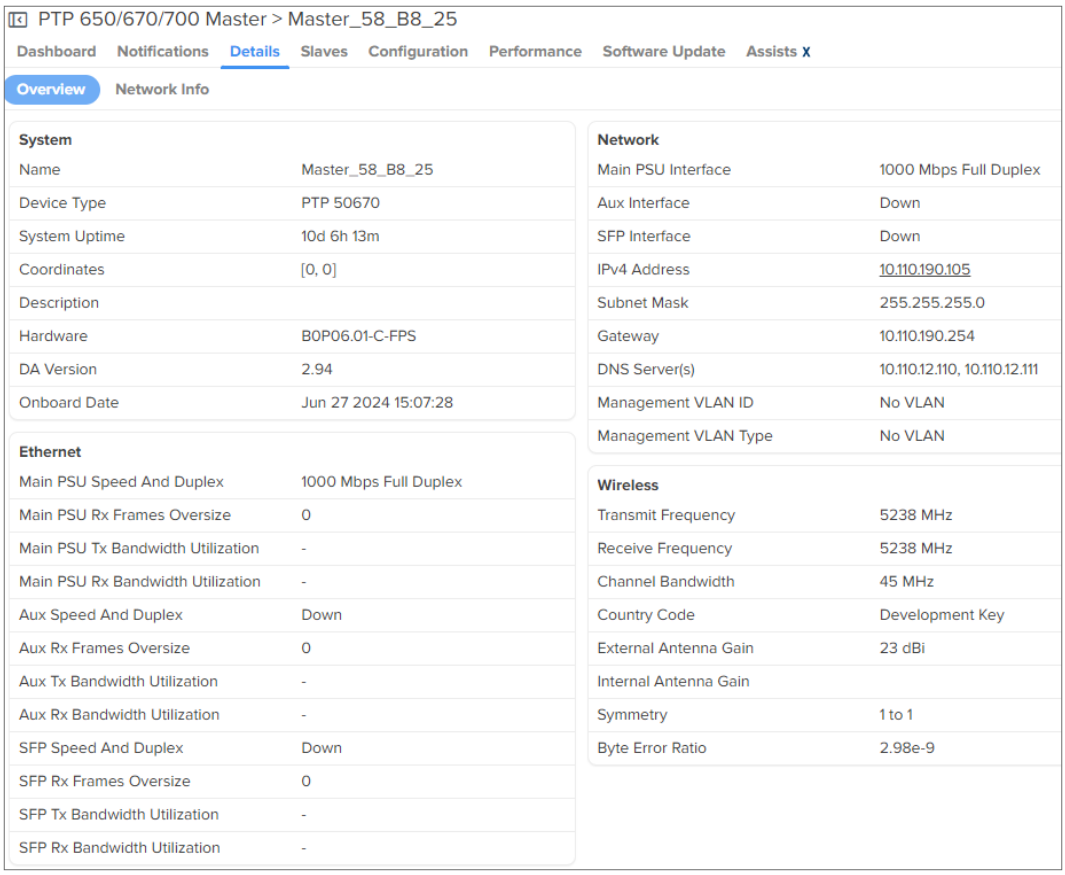
PTP 650/670/700

The **Details** section displays following tabs for PTP 650/670/700:

- Overview
- Network Info

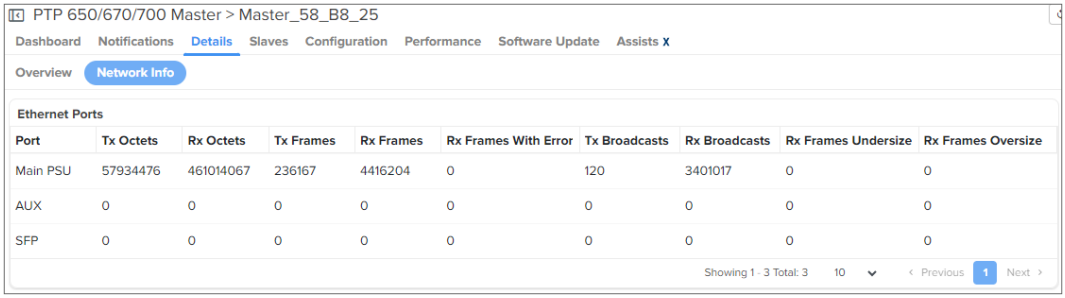
Overview

Figure 129 *PTP 650/670/700: Device > Details > Overview*



Network Info

Figure 130 *PTP 650/670/700: Device > Details > Network Info*



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

PTP 820/850 Details

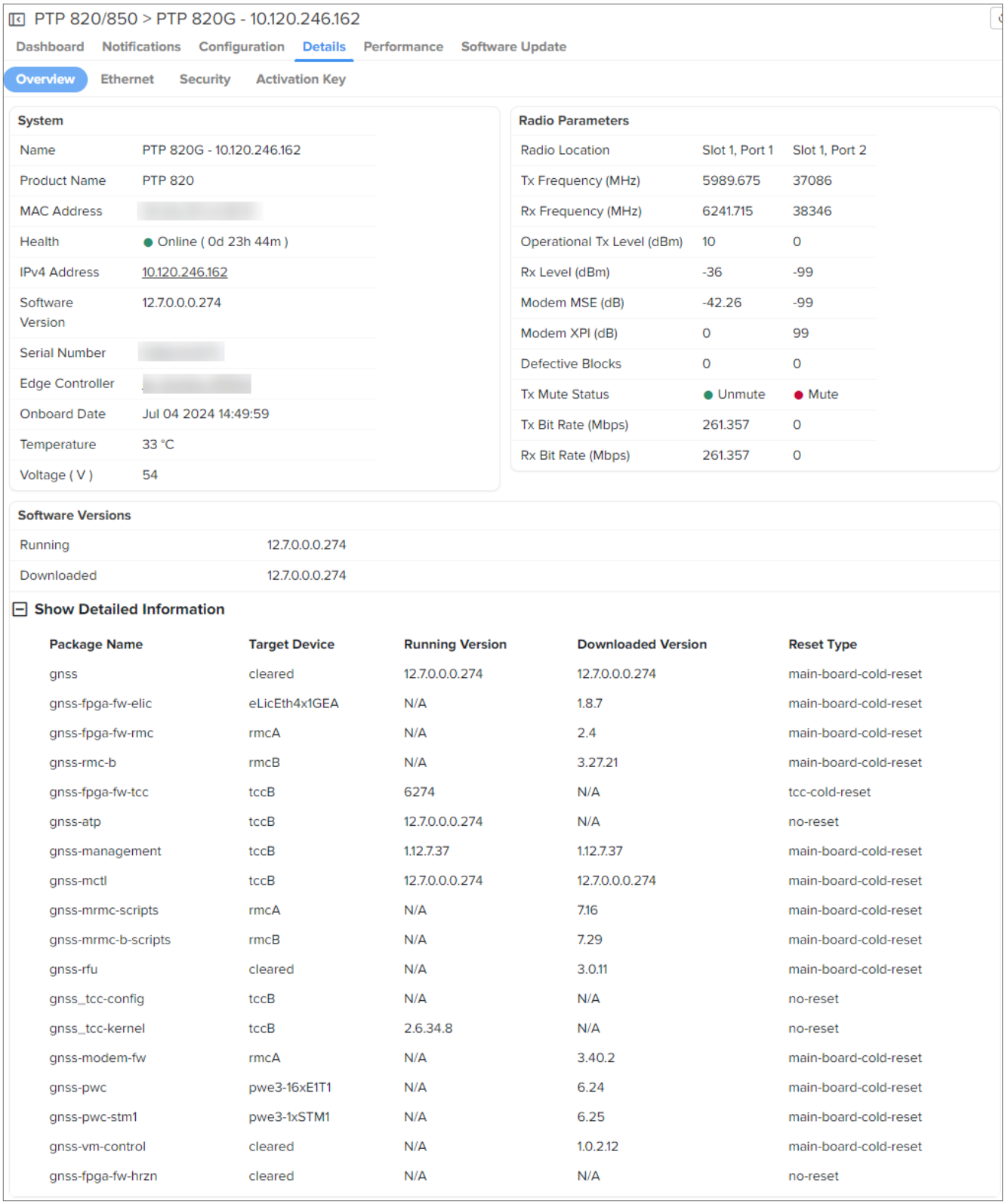
The **Details** section displays following tabs for PTP 820/850:

- Overview
- Ethernet
- Security
- Activation Key

Overview

Overview page provides the information such as System, Radio Parameters and Software Version.

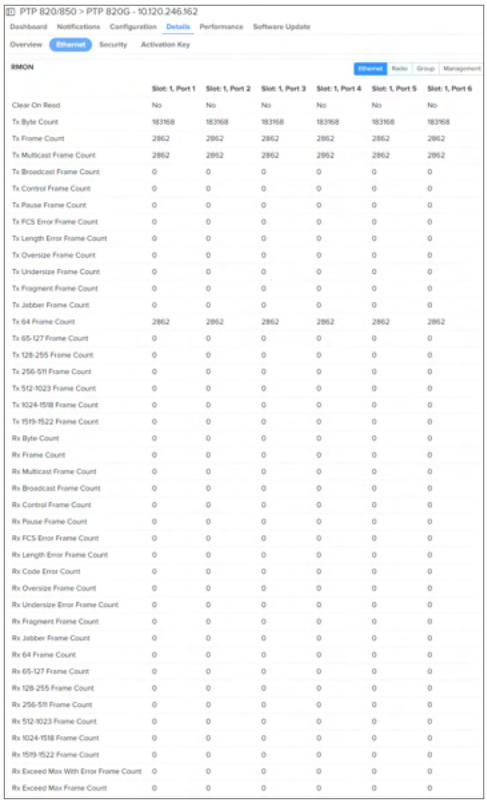
Figure 131 *PTP 820/850: Device > Details > Overview*



Ethernet

Ethernet page provides the information RMON.

Figure 132 *PTP 820/850: Device > Details > Ethernet*

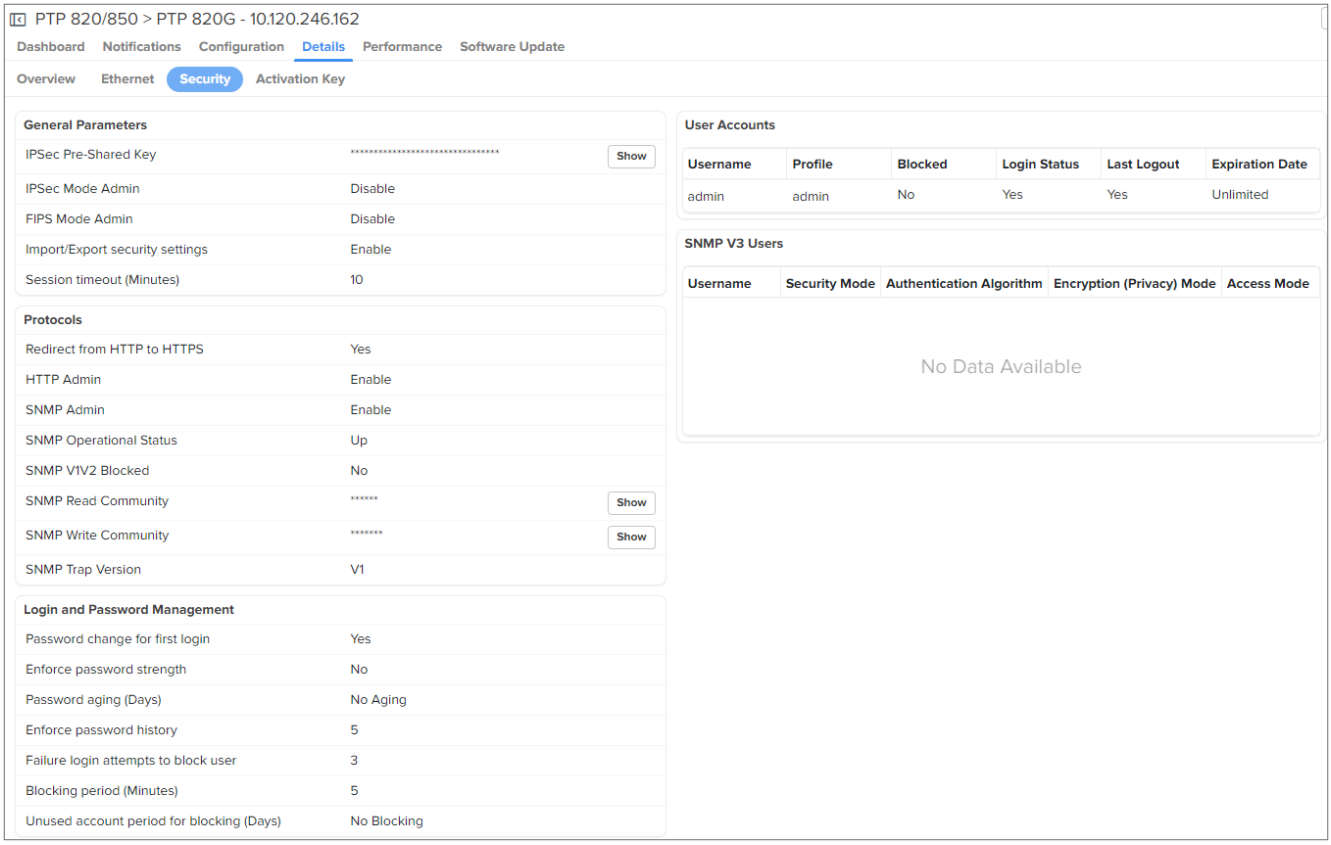


	Slot: 1, Port 1	Slot: 1, Port 2	Slot: 1, Port 3	Slot: 1, Port 4	Slot: 1, Port 5	Slot: 1, Port 6
Clear On Read	No	No	No	No	No	No
Tx Byte Count	183168	183168	183168	183168	183168	183168
Tx Frame Count	2862	2862	2862	2862	2862	2862
Tx Multicast Frame Count	2862	2862	2862	2862	2862	2862
Tx Broadcast Frame 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.

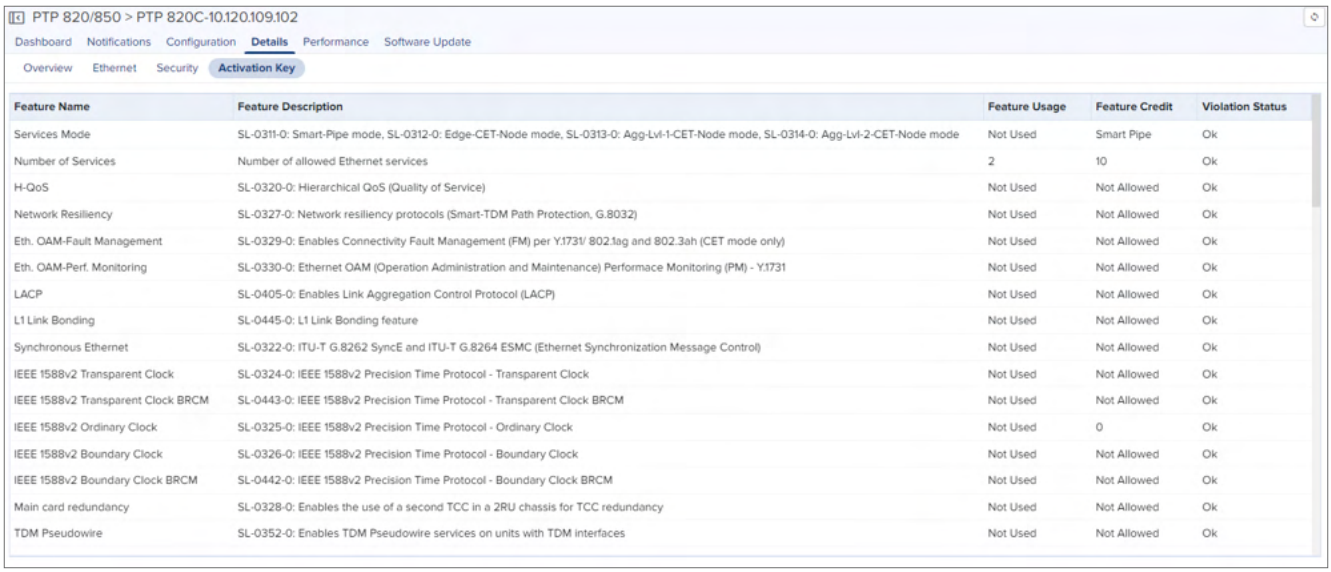
Figure 133 *PTP 820/850: Device > Details > Security*



Activation Key

Activation Key provides the information of Feature Name, Feature Description, Feature Usage, Feature Credit, and Violation.

Figure 134 *PTP 820/850: Device > Details > 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) Performace 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

Performance

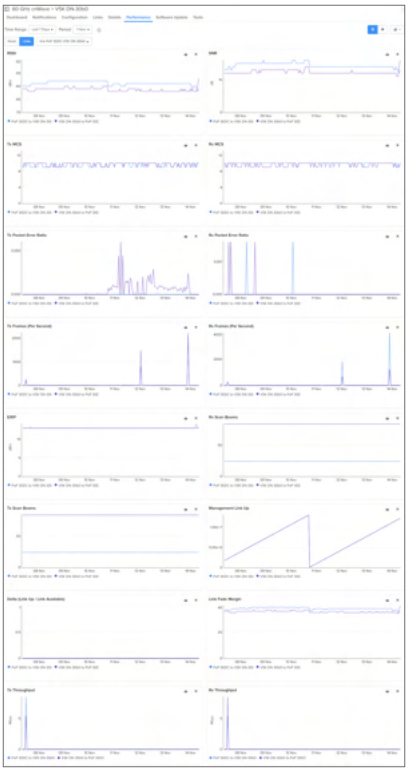
Performance pages display a synchronized view of time-series data for devices. The data can be filtered using the interval ranges in the upper left (last 4 hours to last week for Essentials customers), or by dragging the cursor on the graph to select a specific range. The data presented varies based upon device type.

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:

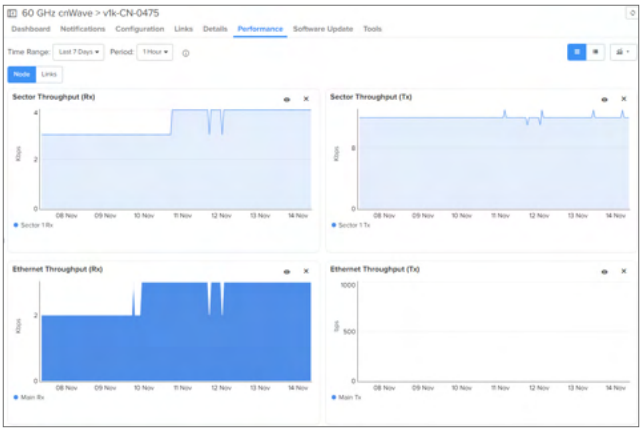
  - Delta (Link Up/Link Available)
  - EIRP
  - Link Fade Margin
  - Management Link Up
  - RSSI
  - Rx Frames (Per Second)
  - Rx MCS
  - Rx Packet Error Ratio
  - Rx Scanbeams
  - Rx Throughput
  - SNR
  - Tx Frames (Per Second)
  - Tx MCS
  - Tx Packet Error Ratio
  - Tx Scanbeams
  - Tx Throughput



- 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

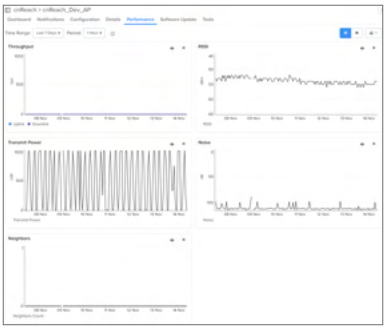
  Displays the following graphs:

  - Clients by Band
  - Clients by Radio
  - CPU
  - Throughput by Band (Downlink)
  - Throughput by Band (Uplink)
  - Throughput by Radio (Downlink)
  - 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

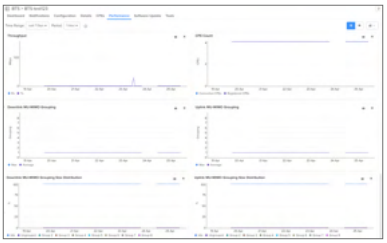
  Displays the following graphs:

  - 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

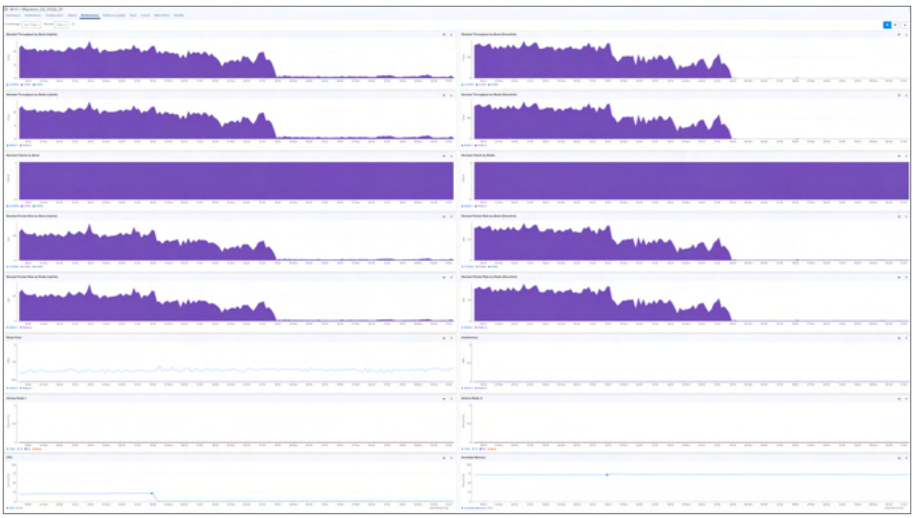
  Displays the following graphs:

  - 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
- Packet Rate by Band (Downlink)
- Packet Rate by Band (Uplink)
- Packet Rate by Radio (Downlink)
- Packet Rate by Radio (Uplink)
- Throughput by Band (Downlink)
- Throughput by Band (Uplink)
- Throughput by Radio (Downlink)
- Throughput by Radio (Uplink)
- Stacked Throughput by Radio (Uplink)



- Enterprise Wi-Fi (Xirrus-Series)

  Displays the following graphs:

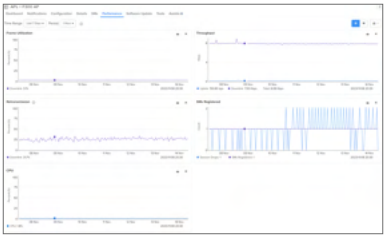
  - Available Memory
  - Clients by Band
  - Clients by Radio
  - CPU
  - Packet Rate by Band (Downlink)
  - Packet Rate by Band (Uplink)

- Packet Rate by Radio (Downlink)
- Packet Rate by Radio (Uplink)
- Throughput by Band (Downlink)
- Throughput by Band (Uplink)
- Throughput by Radio (Downlink)
- Throughput by Radio (Uplink)

- ePMP AP

  Displays the following graphs:

  - CPU
  - Frame Utilization
  - Retransmission
  - SMs Registered
  - Throughput

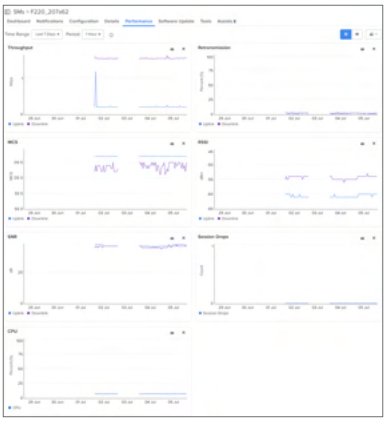


- ePMP SM

  Displays the following graphs:

  - CPU
  - MCS
  - Retransmission
  - RSSI
  - Session Drops

- SNR
- Throughput



- PMP AP

  Displays the following graphs:

  - CPU
  - Frame Utilization
  - SMs Registered
  - Throughput

- PMP 450v 4 X 4 AP

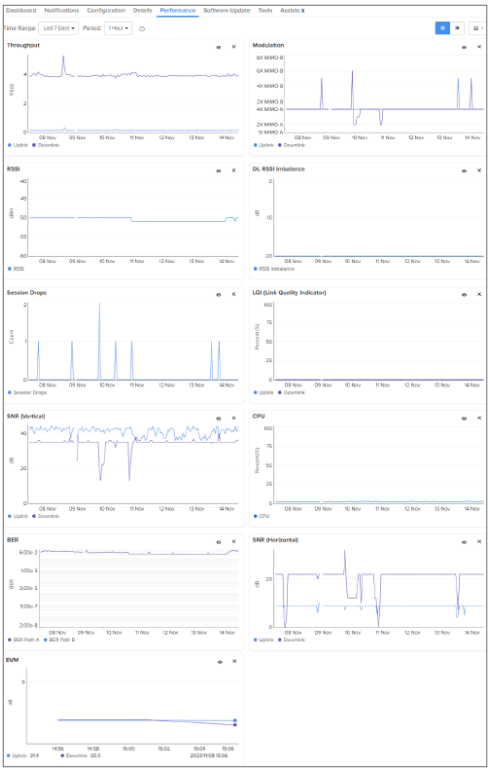
  Displays the following graphs:

  - CPU
  - Frame Utilization : Downlink
  - Frame Utilization : Uplink
  - 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

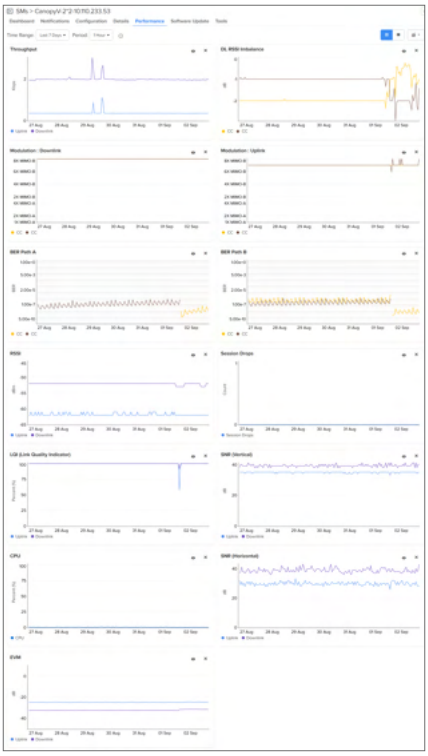


- PMP 450v 4 X 4 and PMP 450v 2 X 2 SMs

  Displays the following graphs:

  - BER Path A
  - BER Path B
  - CPU
  - DL RSSI Imbalance
  - EVM

- LQI (Link Quality Indicator)
- Modulation : Downlink
- Modulation : Uplink
- RSSI
- Session Drops
- SNR (Horizontal)
- SNR (Vertical)
- Throughput



Note

BER with zero values are not plotted on the logarithmic scale graphs.

- PON

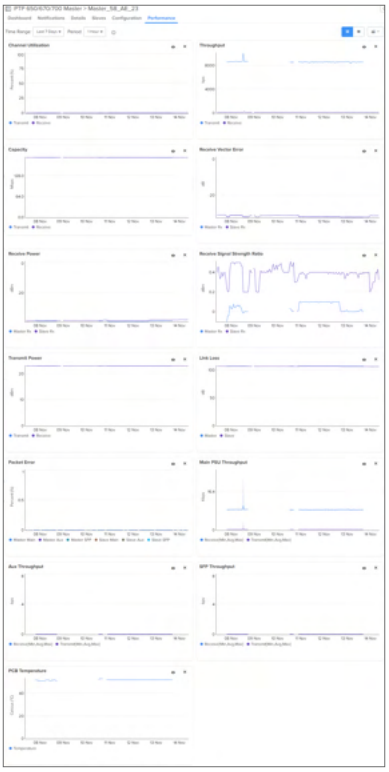
  Displays the following graphs:

  - 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

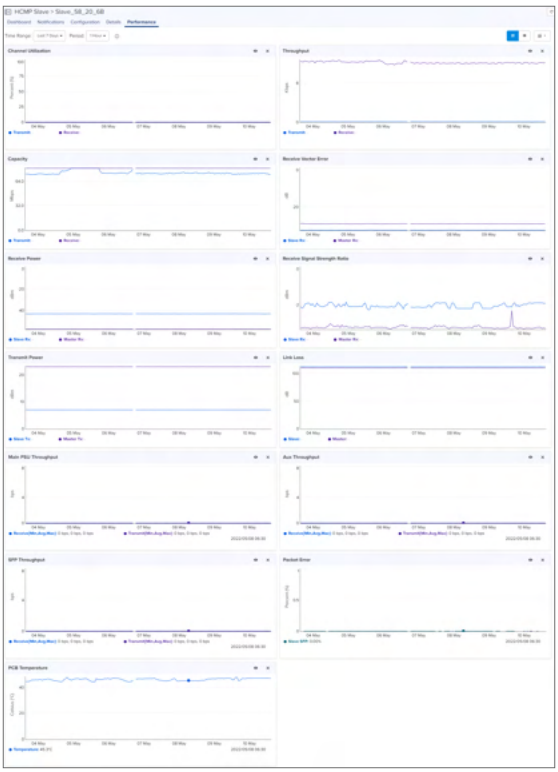


- PTP and HCMP Slaves

  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

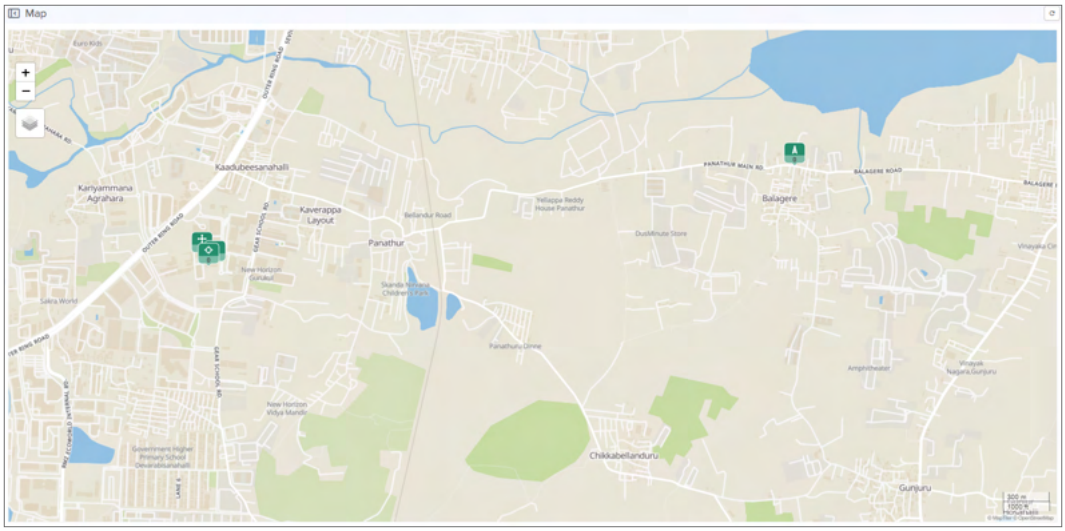
Map

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

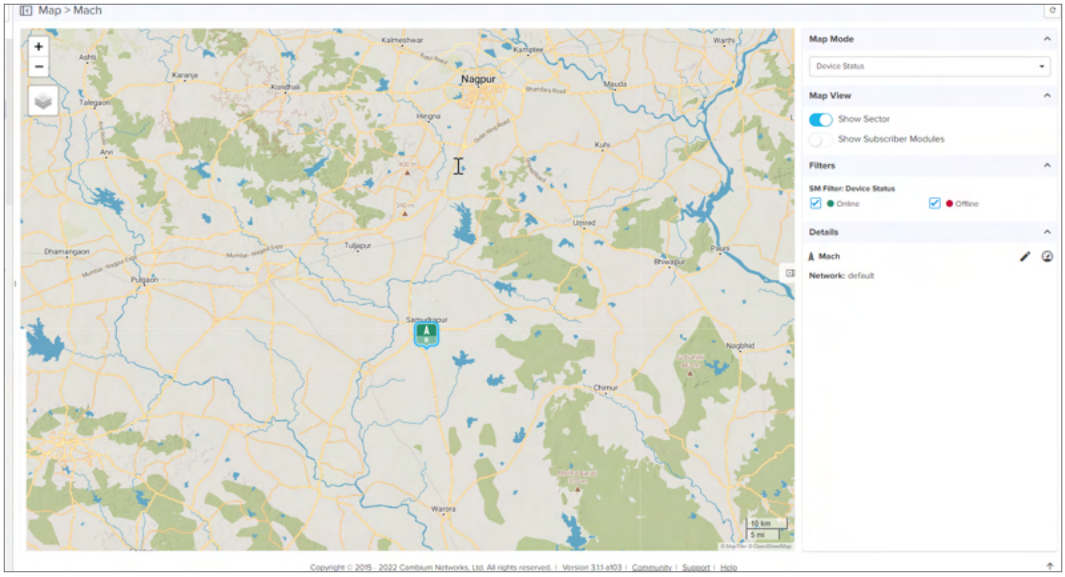
Figure 135 *Map Street View*



The Satellite View is supported in limited US and EU regions.

Figure 136 *Map Satellite View*

Figure 137 *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.

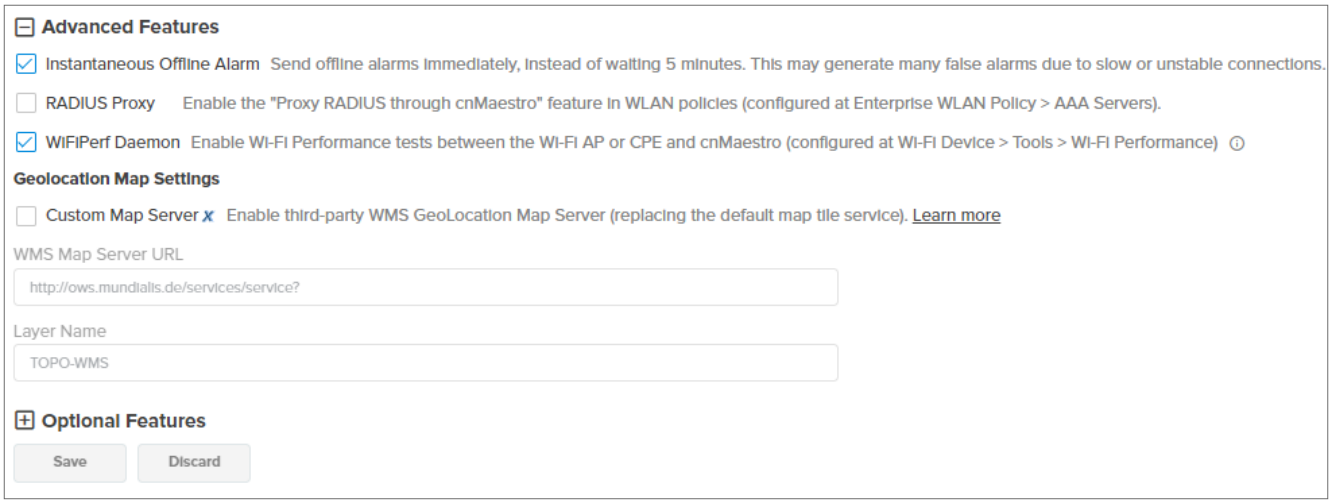
Note

- (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.
- Satellite and Terrain View is available only for cnMaestro X users.

Geolocation Map Settings

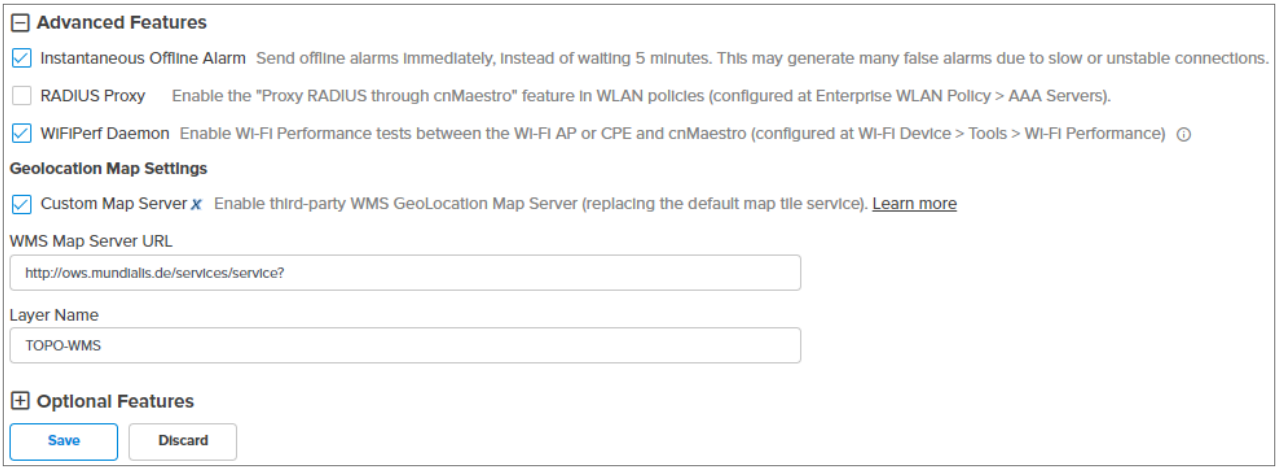
Geolocation Map Settings allows you to customize the on-premises **Map** using a Web Map Service (WMS) map server. The map can be configured to use the WMS map server URL and the Layer Name provided by the service provider.

Example: If you are using the URL http://ows.mundialis.de/services/service?, then enter the layer Name **TOPO-WMS** or **TOPO-OSM-WMS** provided by the map service provider.



To enable Geolocation Map Settings, perform the following steps:

1. Navigate to **Administration** > **Settings** > **Geolocation Map Settings**.
2. Enable **Custom Map Server**.



3. Enter **WMS Map Server URL**.
4. Enter **Layer Name**.
5. Click **Save**.

   If you enable the **Geolocation Map Settings**, it displays the custom tile map as shown below:

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. • ePMP SM

Action	Description
	• Tower
Double-click	Double-click on the following items on the Map to auto-navigate to the Dashboard of that item. • 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 for PMP/ePMP SMs, which define how the device status is presented.

Table 35 *Mode*

Mode	Details
Alarm Status	Highlights devices based upon alarm count (Critical, Major, Minor).
Average MCS (ePMP only)	Displays the Uplink or Downlink average MCS per device.
Device Status	Displays whether a device is Up (Green) or Down (Red).
Frequency	Displays the sector frequency.
Link Quality Indicator (PMP only)	Displays the Uplink or Downlink average indicator 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 only)	Displays the percentage of packets retransmitted between ePMP SM and AP on the wireless link.

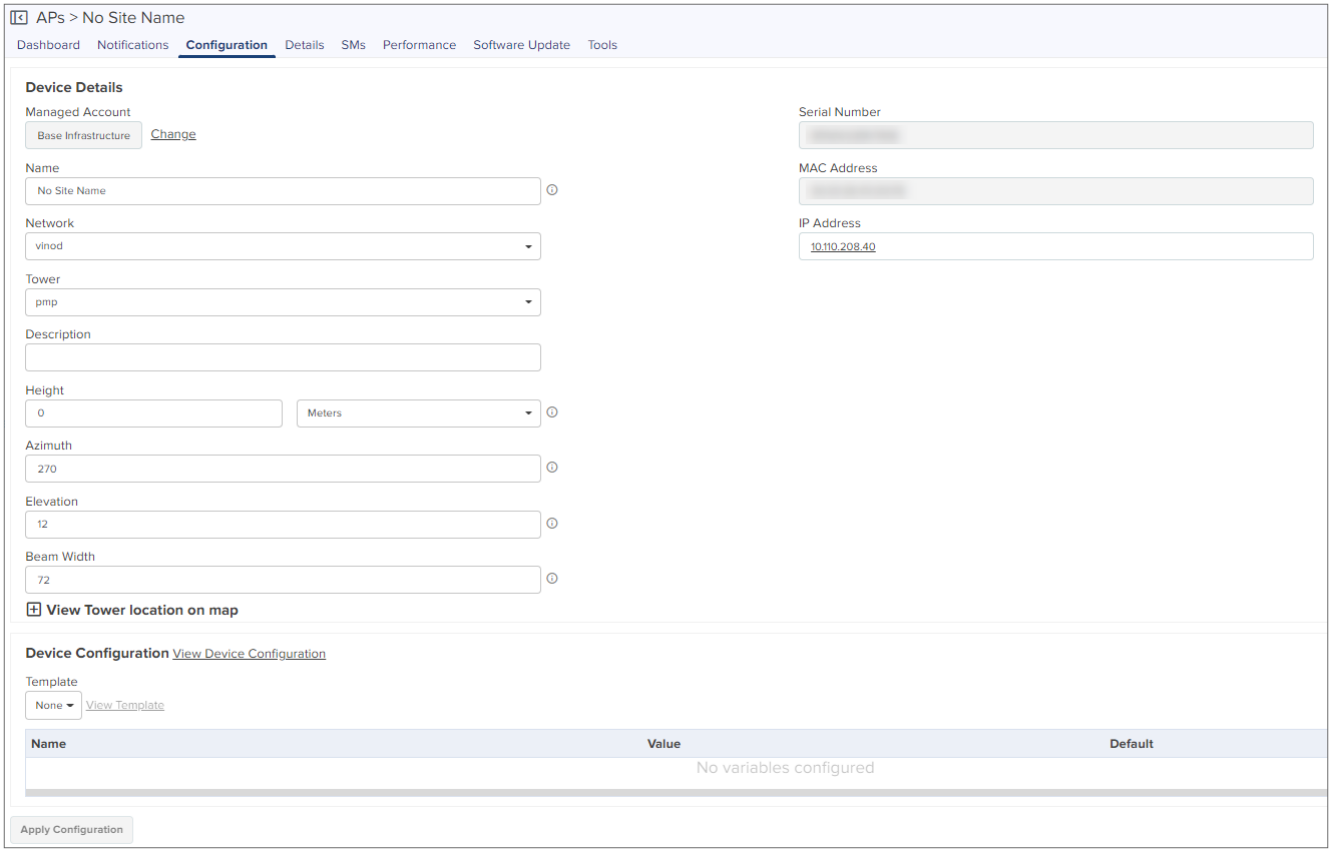
Embedded Maps

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

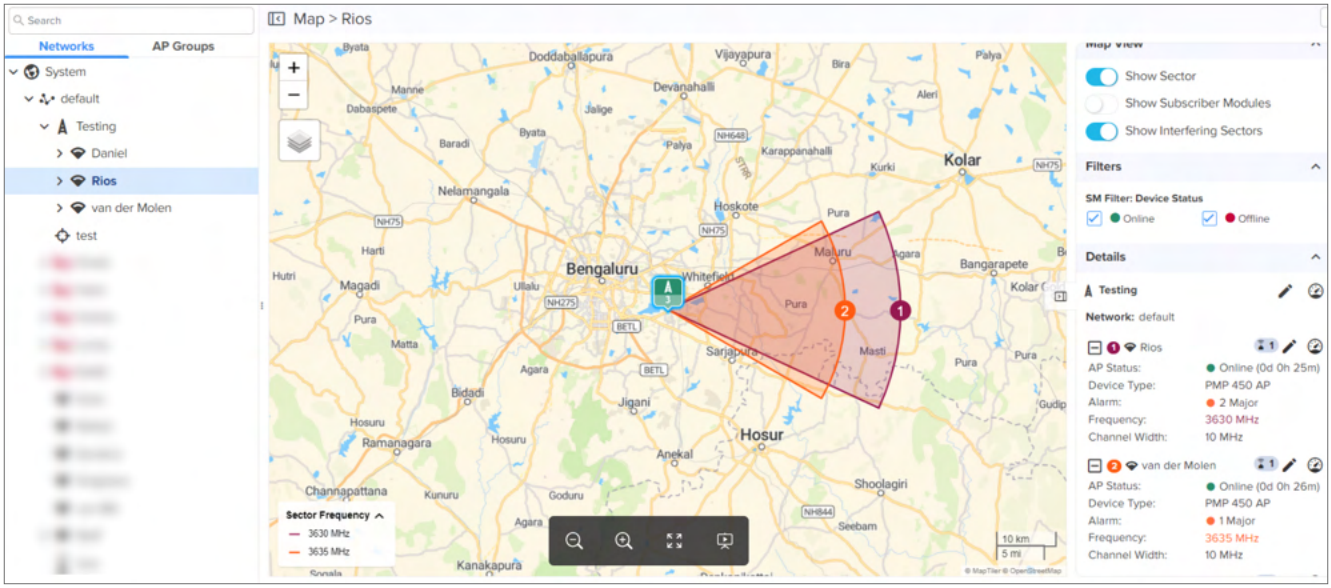
cnMaestro presents a basic sector View for ePMP and PMP fixed wireless devices. This requires configuration of Height, Azimuth, Elevation, and Beamwidth under ePMP/PMP AP configuration. This configured data is used to generate the Sector View. The presentation is not based upon link planning or geographic topology.

Figure 138 *AP Configuration*



Sector Visualization is available in **Map View**. By selecting the **Show Sector** option, the following map is displayed:

Figure 139 *Sector Visualization*



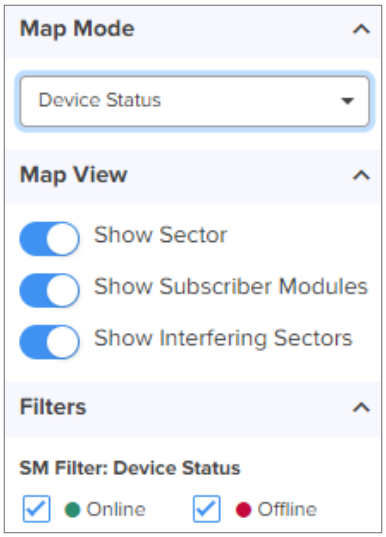
Show Subscriber Modules option is available at System, Network, Tower, and AP levels. User can also choose to set the color of SMs based upon frequency or Online or Offline Status.

Note

- By default **Show Subscriber Modules** is disabled.

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 140.
- Click the Dashboard( ) icon next to the Site or Device name, to view the site or device dashboard details.

Figure 140 *Map: Enterprise Site level*

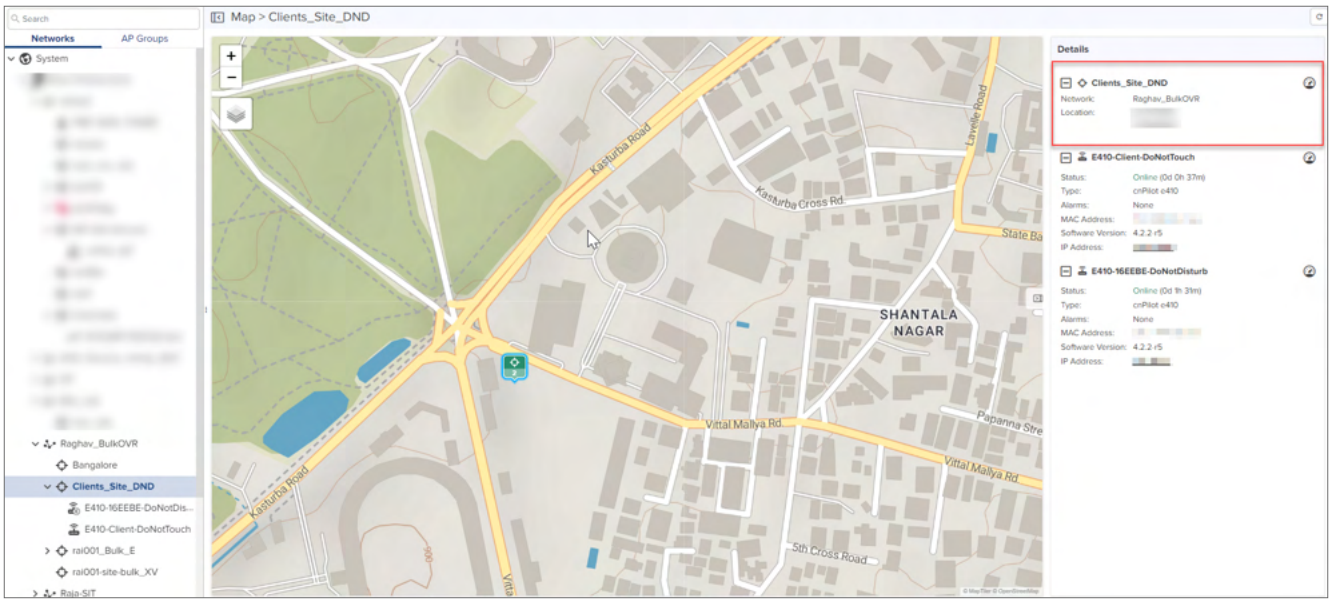


Figure 141 *Map: Home Site level*

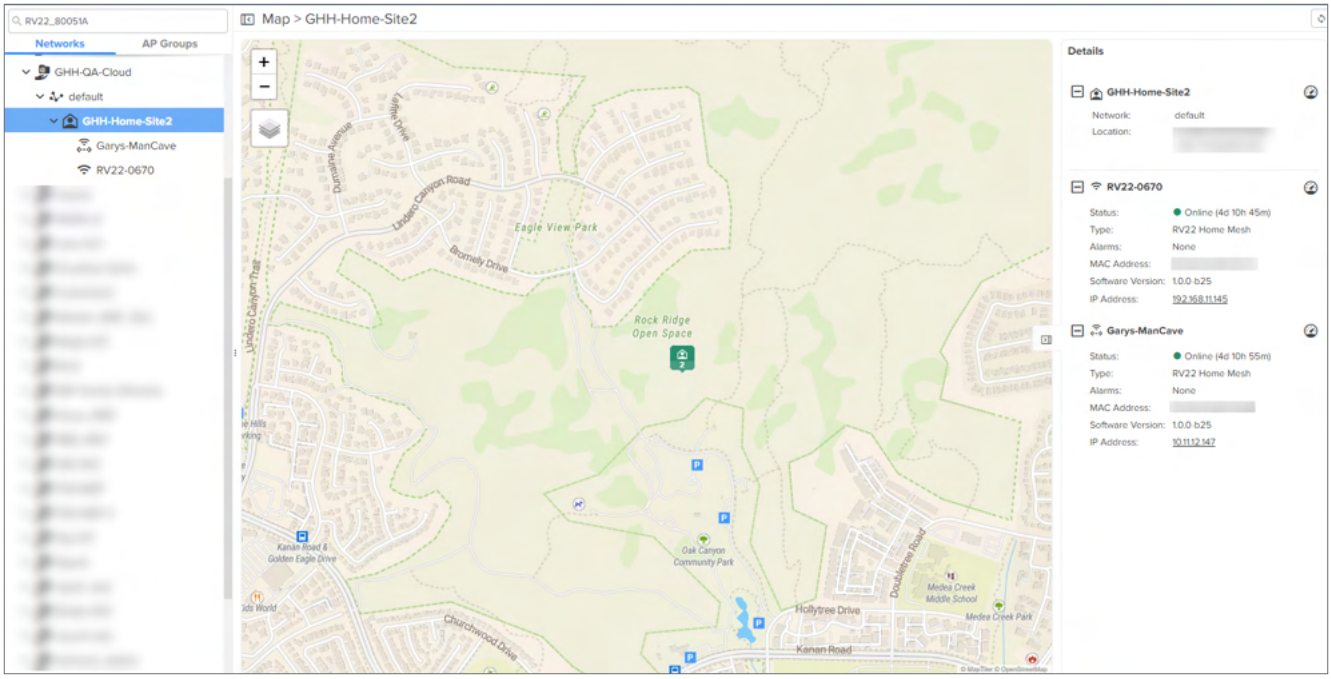


Figure 142 *Map: Device level*

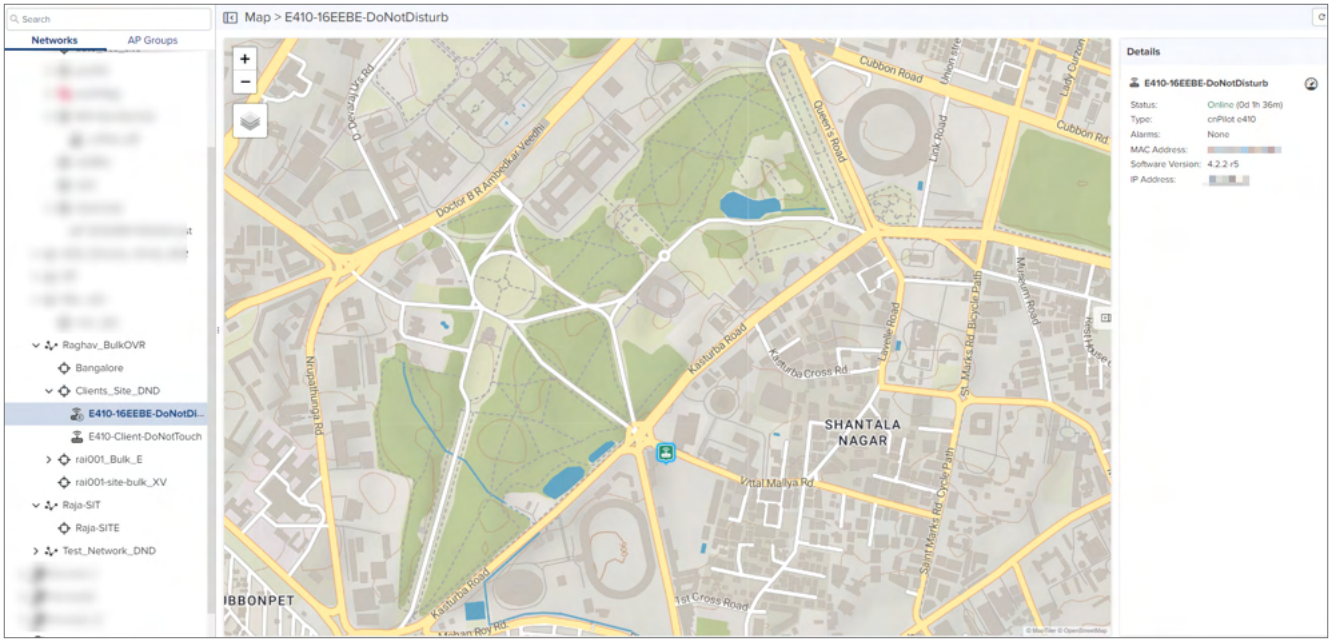


Figure 143 *Map view: cnMatrix*

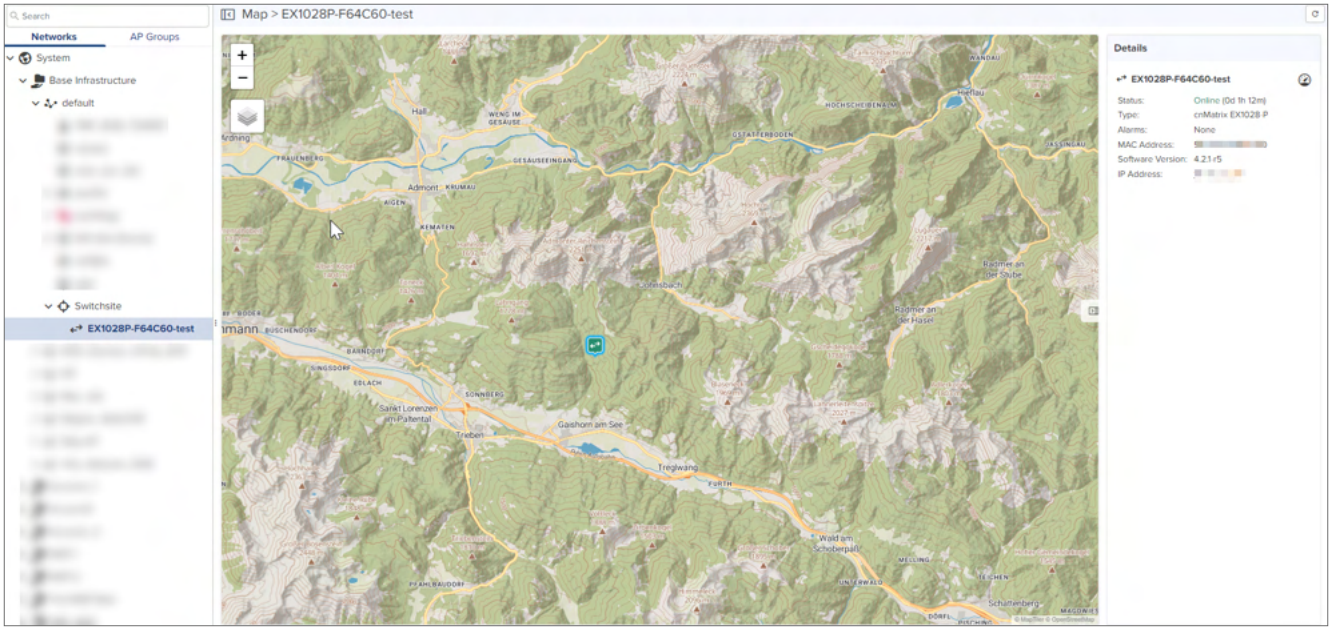


Figure 144 *Map view: Enterprise Wi-Fi (Xirrus-Series)*

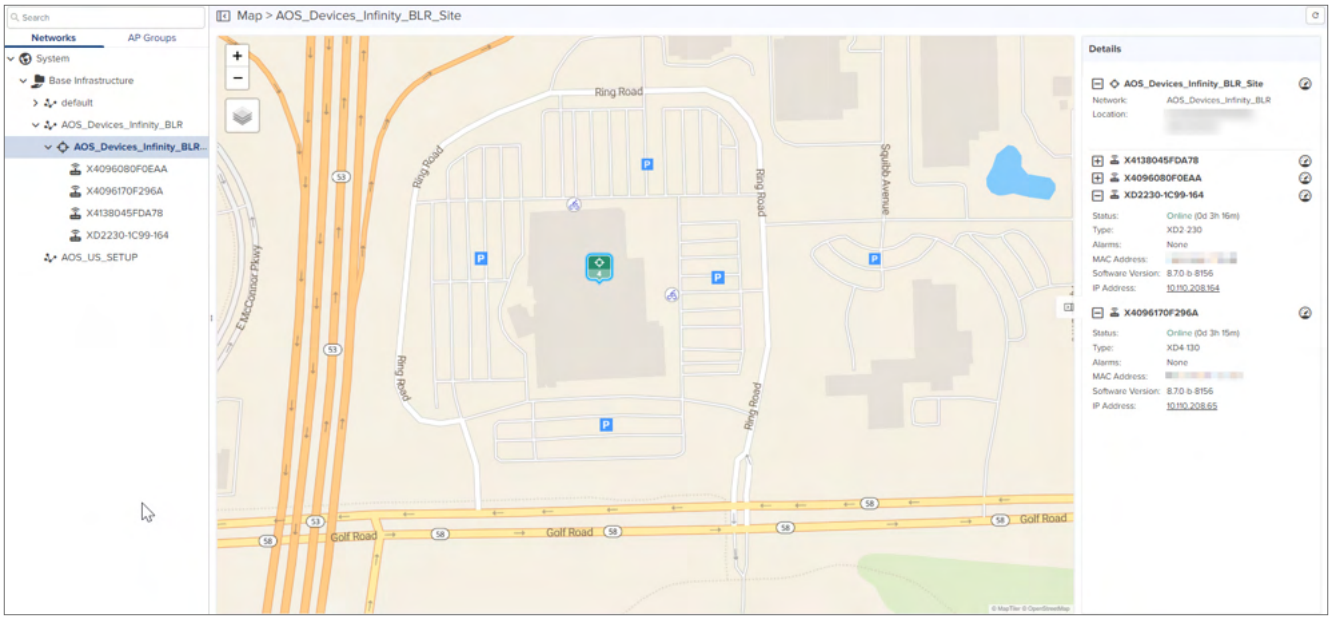
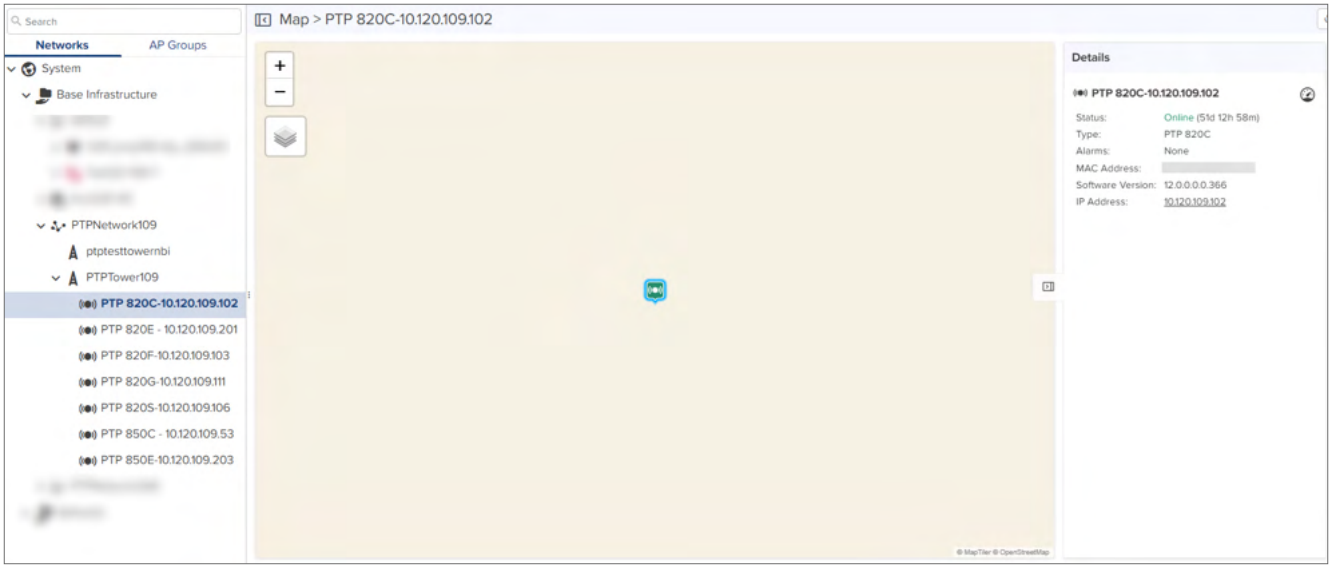


Figure 145 *Map View: PTP 820/850*



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

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

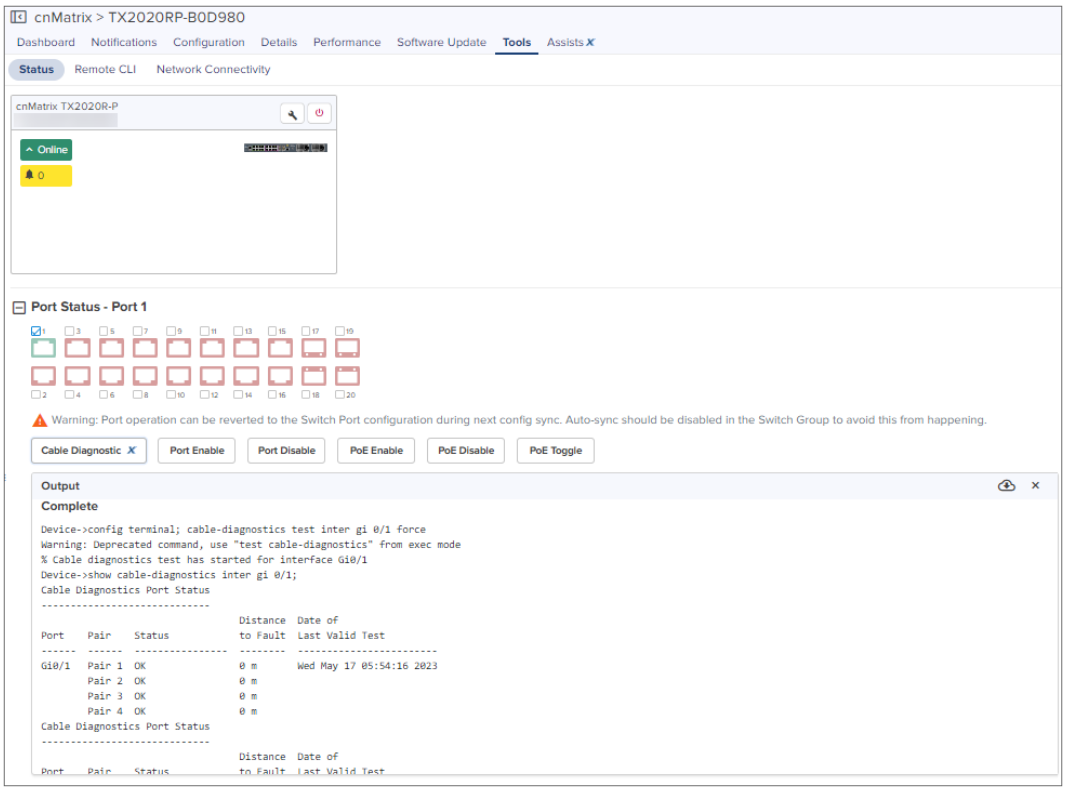
In **Status** tab you can view the status of the device (either Online or Offline). It allows one to reboot the device.

Table 36 *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. • 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.

> **Note**
>
> A minimum software version of 6.2 is required on cnMatrix devices to download the technical support file.

The **Status** tab displays the status of the device (either Online or Offline). It also supports downloading Tech Support File and rebooting the device.

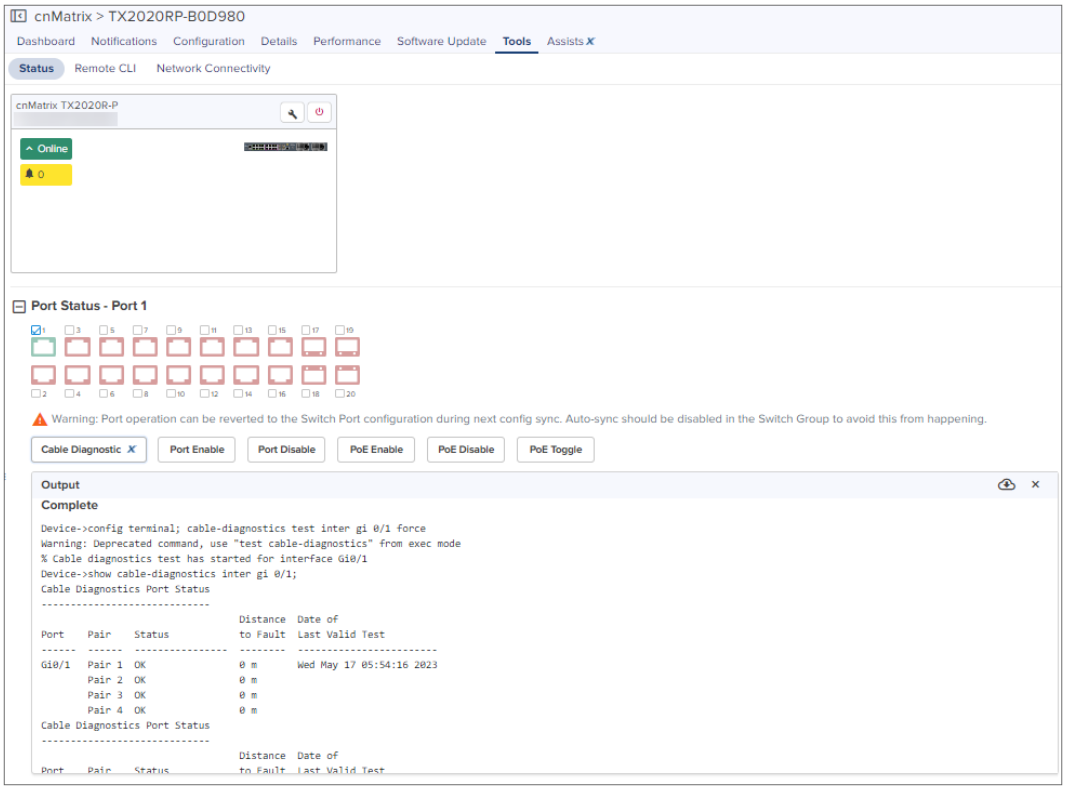


Port Status, presents the following data for the **PoE Switches**:

- 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:

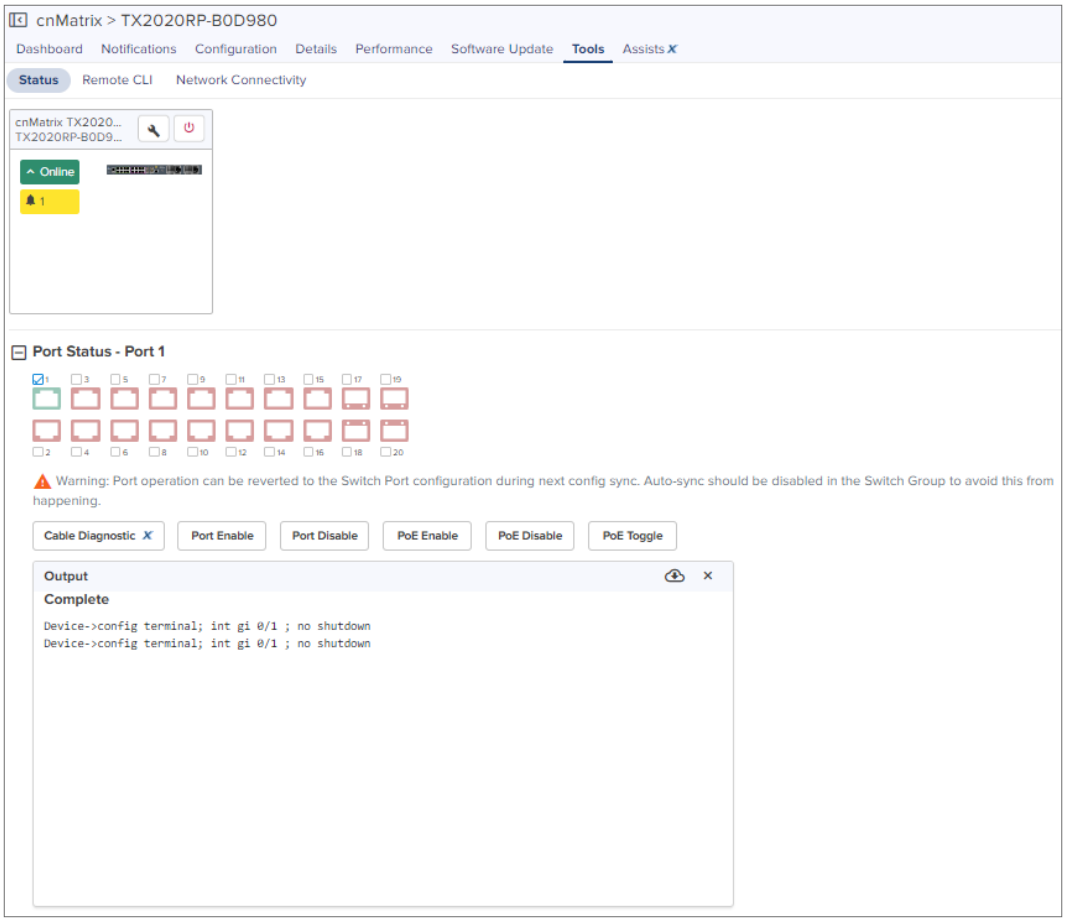


- Download the generated output by clicking the download ( ) icon.
- Clear the generated output by clicking the delete ( ) icon.

> **Note**
>
> Cable Diagnostic is a cnMaestro X feature.

Port Enable or Port Disable

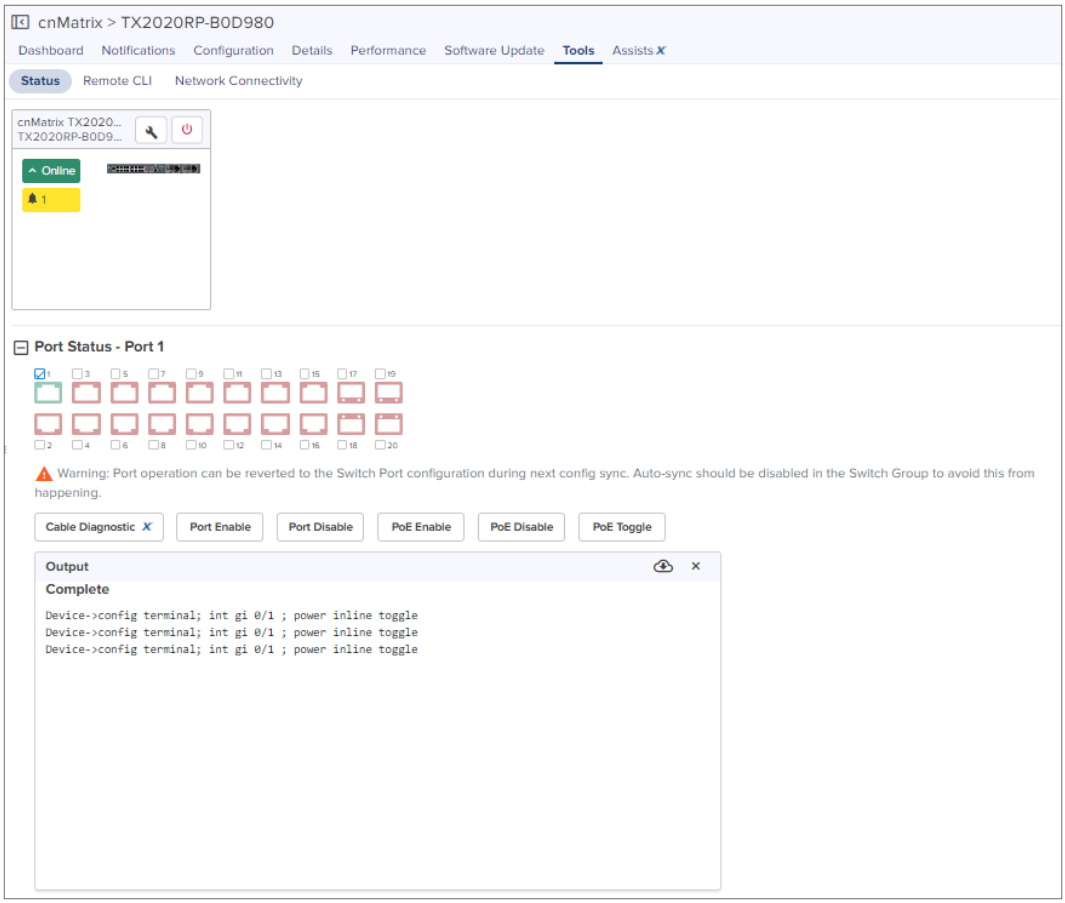
Navigate to **Tools** > **Status** > **Port Status**, select the Port and click **Port Disable** or **Port Enable**, the following output is displayed:



- Download the generated output by clicking the download ( ) icon.
- Clear the generated output by clicking the delete ( ) icon.

PoE Toggle

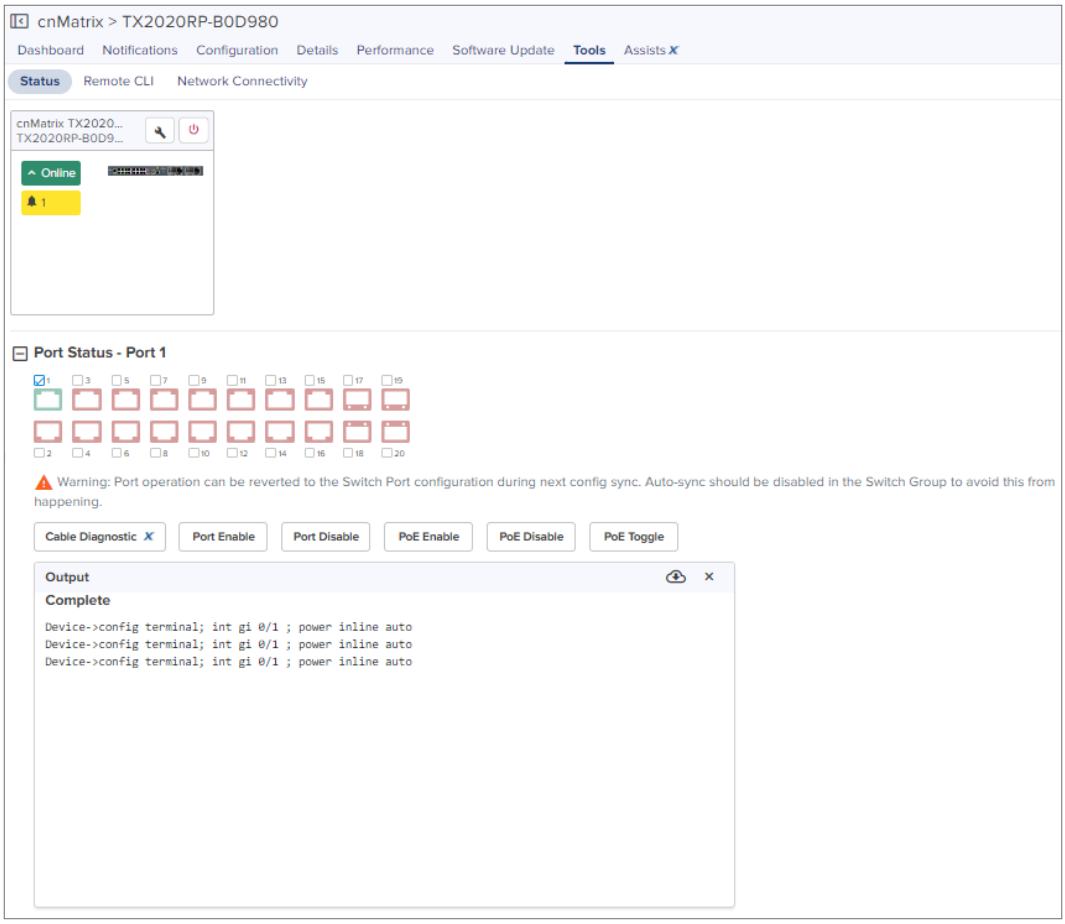
Navigate to **Tools** > **Status** > **Port Status**, select the Port and click **PoE Toggle**, the following output is displayed:



- Download the generated output by clicking the download ( ) icon.
- Clear the generated output by clicking the delete ( ) icon.

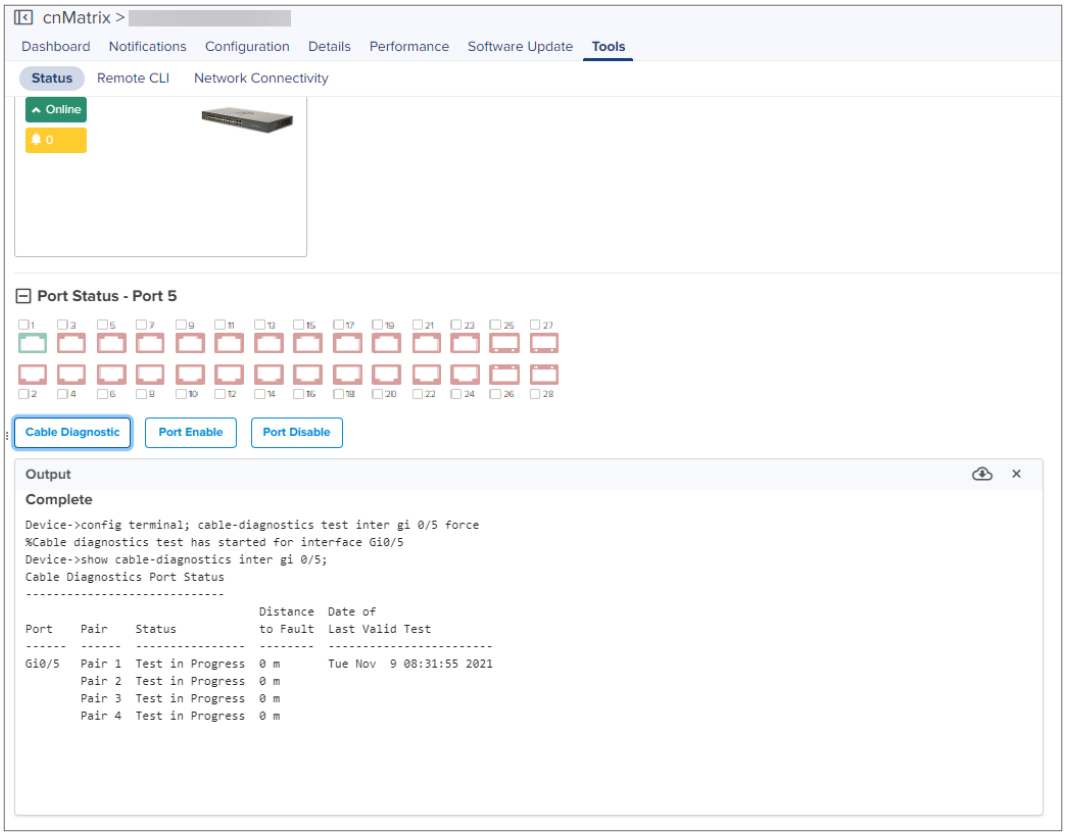
PoE Enable or PoE Disable

Navigate to **Tools > Status > Port Status**, select the Port and click **PoE Enable** or **PoE Disable**, the following output is displayed:



Port Status, presents the following port status for the **non-PoE Switches**:

- Cable Diagnostic
- Port Enable
- Port Disable



Remote CLI

Navigate to **Tools** > **Remote CLI**, when you select a command type and click **Run**, the following output is displayed:

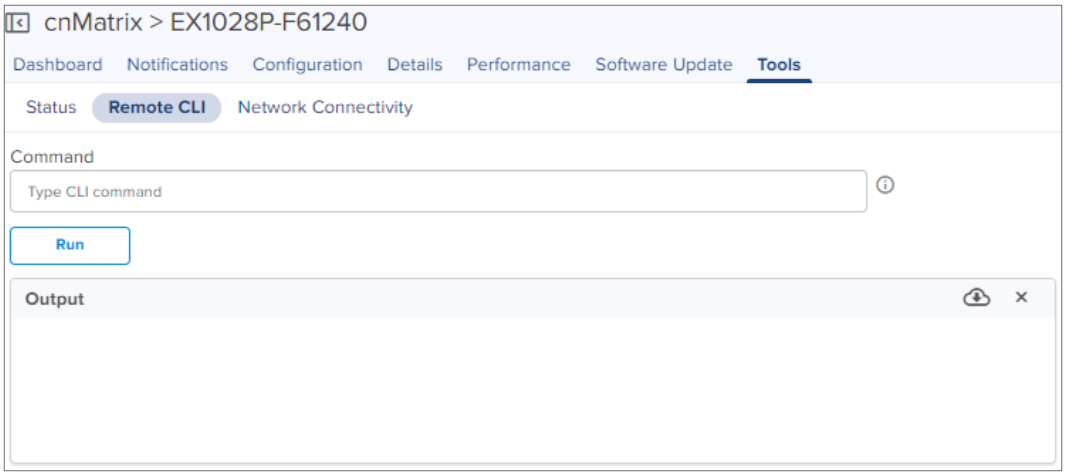
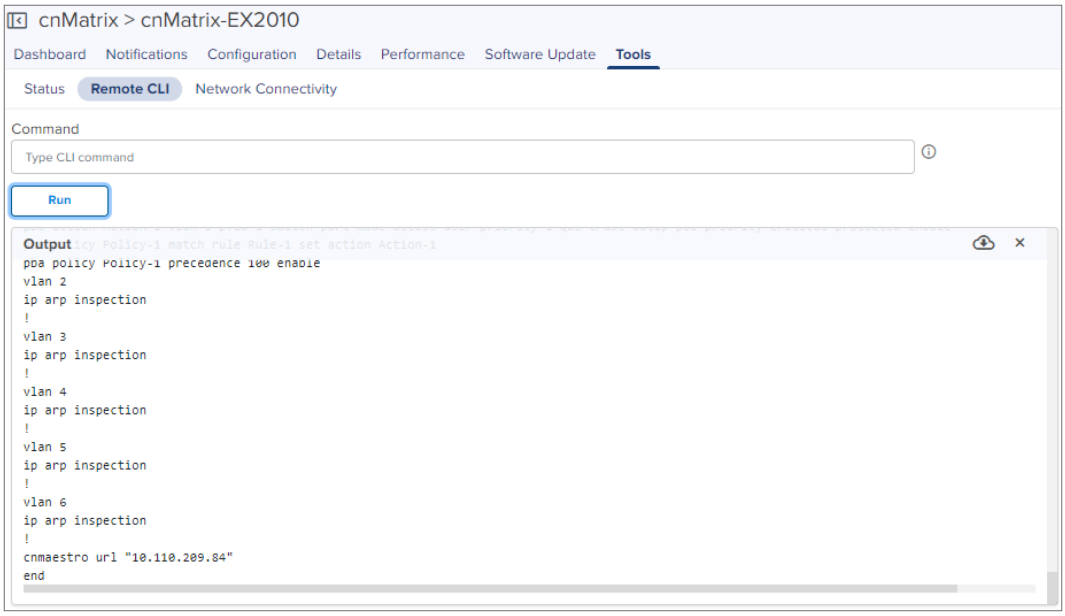
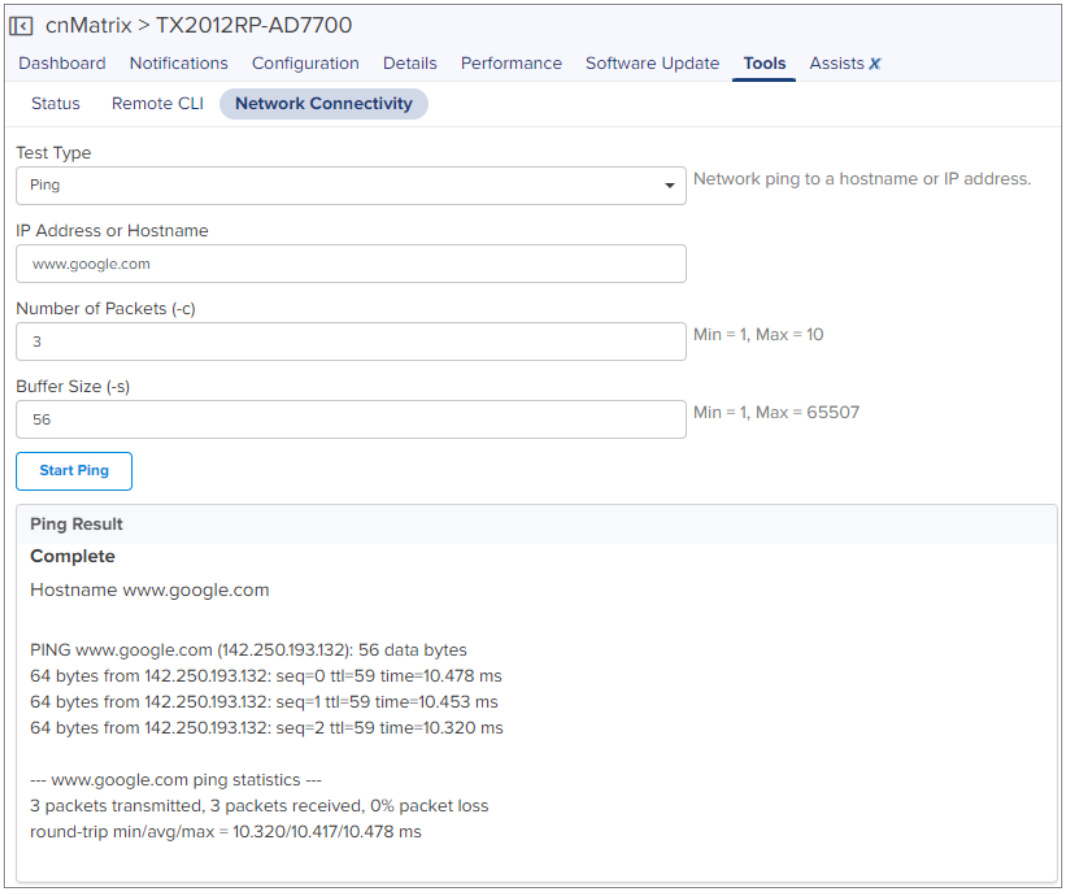


Table 37 *cnMatrix Tools*

Tools	Description
Remote CLI	Enter CLI command in the command text box to execute on device. • Only `Show`command is allowed for Operator users. • All CLI commands are supported by Super Admin and Admin users.



- Download the generated output by clicking the download ( ) icon.
- Clear the generated output by clicking the delete ( ) icon.



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 38 *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 146 *cnPilot Tools*

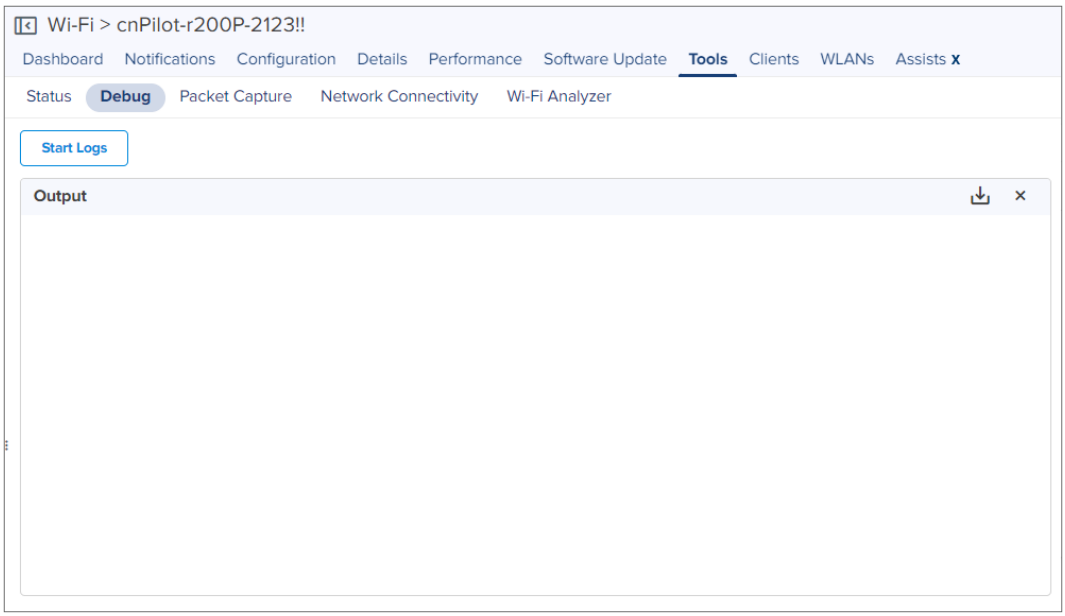


Figure 147 *cnPilot Debug Tools*

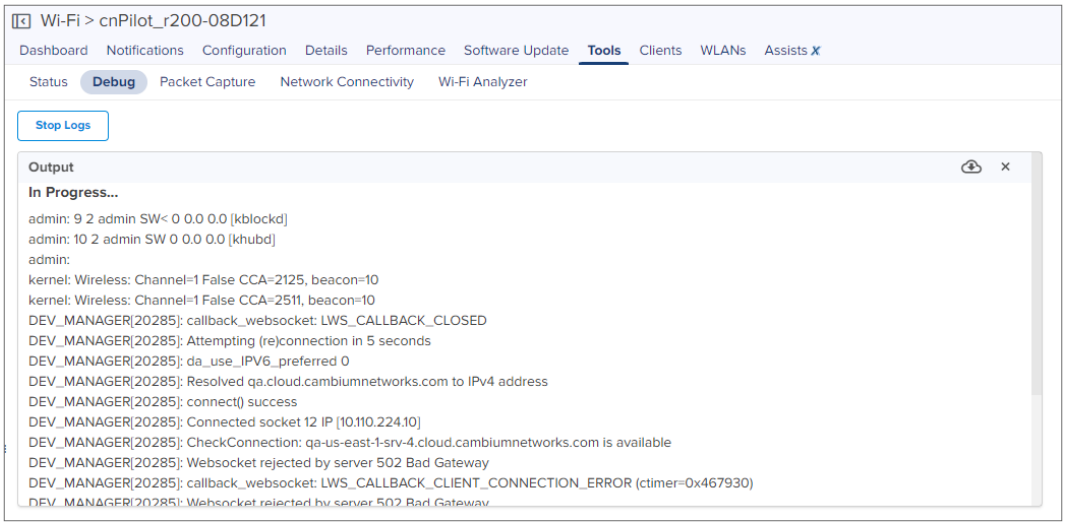


Figure 148 *cnPilot Tools Status*

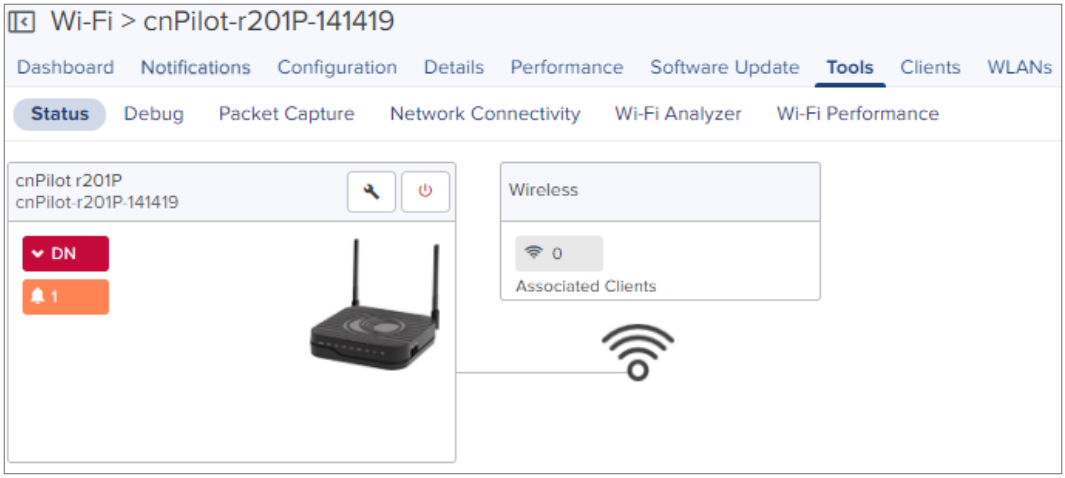


Figure 149 *cnPilot Tools > Packet Capture*

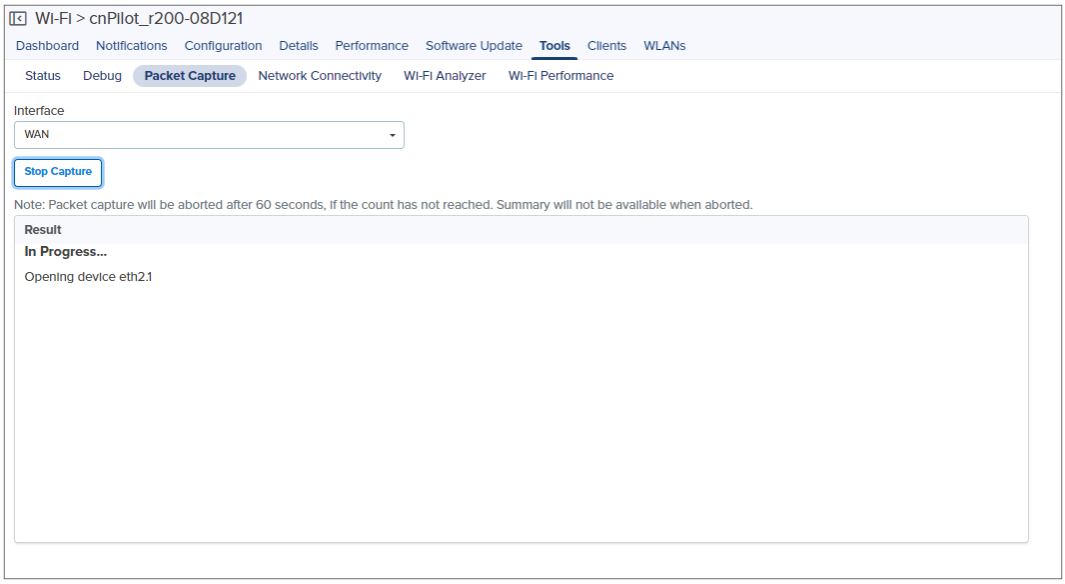


Figure 150 *cnPilot Tools > Network Connectivity*

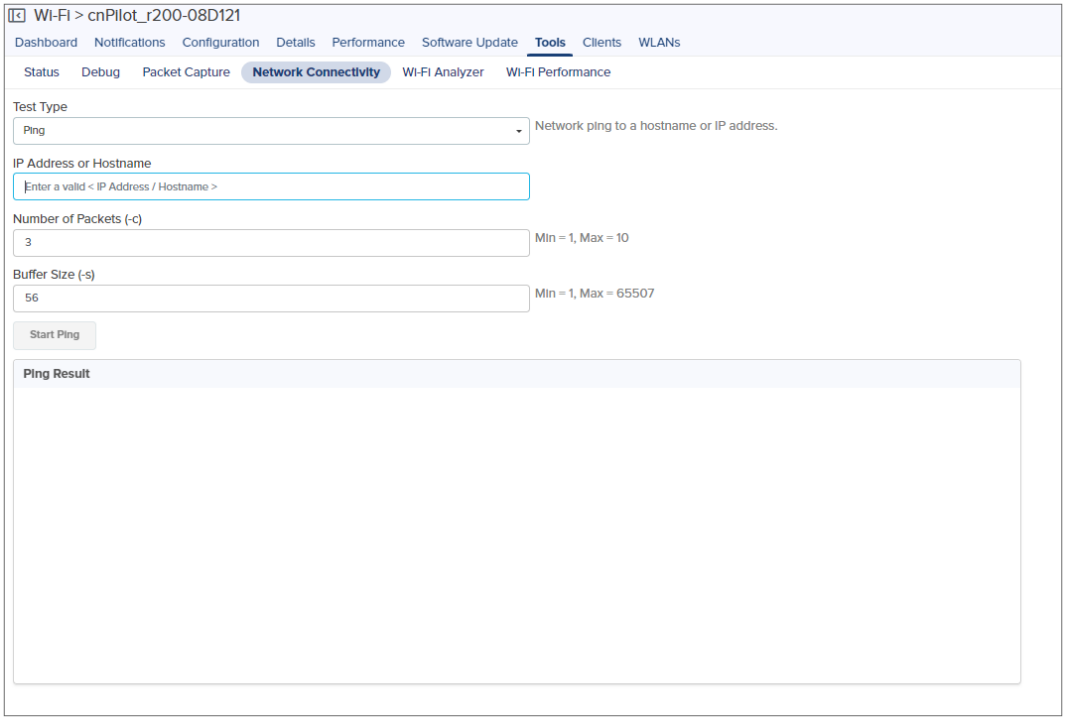
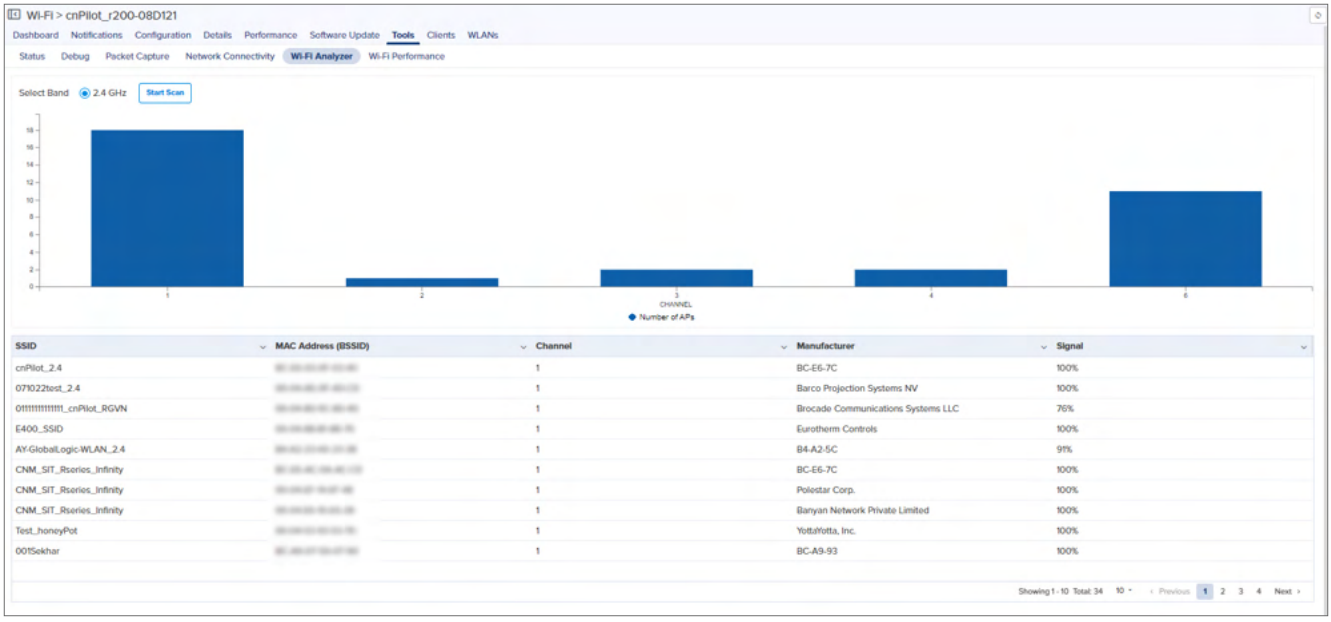


Figure 151 *cnPilot Tools > Network Connectivity*



cnRanger Tools

Note

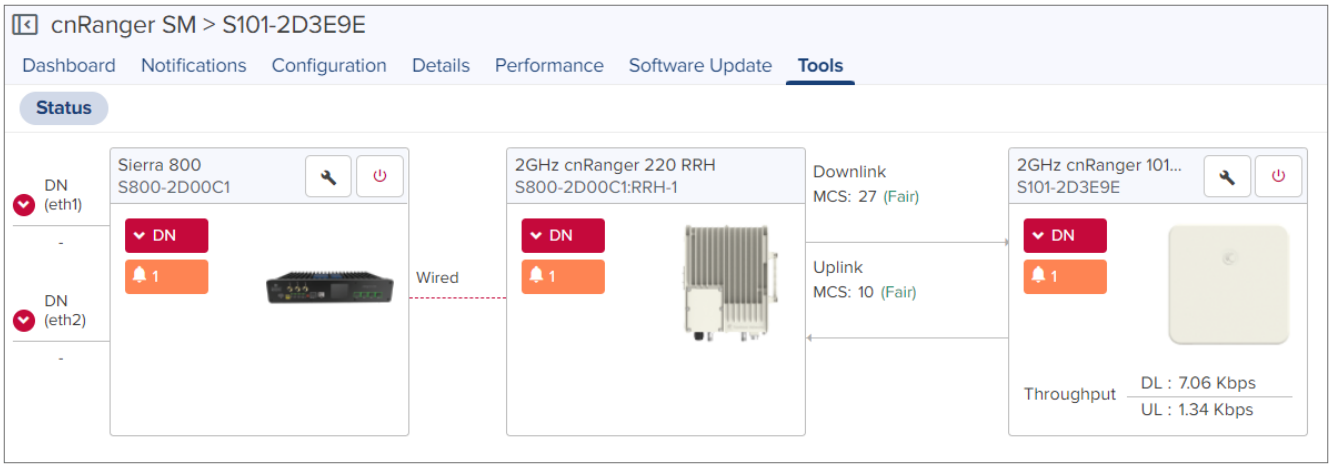
cnMaestro supports the tools page of cnRanger from device version 2.1.0.0-r3.

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.



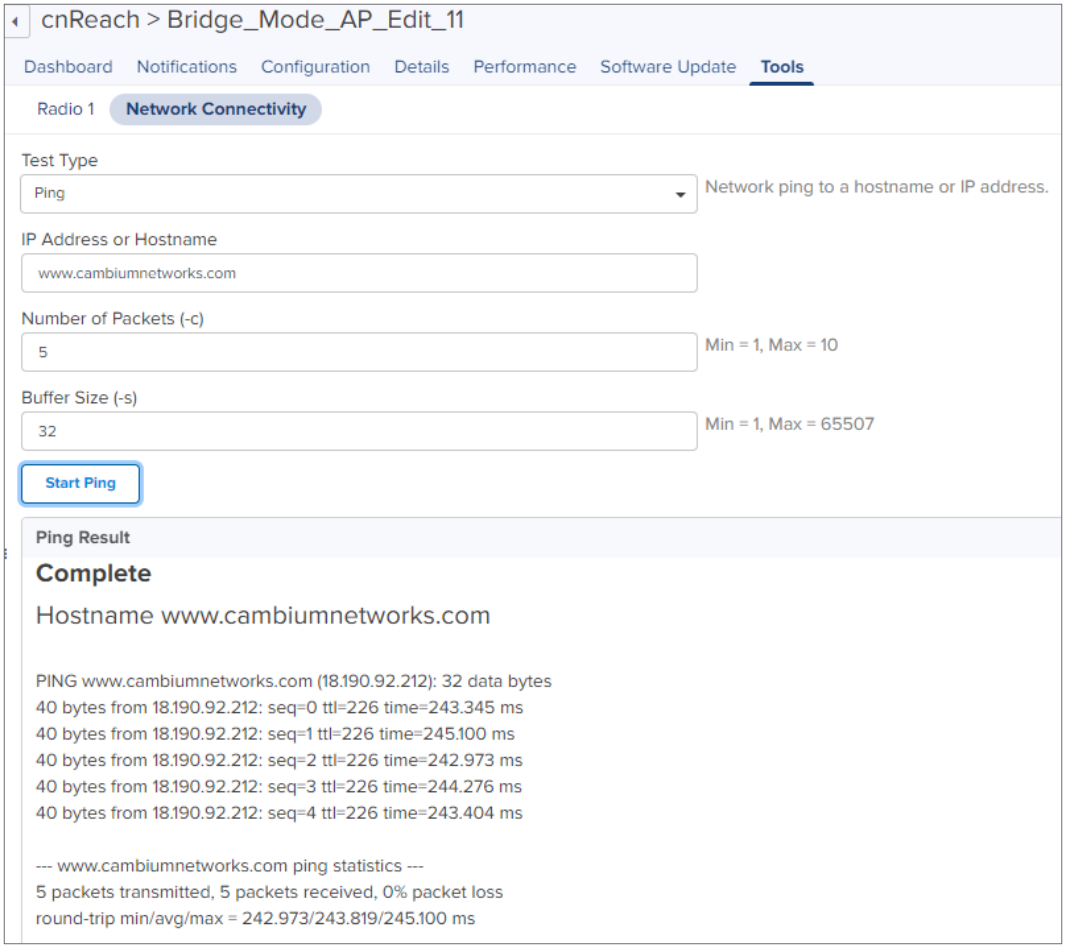
cnReach Tools

The Tools page for cnReach devices consolidates a number of operations into a single troubleshooting interface. The operations are listed below:

Table 39 *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 152 *cnReach Tools*



cnVision Tools

The Tools page for cnVision devices consolidates a number of operations into a single troubleshooting interface. The operations are listed below:

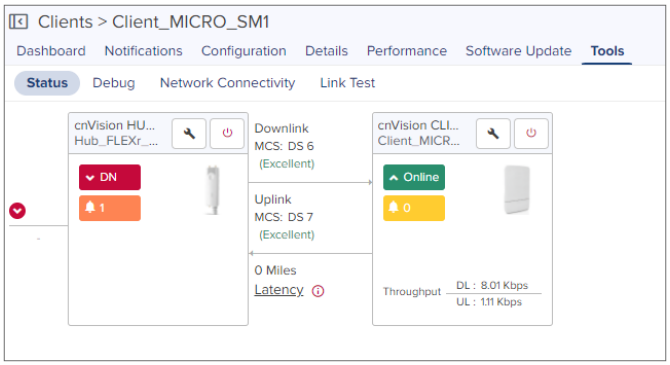
Table 40 *cnVision Tools*

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	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. 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.

Table 40 *cnVision Tools*

Field	Description
	• If cnVision Hub is selected you can choose the SM from the list and start the test. Displays the following fields: ○ **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. Displays the following fields: ○ **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 153 *cnVision Tools*



Edge Controller Tools

In Edge Controller **Tools** tab you can view Operations, Diagnostics, and Services. Refer to Edge Controller Tools.

Enterprise Wi-Fi Tools

The Tools page for Enterprise Wi-Fi devices consolidates a number of operations into a single troubleshooting interface.

The operations of Enterprise Wi-Fi are listed below:

Table 41 *Enterprise Wi-Fi Tools*

Tools	Description
Debug	Displays the log details.
Flash LEDs (Only for E Series Device)	Identifies the device.
Network Connectivity	Executes Ping, DNS, or Traceroute tests.
Packet Capture	Lists packet capture details. **Note** When AP packet capture is configured for 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.
Remote CLI	Enter CLI command in the command text box to execute on device. • 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 (wifiperf)	Wi-Fi performance measures the backhaul speed across devices with respect to cnMaestro.

Figure 154 *Enterprise Wi-Fi Tools*

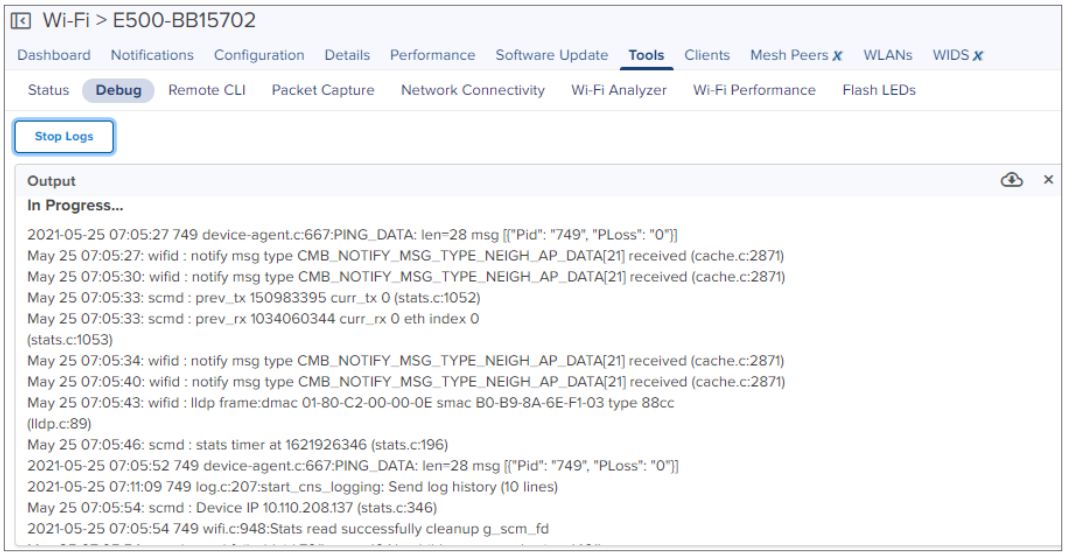


Figure 155 *Enterprise Wi-Fi Packet Capture*

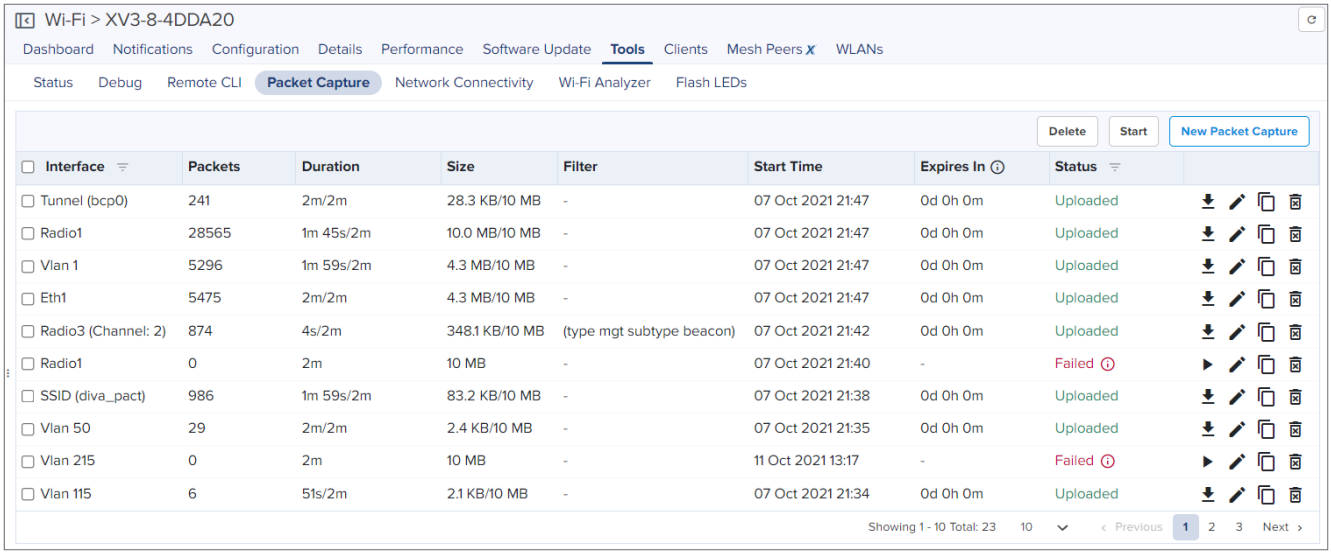


Figure 156 *Enterprise Wi-Fi Remote CLI Tools*

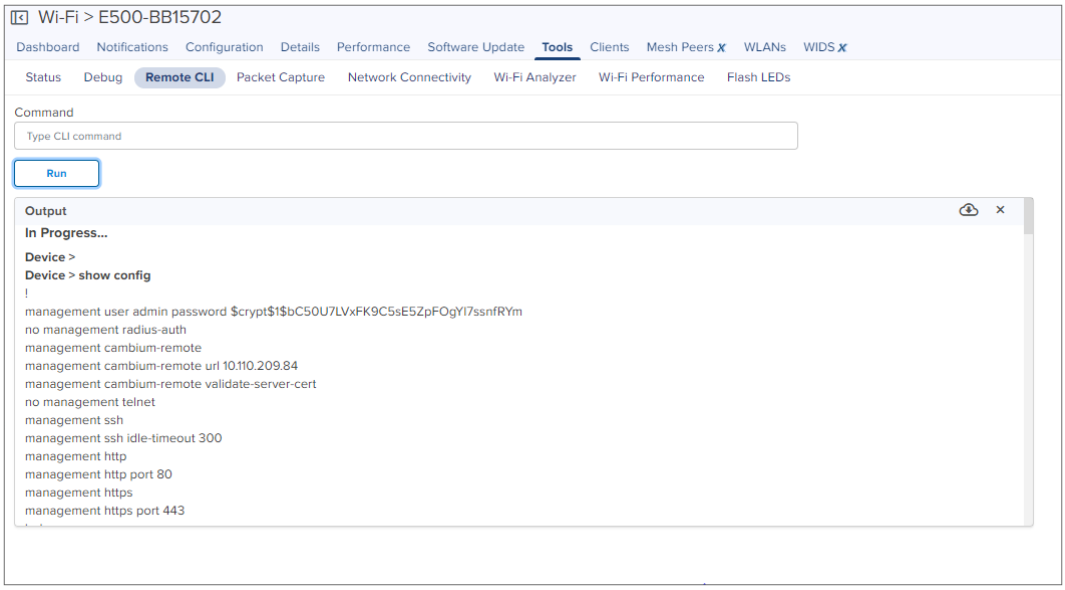


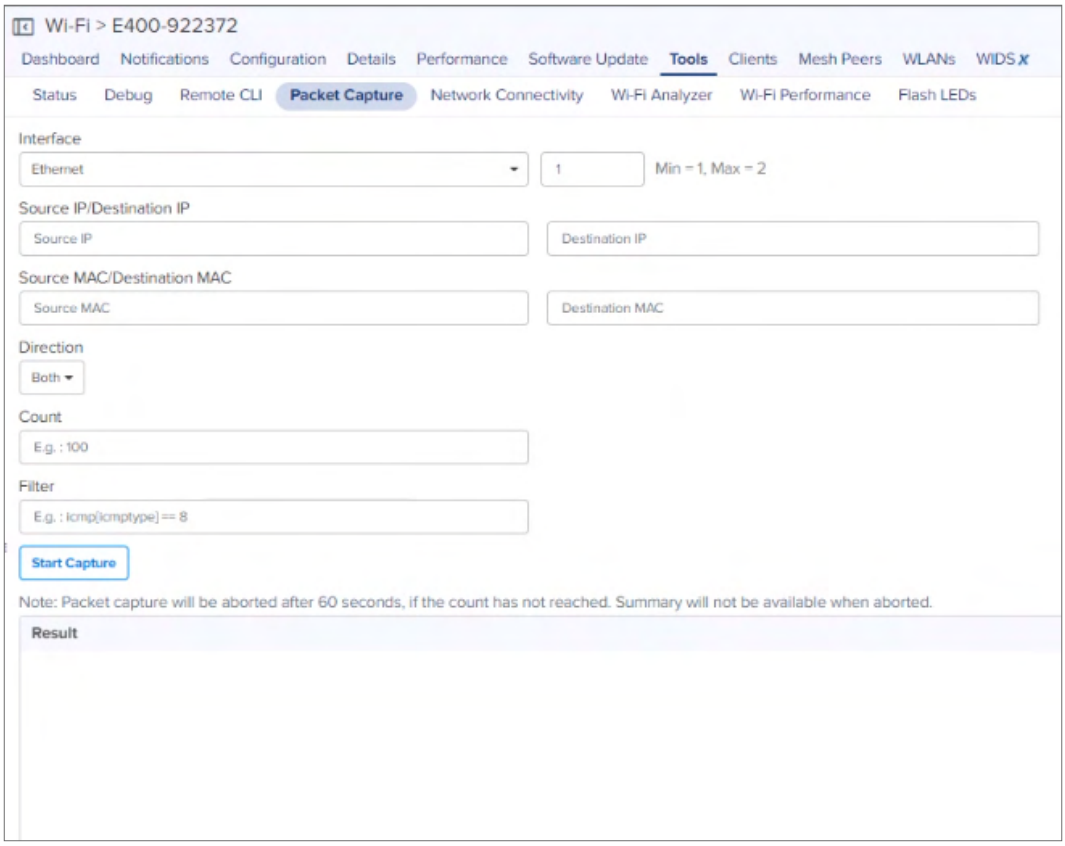
Figure 157 *Flash LEDs*

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.



To view Packet Capture, navigate to **Network** or **Site** > **Wi-Fi AP** > **Tools** > **Packet Capture**.

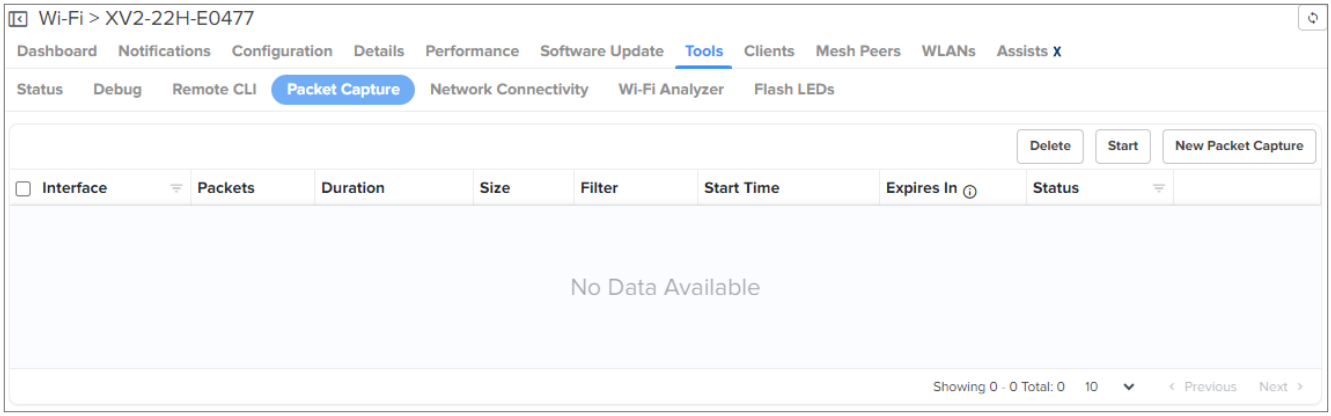


Table 42 *Packet Capture fields*

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: • BRIDGE • Ethernet • PPPoE

Table 42 *Packet Capture fields*

Field	Description
	• 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: • Aborted • Failed • Queued • Skipped

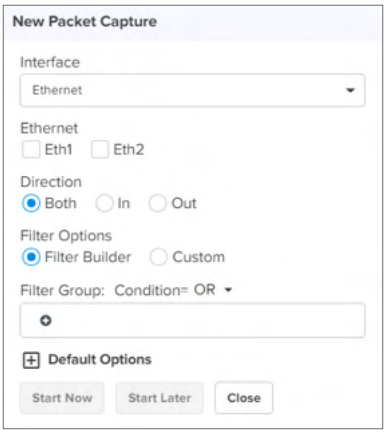
Configuring a new packet capture

Perform the following steps to start a new packet capture:

Note

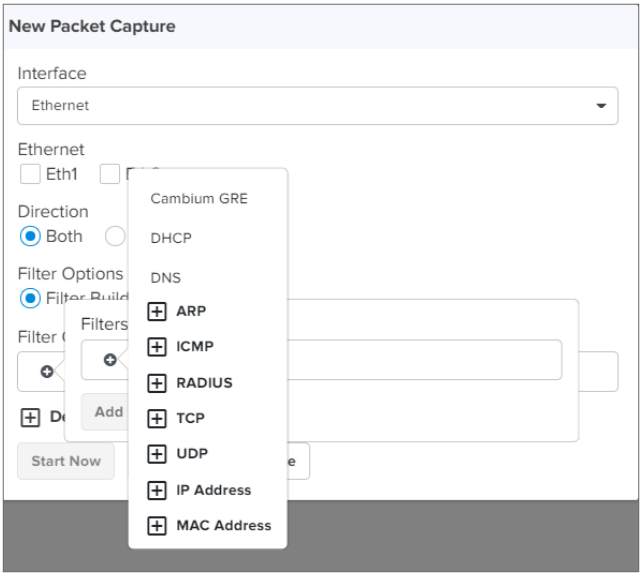
- Filter options vary for different interfaces (Radio, Wireless LAN, VLAN, SSID, TUNNEL, BRIDGE, and PPPoE. Radio, SSID has wireless 802.11 filters, other interfaces has wired 802.3 filters).
- User can also add custom filters if needed.

1. Click **New Packet Capture** to start packet capture**.**



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.

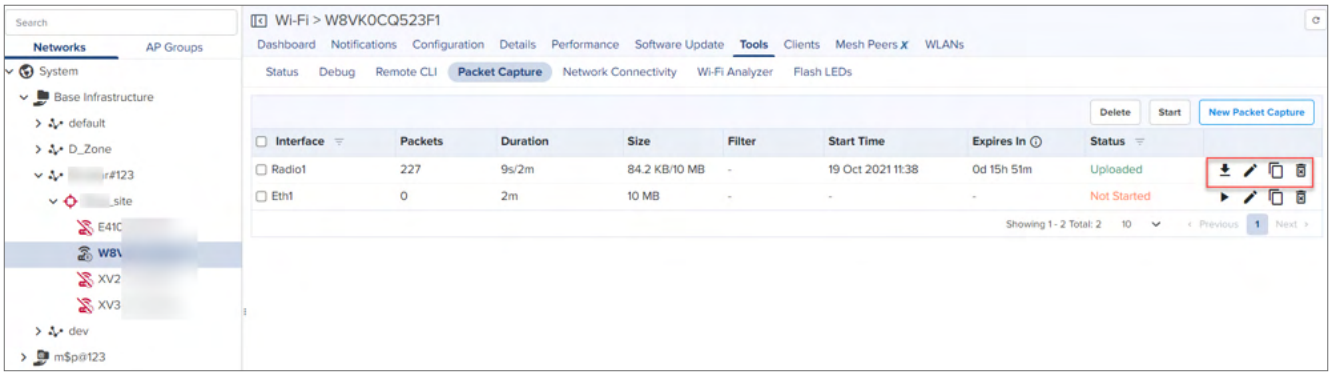


6. Click **Default Options** to configure **Packets**, **Duration**, **Packet Length**, and **File Size**.

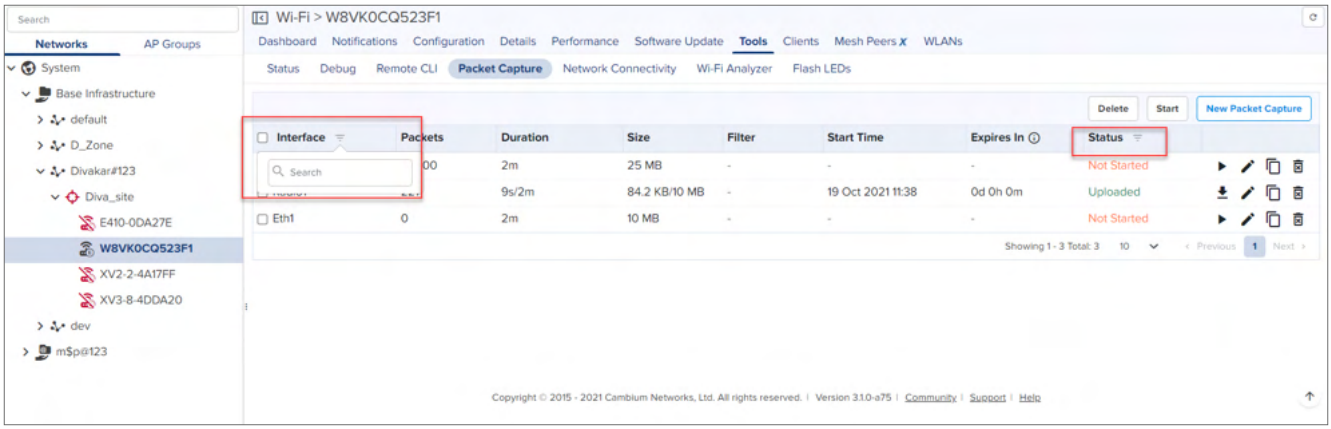
7. Click **Start Now** to capture the packets immediately, or start the capture later by selecting **Start Later** option. The progress of packets captured can be seen in the **Status** field.
8. Click the download (⬇) icon to download the capture in **PCAP** file format.

> **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.



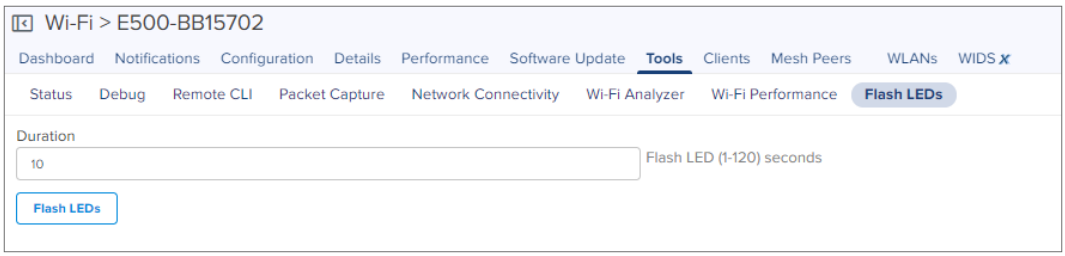
The user can search the packet capture by **Interface** type and **Status.**



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 158 *Flash LEDs*

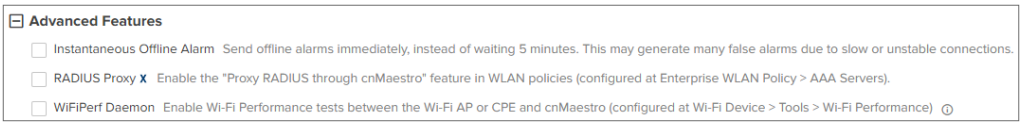


Wi-Fi Performance Test

Wi-Fi Performance Test is supported only on cnPilot devices. Wi-Fi Performance Test will be triggered between the AP and a Wi-FiPerf Endpoint.

Wi-FiPerf Endpoint can be the cnMaestro instance or a locally installed speed test server.

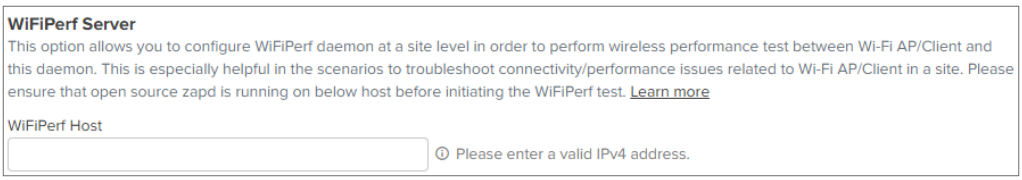
- **cnMaestro Instance:** To enable Wi-Fi performance test, navigate to **Administration > Settings > Advanced Features** page and enable **WiFiPerf Daemon** option.



- **Locally installed Wi-Fi Performance Server**: Wifiperf inter-operates with the open source zapwireless tool. (https://code.google.com/archive/p/zapwireless/). This tool should be installed on a host at the site. It is especially helpful for troubleshooting connectivity/performance issues related to Wi-Fi AP/Client at site.

  To configure locally-installed Site-level speed test server on cnMaestro, perform the following:

  Navigate to **Site** > **Configuration** > **WifiPerf Server**.



Note

- The WiFiPerf manager running on cnMaestro establishes a control session with the AP (and the peer endpoint) using TCP port number 18301. It is mandatory both the AP and the peer endpoint are reachable from cnMaestro. Make sure the NAT/firewall does not block the wifiperf traffic from cnMaestro to any endpoint or AP (also between the endpoints and AP). Ensure the port number 18301 is not blocked in the network for TCP and UDP.
- For more details on Wi-Fi performance (WiFiPerf) feature, refer here.

Performing the Wi-Fi performance test

To run the Wi-Fi performance test, navigate to **Tools > Wi-Fi Performance** page. It can be used to measure the following parameters with intervals of 10, 20 and 30 seconds:

- **Traffic Types**
  - TCP
  - UDP
- **Traffic Direction**
  - Downlink
  - Uplink
- **WiFiPerf Endpoint**
  - cnMaestro
  - WiFi Perf Local Host

ePMP Tools

The Tools page for ePMP devices consolidates a number of operations into a single troubleshooting interface. The operations are listed below:

Table 43 *ePMP Tools*

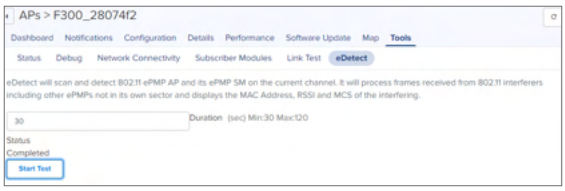
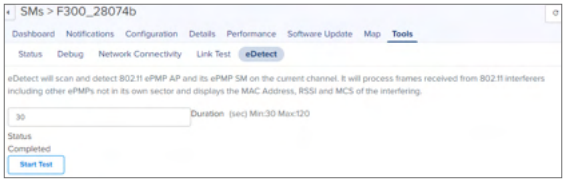
Field	Description
Debug	Displays the log details.
eDetect	eDetect is supported on the ePMP AP or SM. It is also launched from the Tools tab. The eDetect tool (not available in ePMP Master/Slave mode) is used to measure the 802.11 interference at the ePMP radio or system when run from the AP or the SM, on the current operating channel. When the tool is run, the ePMP device processes all frames received from devices not connected to the ePMP system and collects the interfering frame's information such as MAC Address, RSSI, and MCS. Configure the duration for which the AP scans for interference.  Configure the duration for which the SM scans for interference. 
Link Test	The Link Capacity Test measures the throughput of the RF link between two ePMP modules. ePMP 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. Displays the link related test result with respect to Throughput. Link Test can be performed on the ePMP AP and its SM link. In order to run this operation, select the device and then the **Tools** tab. • If an ePMP AP is selected, choose the SM from the list and start the test. Displays the following fields: ○ **Packet Size**: Choose the Packet Size to use for the throughput test.

Table 43 *ePMP Tools*

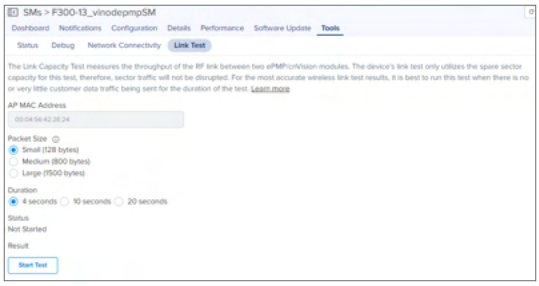
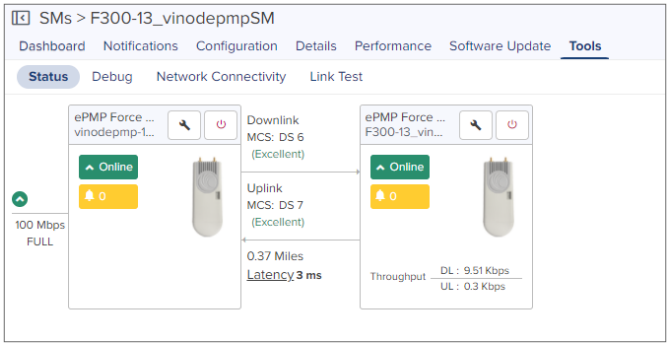
Field	Description
	◦ **Duration**: Choose the time duration in seconds to use for the throughput test. • If an ePMP SM is selected, click Start Test to run the link test.  Displays the following fields: ◦ **Packet Size**: Choose the Packet Size to use for the throughput test. ◦ **Duration**: Choose the time duration in seconds to use for the throughput test.
Network Connectivity	Executes Ping, DNS, or Traceroute tests.
Status	Displays the status.

Figure 159 *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 44 *PMP Tools*

Field	Description
Debug	Displays the log details.
Link Test	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. The Link Capacity Test tool has the following modes: • **Flood Link Test**: Tests the link's performance by flooding it with heavy traffic and assesses

Table 44 *PMP Tools*

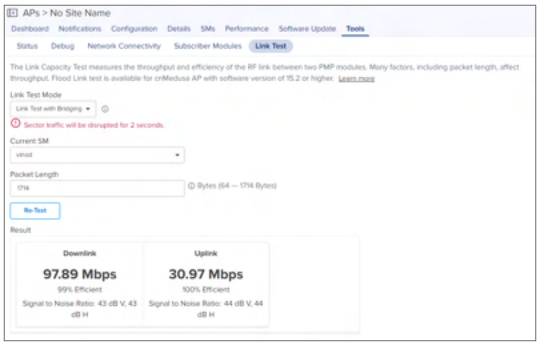
Field	Description
	link's behavior under extreme network loads. An addition **Multiple LUIDs** option is available in the Current SM dropdown list. The Multiple LUIDs feature allows users to specify LUIDs, including single numbers (for example, 23, 32), or to conduct the flood test with ranges (for example, 2-22) as shown in Figure 160. **Figure 160** *Flood Link Test: PMP 450m AP* **Note** **Flood Link Test** is applicable only for 450m APs. • **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 bridged link. • **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. 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. • If a PMP AP is selected you can choose the SM from the list and start the test.  • If a PMP SM is selected, click **Start Test** to run the Link Test.

Table 44 *PMP Tools*

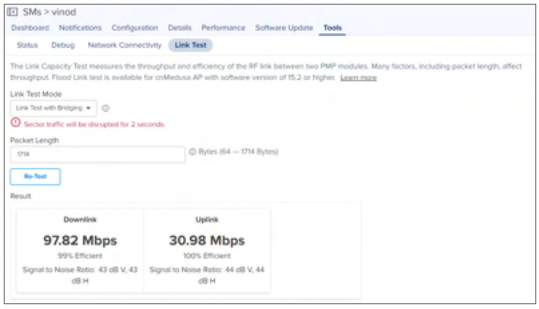
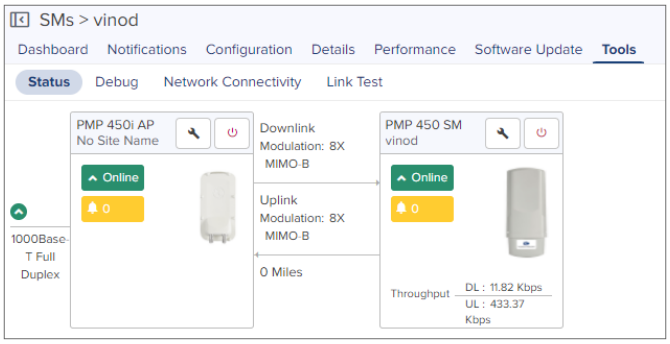
Field	Description
	
Network Connectivity	Executes Ping, DNS, or Traceroute tests.
Status	Displays the status.
Subscriber Modules	Lists all the SMs connected to the selected AP. This is available for PMP APs only.

Figure 161 *PMP Tools*

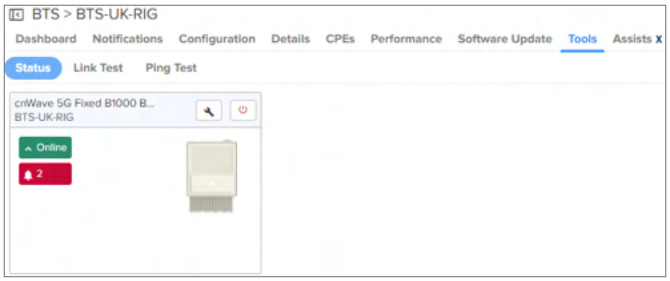


cnWave 5G Fixed Tools

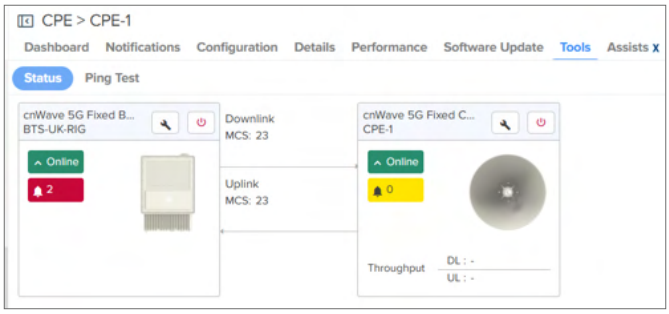
For cnWave 5G Fixed products (BTS and CPE), the **Tools** page in cnMaestro contains the following tabs:

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.



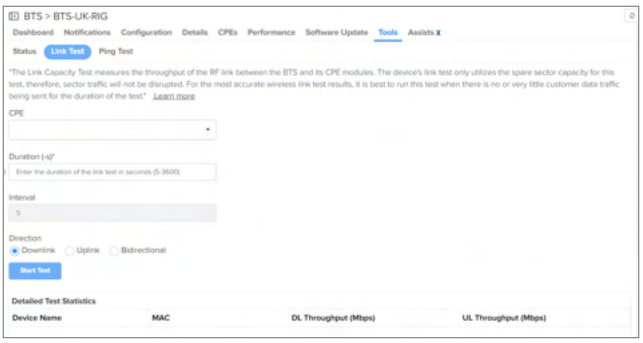
Link Test

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**.



2. Set the parameters, as described in the table below:

Table 45 *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

Table 45 *Parameters on the Link Test page*

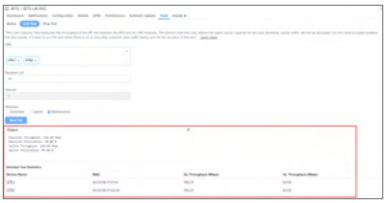
Parameter	Description
	output is updated every 5 seconds. Similarly, if you set a value between 61 and 3600 seconds, the output is updated every 60 seconds.
Direction	Direction of the transmission of the traffic that you want to test. This parameter supports the following options: • Downlink • Uplink • 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.

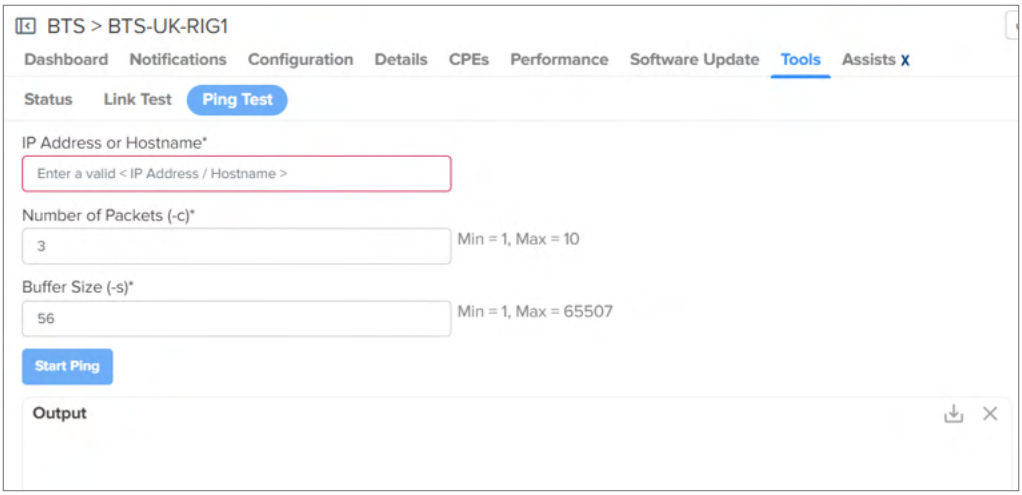
Ping Test

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.



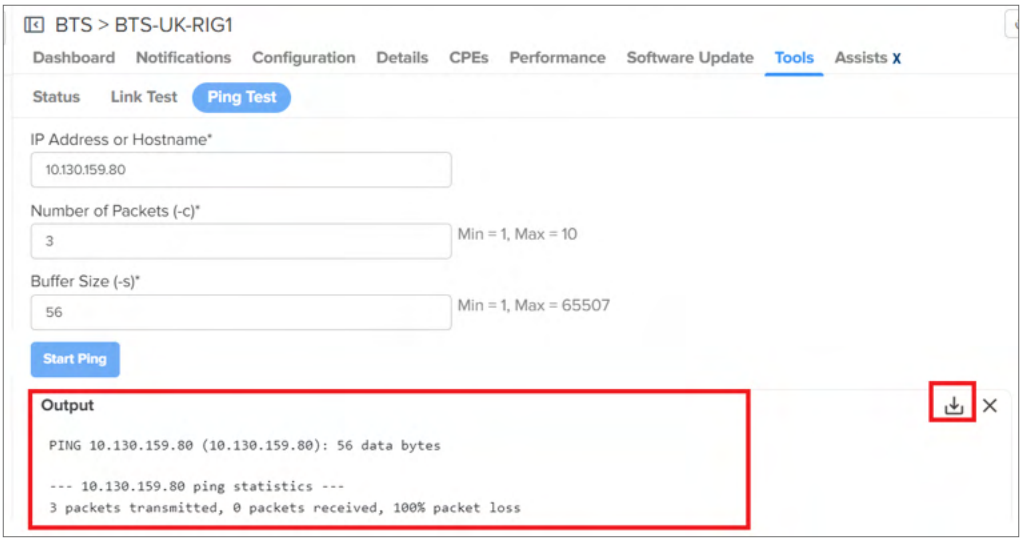
2. Set the parameters, as described in the table below.

Table 46 *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. 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.

Wireless Intrusion Detection System (WIDS)

Note

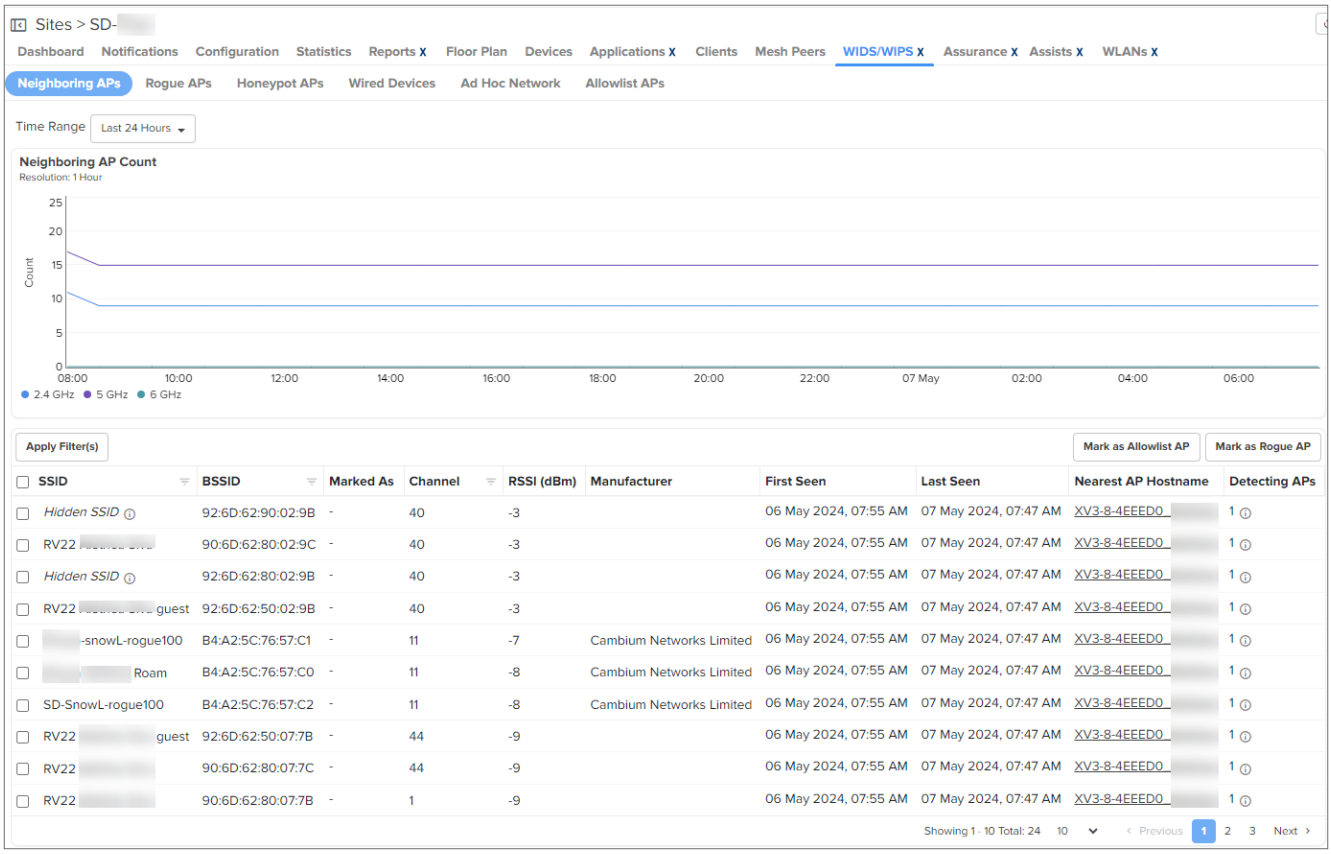
This is a beta feature.

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:

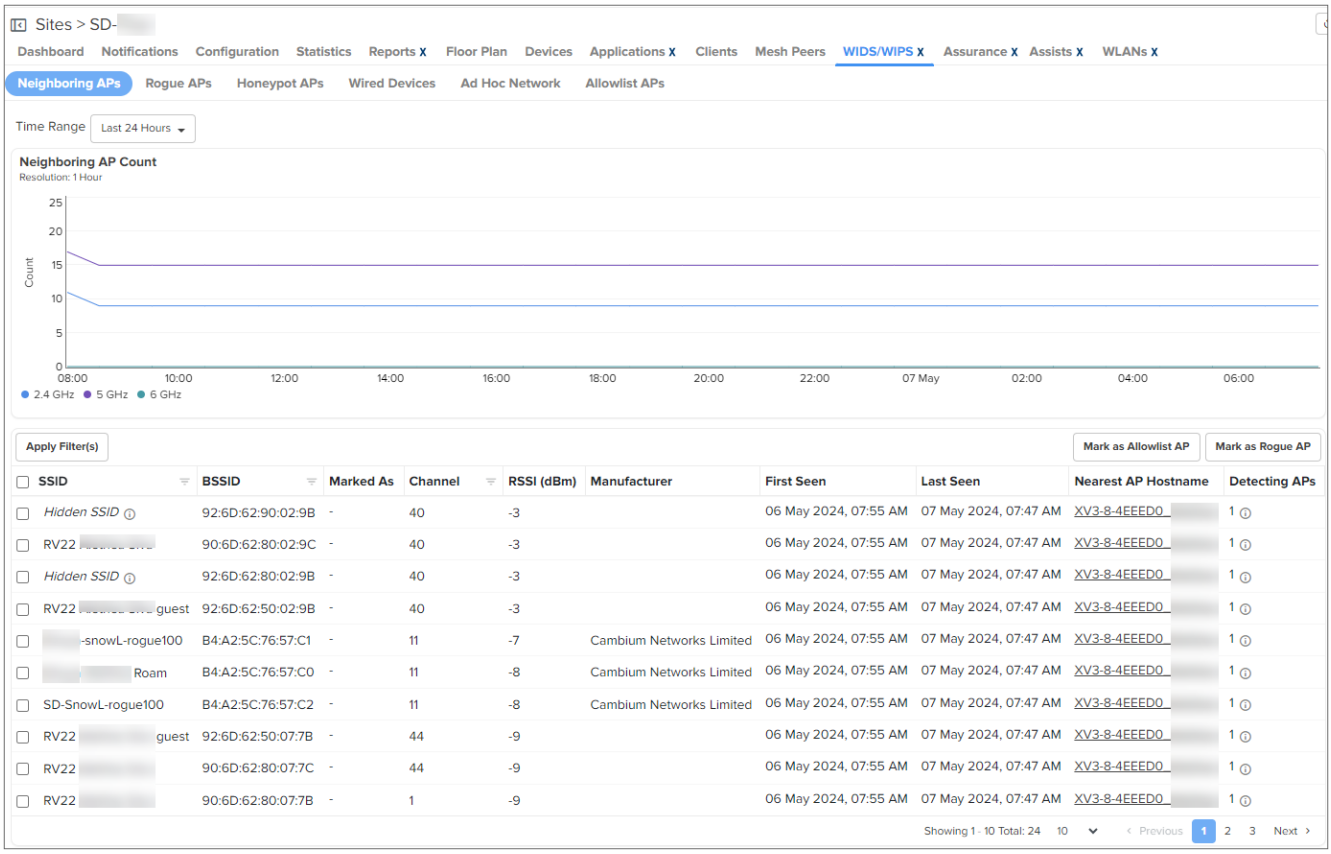
- Neighboring APs
- Rogue APs
- Honeypot APs
- Wired Devices
- Ad Hoc Network
- Allowlist APs

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.

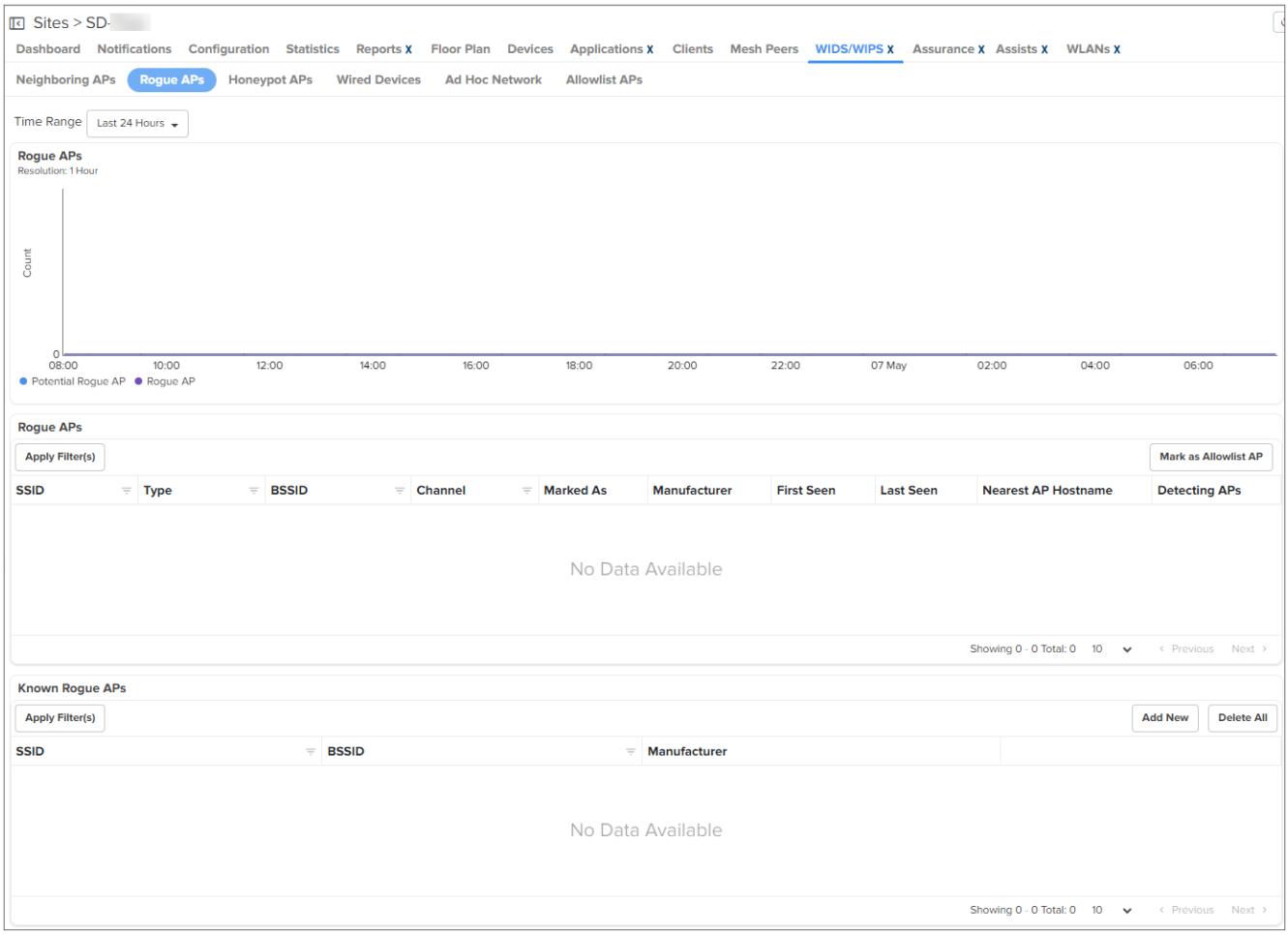
The following Neighboring APs parameters are displayed:

Table 47 *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 48 *Rogue APs parameters*

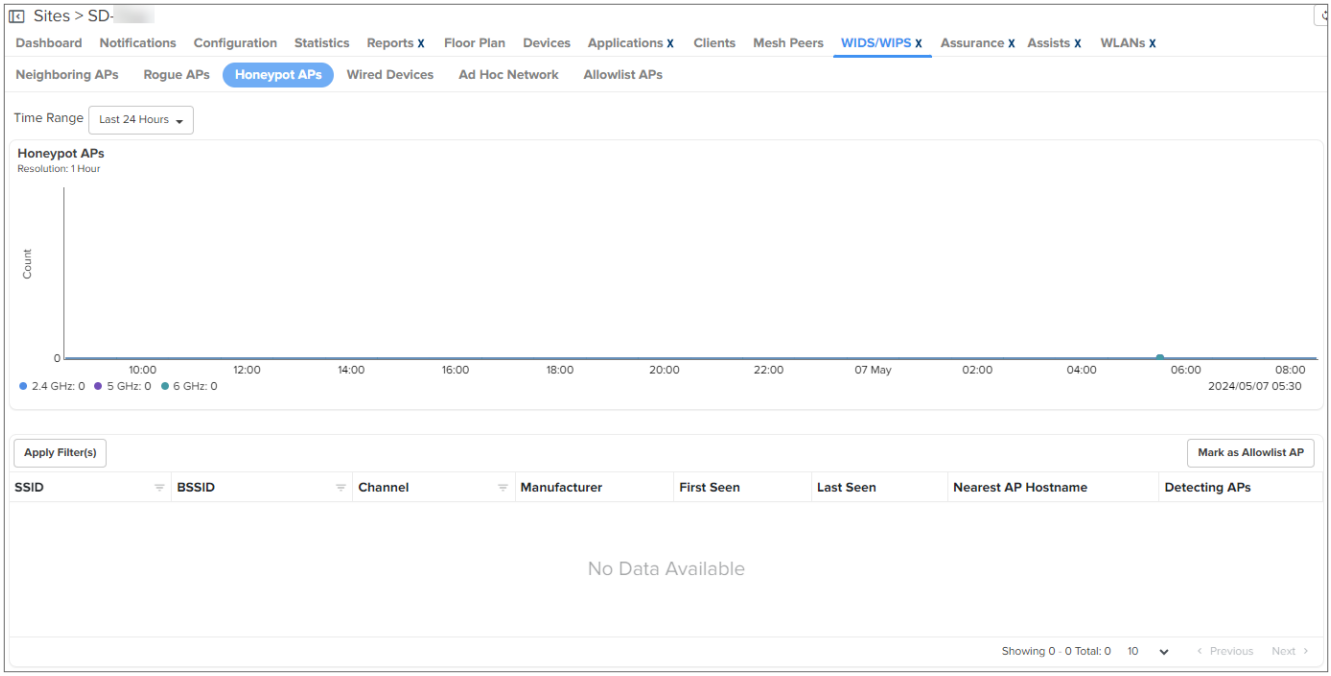
Field	Description
SSID	SSID of the rogue AP.
Type	Indicates the type of the rogue AP. Following are the supported values: • Rogue AP • Potential Rogue AP
BSSID	AP MAC address.
Channel	Channel in which the rogue AP operates.
Marked As	Indicates whether the rogue AP has been marked as an allowlist AP or 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.

Table 48 *Rogue APs parameters*

Field	Description
Last Seen	Time at which the rogue AP was last detected.
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.



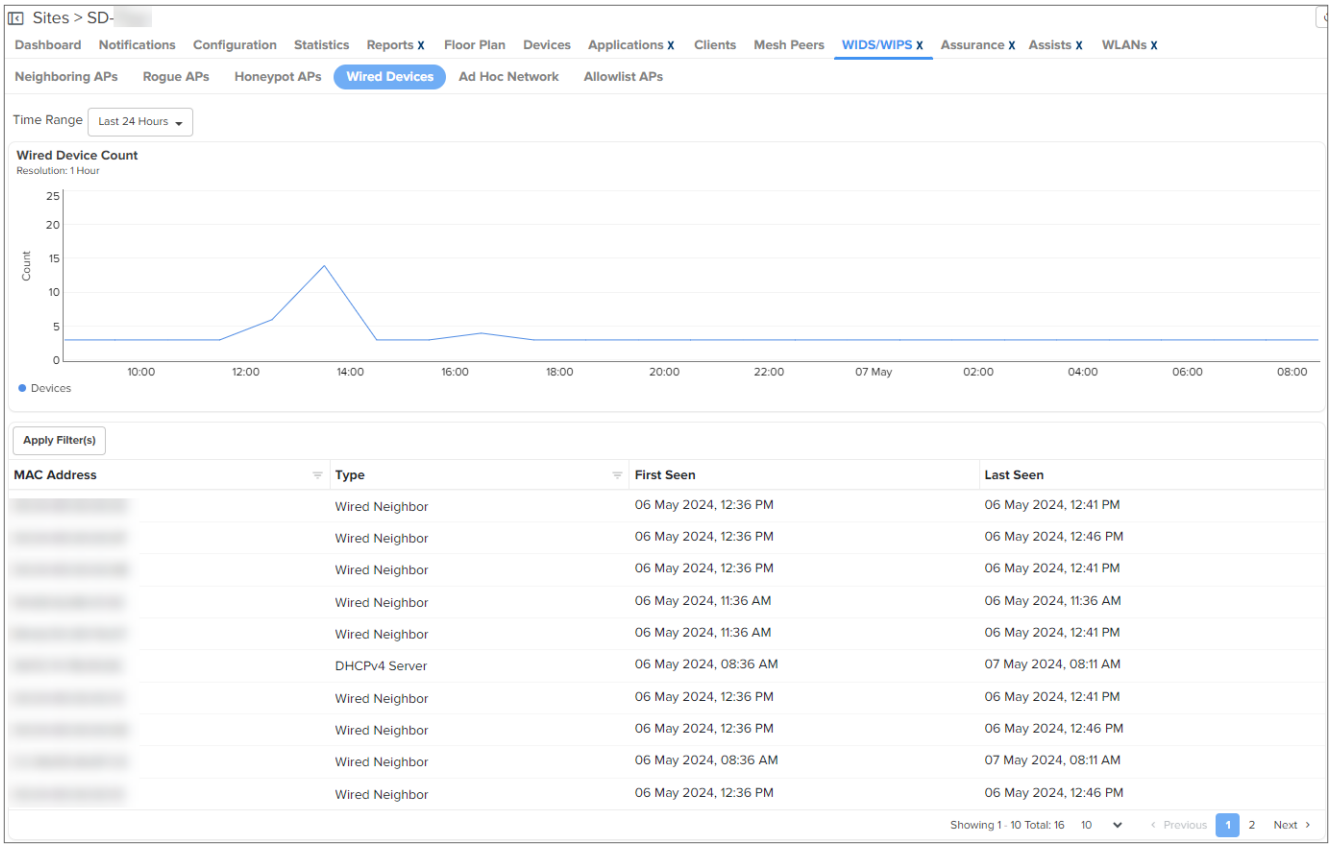
The following parameters related to Honeypot APs are displayed:

Table 49 *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.



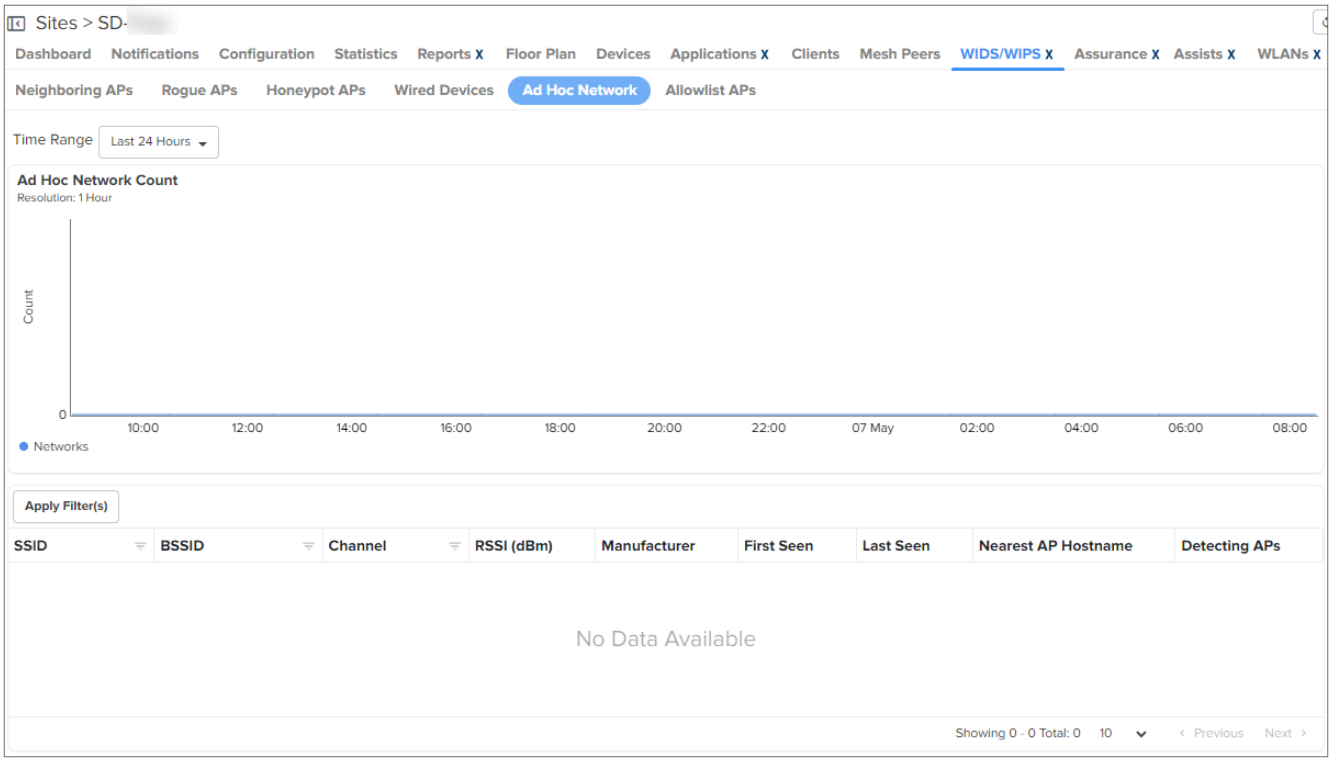
The following parameters related to Wired Devices are displayed:

Table 50 *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 51 *Ad Hoc Networks parameters*

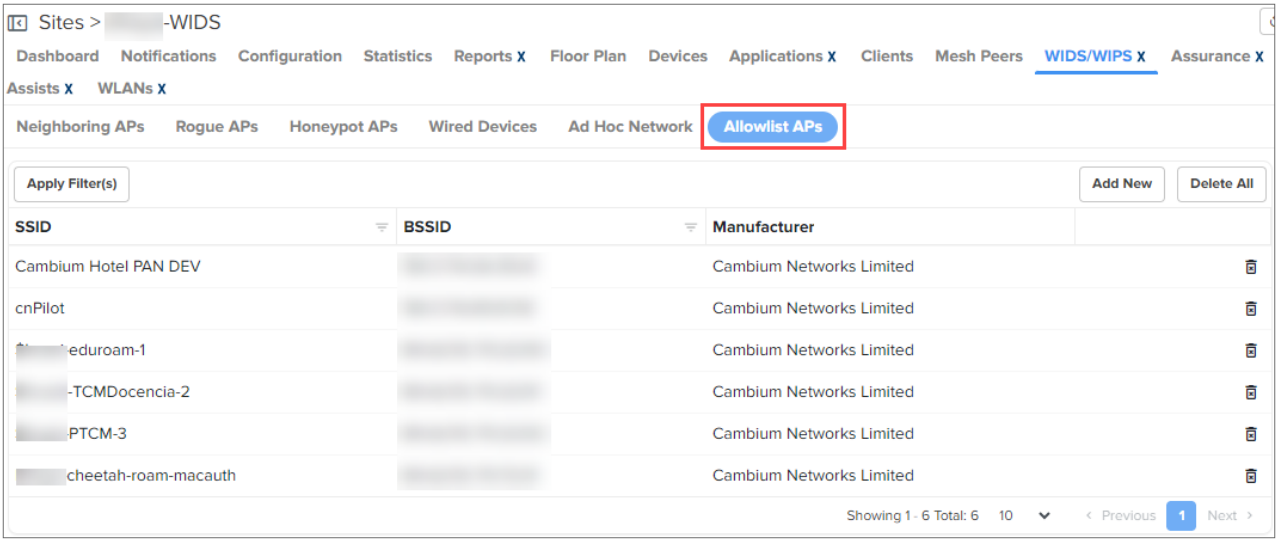
Field	Description
SSID	The name of the ad hoc wireless network.
BSSID	The MAC address of the ad hoc network.
Channel	The radio frequency channel on which the ad hoc network operates.
RSSI (dBm)	The received signal strength indication, measured in decibels relative to one milliwatt (dBm), of the ad hoc 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

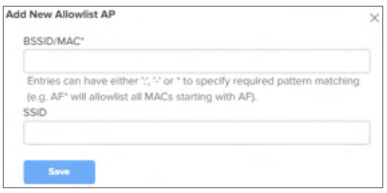
Allowlist APs allow administrators to configure the SSID and MAC addresses of authorized access points, providing control over permitted devices in the network infrastructure.

To add Allowlist APs, follow these steps:

1. Navigate to **WIDS** > **Allowlist APs**.



2. Click **Add New**. The **Add New Allowlist AP** windows appears.



3. Enter the **BSSID/MAC** address.
4. Enter **SSID.**
5. Click **Save**.

The following parameters related to Whiteilist APs are displayed:

Table 52 *Allowlist APs parameters*

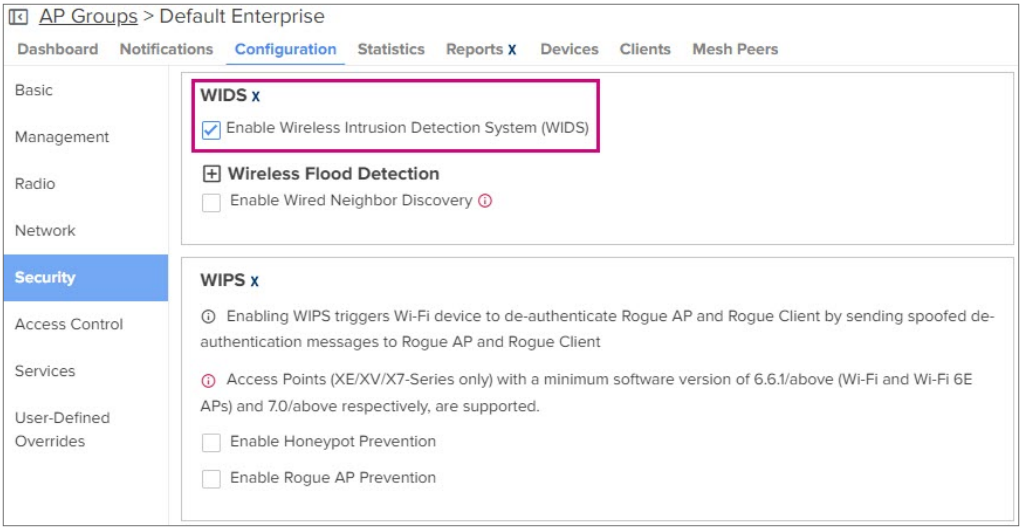
Field	Description
SSID	The name of the wireless network.
BSSID	The MAC address of the AP.
Manufacturer	The manufacturer of the AP.
Delete All	Allows to delete all Allowlist APs in the list.

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.

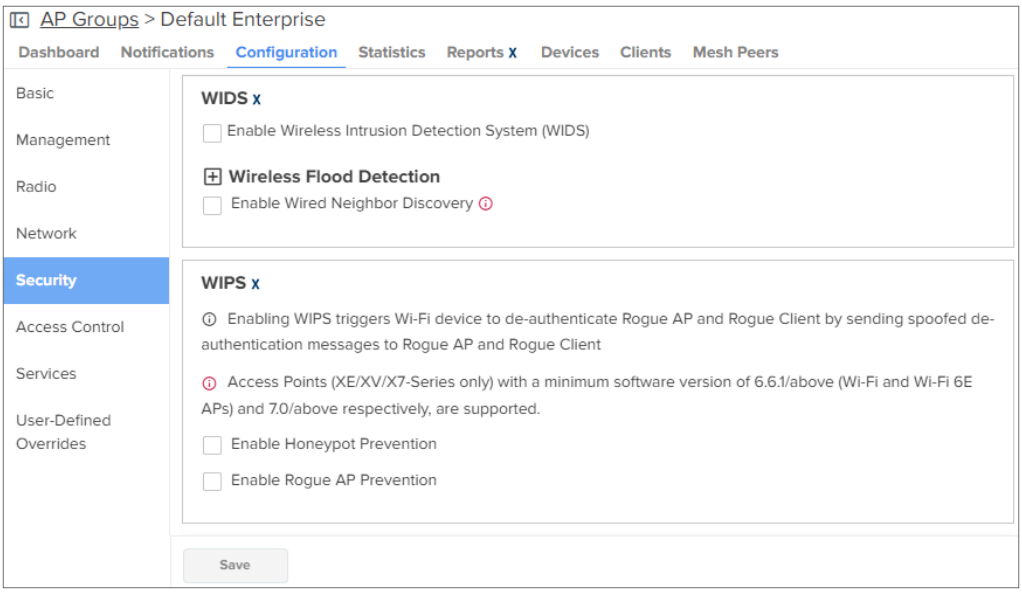
3. Select the **Enable Wireless Intrusion Detection System (WIDS)** checkbox.



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.



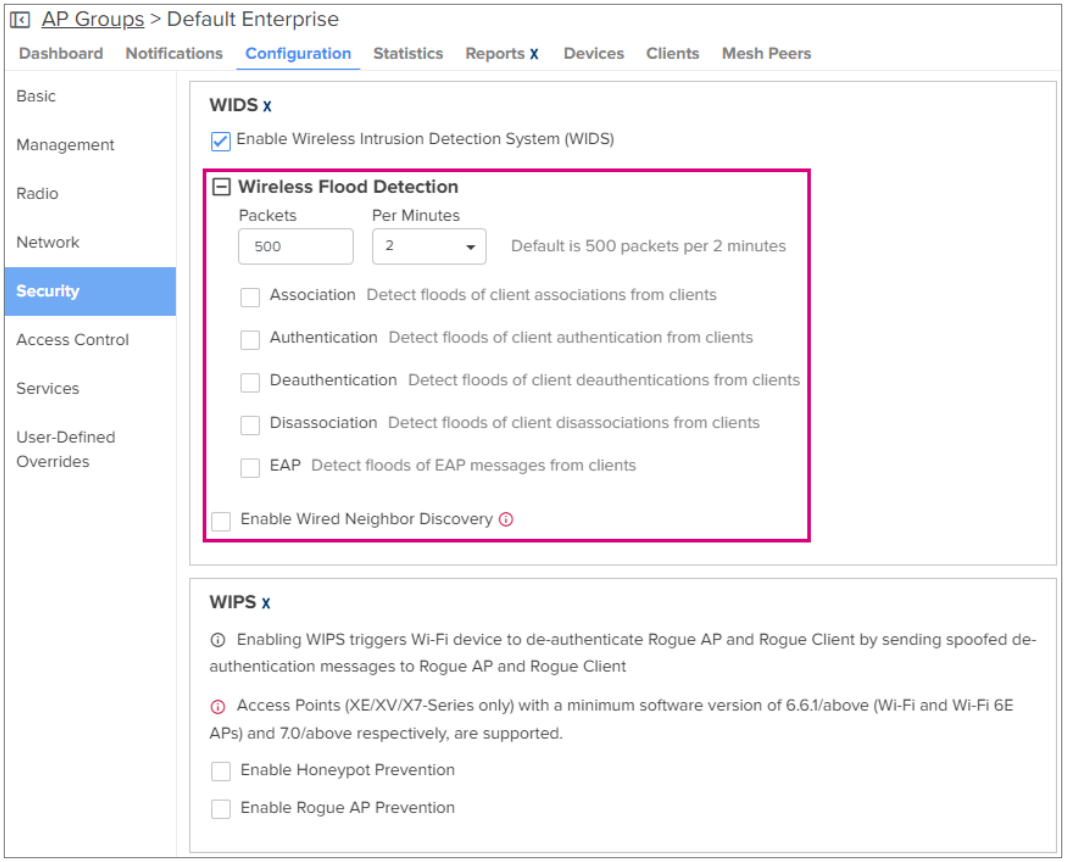
Wireless Flood Detection

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.



Wireless Flood Detection displays the following parameters:

Table 53 *Wireless Flood Detection parameters*

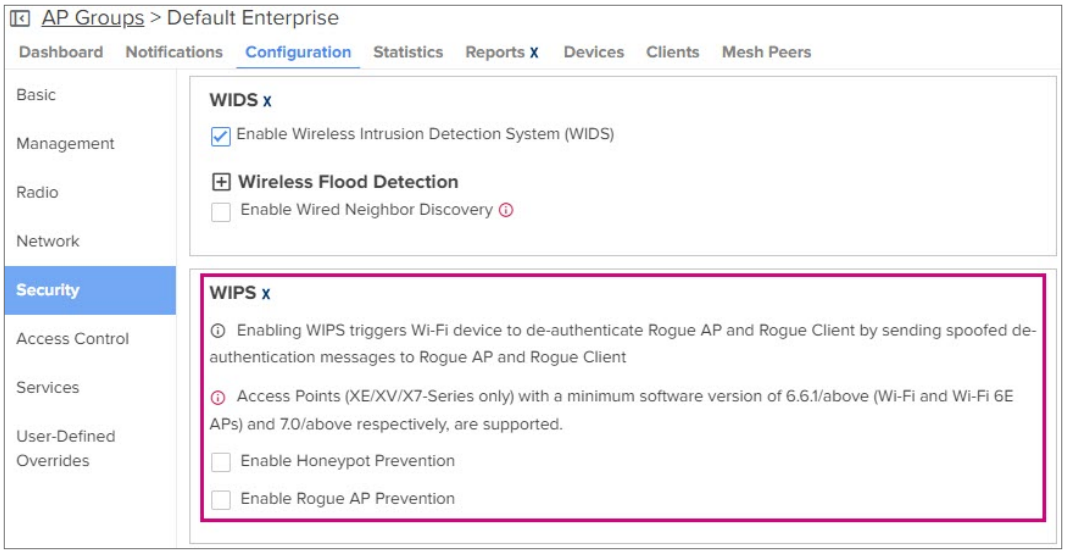
Field	Description
Association	Detect floods of client associations from clients.
Authentication	Detect floods of client authentication from clients.
Deauthentication	Detect floods of client deauthentications from clients.
Disassociation	Detect floods of client disassociations from clients.
EAP	Detect 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.



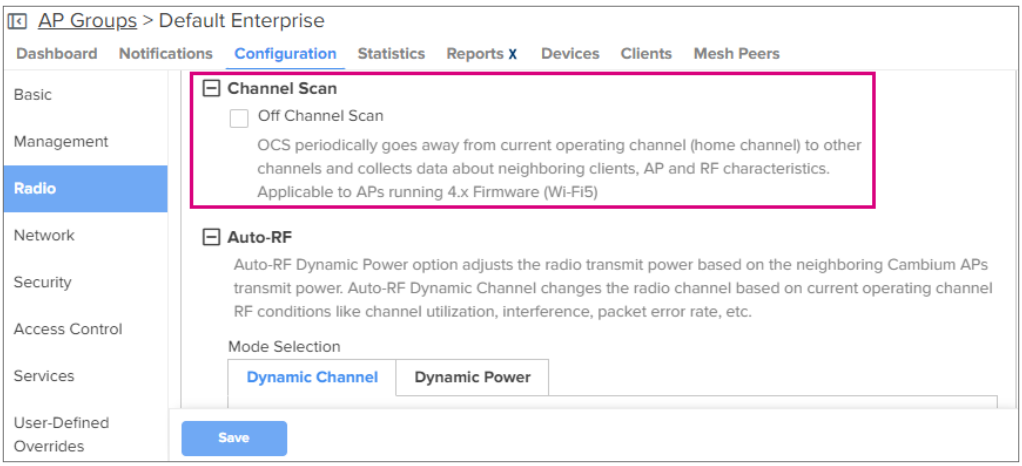
Off Channel Scan (OCS)

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.



3. Click **Save**.

PMP Dashboard

The PMP dashboard displays **Status**, **Connected SMs**, **Throughput**, **Frame Utilization**, **Alarms**, **Device Health**, **Access Point Details**, **Assists**, **Spectrum Analyzer Last Scan**, **Noise Floor**, and **Radio Details**.

Figure 162 *PMP 450 AP/BHM dashboard*

Multiple Component Carrier (CC) Support in PMP 450v

Note:

Multiple CC support is available starting with PMP version 24.2.2 and later.

cnMaestro supports displaying multiple CCs for the PMP 450v devices across various pages such as dashboards, performance, details, device map view, and in **Spectrum Analyzer** page > **Add New** > **Add Spectrum Scan** view displays the multiple frequency. Both the AP and SM can use multiple CCs simultaneously.

The PMP 450v 4x4 supports two component carriers with software 24.2.2 and up to three component carriers with software 25.0, each up to 40MHz wide. The PMP 450v 2x2 supports up to two component carriers, each up to 40MHz wide. the platform is sold as a 2x2 SM or a 2x2 PTP.

The platform is available in 3 models:

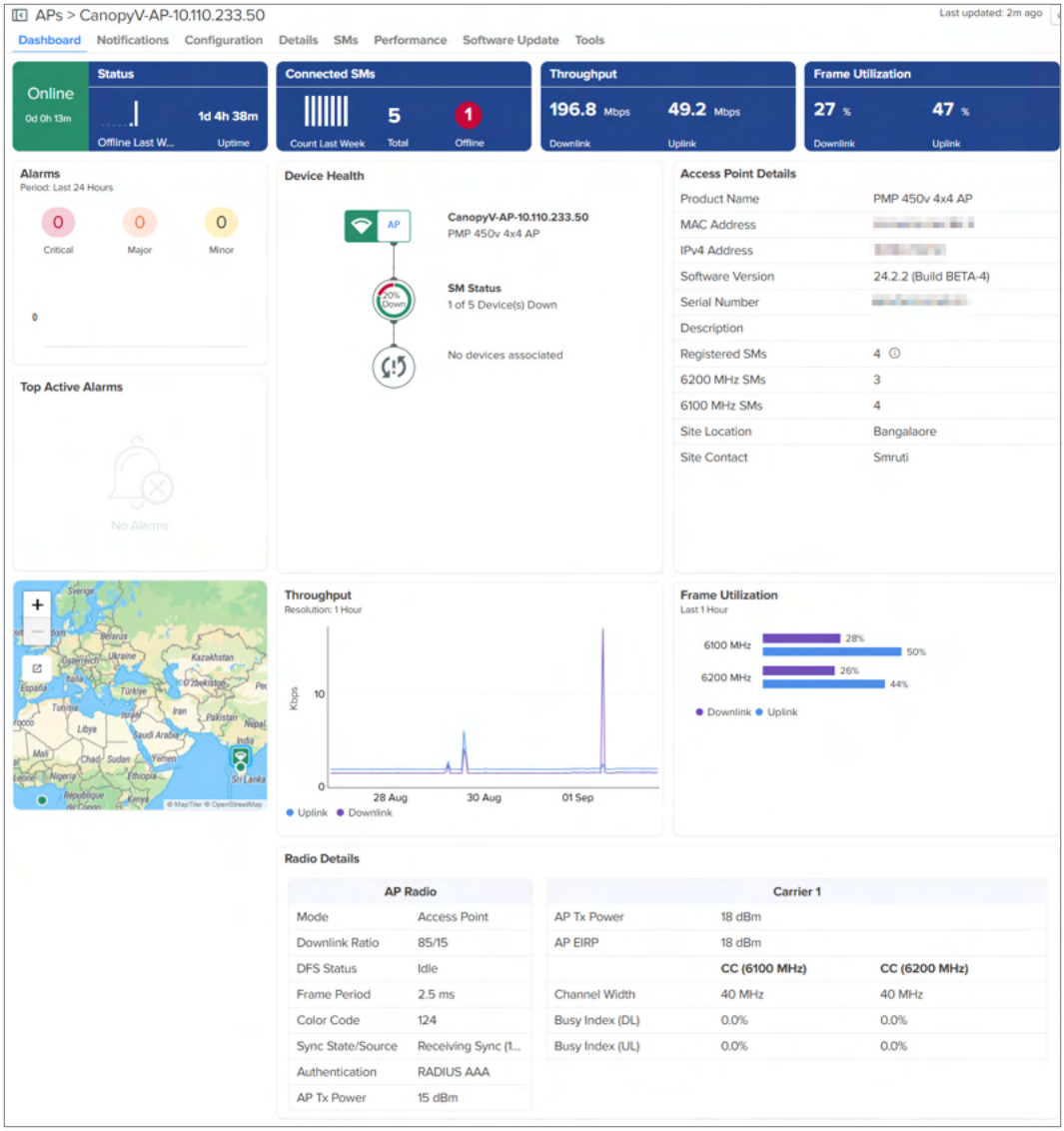
- 4x4 AP
- 4x4 SM
- 4x4 PTP

For more details about the difference between Carriers and CCs, refer to Configuring Radio Parameters in the PMP 450 Series Configuration Guide.

PMP 450v 4×4 AP/BHM dashboard

The PMP 450v 4×4 AP/BHM dashboard displays the parameters such as **Status**, **Connected SMs**, **Throughput**, **Frame Utilization**, **Alarms**, **Device Health**, **Access Point Details**, **Radio Details**, **Carrier,** and **Component Carrier (CC)** information.

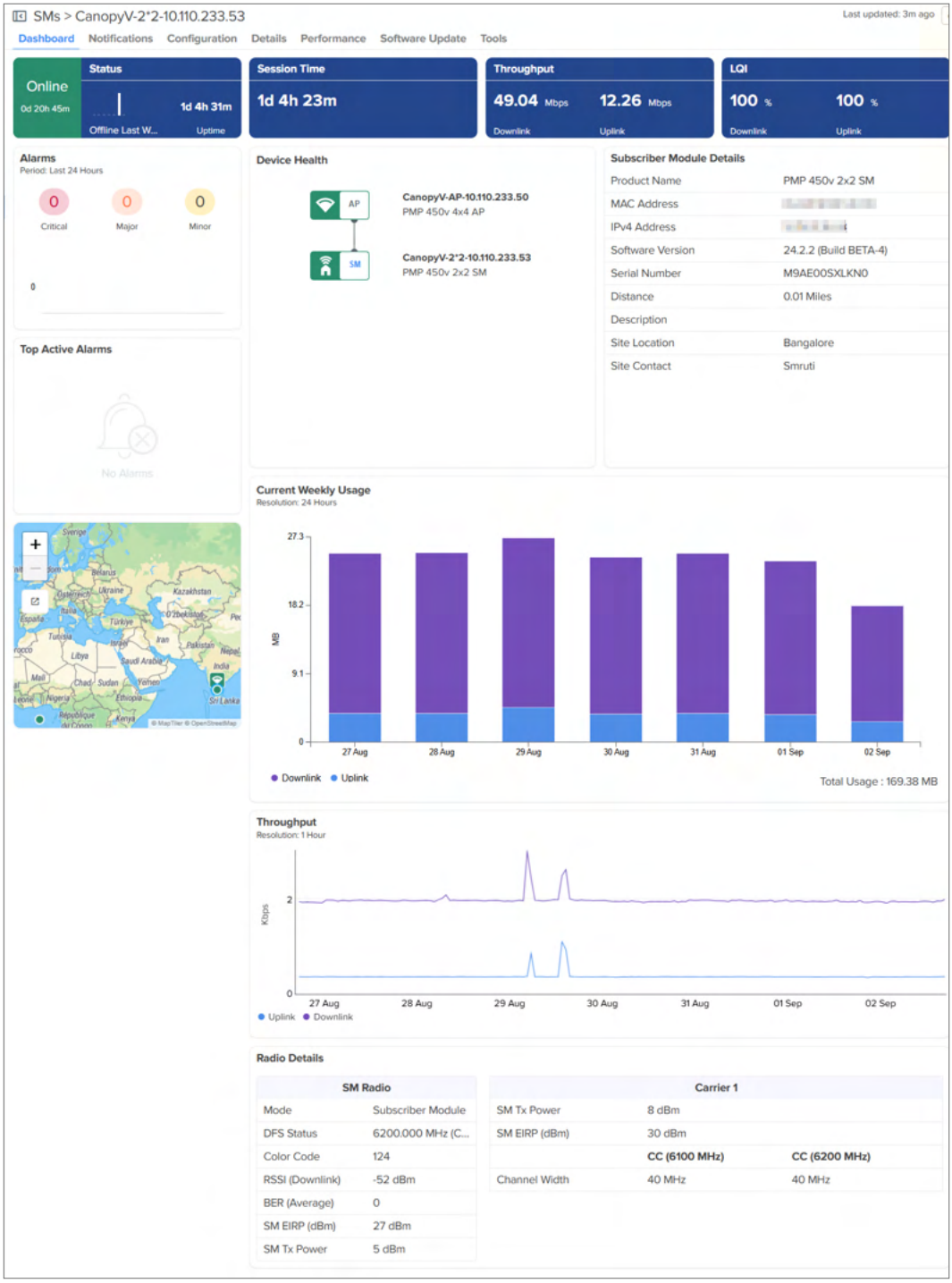
Figure 163 *PMP 450v 4 x 4 AP/BHM dashboard*



PMP 450v 4×4 SM/BHS and PMP 450v 2×2 SM/BHS dashboard

The PMP 450v (4×4 SM/BHS and 2×2 SM/BHS) dashboard displays the parameters such as **Status**, **Session Time**, **ThroughputLQI**, **Alarms**, **Device Health**, **Subscriber Module Details**, **Current Weekly Usage**, **Radio Details**, and **Carrier,** information.

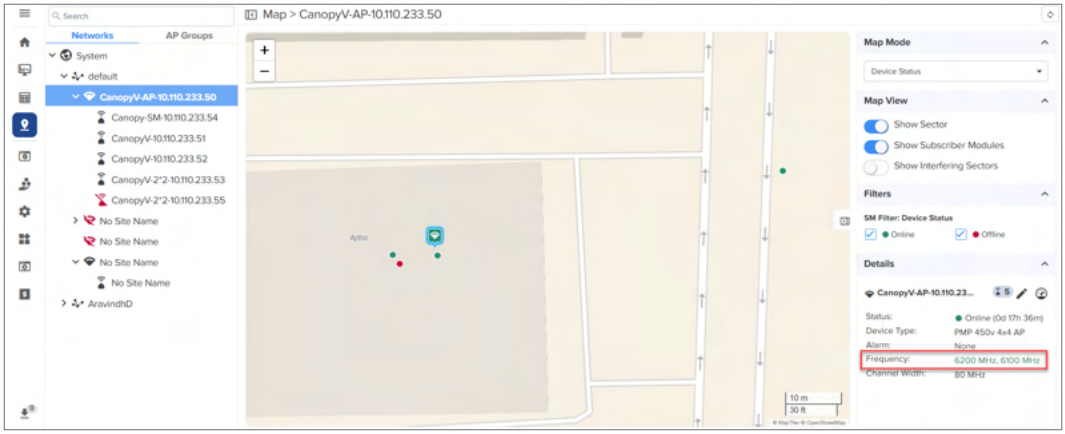
Figure 164 *PMP 450v 4×4 SM/BHS and PMP 450v 2×2 SM/BHS dashboard page*



PMP 450v 4×4 AP/BHM Map View

In the PMP 450v 4×4 AP, the **Map** View > **Details** section displays multiple frequencies.

Figure 165 *PMP 450v 4 x 4 AP/BHM map view*



Wireless LAN Dashboards

This section describes the following topics:

- Wi-Fi Monitoring
- Site Dashboard
- Floor Plan
- Statistics
- Wireless Clients
- WLANs Dashboard

Wi-Fi Monitoring

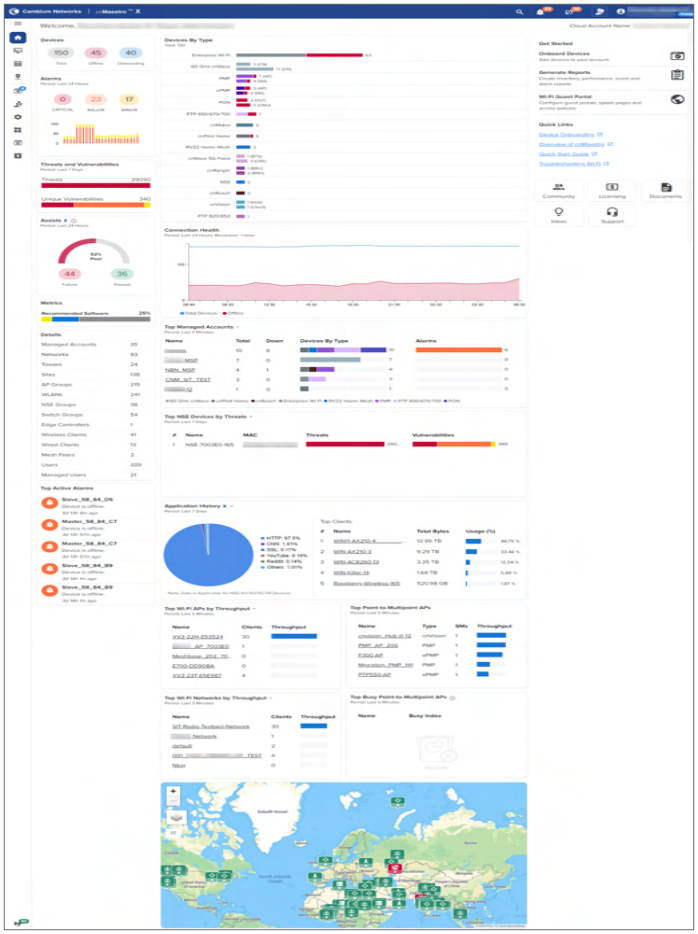
The Wi-Fi Monitoring pages include the following:

- Dashboard
- Clients
- Details
- Mesh Peers

Dashboard

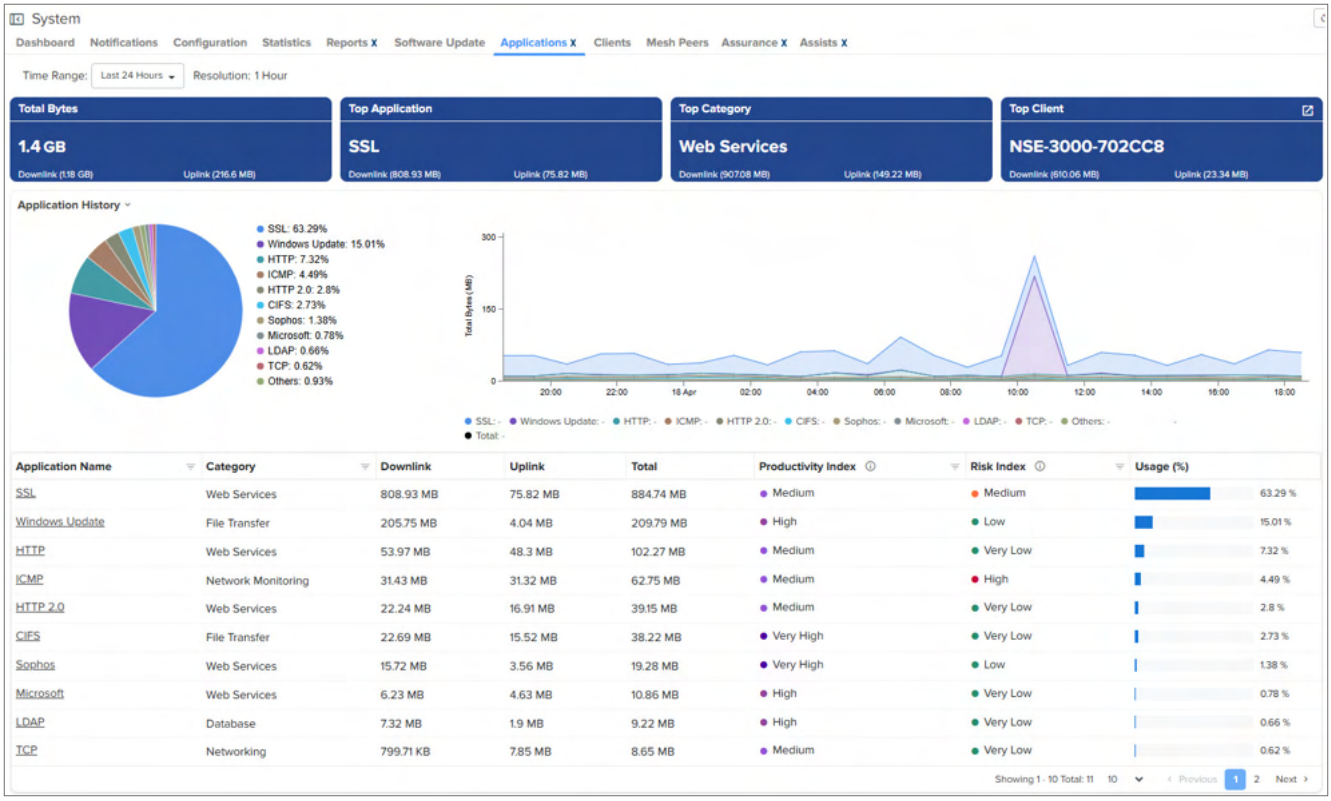
The System Dashboard displays **Devices, Alarms, Metrics, Details, Devices By Type, Connection Health, Top Managed Accounts, Application History, Top Wi-Fi APs by Throughput, Top Point-to-Multipoint APs, Top Wi-Fi Networks by Throughput, and Top Busy Point-to-Multipoint APs**.

Figure 166 *System > Dashboard*



The **System Dashboard** page displays detailed system level application usage in **Application History** and **Category History**. It displays the **Top Clients** names and their top five application usage details. The Application Visibility parameter fields are explained in detail as shown in Table 54.

Figure 167 *System > Application*

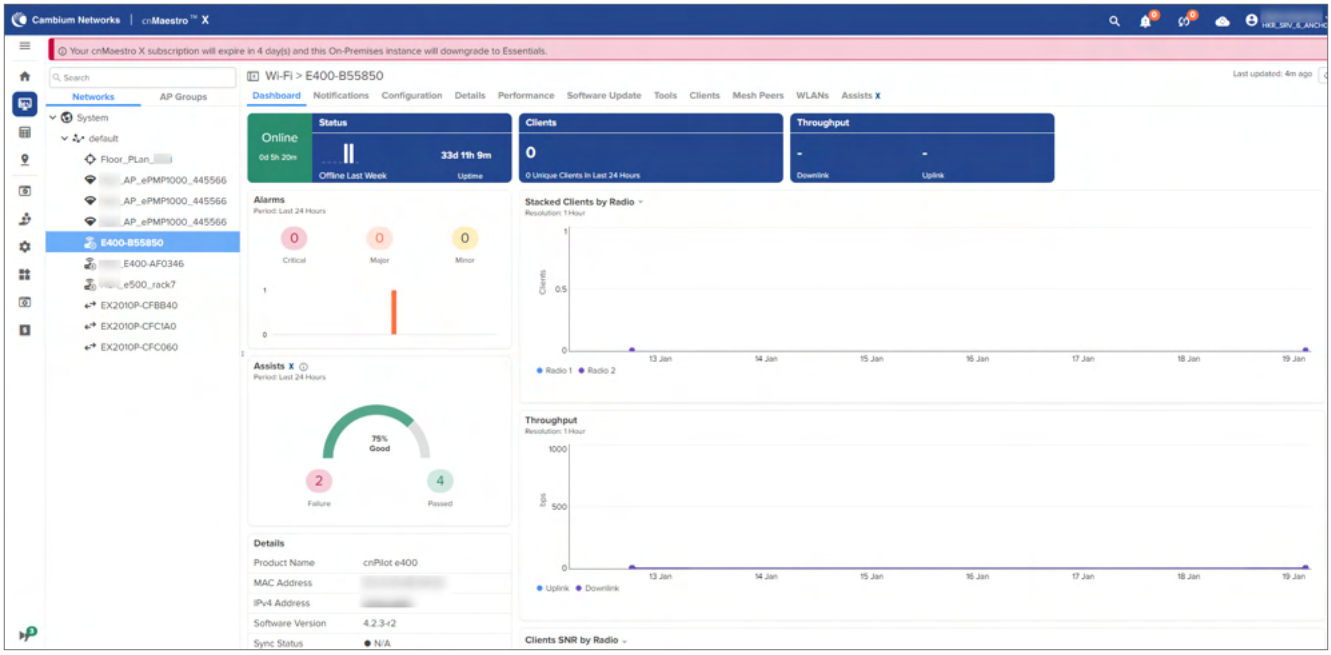


Note

- By default, the application statistics for last 24 hours is displayed.
- Application data is available for Enterprise Wi-Fi (XV, XD, and XE) devices only.

The Dashboard displays **Clients**, **Clients by Performance**, **Stacked Clients by Radio**, **Clients by SNR**, **Details**, **Radio Details, Status**, **Throughput**, **Top Active Alarms**, **Top Clients by Usage**, and **Top WLANs by Throughput**.

Figure 168 *Device > Dashboard*



Clients

The Clients tab displays the details of all the wireless, wired, and unconnected clients.

The following parameters are displayed for wireless clients connected to cnPilot Home (R-Series) APs:

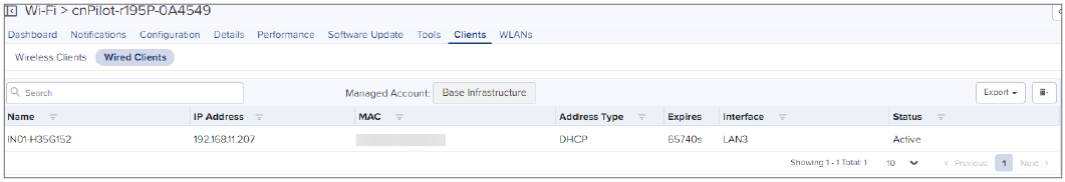
- Actions
  - Edit client name
- Band
- Download
- Host Name
- IPv4 Address
- MAC
- Manufacturer
- Radio ID
- RSSI
- SSID
- Upload

Figure 169 *cnPilot Home: Device > Clients > Wireless Clients*

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 170 *cnPilot Home (R-Series): Device > Wired Clients*

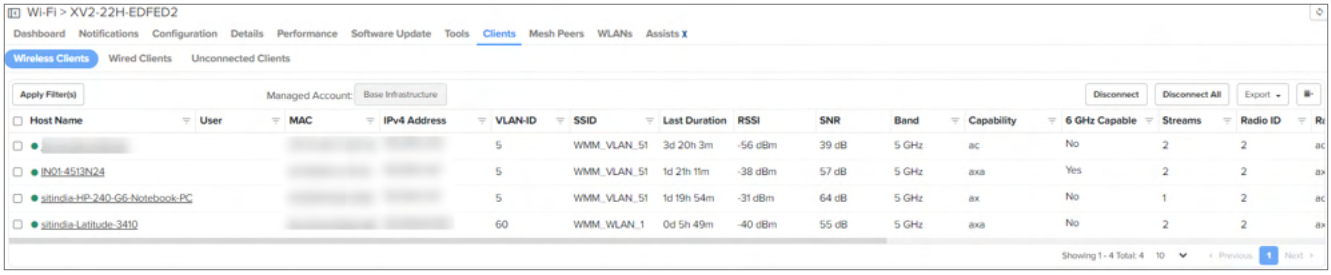


The following parameters are displayed for wireless clients connected to Enterprise Wi-Fi APs (E-, XE-, XV-, and X7-Series):

- 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
- 6 GHz Capable
- 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 171 *Enterprise Wi-Fi: Device Dashboard > Wireless Clients*



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 172 *Enterprise Wi-Fi: Device Wired Clients*

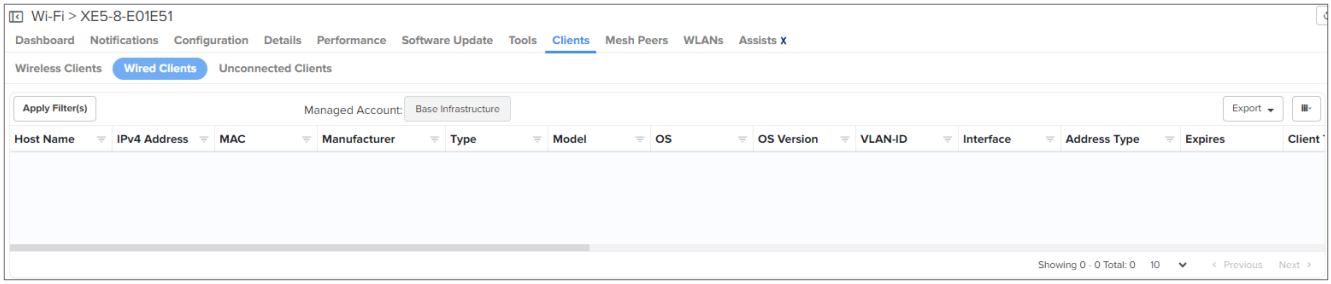
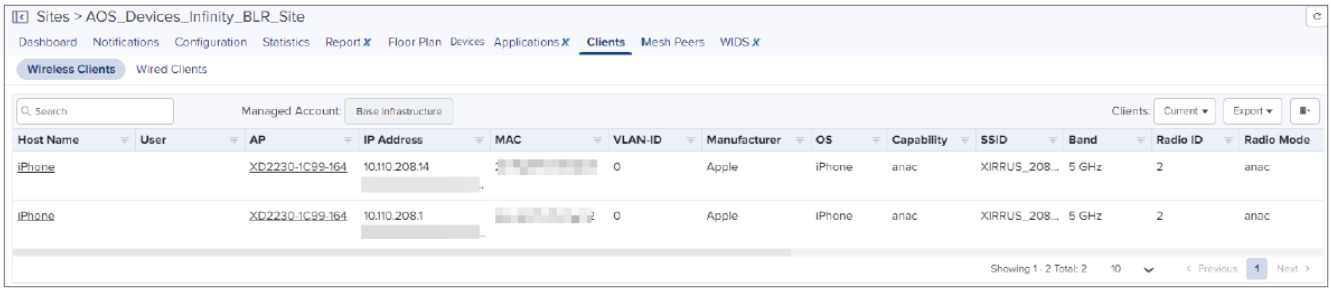


Figure 173 *Enterprise Wi-Fi (Xirrus-Series) Wireless Clients*



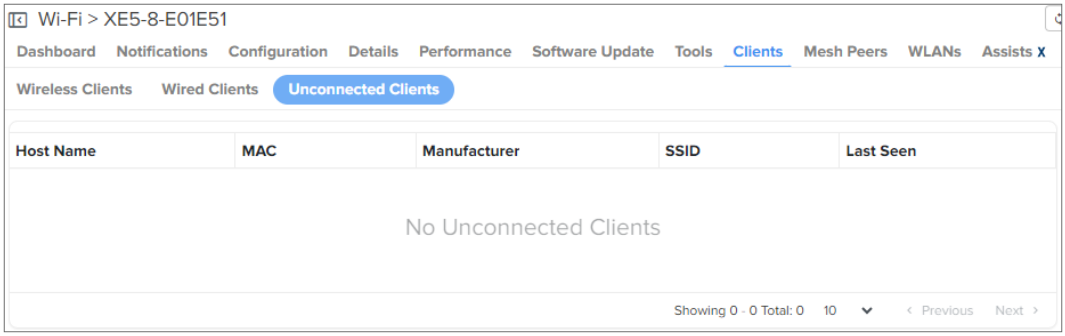
> **Note**
>
> Wired clients are not supported on Xirrus-Series APs.

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

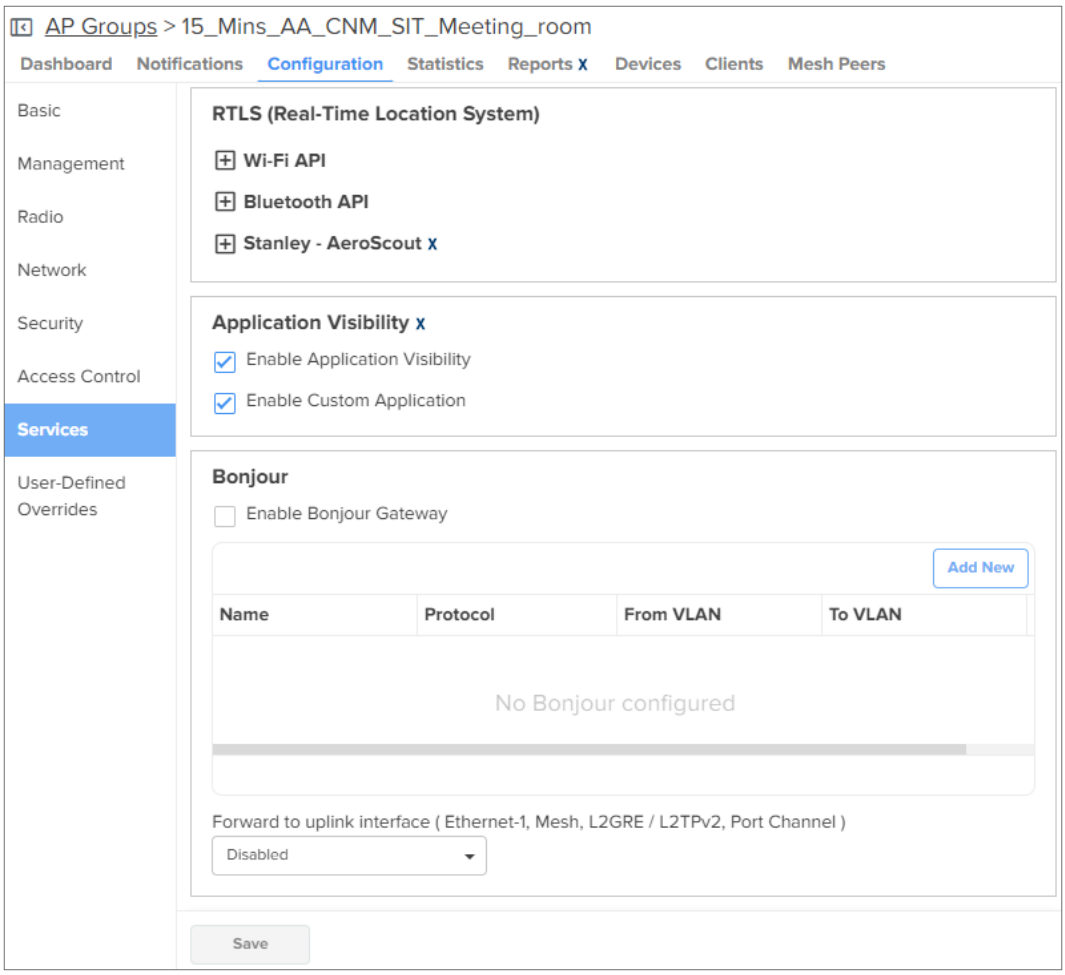
- Host Name
- MAC
- Manufacturer
- SSID
- Last Seen

Figure 174 *Enterprise Wi-Fi: Device Dashboard > Unconnected Clients*



Client Dashboard

The user can view the applications used by client when the **Application Visibility** option is enabled as shown below.

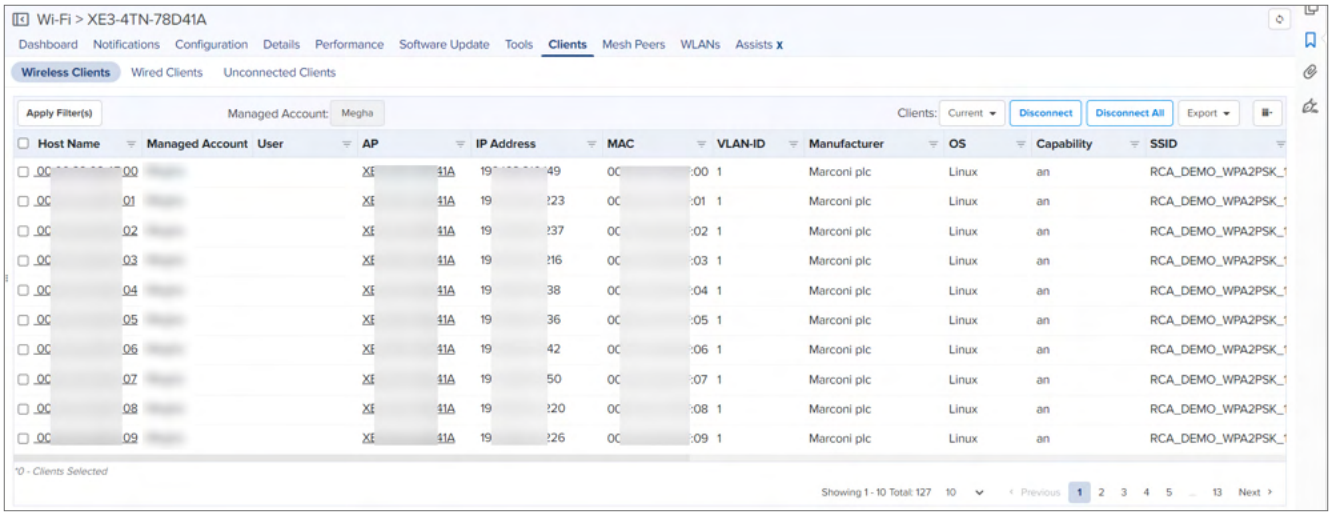


The Client Dashboard displays the details of the clients connected to the Wi-Fi device.

Note

- Enable the **Application Visibility** feature to view **Application** page. It is supported only for 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 175 *XV, and X7 Series: Device Dashboard Wireless Clients*

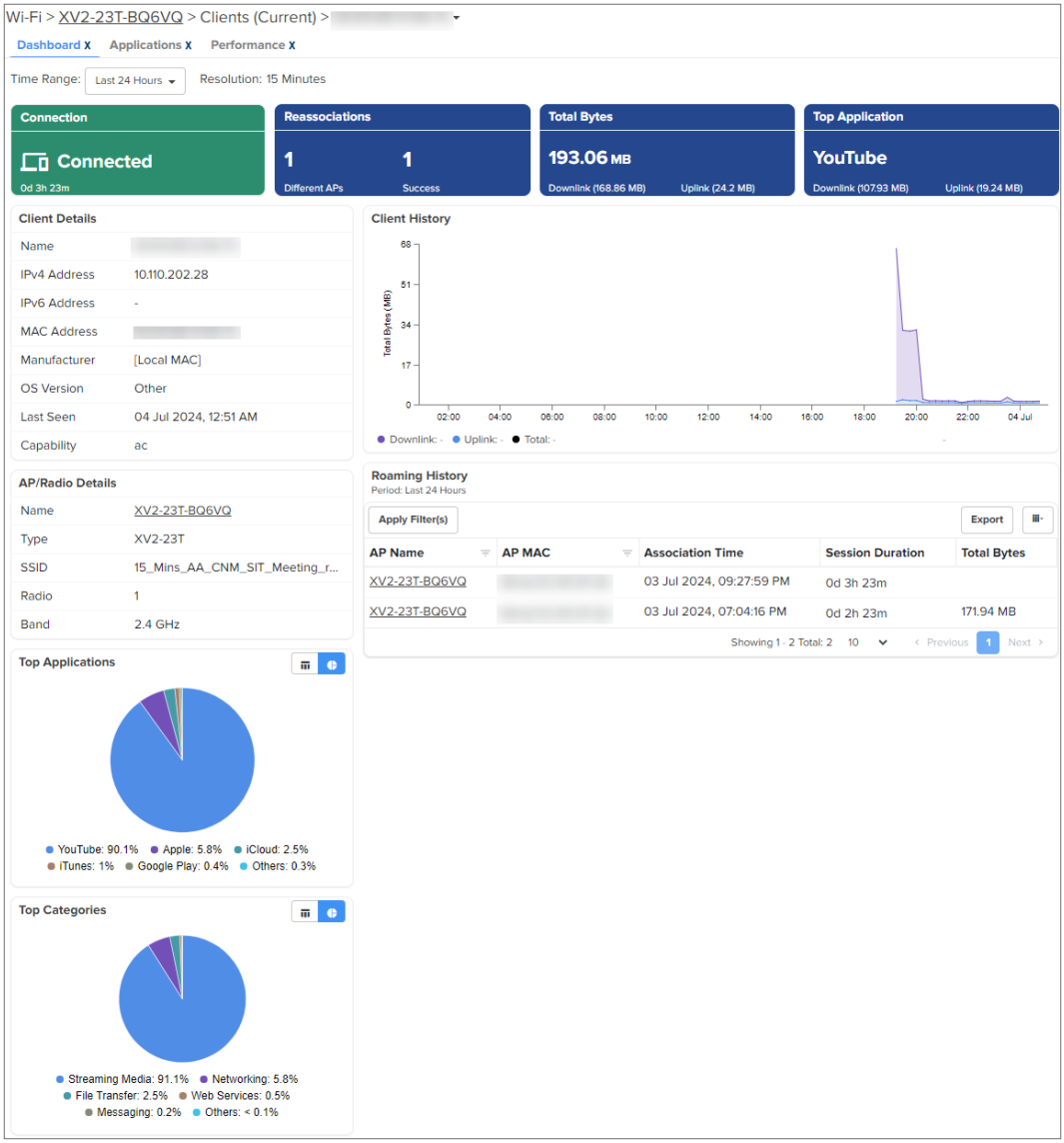


To view the **Dashboard**, navigate to **Clients** > **Wireless Clients** and click a value in the **Host Name** column.

The following parameters are displayed for Wireless Client:

- Widgets displaying connection status, number of reassociations, total bytes (sum of uplink and downlink data usage), and the top application based on data usage.
- Client Details
- AP/Radio Details
- Client History
- Roaming History
- Top Applications
- Top Categories

Figure 176 *Client Dashboard*



Application Visibility

The Application tab displays **Application History, Top Application**, **Top Category**, and **Total Bytes**.

The Application data can be presented for 24 hours or 7 days.

- **Top Application**: represent the most used application by traffic.
- **Total Bytes**: represents the sum of the Uplink and Downlink traffic across applications.
- **Top Category**: represent single category mapped to the top application.

Note

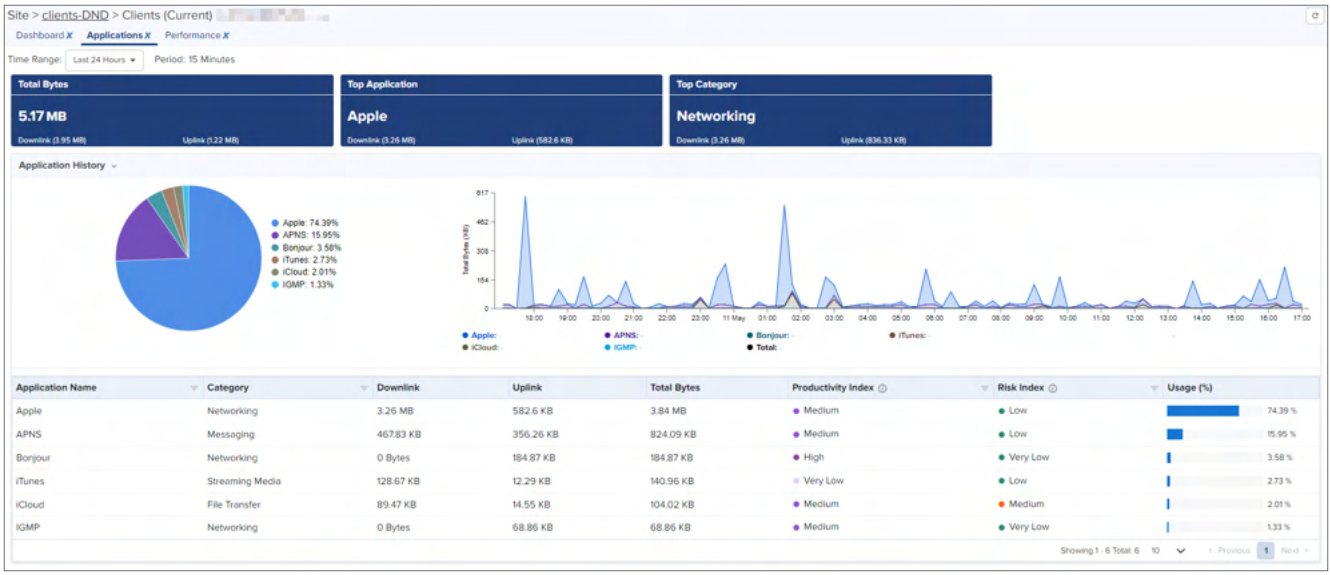
- The graphical Client Dashboard is only available in cnMaestro X.
- Application usage data is only available in cnPilot-XV, and devices must be configured to send the data.

The data is presented as either Application or Category.

- **Application**: displays data as a list of application names.
- **Category**: displays data in light of application categories.

Table 54 *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.
Total Bytes	Total amount of application data (uplink plus downlink).
Uplink	Total number of uplink bytes during the period selected.
Usage	Percentage of usage by this application in comparison to all applications.



The Productivity Index is scored relative to a work environment. The productivity score reflects likelihood to be used for work or office purposes. The Productivity Index is mapped with labels (Very Low, Low, Medium, High, and Very High) associated with value points from 1 to 5.

Table 55 *Productivity labels*

Productivity Label	Description
Very Low	Not suitable for working environment.
Low	Unlikely to be used for work tasks.
Medium	Broad usage of traffic that could be used for either personal or work related tasks.
High	Likely work oriented traffic.
Very High	Traffic is solely for work or office purposes.

The Risk Index is determined on a scale of 1 to 5. Only four weighted risk factors are considered. The risk score considers excessive bandwidth, potential data leakage, capacity to misuse, and association with malware.

Table 56 *Risk labels*

Risk Label	Value
Very Low	1
Low	2

Table 56 *Risk labels*

Risk Label	Value
Medium	3
High	4
Very High	5

Table 57 *Risk Index Calculations*

Point	Description
1 point	Excessive bandwidth usage.
1 point	Potential data leakage.
1 point	Prone to misuse.
2 points	Contains or is used by malware.

Note

Risk and Productive Indexes are cross-checked against similar GUIDs to ensure consistency.

Performance

The Performance tab displays a synchronized view of time-series data, including connection health and application usage.

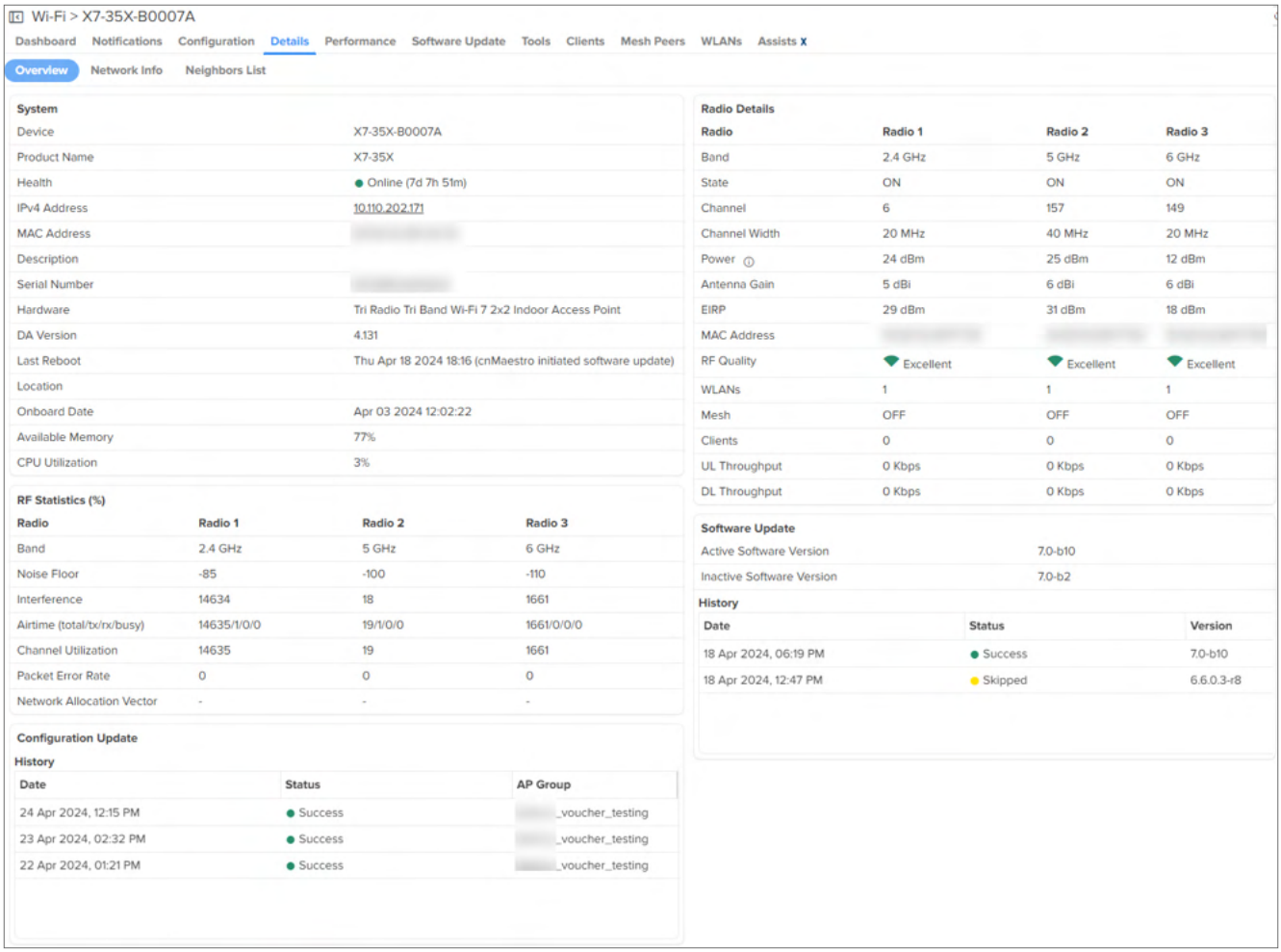
- Supported time ranges are **Last 24 Hours** or **Last 7 Days.**

The following client data parameters are displayed:

- Application Throughput
- Data Rate
- RSSI
- SNR
- Throughput

Details

Details page displays the Overview, Network Info, and Neighbors List.



Overview

The **Details** > **Overview** page displays information, such as System, RF Statistics (%), Configuration Update, Radio Details, Software Update, and History.

Network Info

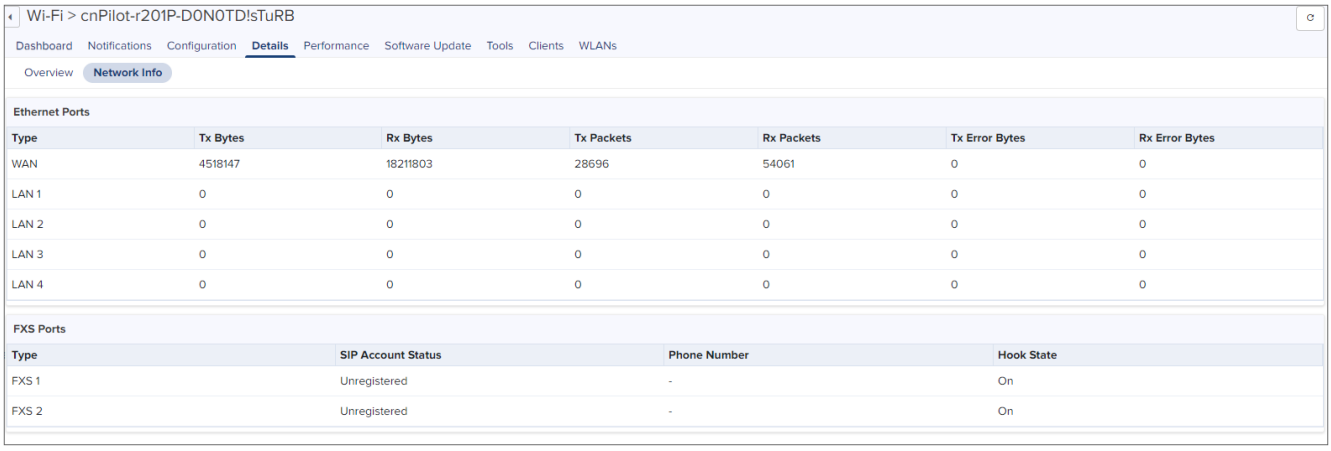
The **Details** > **Network Info** page displays the following parameters for cnPilot Home (R-Series) router:

- 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

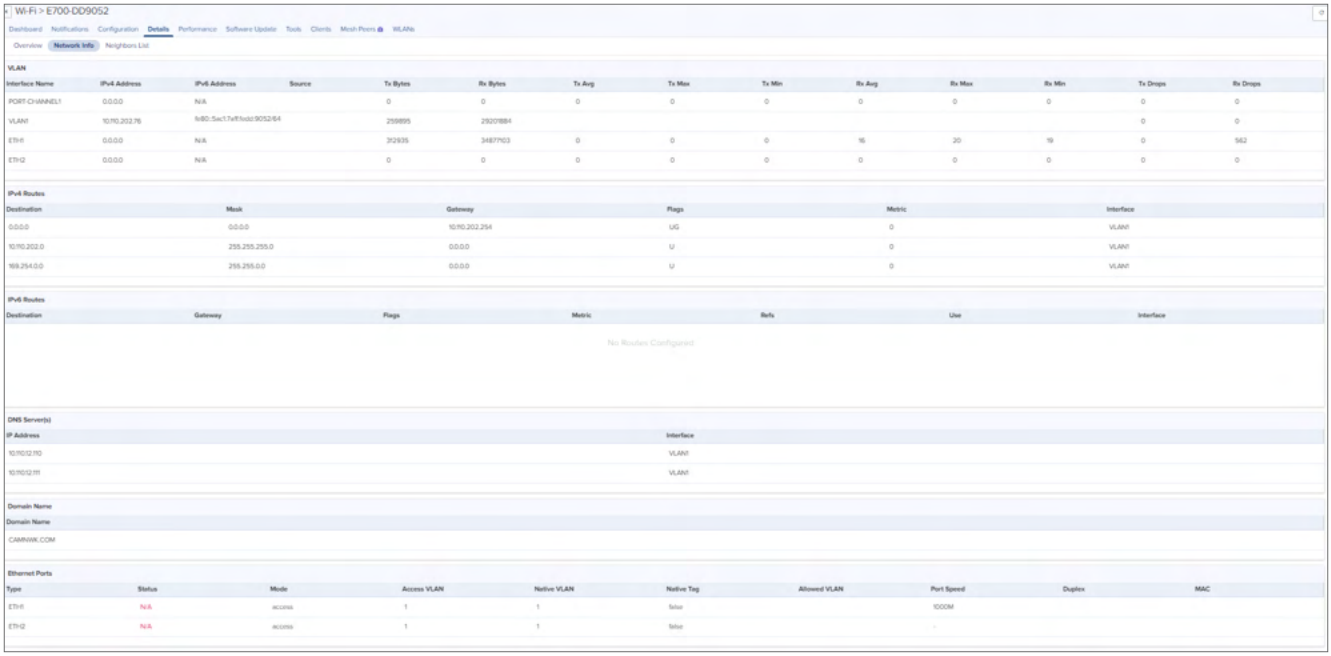
Figure 177 *cnPilot Home: Device > Details > Network Info*



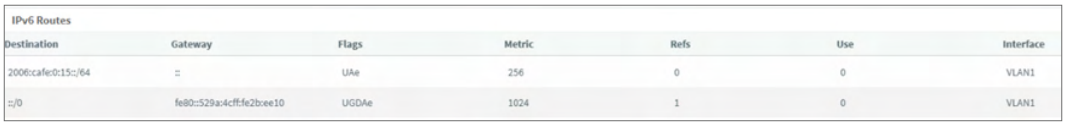
The following parameter details are displayed in E-Series:

- DNS Server(s)
- DHCP Server
- Domain Name
- Ethernet Ports
- PPPoE
- Routes
- IPv4 Routes
- IPv6 Routes
- Tunnels
- VLAN Pool

Figure 178 *Enterprise Wi-Fi: Device >Details > Network Info*



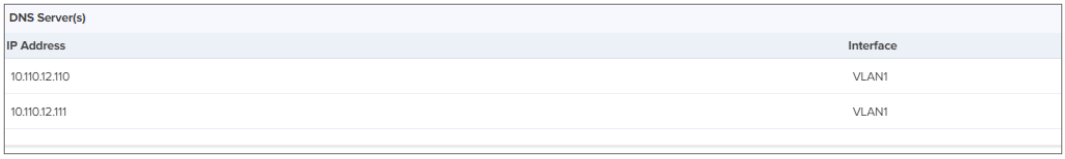
IPv6 Routes



IPv6 Routes

Destination	Gateway	Flags	Metric	Refs	Use	Interface
2006:cafe:0:15::/64	::	UAe	256	0	0	VLAN1
::/0	fe80::529a:4cff:fe2b:ee10	UGDAe	1024	1	0	VLAN1

DNS Servers



DNS Server(s)

IP Address	Interface
10.110.12.110	VLAN1
10.110.12.111	VLAN1

Neighbors List

The **Neighbors List** displays the BSSID, SSID, Channel, and SNR details of neighboring 2.4 GHz and 5 GHz radios.

Figure 179 *Neighbors List*

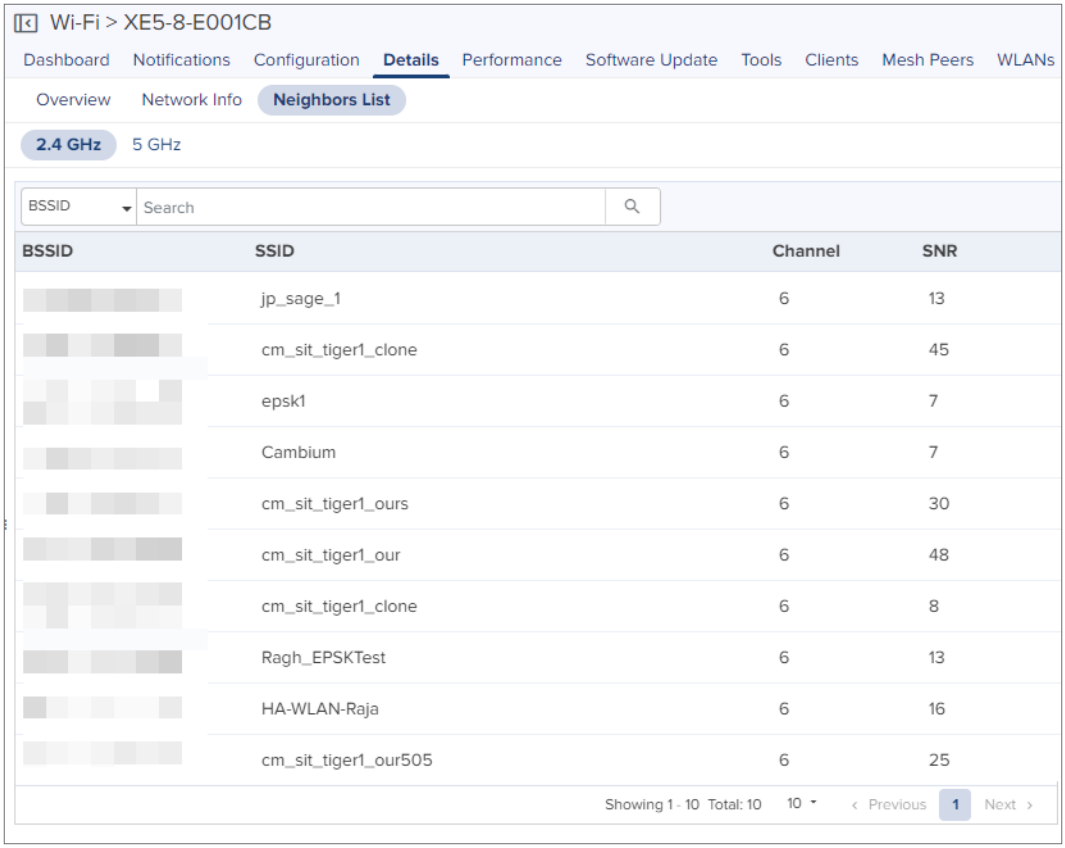


Figure 180 *PTP 650/670/700: Device >Dashboard > Network Info*

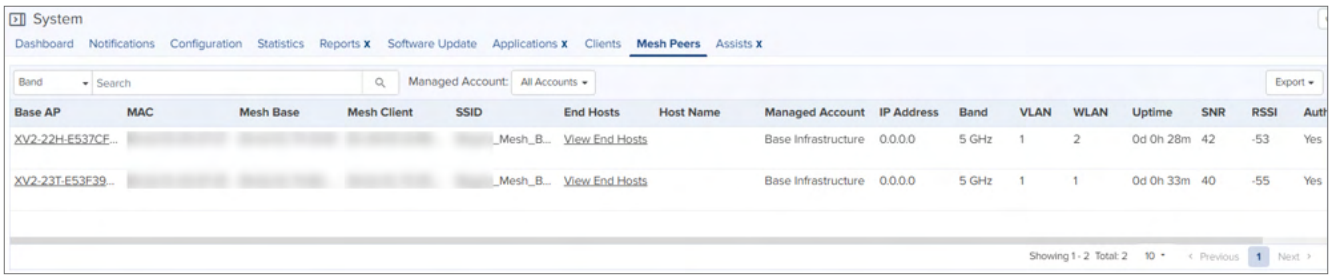
Ethernet Ports

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		-		

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 181 *Device > Mesh Peers*



Roaming History for Mesh Peers

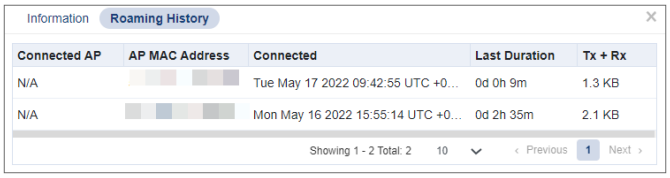
The Roaming History details the Connected AP, AP MAC, Duration, number of packets transferred and received by the clients (Tx and Rx), during roaming from one mesh base to a different mesh base.

To view the **Information** and **Roaming History,** perform the following**:**

In **the Mesh Peers** tab, click the **Host Name.**

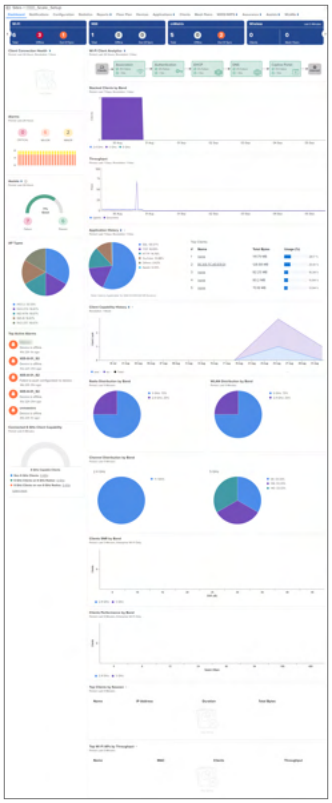
A detailed Information and Roaming History window pops up.

Figure 182 *Mesh Peers > Host Name > Roaming History*



Site Dashboard

The Site Dashboard provides the overview of site-related parameters and devices.



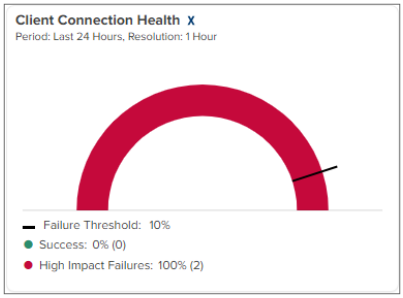
The Site Dashboard displays the following graphics:

- Client Connection Health X
- Assists X
- Alarms
- Top Active Alarms

- AP Types
- Channel Distribution by Band
- Clients Performance by Band (Enterprise Wi-Fi)
- Clients SNR by Band (Enterprise Wi-Fi)
- Connected 6 GHz Client Capability
- Application History X (Category History X)
- Client Capability History
- Radio Distribution by Band
- WLAN Distribution by Band
- Throughput
- Throughput Graph
- Top Wi-Fi APs by Throughput or Clients
- Wi-Fi devices widget (Total, Offline, Out of Sync)
- Top Clients by Session
- Top Clients by Usage

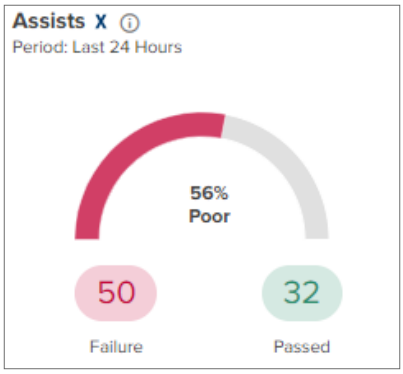
Client Connection Health X

Displays the percentage of success and failed client connections in that site.



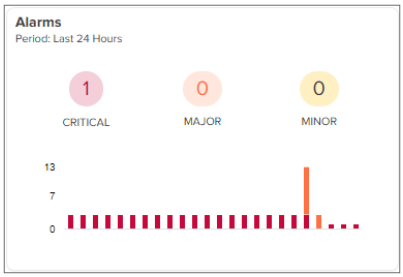
Assists X

Assists X displays scanned configuration scores and results for last 24 hours for that site. For more information, see Assists X.



Alarms

Displays the alarms raised for the devices in the Site in the last 24 hours as a bar graph. It also displays the count of critical, major and minor alarms raised. Clicking the number displays the **Site** > **Notifications** > **Alarms** page. For details about the **Alarms** page, see Alarms.

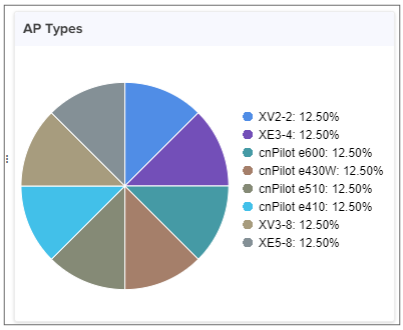


Top Active Alarms

Displays the topmost active alarms raised in that Site.

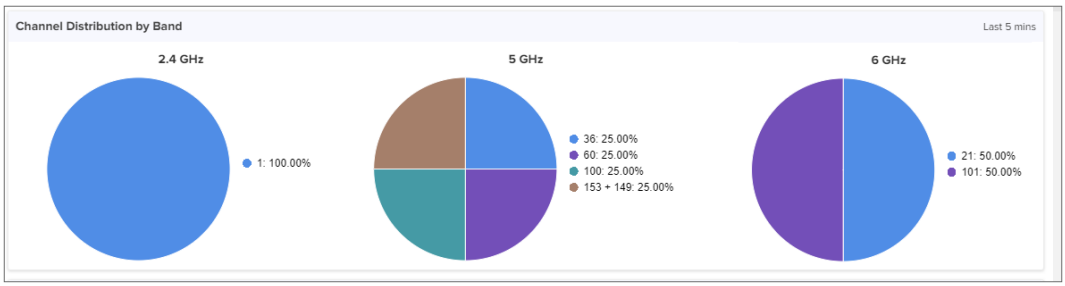
AP Types

Displays the distribution of different AP models in a pie chart.

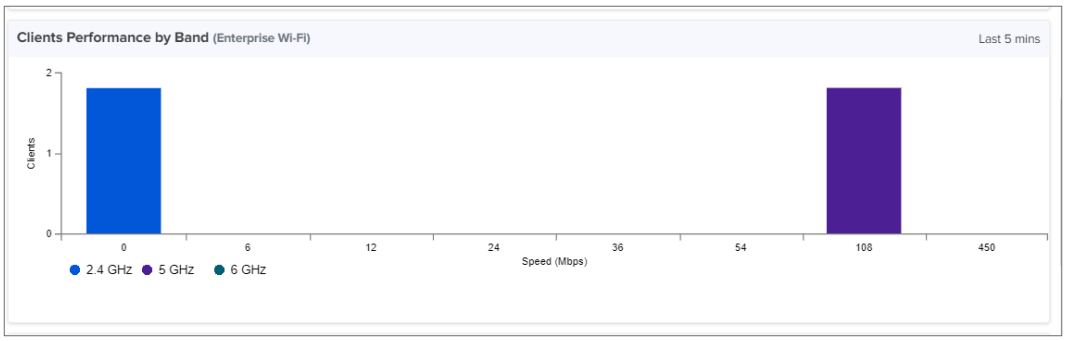


Channel Distribution by Band

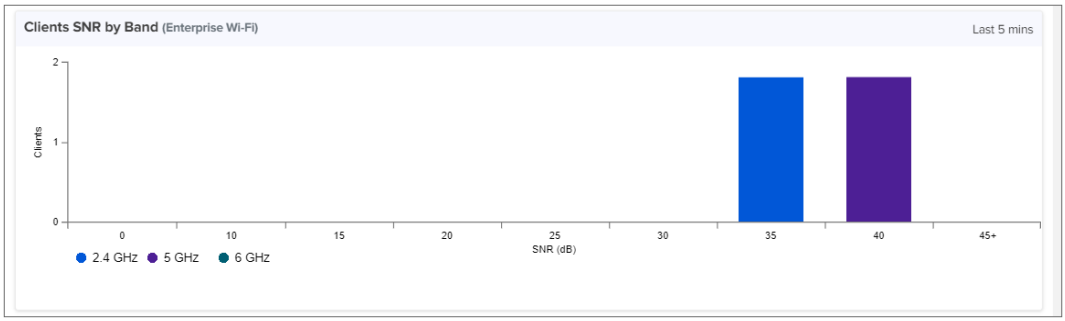
Channel distribution displays usage of channels in 2.4 GHz, 5 GHz. This helps in planning and implementing WLANs within a high-density environment. .



Clients Performance by Band (Enterprise Wi-Fi)



Clients SNR by Band (Enterprise Wi-Fi)



Connected 6 GHz Client Capability

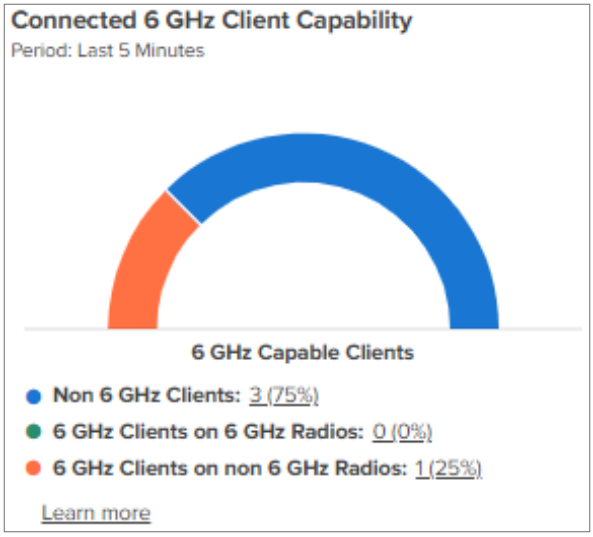
The Connected 6 GHz Client Capability widget presents a point-in-time view of Wi-Fi 6 GHz clients associating to non-6 GHz radios. These clients may experience better service if SDR radios are upgraded from 5 GHz to 6 GHz. A high percentage of 6 GHz capable clients connecting to non-6 GHz radios is an indication to upgrade radios to 6 GHz. The Connected 6 GHz Client Capability widget is represented using different colors and corresponding percentage values as described below:

- Non 6 GHz Clients: represents non 6 GHz clients connected across the devices at the Site level.
- 6 GHz Clients on 6 GHz Radios: represents 6 GHz clients connected across the devices at the Site level.
- 6 GHz Clients on non 6 GHz Radios: represents 6 GHz clients connected across the devices on non 6 GHz radios at the Site level.

Note

For best results, deploy a few radios in 6 GHz mode in high traffic areas.

Figure 183 *Connected 6 GHz Client Capability*

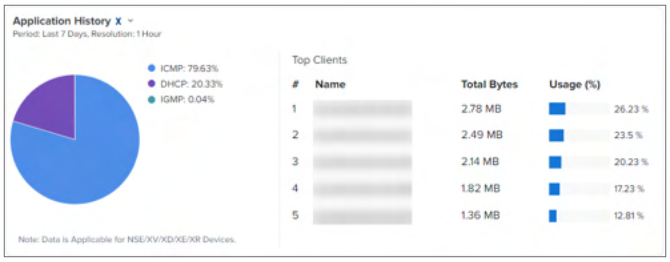


Clicking next to clients number navigates to **Wireless Clients** page.

Application History X (Category History X)

The Application History X (Category History X) section displays a pie chart with the distribution of the top protocols used by clients connected to the Enterprise devices (XV/XD/XE/XR). It also displays the details of the top five clients based on data usage.

From the section title dropdown, select Category History X to display the pie chart with the distribution of categories.



Client Capability History

The Client Capability History graph displays the highest detected Wi-Fi protocol for Clients active at a Site on a weekly basis. Wi-Fi 6 GHz devices are grouped into a single 6 GHz category. A large number of 6 GHz Capable Clients is an indication 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 184 *Clients History in line chart*

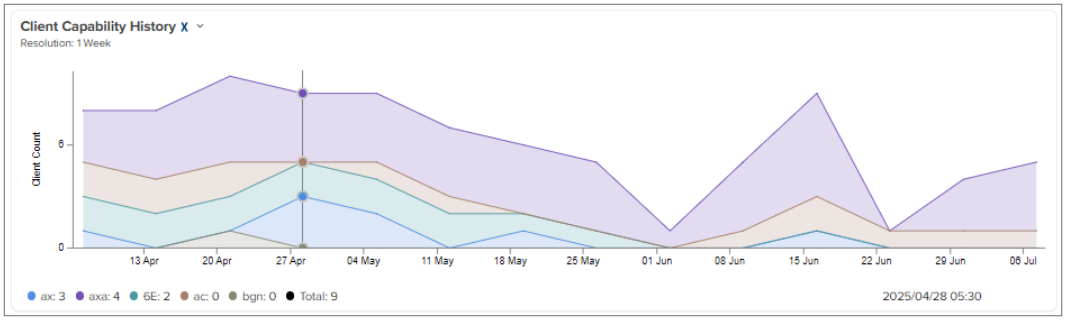
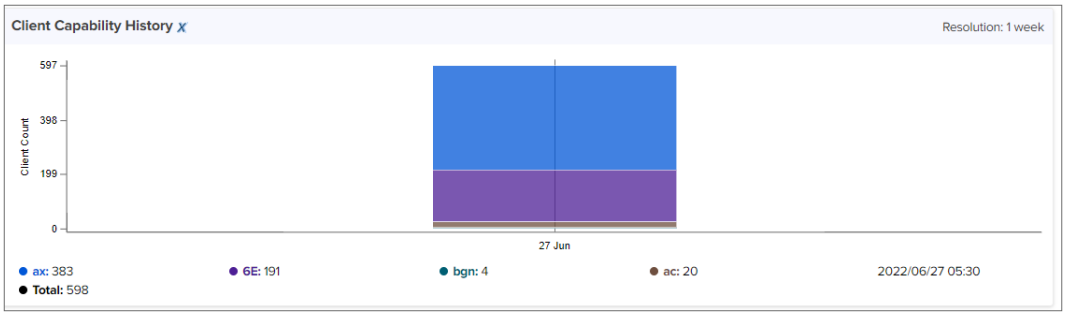
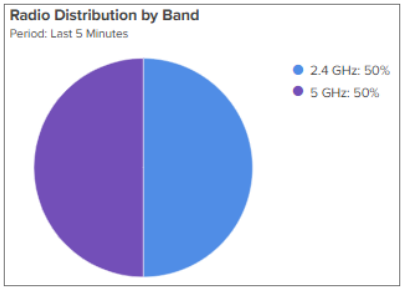


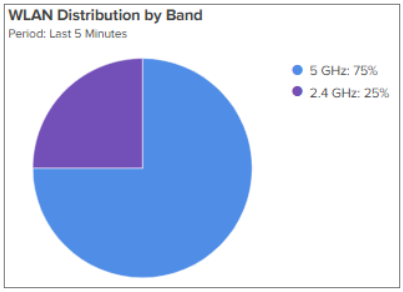
Figure 185 *Clients History in bar chart*



Radio Distribution by Band



WLAN Distribution by Band

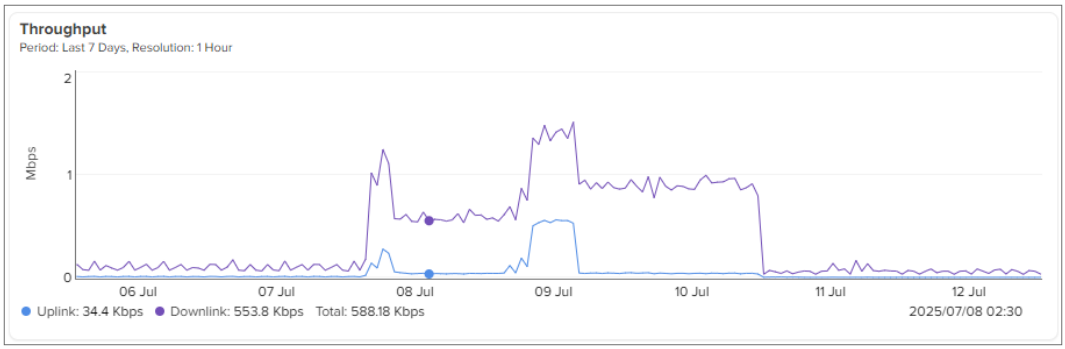


Throughput

Displays aggregated throughput for all the clients.

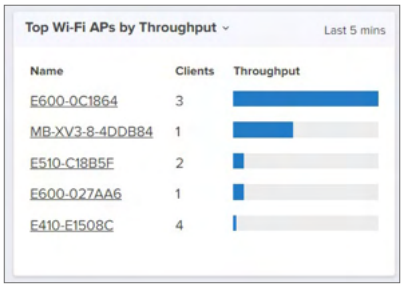
Throughput Graph

Throughput graph displays client traffic for the last week.



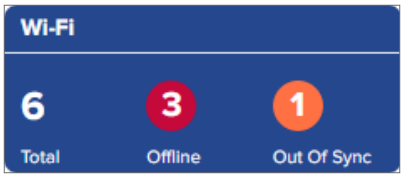
Top Wi-Fi APs by Throughput or Clients

Displays a bar graph with the top APs listed by the throughput or by the number of clients connected to them.



Wi-Fi devices widget (Total, Offline, Out of Sync)

Displays total number of Access Points in the Site and the devices that are offline and out of sync.

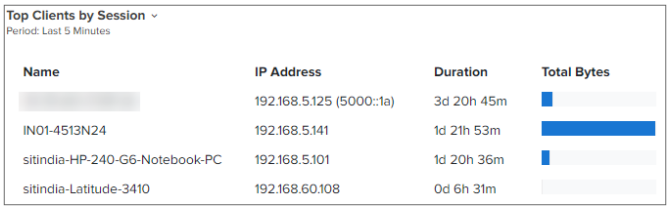


- **Total**—Click the number to display the **Sites** > **Devices** > **List** page with the device type filter applied.
- **Offline**—Click the number to display the **Sites** > **Devices** > **List** page with the **Status** filter applied as **Offline**.
- **Out Of Sync**—Click the number to display the **Sites** > **Devices** > **Configuration** page with the **Sync Status** filter applied as **Not In Sync**.

  To sync the configuration, select the required APs and click **Sync Configuration**.

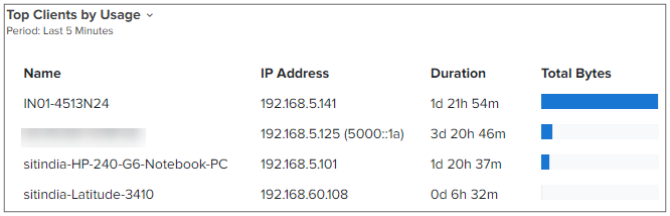
Top Clients by Session

Displays the top clients by session and the respective details.



Top Clients by Usage

Displays the top clients by usage and the respective details.



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.

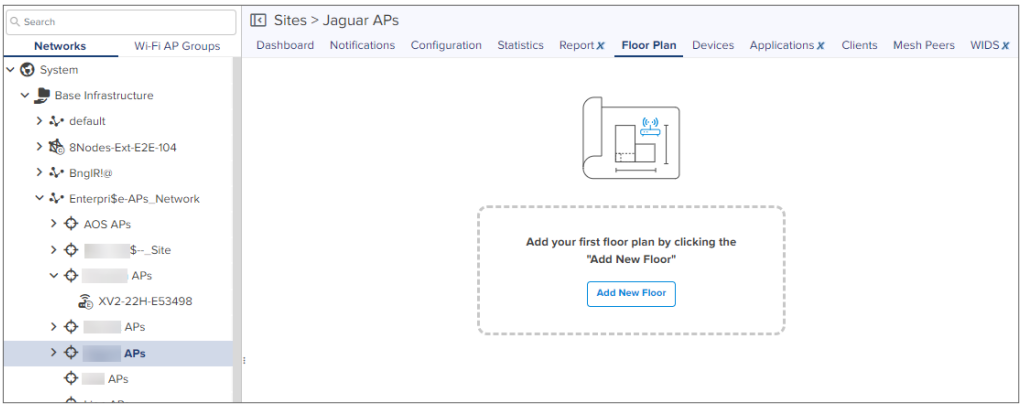
To create a floor plan, perform the following steps:

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.

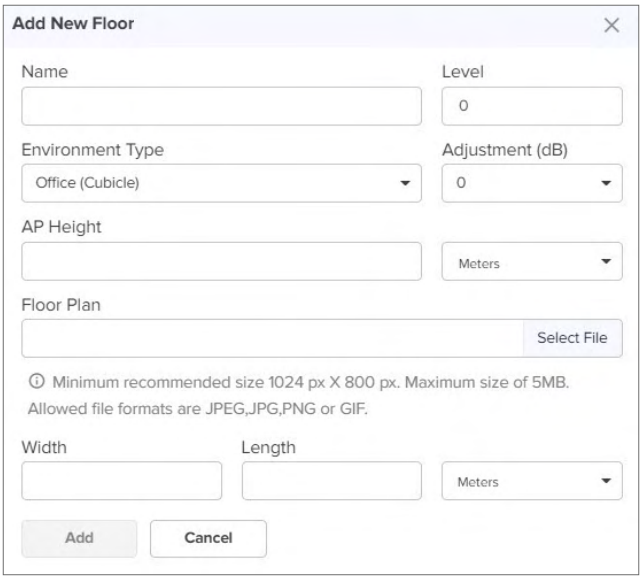


Table 58 *Fields in Floor Plan*

Field	Description
Name	Name of the floor.
Level	Level of the floor.
Environment Type	Floor type such as the following: • Apartment • Hospital • Hotel • Office (Cubicle) • Office (Walled) • Outdoors • 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.

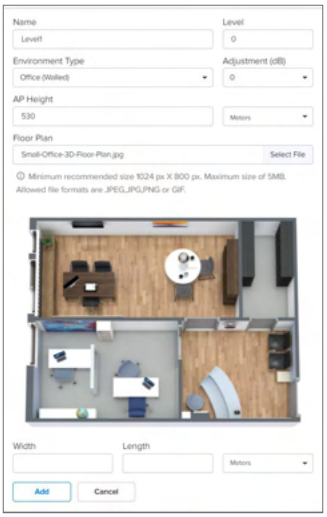
Note

Environment Type, Adjustment, and Height are currently unused by cnMaestro. They will become important when RF Heat Maps are added in a later release.

4. 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

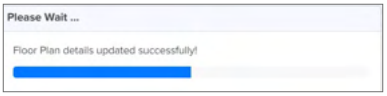


Note

- 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.

5. 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 1 to 50 floor plans.
- 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 186 *Configure Floor Plan*

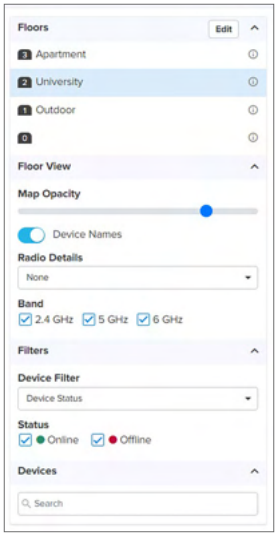


Table 59 *Fields to configure floor plan page*

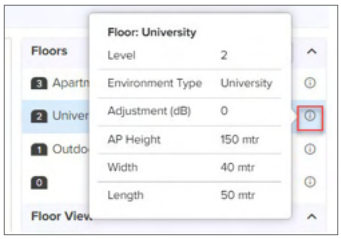
Field	Description
Floors	Indicates the floor level. The following actions are available: • Click **Add** to add new floor level. Drag and drop the selected devices from the right pane to the required floor level. If multiple floor levels are available, then select required floor level from the dropdown. • 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.  • In the **Devices on this floor** dropdown, you can view the following options: ○ Unmapped Devices: Devices not mapped to the floor plan. ○ 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	Configure device presentation. The following options are available: • 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).

Table 59 *Fields to configure floor plan page*

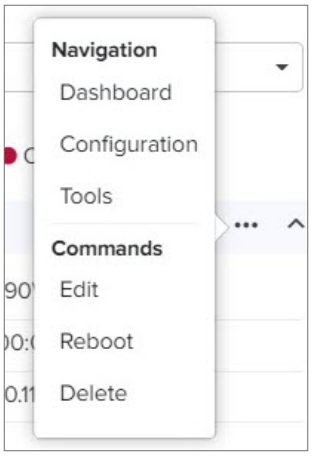
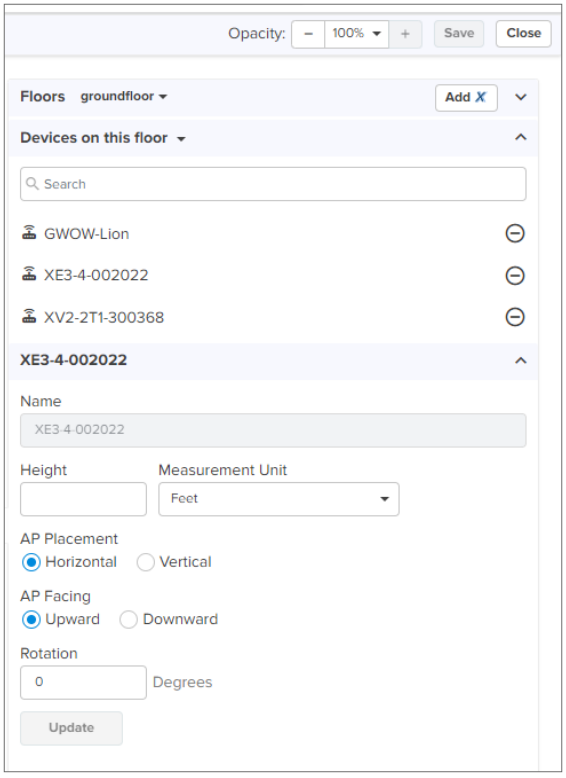
Field	Description
Filter	Filter devices by Device Status, Channel, and Power.
Devices	View and edit the device details. The following actions are available: • Select the device on the floor plan or type the device name in the search field. • Click the eye icon ( ) to **Show** or **Hide** the device on the floor plan. • Click on the device name to view device details, as shown below: • Click ellipsis (...) icon next to the device name, to navigate to the device homepage.  • Click **Edit** on the top right corner and select the device in the current floor.

Table 59 *Fields to configure floor plan page*

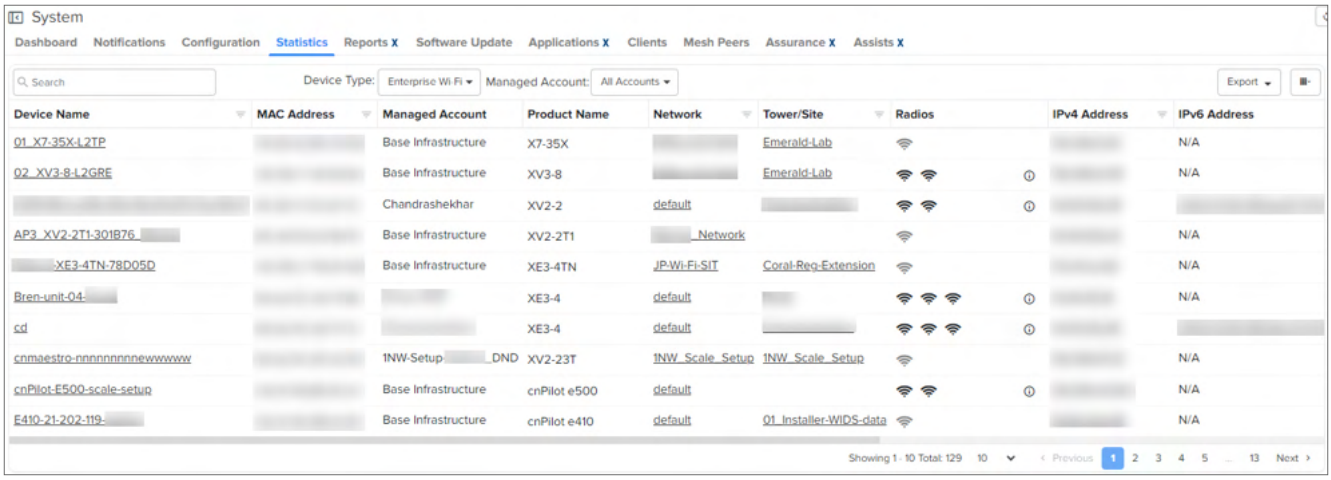
Field	Description
	 Edit the **AP Placement**, **AP Facing** and **Rotation** options. • Click **Update** and **Save.** • Click **Remove** (⊖) icon to remove device from the floor plan. • Click **Save**.

Statistics

Statistics tab displays the following parameters for Enterprise Wi-Fi devices:

- Device Name
- MAC Address
- Managed Account
- Product Name
- Network
- Tower/Site
- Radios
- IPv4 Address
- IPv6 Address
- Status
- Uptime

- AP Group
- Port Speed

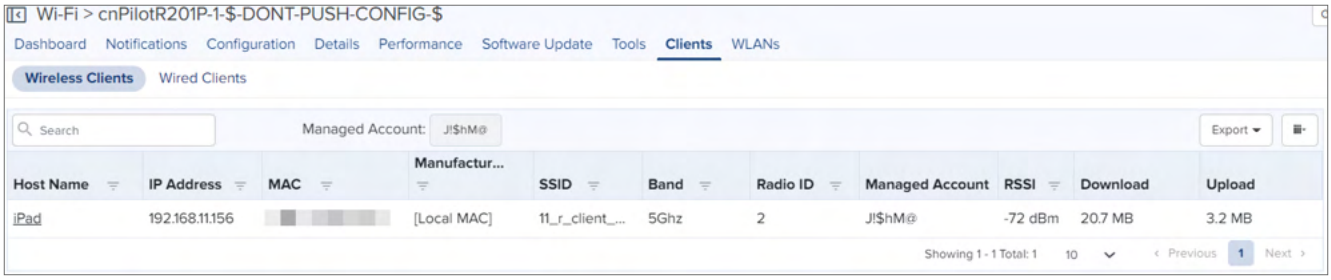


Wireless Clients

Wireless Clients tab displays following parameters:

- Auth Status
- Authentication Type
- Band
- Client Type
- Host Name
- IP Address
- MAC
- Manufacturer
- Mode
- OS
- Portal Mode
- RSSI
- Session Expiry
- SNR
- User
- VLAN-ID
- WLAN

The table can be exported as PDF or CSV.



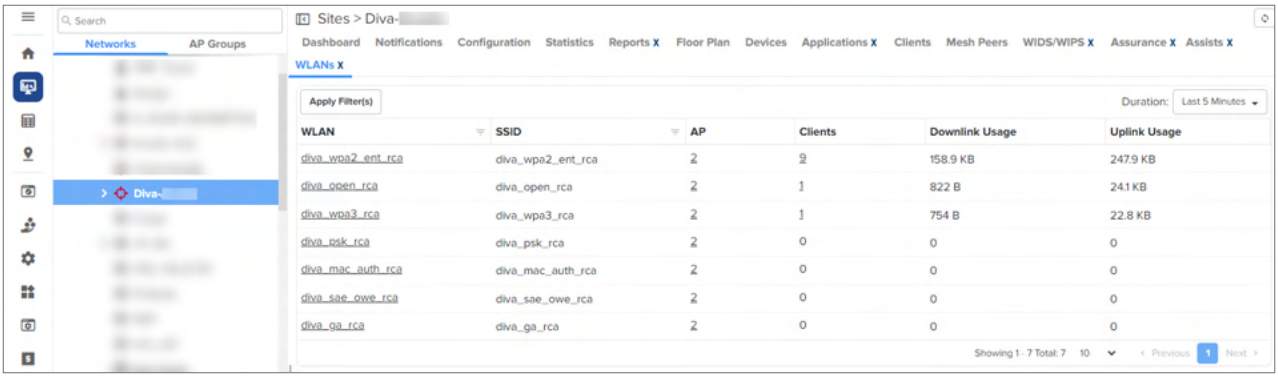
WLANs Dashboard

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 187 *WLANs Dashboard*

  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.

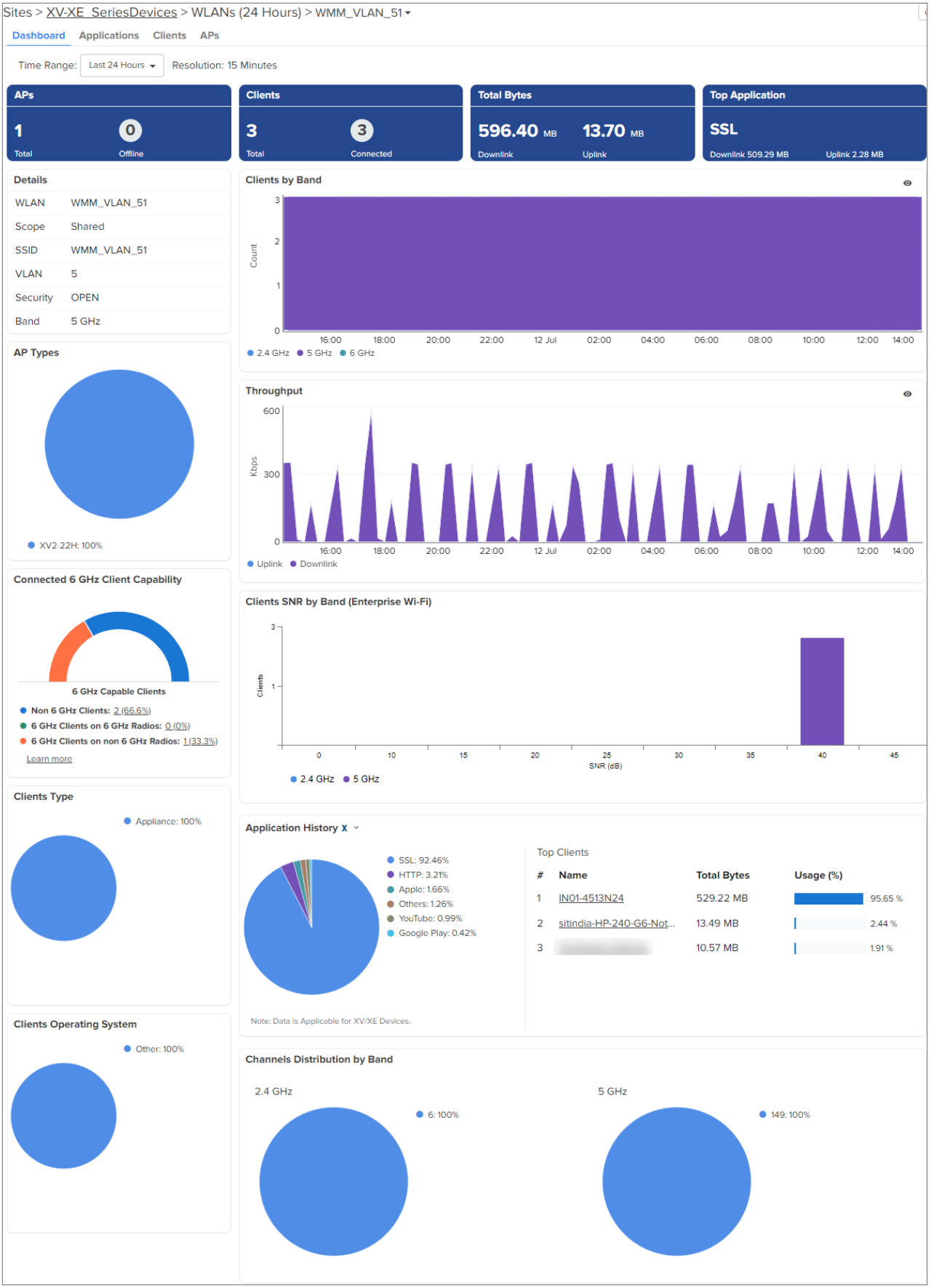
- Click a WLAN in the WLANs page to view the WLAN-specific dashboard.

  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 6 GHz 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 188 *WLAN-specific Dashboard*



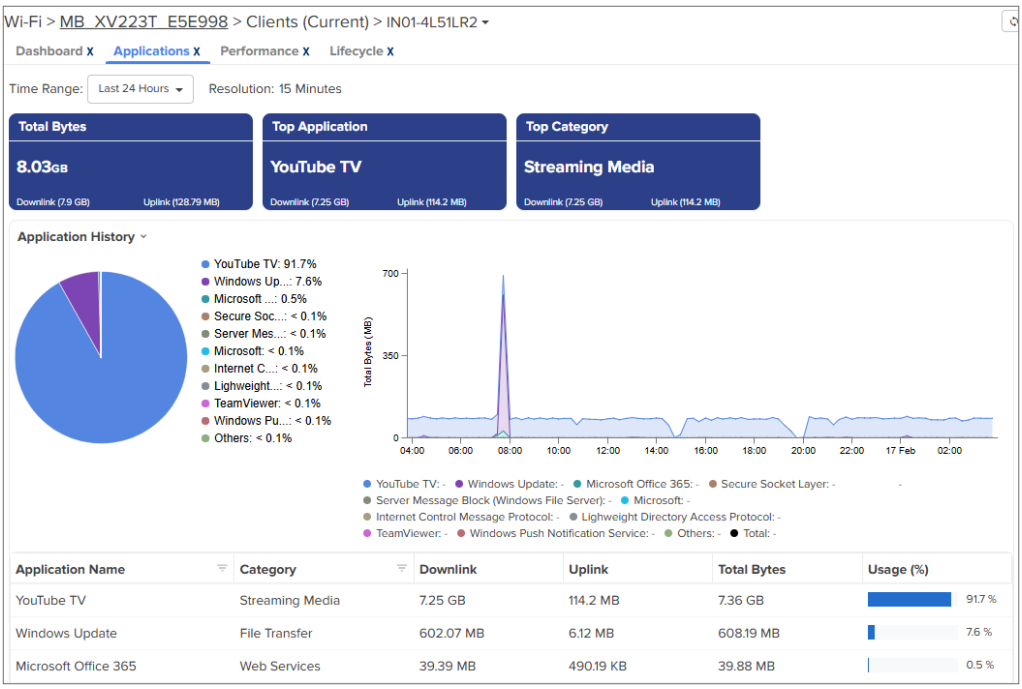
- To view the details of the applications accessed through this WLAN, click the **Monitor and Manage** > ***<Site-Name>*** > **WLANs**[X] > <WLAN-Name> > **Applications** tab.

  The **Applications** dashboard displays both a graphical data and details in a table with the following fields:

Table 60 *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).
Usage (%)	Percentage of usage by this application in comparison to all applications.

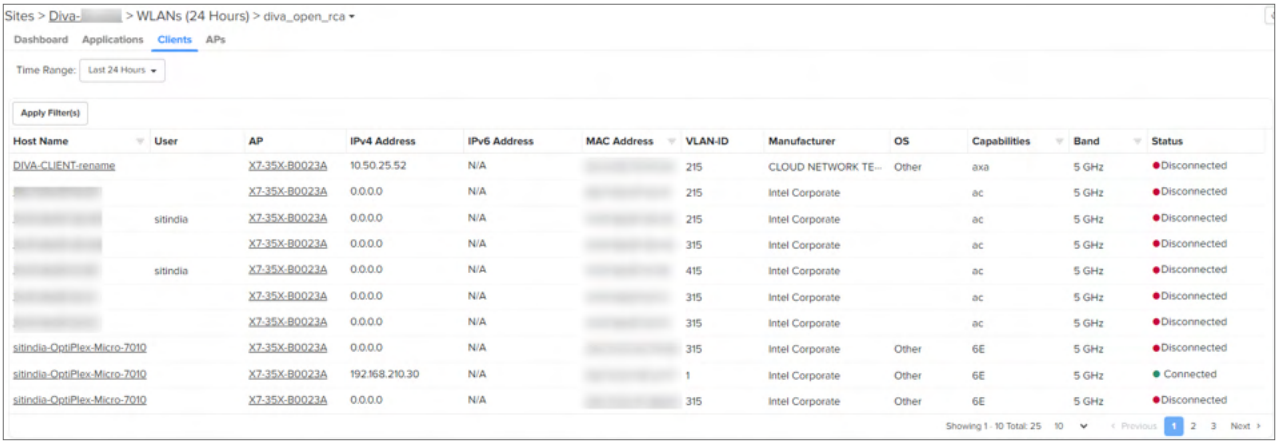
Figure 189 *WLAN-specific Application Dashboard*



- 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 190 *WLAN-specific Clients Dashboard*



- 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 191 *WLAN-specific APs Dashboard*

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
- Tools

Dashboard

Displays the monitoring information of the OLT.

Figure 192 *Fiber OLT dashboard*

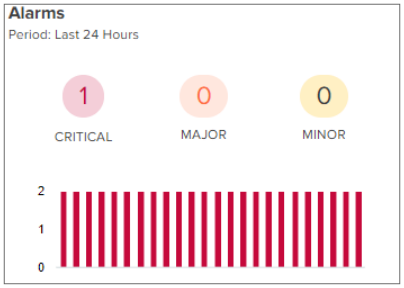
Dashboard has the following elements:

- 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

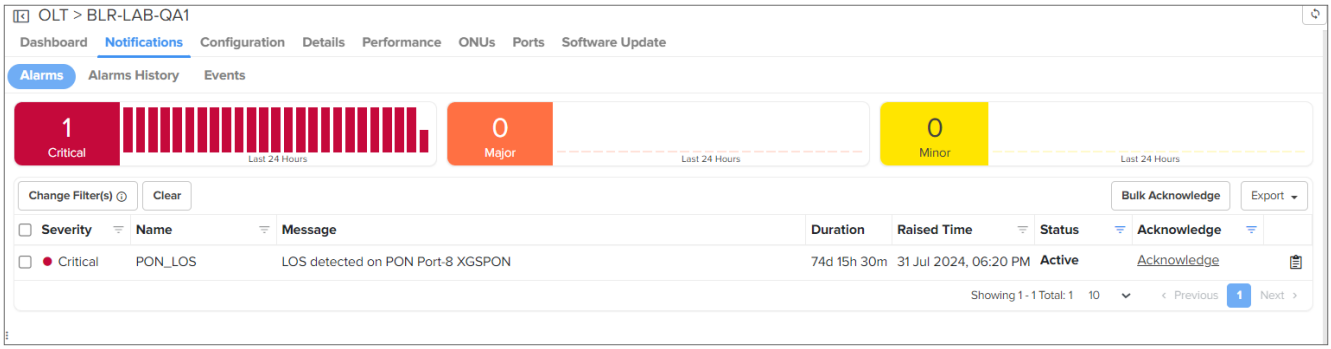
Alarms

Displays the critical, major, and minor alarms. Figure 193 shows the status of the alarms.

Figure 193 *Alarms*



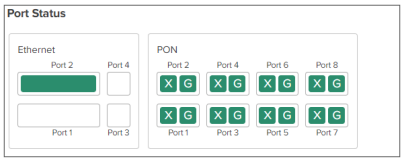
To view the detailed information, click on the respective alarm count.



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 XGS-PON.

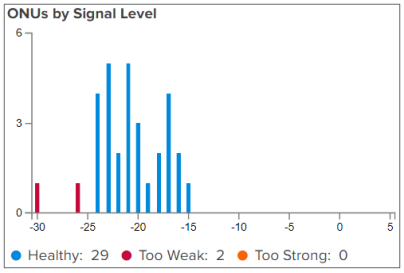
Figure 194 *Port status*



ONU by Signal Level

Displays the signal level received by the ONU.

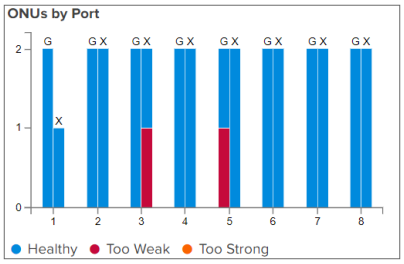
Figure 195 *ONU by signal level graph*



ONU by Signal Level per Port

Displays the number of ONU connected and their corresponding power levels.

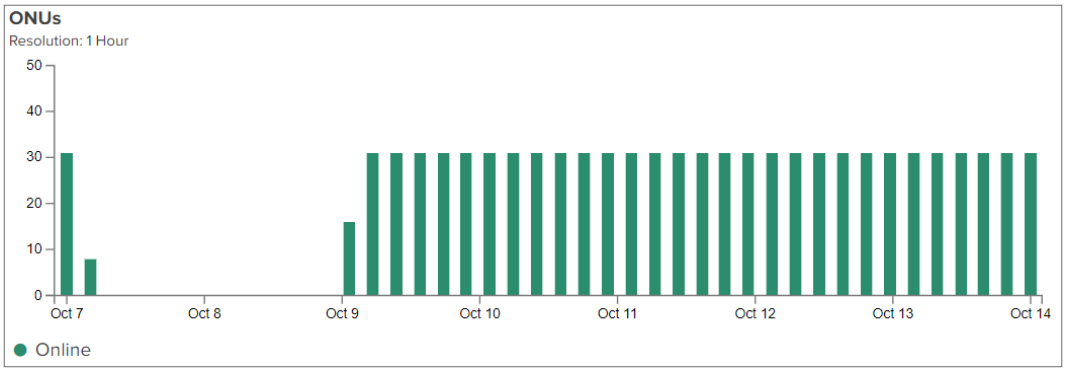
Figure 196 *ONU by signal level per port*



ONUs

Displays the number of ONUs connected to the OLT.

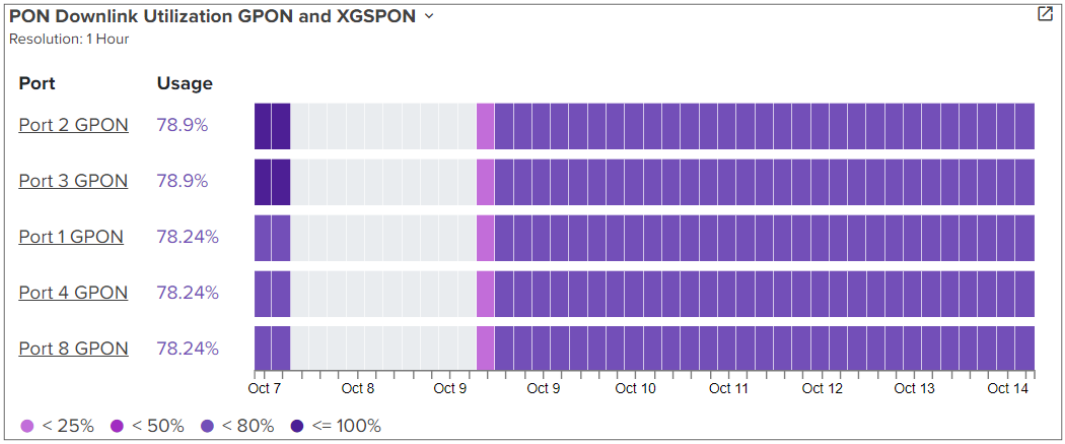
Figure 197 *ONU*



PON Downlink Utilization

Displays the utilization of GPON and XGS-PON.

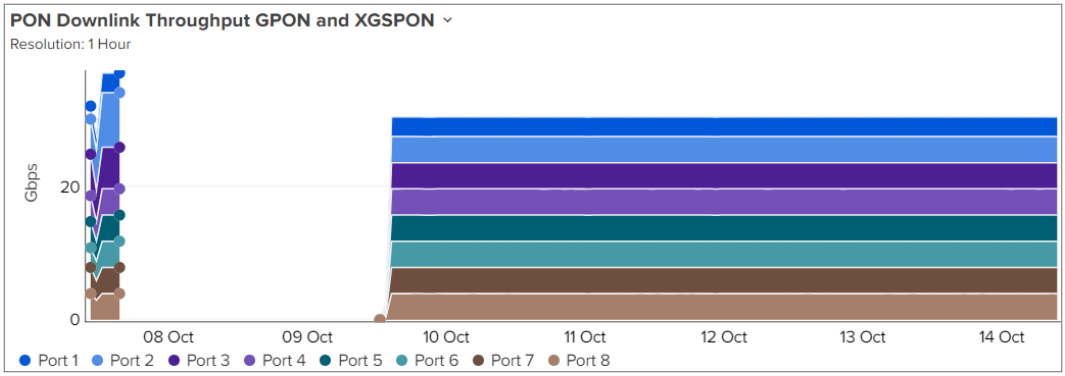
Figure 198 *PON Downlink Utilization*



PON Downlink Throughput

PON Downlink throughput displays the downlink throughput information of GPON and XGS-PON.

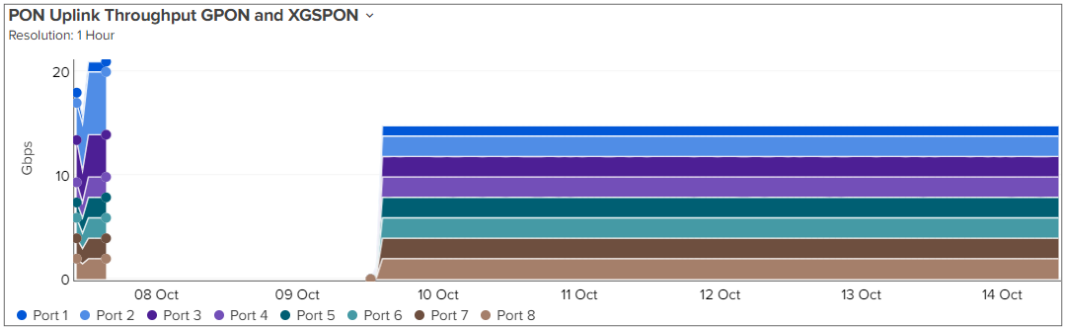
Figure 199 *PON Downlink Throughput*



PON Uplink Throughput

Displays the uplink throughput information of GPON and XGS-PON.

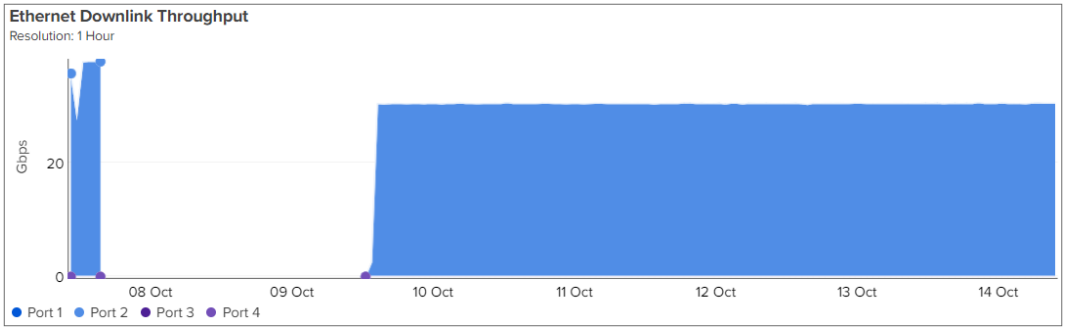
Figure 200 *PON Uplink Throughput*



Ethernet Downlink Throughput

Displays the Ethernet Downlink information of GPON and XGS-PON.

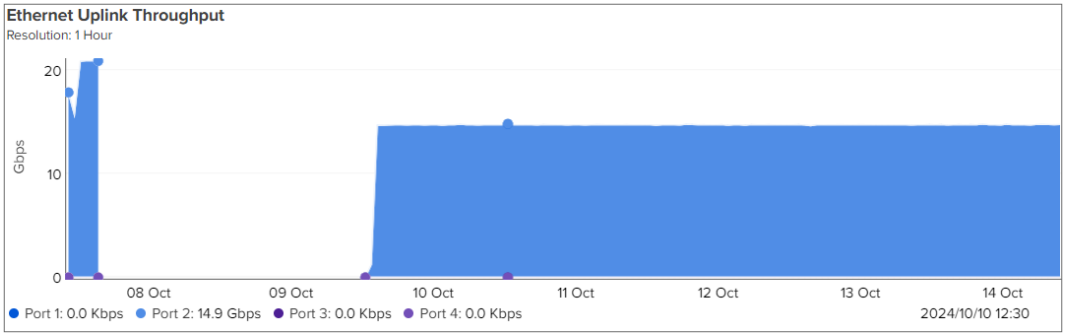
Figure 201 *Ethernet Downlink throughput*



Ethernet Uplink Throughput

Displays the Ethernet Uplink information of GPON and XGS-PON.

Figure 202 *Ethernet Uplink Throughput*



Notifications

Displays the alarm information of the OLT.

Figure 203 *Notifications*

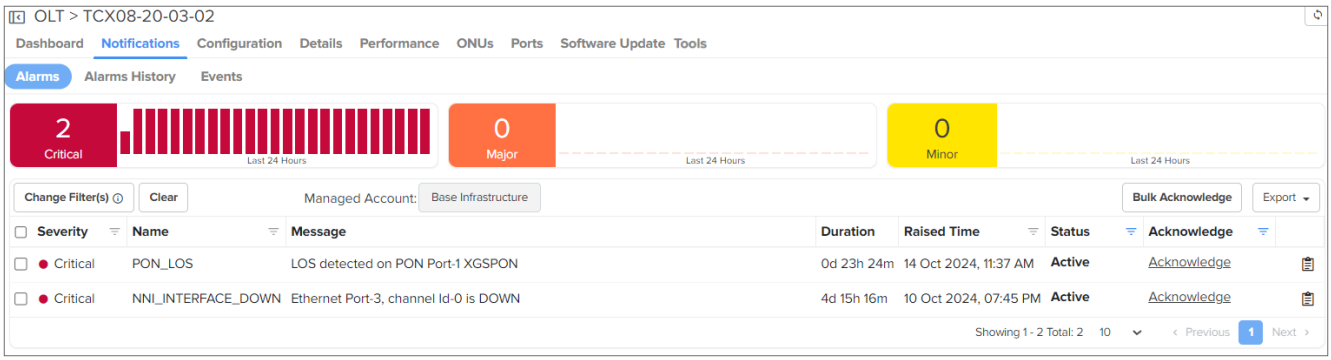


Table 61 *Parameters on the Notifications page*

Parameter	Description
Severity	Severity level of the alarm. This parameter supports the following severity levels: • Critical • Major

Parameter	Description
	• Minor
Source	Name of the OLT.
Mode	Type of the device. The following device types are supported: • 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: • 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 204 *Configuration*

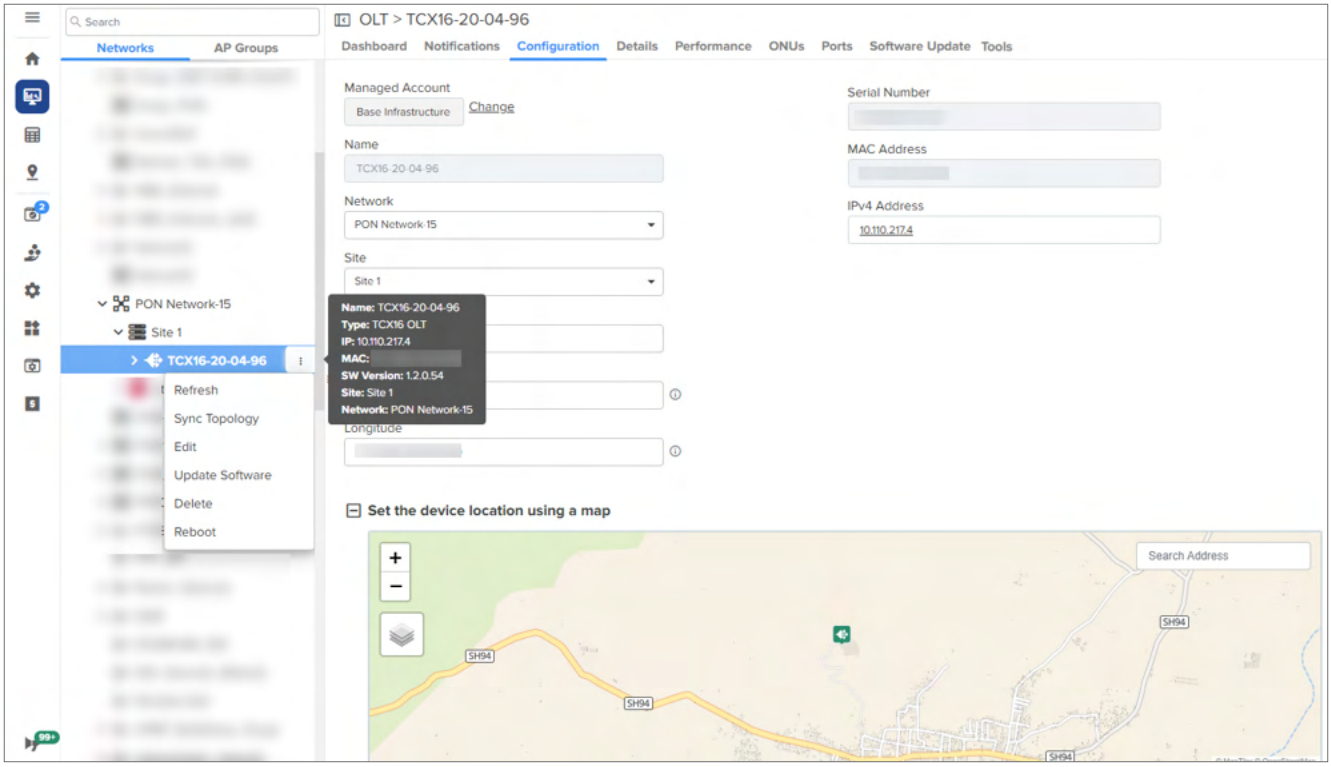


Table 62 *Parameters on the Configuration page*

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 205 *Details*

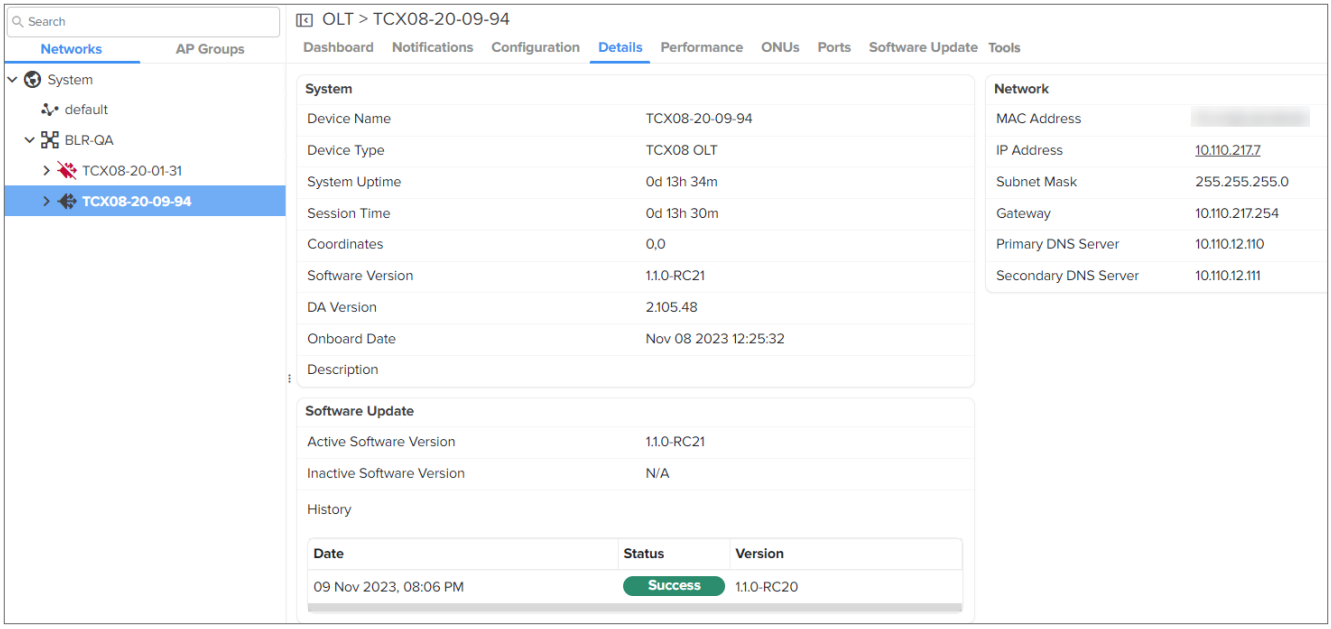


Table 63 *Parameters on the Details page*

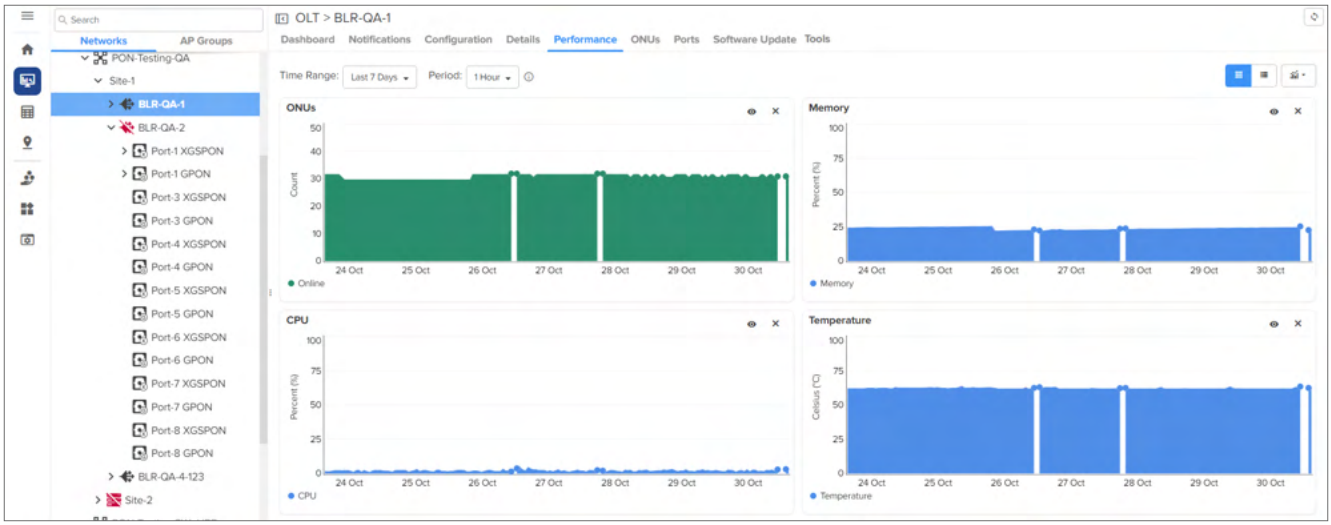
Parameter	Description
System	
Device Name	Name of the device.
Device Type	Type of the device. This parameter supports the following device types: • OLT • ONU

Parameter	Description
System Uptime	Date and time configured for the device.
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 206 *Performance*



ONUs

Displays the number of ONUs connected to the OLT and their information.

Figure 207 *ONU*

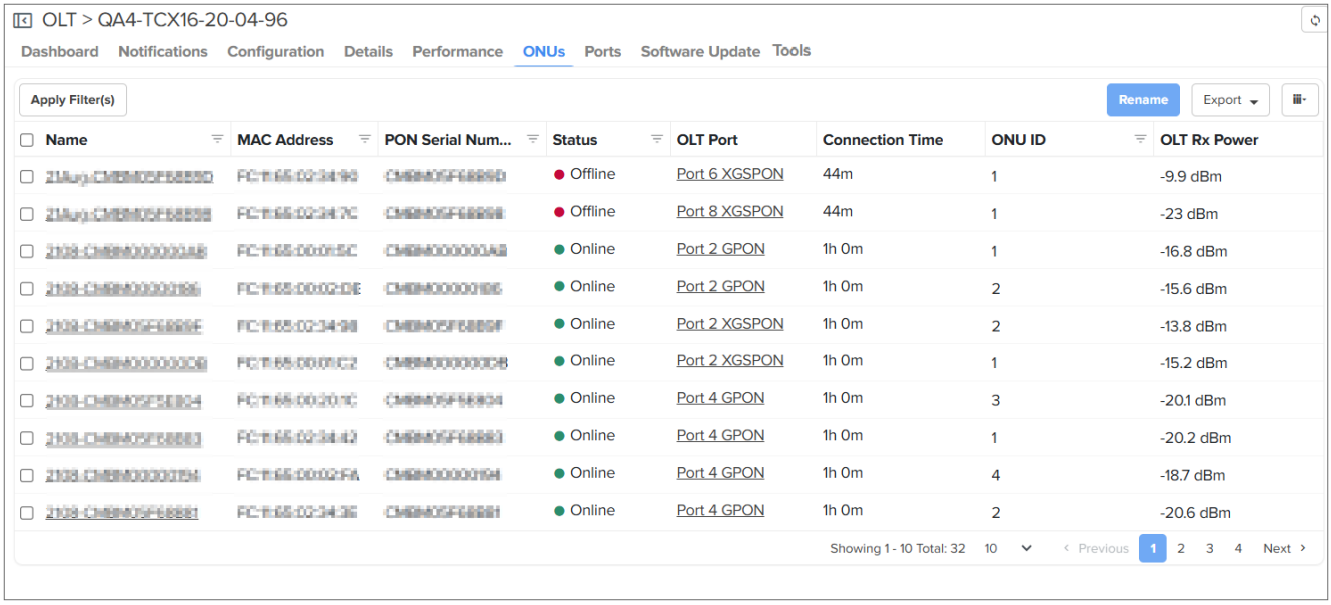


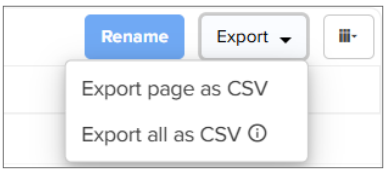
Table 64 *Parameters on the ONU page*

Parameter	Description
Name	Name of the OLT. Click the **Name** to view the ONU-specific Dashboard page as shown in Figure 210.
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.

Rename ONUs

The ONUs can be renamed either individually or using the bulk rename option. Bulk rename is available at the Port, OLT, and Site levels.

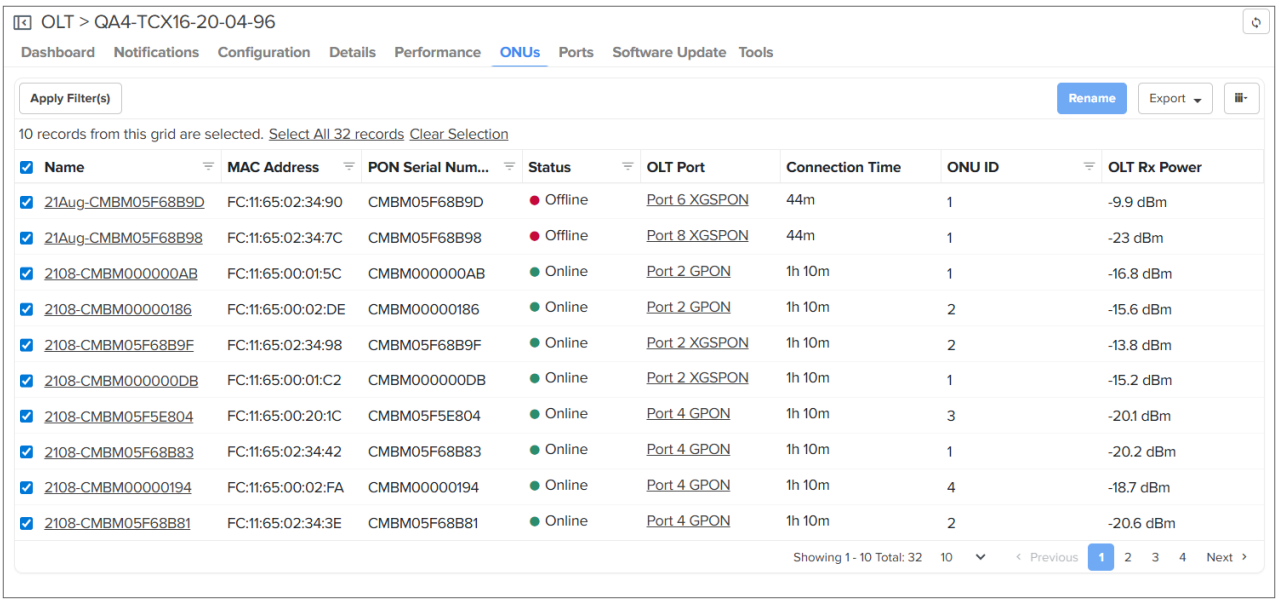
> **Note**
>
> Bulk rename of ONUs is supported on OLTs running version 1.3.0 or higher.

Perform the following procedure to rename the ONUs:

1. Navigate to the **Monitor and Manage** > **<Site-Name>** > **OLT** > **ONUs** tab.

   The **ONUs** page appears.

2. Select the required ONUs to rename.



Name	MAC Address	PON Serial Num...	Status	OLT Port	Connection Time	ONU ID	OLT Rx Power
21Aug-CMBM05F68B9D	FC:11:65:02:34:90	CMBM05F68B9D	Offline	Port 6 XGSPON	44m	1	-9.9 dBm
21Aug-CMBM05F68B98	FC:11:65:02:34:7C	CMBM05F68B98	Offline	Port 8 XGSPON	44m	1	-23 dBm
2108-CMBM000000AB	FC:11:65:00:01:5C	CMBM000000AB	Online	Port 2 GPON	1h 10m	1	-16.8 dBm
2108-CMBM00000186	FC:11:65:00:02:DE	CMBM00000186	Online	Port 2 GPON	1h 10m	2	-15.6 dBm
2108-CMBM05F68B9F	FC:11:65:02:34:98	CMBM05F68B9F	Online	Port 2 XGSPON	1h 10m	2	-13.8 dBm
2108-CMBM000000DB	FC:11:65:00:01:C2	CMBM000000DB	Online	Port 2 XGSPON	1h 10m	1	-15.2 dBm
2108-CMBM05F5E804	FC:11:65:00:20:1C	CMBM05F5E804	Online	Port 4 GPON	1h 10m	3	-20.1 dBm
2108-CMBM05F68B83	FC:11:65:02:34:42	CMBM05F68B83	Online	Port 4 GPON	1h 10m	1	-20.2 dBm
2108-CMBM00000194	FC:11:65:00:02:FA	CMBM00000194	Online	Port 4 GPON	1h 10m	4	-18.7 dBm
2108-CMBM05F68B81	FC:11:65:02:34:3E	CMBM05F68B81	Online	Port 4 GPON	1h 10m	2	-20.6 dBm

3. Click **Rename**.

   The **Rename Selected Devices** window appears.

4. Click **download CSV** to download the .csv file.
5. Open the CSV file and update the names as required.
6. Save the file and **Select File** to upload it back.
7. Click **Rename**.

Ports

Displays the port details. Fiber OLT has 8 ports and 16 ports.

Figure 208 *Ports*

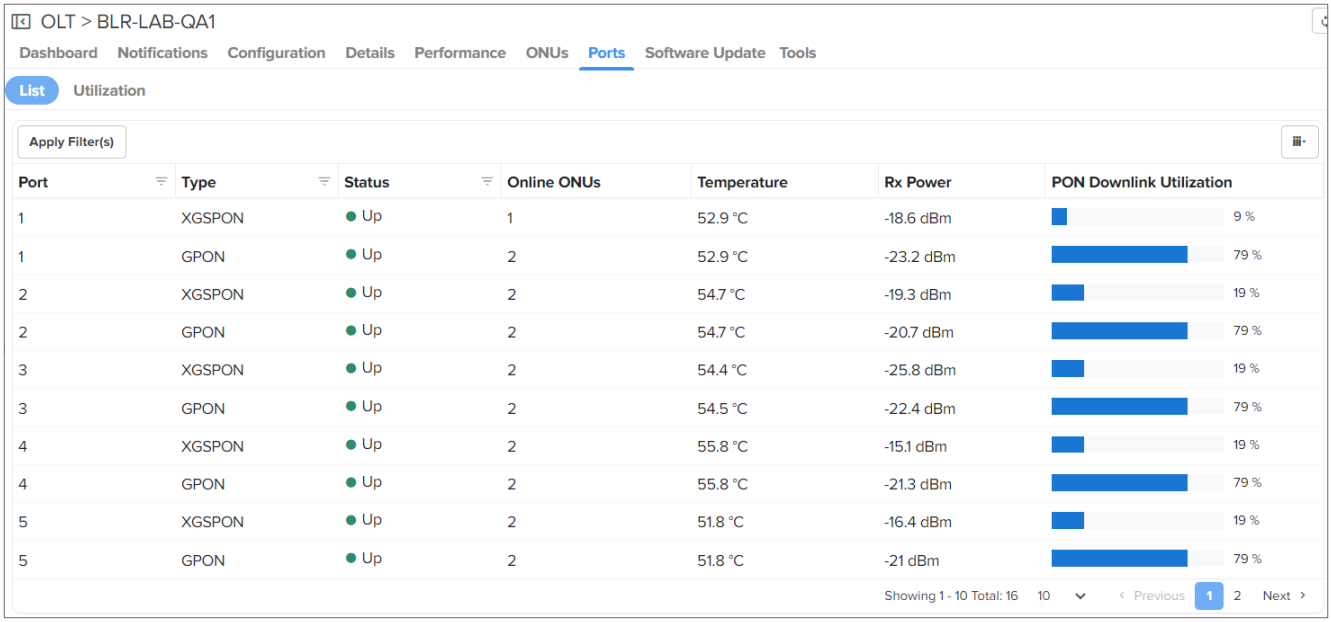
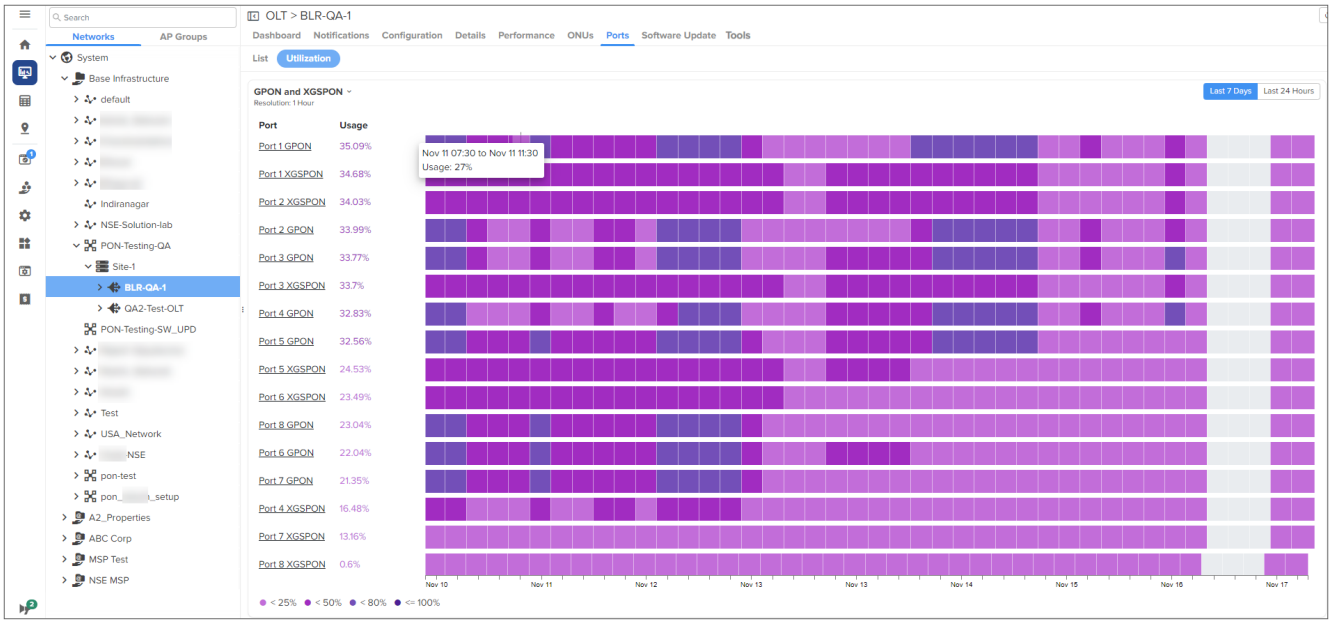


Figure 209 *Ports utilization*



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)**.

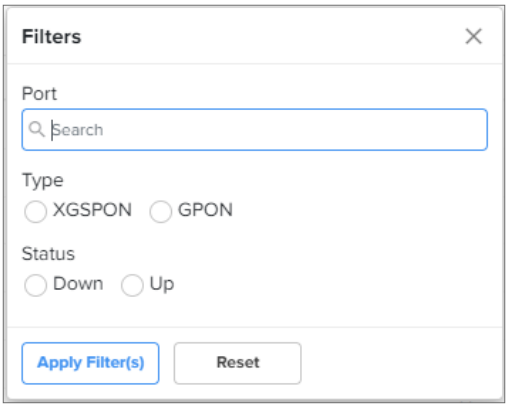


Table 65 *Parameters on the Ports page*

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.

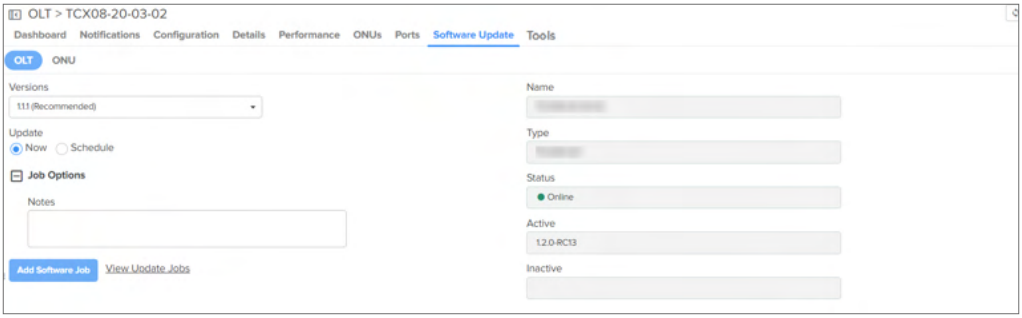
OLT Software Update

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.



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.

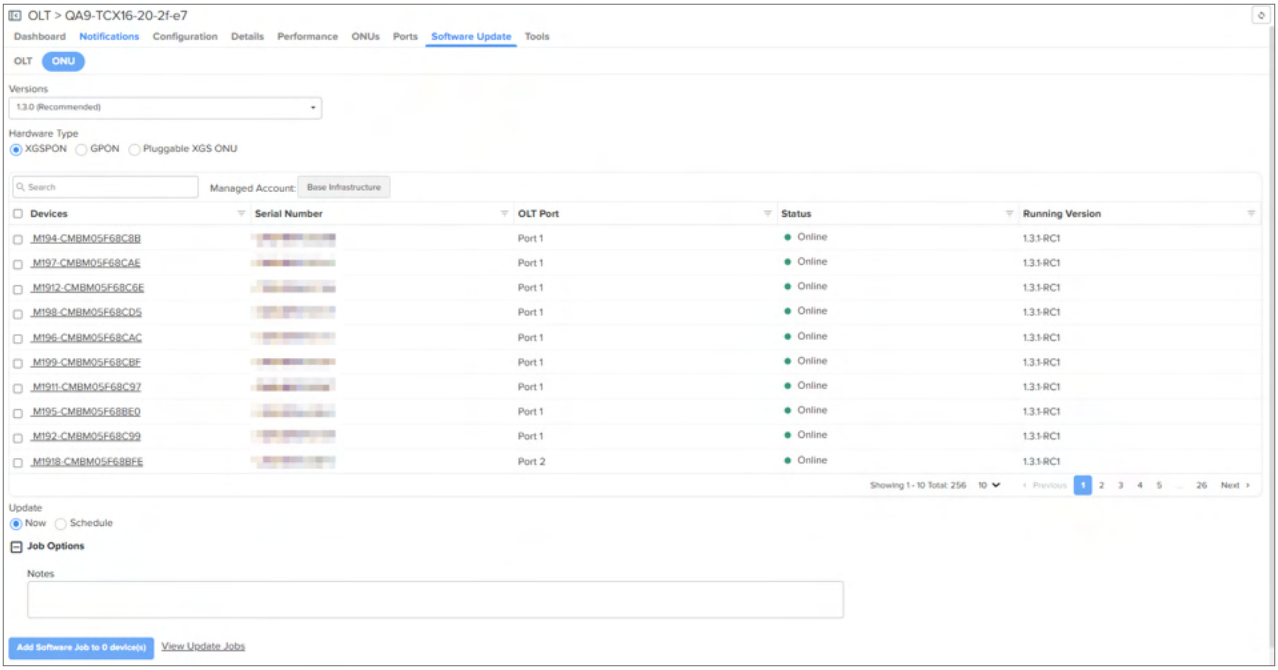
To upgrade the software for ONU, perform the following steps:

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 required **Hardware Type**, such as XGSPON, GPON, or a Pluggable XGS ONU.

   > **Note**
   >
   > The Pluggable XGS ONU software update is supported only for version 1.3.0 or later when upgraded through cnMaestro.
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.



Click **View Update Jobs** to view the history of the software updates. This provides a record of all previous software update jobs.

Tools

> **Note**
>
> The ONU Tech Support is applicable only when the OLT software is upgraded to version 1.3.0 or higher.

In **Tools** tab, user can view the status of the device (either Online or Offline). It also supports downloading the Tech Support File and rebooting the device.

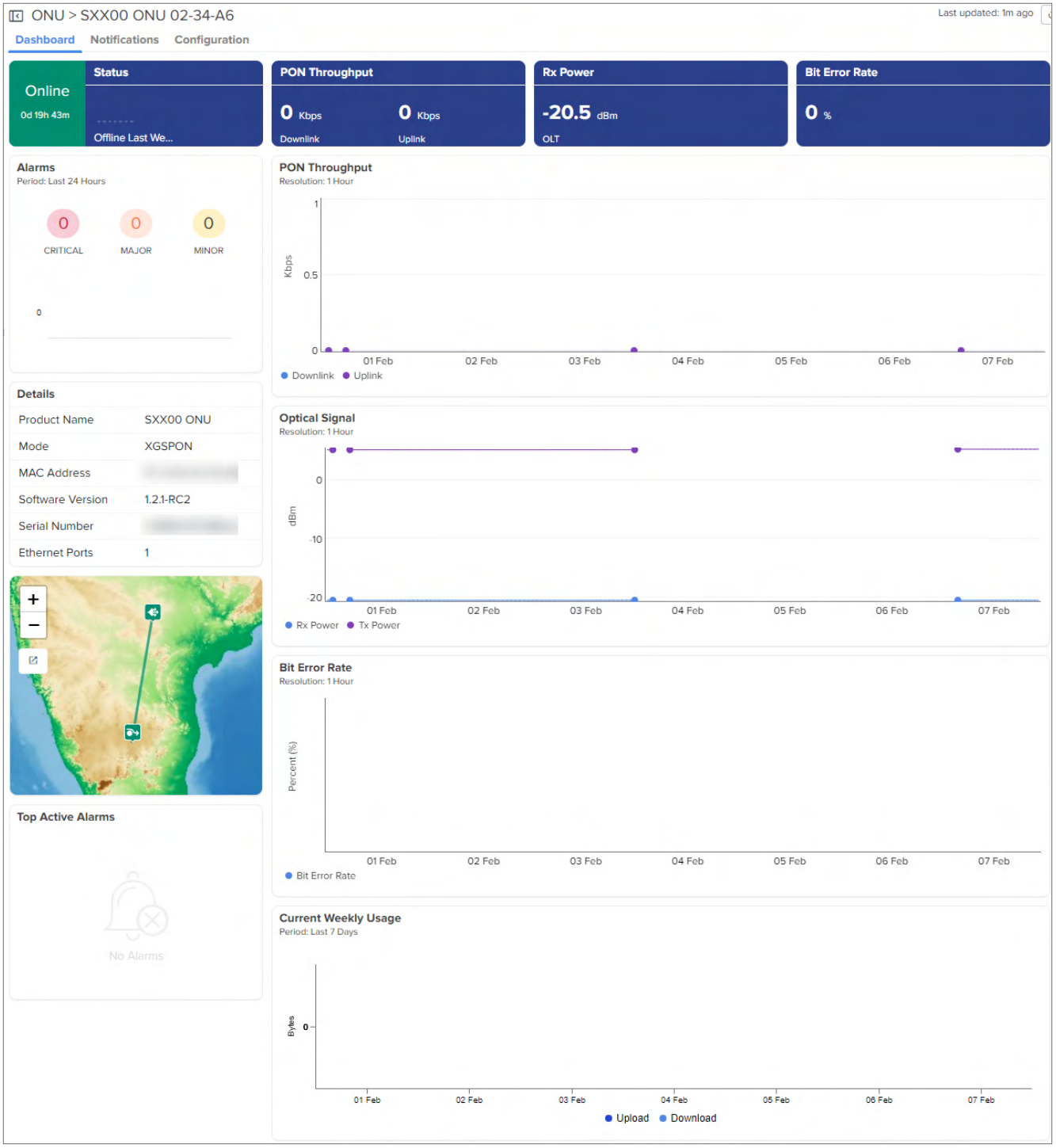
ONU Dashboard

> **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

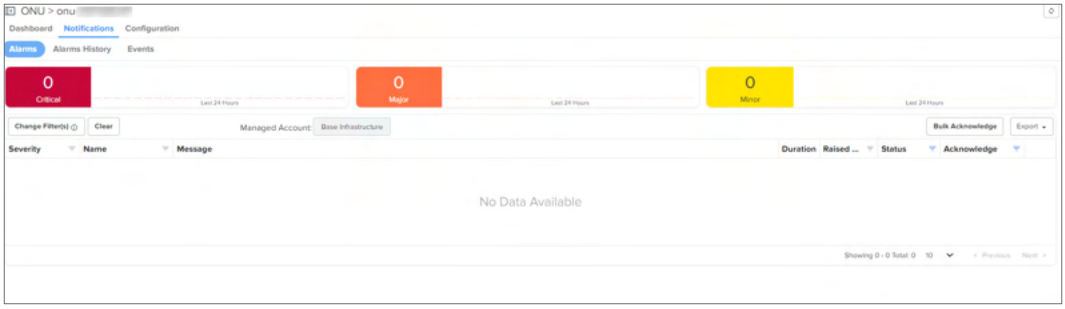
Figure 210 *ONU Dashboard*



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 Notifications tab displays ONUs information, such as the Alarms, Alarms History, and Events.

Figure 211 *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. Edit the **Name**.
2. Enter **Description**.
3. Enter **Latitude**.
4. Enter **Longitude**.
5. Click **Apply Configuration**.

Figure 212 *ONU Configuration*

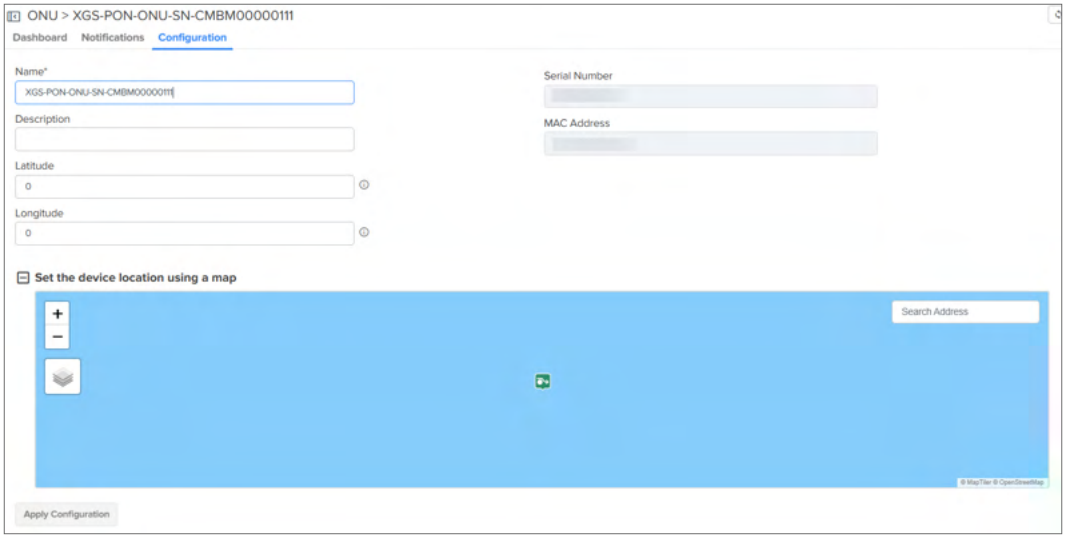


Table 66 *Parameters on the Configuration page*

Parameter	Description
Name	Name of the ONU. **Note** Starting from Release 5.2.2, cnMaestro supports editing the ONU name. This feature is supported when the OLT is running version 1.3.0 or later.
Description	A brief description of the ONU.
Latitude	Latitude of the ONU.

Parameter	Description
Longitude	Longitude of the ONU.
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 213 *Inventory page at the System-level*

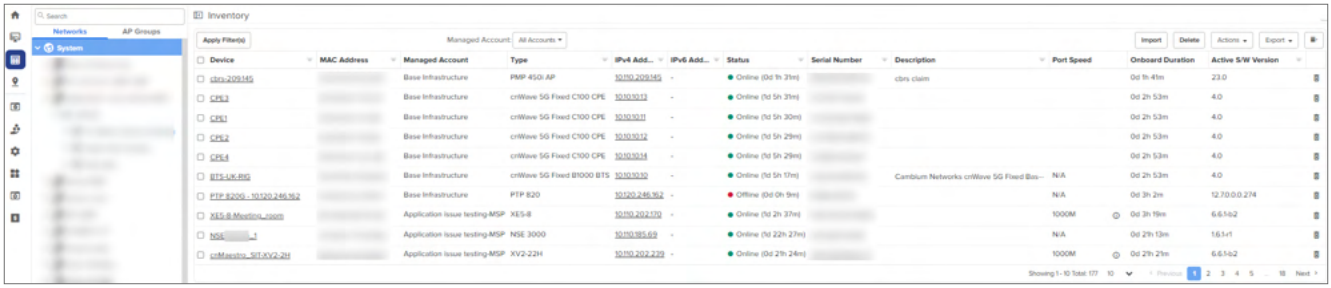


Figure 214 *Inventory page at the Site-level*

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

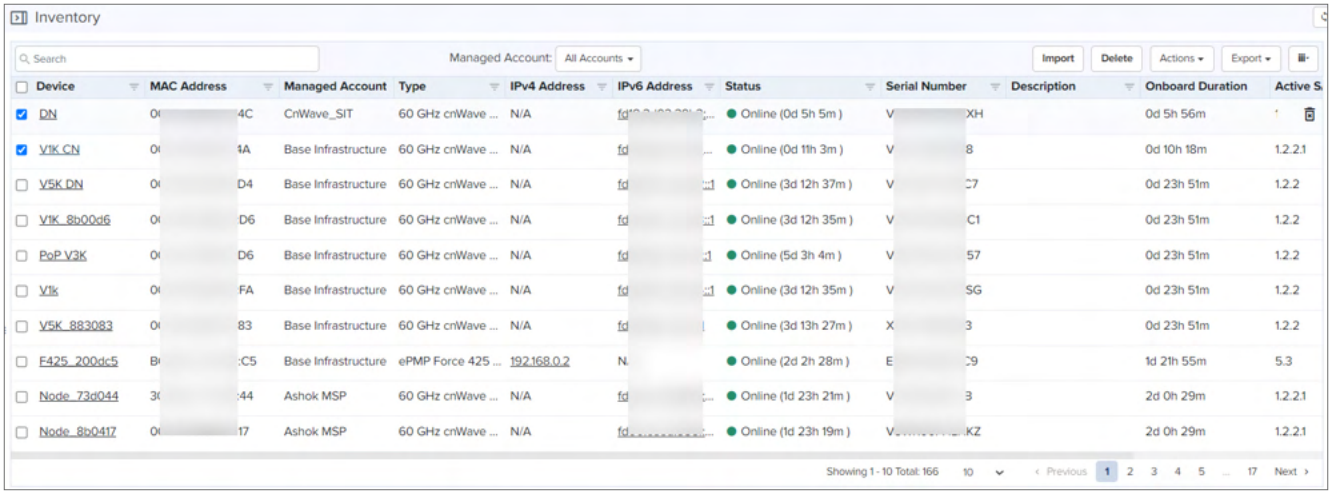
Inventory export is supported for PON devices starting from version 5.2.1.

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.

Bulk Delete

The **Bulk Delete** option is available in the inventory page of System/MSP/Tower/Network/Site.

Figure 215 *Bulk Delete*



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.

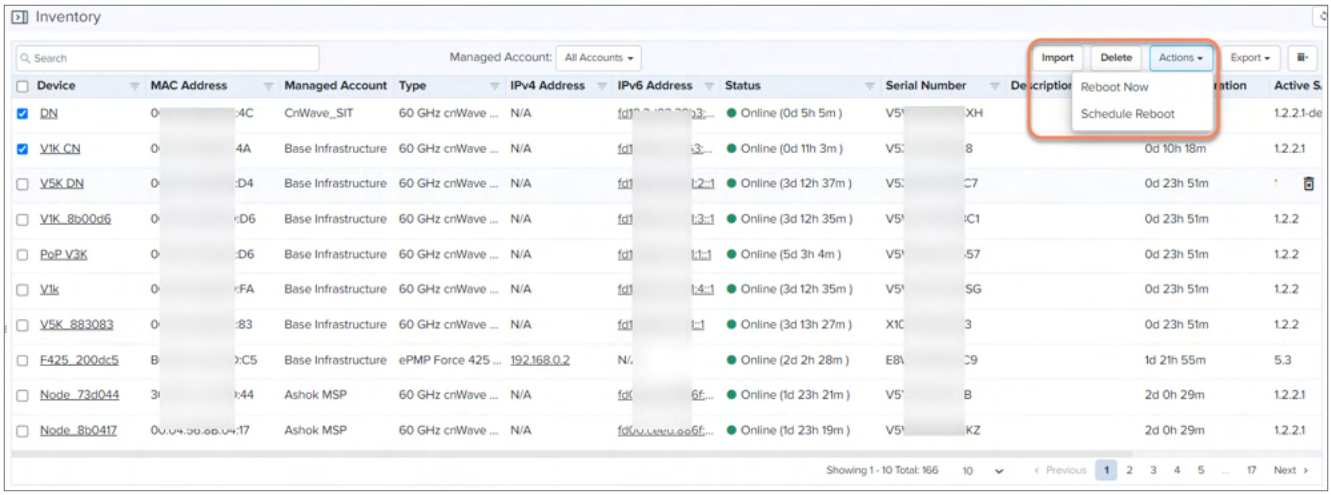
For more information about deleting devices in bulk, see Deleting Devices in Bulk.

> **Note**
>
> The maximum number of devices allowed for bulk deletion is 5000 devices. If it is more than that, then filter the inventory and start deleting the devices.

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 216 *Bulk Reboot*



To reboot devices using bulk reboot, perform the following steps:

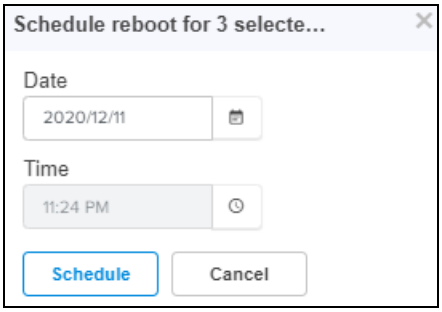
1. Navigate to **Inventory** page of Network/Tower/Site.
2. Select one or multiple devices.
3. Click **Actions** and choose **Reboot Now**.

Schedule Reboot

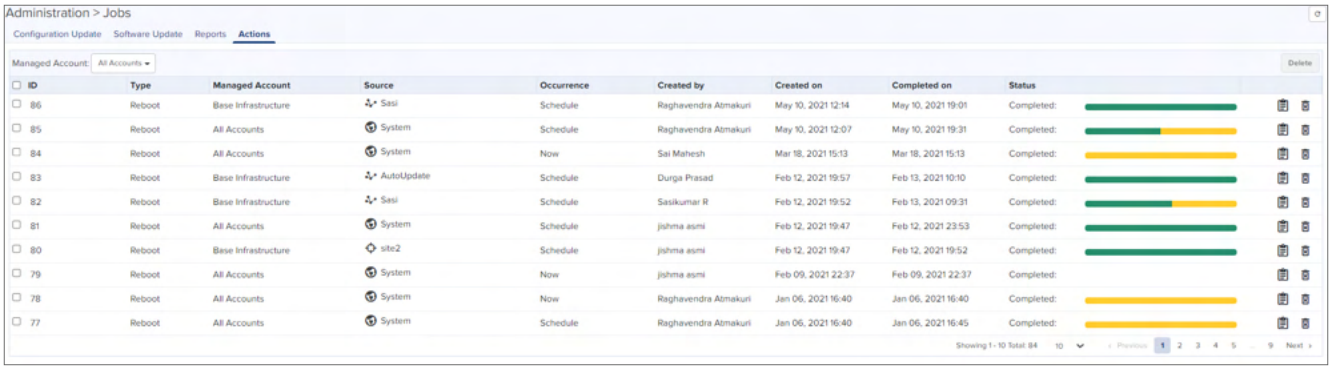
Schedule a reboot of the device(s) by selecting **Schedule Reboot** from **Actions** dropdown.

To reboot devices using schedule reboot, perform the following steps:

1. Navigate to **Inventory** page of Network/Tower/Site.
2. Select one or multiple devices.
3. Click **Actions** and choose **Schedule Reboot**.
4. Enter **Date** and **Time**.
5. Click **Schedule**.



After creating a scheduled reboot job, you can view the status in the **Administration** > **Jobs** > **Actions** page.



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.

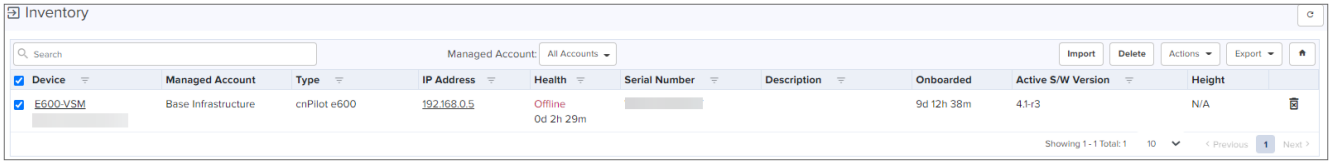
The following parameters are supported for ePMP/PMP AP in the CSV file:

- Azhimuth
- Beamwidth
- Elevation
- Height
- Latitude
- Longitude

The following parameters are supported for ePMP/PMP SM is in the CSV file:

- Latitude
- Longitude

Figure 217 *Import Device Configuration*

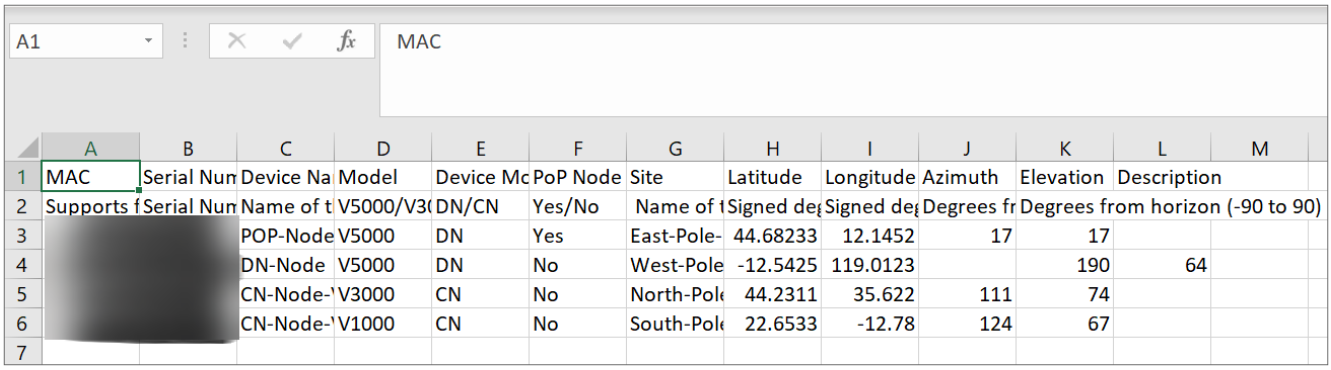


Sample Configuration File

MAC	LATITUDE	LONGITUDE	AZIMUTH	ELEVATION	BEAM WIDTH	HEIGHT	HEIGHT UNIT
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)

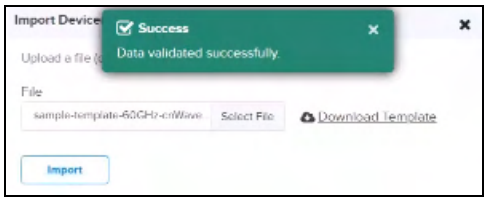
Figure 218 *Sample Configuration file: 60 GHz cnWave*



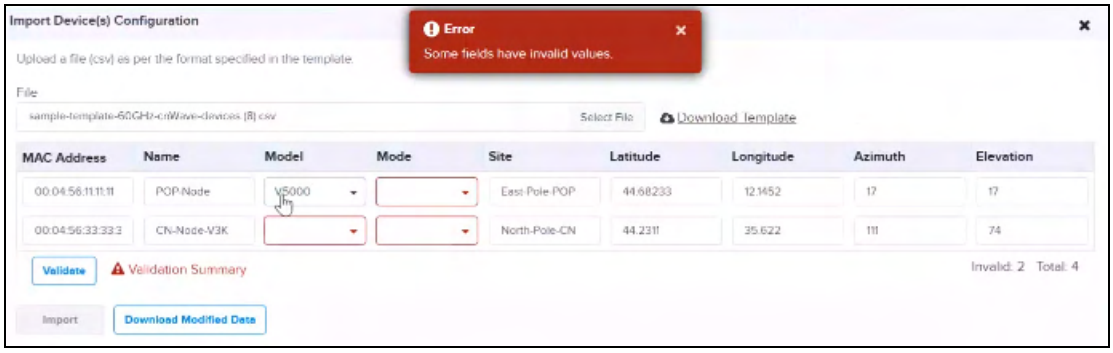
A1 | MAC

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	MAC	Serial Nun	Device Na	Model	Device Mc	PoP Node	Site	Latitude	Longitude	Azimuth	Elevation	Description	
2	Supports f	Serial Nun	Name of t	V5000/V3(	DN/CN	Yes/No	Name of t	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:



Uploading a Configuration File

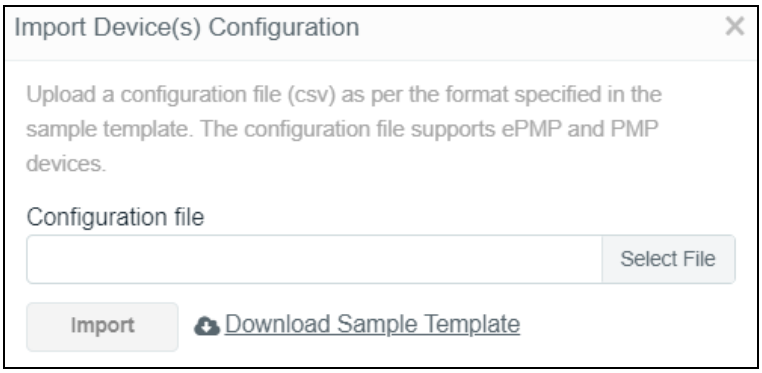
To upload a configuration file (CSV) using the format specified in the sample template, perform the following steps:

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.

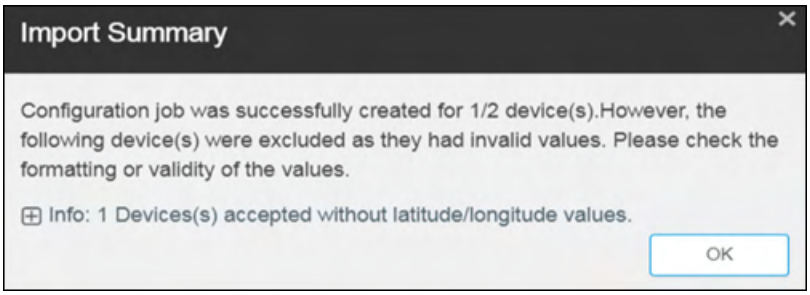
> **Note**
>
> You must know the MAC address of the device to push the configuration.

3. Click **Import**.

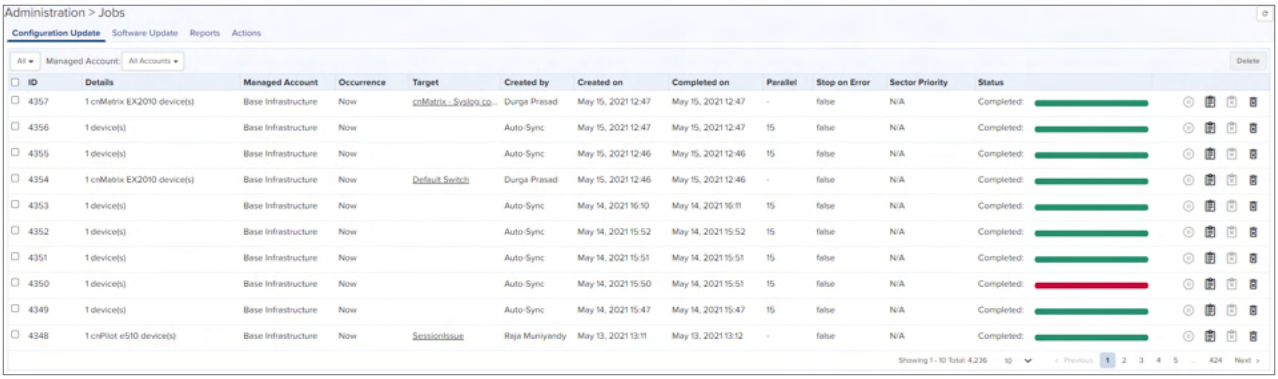
Figure 219 *Uploading Configuration file*



4. A configuration job will be created.



5. You can view the completed status of the configuration import in the configuration update page.



The following table provides details on different errors that might occur while importing a CSV file:

Table 67 *Importing Error*

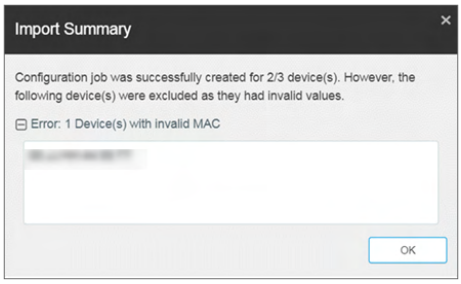
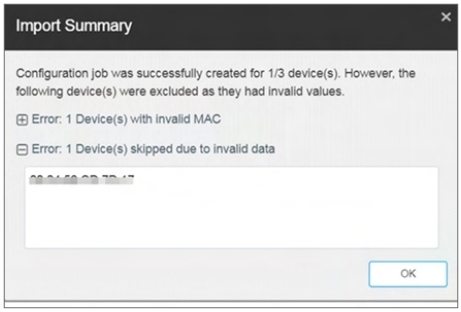
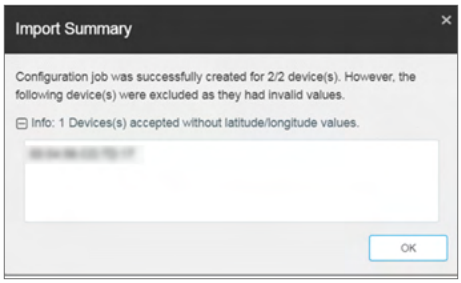
Error	Description
{Count of Devices} Device(s) with invalid MAC	This error is displayed if the uploaded CSV file contains an invalid MAC Address. 
{Count of Devices} Device(s) skipped due to invalid data	This error is displayed if the uploaded CSV file contains invalid Data or data not relevant for Latitude, Longitude, Azimuth, Height, and Elevation. 

Table 67 *Importing Error*

Error	Description
Devices were not found for supplied MAC Address	This error message is displayed if the devices were not found with correct MAC address in the CSV file.
Info: 1 Devices(s) accepted without latitude/longitude values	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. 

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.

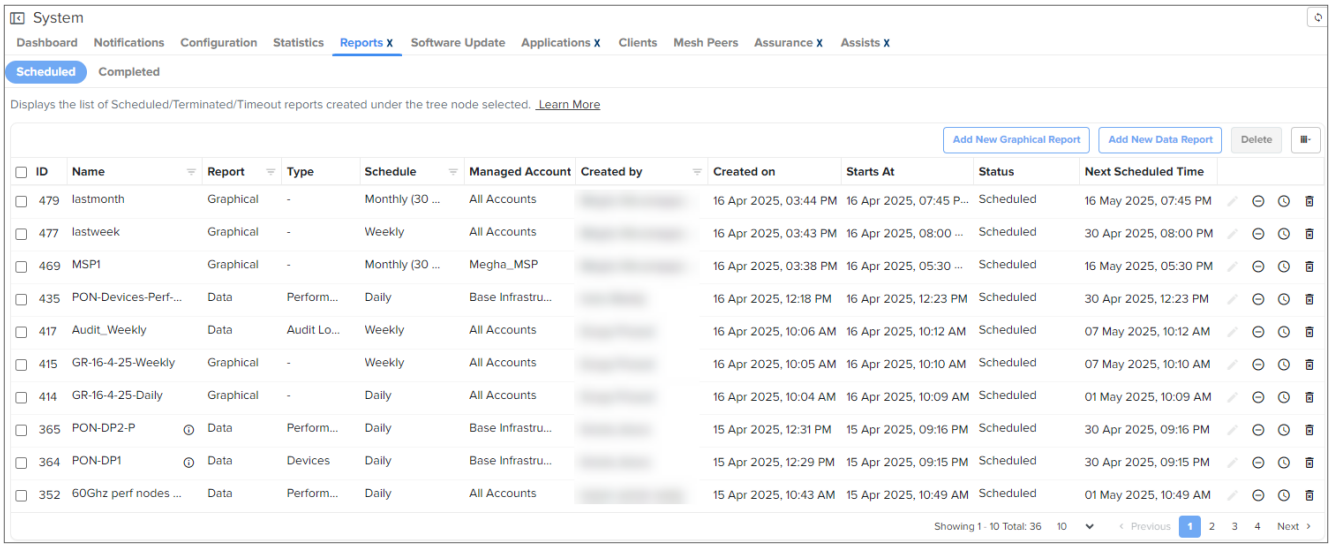
Scheduled Reports include the Scheduled, Terminated, and Timeout status in the Status column. **Completed Reports** include the Completed and Failed status is the Status column. Data reports are displayed only in a tabular format while graphical reports include charts and graphs.

Note

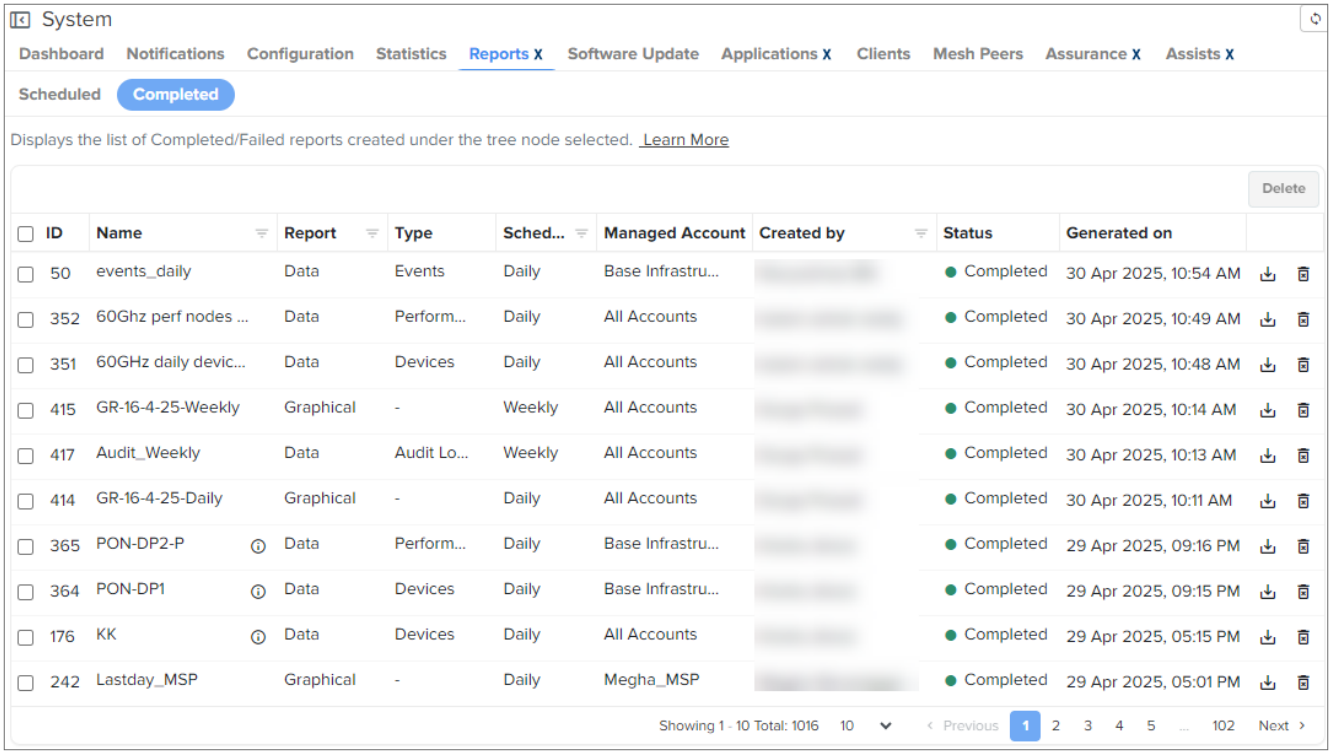
You can schedule and view reports (data and graphical) at the following levels in cnMaestro:

- System
- Network—Only data reports are available
- Site
- MSP

To view all scheduled data and graphical reports, navigate to **Monitor and Manage** > **System/<Nework-name>/<Site-name>/<MSP-name>** > **Reports** X > **Scheduled**.



To download completed reports, navigate to **System** > **Monitor and Manage** > **Reports X** > **Completed**.



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.

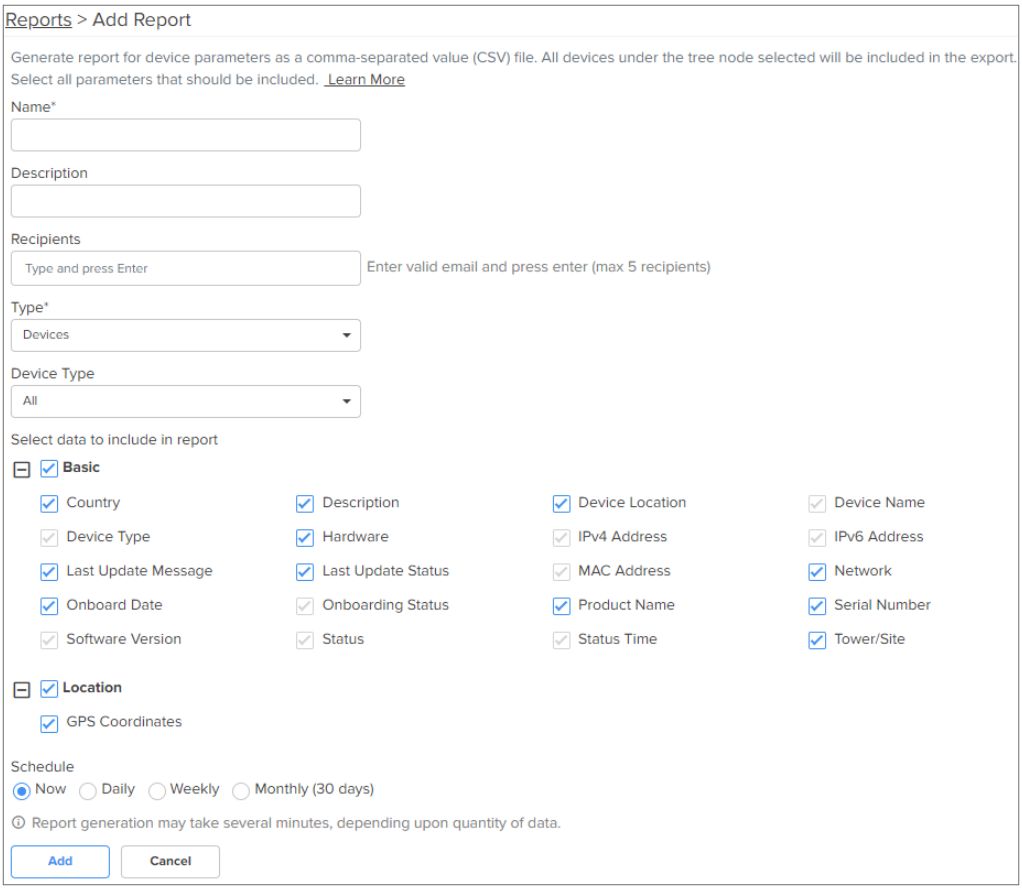
- Devices Report
- Audit Logs Report
- Performance Report
- Active Alarms Report
- Alarm History Report
- Events Report
- Wireless Clients Report
- Wi-Fi Events Report
- Mesh Peers Report
- Guest Access Login Events
- Remote Upload
- Reports jobs

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.



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:

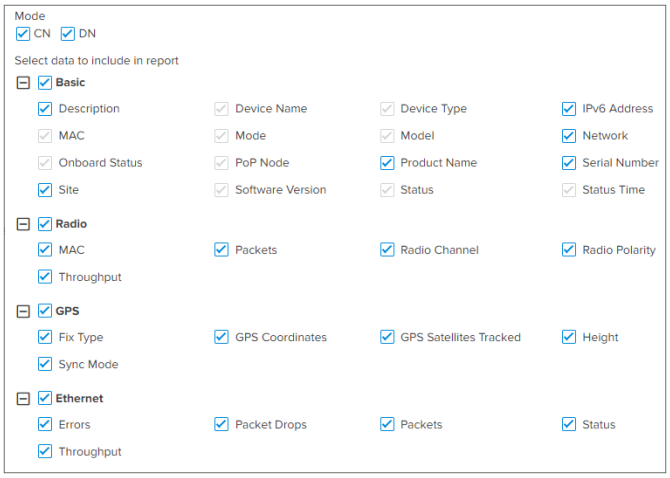
- 60 GHz cnWave
- cnMatrix
- cnPilot Home (R-Series)
- cnRanger
- cnReach
- cnReach XIO
- cnVision
- cnWave 5G Fixed
- Enterprise Wi-Fi

- ePMP
- PMP
- PON
- PTP 650/670/700
- PTP 820/850

If 60 GHz cnWave device is selected as **Device Type**, then the following parameter sections are available:

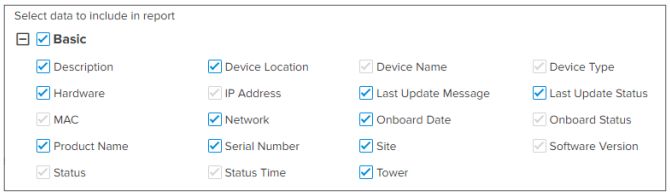
- Mode (CN or DN)
- Basic
- Ethernet
- GPS
- Radio

Figure 220 *Device Report: 60 GHz cnWave*



If cnMatrix is selected as the **Device Type**, then **Basic** data export parameters will be exported.

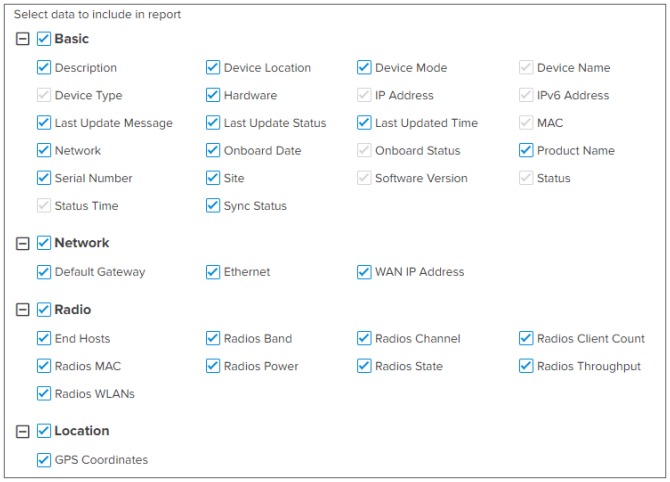
Figure 221 *Device Report: cnMatrix*



If cnPilot Home (R-Series) is selected as the **Device Type**, then the following parameter sections are available:

- Basic
- Location
- Network
- Radio

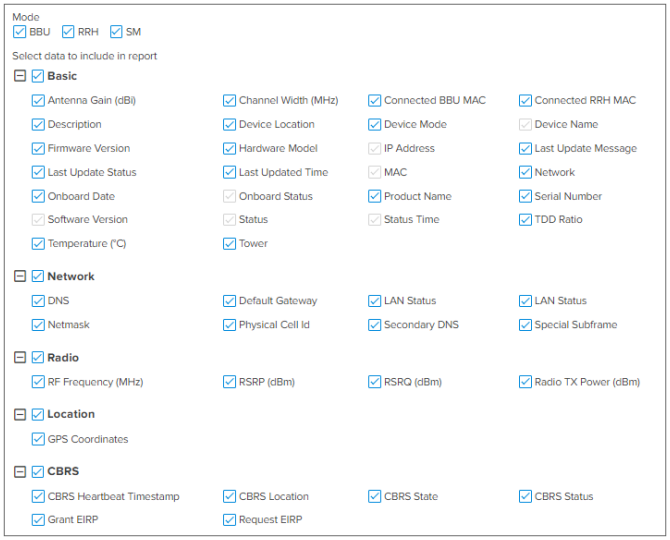
Figure 222 *Device Report: cnPilot Home (R-Series)*



If cnRanger is selected as the **Device Type**, then the following parameter sections are available:

- Basic
- CBRS
- Location
- Network
- Radio

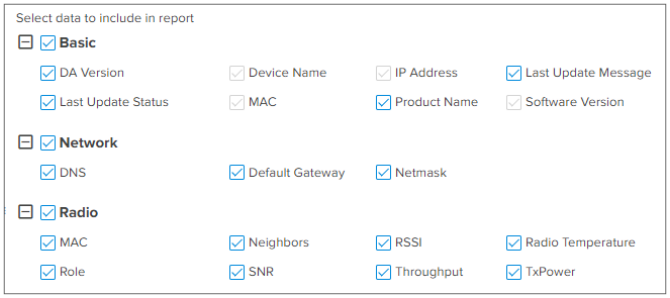
Figure 223 *Device Report: cnRanger*



If cnReach is selected as the **Device Type**, then the following sections are available:

- Basic
- Network
- Radio

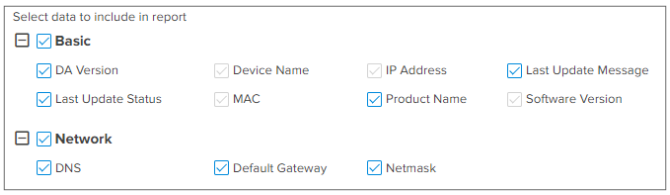
Figure 224 *Device Report: cnReach*



If cnReach XIO is selected as the **Device Type**, then the following sections are available:

- Basic
- Network

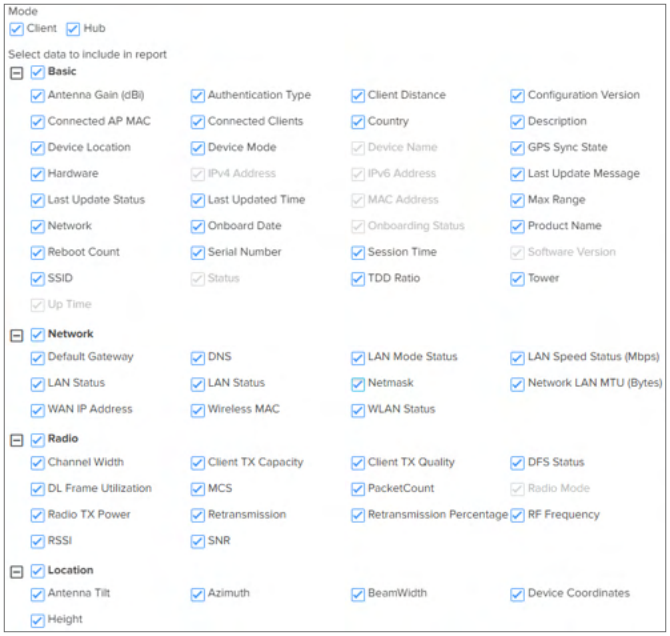
Figure 225 *Device Report: cnReach XIO*



If cnVision is selected as the **Device Type**, then the following sections are available:

- Mode (Client or Hub)
- Basic
- Location
- Mode
- Network
- Radio

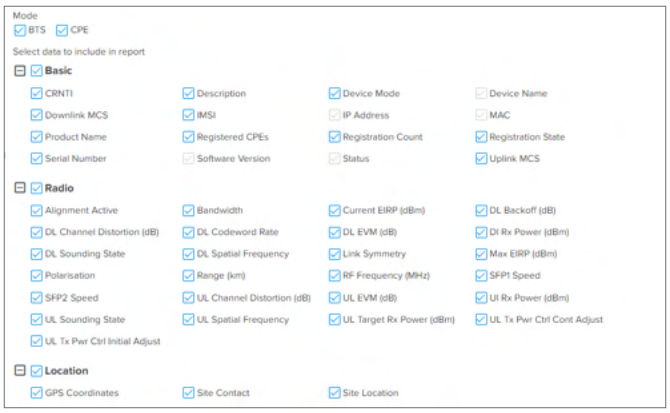
Figure 226 *Device Report: cnVision*



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

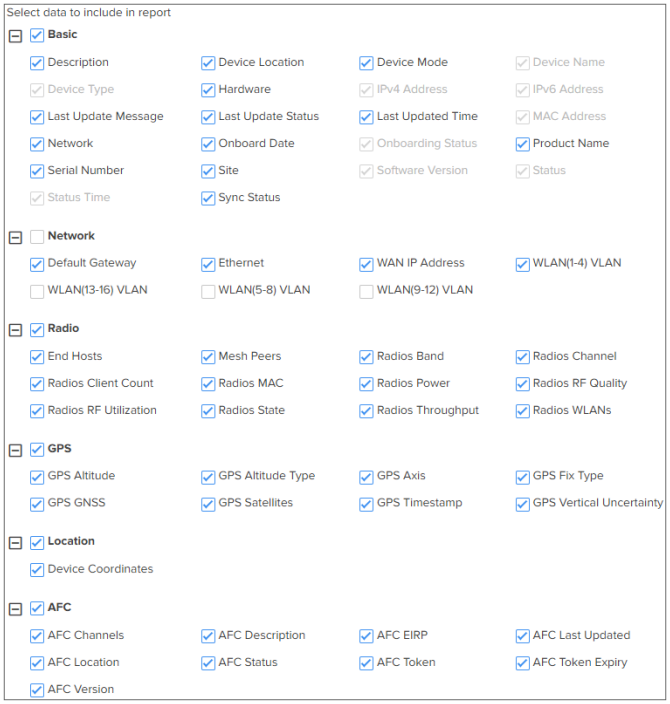
Figure 227 *Device Report: cnWave 5G Fixed*



If Enterprise Wi-Fi is selected as the **Device Type**, then the following sections are available:

- AFC
- Basic
- GPS
- Location
- Network
- Radio

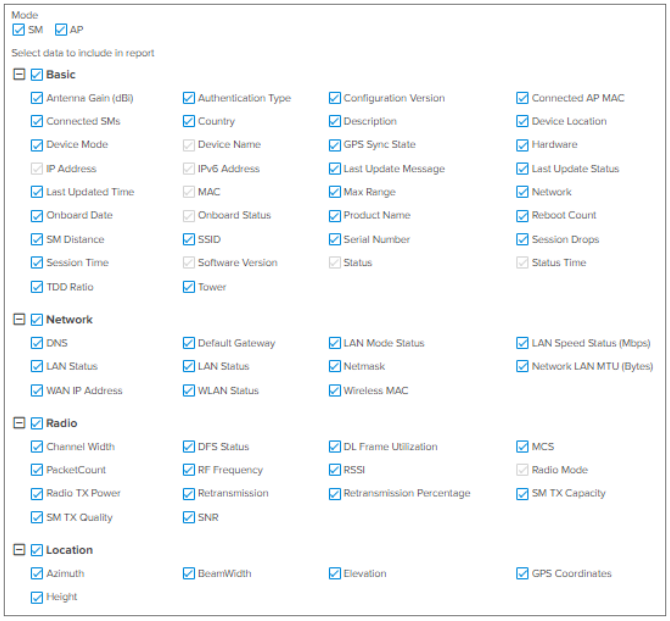
Figure 228 *Device Report: Enterprise(Wi-Fi)*



If ePMP is selected as the **Device Type** then the following sections are available:

- Mode (AP or SM)
- Basic
- Location
- Network
- Radio

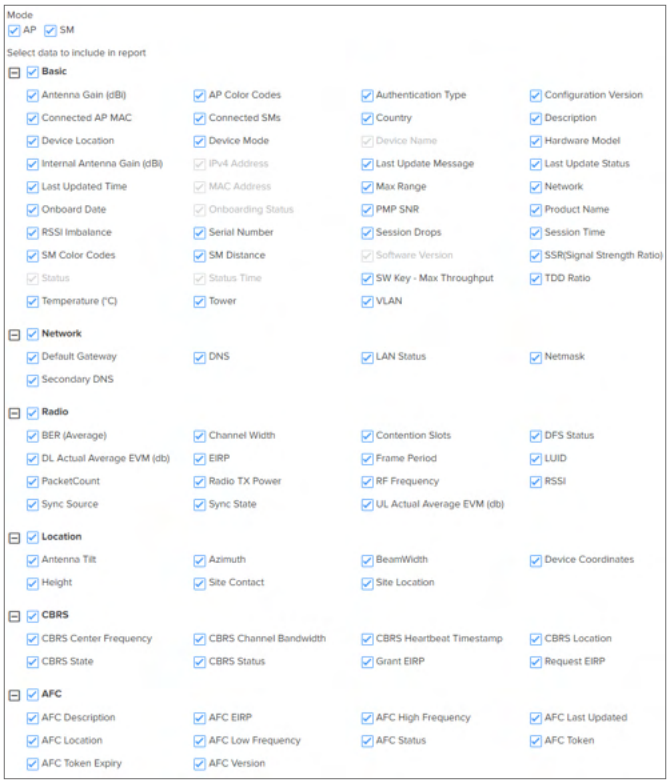
Figure 229 *Device Report: ePMP*



If PMP is selected as the **Device Type**, then the following sections are available:

- Mode (AP or SM)
- AFC
- Basic
- CBRS
- Location
- Network
- Radio

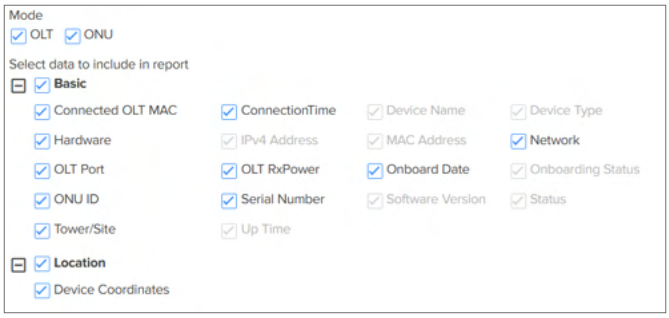
Figure 230 *Device Report: PMP*



If PON is selected as the **Device Type**, then the following sections are available:

- Basic
- Location

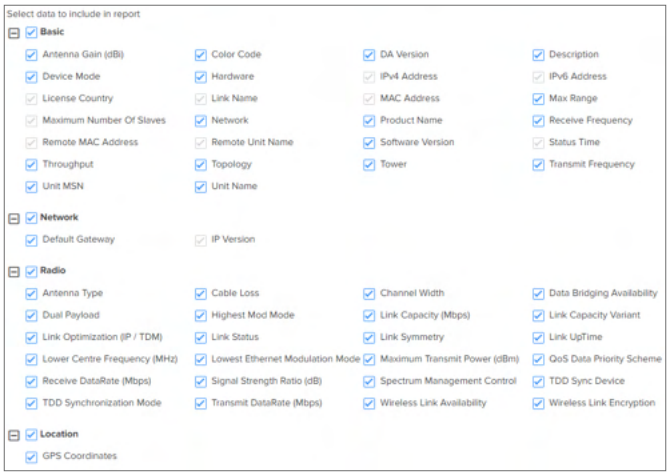
Figure 231 *Device Report: PON*



If PTP 650/670/700 is selected as the **Device Type**, then the following sections are available:

- Basic
- Location
- Network
- Radio

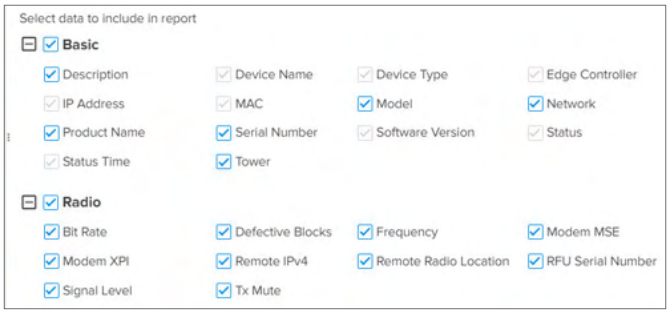
Figure 232 *Device Report: PTP 650/670/700*



If PTP 820/850 is selected as the **Device Type**, then the following sections are available:

- Basic
- Radio

Figure 233 *Device Report: PTP 820/850*



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.

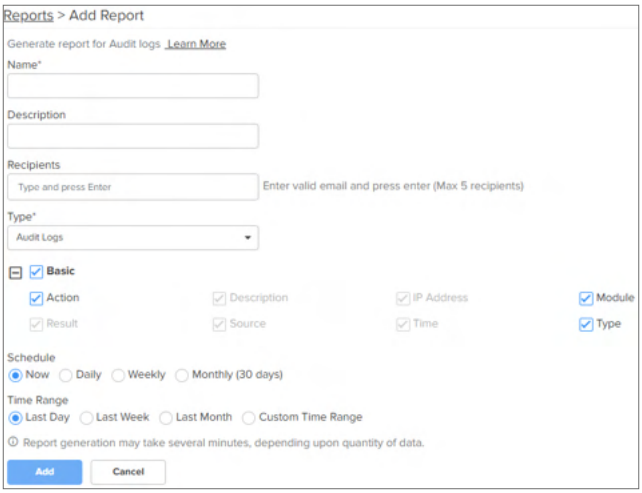
To generate the Audit Logs report, perform the following steps:

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, or Weekly.)
   - Time Range (Last Day, Last Week. Last Month, or Custom Time Range)
8. Click **Add**. The report is saved and listed in the **Scheduled Reports** page.

   Figure 234 *Audit Logs Report*



Performance Report

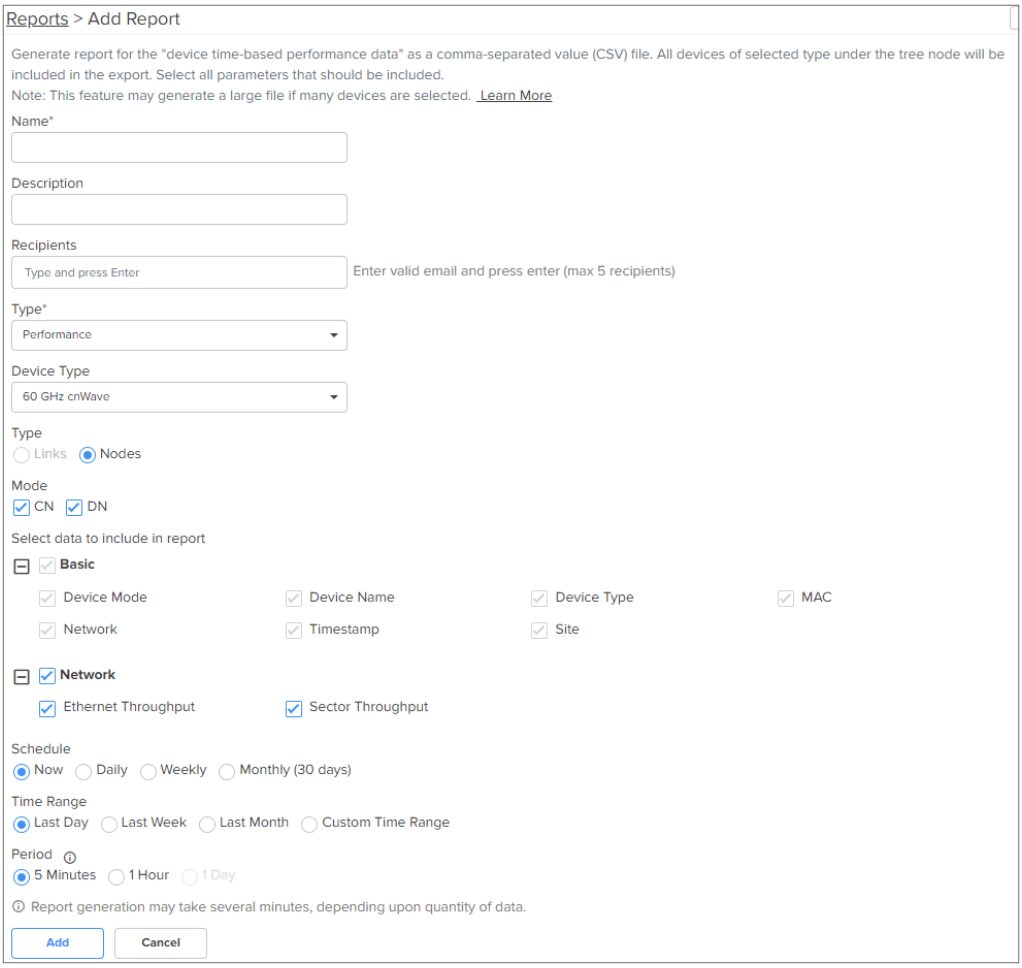
The Performance Report generates device time-series performance data as a comma-separated value (CSV) file. All devices of selected type under the tree node will be included in the export.

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**.



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 235 *Performance Report: 60 GHz cnWave (Links Type)*

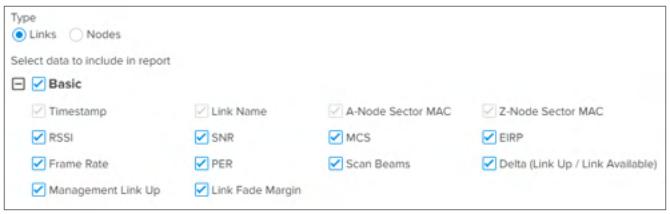
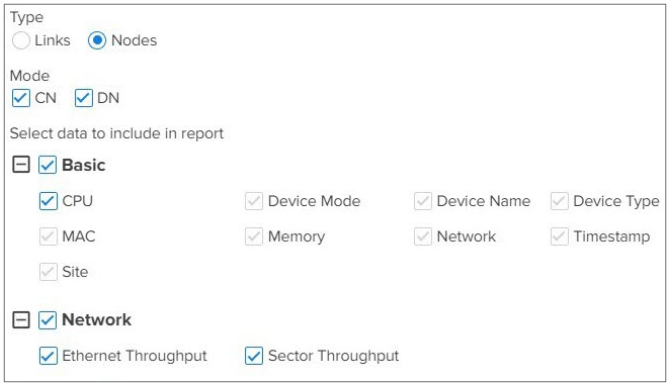
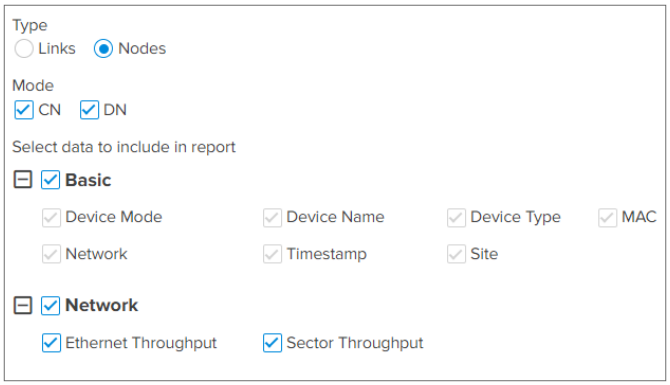


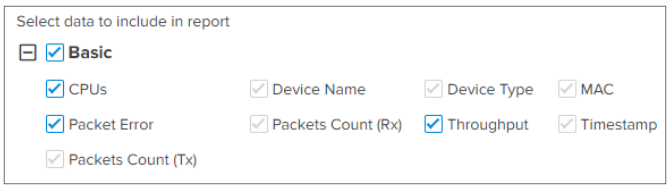
Figure 236 *Performance Report: 60 GHz cnWave (Node Type)*





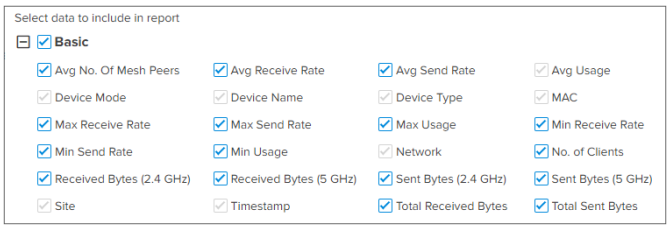
cnMatrix Performance Report

Figure 237 *Performance Report: cnMatrix*



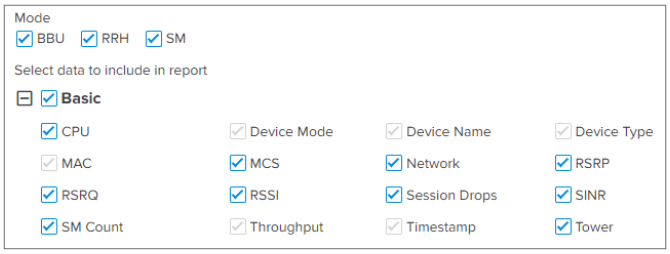
cnPilot Home (R-Series) Performance Report

Figure 238 *Performance Report: cnPilot Home (R-Series)*



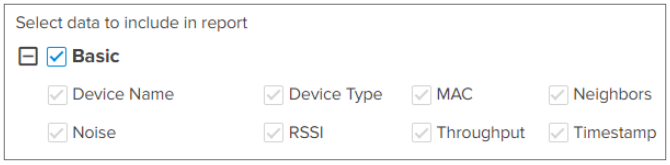
cnRanger Performance Report

Figure 239 *Performance Report: cnRanger*



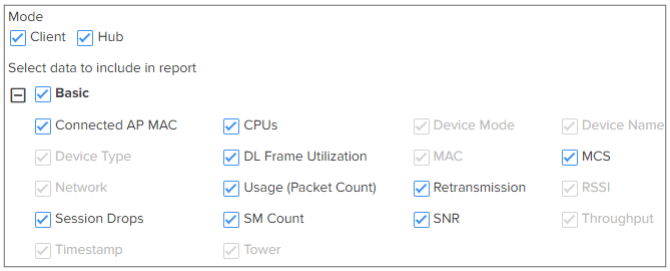
cnReach Performance Report

Figure 240 *Performance Report: cnReach*



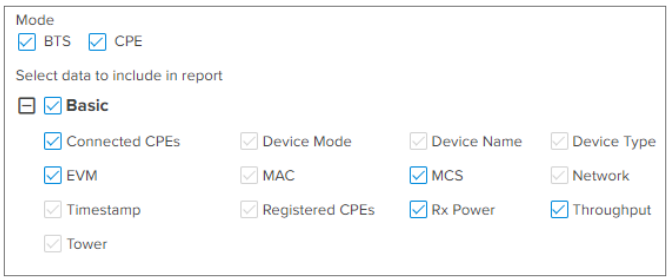
cnVision Performance Report

Figure 241 *Performance Report: cnVision*



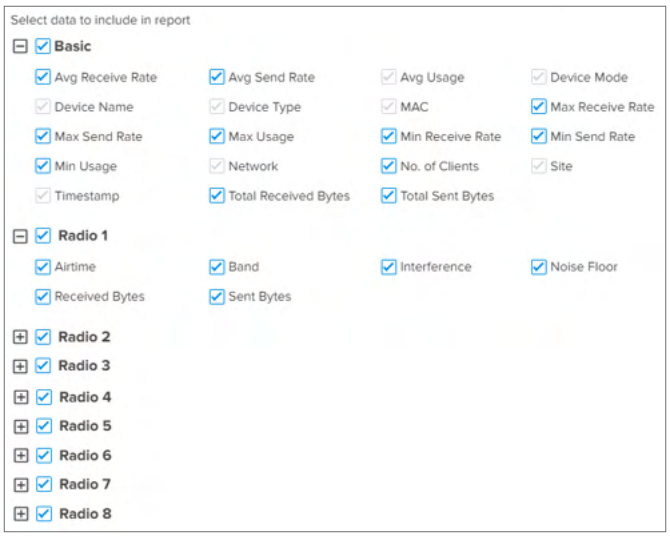
cnWave 5G Fixed Performance Report

Figure 242 *Performance Report: cnWave 5G Fixed*



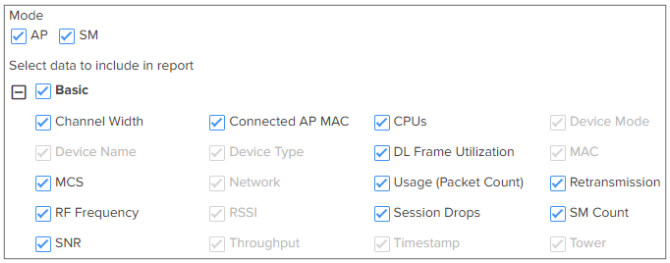
Enterprise Wi-Fi Performance Report

Figure 243 *Performance Report: Enterprise Wi-Fi*



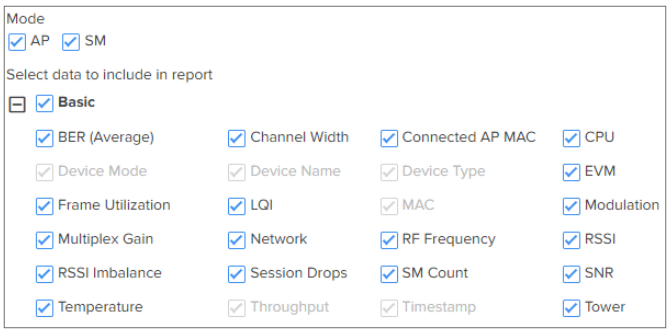
ePMP Performance Report

Figure 244 *Performance Report: ePMP*



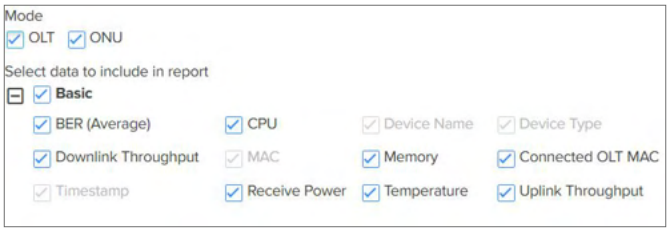
PMP Performance Report

Figure 245 *Performance Report: PMP*



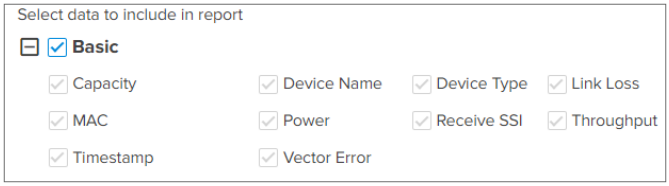
PON Performance Report

Figure 246 *Performance Report: PON*



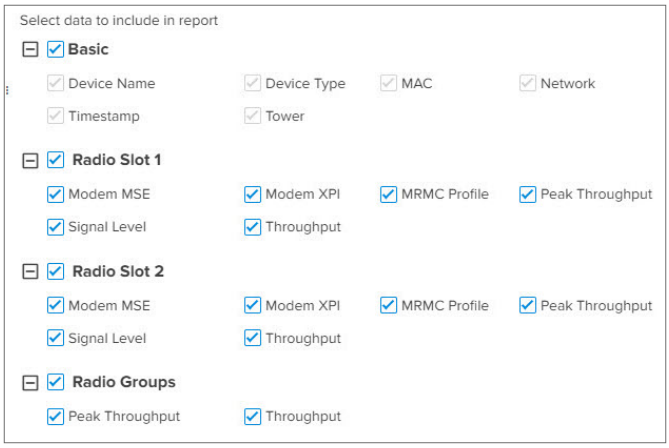
PTP 650/670/700 Performance Report

Figure 247 *Performance Report: PTP 650/670/700*



PTP 820/850 Performance Report

Figure 248 *Performance Report: PTP 820/850*

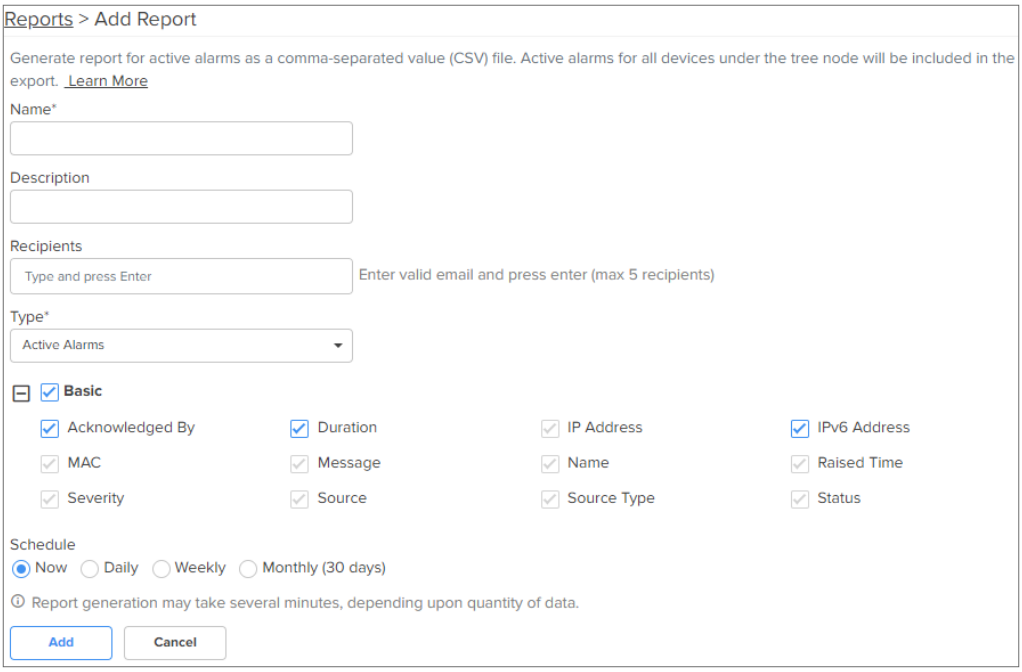


Active Alarms Report

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)
7. Click **Add**. The report gets added to the Scheduled Reports page.



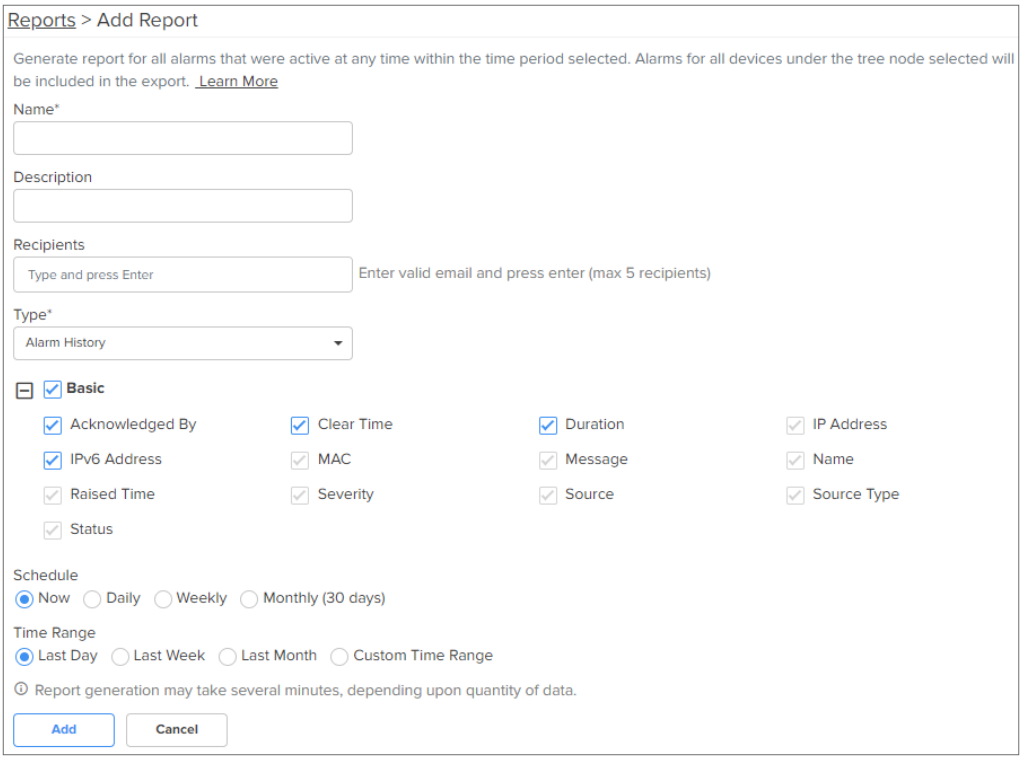
Alarm History Report

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:

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 Alarms History.
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)
7. Click **Add** . The report gets added to the **Scheduled Reports** page.
8. Click **View Jobs** to view the reports.



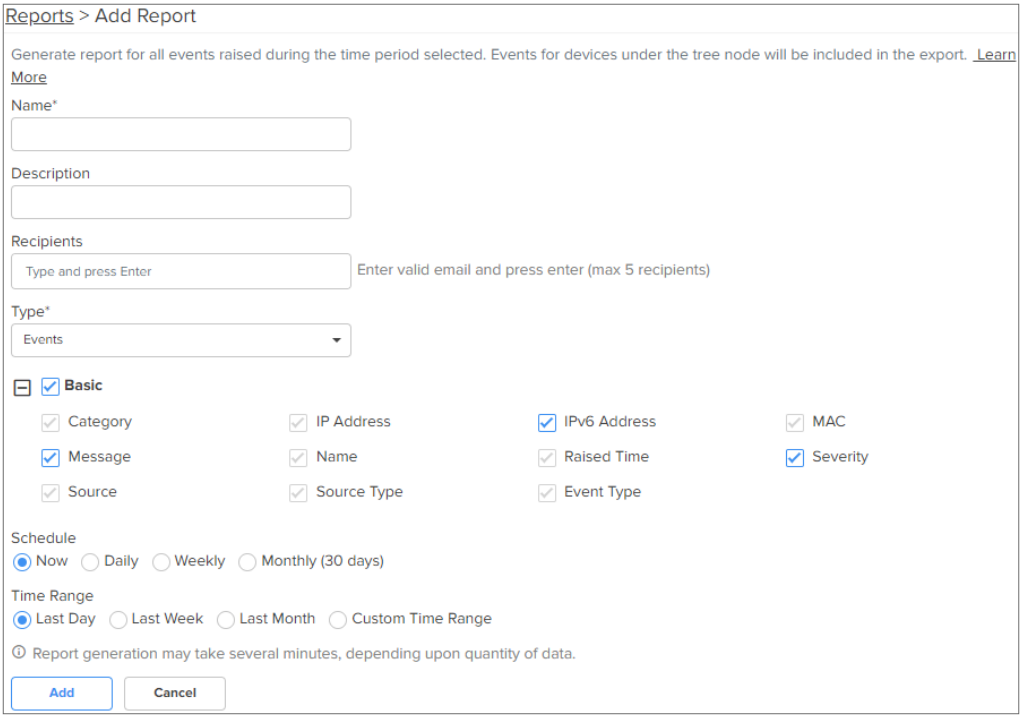
Events Report

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)

7. Click **Add**. The report gets added to the **Scheduled Reports** page.



Wireless Clients Report

The Wireless Clients report generates data for Wi-Fi clients.

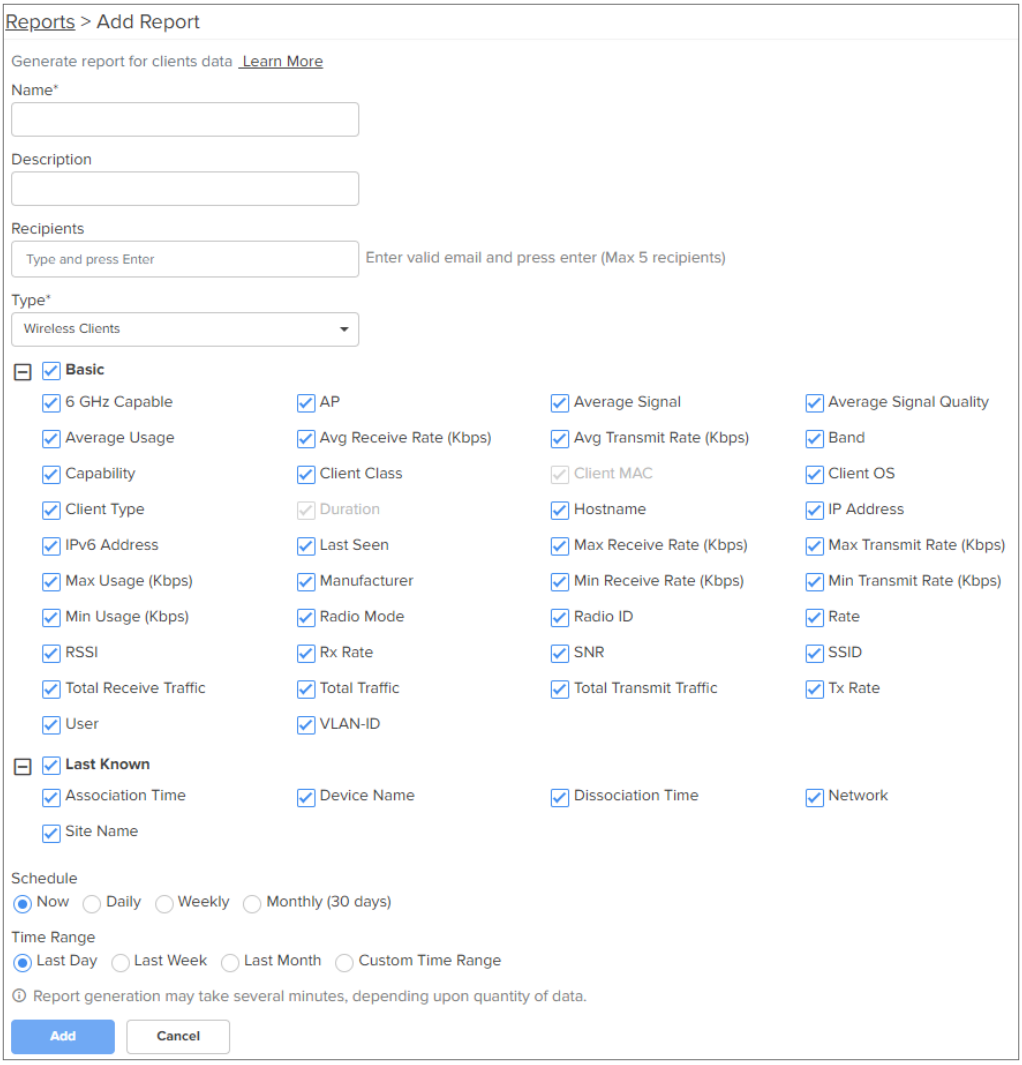
> **Note**
>
> Client Data is available for the last day, last 24 hours, and last week.

To generate the Wireless Clients 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 Wireless Clients.
6. Select data parameters to include in the report.
7. Select the following options:
   - Schedule type (Now, Daily, or Weekly.)
   - Time Range (Last Day, Last Week. Last Month, or Custom Time Range)
8. Click **Add**. The report is saved and listed in the **Scheduled Reports** page.

Figure 249 *Wireless Clients Report*



Wi-Fi Events Report

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**.

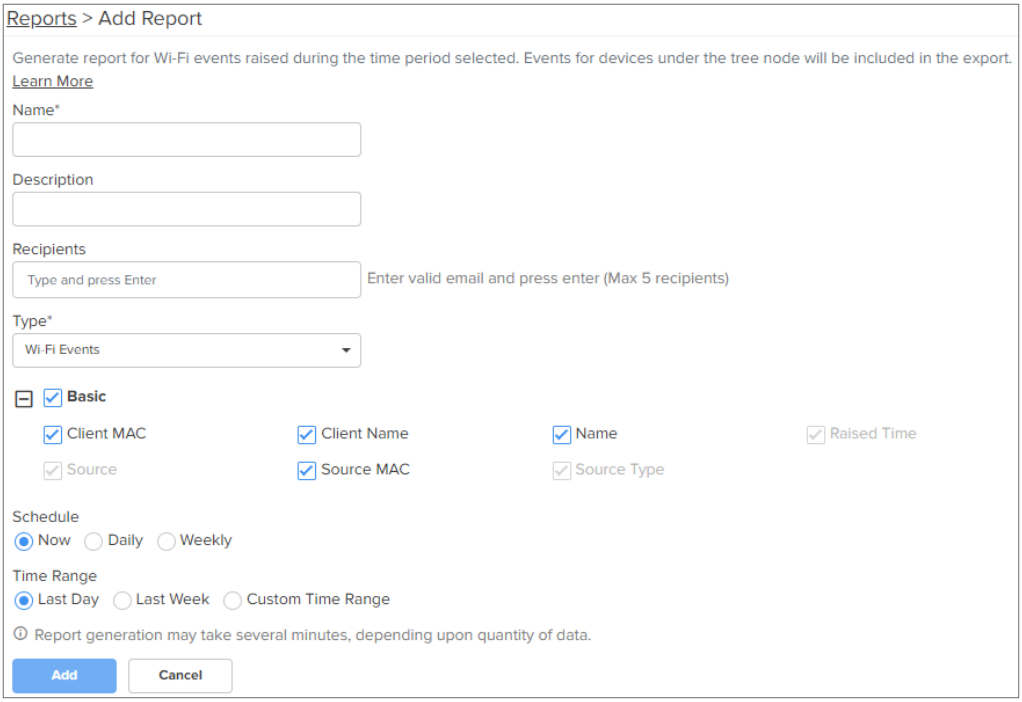
   The Add Report page appears.
3. Enter a **Name** and **Description** for the report.
4. Enter email addresses (maximum of 5) in the **Recipients** field to send reports.
5. Select the **Report Type** as Wi-Fi Events.
6. Select data parameters to include in the report.

   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 250 *Wi-Fi Events Report*



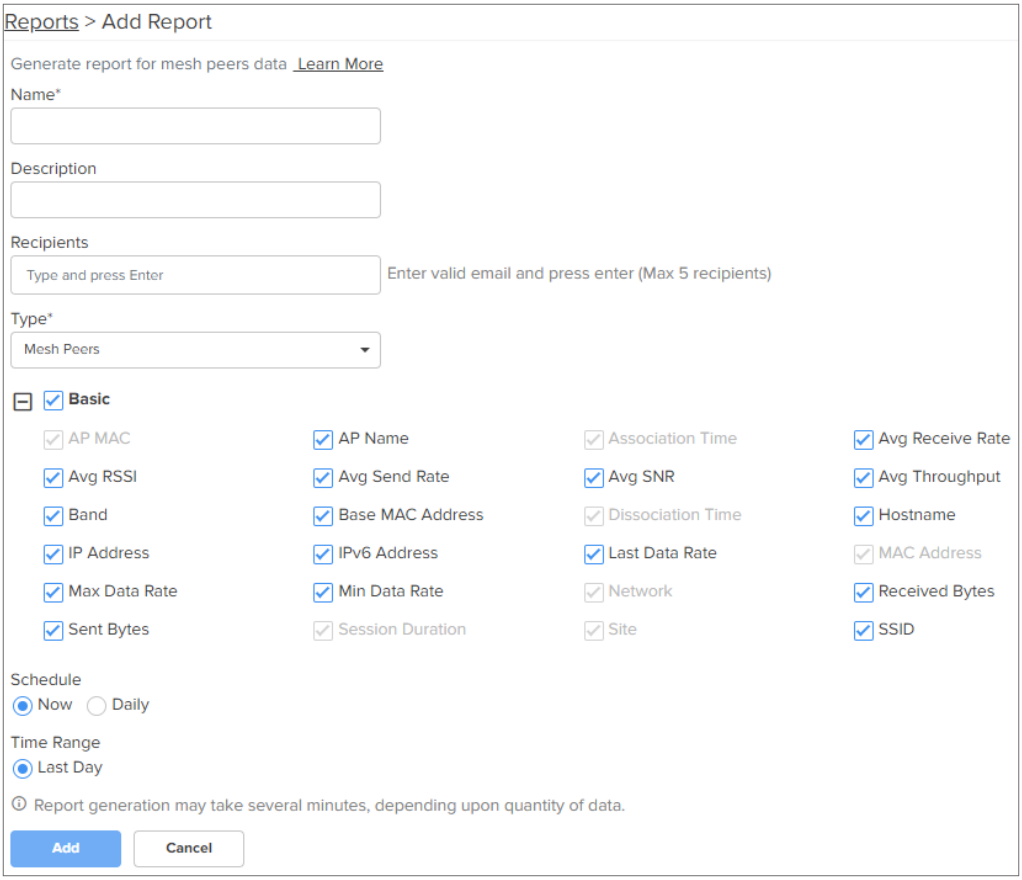
Mesh Peers Report

The Mesh Peers report is generated for mesh peers data.

To generate the Mesh Peers report, perform the following steps:

1. Navigate to **Report** > **Mesh Peers** tab.
2. Select the following options:
   - Schedule type (Now, Daily, Weekly, or Monthly)
   - Time Range (Last Day)
3. Select data parameters to include in the report.
4. Click **Start Job** to generate report.
5. Click **View Jobs** to view the reports.

Figure 251 *Mesh Peers Report*



The Mesh Peers report will export the data for the events for the specified time period and Interval.

Note

1. Every report page has a **View Report Jobs** link that directs the user to the **Report Jobs** page under **Administration** > **Jobs** > **Reports**.
2. To schedule a report **Now**, click **StartJob** under the respective report section. cnMaestro downloads the report immediately for the current system time.

   Daily report will generate reports on a daily basis depending upon the start and the end time. The weekly report generates report for seven days interval depending upon the start and the end time. Click **Schedule** and configure start and end time to schedule daily or weekly reports under the **Reports** tab.
3. **Export Now** option helps the user create export jobs stored under **Administration** > **Jobs** > **Report** tab in the export page. These reports can be downloaded within seven days from the date of generation.

Guest Access Login Events

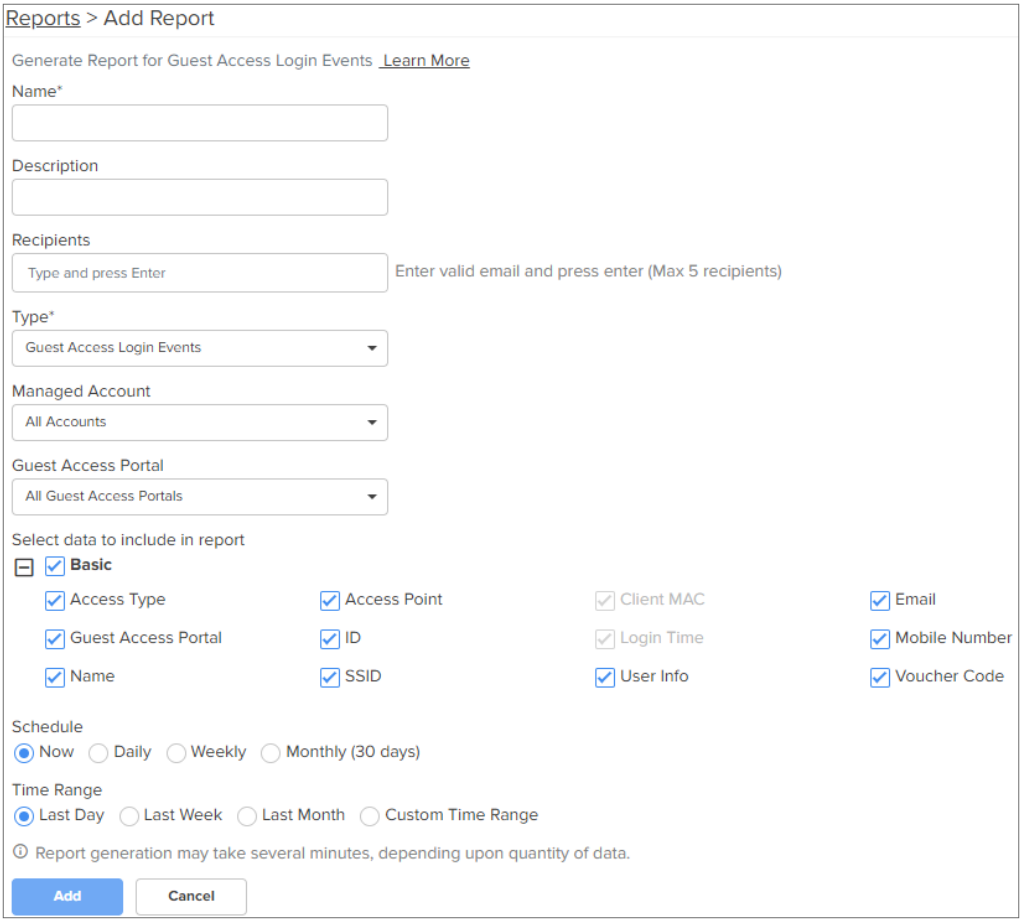
The Guest Access Login Events represent Wi-Fi guest access logins.

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, or Weekly.)
   - Time Range (Last Day, Last Week. Last Month, or Custom Time Range)
9. Click **Add**. The report gets added to the **Scheduled Reports** page.



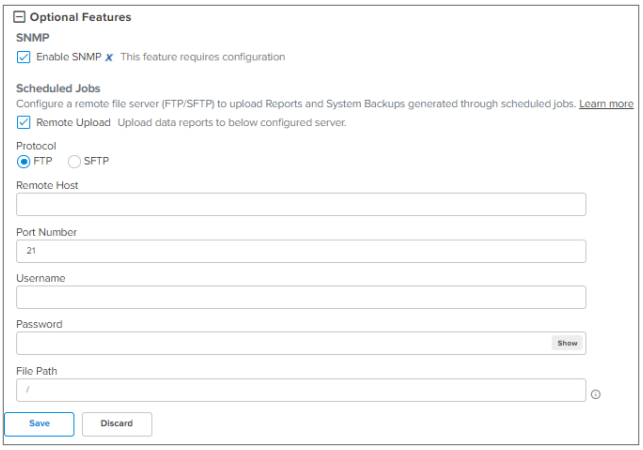
Remote Upload

Reports scheduled for **Now**, **Daily,** or **Weekly** can be downloaded directly through the UI, or from an FTP or SFTP server.

To transfer reports to FTP or SFTP server:

1. Navigate to **Administration > Settings** and select **Optional Features**.
2. Select the **Report Scheduler** checkbox to enable scheduling feature for data reports.
3. Select **Remote Upload** checkbox to upload the generated reports to the configured file server by FTP or SFTP.
4. Enter the following details:
   - File Path
   - Password
   - Port Number
   - Remote Host
   - Username
5. Click **Save.**

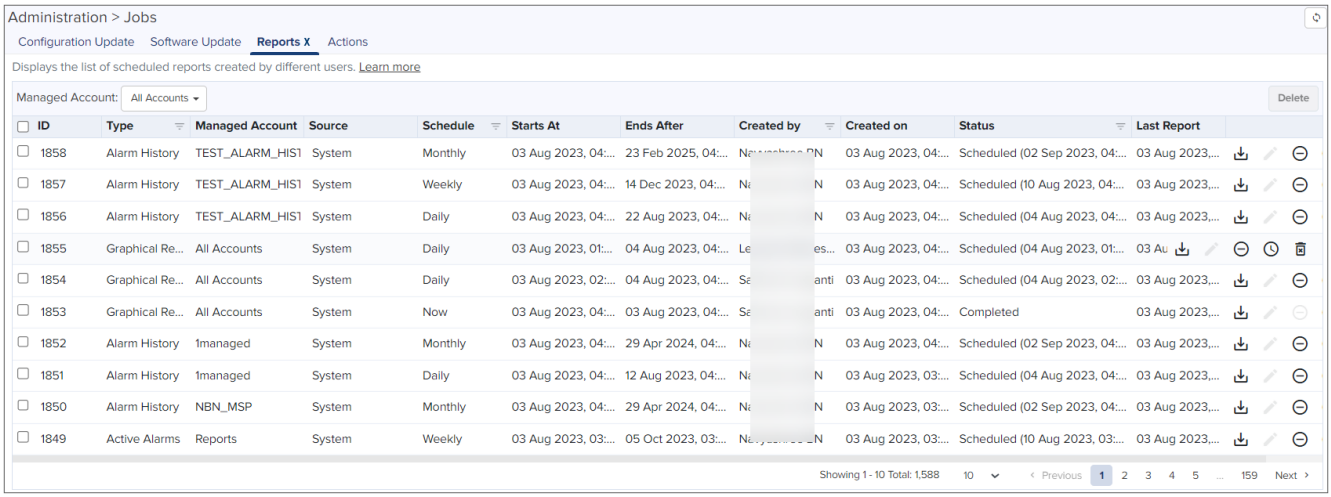
Figure 252 *Scheduling Reports*



Reports jobs

The report jobs displays the list of scheduled jobs created by different users. To view jobs, navigate to **Administration** > **Jobs** > **Reports**.

Figure 253 *Reports jobs*



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 254 lists the Graphical Reports widgets available in cnMaestro and the version they were introduced in.

Figure 254 *List of Graphical Reports widgets available*

Name of Widget	Version Introduced
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	
6 GHz Clients by Radio—Comparison between 6 GHz clients on 6 GHz radios and 6 GHz clients on 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
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

Name of Widget	Version Introduced
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

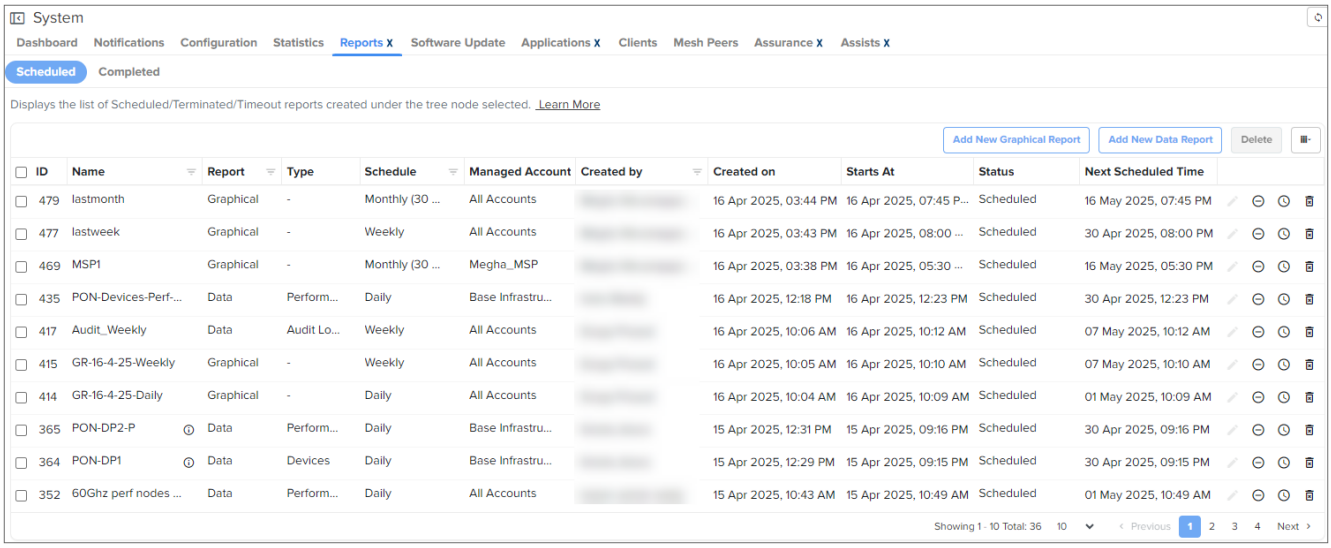
The standard process for graphical report generation includes the following:

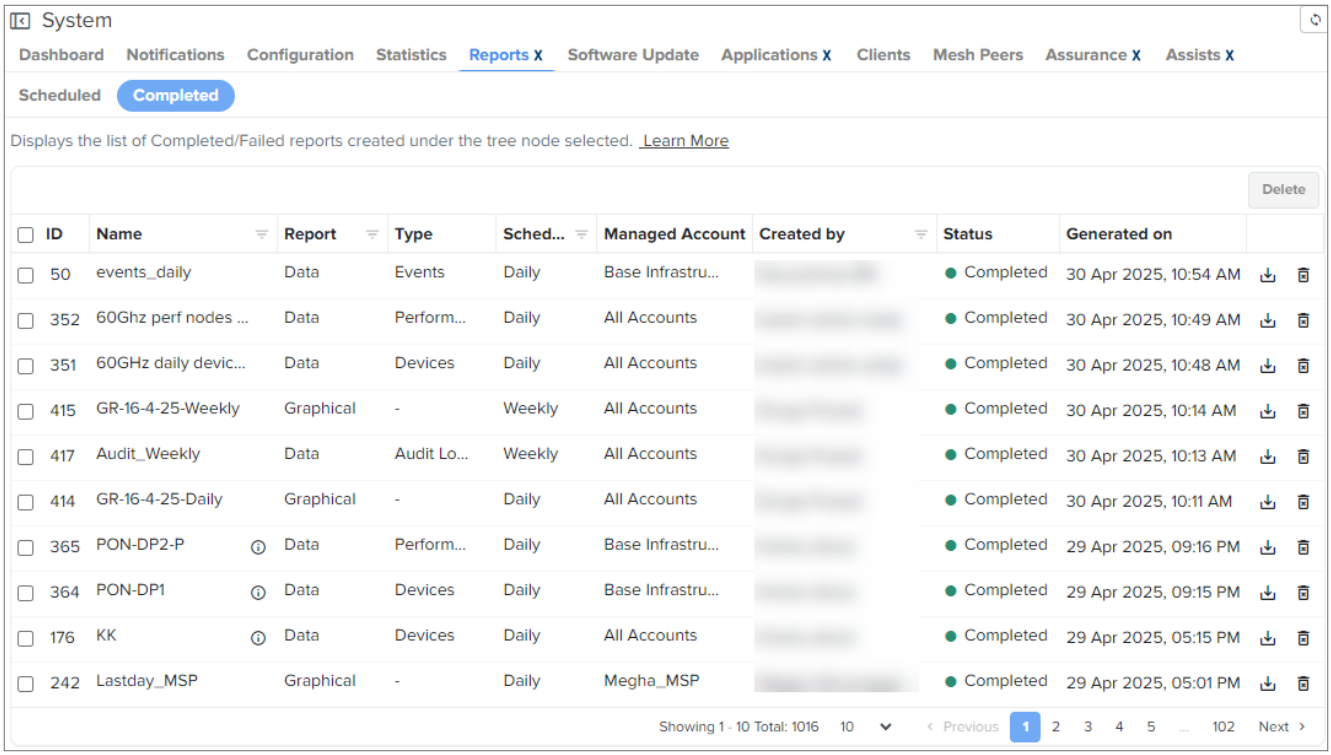
1. Create a template using the widgets listed above.
2. Select a level of the hierarchy on which to apply the template.
3. Schedule the report to either execute one-time or periodically.

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).





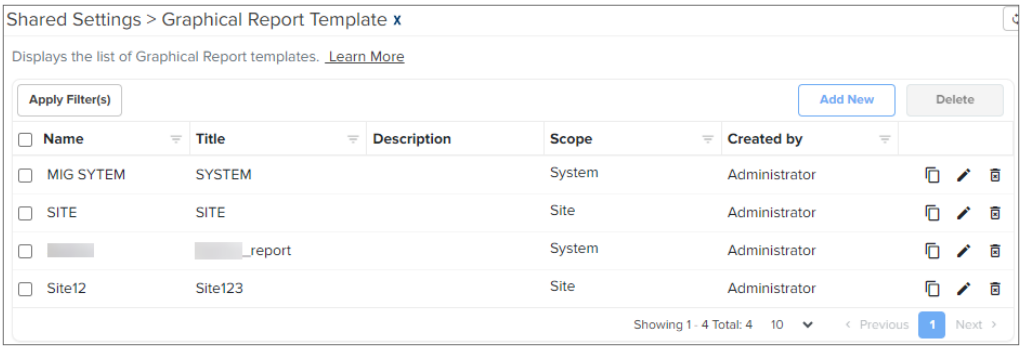
Refer to the following topics to create templates and schedule reports:

- Create Graphical Report Templates
- Generate Reports Based on Templates

Create Graphical Report Templates

To create a graphical report template, complete the following steps:

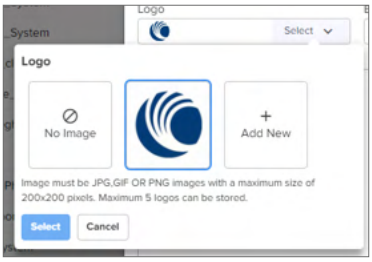
1. Navigate to **Shared Settings** > **Graphical Report Template X** page.



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.

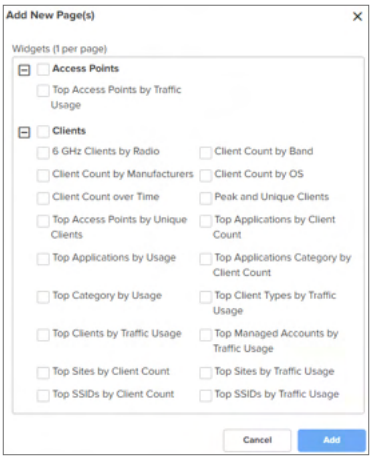
3. Optionally, brand the report as per your requirement.
   - **Logo**—To select an existing logo, click the down arrow and then click **Select**. You can also add a new logo by clicking **Add New**.



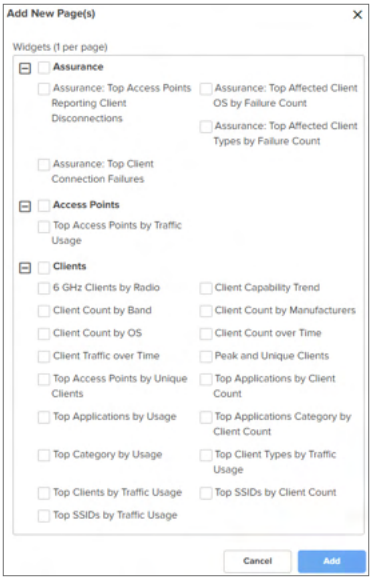
   - **Brand Image**—To select an existing brand image, click the down arrow, and then click **Select**. You can also add a new brand image by clicking **Add New**.
   - **Themes**—Select a theme for the title page of the report as either **Vertical Lines**, **Brand Box**, or **Plain**.

   - **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:



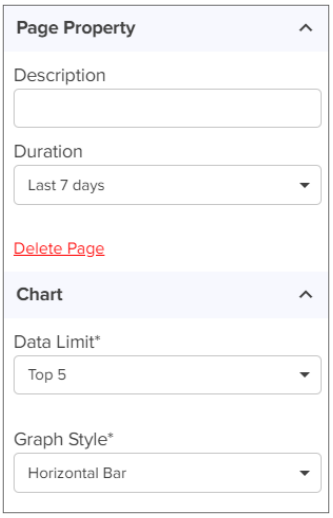
- For the **Site** scope:



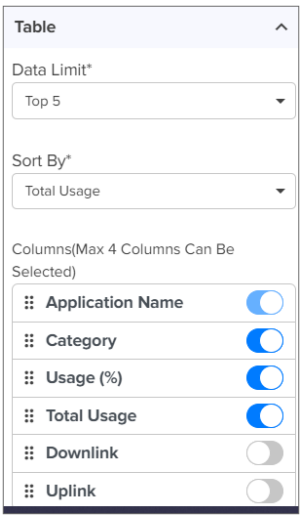
6. Select the checkbox for one or more Widgets and click **Add**. Each page can have only one widget. Drag and drop the pages in the left pane to rearrange the widgets.

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**.



8. You can also select the Table columns for each page.



The following options are available based on the page type:

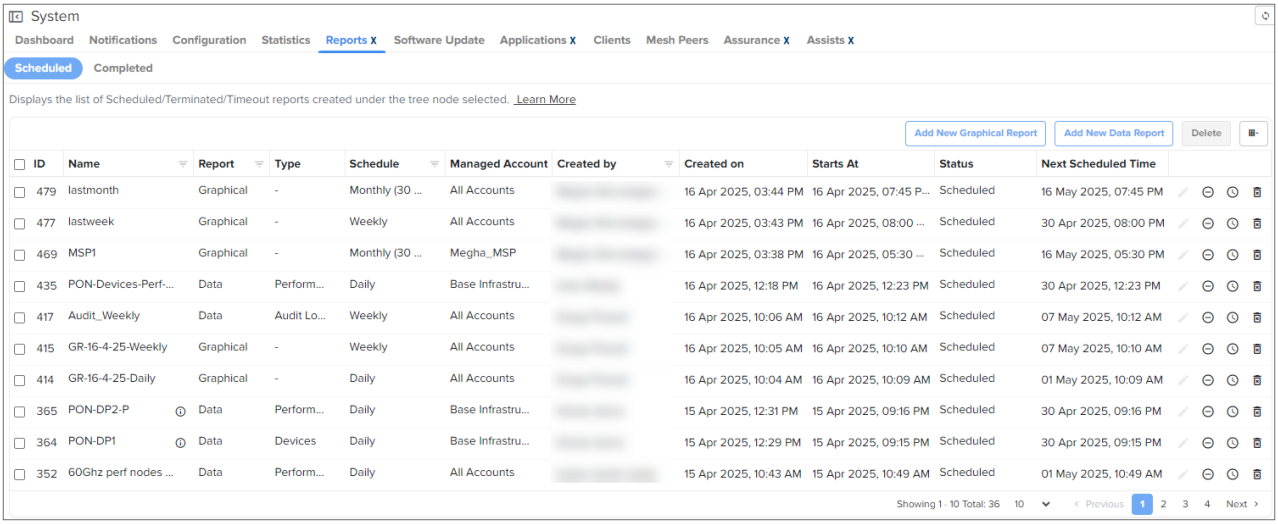
- **Title**—Title for the report.
- **Description**—Detailed information about the report criteria.
- **Duration**— Time interval. For example, **Last Day** or **Last 7 Days**.
- **Chart/Graph Style**— Type of graph. For example, **Horizontal Bar** or **Pie Chart**
- **Data Limit**—Volume of data to 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**.

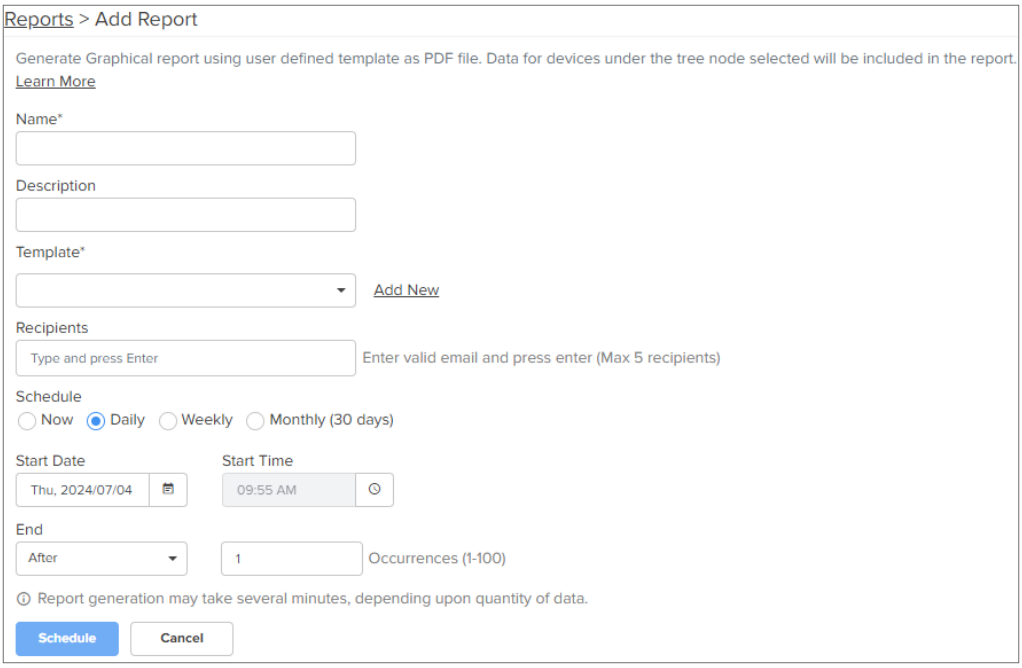
Generate Reports Based on Templates

To add a new report, follow the steps below:

1. Navigate to **Monitor and Manage** > **System** or **Site** > **Reports X** > **Scheduled** tab.



2. Click **Add New Graphical Report**.



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
- cnMatrix Switch Profiles
- 60 GHz cnWave Configuration
- Configuring Advanced Features
- Creating Auto-Provisioning Rules

Software Update

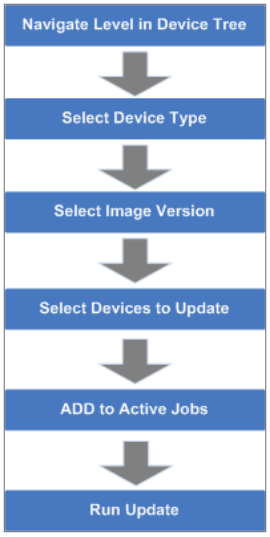
The **Software Update** tab displays the device update details. This section includes the following:

- Software Update Overview
- Create Software Update Job
- Software Update Jobs and Parameters
- Viewing Running Jobs in header
- cnReach Bulk Software Upgrade

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 255 *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

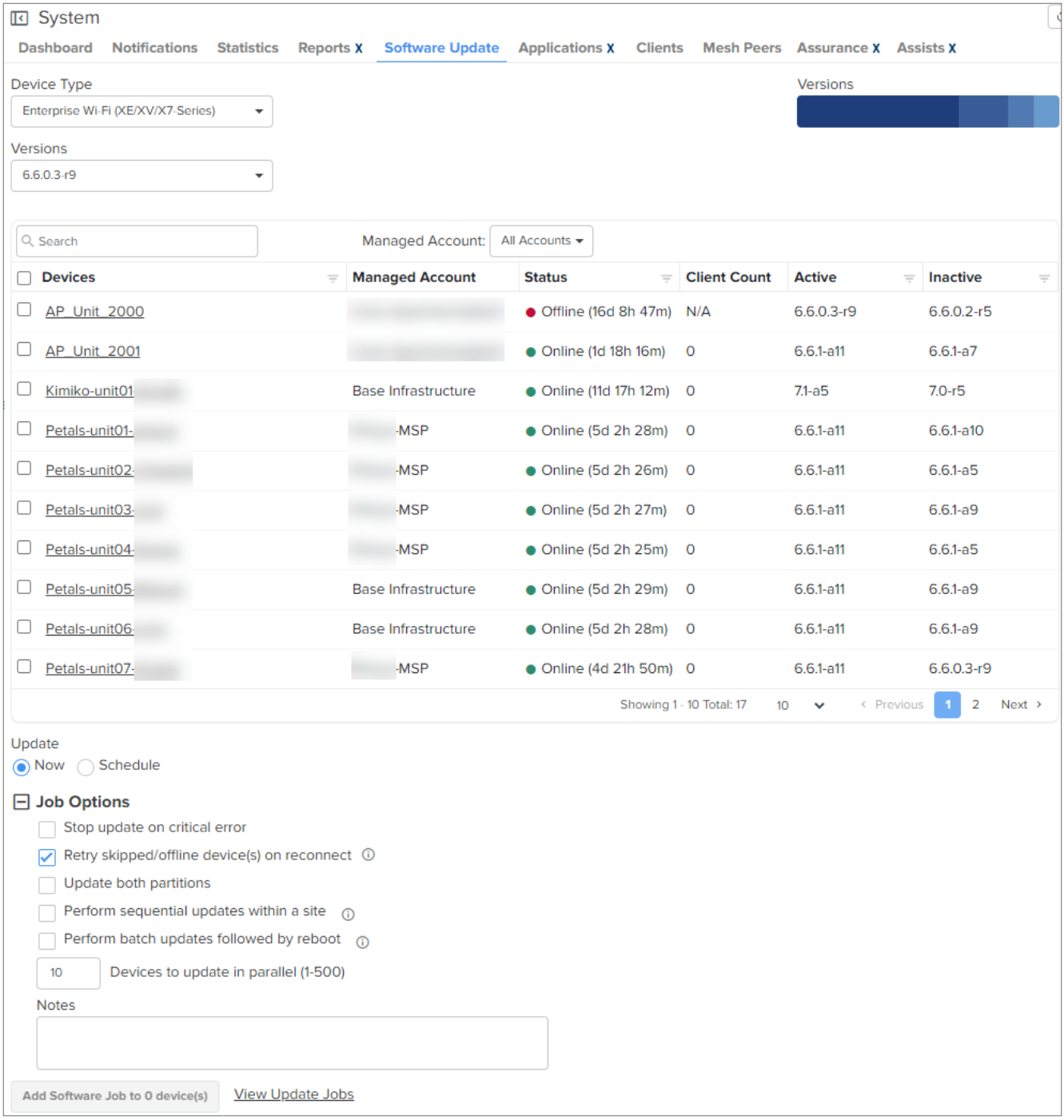
Once the device type is chosen, the UI displays the most recent software release version for that device type. It also displays a breakdown of the different software versions currently installed on the devices.

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 256 *Software Update: Enterprise Wi-Fi*



Note

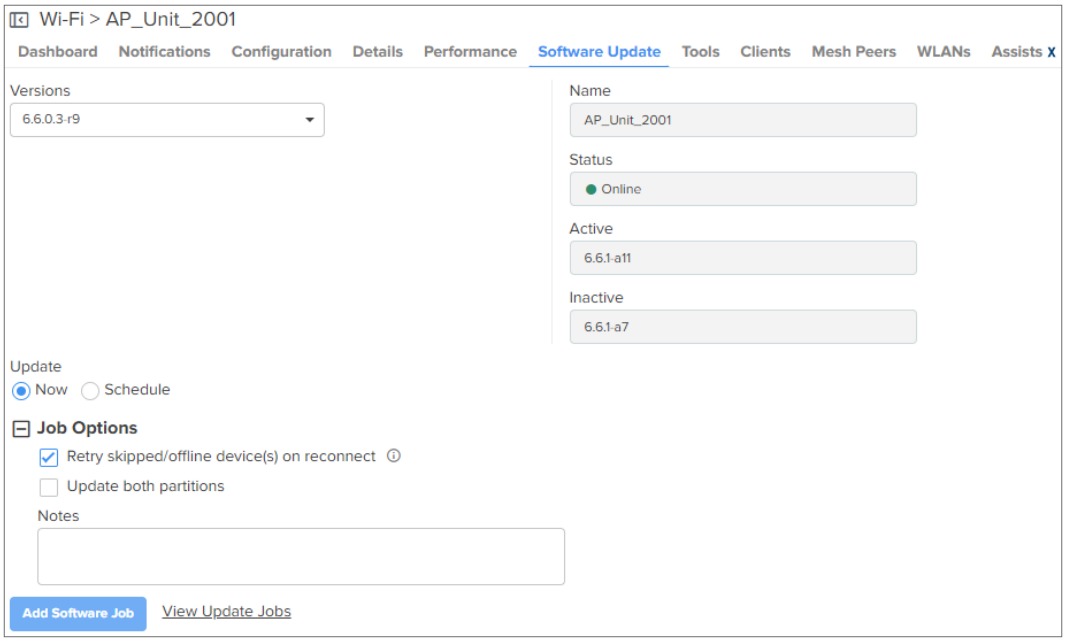
- **Update both partitions** option is available at System/Managed Account/Network/Site/Device levels. It is only available for the devices that support it.
- **Perform sequential updates within a site** option is available at System/Managed Account/Network/Site level except the Device level.

If the **Update both partitions** option is enabled/ disabled, the device level of the Software Update will be displayed as follows:

- **Enable**: Tp

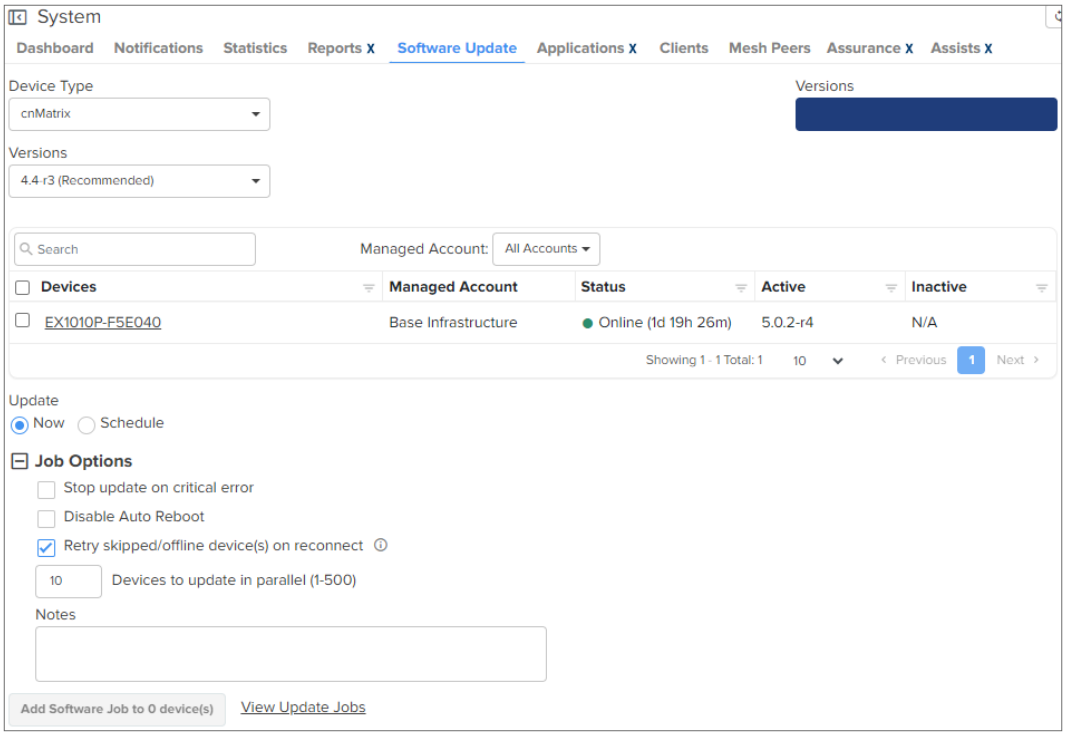
- Selected target image will be upgraded in only active portion of the device.

Figure 257 *Software Update: Device level*



If **Perform sequential updates within a site** is enabled, the image upgrade will happen only on one device at a time.

Figure 258 *Software Update: cnMatrix*



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 259 *Software Update: cnRanger*

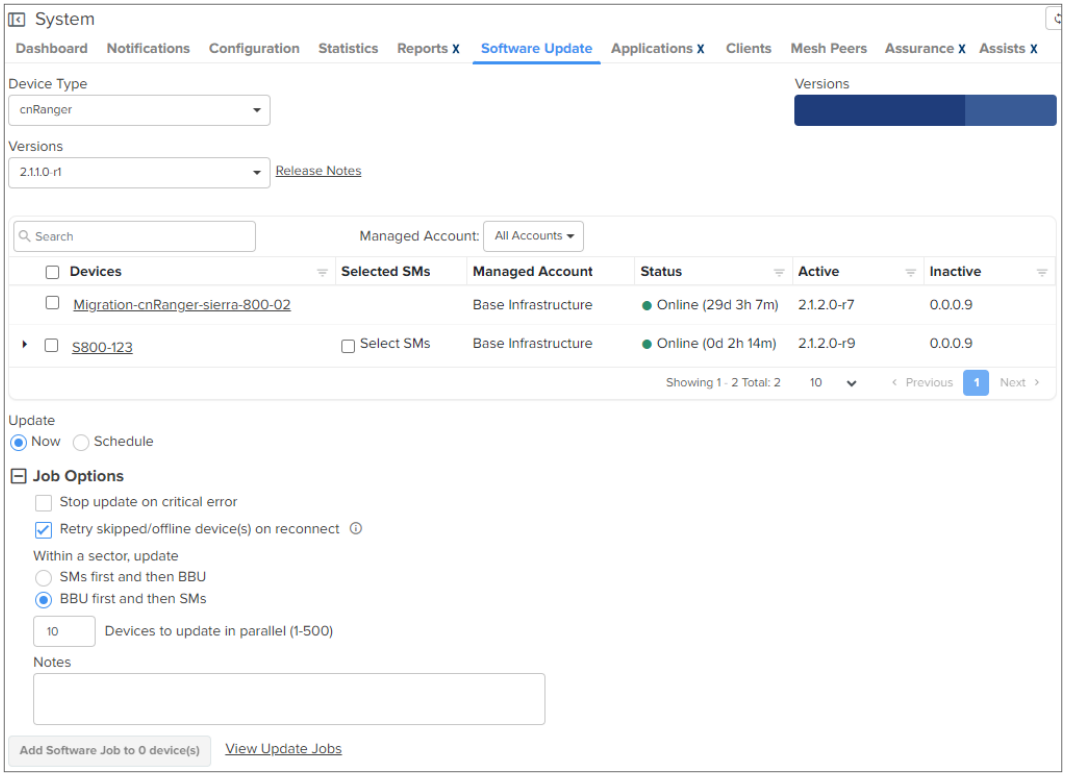


Figure 260 *Software Update: 60 GHz cnWave*

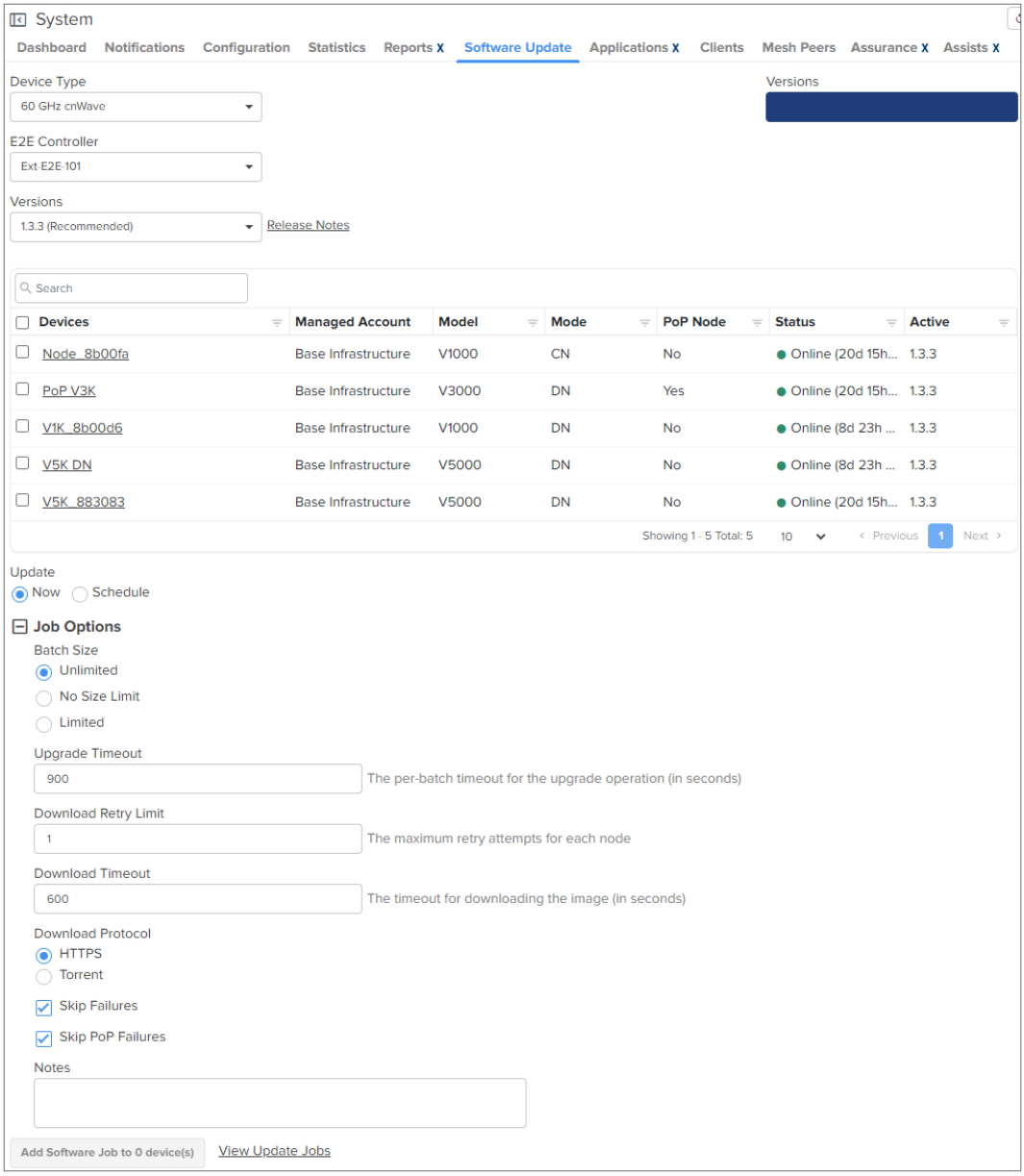
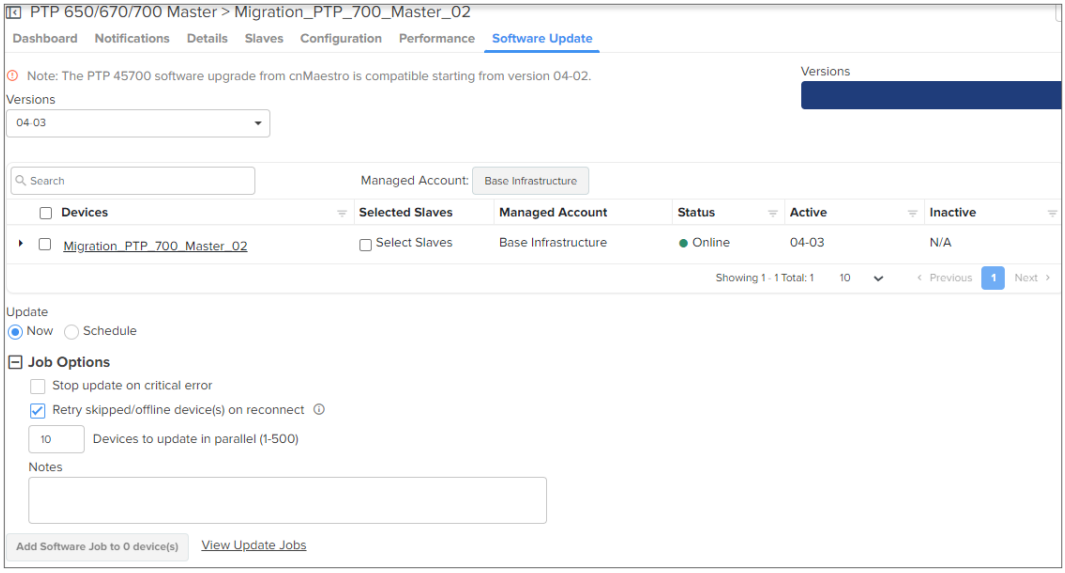


Figure 261 *Software Update: PTP 670/700*



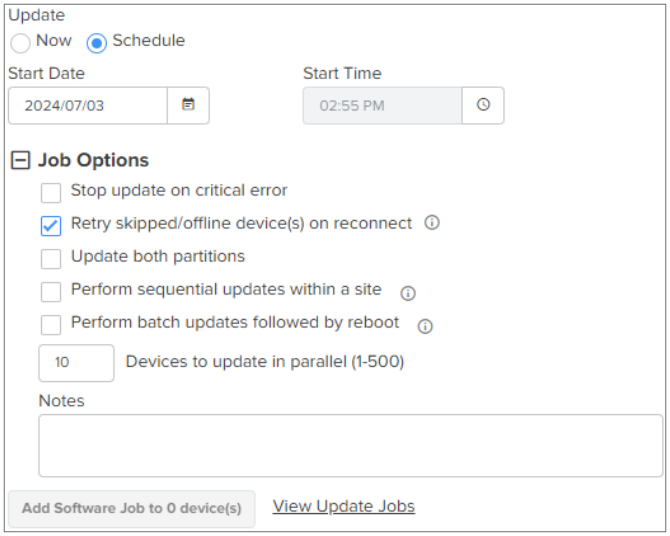
Note

- 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.

Scheduling Software Update Job

You can schedule a Software Update Job on the devices by selecting **Schedule** option and providing the **Start Date** and **Start Time**.

Figure 262 *Scheduling Software Update Job*



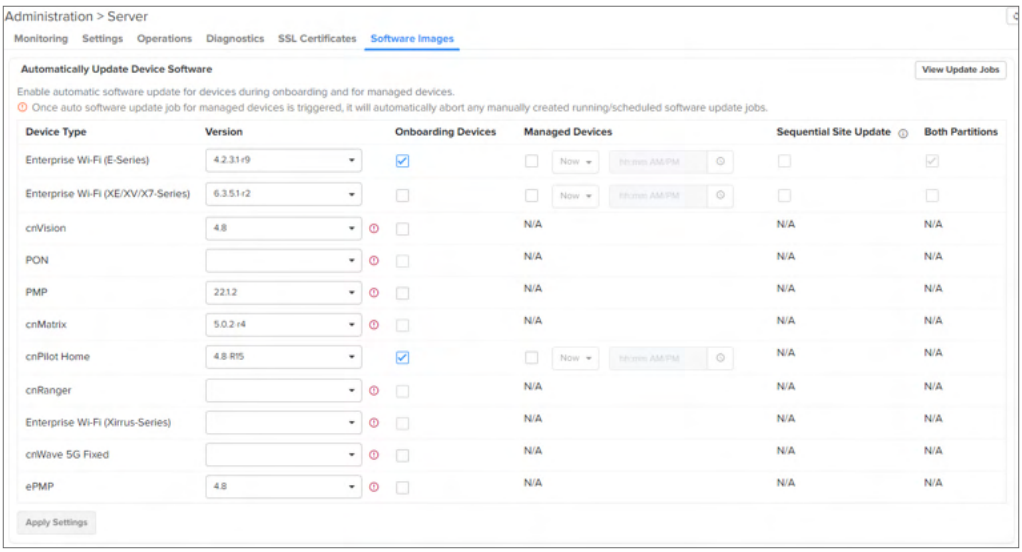
You can view the status of software update job in **Administration** > **Jobs** > **Software Update** > **Manual** or **Auto** page.

Software Update while Onboarding

The software version on the devices can be auto updated to the preferred version when the device first contacts cnMaestro.

To enable the device software feature, perform the following steps:

1. Navigate to **Administration** > **Server** > **Software Images**.
2. Click the **Onboarding** checkbox for the particular device version.
3. Click **Apply Settings.**



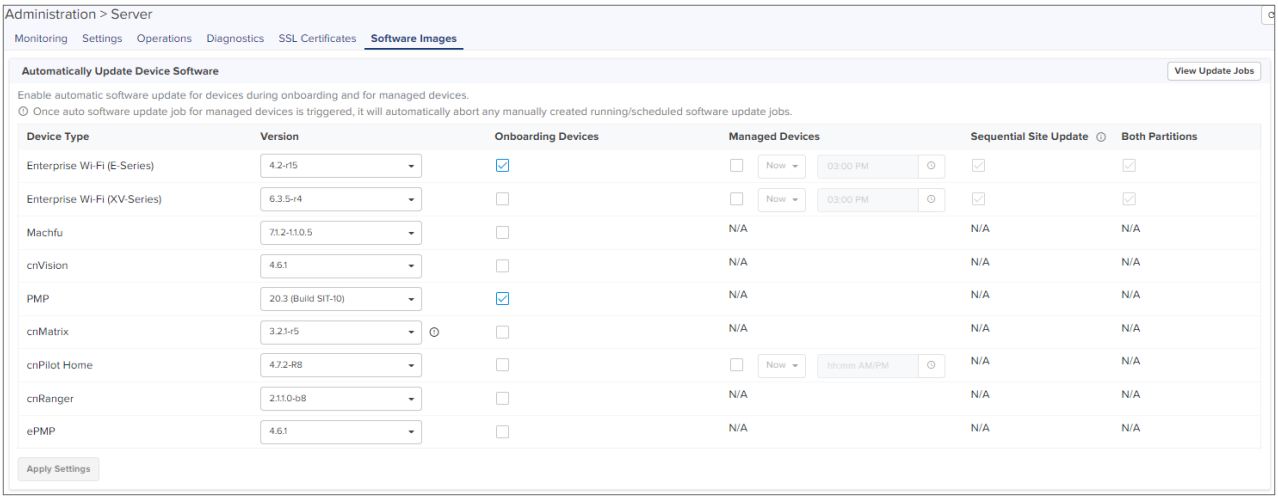
The device will automatically upgrade based on the software selected while onboarding.

Software Update through Managed Devices

The software version on the devices can be auto updated to the preferred version through the Managed Devices.

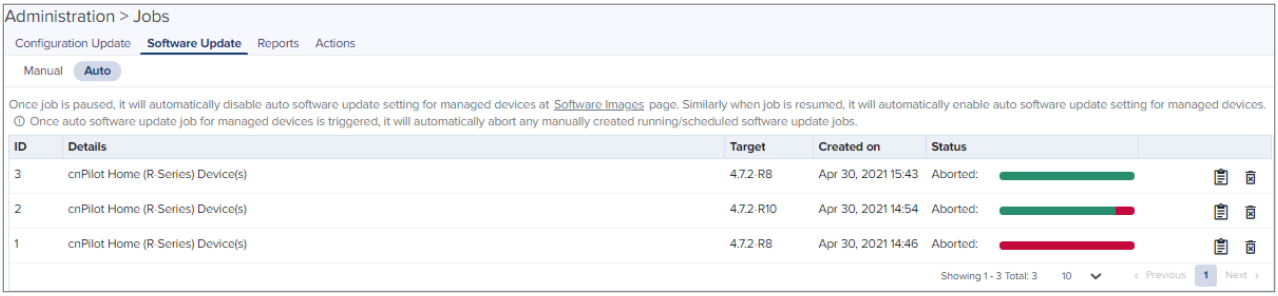
To enable the device software update feature, perform as follows:

1. Navigate to **Administration** > **Server** > **Software Images**.
2. Click the **Managed Devices** checkbox for the particular device version.
3. Click **Apply Settings.**



Once the setting is applied, you can view the jobs on the **Administration** > **Jobs** > **Software Update** > **Auto** page.

Figure 263 *Auto update*



Note

Auto update can be aborted when the job is in-progress or idle.

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 68 *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	If a Fixed Wireless AP is selected, the corresponding SMs or CPEs will also be selected.

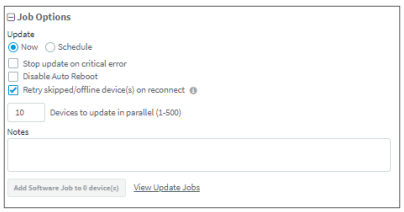
Table 68 *Parameters in Device Table*

Parameter	Description
SMs	
Status	The status of a particular device in a system. Devices that are not connected cannot 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 264 *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 soft ware 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-, Nework-, 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. ePMP 1000 Hotspot
   m. PMP (Sectors)
   n. PON
   o. PTP 670/700
   p. PTP 820/850
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 69 *Parameters in Software Update Jobs*

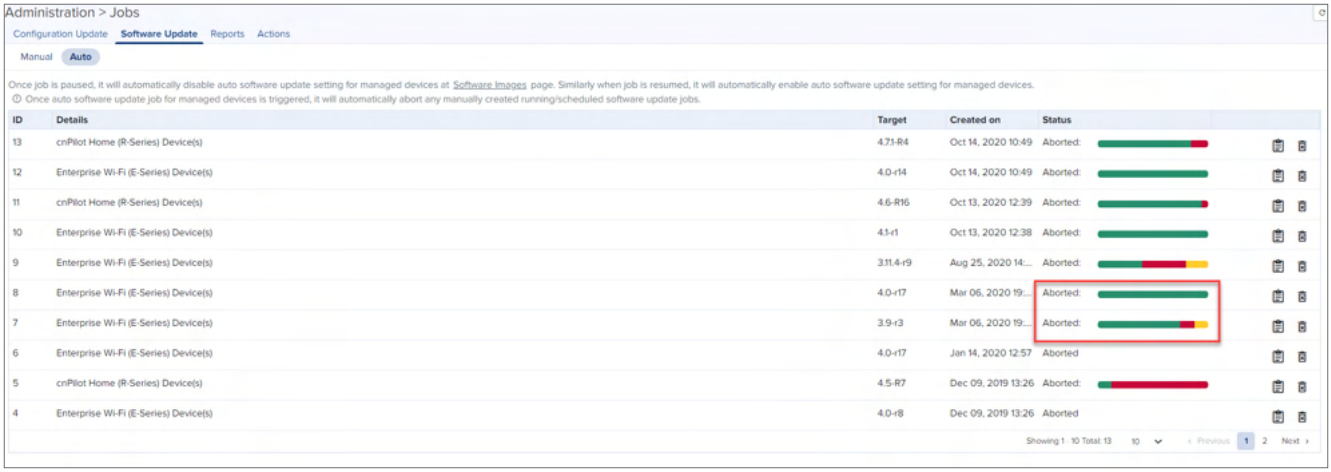
Parameter	Description
Action	Use the **Start** or **Delete** button to manage the upgrade process. After the upgrade has started, the **Pause** button will stop new upgrades from the beginning. If the upgrade process fails or the upgrade has been paused, you can restart the process by clicking the **Resume** button.
Created By	The user who has created this job.
Created On	Date and time the job is created.
Completed On	Date and time the job is completed.
Details	Count of devices and date and time the upgrade process is initiated.
ID	Identification number of the active job.
Image Type	The type of image selected for the device.
Managed Account	The Managed Account Name.
Occurrence	The occurrence of the update as Now or Scheduled.
Status	Status of update.
Target	Target software version to upgrade.

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 265 *Abort Software Job*



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.

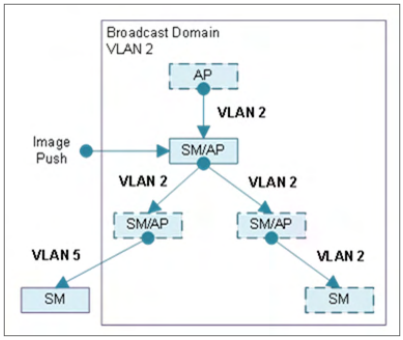
3. Devices that have not yet started display as **Skipped** with a message **Job was aborted** with the status as **Skipped**.
4. Software update jobs can be scheduled in parallel irrespective of other running jobs in cnMaestro X accounts.
5. Only **Configuration** or **Software Update Job** operation 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

cnReach Bulk Software Upgrade

Distributing software to cnReach devices can take many hours, due to the relatively low RF bandwidth. In order to minimize wireless traffic, cnMaestro supports the cnReach mechanism by which a single AP coordinates the broadcast distribution of firmware to every cnReach device within its VLAN. In the below figure, the bulk upgrade operation transfers an image to the middle AP, which then distributes it to all APs with VLAN 2. The APs are not updated in this process; the firmware is just pushed into their storage, where it can be applied later (once the distribution completes). cnReach has a mechanism to handle offline devices during the distribution (which can take upwards of a day), as well as devices added midway through the transfer. Often this means the process repeats a second time to handle any updates.



The **Bulk Software Upgrade** is optional and meant to be used for efficiency. One can still employ the standard Software Update mechanism to transfer images to cnReach devices one-at-a-time, though the distribution could be many hours or days.

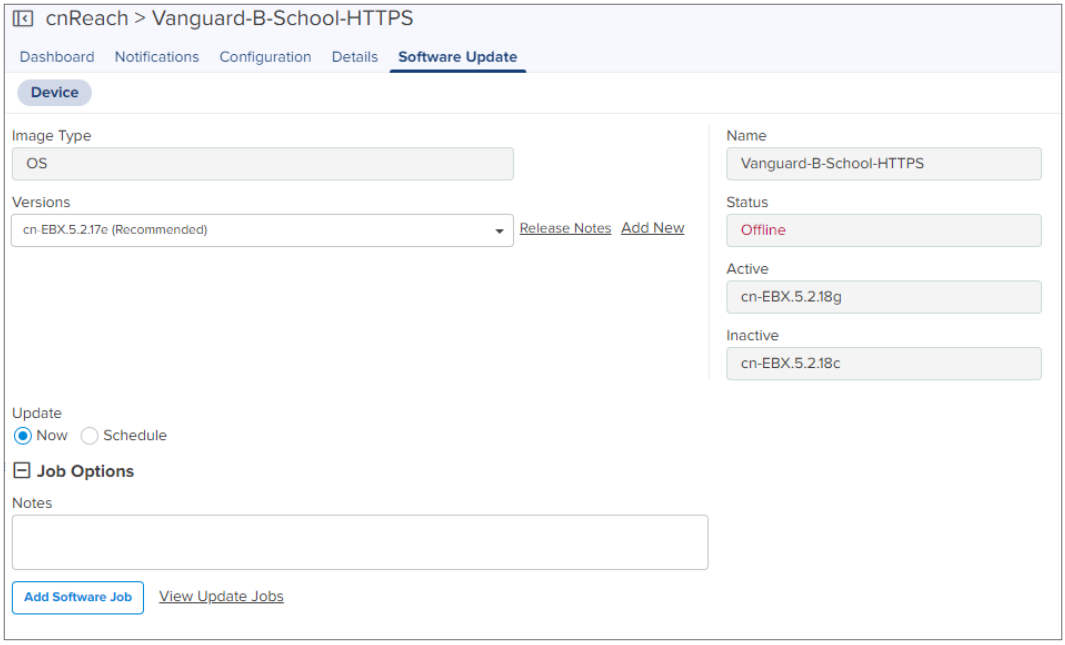
Firmware versions (OS and Radio)

cnReach devices have two versions of software: one for the Motherboard OS and another for the Radio. Each Radio can have a different version of firmware. When selecting software to distribute, one should choose either OS or Radio. During the apply phase, when the image is updated, one or both Radios can be selected.

Bulk Upgrade

The Bulk Upgrade tab is accessed by selecting a cnReach AP then **Software Update** > **Bulk Upgrade**. The Motherboard (OS) or Radio software is available, and the distribution started and stopped. Once the bulk upgrade is started, the distribution continues until stopped, so be sure to manually stop the process when complete.

Figure 266 *Bulk Upgrade*

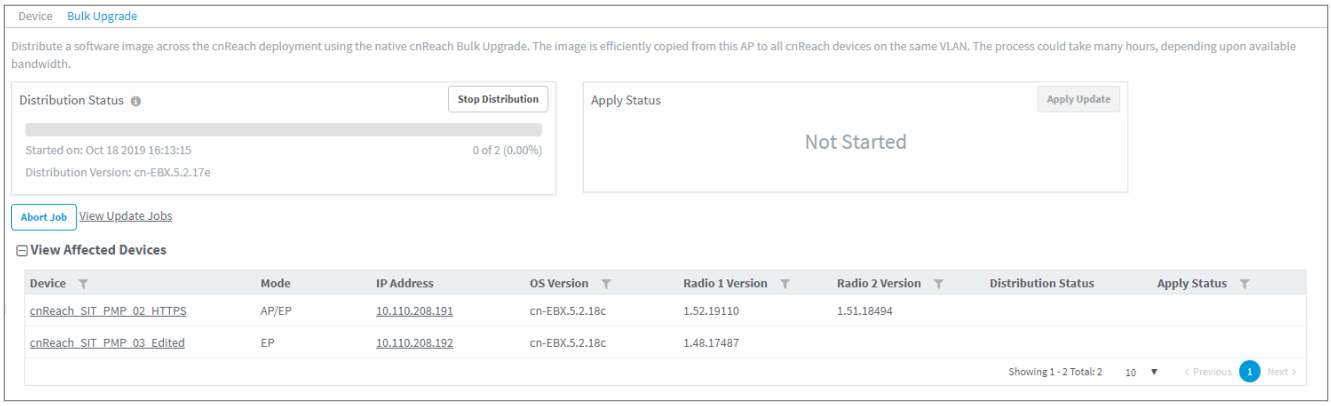


Note

You must start the distribution on a single AP in a cnReach VLAN, and only run it from that AP. Executing Bulk Software Upgrade on more than one AP in a VLAN will not be prevented by cnReach devices, and it could lead to distribution failures.

Upgrade Tracking

The following page is displayed when an AP is actively distributing software. One can view other devices in the VLAN (and their current software versions), and the distribution status. Distribution can be stopped at any time, and images can be applied directly to the devices in the list.



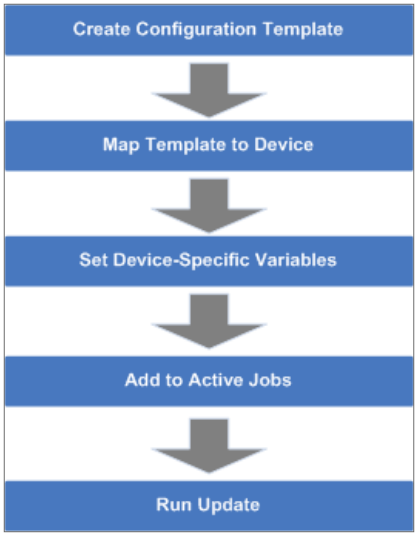
Fixed Wireless Configuration

Overview

Template configuration is supported for cnMatrix, cnPilot Enterprise, cnPilot Home, cnRanger, cnReach, cnVision, ePMP, and PMP 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 267 *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 268 *Sample ePMP Template*


```
"device_props": {
      "acsEnable":      "0",
      "acsScanMinDwellTime":  "200",
      "acsScanMaxDwellTime":  "300",
      "acsControl":     "0",
      "bcPriority":     "0",
      "cambiumInternetConnectionServerIP":      "",
      "centerFrequency":      "5670",
      "dataVLANEnable": "0",
      "dataVLANVID":    "",
      ...,
      "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:

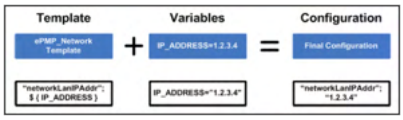
“networkLanIPAddr”: ${IP ADDRESS="10.1.1.254"},

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 269 *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

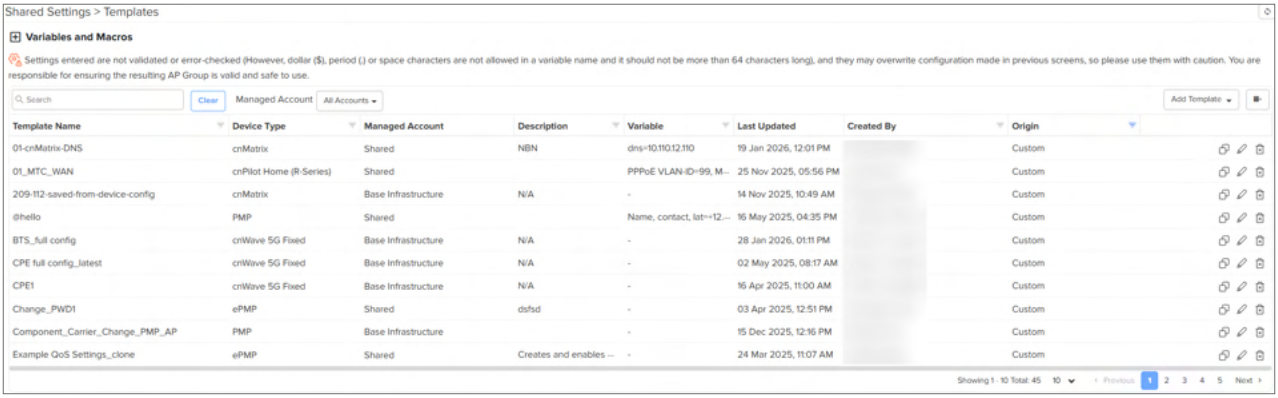
The typical process for creating your own configuration templates is below:

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.

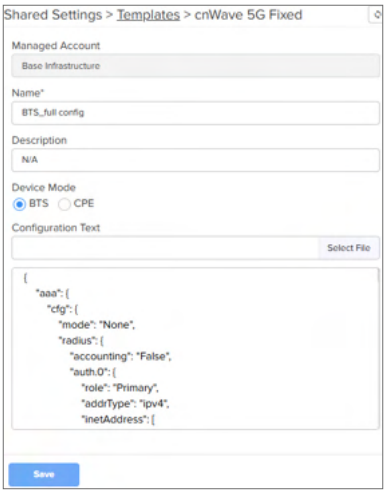
Template

To create a configuration template:

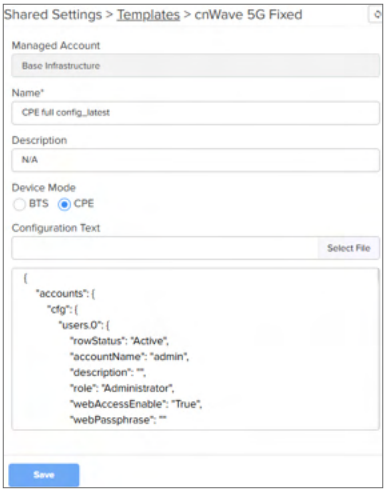
1. Navigate to **Configuration > Templates** in the main menu.



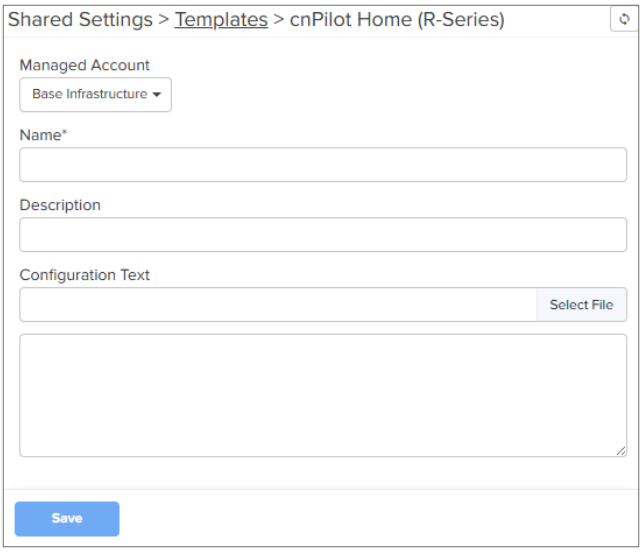
The following template is for BTS:



The following template is for CPE:



2. Click **Add Template** button.



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.

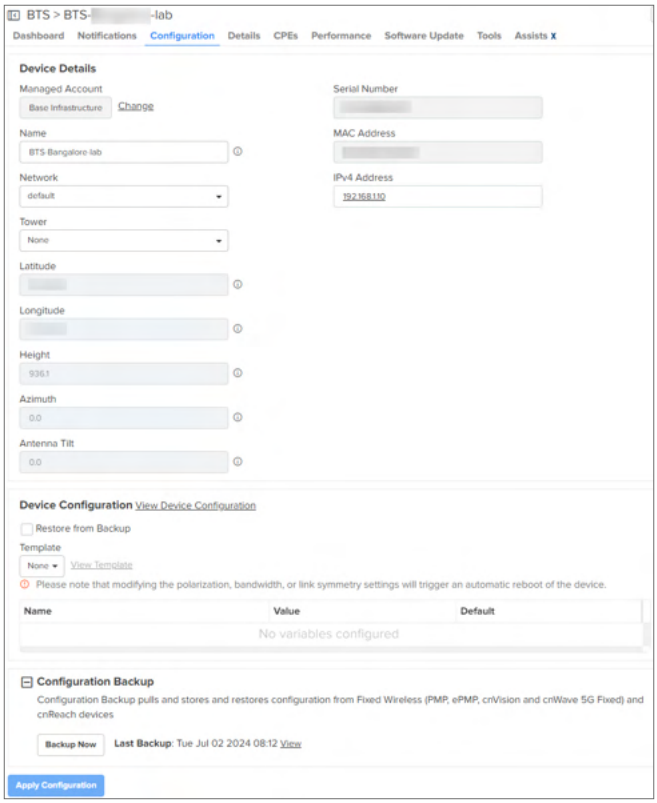
> **Note**
>
> No default templates available for R-series. User needs to create a new template.

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.

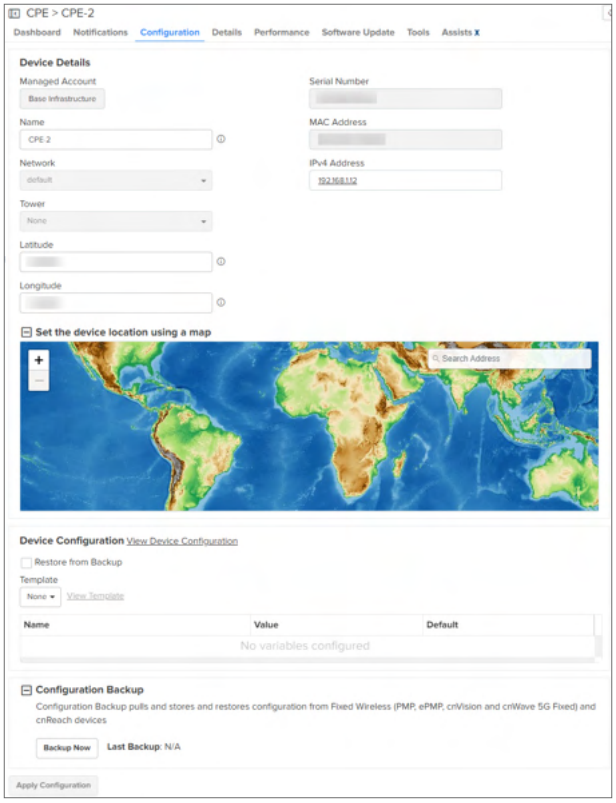
> **Note**
>
> When you navigate to the Template page default template type filter will be custom. User needs to select **All** or **Default** to view other templates.

BTS and CPE Configuration

To configure BTS, navigate to **Monitor and Manage** > **BTS** > **Configuration**.



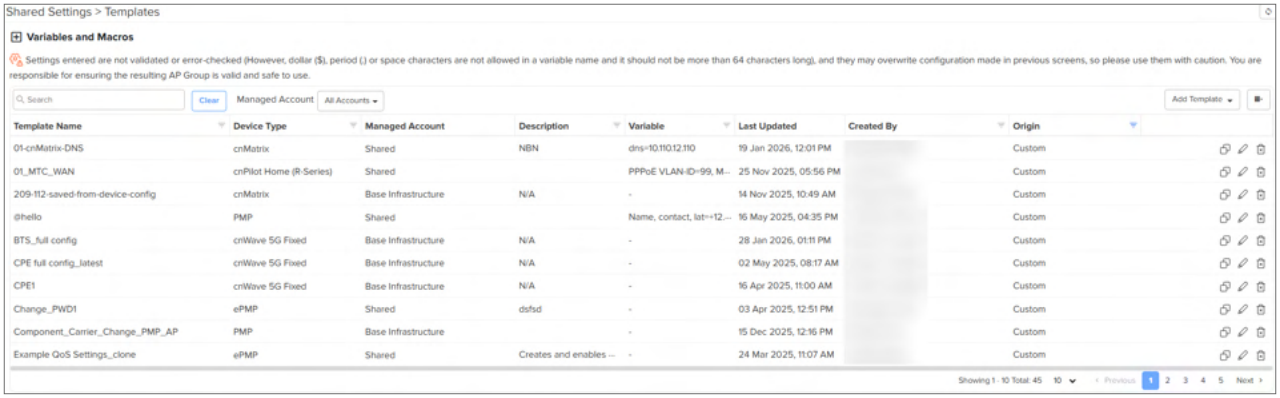
To configure CPE, navigate to **Monitor and Manage** > **BTS** > **CPE** > **Configuration**.



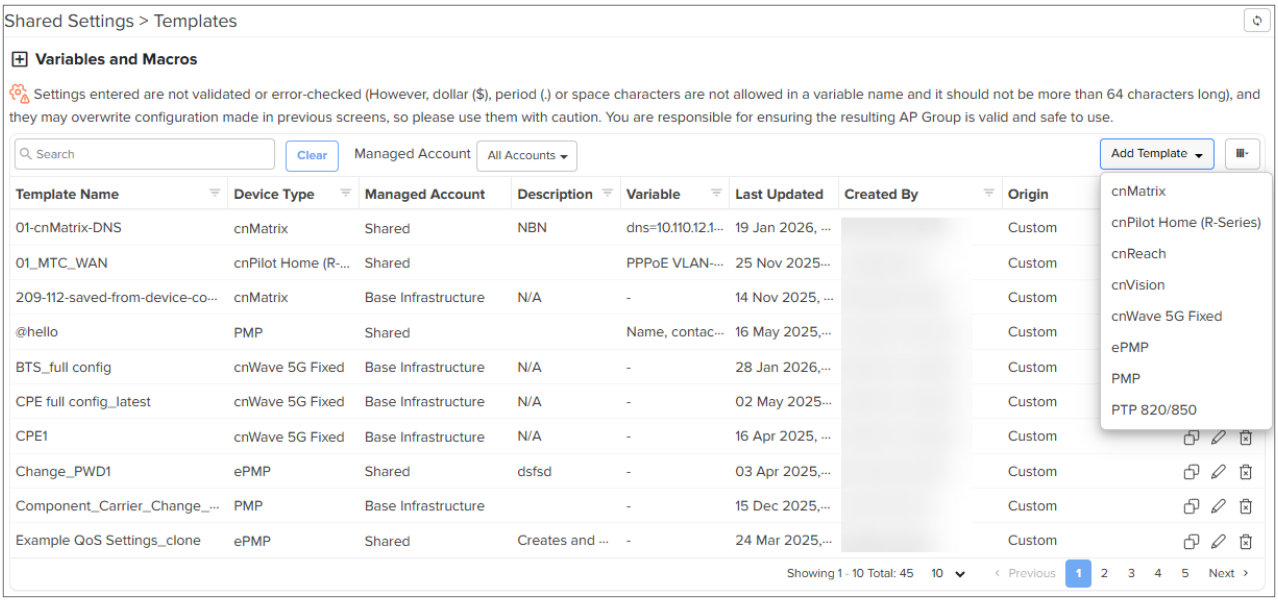
Configuration Template for PTP 820/850

To create a configuration template of PTP 820/850 device, perform the following steps:

1. Navigate to **Configuration > Templates** in the main menu.



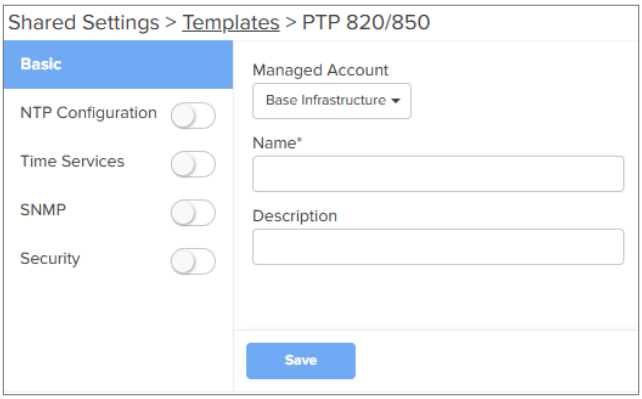
2. In the **Add Template** dropdown, select PTP 820/850.



The **Basic** template page appears.

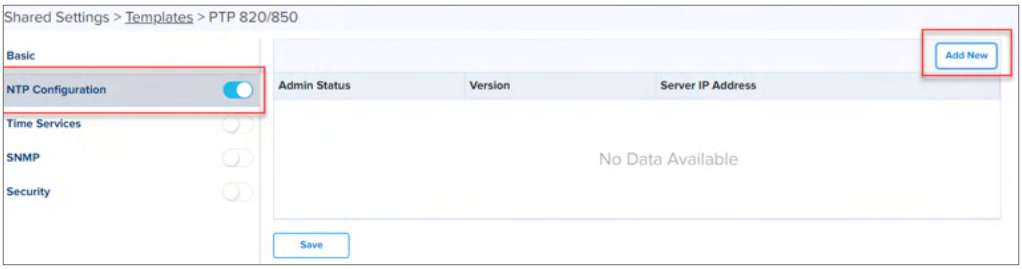
3. In the **Basic** page, enter **Name** and **Description** and click **Save**.

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.



NTP Configuration

1. In the **NTP Configuration,** click **Add New**.



Create window appears.

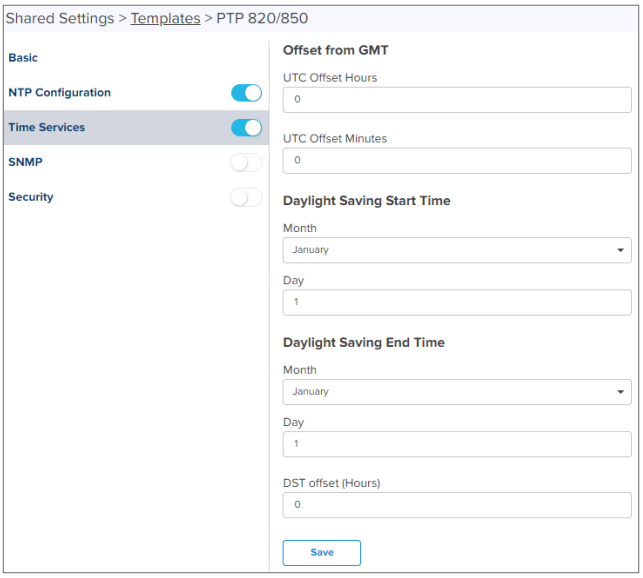
2. Select **Admin Status** from dropdown.
3. Select **Version** from dropdown.
4. Enter **Server IP Address**.
5. Click **Save.**

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

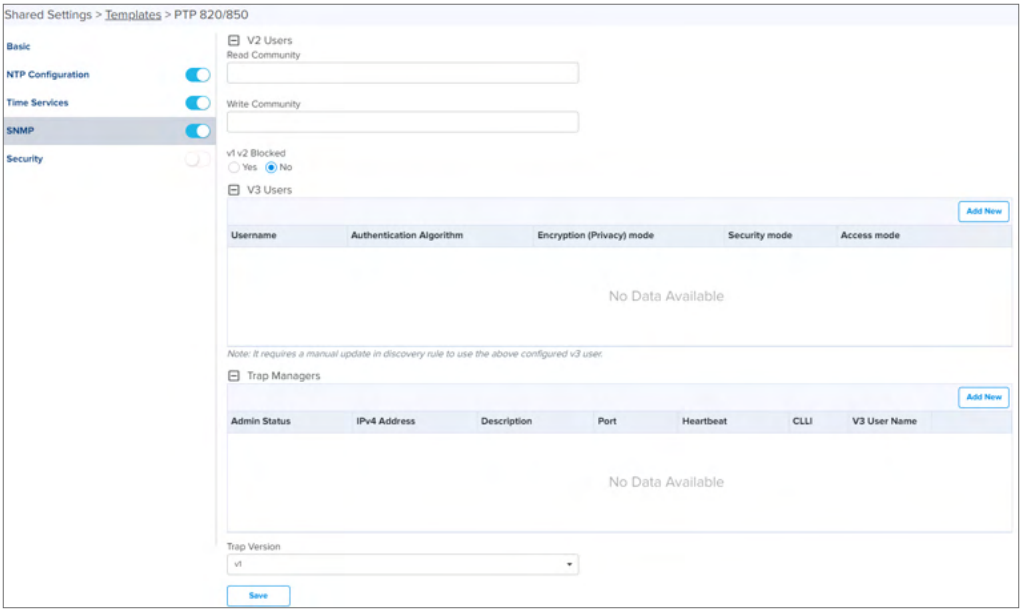
1. Enter the values for the following fields:
   - Offset from GMT
   - Daylight Saving Start Time
   - Daylight Saving End Time



2. Click **Save**.

SNMP

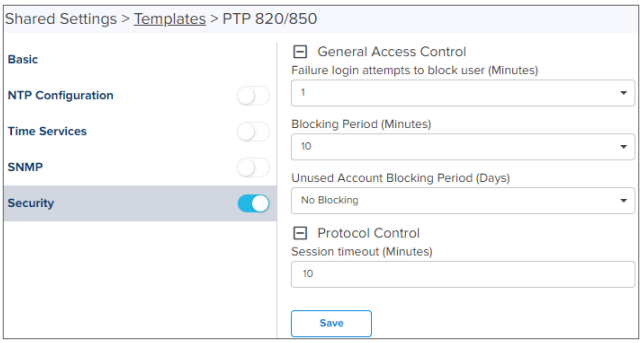
1. Enter the details for **V2 Users**, add **V3 Users** and **Trap Managers**, and select **Trap Version**.



2. Click **Save**.

Security

1. Select the values for **General Access Control**.
2. Select **Protocol Control**.



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 70 *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

To save and download the existing Device Configuration as Template, click **View Device Configuration** link.

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.

Start Job Now

If enabled, attempts to automatically start the configuration job immediately after creation.

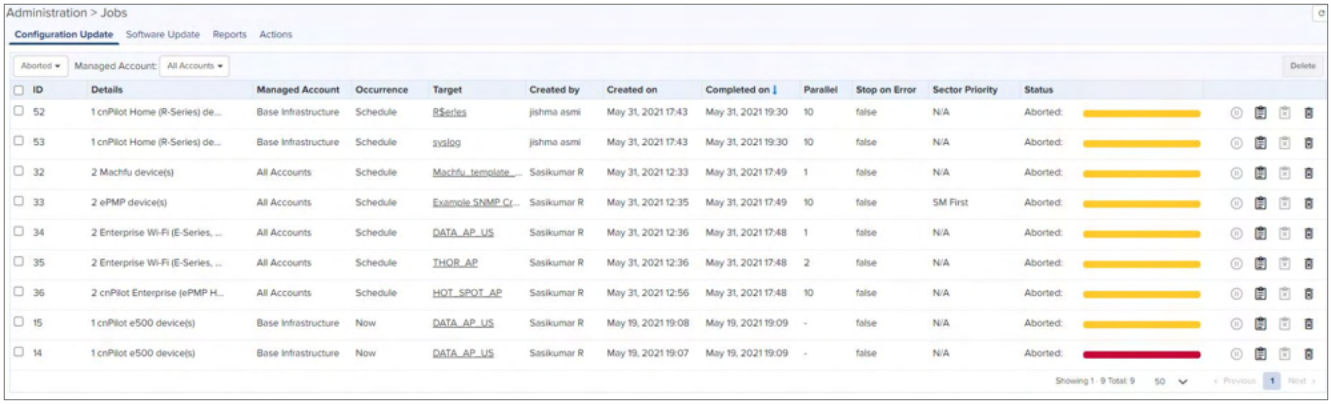
Update Ordering

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 270 *Abort Configuration*



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.
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 Backup

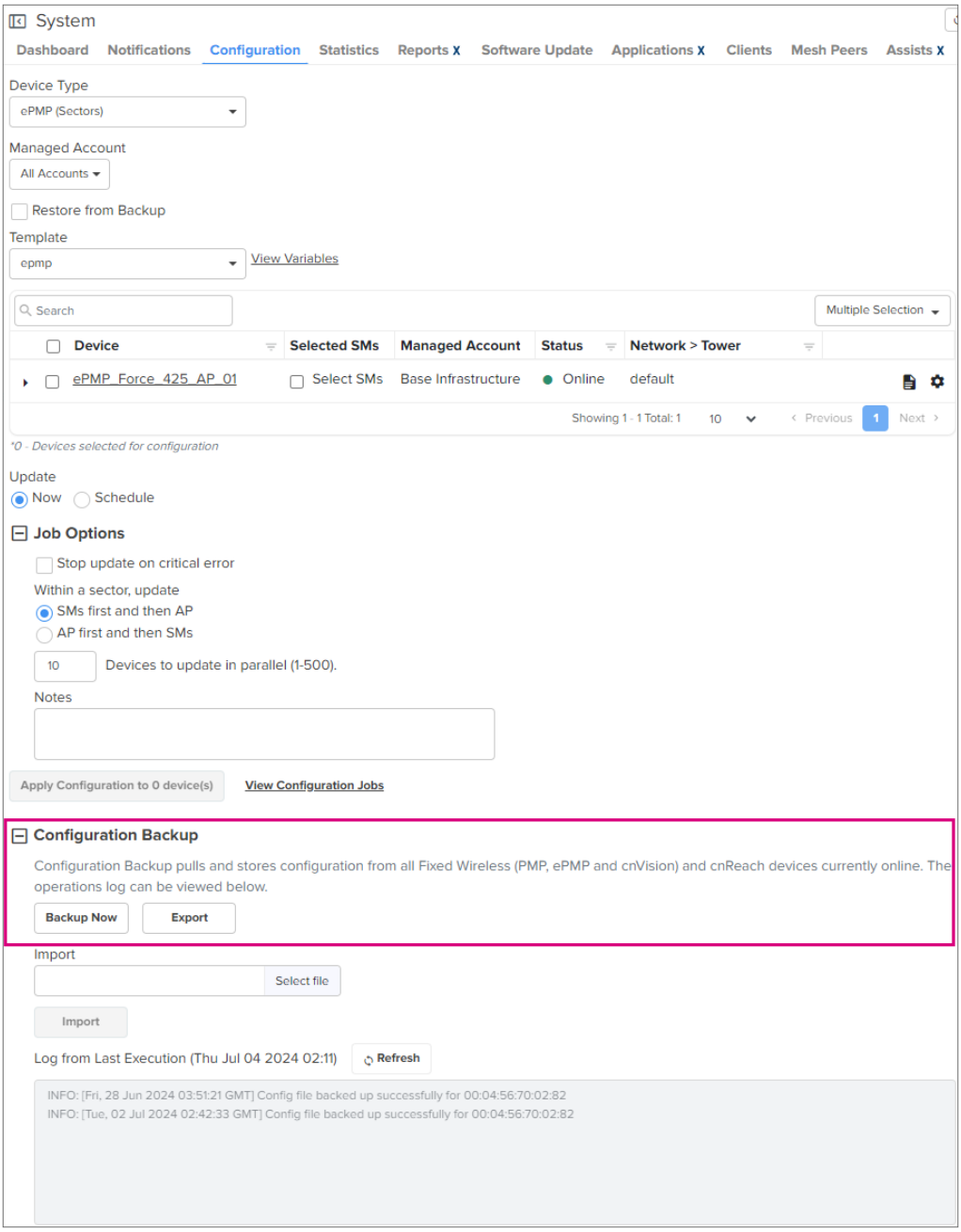
Configuration Backup pulls and stores configuration from Fixed Wireless (PMP, ePMP and cnVision) and cnReach devices which are currently online.

The backup operations can be performed at:

- System level
- Device level

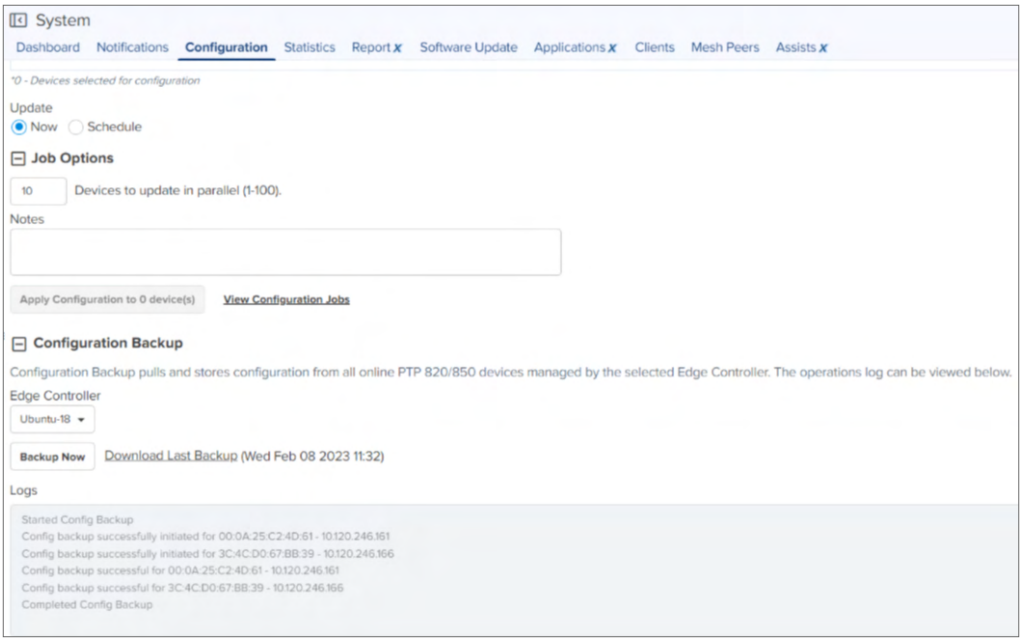
System level

1. Navigate to **Manage** > **Configuration**.
2. Select the **Device Type** (cnReach/cnVision/PMP/ePMP (Sectors)/PTP 820/850) from the dropdown.
3. Click the plus sign (+) next to **Configuration Backup** and click **Backup Now.**



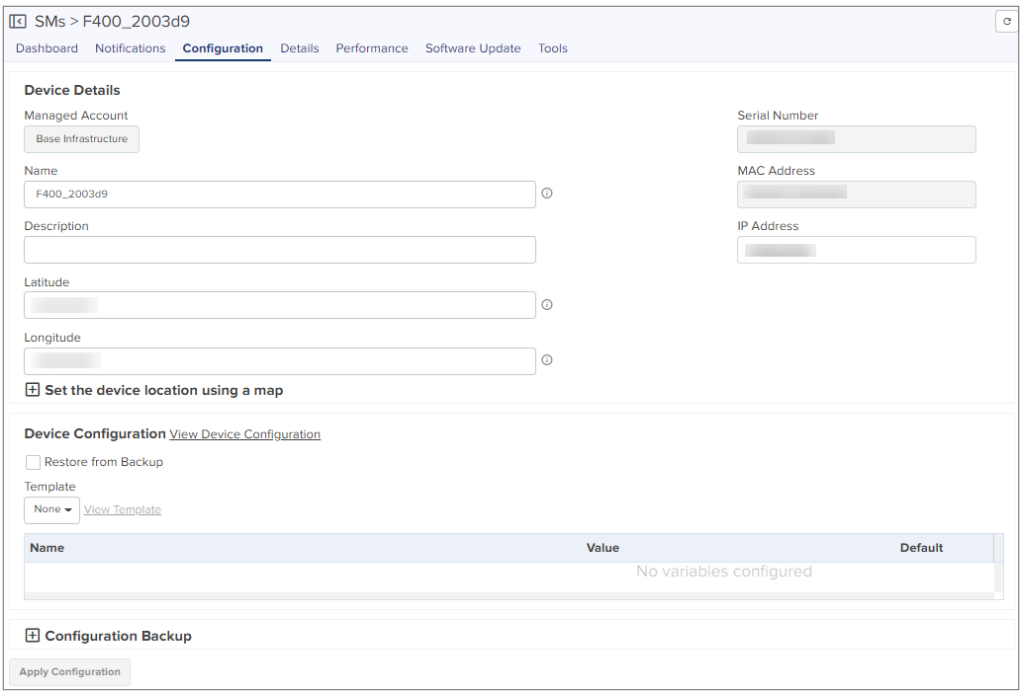
The last backup logs are displayed in **Log from Last Execution** tab with the date and time.

4. Click **Export** to export the backup in JSON format for other devices.
5. Click **Download Last Backup** for PTP 820/850 devices.



Device level

1. Navigate to **Manage > System.**
2. Select the **Device (cnReach/cnVision/PMP/ePMP)** in the Device Tree.
3. Click the plus sign (+) nextto **Configuration Backup** and click **Backup Now.**

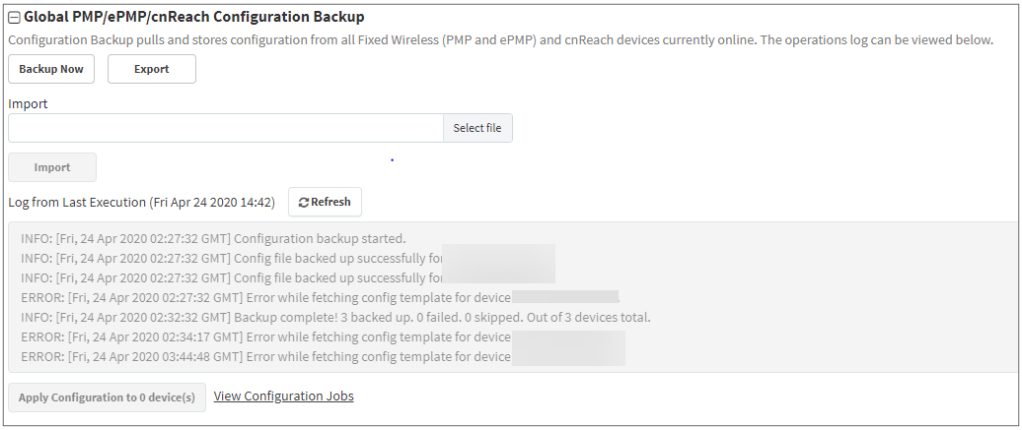


4. Click **View** to view the backup data.

Import Configuration Backup

To import the configuration backup of the device, perform the following steps:

1. Navigate to **Manage** > **Configuration** > **Device Details** in the Main Menu.
2. Select the **Device Type** (cnReach/cnVision/PMP/ePMP (Sectors)) from the dropdown.
3. Click the plus sign (+) nextto **Global cnReach/PMP/ePMP Configuration Backup.**
4. Browse to select the file to import**.**



5. Click **Import**.

Restore from Backup

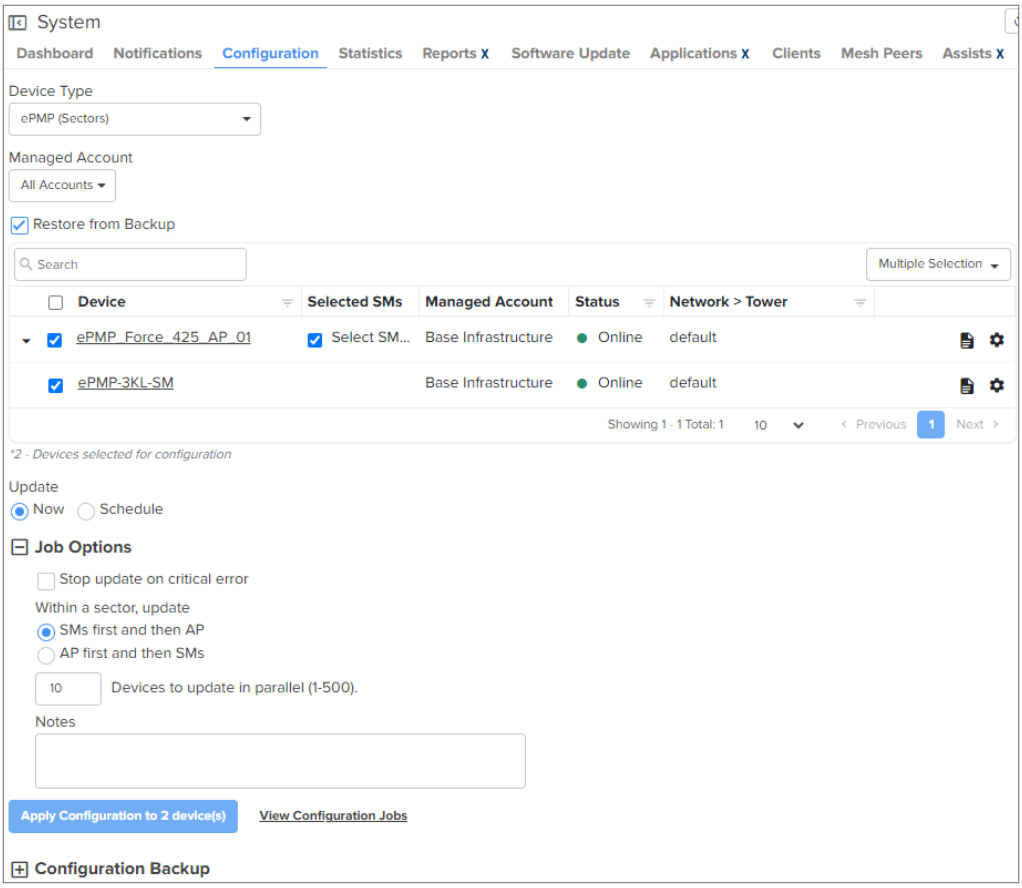
Restore from backup operations can be performed at two levels:

- System
- Device

System level

To restore the configuration backup of the device from system level, perform the following steps:

1. Navigate to **Monitor and Manage**.
2. Select **System/Managed Account/Network/Tower > Configuration** in the Main Menu.
3. Select **Device Type** (cnReach/cnVision/PMP/ePMP (Sectors)) from dropdown.
4. Select the **Restore from Backup** checkbox.
5. Select the device from the list.
6. Click **Apply Configuration.**

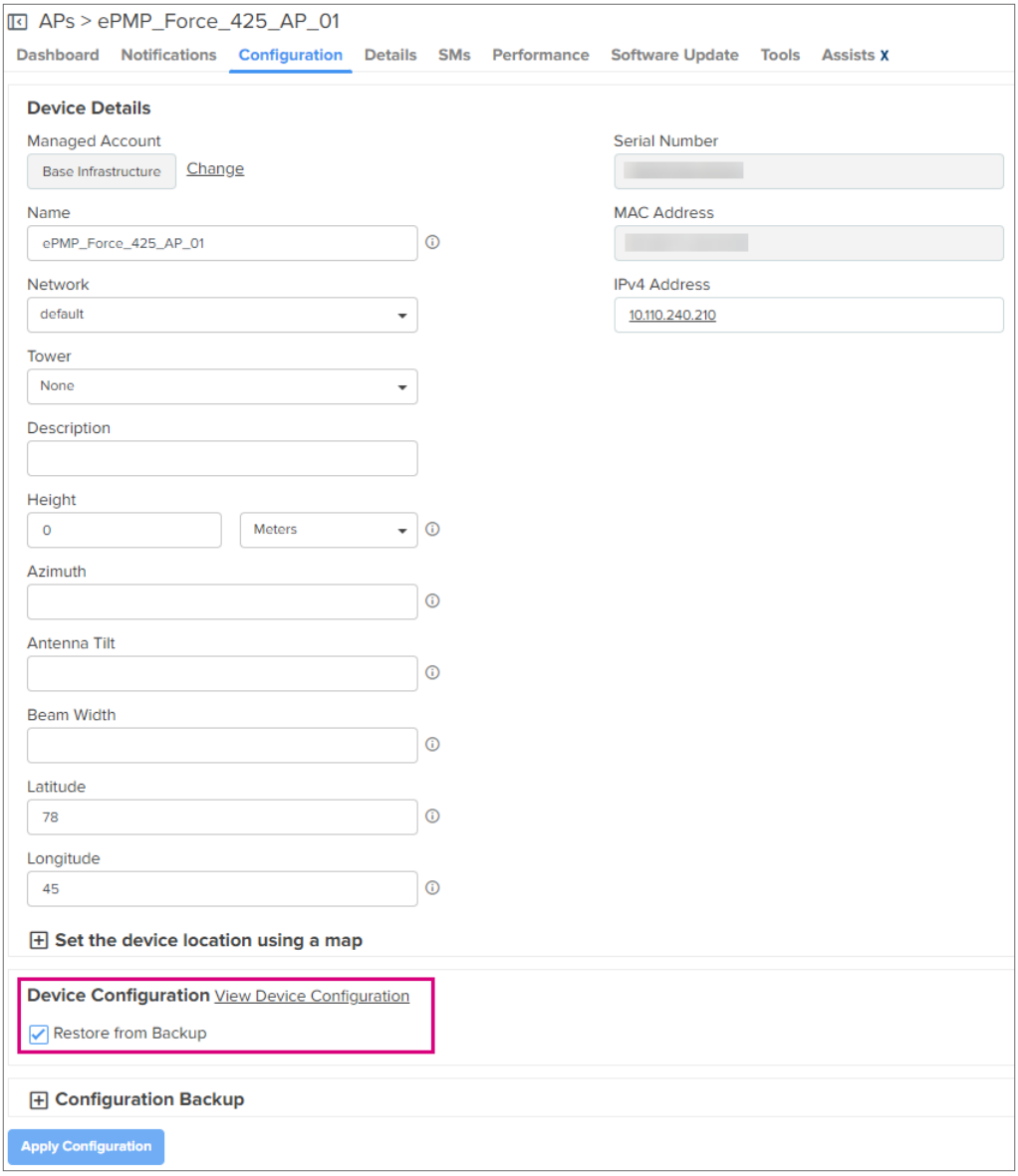


Device level

To restore the configuration backup of the device, perform the following steps:

1. Navigate to **Monitor and Manage > System.**
2. Select **cnReach/cnVision/PMP/ePMP Network** in the Device Tree.
3. Navigate to **Configuration > Device Configuration >** click **Restore from Backup**.

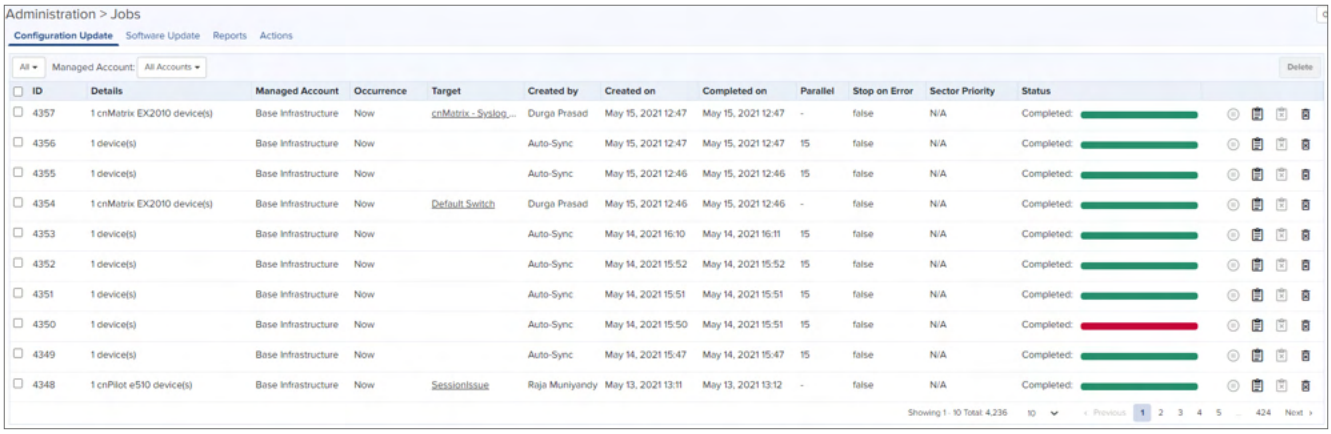
4. Click **Apply Configuration.**



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:



The following table displays the list of parameters in the **Jobs** tab:

Table 71 *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 can be managed through AP Groups and WLANs. Templates are also supported as a separate mechanism. This chapter focuses on AP Groups and WLANs.

This chapter provides details on the following sections:

- Enterprise Wi-Fi AP
- Association ACL
- Custom Applications

Enterprise Wi-Fi AP

This section provides the following details:

- Configuring Enterprise Wi-Fi APs using Wi-Fi Profiles
- Pre-Defined Overrides
- User-Defined Overrides
- User-Defined Variables
- Bulk Overrides
- Synchronize (Sync) Configuration
- Configuration Job Status
- Factory Reset

Following are the various types of Wi-Fi hardware available:

- Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)
- cnPilot Enterprise APs (ePMP 1000 Hotspot devices)
- cnPilot Home (cnPilot R-series devices)
- Enterprise Wi-Fi (Xirrus-Series)

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)

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 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.

This section covers the following topics:

- Create an AP Group
- Configuring 802.1X port-based authentication
- IPv6 Support
- Map WLANs to AP Groups
- Lock device Configuration
- Retrying configuration
- Apply AP Group to Device
- AP Group and WLAN Import/Export
- Creating a WLAN
- Creating an ePSK WLAN
- Configuring Wi-Fi offloading and Passpoint
- Access Control
- Services

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

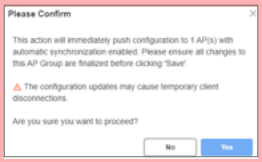
configuration template of CLI commands that needs to be updated manually. The Xirrus AP Group will support Auto Synchronization when the embedded template is changed, which makes it different than applying the configuration through the standalone Template mechanism.

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 271 *Warning when modifying WLAN*

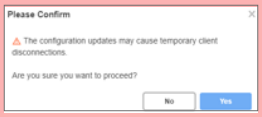
  

- Auto Sync is enabled and if no devices are present in the AP Group:

  OR

  Auto Sync is disabled and regardless of devices present or not in the AP Group:

  Figure 272 *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 273 *Basic: cnPilot Home (R-Series)*

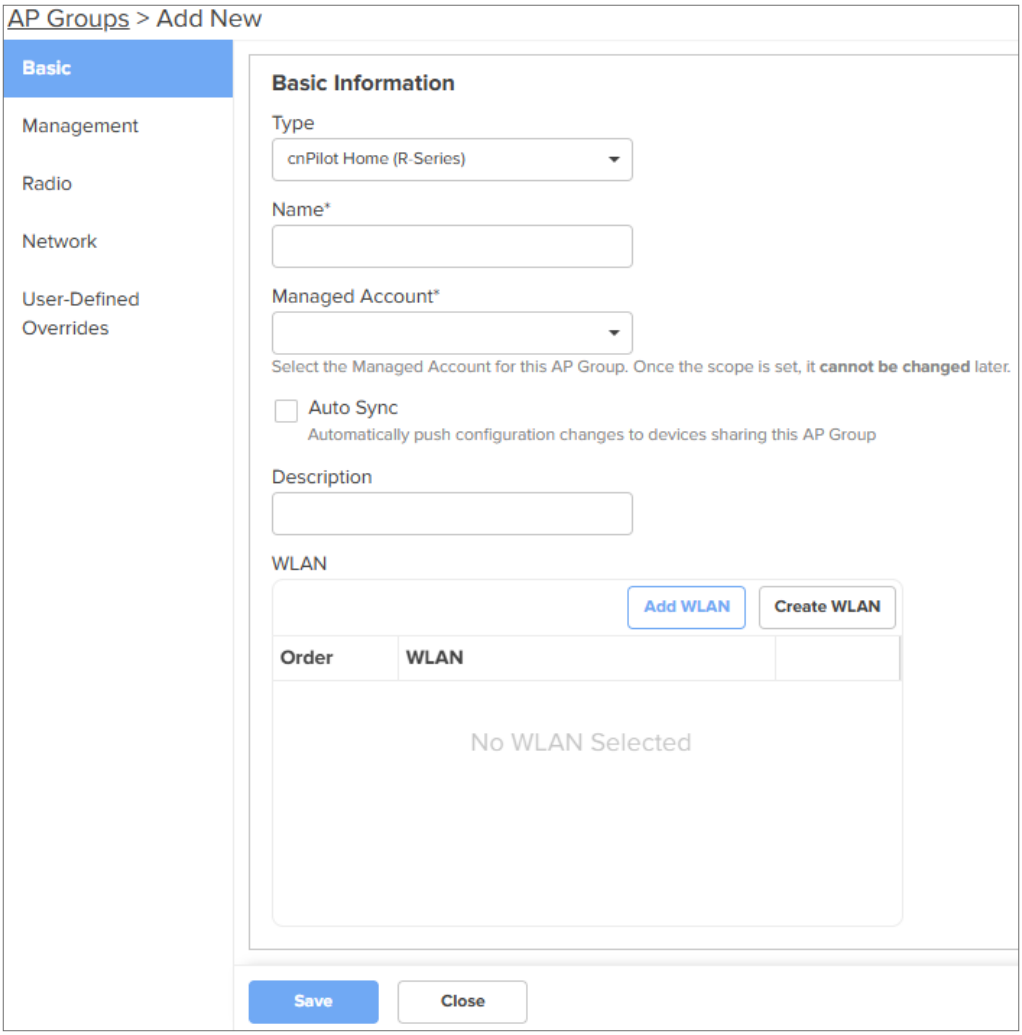


Figure 274 *Basic: Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)*

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-...

Name*

Managed Account*

Select the Managed Account for this AP Group. Once the scope is set, it **cannot be changed** later.

☑ Auto Sync

Automatically push configuration changes to devices sharing this AP Group

Country*

United States

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)

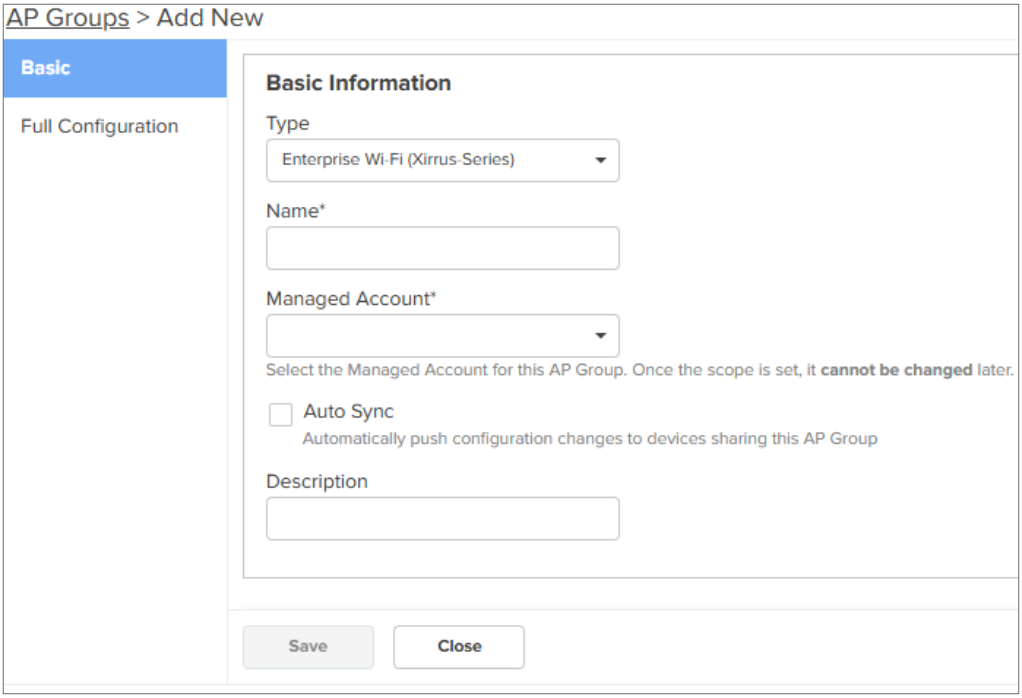
WLAN

Add WLAN | Create WLAN

Order	WLAN	
No WLAN Selected		

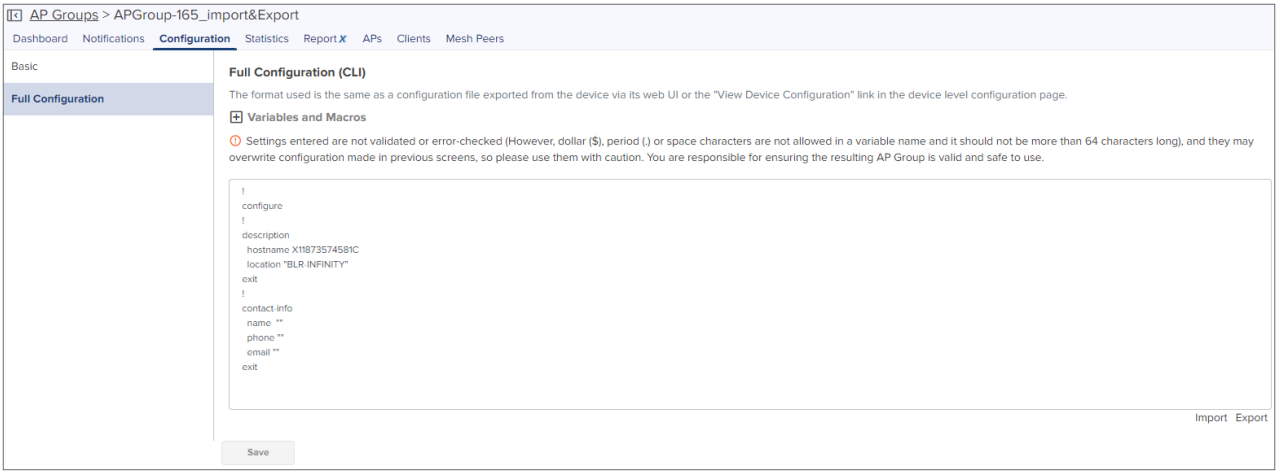
Save | Close

Figure 275 *Basic: Enterprise Wi-Fi (Xirrus-Series)*



The Xirrus AP Group embeds a Full Configuration of CLI commands.

Figure 276 *Full Configuration: Enterprise Wi-Fi (Xirrus-Series)*



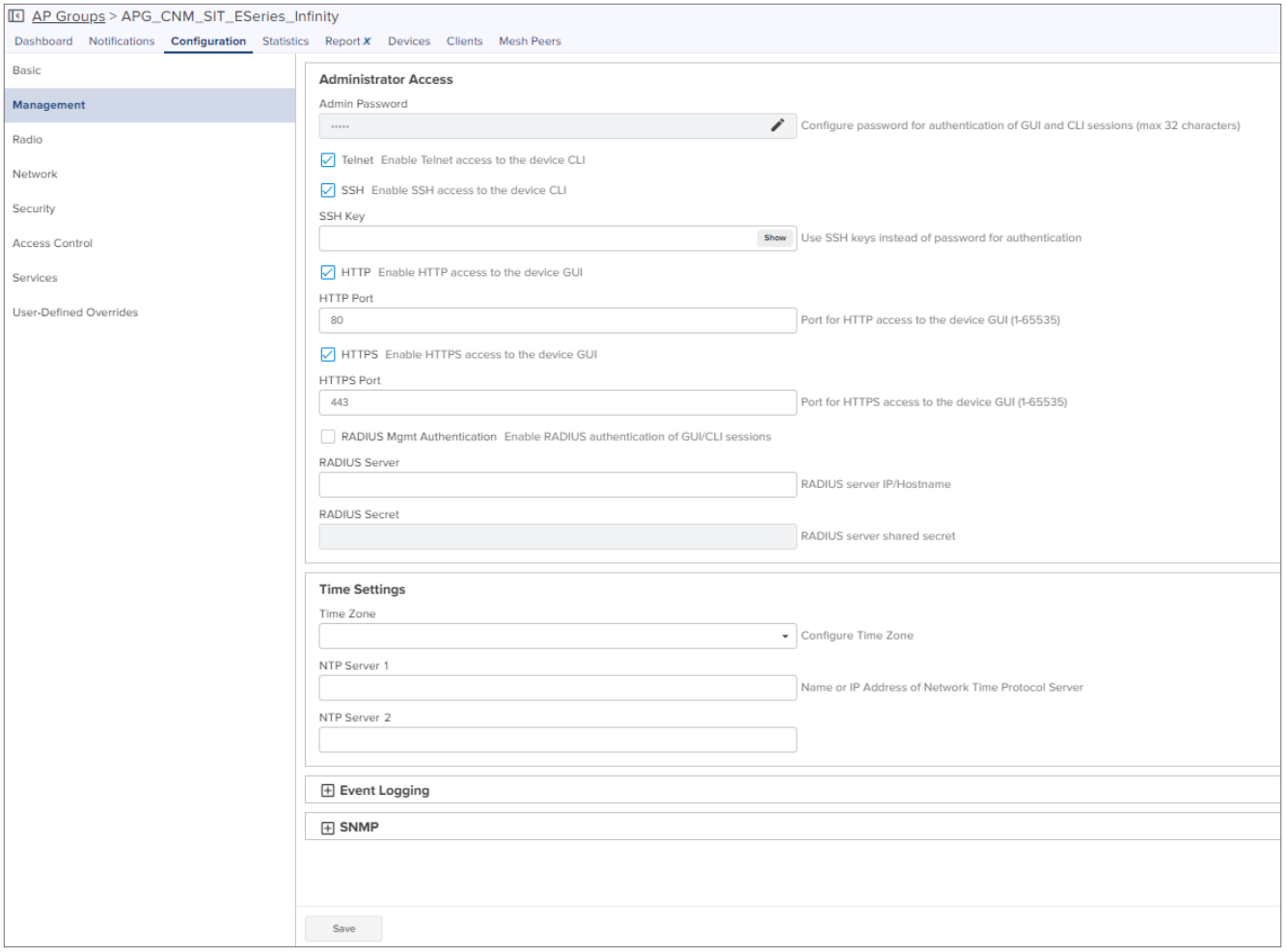
Management

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.

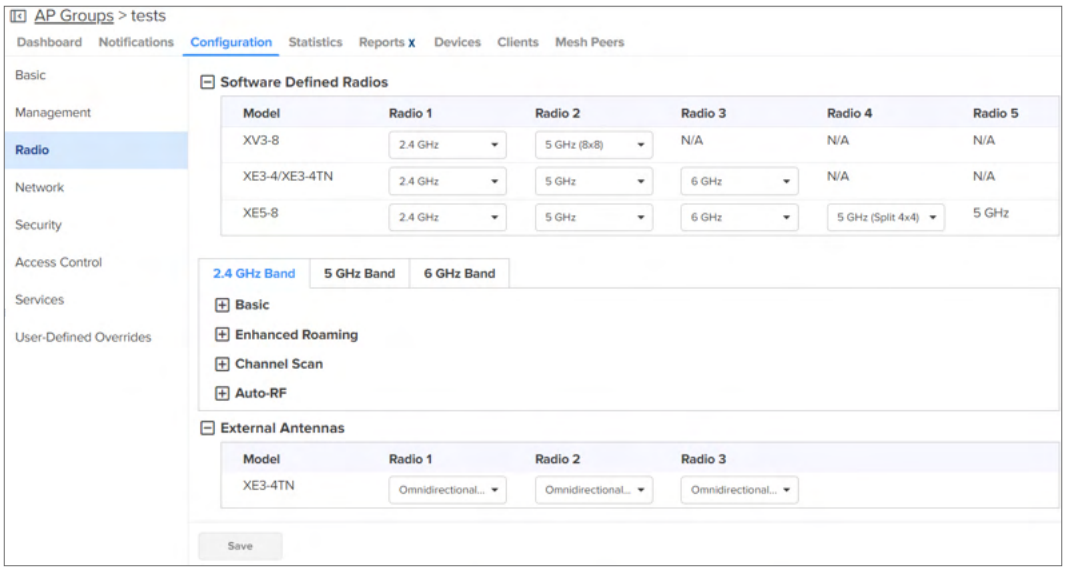
Figure 277 *Management: Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)*



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 278 *Radio: Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)*



> **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 278. The other radio bands for which the devices can be configured are as shown in Table 72.

Table 72 *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	• 100 to 165 in Split 4x4 dual radio • 36 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 73 for Supported Channel list in 5 GHz and 6 GHz
	Radio 3	5 GHz or 6 GHz	20 / 40 / 80 / 160	20*/80**	
	Radio 4	5 GHz (8x8 - single radio) or 5 GHz (Split 4x4 dual radio)	20 / 40 / 80	20	
	Radio 5		20 / 40 / 80		
* 5 GHz **6 GHz					

Note

- Split 4x4 is applicable only for 8x8 spatial streams supported devices. (Supported device models are XV3-8 and XE5-8).
- Dual 5 GHz Radio (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 73 *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
!
```

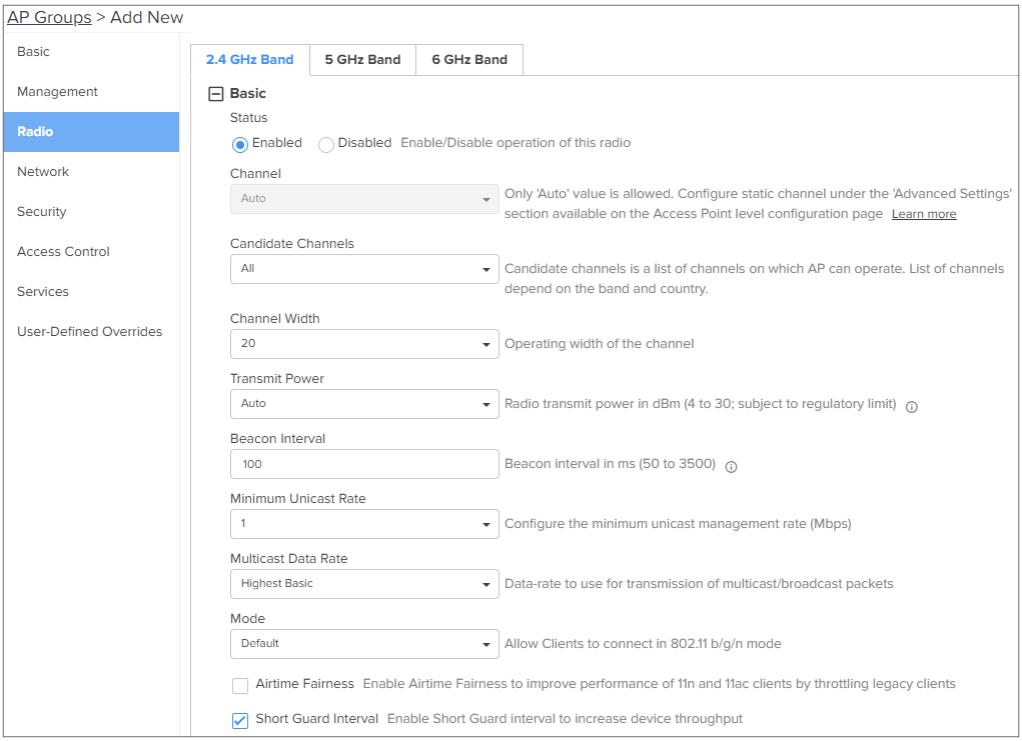
5. Click **Save**.

1. In the **Radio** tab, you can configure **Software Defined Radios** for the required **Model** as shown in Table 72.

   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.

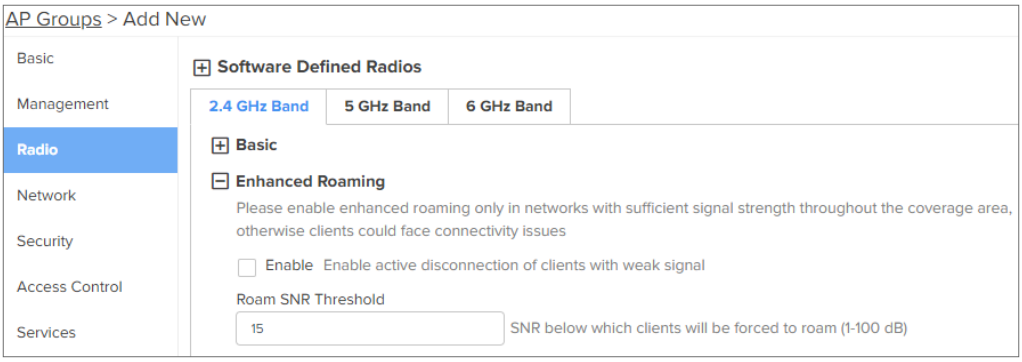
2. Expand the **Basic** section, select either **Enable** or **Disable** option to enable or disable the radio.
3. Select **Auto** in the **Channel** dropdown.
4. In the **Candidates Channel** select **All.**
5. Select the parameter values from the dropdown for the following fields:.
   - Channel Width
   - Transmit Power
   - Beacon Interval
   - Minimum Unicast Rate
   - Multicast Data Rate
   - Mode

   Figure 279 *Radio page - Basic section*



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.



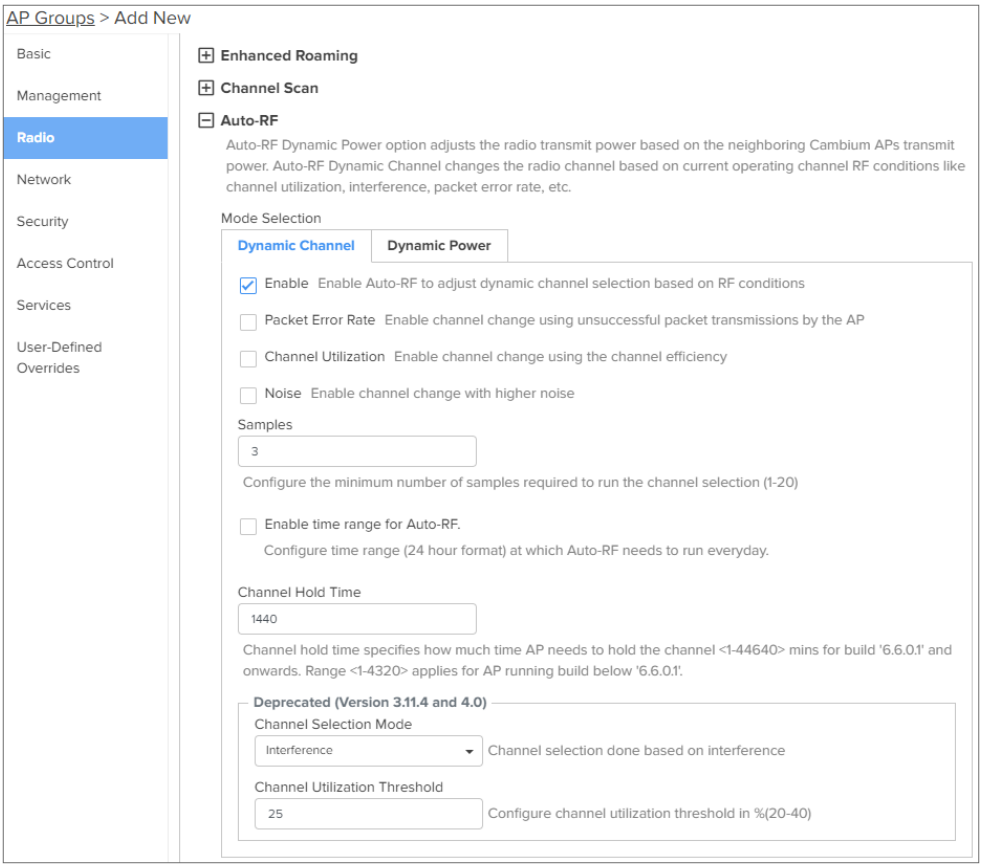
Note

Enable **Enhanced Roaming** only in networks with sufficient signal strength throughout the coverage area, otherwise clients could face connectivity issues.

7. Expand the **Channel Scan** section and select the **Off Channel Scan** checkbox:

8. Expand the **Auto-RF** section and configure any of the following modes:

   - **Dynamic Channel**



Note

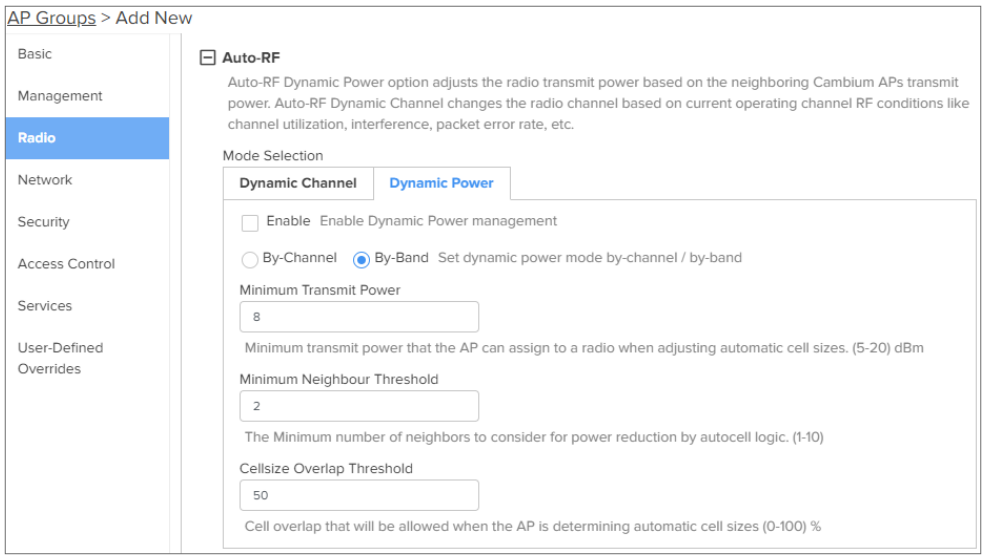
The **Channel Hold Time** parameter specifies the time (in minutes) for which the AP will hold the channel.

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**



9. Click **Save**.

External Antennas

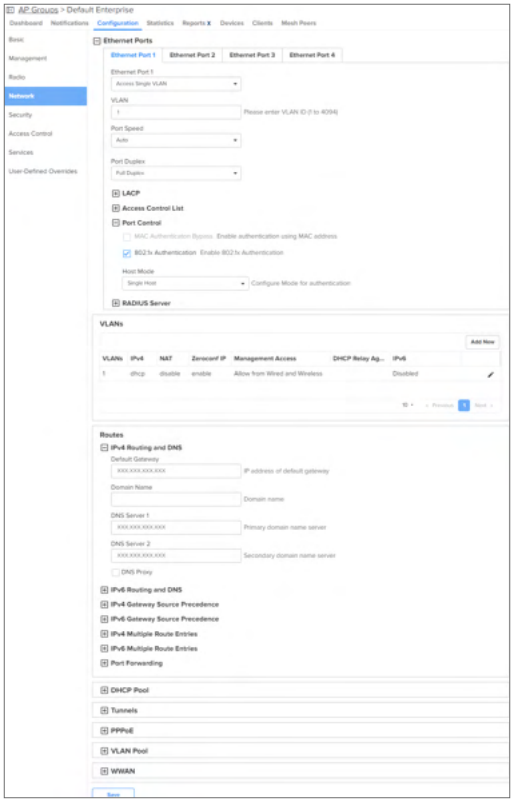
This feature allows users to customize the antenna models for each of the three radios in the XE3-4TN AP as shown in Figure 280. This customization helps in achieving optimal wireless network performance customized for specific deployment scenarios.

Figure 280 *External Antennas for XE3-4TN APs*

Network

The **Network** page allows to configure **Ethernet Ports**, **VLANs**, **Routes** for IPv4 and IPv6, **DHCP Pool, Tunnels, PPPoE , VLAN Pool,** and **WWAN**.

Figure 281 *Network: Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)*



Configuring tunnels

The following table lists the fields that are displayed in **AP Groups** > **Network** > **Tunnel** section.

Figure 282 *WLAN Concentrator > L2GRE parameters*

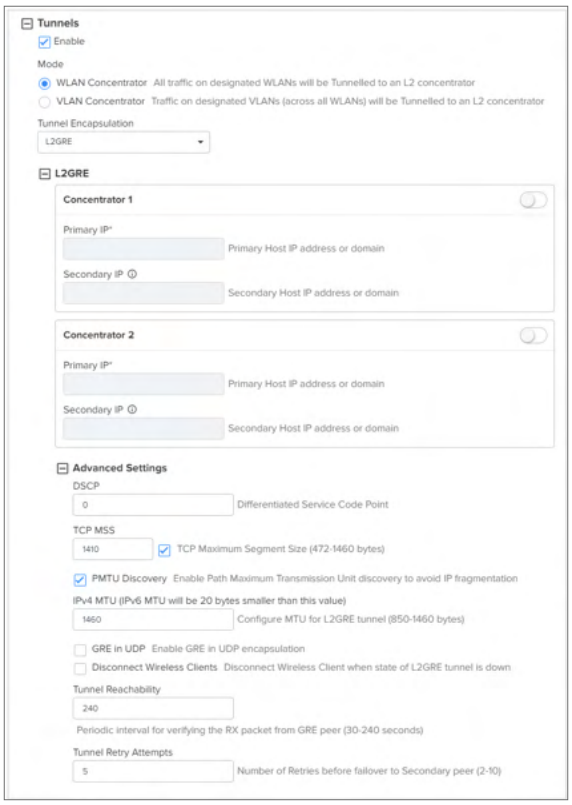


Figure 283 *WLAN Concentrator > L2TP parameters*

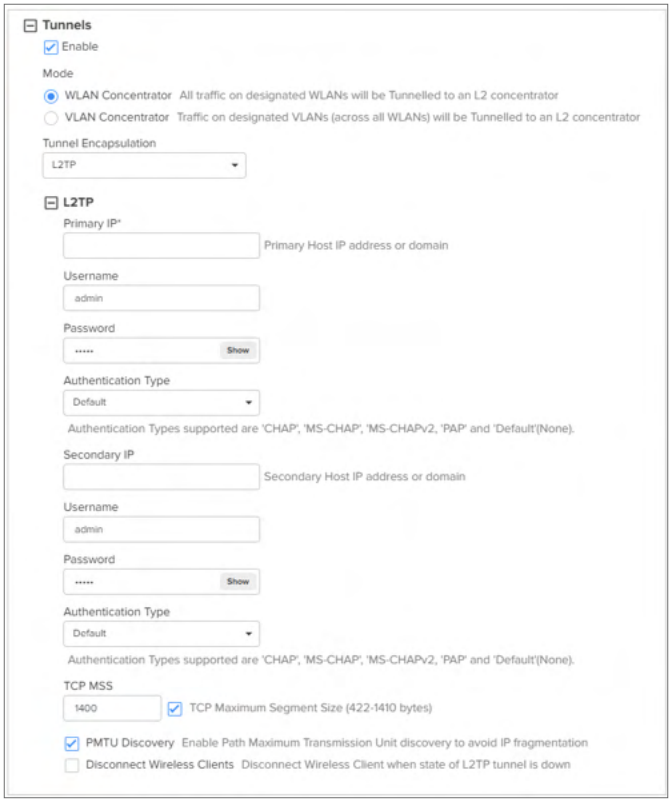


Figure 284 *VLAN Concentrator—Only L2GRE parameters*

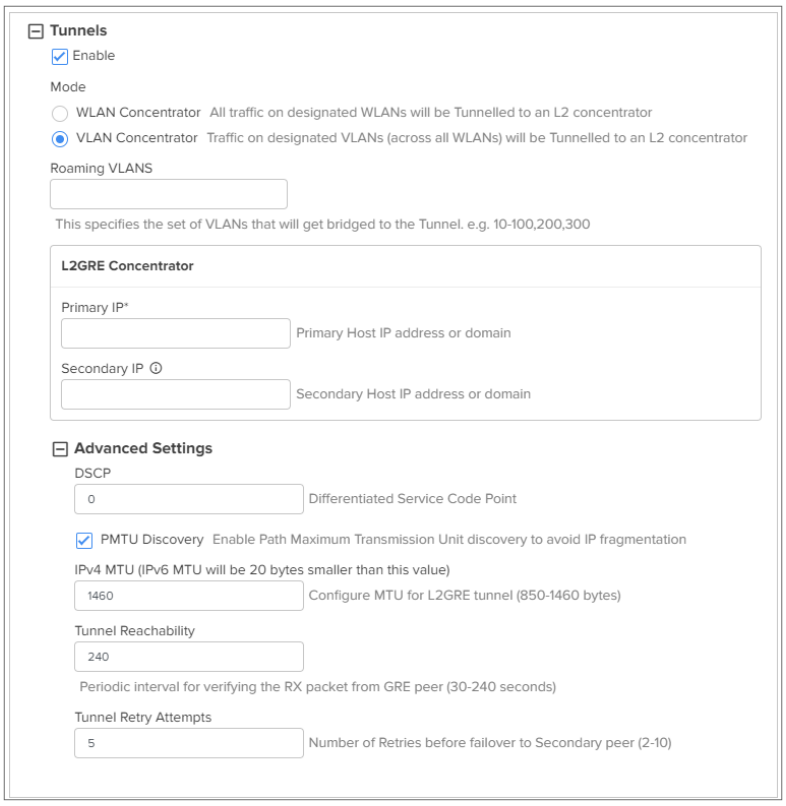


Table 74 *Tunnels parameters*

Parameters	Description	Range	Default
Enable	Enables or disables tunneling for the AP Group.	–	Disabled
Mode	Indicates the mode in which the tunnel must function. The following modes are supported: • **WLAN Concentrator**—All traffic on designated WLANs will be tunneled to an L2 concentrator You can configure both L2GRE and L2TP tunnels in this mode. • **VLAN Concentrator**—All traffic on designated VLANs (across all WLANs) will be tunneled to an L2 concentrator You can configure only L2GRE tunnels in this mode.	–	**WLAN Concentrator**
Tunnel Encapsulation	This parameter is available only when you select **WLAN Concentrator** in the **Mode** field. Indicates the tunnel type. Following tunnel types are supported: • L2TP • L2GRE	–	L2GRE
WLAN Concentrator-related parameters			
L2GRE You can configure a maximum of two L2GRE tunnels. Configure L2GRE-1 tunnel by configuring the below parameters in the **AP Groups** > **Network** > **Tunnels** section. However, configuring L2GRE-2 tunnel is allowed using the device CLI only.			
Concentrator-1 To enable concentrator 1, toggle the switch ( ) to the on ( ) position.			
Primary IP	IP address of the primary L2GRE concentrator 1. Either IPv4/IPv6 address or primary hostname of an endpoint is supported.	–	–
Secondary IP	IP address of the secondary L2GRE concentrator 1. Either IPv4/IPv6 address or Secondary hostname of an endpoint is supported.	–	–

Parameters	Description	Range	Default
	Note The tunnel operates in failover mode. After determining the peer is down (no Rx packet received from PEER), AP sends periodic ICMP packet to verify the reachability to the peer before failing over to secondary peer. So ensure ICMP reachability to the tunnel PEER.		
Concentrator-2 To enable concentrator 2, toggle the switch ( ) to the on ( ) position.			
Primary IP	IP address of the primary L2GRE concentrator 2. Either IPv4/IPv6 address or primary hostname of an endpoint is supported.	–	–
Secondary IP	IP address of the secondary L2GRE concentrator 2. Either IPv4/IPv6 address or Secondary hostname of an endpoint is supported. **Note** The tunnel operates in failover mode. After determining the peer is down (no Rx packet received from PEER), AP sends periodic ICMP packet to verify the reachability to the peer before failing over to secondary peer. So ensure ICMP reachability to the tunnel PEER.	–	–
Advanced Settings			
DSCP	Specifies the value of the Differentiated Services Code Point (DSCP) to configure priority of GRE packets.	–	0
TCP MSS	TCP Maximum Segment Size (MSS) in bytes.	472-1460	1410
PMTU Discovery	Provision to enable to discover Path Maximum Transmission Unit (PMTU) in network.	–	–

Parameters	Description	Range	Default
IPv4 MTU	Maximum Transmission Unit in bytes. **Note** IPv6 MTU will be 20 bytes smaller than this value.	850-1460	1460
GRE in UDP	GRE protocol is designed to establish a tunnel between any third-party vendor which complies with RFC 8086.	–	Disabled
Disconnect Wireless Clients	Provision to disconnect Wireless Client when a state of L2TP tunnel is down.	–	Enabled
Tunnel Reachability	The periodic interval for verifying the RX packet from GRE peer.	30-240	240
Tunnel Retry Attempts	Number of retries before failover to secondary peer.	2-10	5
L2TP			
Primary IP	IP address of the primary L2TP endpoint. Either IPv4/IPv6 address or primary hostname of an endpoint is supported.	–	–
(Primary) Username and Password	Credentials required for authentication of primary L2TP endpoint.	–	admin/admin
(Primary) Authentication Type	Provision to select the authentication method for secondary L2TP endpoint. Following are the options available: • DEFAULT (None) • CHAP • MS-CHAP • MS-CHAPv2 • PAP	–	DEFAULT
Secondary IP	IP address of the secondary L2TP endpoint. Either IPv4/IPv6 address or primary hostname of an endpoint is supported.	–	–
(Secondary) Username and Password	Credentials required for authentication of secondary L2TP endpoint.	–	admin/admin
(Secondary) Authentication Type	Provision to select the authentication method for secondary L2TP endpoint. Following are the options available: • DEFAULT (None) • CHAP • MS-CHAP	–	DEFAULT

Parameters	Description	Range	Default
	• MS-CHAPv2 • PAP		
TCP MSS	TCP Maximum Segment Size (MSS) in bytes.	422- 1410	1400
PMTU Discovery	Provision to enable to discover PMTU in a network.	–	Enabled
Disconnect Wireless Clients	Provision to disconnect Wireless Client when the state of L2TP tunnel is down.	–	Disabled
VLAN Concentrator-related parameters			
Roaming VLANs	List of VLANs that must be bridged to the tunnels.	–	–
L2GRE Concentrator			
Primary IP	IP address of the primary L2GRE concentrator. Either IPv4/IPv6 address or primary hostname of an endpoint is supported.		
Secondary IP	IP address of the secondary L2GRE concentrator. Either IPv4/IPv6 address or Secondary hostname of an endpoint is supported. **Note** The tunnel operates in failover mode. After determining the peer is down (no Rx packet received from PEER), AP sends periodic ICMP packet to verify the reachability to the peer before failing over to secondary peer. So ensure ICMP reachability to the tunnel PEER.		
Advanced Settings			
DSCP	Specifies the value of the Differentiated Services Code Point (DSCP) to configure priority of GRE packets.	–	0
PMTU Discovery	Provision to enable to discover PMTU in a network.	–	Enabled
IPv4 MTU	Maximum Transmission Unit in bytes. **Note** IPv6 MTU will be 20 bytes smaller than this value.	850-1460	1460

Parameters	Description	Range	Default
Tunnel Reachability	The periodic interval for verifying the RX packet from GRE peer.	30-240	240
Tunnel Retry Attempts	Number of retries before failover to secondary peer.	2-10	5

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 75 *RADIUS Server parameters*

Parameters	Description	Range	Default
Authentication Server	Specifies the authentication server details, such as: • **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`	-	Disabled

Parameters	Description	Range	Default
	A maximum of three RADIUS authentication servers can be configured.		
Accounting Server	Specifies the accounting server details, such as: • **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` A maximum of three RADIUS accounting servers can be configured.	-	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	Specifies the accounting mode to be used. The following modes are supported: • **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 choose Failover mode. • **Load Balance**—AP equally distributes the requests between the configured RADIUS servers, • **Failover**—AP selects the RADIUS server that is functional based on the order of configuration.	-	Failover
Interim update interval	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

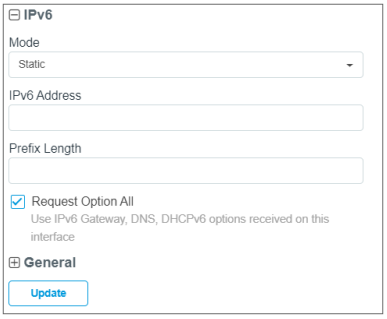
IPv6 enables the next generation of large-scale IP networks by supporting addresses that are 128 bits long.

Configuring IPv6

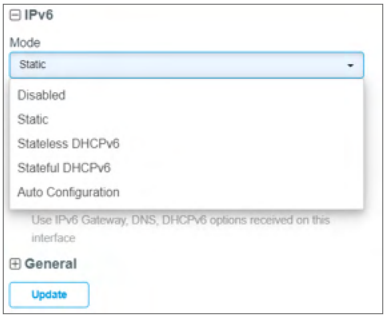
To configure IPv6, perform the following:

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.



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**.



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.

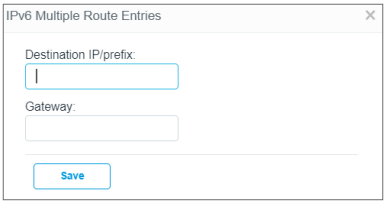
5. Enable **Request Option All** to use the IPv6 Gateway, DNS, DHCPv6 options received on this interface.

   By default the priority of **IPv6 Gateway Source Precedence** is **Static** and then **Auto-config/DHCPv6**.

To create a new static Route,

1. Navigate to **IPv6 Multiple Route Entries** section.
2. Click **Add New.**

3. Enter **Destination IP/Prefix** and **Gateway**.



4. Click **Save**.

To set the preference of IPv4 and IPv6:

1. Navigate to **Routes** tab.
2. Select the **IPv6 Preference** checkbox.

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:

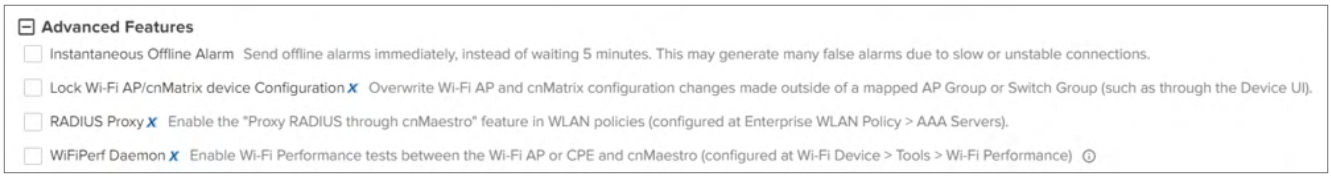
1. Client (maximum of one Mesh Client is selected)
2. Base (maximum of two Mesh Base is selected)
3. Recovery (maximum of one Mesh Recovery is selected)
4. WLANs with Mesh Mode Off (total WLAN limit including Mesh WLANs)

Note

Maximum of 16 WLAN policies are supported for E-Series and XV-Series devices and 8 WLAN policies are supported for ePMP 1000 Hotspot. 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.

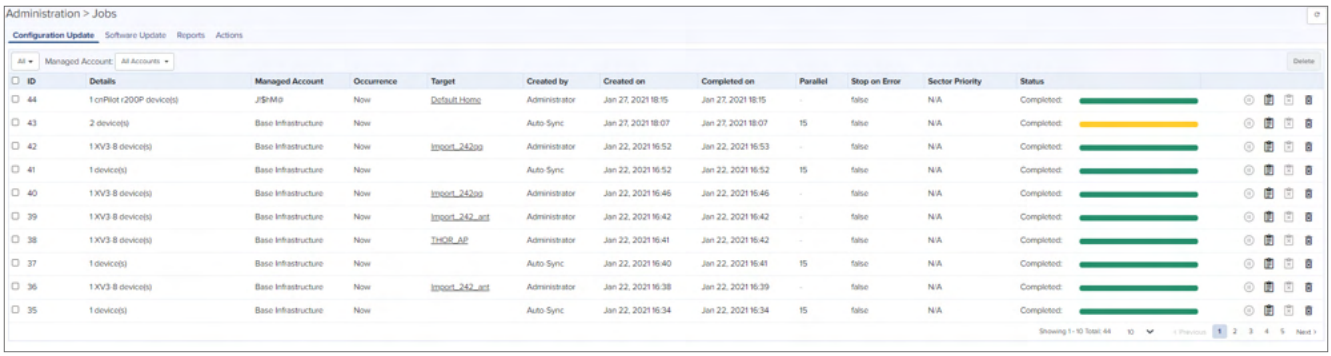


To enable this feature, perform the following steps:

1. Navigate to **Configuration** > **Advanced Features** page.
2. Select the **Lock cnPilot/cnMatrix device Configuration** checkbox.
3. Click **Save**.

When a configuration change is made on the device using UI or CLI, cnMaestro detects the change and the device is marked **Not In Sync**. In this scenario, an **Auto-Sync** job is triggered to automatically revert the changes.

The **Auto-Sync** job can be viewed in **Administration** > **Jobs** > **Configuration Update** page.

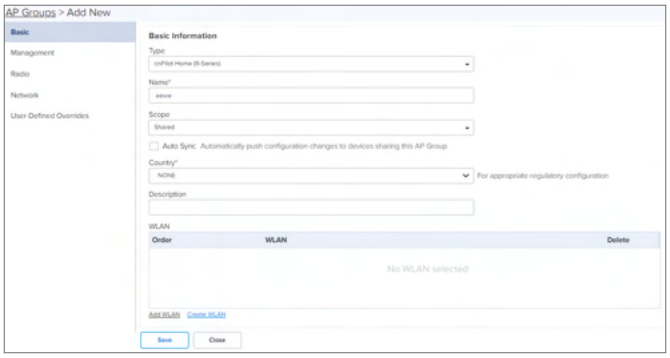


Retrying configuration

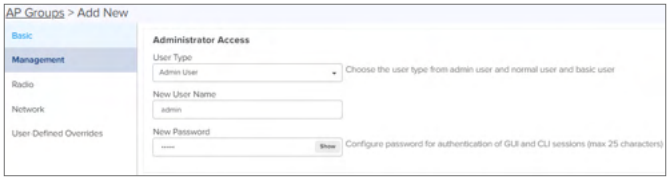
When the user applies an AP Group to the device, and the Job is skipped because the device is Offline, the reason for the skip will be displayed as **Device was offline** in the **Jobs** page. When device comes up and connects to cnMaestro, an **Auto-Sync** job pushes the AP Group to the device. (It will not apply the AP Group if **Auto-Sync** is disabled in the AP Group).

Note

The Config Update (**Auto-Sync**) will happen only when the **Auto-Sync** option is enabled in the AP Groups page. If the device was Skipped/Failed for any reason other than the **Device was offline**, the device will not be updated.



The default password **admin** of cnPilot R-Series should be changed before upgrading to the build 4.6-RX.



After upgrading to 4.6-RX, the default password **admin** is invalid and needs to be reset through the WAN.

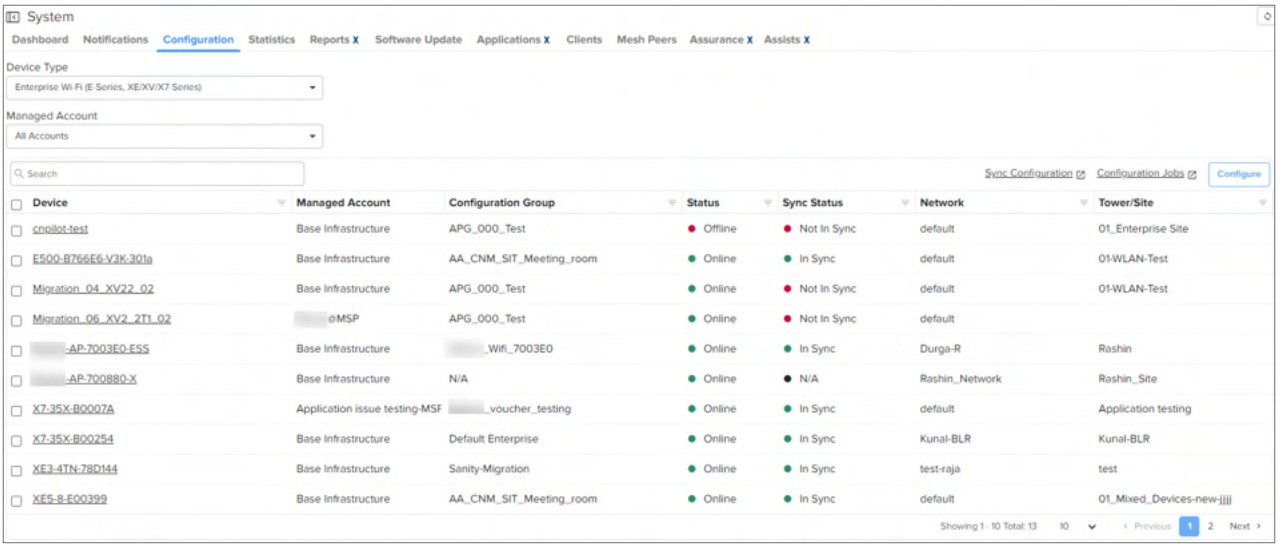
> **Note**
>
> Default User Name: **admin** can be used after the upgrade.

Apply AP Group to Device

A Configuration Job can be created as follows:

1. Navigate to **Monitor and Manage > System > Configuration**.

   Figure 285 *System Configuration (Enterprise Wi-Fi E-Series, XE,/XV/X7-Series)*



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 286 *Configuration page: Enterprise Wi-Fi (E-Series, XE,/XV/X7-Series)*

   Figure 287 *Configuration page: cnPilot Home (R-Series)*

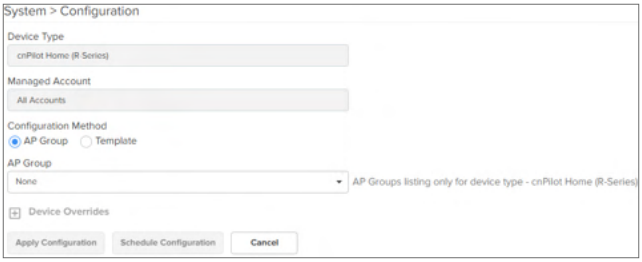
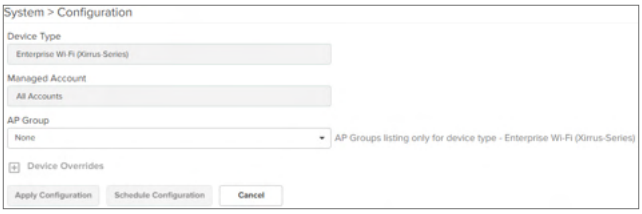


   Figure 288 *Configuration page: Enterprise Wi-Fi (Xirrus-Series)*



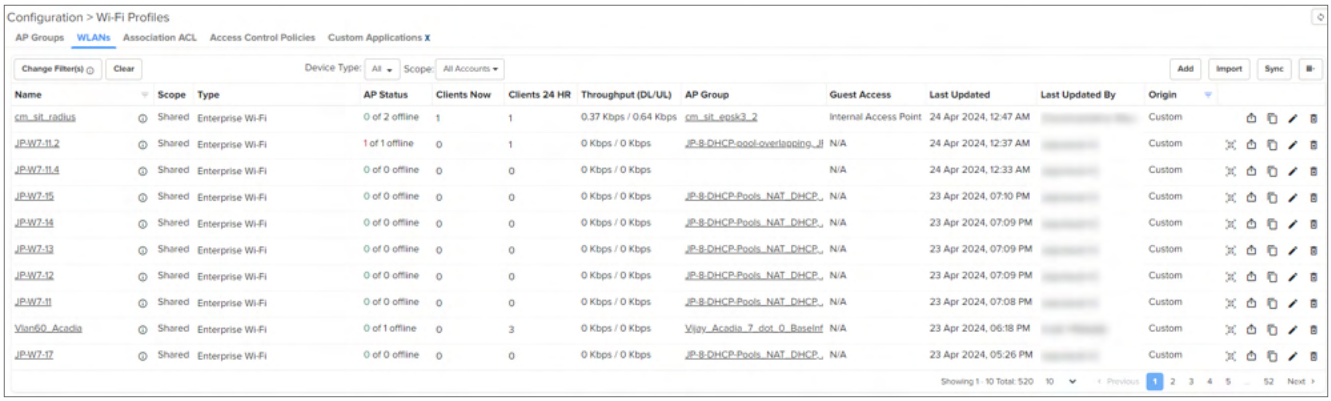
5. Select the AP group from the **AP Group** dropdown list.
6. Click **Apply Configuration.**

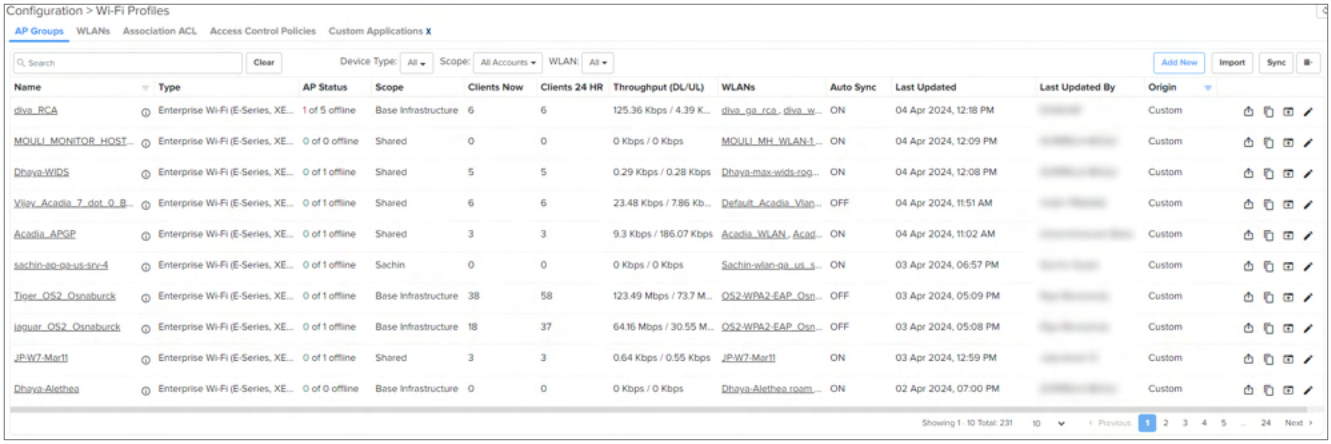
AP Group and WLAN Import/Export

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.





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 **Managed Account** from the 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**.

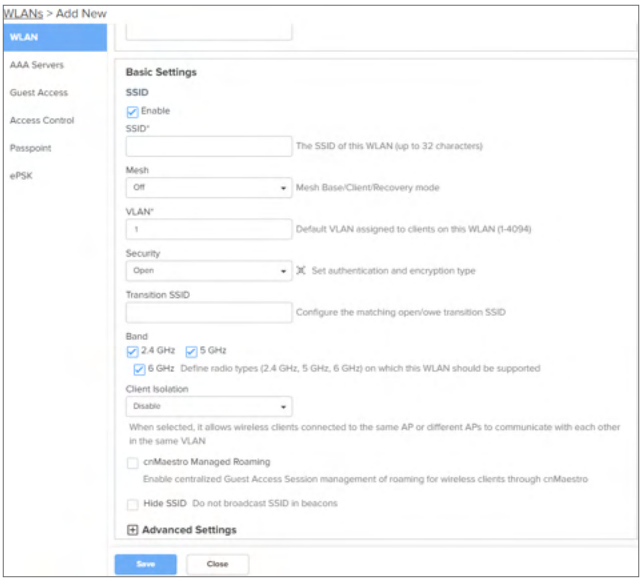
As with AP Groups, WLANs are separated into cnPilot Home and Enterprise Wi-Fi. You can configure WLAN, RADIUS, Guest Access, Usage Limits, Scheduled Access, and Access parameters with Enterprise Wi-Fi WLANs. With the cnPilot Home WLANs, you can configure SSID, Scheduled Access, and Access parameters.

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.



The following table lists the description of the basic and advanced parameters available in the WLAN tab:

Table 76 *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: • **Base**: A WLAN profile configured with a mesh-base will operate as a normal AP. Its radio will beacon on startup so its SSID can be seen by radios configured as mesh-clients. • **Client**: A WLAN profile configured with mesh-client will scan all available channels on startup, looking for a mesh-base AP to connect. • **Recovery**: WLAN profile configured as mesh-recovery will broadcast a pre-configured SSID upon detection of mesh link failure after a successful connection. This needs to be exclusively configured on a mesh-base device. Meshclient will auto scan for mesh-recovery SSID upon failure of mesh link. • **Off**: Mesh support disabled on WLAN profile.	-	Off (Access Profile Mode)
VLAN	Segregates wireless station traffic from AP traffic in the network. Wireless stations obtain an IP address from the subnet configured in the VLAN field of the WLAN profile.	1-4094	1
Security	Determines key values that are encrypted based on the selected algorithm. Following security methods are supported:	-	Open

Parameters	Description	Range	Default
	• **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 `allow-tkip` CLI option. **Note** 6 GHz clients connect to the AP using the secure Simultaneous Authentication of Equals (SAE) method. • **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** 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. **Note** When you select **WPA2/WPA3 Pre-shared Keys** or **WPA3 Pre-shared Keys**, you can enable registration flow for WPA3 clients. 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 Wi-Fi Configuration.		

Parameters	Description	Range	Default
	• **WPA3 Enterprise** WPA3 also introduces Enterprise AES CCMP encryption. This level of security provides consistent cryptography and eliminates the mixing and matching of security protocols that are defined in the 802.11 standards. • **WPA3 Enterprise CNSA** WPA3 also introduces a 192-bit cryptographic security suite. This level of security provides consistent cryptography and eliminates the mixing and matching of security protocols that are defined in the 802.11 standards. This security suite is aligned with the recommendations from the Commercial National Security Algorithm (CNSA) Suite and is commonly used in high-security Wi-Fi networks in government, defense, Finance, and industrial verticals. • **User Pre-shared keys** The U-PSK (User-PSK) Authentication settings are only used in conjunction with XMS Cloud's EasyPass Onboarding Portals. The Cloud automatically configures this setting for an WLAN when you create an Onboarding portal and you assign that WLAN to the portal. Thus, you should not normally change this setting manually. Note that the User- PSK settings are only available on the WLAN profile.		
Band	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: • 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
Client Isolation	Enable this feature when there is a need for restriction of wireless station-to-station communication across the network or on an AP. **Note** • 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		

Parameters	Description	Range	Default
	must restart the AP for the AP to learn the new gateway MAC address and to make sure the client isolation functions correctly. The following options are available to configure based on requirement: • **Disable** This option when selected disables the client isolation feature. that is, any wireless station can communicate to other wireless stations. • **Local** This options when selected enable the client isolation feature. This option prevents wireless station communications connected to the same AP. • **Network Wide** This options when selected enable the client isolation feature. It prevents wireless stations communications connected to different AP deployed in the same L2 network. **Note** • 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. • **Network Wide Static** 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. **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.		
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

Parameters	Description	Range	Default
Session Timeout	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. **Note** Following priority takes precedence for the session timeout: a. Configured from the RADIUS server b. Configured from the AP	60-604800	28800
Inactivity Timeout	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. **Note** Following priority takes precedence for the inactivity timeout: a. Configured from the RADIUS server b. Configured from the AP	60-28800	1800

Table 77 *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 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	–	Disabled

<table>
<tr><th>Parameters</th><th>Description</th><th>Range</th><th>Default</th></tr>
<tr><td></td><td>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.</td><td></td><td></td></tr>
<tr><td>Max Clients</td><td>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.</td><td>1-512 (Refer)</td><td>256</td></tr>
<tr><td>UAPSD</td><td>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="8">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></td><td>–</td><td>Disabled</td></tr>
<tr><td>QBSS</td><td>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.</td><td>–</td><td>Disabled</td></tr>
<tr><td>DTIM interval</td><td>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.</td><td>1-255</td><td>1</td></tr>
<tr><td colspan="4">Monitored Host</td></tr>
<tr><td>Host</td><td>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.</td><td>-</td><td>Disabled</td></tr>
<tr><td>Interval</td><td>The frequency of monitoring the network health based on the status of the keep-alive mechanism w.r.t configured monitored host.</td><td>60-3600 sec</td><td>300</td></tr>
<tr><td>Attempts</td><td>The number of packets in the keep-alive mechanism to determine the status.</td><td>1-20</td><td>1</td></tr>
<tr><td>DNS Logging Host</td><td>By enabling this feature, the Administrator can monitor the websites accessed by wireless stations connected to WLAN profile.</td><td>–</td><td>Disabled</td></tr>
<tr><td>Connection Logging Host</td><td>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.</td><td>–</td><td>Disabled</td></tr>
</table>

Parameters	Description	Range	Default
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. • 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: **Note** The total Option 82 field length must be less than 128 characters. • Hostname • AP MAC • BSSID • SSID • VLAN ID • SITEID • Custom • All **Note** In case DHCP Option 82 is configured at the device-, WLAN profile-, and L3 interface-levels, the following priority order is considered: 1. Device-level configuration 2. WLAN profile-level configuration 3. L3 interface-level configuration	–	Disabled
Tunnel Mode	This option is enabled when user traffic is tunneled to the DMZ	–	Disabled

Parameters	Description	Range	Default
	network either using L2TP or L2GRE.		
Fast-Roaming Protocol	One of the important aspects to support voice applications on a Wi-Fi network (apart from QoS) is how quickly a client can move its connection from one AP to another. This should be less than 150 ms to avoid any call drop. This is easily achievable when the WPA2-PSK security mechanism is in use. However, in enterprise environments, there is a need for more robust security (the one provided by WPA2-Enterprise). With WPA2-Enterprise, the client exchanges multiple frames with the AAA server, and hence depending on the location of the AAA server the roaming time will be above 700 ms. Select any one of the following: • **OKC** 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. • **802.11r** 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.	–	Disabled
RRM (802.11k)	AP sends the SSID name of the neighbor APs (SSID configured on multiple APs) to 802.11k clients. The following parameter must be enabled: • **Enable RRM** • Support for WPA2 authentication method	–	Disabled
802.11v	Provision to enable 802.11v BSS Transition Management.	–	Disabled
PMF (802.11w)	802.11w also termed as Protected Management Frames (PMF) Service, defines encryption for management frames. Unencrypted management frames make wireless connection vulnerable to DoS attacks as well as they cannot protect important information exchanged using management frames from eavesdroppers.	–	Optional
SA Query Retry Time	The legitimate 802.11w client must respond with a Security Association (SA) Query Response frame within a pre-defined amount of time (milliseconds) called the SA Query Retry time.	100-500	100ms

Parameters	Description	Range	Default
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**.

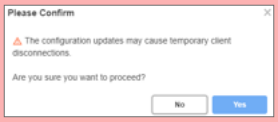
Note

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 289 *Warning when modifying WLAN*



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**.

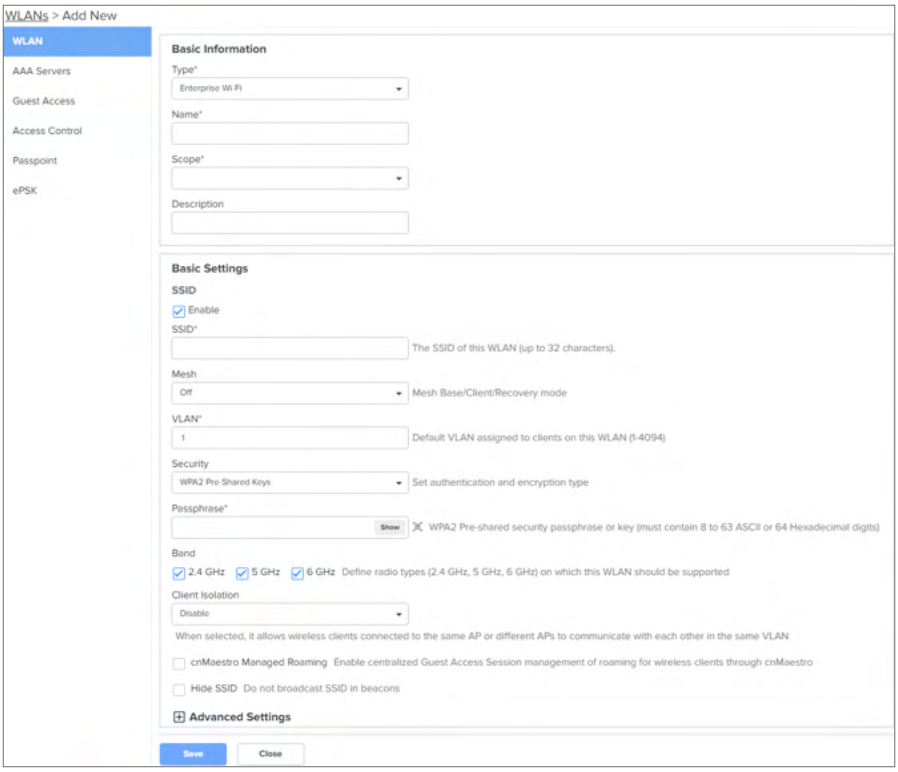
As with AP Groups, WLANs are separated into cnPilot Home (R-Series), Enterprise Wi-Fi types. You can configure WLAN, RADIUS, Guest Access, Usage Limits, Scheduled Access, and Access parameters with Enterprise Wi-Fi WLANs. With the cnPilot Home WLANs, you can configure SSID, Scheduled Access, and Access parameters.

Note

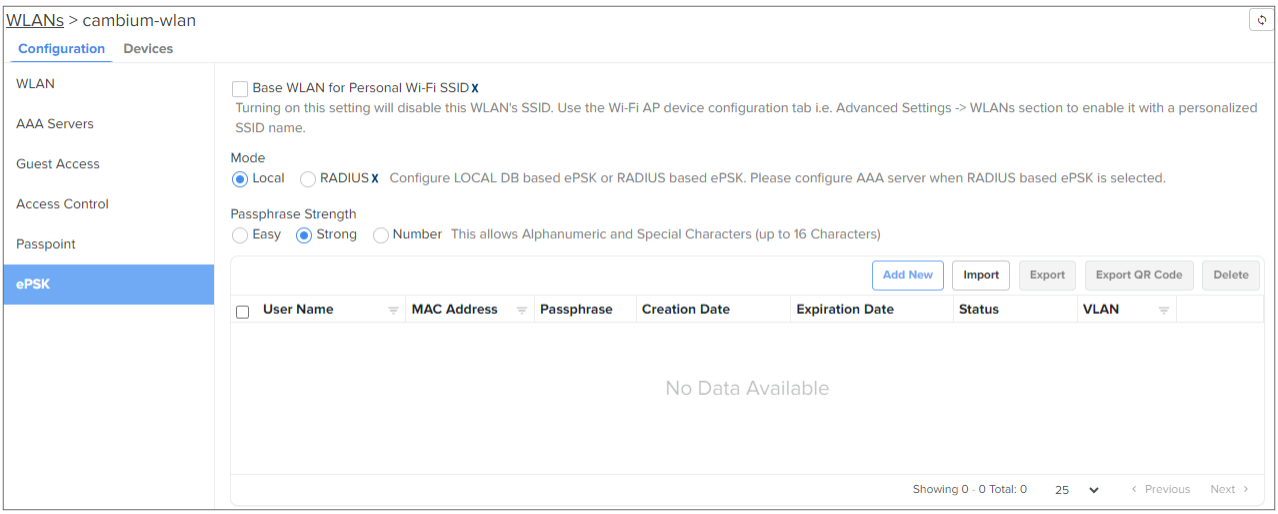
- The special characters can be used to create AP Group and WLAN names (Eg: a-zA-Z_-*&%#@!<>.() []^~`$1234567890). The user can also rename them if required.
- cnMaestro X users are allowed to create 2000 ePSKs per WLAN.
- By default, password will not be configured. User has to configure the password 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.



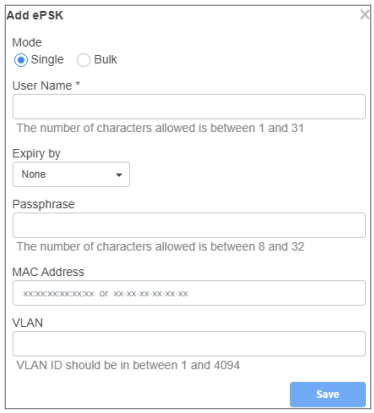
5. Click **Save**.
6. In the **ePSK** page select the type of passphrase strength in the **Passphrase Strength** field (Available options: **Easy**, **Strong**, or **Number**).



7. Click **Add New**.

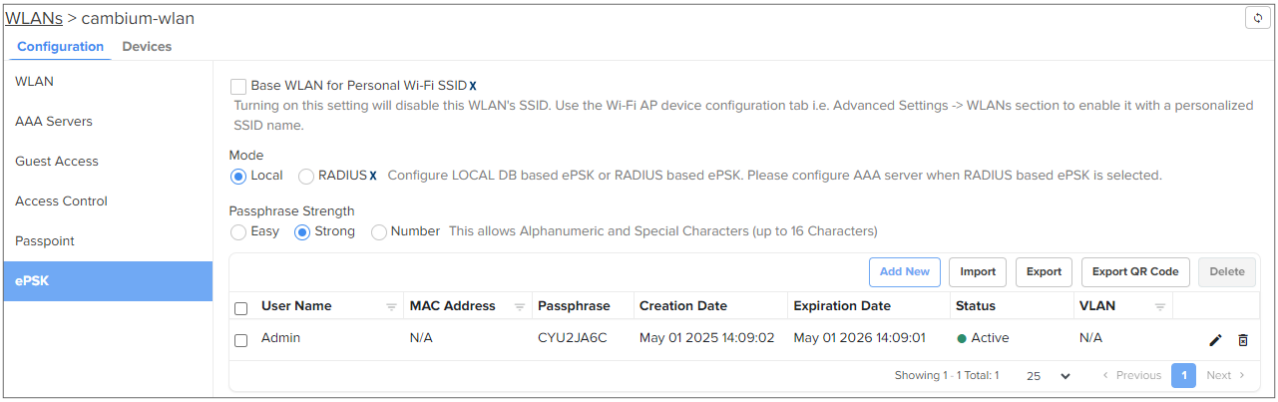
   The **Add ePSK** window is displayed.

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.



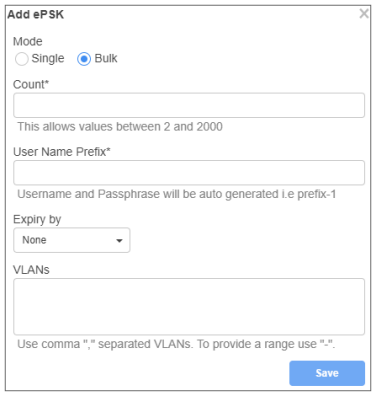
Note

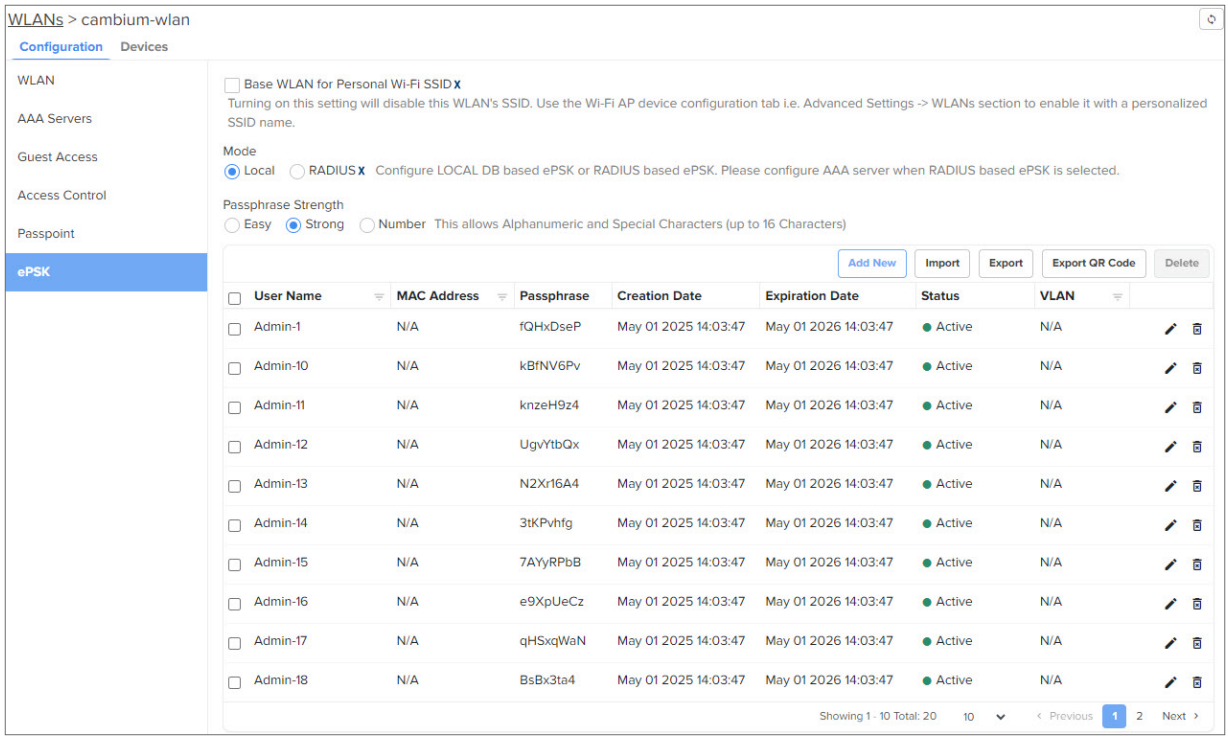
Passphrase is optional and unless manually configured, it will be automatically generated based on the selected **Passphrase Strength**.



- 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.





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 290 *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.

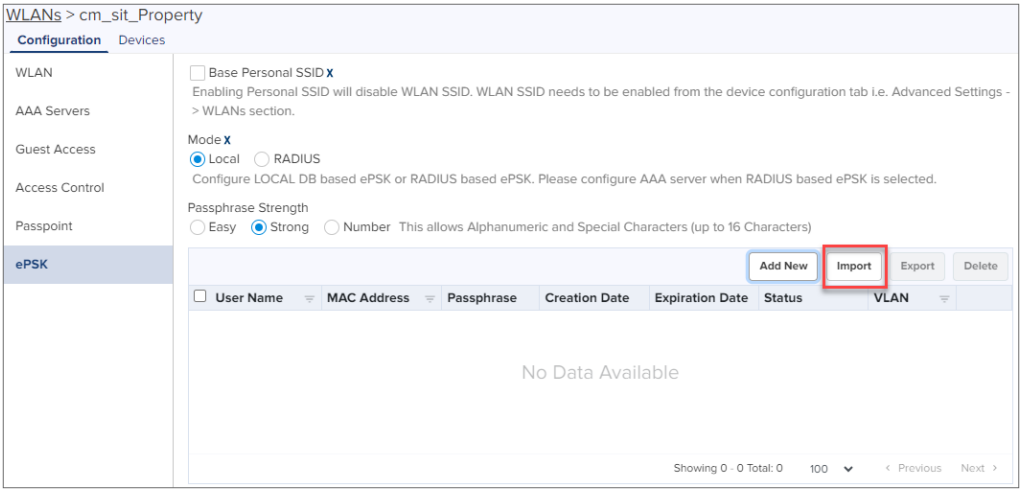
To configure personal Wi-Fi on the AP, complete the following steps:

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.

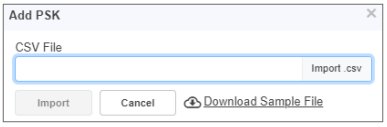
By default, this feature is disabled. Once enabled, the **Enable** checkbox (under **WLANs > WLAN > Basic Settings > SSID**) is cleared. Also, the local and RADIUS ePSKs are disabled.

Import ePSK

1. Click **Import**.

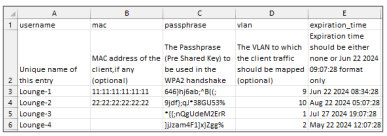


2. Select **Import.csv** file.



Alternatively, one can import a CSV file containing a list of ePSK entries. A sample file format is available from the Import dialog.

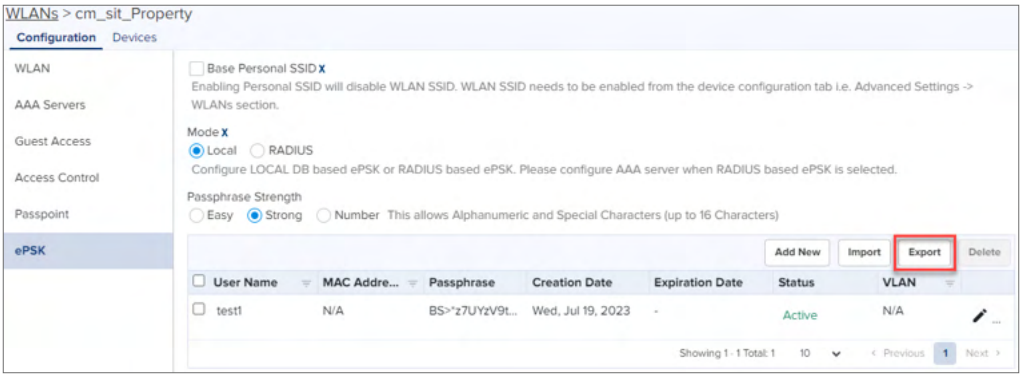
3. Click **Download Sample File**, to view sample ePSK Excel sheet.

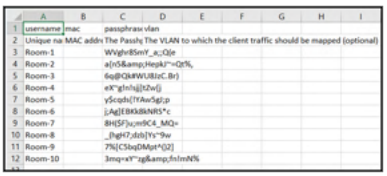


	A	B	C	D	E
1	username	mac	passphrase	vlan	expiration_time
2	Unique name of this entry	MAC address of the client,if any (optional)	The Passhprase (Pre Shared Key) to be used in the WPA2 handshake	The VLAN to which the client traffic should be mapped (optional)	Expiration time should be either none or Jun 22 2024 09:07:28 format only
3	Lounge-1	11:11:11:11:11:11	646)hj6ab;*B((;	9	Jun 22 2024 08:34:28
4	Lounge-2	22:22:22:22:22:22	9jdf);qj*38GU53%	10	Aug 22 2024 05:07:28
5	Lounge-3		*(;rzQg)JdeM2Er9	1	Jul 27 2024 19:07:28
6	Lounge-4		)j)zam4F1)xjZgg%	2	May 22 2024 12:07:28

Exporting ePSK

1. Click **Export**.
2. Select **export.csv** file.





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.

Configuring Wi-Fi offloading and Passpoint

Wi-Fi offloading helps mobile network operators to reduce congestion on cellular networks by shifting data traffic to Wi-Fi networks whenever possible.

Cambium Networks supports the following Wi-Fi offloading vendors:

- Custom
- Google Orion
- Helium
- WayFi
- WBA OpenRoaming Demo
- XNET

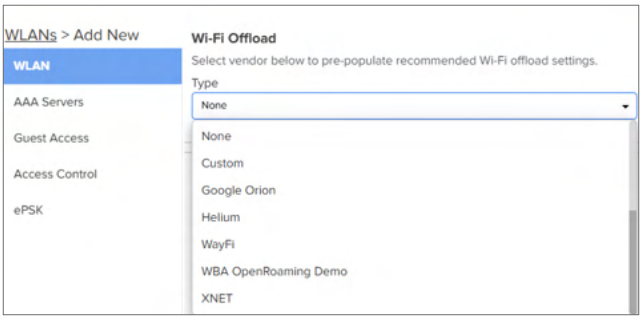
In addition to the above vendors, Cambium also supports custom Wi-Fi offloading configuration.

To configure Wi-Fi offloading, complete the following steps:

1. Select an appropriate vendor in the **WLANs** > **Wi-Fi Offloading** section.
2. Configure the required VLAN in the **WLANs** > **Basic Settings** section.
3. Configure the RADIUS security proxy details in the **WLANs** > **AAA Servers** section.
4. Modify the default Passpoint parameter values that are populated for the vendors in the **WLANs** > **Passpoint** section.

   For information on Passpoint parameters, refer to Configuring Passpoint parameters.

   Figure 291 *WLANS > Wi-Fi Offloading*

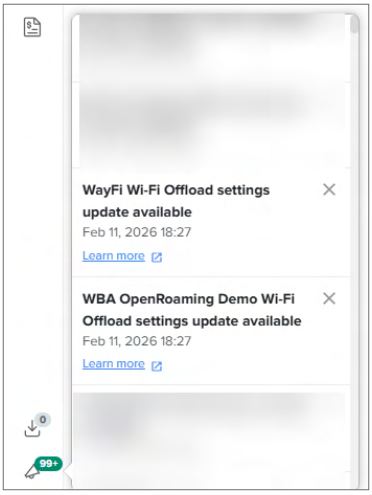


5. When a vendor updates the configuration, then cnMaestro displays notifications in the following locations:

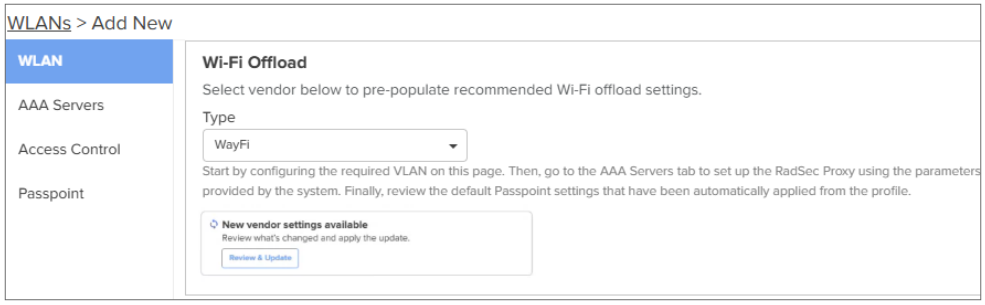
   Note

   Notifications will only appear if that particular vendor configurations is configured for that account.

   - Notifications window

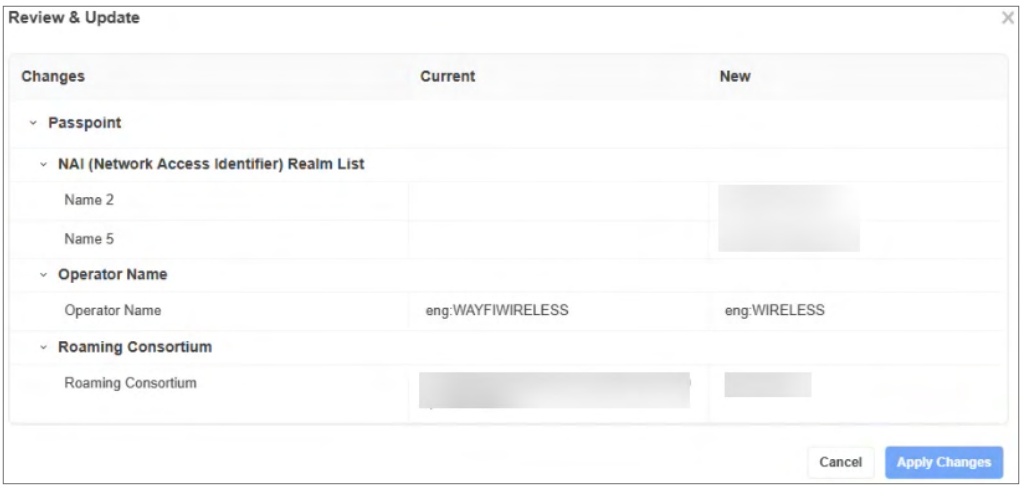


- **WLANs** page



6. To update the Passpoint configuration, on the **WLANs** > **WLAN** > **Wi-Fi Offload** page, click **Review & Update**.

   The Review & Update page is displayed with a list of all modified values between the existing and the new parameters.



7. If the updated configuration is okay, click **Apply Changes**.
8. To acknowledge the notification in the Notifications window, click the clear (✕) icon.

Configuring Passpoint parameters

Below table lists configurable fields that are displayed in the **Configuration** > **Wi-Fi Profiles** > **WLANs** > **Passpoint** tab.

> **Note**
>
> The **Passpoint** tab is available only when you select a Wi-Fi offloading vendor in the **Wi-Fi Offloading** section.

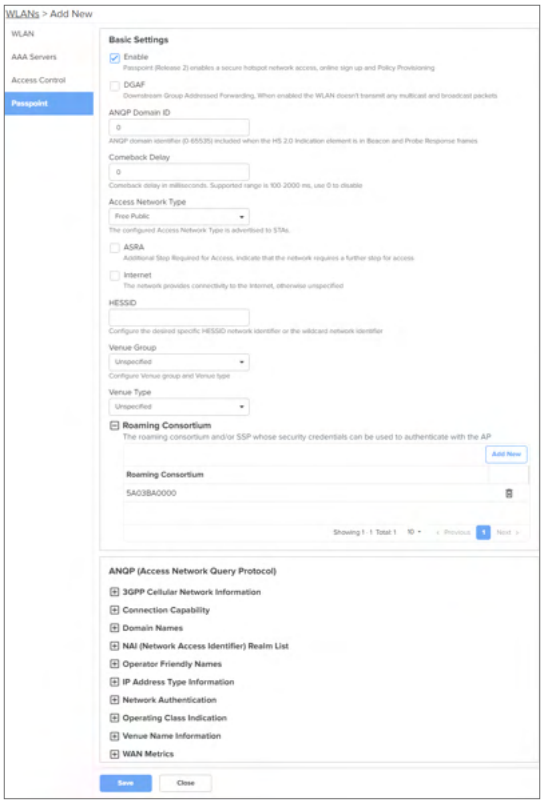
Table 78 *Passpoint parameters*

Parameters	Description	Range	Default
Configuration > Hotspot 2.0 / Passpoint parameters			
Enable	Passpoint (Release 2) enables secure hotspot network access, online sign up, and policy provisioning.	–	Disabled
DGAF	Downstream Group Addressed Forwarding when enabled the WLAN does not transmit any multicast and broadcast packets.	–	Disabled
ANQP Domain ID	ANQP domain identifier is included when the HS 2.0 indication element is in Beacon and Probe Response frames.	0-65535	0

Parameters	Description	Range	Default
Comeback Delay	Comeback delay in milliseconds.	100-2000	0 (Disabled)
Access Network Type	The configured Access Network Type is advertised to STAs. The following are the supported access network types: • Chargeable Public • Emergency Services • Free Public • Personal Device • Private • Private with Guest • Test • Wildcard	–	Private
ASRA	This indicates that the network requires a further step for access.	–	Disabled
Internet	The network provides connectivity to the Internet if not specified.	–	Disabled
HESSID	Configures the desired Homogenous Extended Service Set Identifier (HESSID) or the wildcard network identifier.	–	–
Venue Group	Select the group to which the venue may belong from the dropdown list. You can also select the corresponding venue type from the **Venue Type** dropdown list. The following are the supported venue groups: • Unspecified • Assembly • Business • Education • Factory and Industrial • Institutional • Mercantile • Residential • Storage • Utilities and Miscellaneous • Vehicular • Outdoor	–	–
Venue Type	Based on the venue group you select, select the corresponding venue type from the dropdown list.		
Roaming Consortium	The roaming consortium and/or SSP whose security credentials can be used to authenticate with the AP.	–	–
ANQP	Expand any of the following Access Network Query Protocols (ANQP) and	–	–

Parameters	Description	Range	Default
Elements	configure the corresponding parameters: • 3GPP Cellular Network Information • Connection Capability • Domain Names • NAI (Network Access Identifier) Realm List • Operator Friendly Names • IP Address Type Information • Network Authentication • Operating Class Indication • Venue Name Information • WAN Metrics		

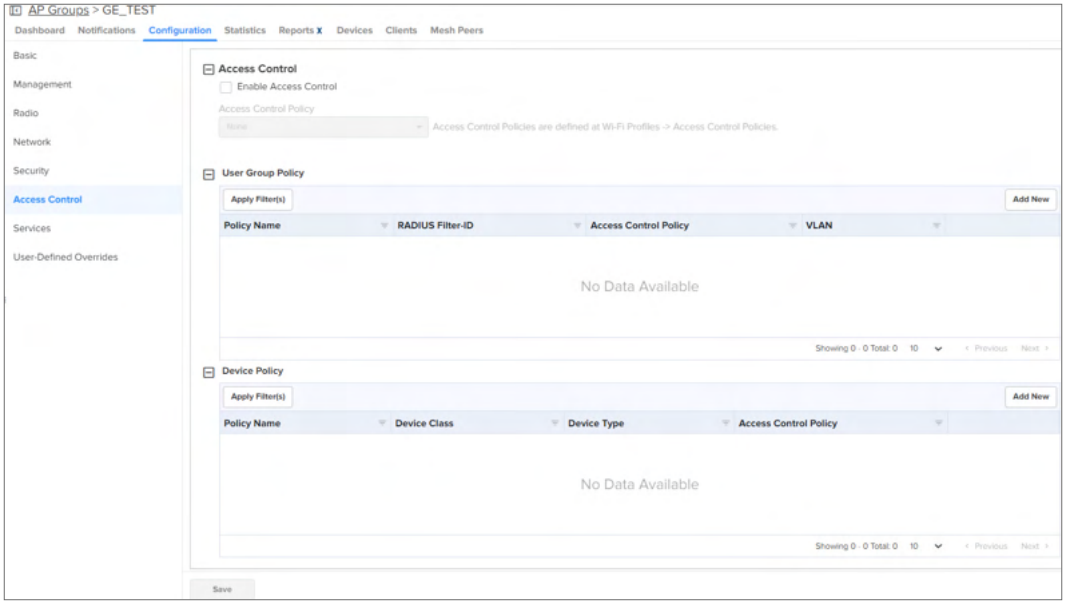
Figure 292 *Passpoint parameters*



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 293 *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 294.

Figure 294 *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 294. This provides a comprehensive view of the policies and rules within the network.

User Group Policy

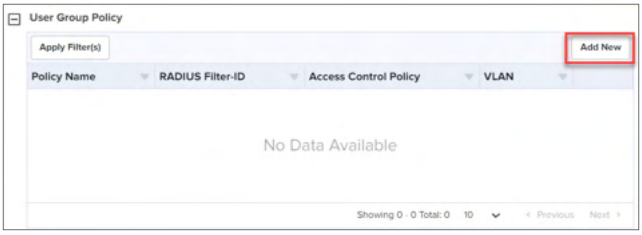
User Group Policy enables users to categorize into specific roles with customized access permissions and restrictions, facilitating fine-tuned control over network access.

Adding a new User Group Policy

To add a new User Group Policy, perform the following steps:

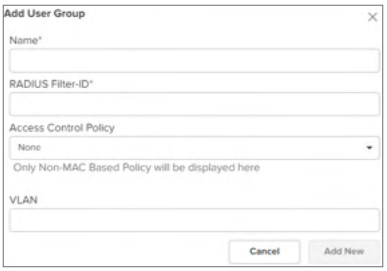
1. Navigate to **Configuration** > **Access Control** page.
2. Click **Add New** in the top right corner of the User Group Policy as shown in Figure 295.

Figure 295 *User Group Policy*



3. Complete the details in the **Add User Group** pop-up window as shown in Figure 296.

Figure 296 *Add User Group*



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

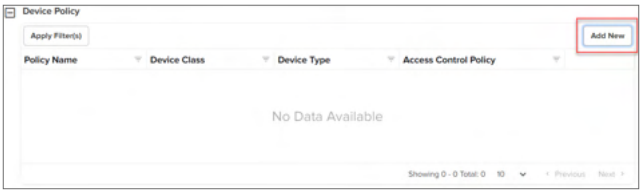
Device Policy allows users to apply specific rules and access control policies based on the type and characteristics of devices, offering customized control over device behavior within the network.

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 297.

Figure 297 *Device Policy*



3. Complete the details in the **Add Device Policy** pop-up window as shown in Figure 298.

Figure 298 *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.

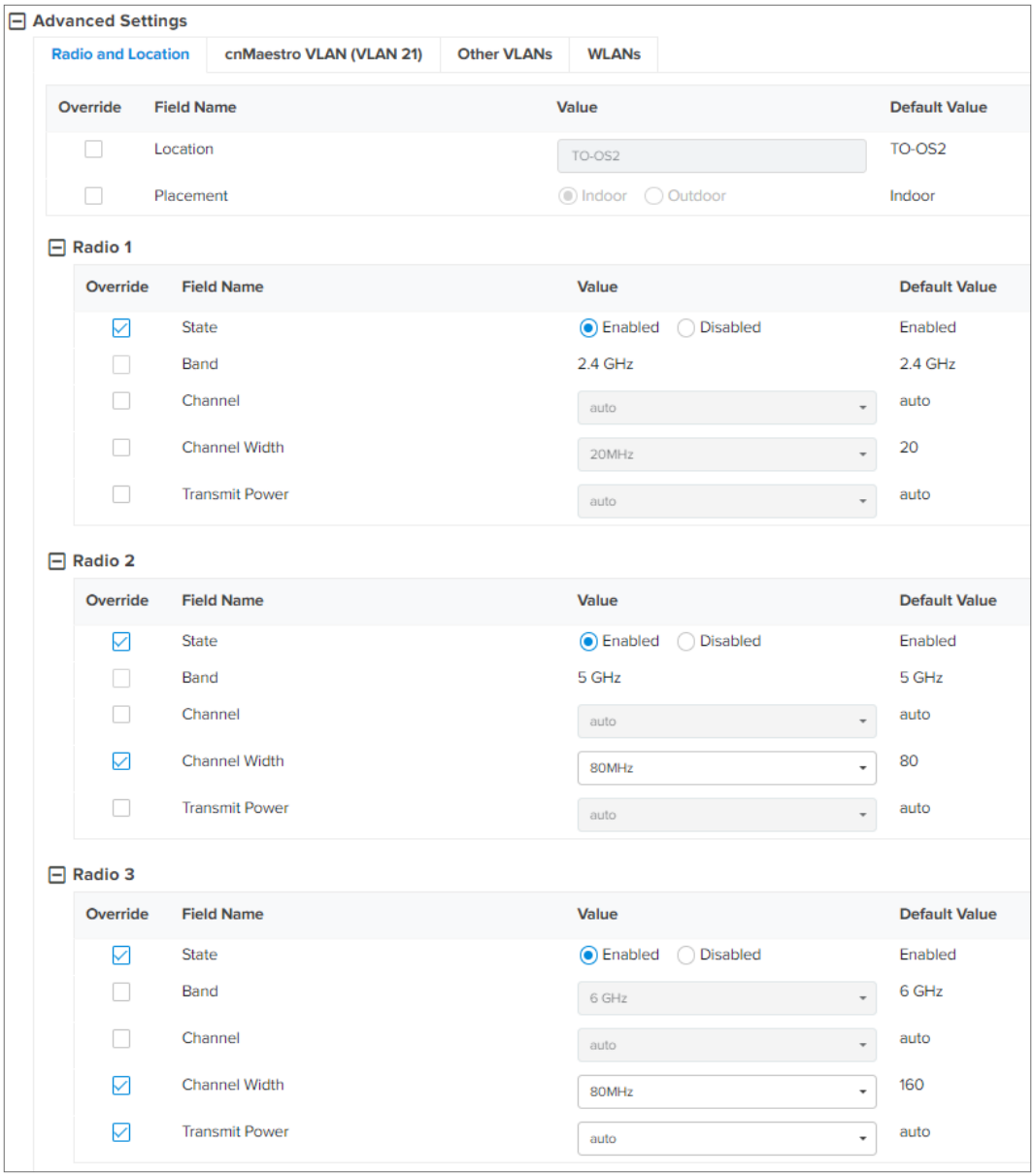
Pre-Defined Overrides

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 or Disabling SSID, Enabling or Disabling Radio 2.4 GHz and 5 GHz, and Passphrase. These items can be configured in the device **Configuration** tab.

Navigate to **Manage** > **Configuration** and select a device in the tree to update.

You can choose values from AP Group to be overridden. The icon to the left of a field must be selected to override that parameter. 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.

By default, Enterprise Wi-Fi devices will have **Auto-set** from device enabled. This option reads network related configuration fields from the device and uses them as override values. This protects the device from losing connectivity when the AP Group is first pushed.



User-Defined Overrides

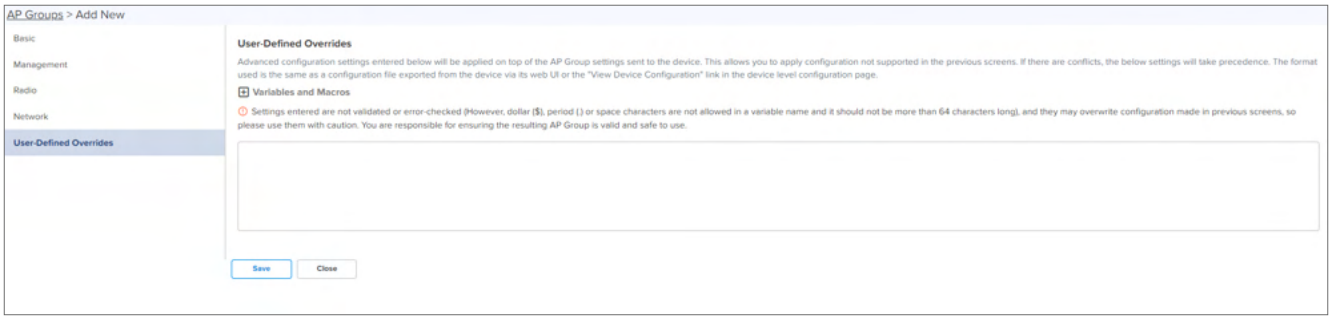
User-Defined Overrides can be entered into the end of an AP Group configuration. They will be appended to the AP Groups before the configuration is applied to the device. This allows setting configuration parameters which are not supported by GUI; this is an advanced operation that should rarely be used. 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 can 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 hypen (-).
- `%{esn-}` will be replaced with the MAC address of the device in lowercase separated by a hypen (-).

- `%{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.

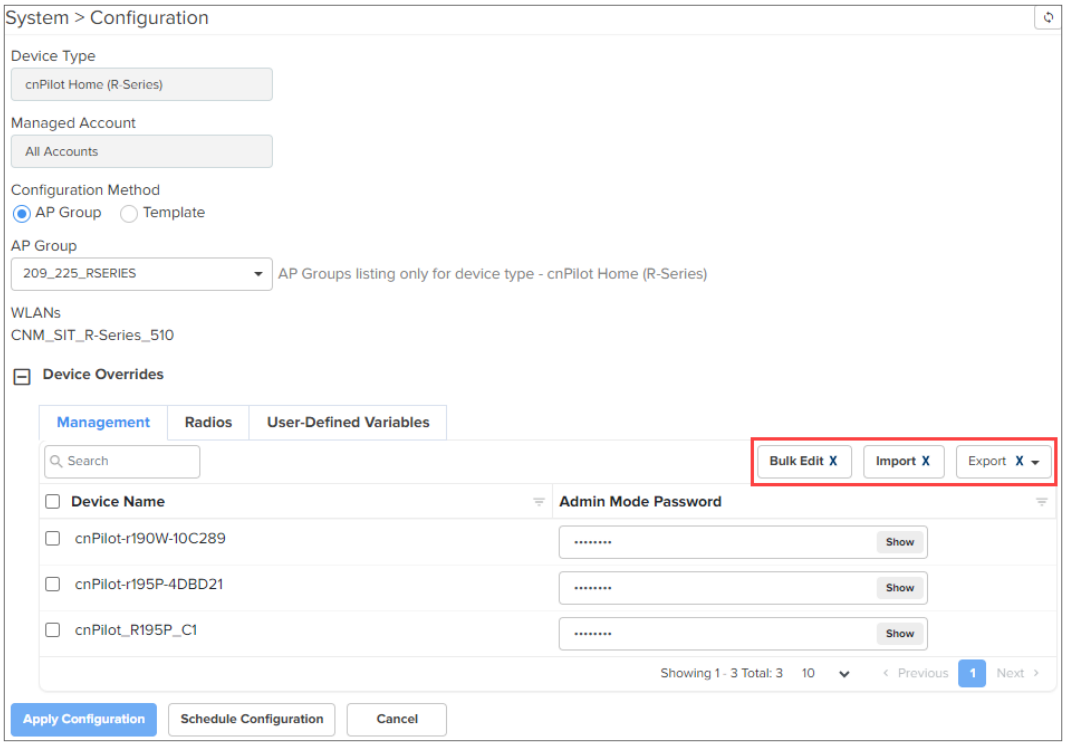
> **Note**
>
> **Bulk Edit** option under **Configuration** > **Devices Overrides** is supported only for cnMaestro X.

The user can override for the following configurations in cnPilot (R-Series):

- Management
- Radios
- User-Defined Variables

- Management
- Radios
- User-Defined Variables

Figure 299 *Bulk Override: cnPilot (R-Series)*

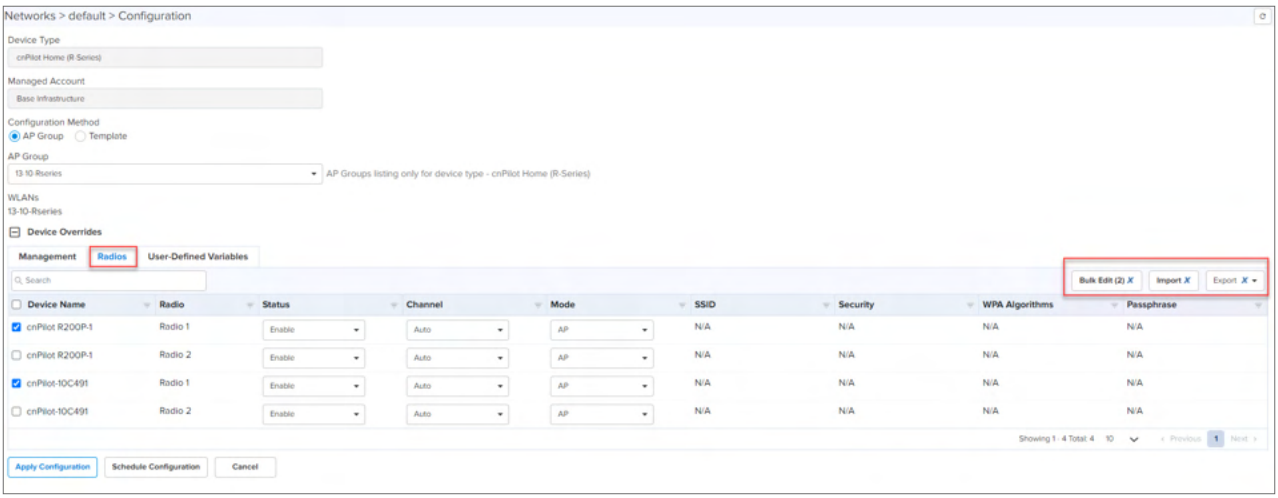


- Management
- Radios
- User-Defined Variables

Management

Radios

1. In **Radio** tab, select the radios from the device list.
2. Click **Bulk Edit**.

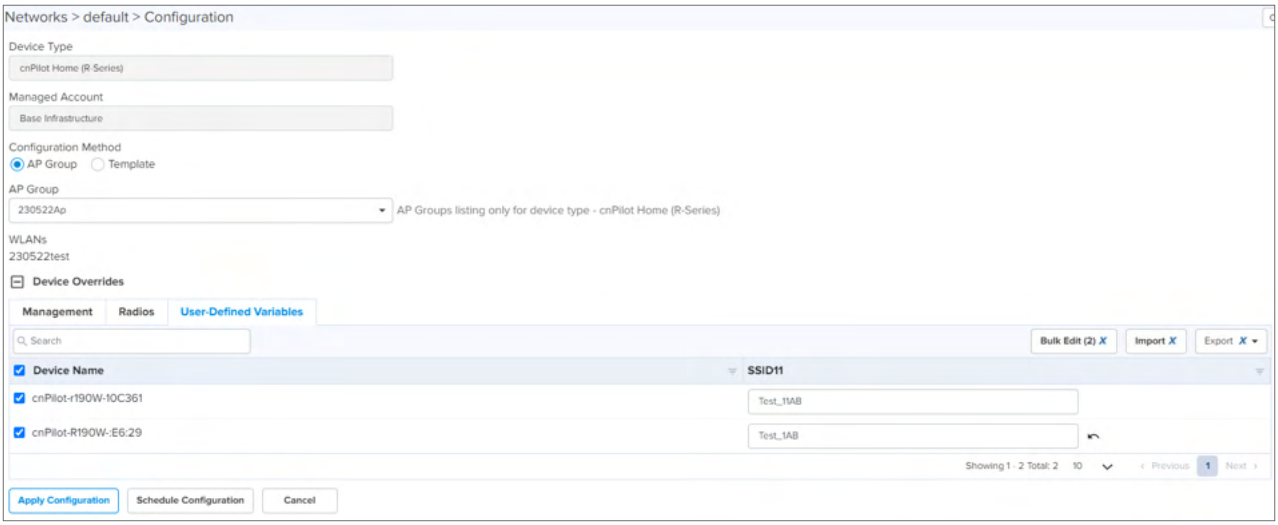


3. Export the report to edit the radio parameters. You can export the radio parameter details as described:
   - Export page as CSV
   - Export all as CSV

   After modifying the field values, the CSV file is imported.
4. Click **Import**, to import the file.
5. Select the file to import in CSV file format.
6. Click **Apply Configuration** to start immediately, or click **Schedule Configuration** to schedule later.

User-Defined Variables

1. In **User-Defined Variables** tab, select the devices from the list.



2. Click **Bulk Edit**.

   A pop-up window appears for the fields to reconfigure.

3. Click **Save**.

   You can export, as described:

   - Export page as CSV
   - Export all as CSV

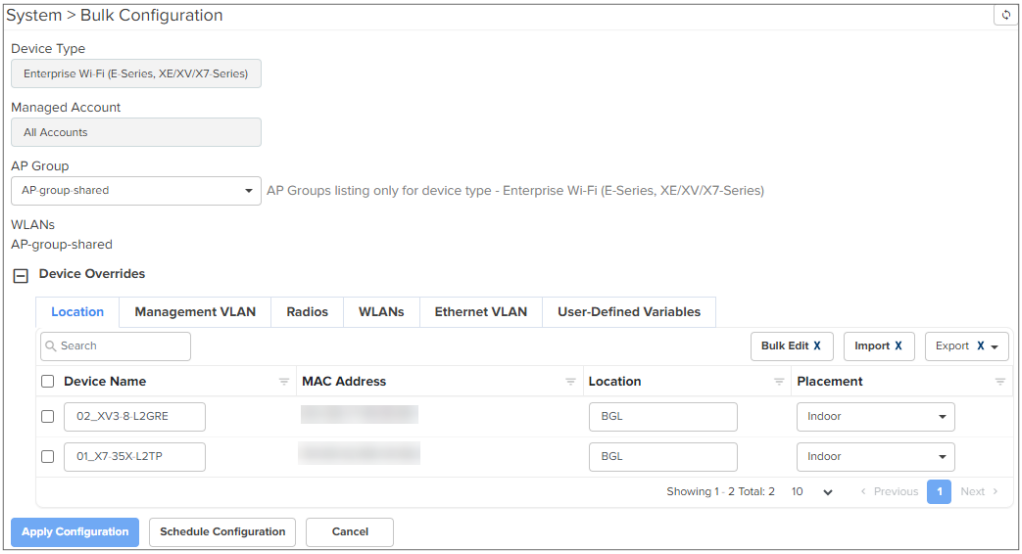
   After modifying the field values, the CSV file can be imported.

4. Click **Import**, to import the file.
5. Select the file to import in CSV file format.
6. Click **Apply Configuration** to start immediately, or click **Schedule Configuration** to schedule later.

The user can override the following configurations in Enterprise Wi-Fi (E-Series, XV-Series):

- Location
- Management VLAN
- Radios
- WLANs
- Ethernet VLAN
- User-Defined Variables

Figure 300 *Bulk Override: Enterprise Wi-Fi (E-Series, XE-Series, XV-Series)*



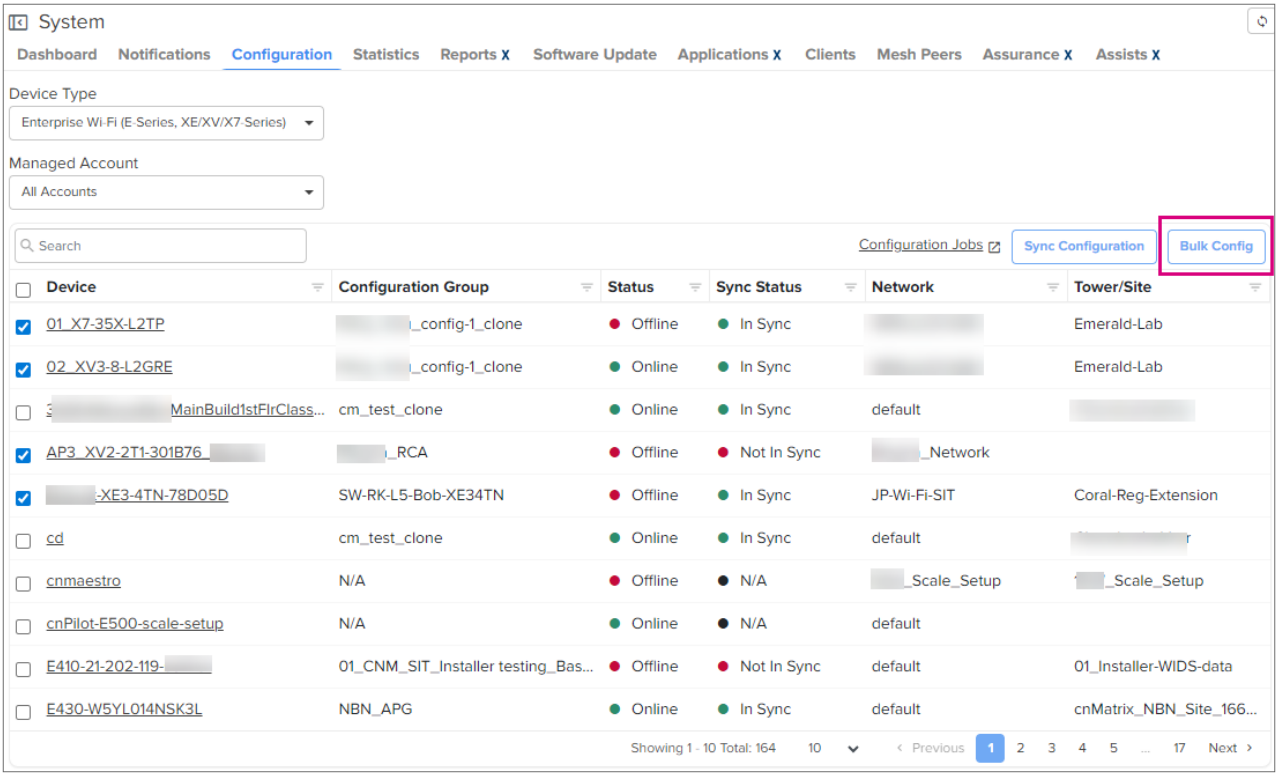
Note

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:

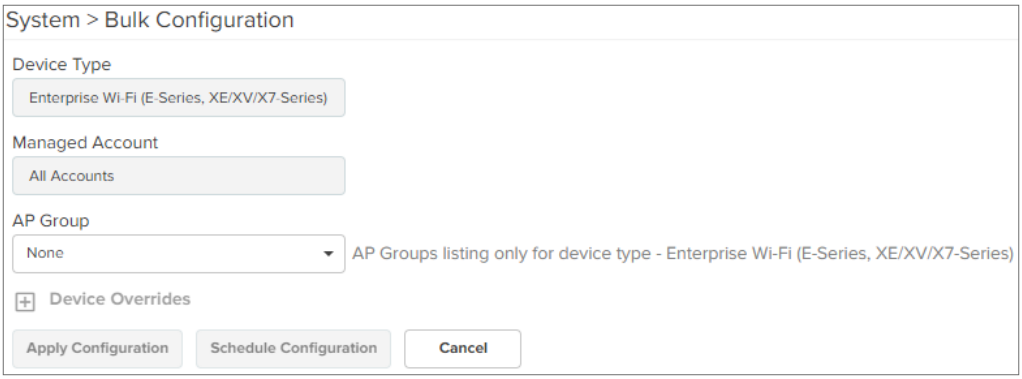
1. Navigate to **Monitor and Manage** > **System** > **Configuration.**
2. Select **Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)** from the **Device Type** from the dropdown.
3. Select the checkboxes corresponding to the devices you want to configure and click **Bulk Config**.

   To select all devices, select the checkbox next to the **Device** column name.

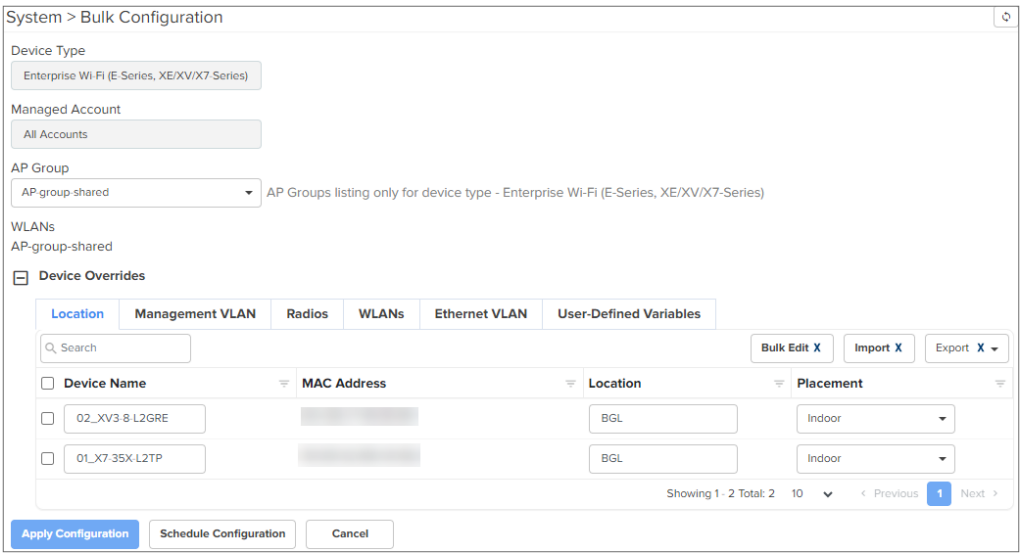


The **System** > **Bulk Configuration** page is displayed.

4. Select an appropriate AP group from the dropdown if **None** is selected by default.



5. Expand the **Device Overrides** section by clicking the plus (+) icon.

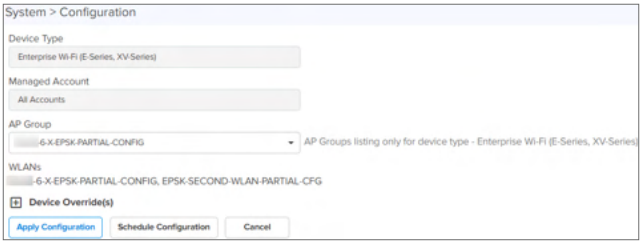


6. In the Device Overrides table, reconfigure tabs and perform the following actions:
   - Bulk Edit X
   - Export X
   - Import X
7. Select the devices from the table to configure overrides and click **Bulk Edit**.

   A pop-up window appears with tab-specific parameters to reconfigure.
8. Edit the fields and click **Save**.
9. To override the configuration using CSV files, you can use CSV files.

   To export the configuration details in that tab, select any of the following options:
   - Export page as CSV
   - Export all as CSV
10. After modifying the parameter values in the CSV file, you can import the CSV file to apply the configuration.
11. To import the file, click **Import**.
12. Select the CSV file to import.

13. Click **Apply**.



14. Click **Apply Configuration** to apply the configuration immediately, or click **Schedule Configuration** to schedule later.

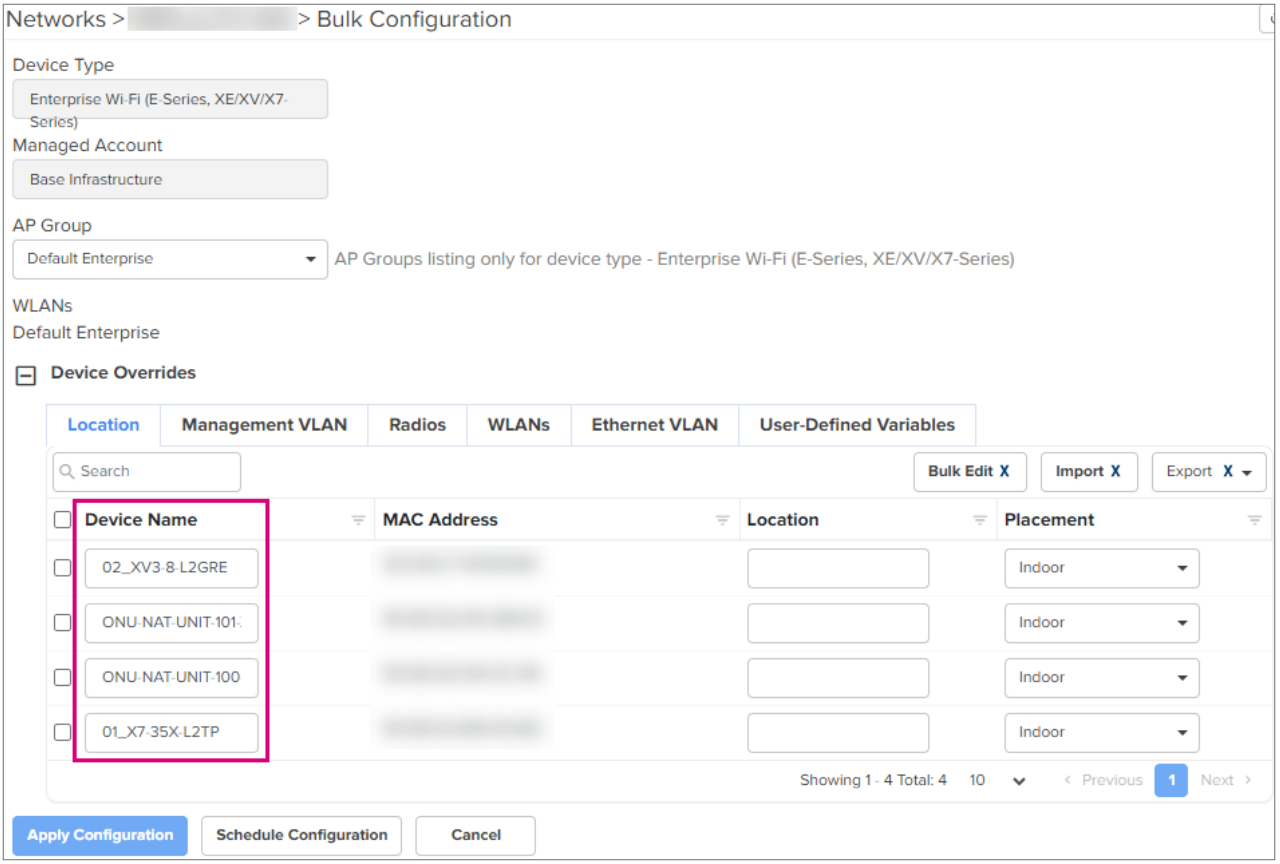
Location

In this tab, users are allowed to modify the location details and also rename the device names in bulk.

1. To update device names in bulk, edit the names in the respective fields under the **Device Name** column.

   You can also update the device names in bulk by exporting the details in the CSV file, modifying the names, and then uploading the updated CSV file.

2. To modify location details, select the devices from the list.
3. Click **Bulk Edit.**

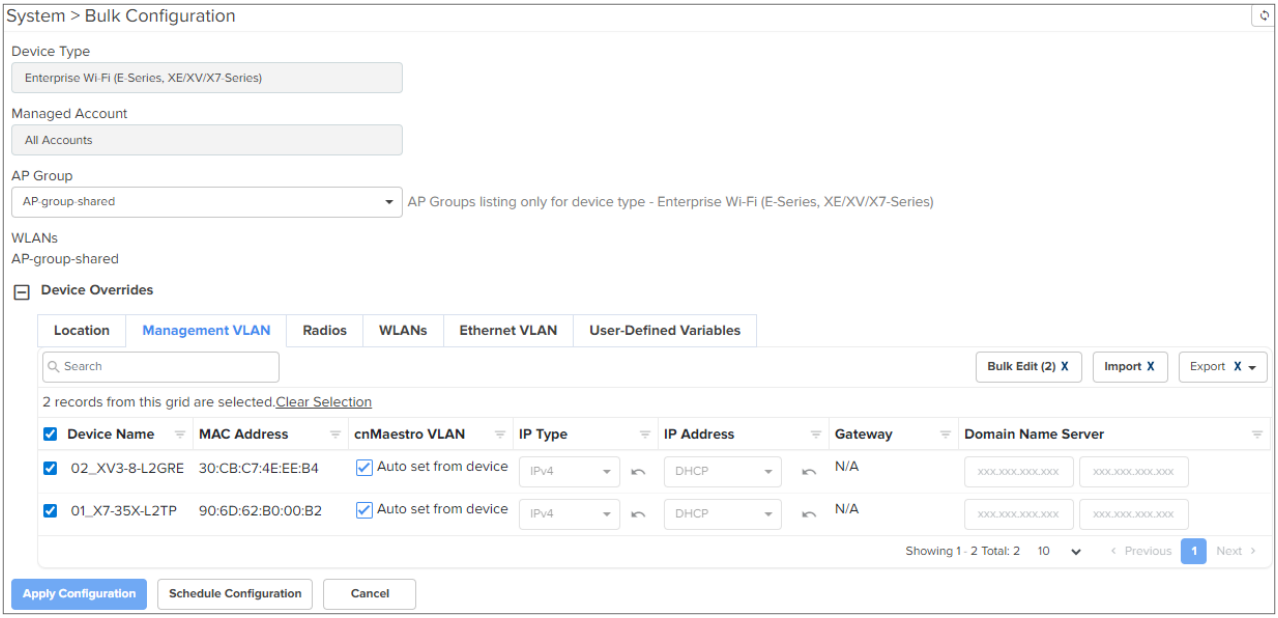


4. **Override Location** window appears, edit the configuration details and click **Save**.

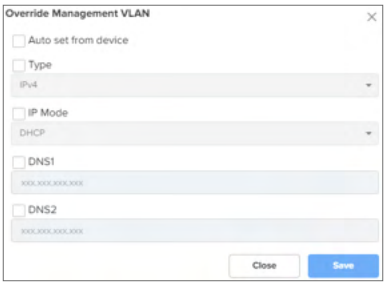
5. Click **Save**.

Management VLAN

1. In the **Management VLAN** tab, select the devices from the list and click **Bulk Edit**.



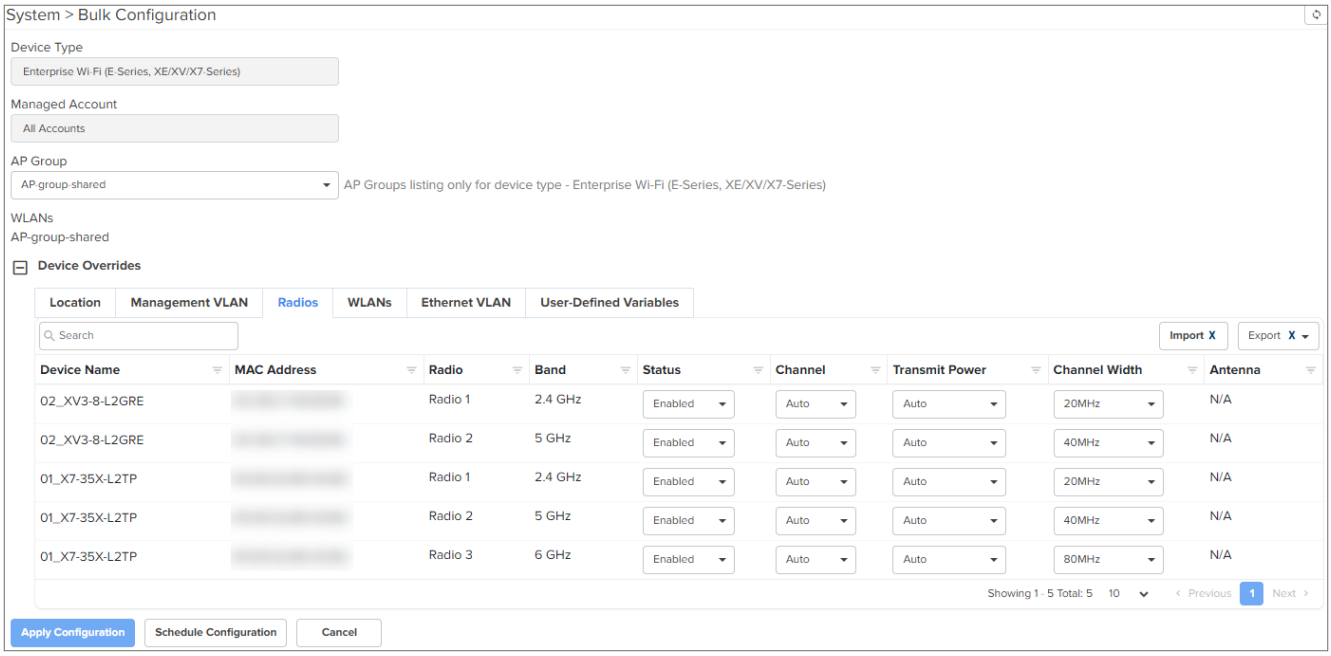
2. In the **Override Management VLAN** window appears.



3. Select the checkbox corresponding to the parameter you want to modify and configure the appropriate values.
4. Click **Save**.

Radios

In the **Radio** tab, select the radios from the device list, to perform **Import** and **Export** actions.

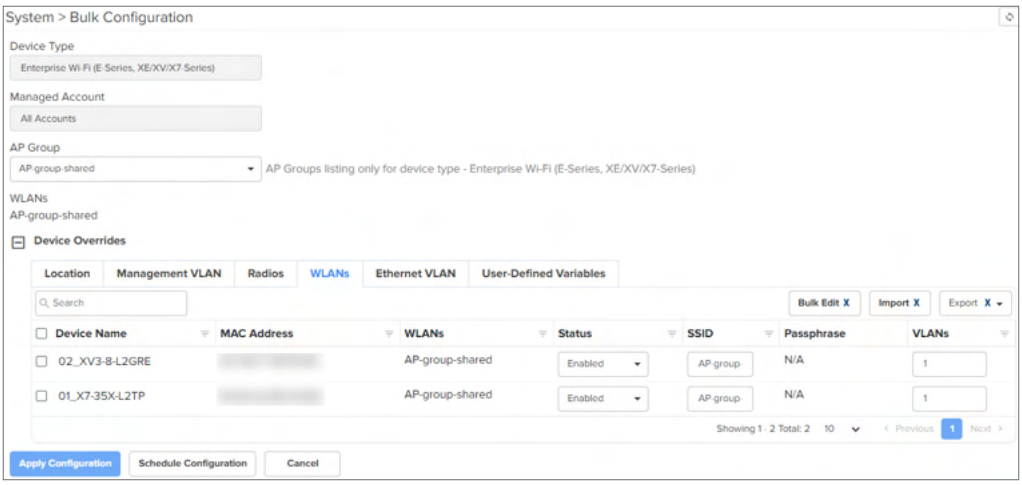


1. Export the report to edit the radio parameters. You can export the radio parameter details as described:
   - Export page as CSV
   - Export all as CSV

   After modifying the field values, the CSV file is imported.
2. Click **Import**, to import the file.
3. Select the file to import in CSV file format.
4. Click **Apply Configuration** to start immediately, or click **Schedule Configuration** to schedule later.

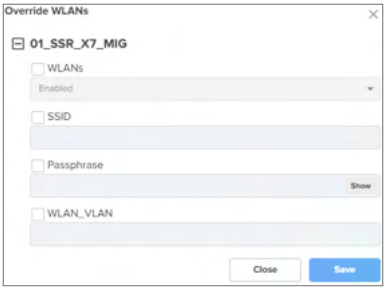
WLANs

1. In the **WLANs** tab, select the WLAN of the devices from the list.



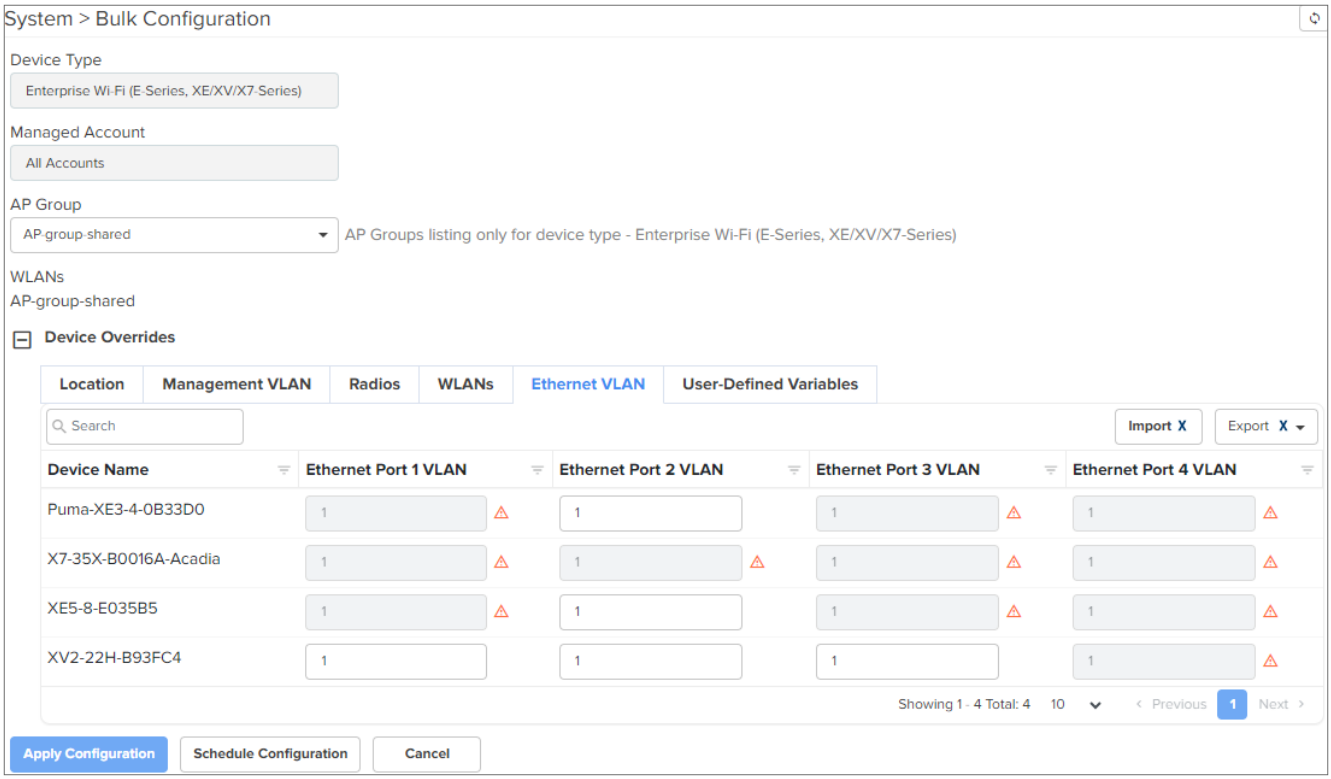
2. Click **Bulk Edit**.

3. **Override WLANs** window appears, edit the configuration details and click **Save**.



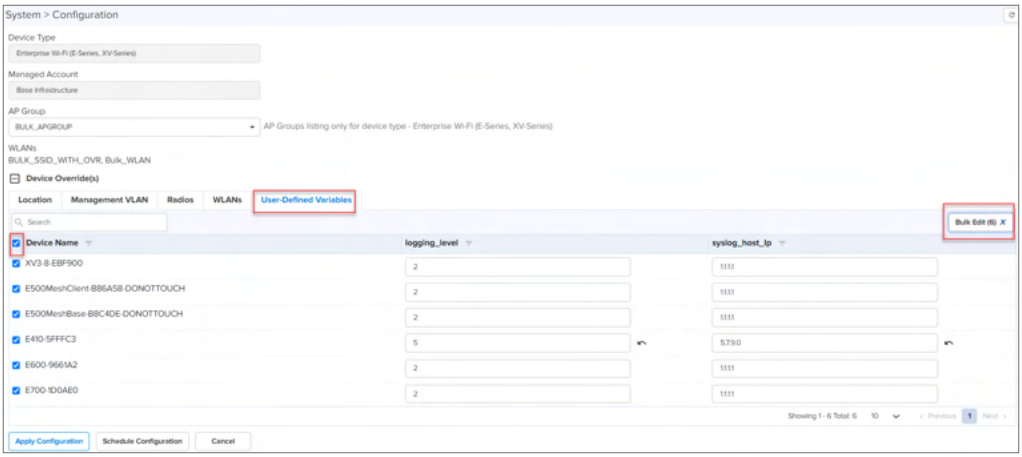
Ethernet VLAN

The **Ethernet VLAN** tab allows you to override VLAN assignments in the non-management Ethernet ports, on the devices where there are multiple Ethernet ports.



User-Defined Variables

1. In the **User-Defined Variables** tab, select the devices from the list.



2. Click **Bulk Edit**.

   The **Override User-Defined Variables** window appears.

3. Edit the configuration details and click **Save**.

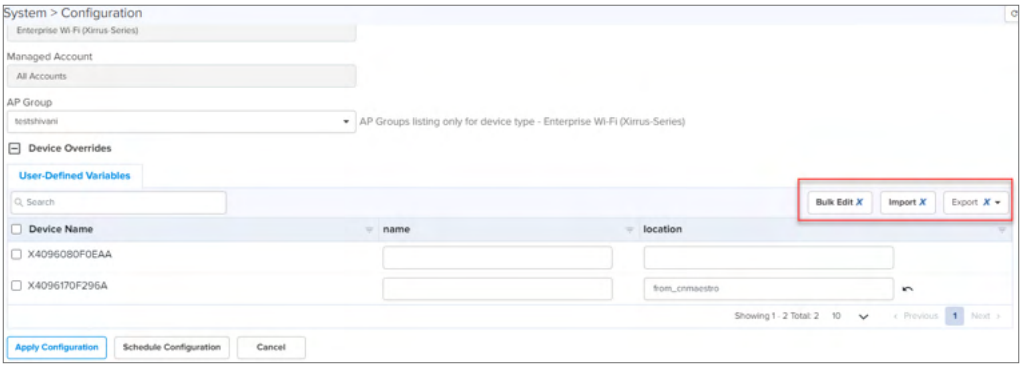
> **Note**
>
> For Bulk overrides to be enabled in **User-Defined Overrides** tab, you must define the overrides in the **User-Defined Overrides** section of AP groups. For more details, see User-Defined Overrides

4. Click **Apply Configuration** to start immediately, or click **Schedule Configuration** to schedule later.

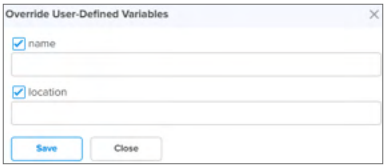
The user can override for the following configurations in Enterprises Wi-Fi (Xirrus-Series):

- User-Defined Variables

  Figure 301 *Bulk Override: Enterprises Wi-Fi (Xirrus-Series)*



5. In the **User-Defined Variables** tab, select the devices from the list.



6. Click **Bulk Edit**. The **Override User-Defined Variables** window appears, edit the configuration details and click **Save**.
7. 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 that are currently out of sync with a mapped Configuration Group.

The **Sync Configuration** page has the following fields:

- Device (Hostname)
- Device Type
- Status (Online/Offline)
- Managed Account
- Network (Network in which device is present)
- Site (Site under which device is present)
- Configuration Group
- Sync Status (Sync status will tell whether job is completed or failed)

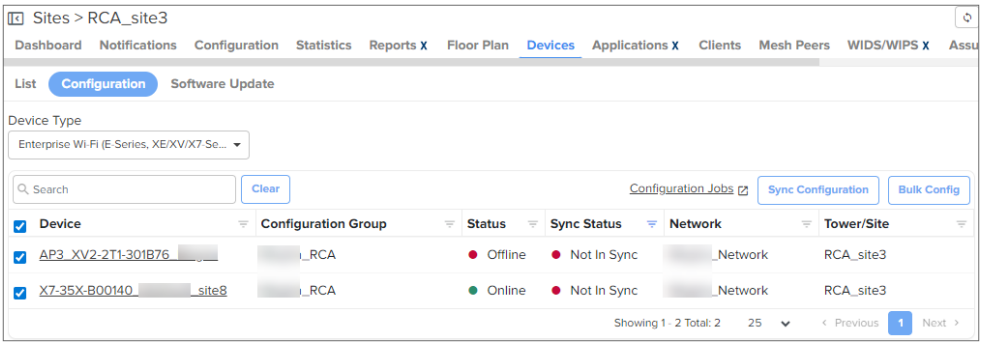
Steps to sync configuration

1. Navigate to one of the following pages:
   - **Configuration** > **Wi-Fi Profiles** > **AP Groups** tab or **WLANs** tab.

     The **Sync** option on these pages will lead to the **Administration** > **Sync Configuration** page.
   - **Monitor and Manage** > **Networks** tab > System-level or Network-level > **Configuration** tab.

At the Site-level, navigate to **Devices** > **Configuration**.

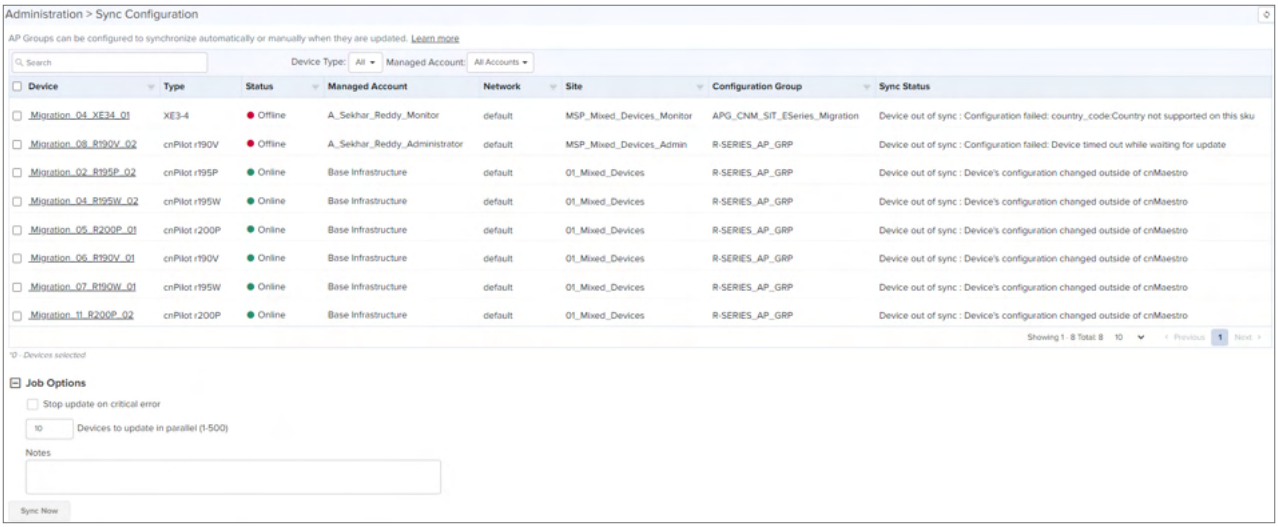
Figure 302 *Site-level out of sync devices*



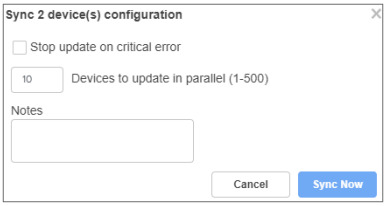
- **Administration** > **Sync Configuration**.

  Select **Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)** from the **Device Type** dropdown to list only Enterprise Wi-FI devices that are out of sync.

2. Select the devices for which you want to sync the configuration.
3. Click **Sync Configuration**.



4. At the System-, Network-, and Site-level, clicking **Sync Configuration** displays a confirmation window.



5. Click **Sync Now**.

   A configuration job is created and users can monitor the progress at **Administration** > **Jobs** > **Configuration Update** tab.

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

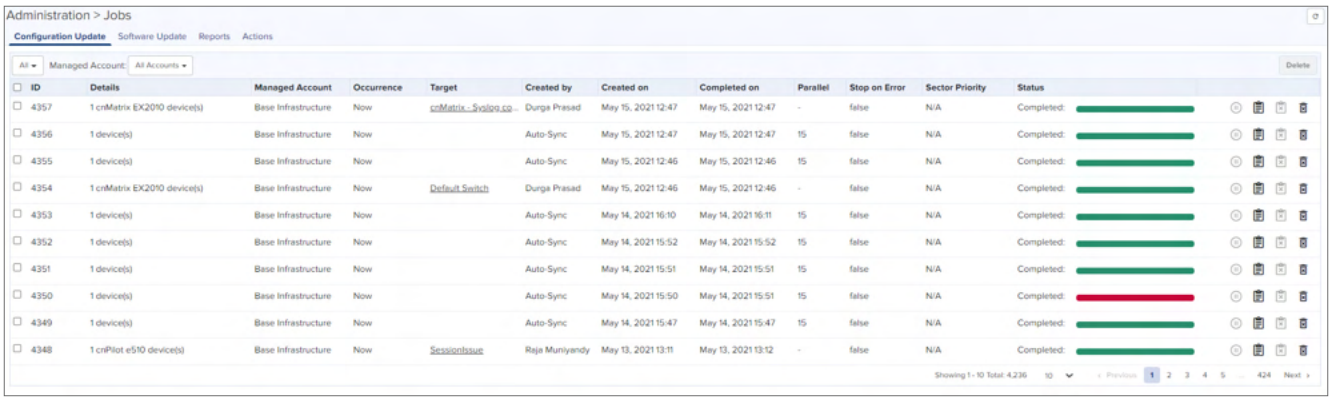
same device.

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.



Note

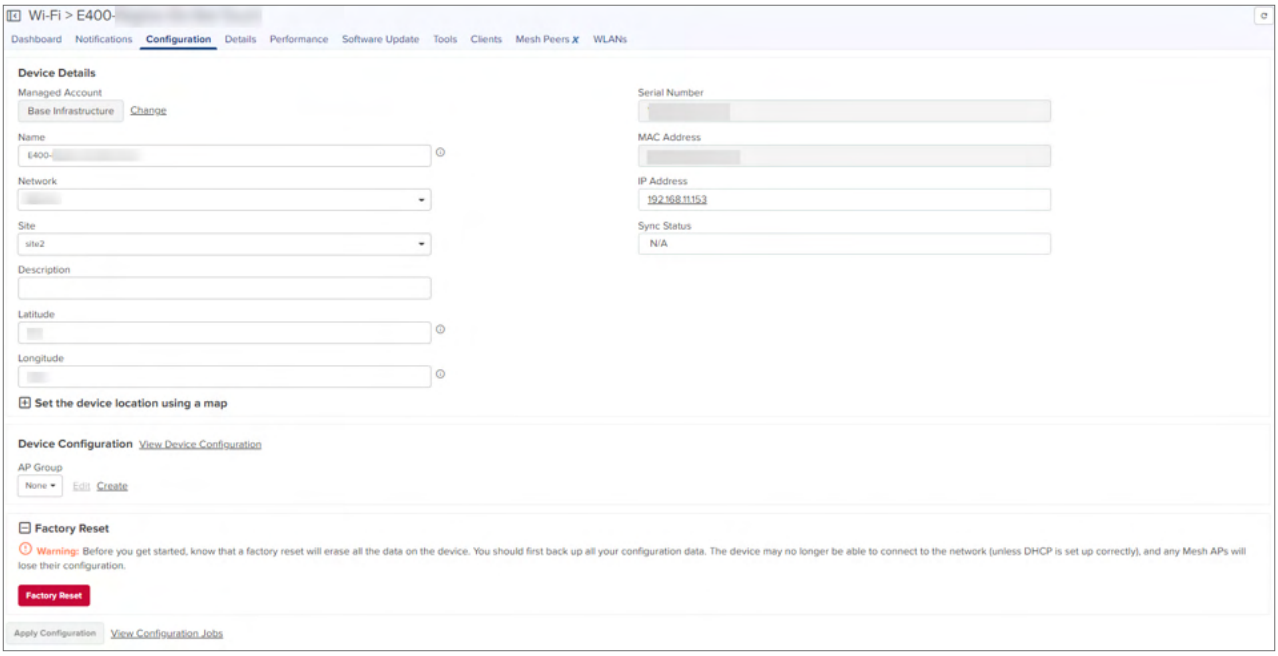
- Configuration jobs skip offline devices. With manual synchronization, they need to be synchronized by the administrator.
- For more information on Wi-Fi AP configuration, refer to the following URLs:
  - Unique per-Device values in Profiles Using User-Defined Overrides
  - AP Groups and Overrides for 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.

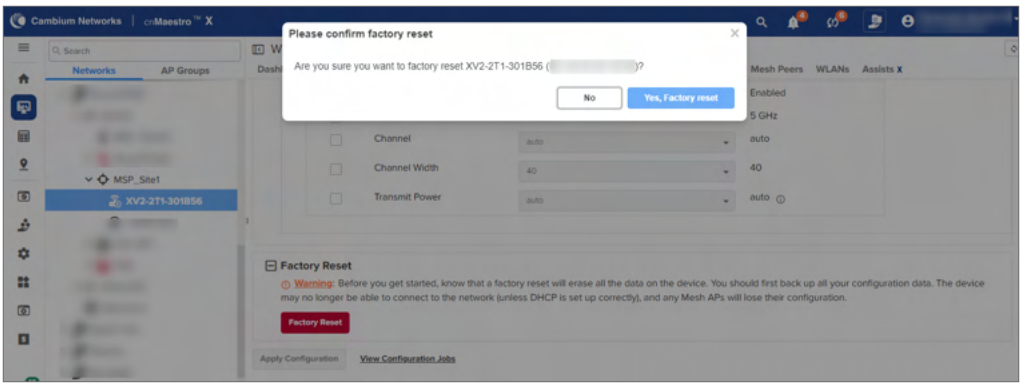
To factory reset the device perform as follows:

1. Navigate to the **Configuration** page of the device.
2. Select **Factory Reset.**

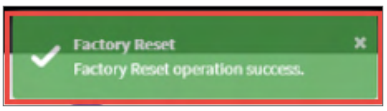


3. Click **Factory Reset**.

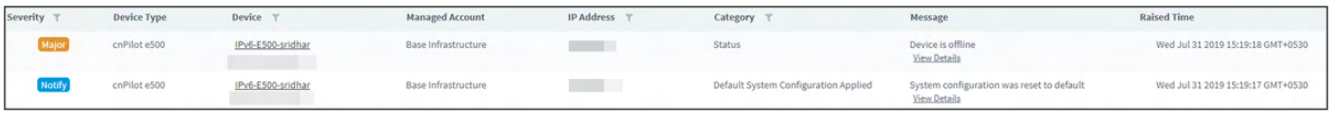
   It displays **Please confirm factory reset** message as shown below:



4. Click **Yes, Factory reset** option.

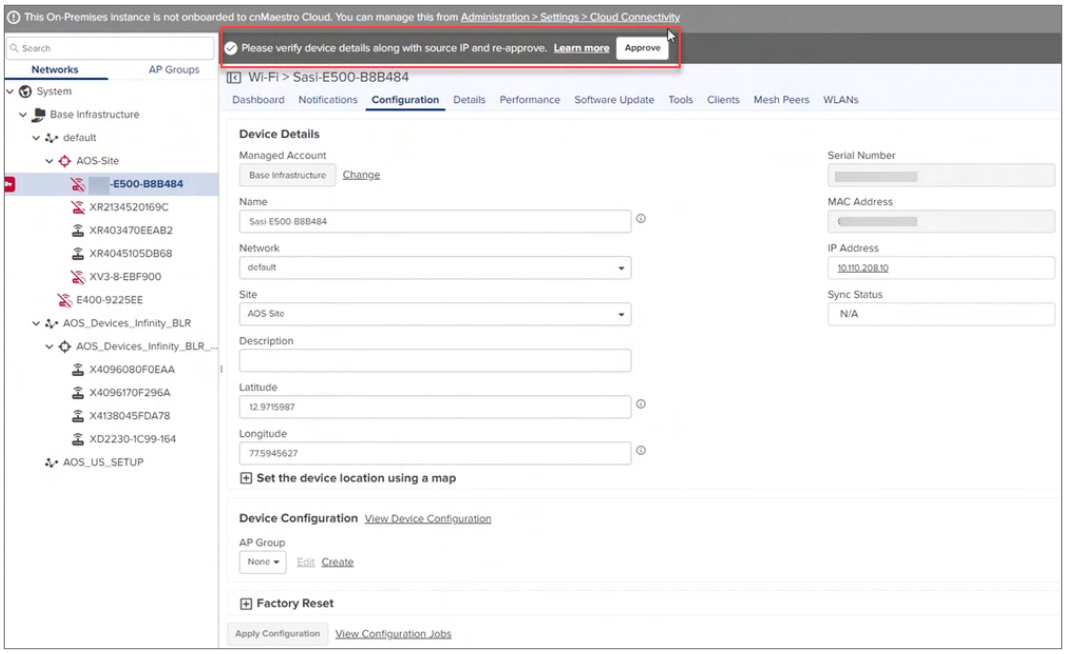


If the Factory Reset is successful, the following message is displayed on the **Notifications** tab.

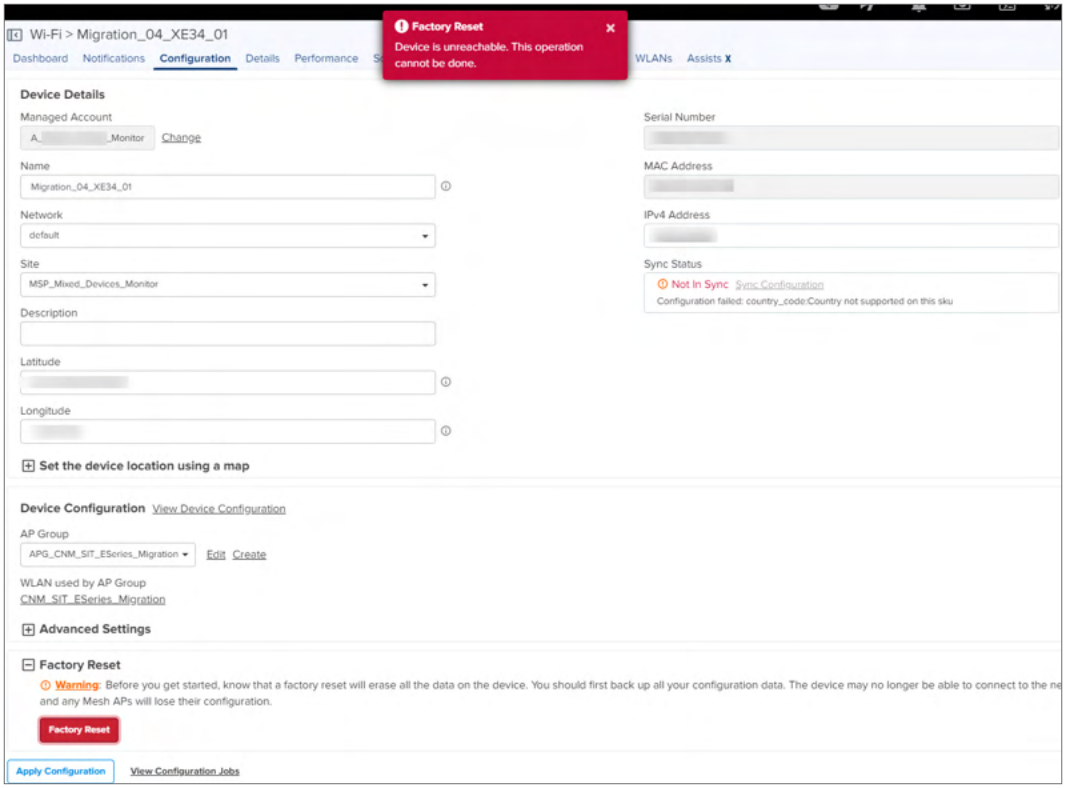


Severity	Device Type	Device	Managed Account	IP Address	Category	Message	Raised Time
Major	cnPilot e500	IPv6-E500-sridhar	Base Infrastructure		Status	Device is offline View Details	Wed Jul 31 2019 15:19:18 GMT+0530
Notify	cnPilot e500	IPv6-E500-sridhar	Base Infrastructure		Default System Configuration 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:



When Factory Reset is applied to an offline device, it displays an error as shown below:



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

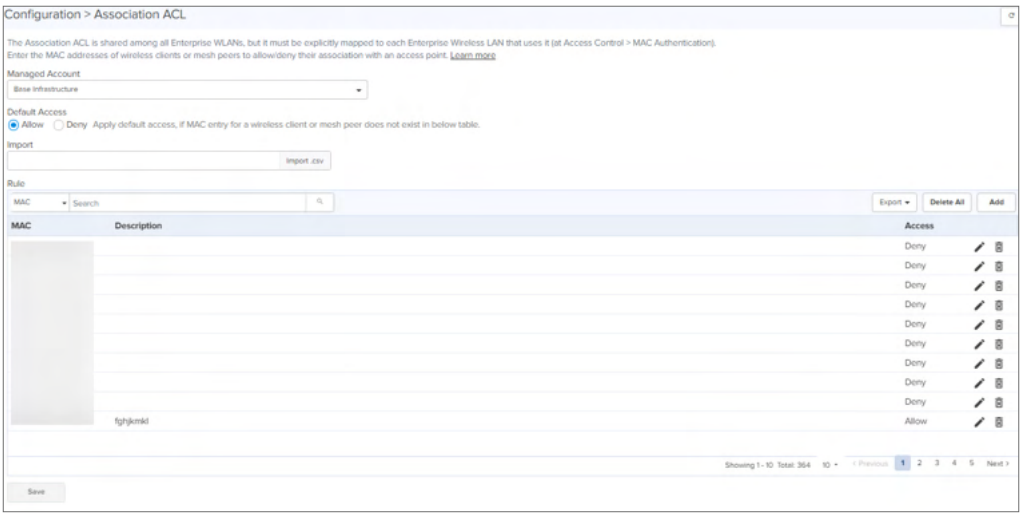
When a client tries to connect to an AP, the following occurs:

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.

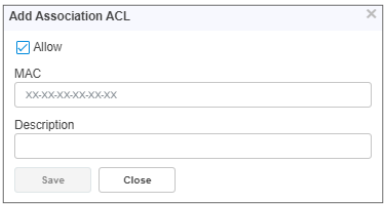
Configuring Association ACL

To configure the Access Control List (ACL) in cnMaestro:

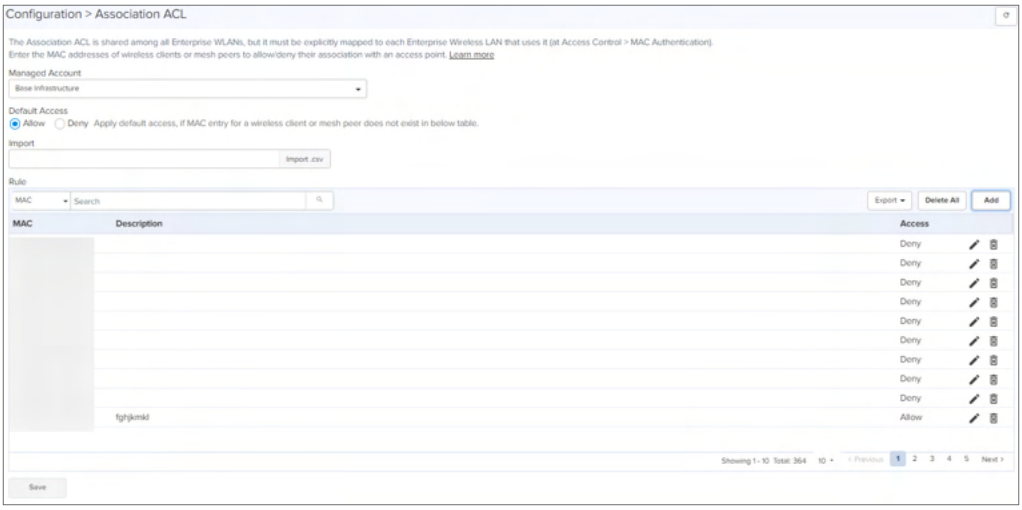
1. Navigate to **Configuration** > **Wi-Fi Profiles** > **Association ACL** tab**.**
2. Click **Add.**



3. Select **Allow.**
4. Enter the **MAC** and **Description**.
5. Click **Save**.



It displays the **Success** message.



6. To configure MAC authentication as cnMaestro:

   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**).

Note

- If MAC is not configured under the policy (to Allow or Deny), the default action will be applied.
- You can perform the following actions by selecting the respective icons in the table:
  - Edit
  - Delete
  - Export
  - Import Association ACL, by selecting **Import.csv** file.

Custom Applications X

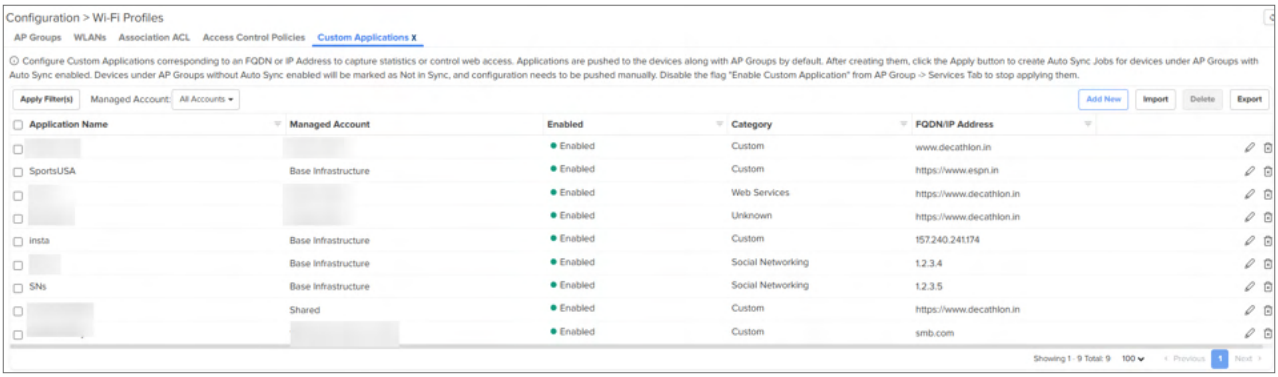
Custom applications allow you to configure applications with a specific IP address or a domain name, and apply filter rules, such as enable or disable traffic from these applications. By default, these applications are applied on the devices along with the AP group configuration.

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.

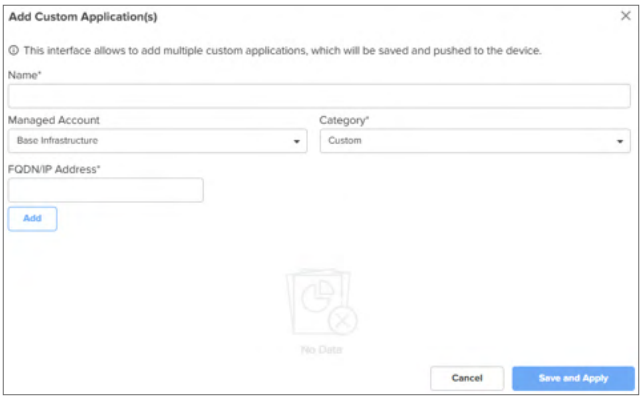
To add a new custom application, complete the following steps:

1. Navigate to **Configuration** > **Wi-Fi Profiles** > **Custom Applications X**.



2. Click **Add New** on the **Custom Applications X** page.

   The **Add Custom Application(s)** window is displayed.



   Configure the following parameters:

Table 79 *Custom Application Parameters*

Parameter	Description
Name	Specifies the name for the custom application. Supports a maximum of 20 characters.
Managed Account	Specifies the availability of the custom application across managed accounts. The following values are supported: • Base Infrastructure—Custom application is available only for the global account. It is not shared with other managed accounts. • Managed Account—Custom application is available only for that specific managed account. **Note**: Once the Managed Account 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.
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 Switch Profiles

Port Templates allow users to create and reuse predefined port configurations across multiple ports within a Switch Group.

cnMaestro simplifies the network deployment and operation of cnMatrix switches through the use of Switch Groups, which allow configuration sharing across multiple switches. Within Switch Groups, Policy-Based Automation (PBA) can be used to further streamline operations and improve network security.

Switch Groups

A Switch Group is the equivalent of a virtual stack. The Switch Group allows users to manage multiple switches with the same configuration.

Configuration is common to all Switches belonging to a Switch Group:

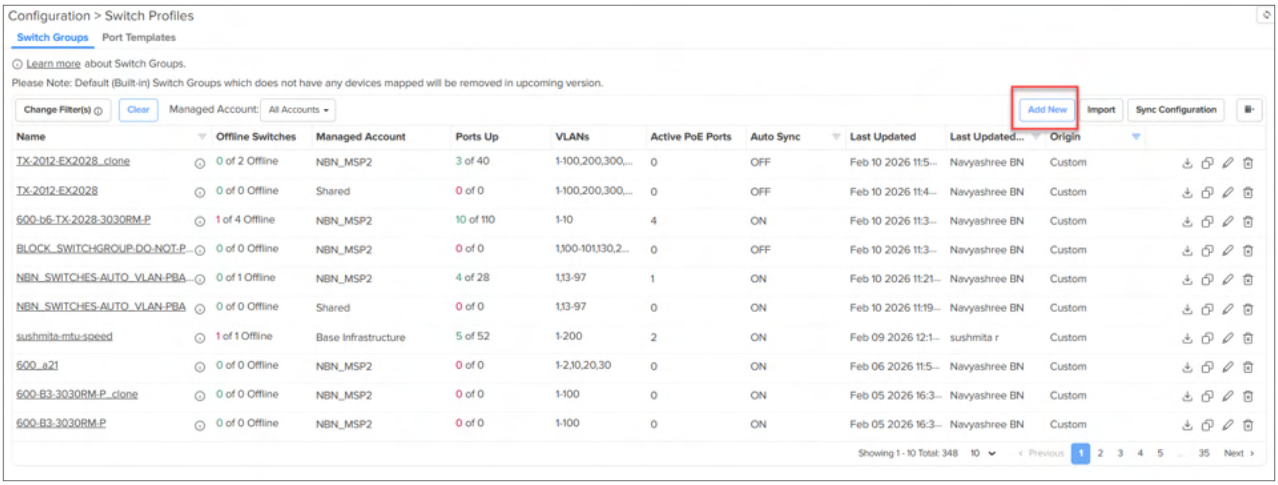
- Configuration changes are synchronized and applied to all Switches whenever the Switch Group is updated.
- A subset of configuration attributes can be overruled for an individual Switch.
- Switch ports across all physical switches associated with a Switch Group can be edited in bulk.

This section contains the following topics:

- Synchronize (Sync) Configuration
- Policy Based Automation (PBA)
- Devices
- Port Stack
- Device Details

The process for creating a new switch group configuration is as follows:

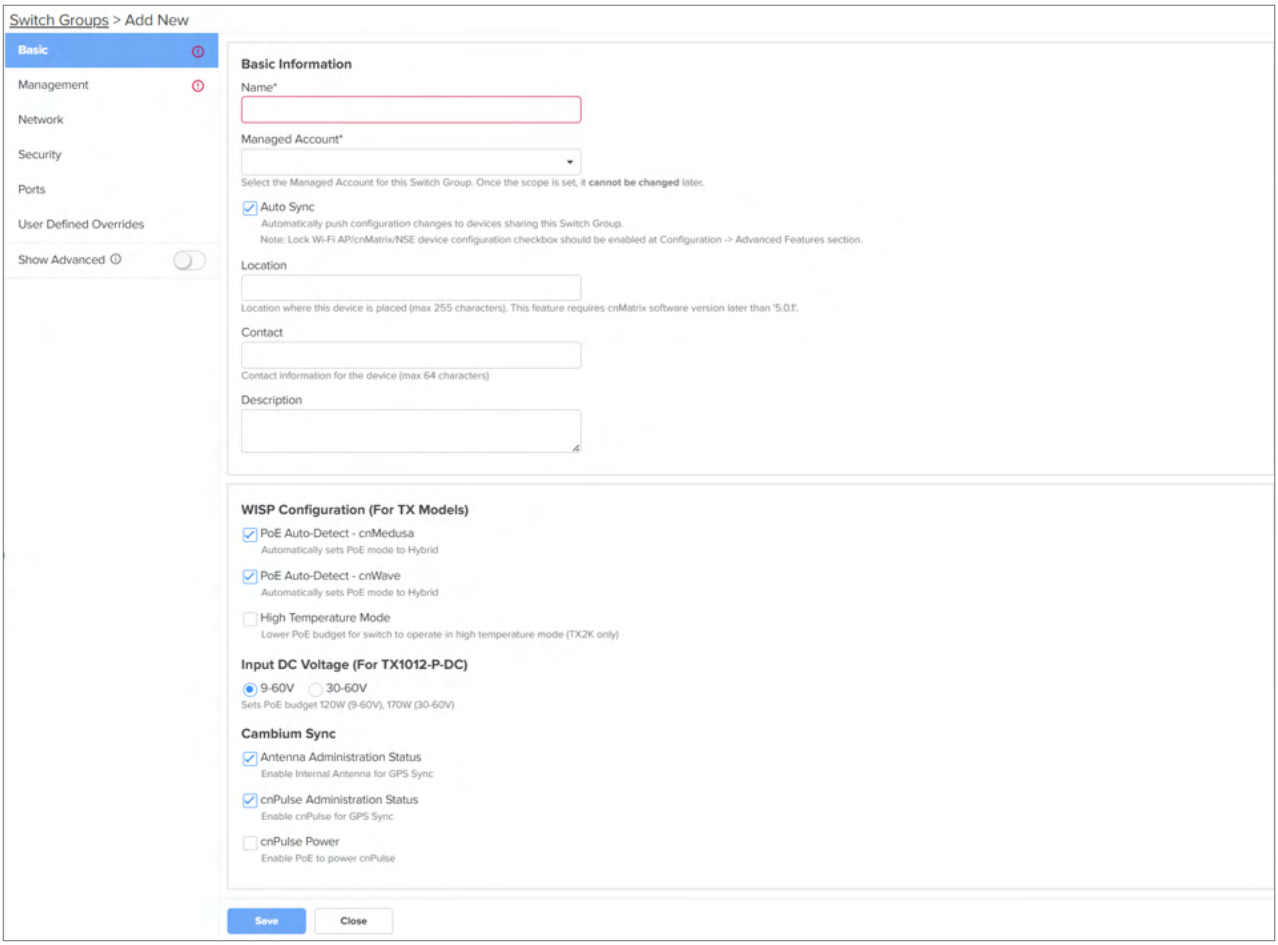
1. Navigate to **Configuration** > **Switch Profiles** > **Switch Groups** tab.
2. Click **Add New**.



Note

You can also navigate to **Configuration > Switch Profiles** page by using the edit ( ) icon in the Switch Group list.

3. The following configuration sections are available when creating a Switch Group:
   - Basic
   - Management
   - Network
   - Security
   - Ports
   - User-Defined Overrides



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

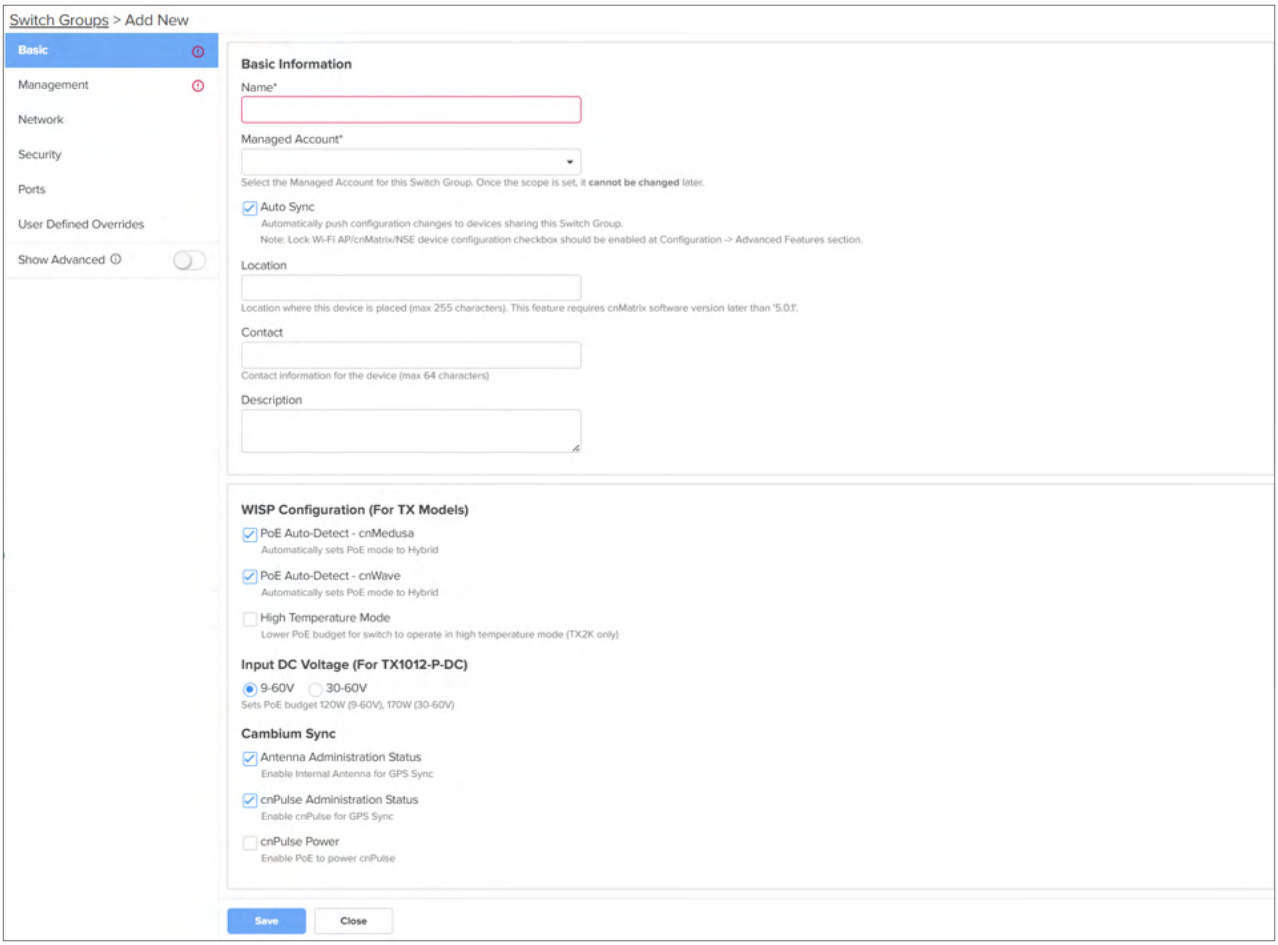
The Basic tab provides options to the user to configure the device name as well as other standard values used to identify a switch.

1. Navigate to **Switch Groups** > **Basic**.
2. On the Basic page, enter device identification data such as:
    - Name
    - Contact
    - Description
    - Managed Account
    - Location
    - WISP Configuration

- Input DC Voltage
- Cambium Sync

Note

- 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. If required, enable the **Daylight Saving Time** and enter the details.

Switch Groups > Add New

Basic
Management
Network
Security
Ports
User Defined Overrides
Show Advanced

Administrator Access

Telnet
HTTP
HTTPS
Enable HTTPS. This feature requires cnMatrix software version later than '5.0.3'.
SSH
Change your passwords, do not use default passwords!

Add

Username	Password	Privilege
admin	Set new password	Root
guest	Set new password	Guest

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*
UTC
Set Time Zone Name (3-6 upper case characters, e.g. EST, PST, UTC). Default is UTC.
Daylight Saving Time
Disabled Enabled

DNS

DNS Server 1
XXX.XXX.XXX.XXX
DNS Server 2
XXX.XXX.XXX.XXX

SNMP

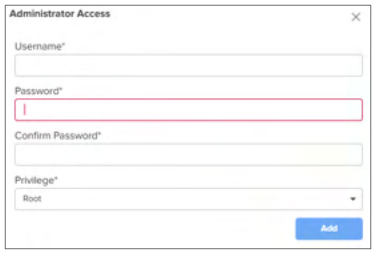
Enable
Controls SNMP support on the device
SNMPv2c RO Community
SNMPv2c read-only community string (max 32 characters)
SNMPv2c RW Community
SNMPv2c read-write community string (max 32 characters)
Trap Receiver IP
XXX.XXX.XXX.XXX
SNMP trap server IPv4 address
SNMPv3 Username
SNMPv3 user name (max 32 characters)
SNMPv3 Authentication Key
Show
SNMPv3 Authentication Key (0, 8 to max 32 characters)
SNMPv3 Privacy Key
Show
SNMPv3 Privacy Key (0, 8 to max 32 characters)
Access
Read-Only Read-Write
Authentication
None
Encryption
None
Reset SNMP Settings
Clears non-read-only/non-permanent entries in the SNMP Community and USM User tables

Event Logging

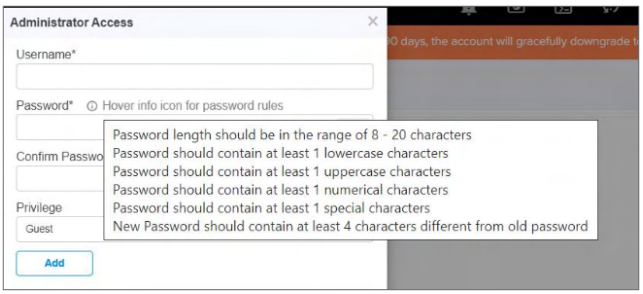
Minimum Syslog Level
Notification
Server Address
Port

Save Close

3. By default, the switch group includes Admin and Guest accounts
    - If required to create an additional user account, click **Add New** and enter the required details.
    - Click **Add.**



4. Set new Password and new password should match the special characters as shown below:

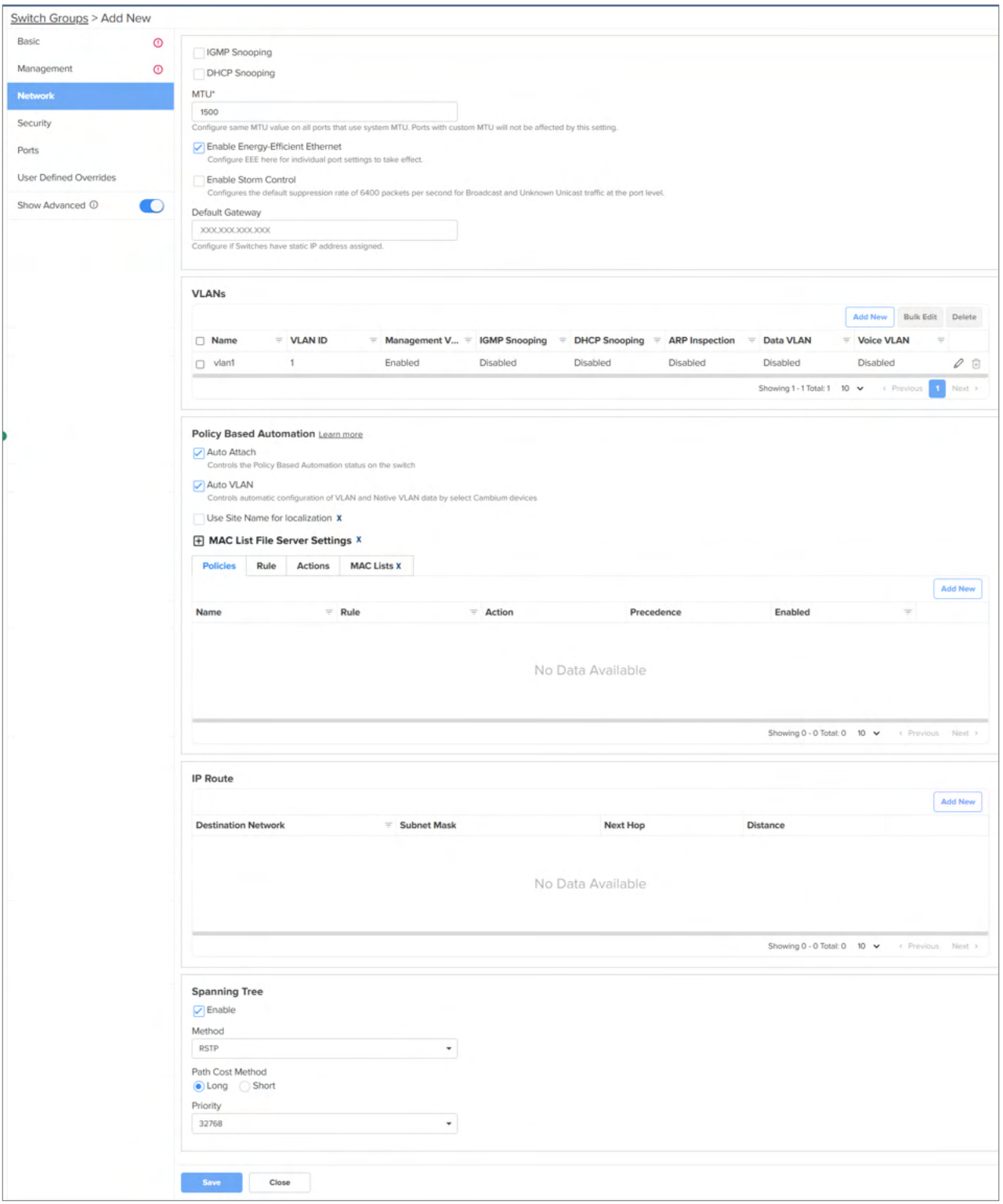


5. **Time Settings**: Enable the **Daylight Saving Time** and enter the corresponding details.
6. **DNS**: Enter DNS server details.
7. **SNMP**: Enter SNMP details.
8. By default, event logging is set to Notification; users can change the severity if needed and optionally configure an external syslog server.
9. Click **Save.**

Network

The Network page allows the user to configure VLANs, PBA, IP Route, and Spanning Tree details.

1. Navigate to **Switch Groups** > **Add New** > **Network**.



Note

Use Site Name for localization, **MAC List File Server Settings**, and **MAC Lists** are cnMaestro X features.

2. Enable **IGMP Snooping** and **DHCP Snooping**, if required.

3. **MTU** displays the default value.
4. If required, **Enable Storm Control**.

> **Note**:
>
> Enabling storm control allows you to configure the default suppression rate of 6,400 packets per second for broadcast and unknown unicast traffic at the port level.
>
> If disabled, traffic suppression is not applied.

5. Enter the **Default Gateway**.
6. By default, the switch group includes a VLAN. To add additional VLANs, click Add New if required.
   - Enter the **VLAN ID**.
   - Enter the **VLAN Name**.

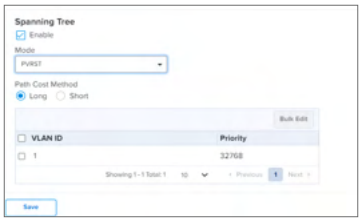
   - Enable or disable the following options:
     - Management VLAN
     - IGMP Snooping
     - DHCP Snooping
     - ARP Inspection
     - Voice VLAN
     - Data VLAN
   - Click **Add**.
   - Click the **Edit** icon or **Bulk Edit** to modify the configuration of the corresponding VLANs, and then click

Update to apply the changes.

7. If required to add a new IP Route, click **Add New.**
   a. Enter the **Destination Network**.
   b. Enter the **Subnet Mask**.

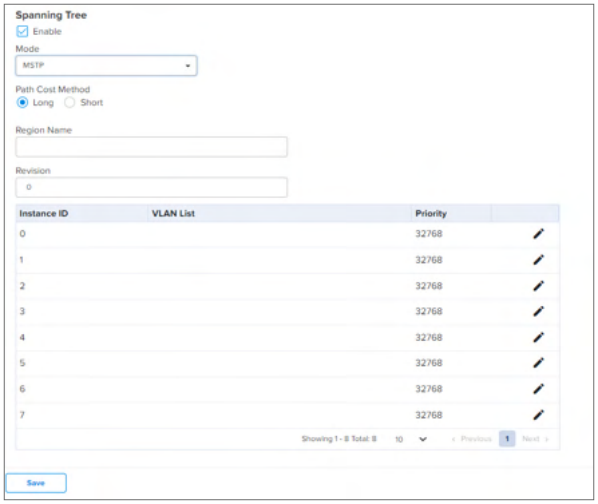
   c. Enable the **Next Hop.**
   d. Enable the **Distance.**
   e. Click **Add.**
8. By default, **Spanning Tree** is enabled with default values. If required, change the default mode by selecting one of the available options from the drop-down menu as shown below:
   a. By default, **RSTP** is selected. Select a different mode from the drop-down menu if required.
      - Select Path Cost Method **Long** or **Short.**
      - Select **Priority**.

   b. Select the Mode **PVRST** from the drop down.
      - Select Path Cost Method **Long** or **Short.**
      - Select **Priority**.

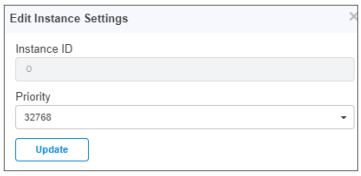


c. Select the Mode **MSTP** from the drop down.

- Select Path Cost Method **Long** or **Short.**
- Enter the **Region Name** and **Revision.**



- User can edit **Priority** by clicking the edit (✎) icon.
- Select the Priority and click **Update.**

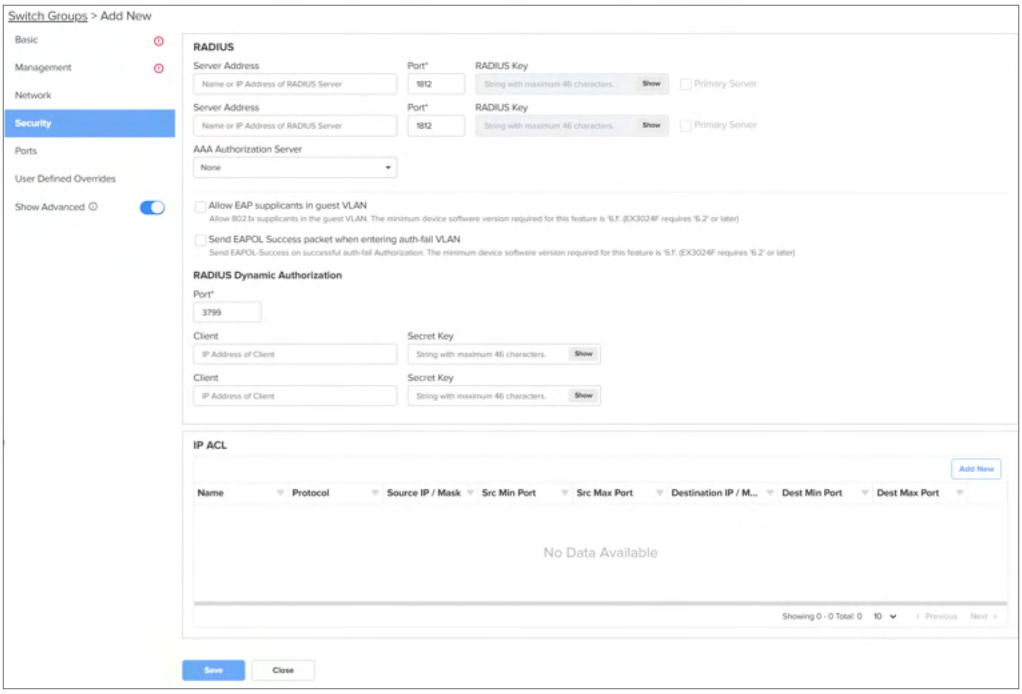


9. Click **Save.**

Security

The Security page is configured with default values. If required, users can optionally configure RADIUS and Access Control List (ACL) settings as needed:

1. Navigate to **Switch Groups** > **Security** tab.
2. Enter **Server Address**.
3. Enter **RADIUS Key**.
4. In **AAA Authorization Server**, select **None** or **RADIUS** from the dropdown.
5. Enable **Allow EAP supplicants in guest VLAN** and **Send EAPOL Success packet when entering auth-fail VLAN**.
6. Enter **RADIUS Dynamic Authorization**.



7. If required, to configure the **IP ACL**, click **Add New**.

- Enter **ACL Name**.
- Select the appropriate **Protocol** from the dropdown.
- Enter **Source IP/Mask**.
- Enter **Destination IP/Mask**.
- Click **Add**.

8. Click **Save**.

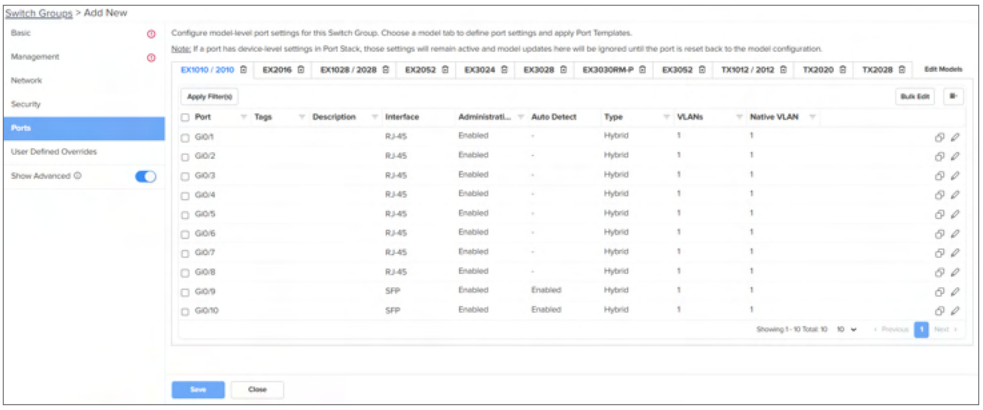
Ports

The Ports tab allows user to configure common port settings for each switch model in a switch group. These settings are automatically applied and shown in the **Port Stack** > **Configuration** tab. For device specific changes, user can update the settings directly in the **Port Stack** > **Configuration** tab.

> **Note**:
>
> Configuration changes made in the **Port Stack** tab always take priority and overrides the model configuration port settings on the **Ports** page.

To configure Ports, perform the following steps:

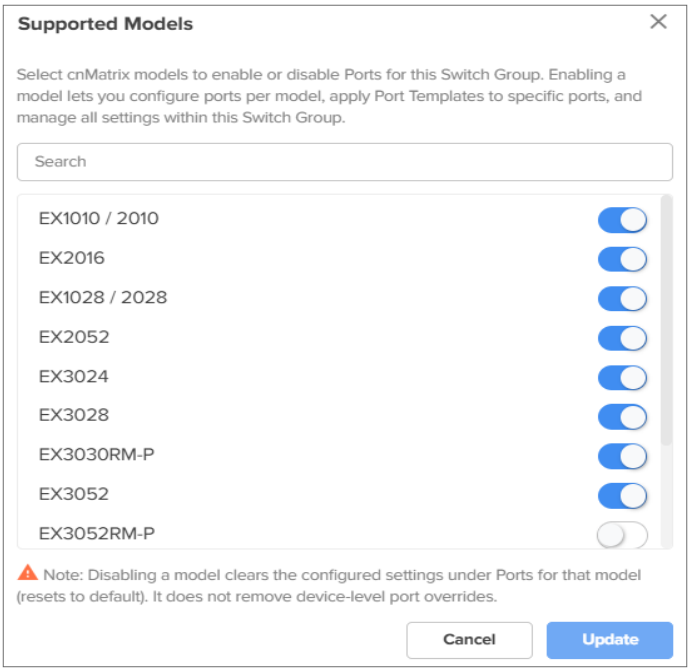
1. Navigate to **Switch Groups** > **Ports** tab.
   - For new switch groups or switch groups already running the current release, Ports is available by default.



   - For existing switch groups upgraded from earlier releases, users must enable Ports before configuring port-level settings.

2. Click icon to delete models, or use **Edit Models** to enable or disable.

   Enable Ports for Supported Models pops up.



a. Toggle the button to enable or disable the device models for ports.

> **Note**:
>
> Once a device model is disabled in Ports and the changes are saved, the configuration cannot be restored. Re-enabling the model applies the default port configuration.

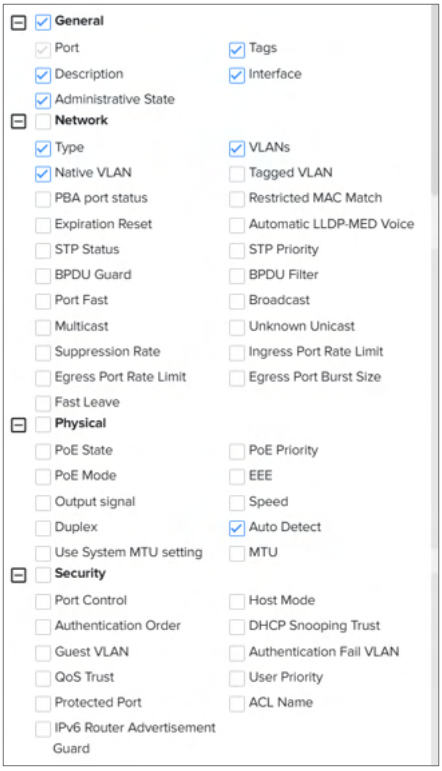
b. Click **Update**.

3. Click **Save**.

The **Ports** section details view displays the following fields by default:

- Port, Tags, Description, Interface, Administrative State, Auto Detect, Type, VLANs, Native VLAN, Clone, and Edit.

  User can click on the Hamburger icon on the top right corner of Ports section and to include additional fields in the Ports related information.



Edit Ports

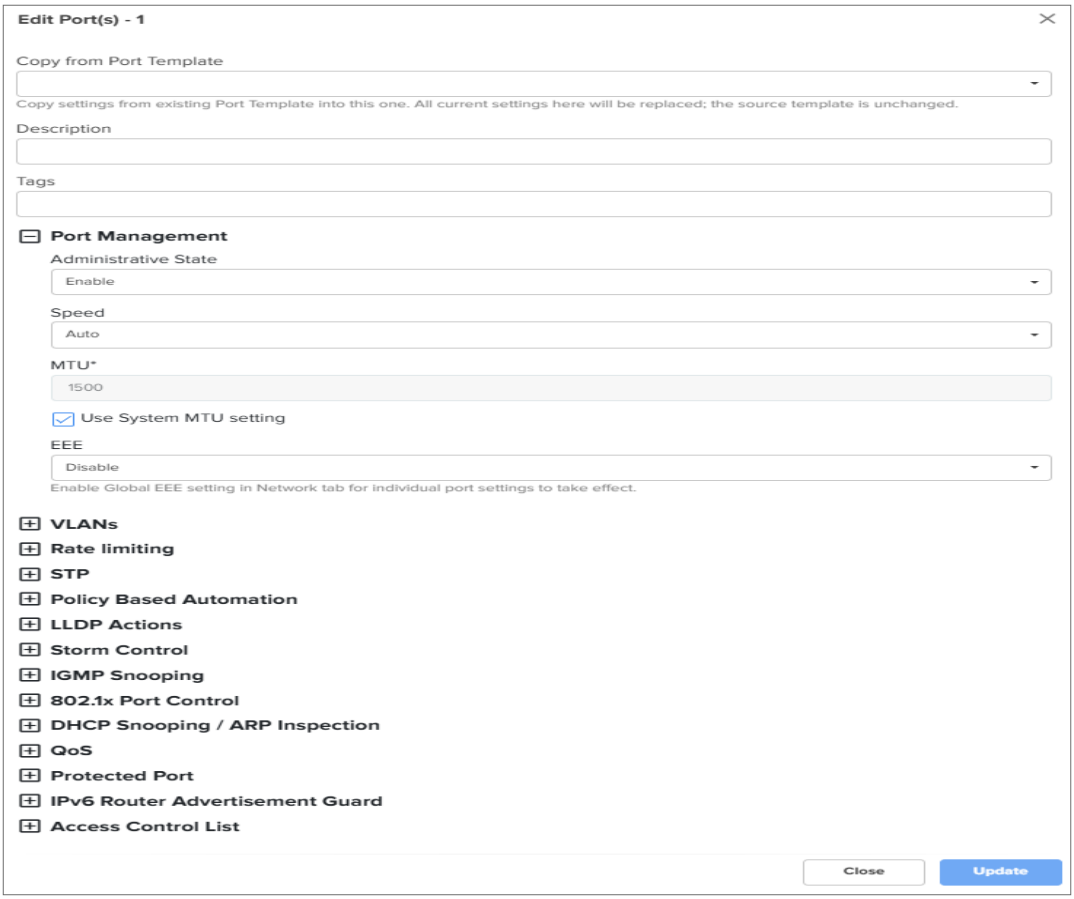
> **Note**
>
> Model-specific settings from templates are automatically ignored if applied to incompatible devices.

Edit Ports or bulk edit allows user to modify port configurations or apply templates to one or more ports within a Switch Group.

To edit a Port, perform the following steps:

1. Select a **Port** from the list.
2. Click **Edit** icon.

   Edit Ports window pops up



3. In the **Copy from Port Template**, select the required template from the drop down.
4. Configure the parameters as shown in Table 81.
5. Click **Update**.

Clone Ports

To clone the port templates, perform the following steps:

1. in the Ports table, click the save as port template ( ) icon corresponding to the port configuration you want to clone.

   Save as Port Template pops up.

2. Enter the **Port Template Name**.

3. Enter the **Description**.
4. Click **Save**.

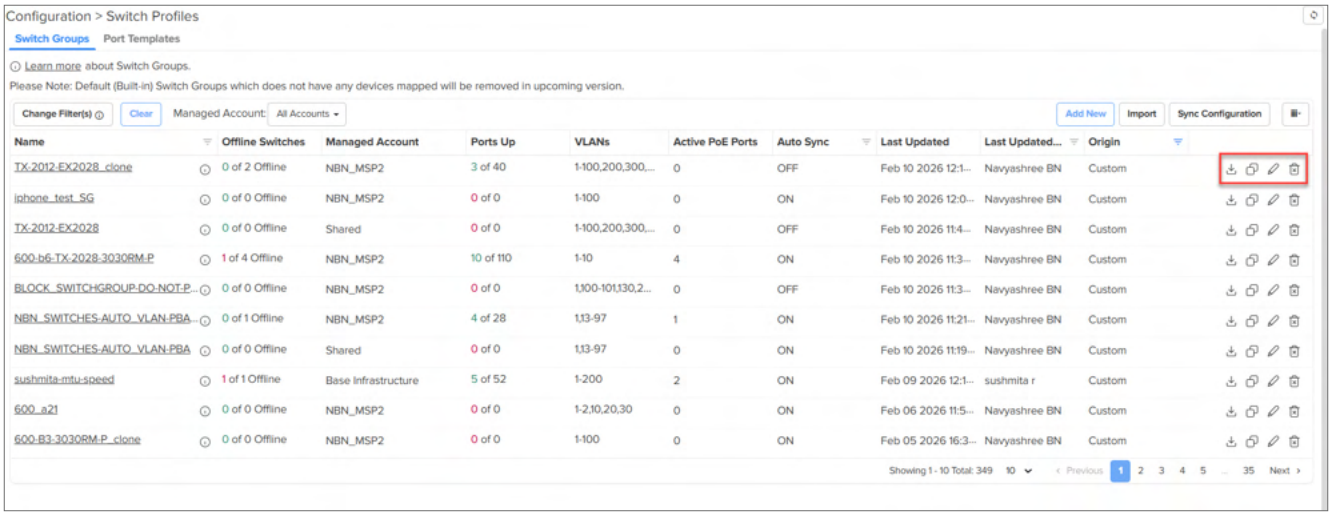
User-Defined Overrides

> **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 following 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.



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 **Managed Account** from the dropdown list.
3. Select **import.json** and import the file.

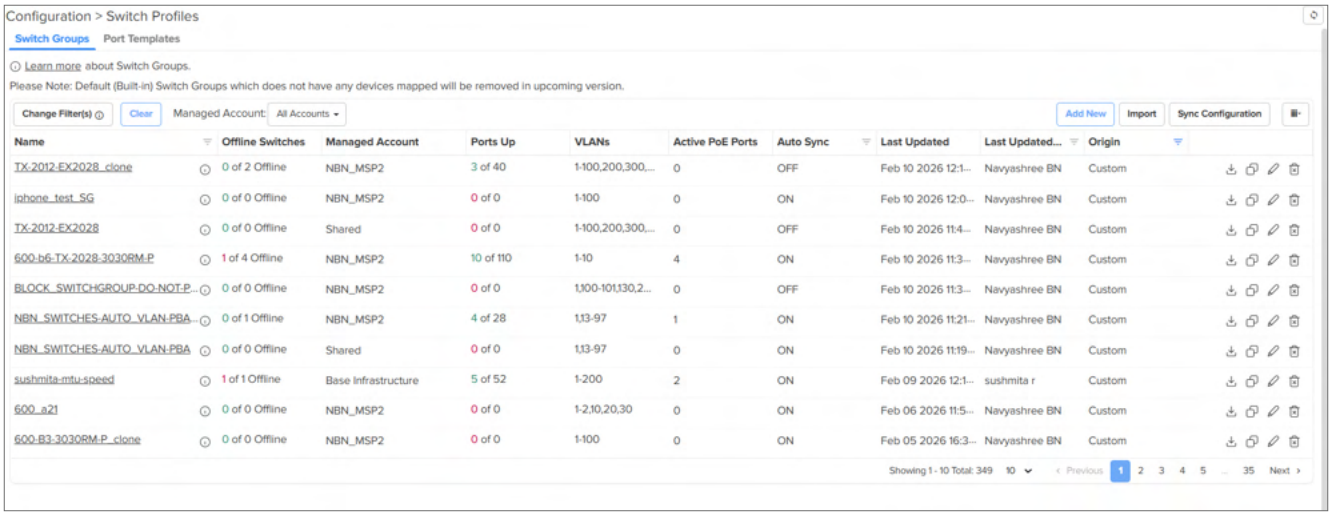
4. Click **Import.**

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.



Auto Sync Configuration

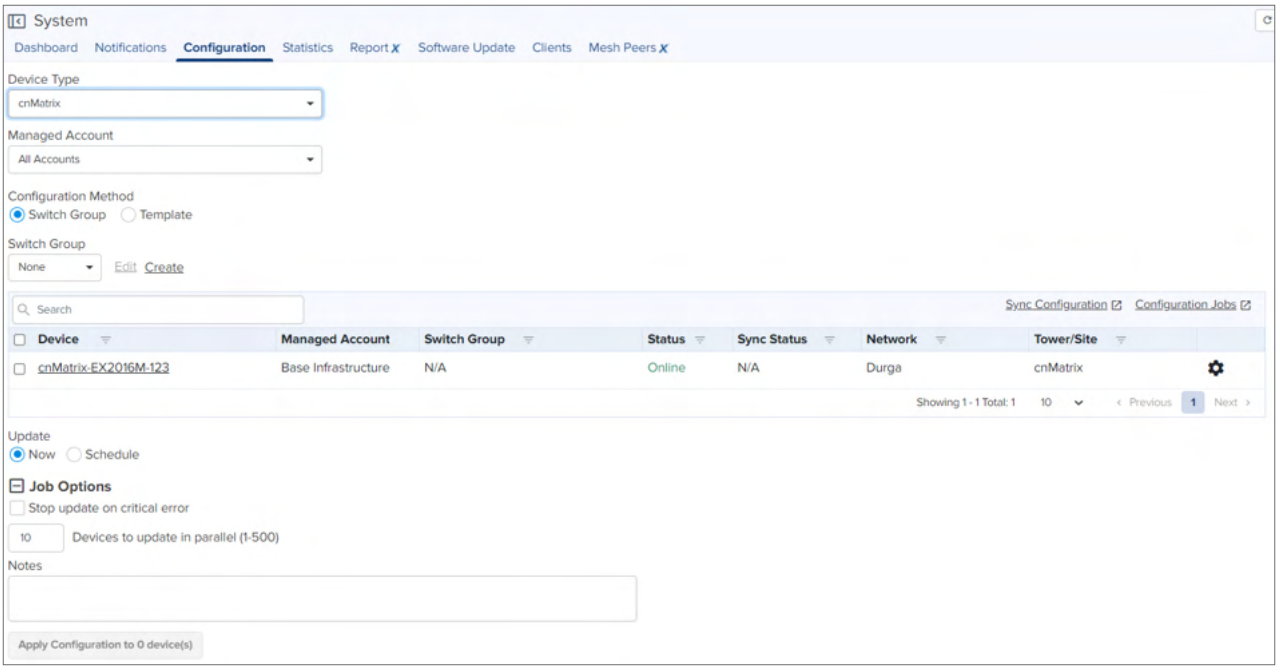
Switch Groups can be configured to Automatically Synchronize all configuration when they are updated. This setting is found in the Basic Information page of the Switch Group configuration.

When the user tries to apply a Switch Group on a device and fails because device was Offline, the reason for the skip will be displayed as **Device was offline**, in the **Jobs** page. In this case, when the device is available online and connects to cnMaestro, then cnMaestro creates an **Auto-Sync** job for that device and pushes the Switch Group.

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 drop down.
2. Select the list of Switch Group **Device**.
3. Click **Apply Configuration**



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 under Auto Sync.

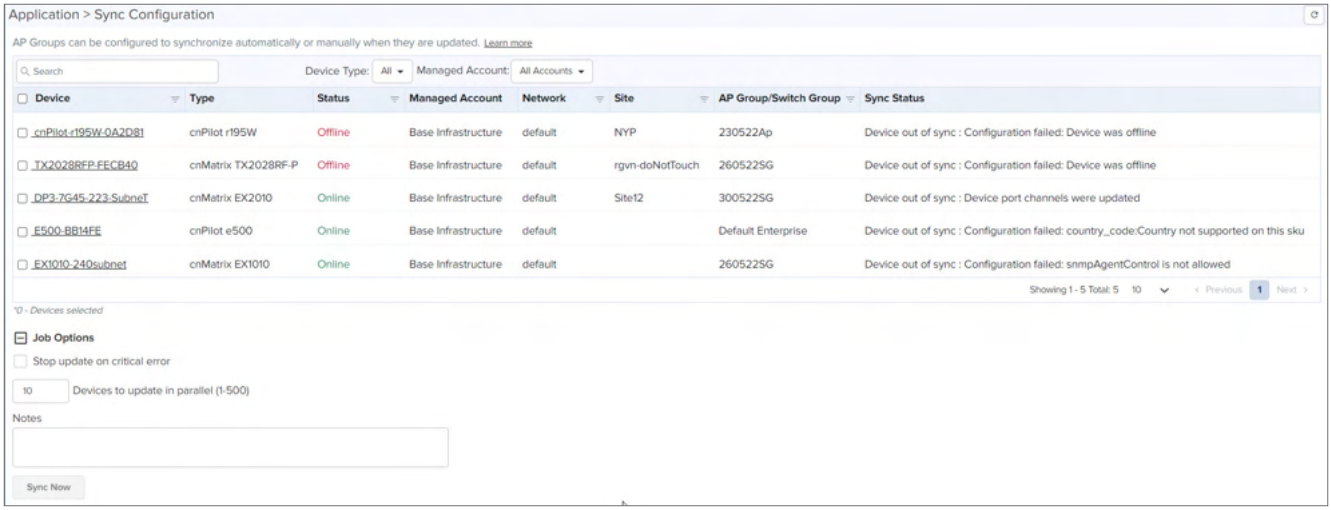
If the Auto-Sync is enabled, then by default switches synchronize (so any change of Switch Group, followed by a **Save**, will immediately push configuration to the devices without manual intervention). When Switches are not configured to synchronize automatically, or there is a failure in synchronization, then manual action is required.

Manual Synchronization

Manual configuration synchronization through the **Sync Configuration** page allows the user to synchronize and unsynchronize any devices as a group than updating each device separately.

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 303 *Sync Configuration page*



Sync Configuration has the following fields:

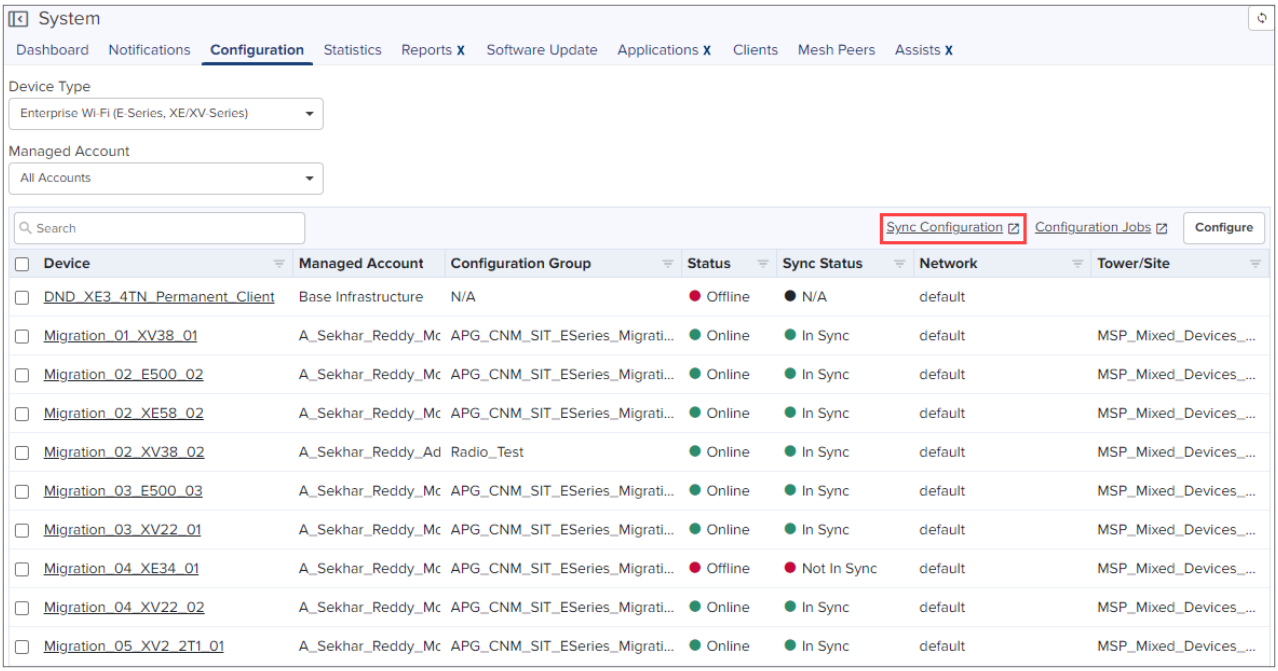
- Device (Hostname)
- Type
- Status (Online/Offline)
- Network (Network in which device is present)
- Site (Site under which device is present)
- Configuration Group (AP Group/Switch Group to which device is mapped)
- Sync Status (Sync status will tell whether job is completed or failed)

Table 80 *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.

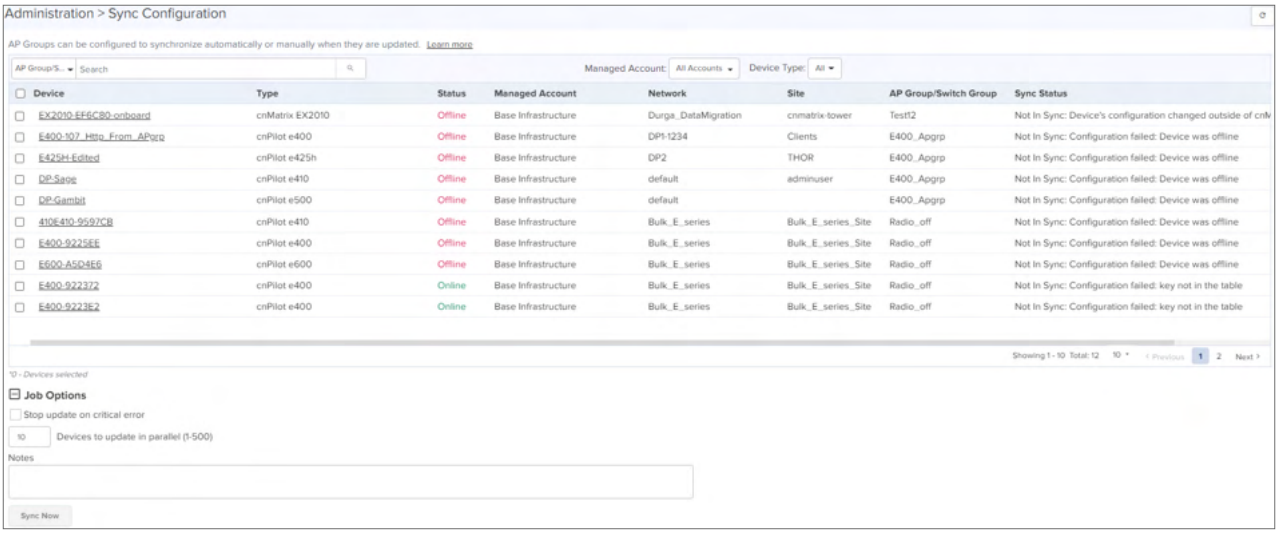
Perform the following steps to Sync Configuration:

1. Navigate to **Monitor and Manage** > **System** > **Configuration** or the **Jobs** tab.
2. Select the devices to synchronize and click **Sync Configuration.**

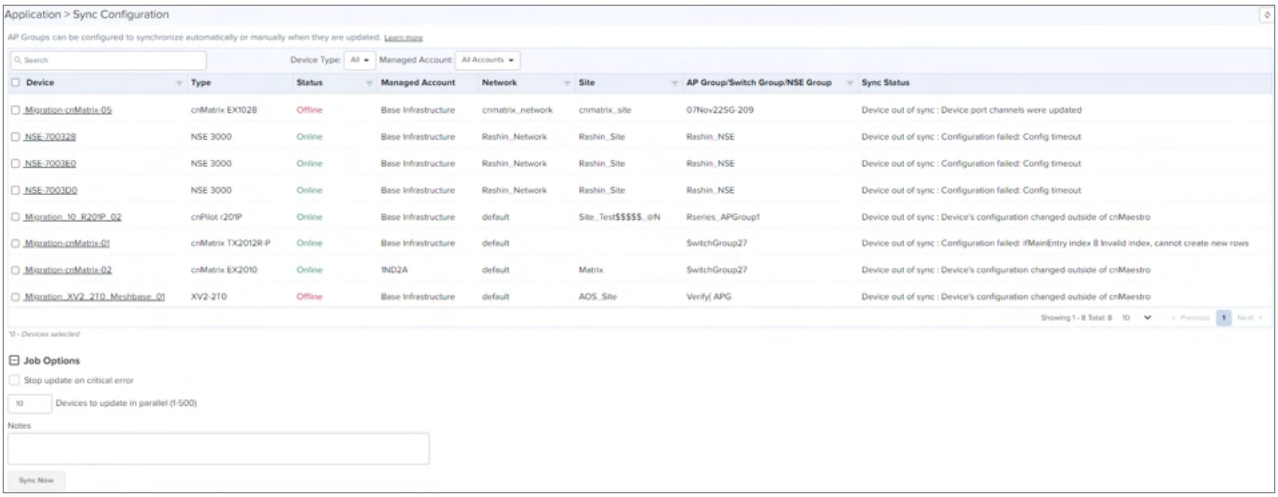


3. The **Administration** > **Sync Configuration** page is displayed.

   Select the devices to synchronize.



4. Click **Sync Now**.



User can also synchronize devices from **Administration** > **Sync Configuration**.

> **Note**
>
> Sync configuration is only available if a Switch Group is 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.

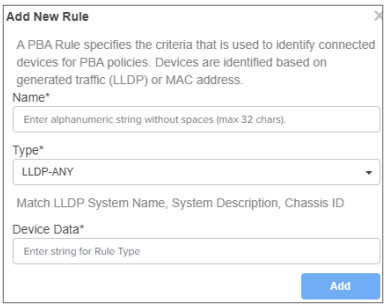
PBA Policies are an ordered list of PBA Rules (filters) and PBA Actions (configuration) that allow automatic configuration of ports based upon traffic. The policies are applied in increasing order of precedence until there is a positive match.

You need to configure **Rule** and **Action** before configuring a new **Policy**.

Configure the PBA as follows:

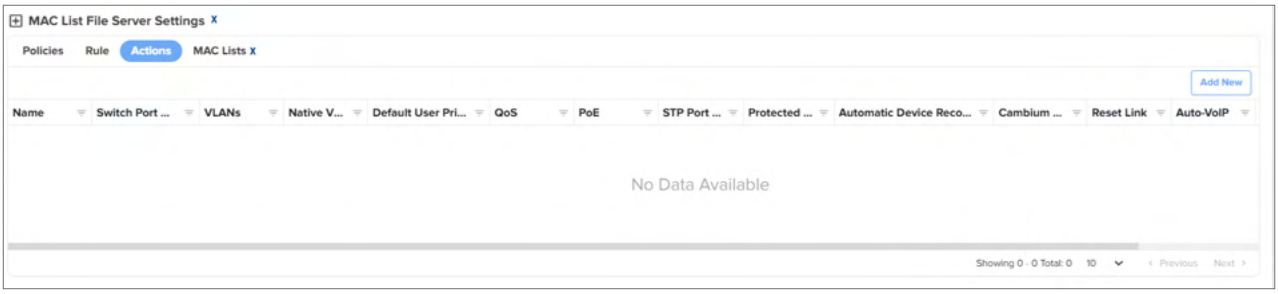
1. Navigate to **Configuration** > **Switch Groups** > **Network** > **Policy Based Automation.**
2. Navigate to **Rules** tab**.**

3. Click **Add New** to set the rules.



After new **Rule** is created, enter the actions for the newly created rule.

4. Click **Add**.
5. Navigate to **Actions** tab.



6. Click **Add New** to set the actions.

When the new action is added, navigate to **Policies** tab**.**

7. Click **Add**.
8. Navigate to **Policies.**

9. Click **Add New** to set the policies.

Devices

The Devices page is accessed by selecting the **Switch Groups** > **Devices** tab. The page lists all the physical switches assigned to the Switch Group. The Switch Dashboard and switch override configuration settings are accessible through this page. From the devices table, you can navigate to the individual Switches and view their Dashboard and optional Override Configuration settings. Switch Overrides allow you to override parameters for selected switches in the Switch Group.

> **Note**
>
> For configuration, a switch must belong to a Switch Group.

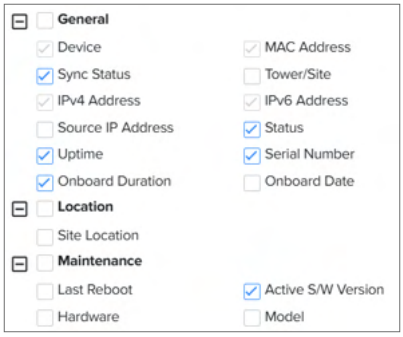
Configure the Switch Group as follows:

- Navigate to **Switch Groups** > select the switch from the list, and click **Devices** page to view and edit the onboarded switches.

The Devices details view displays the following fields by default:

- Device, MAC Address, IPv4 Address, IPv6 Address, Status, Uptime, Serial Number, Onboard Duration, Sync Status, and Active S/W Version tab.

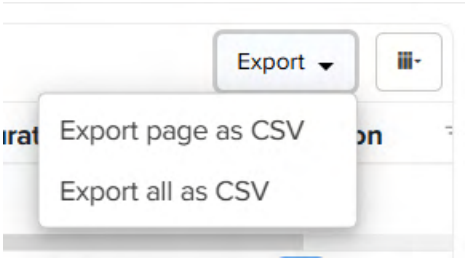
User can click on top bar to include additional fields in Devices Detail view.



Export Devices

Perform the following steps to export the Device table:

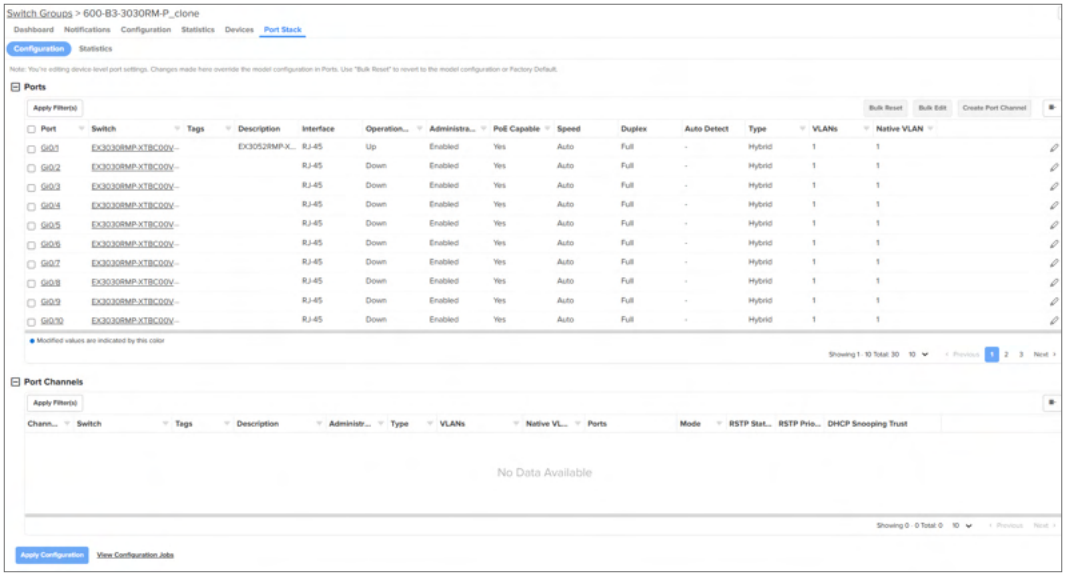
1. Click **Export**. A dialogue box appears.



2. Select **Export page as CSV/all as CSV** and export the file.

Port Stack

The **Port Stack** table displays the list of Ports and the Port Channel assigned to the specific switch. The **Port Stack** table allows administrators to configure the port settings by port ID for all ports within the **Switch Group**.



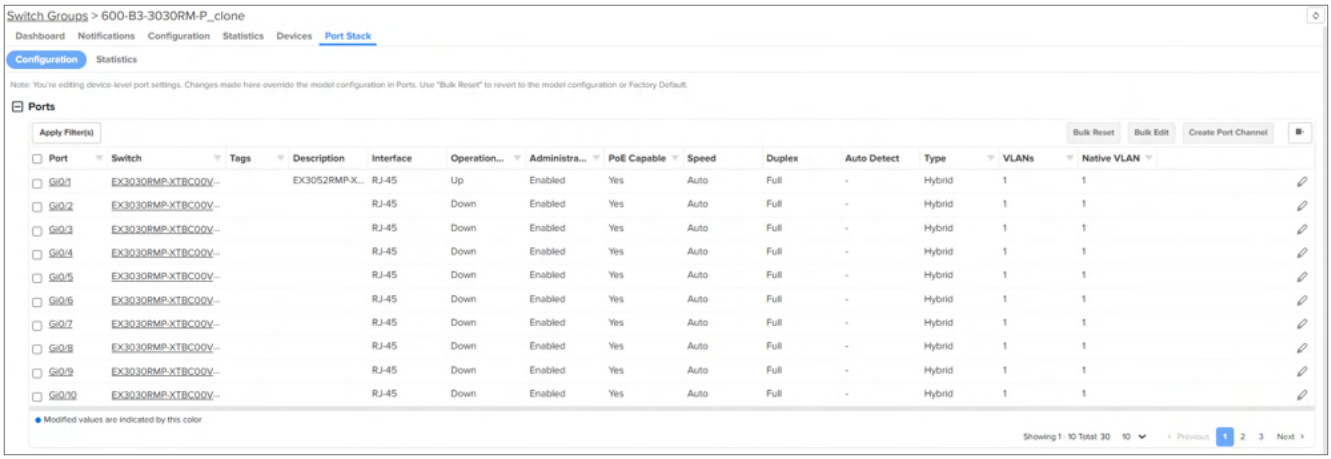
For example: Gi0/1

It supports bulk editing of Port stack settings across all physical switches.

To view the **Ports**, navigate to **Configuration** > **Switch Groups** > **Port Stack**.

Port Stack Configuration

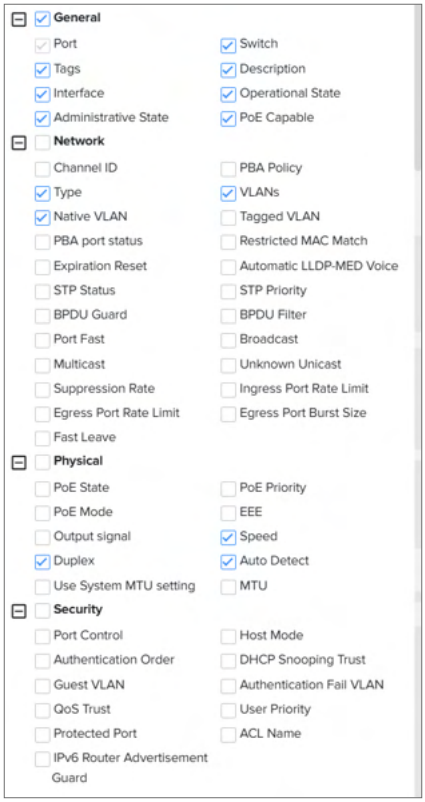
The Ports section table in Port Stack configuration supports creating port channels, editing port configuration, and configuring port parameters.



The **Ports** section details view displays following fields by default:

- Port, Switch, Tags, Description, Interface, Administrative State, Operational State, PoE Capable, Auto Detect, Type, VLANs, Native VLAN, 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** view.



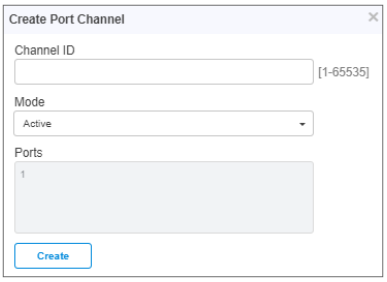
Click the edit ( ) icon or Port device in the list to edit the Ports Configuration details.

Create Port Channel

To create a Port Channel, perform the following steps:

1. Select a **Port** from the list.
2. Click **Create Port Channel**.

   Create Port Channel window pops up.



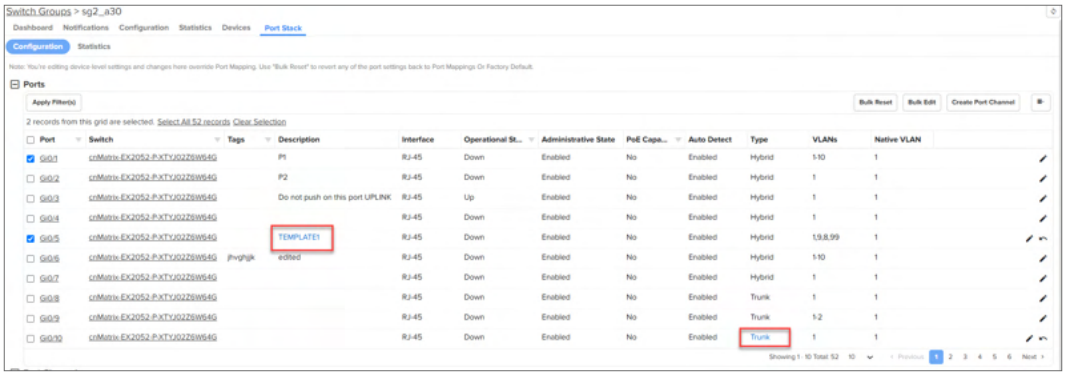
3. Enter **Channel ID**.
4. Select the **Mode** from the drop down.
5. Click **Create**.

Edit Ports

Edit Ports in Port Stack allows user to modify port configurations or apply templates to one or more ports within a Switch Group.

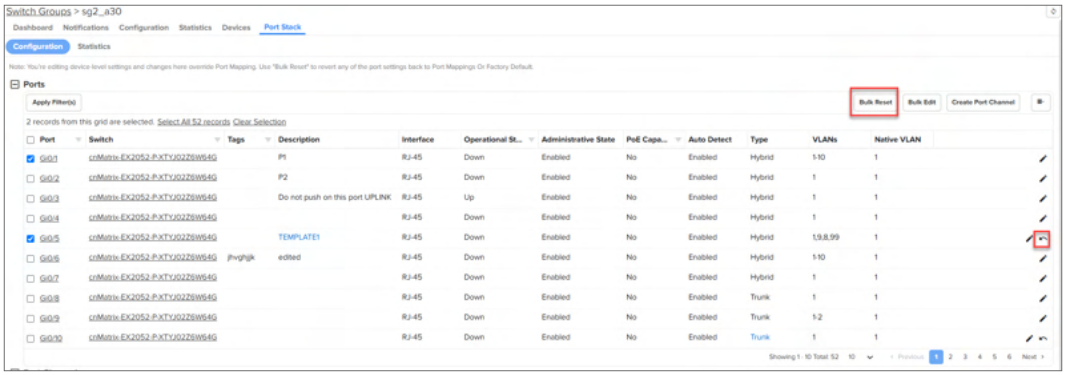
To edit a Port Channel, refer to Edit Ports.

Ports in Port Stack that have been modified are highlighted in blue, indicating they contain overrides different from the Ports configuration.



Reset

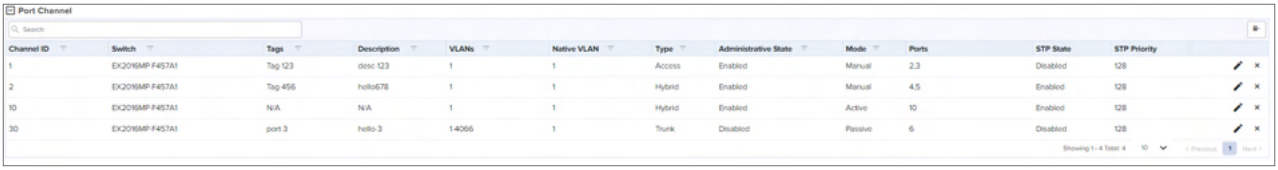
Upon Reset or Bulk Reset, the selected ports are restored to the Ports configuration defined in the ports, if available; otherwise, they are reset to the factory default configuration.



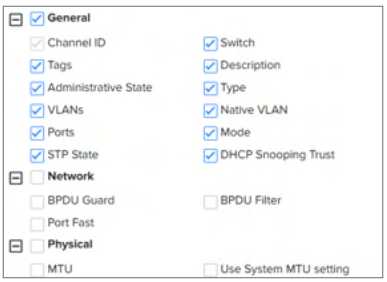
Port Channel

The **Port Channel** details view displays the following fields by default:

- Channel ID, Switch, Tags, Description, VLANs, Native VLAN, Type, Administrative State, Mode, Ports, STP State, and STP Priority.



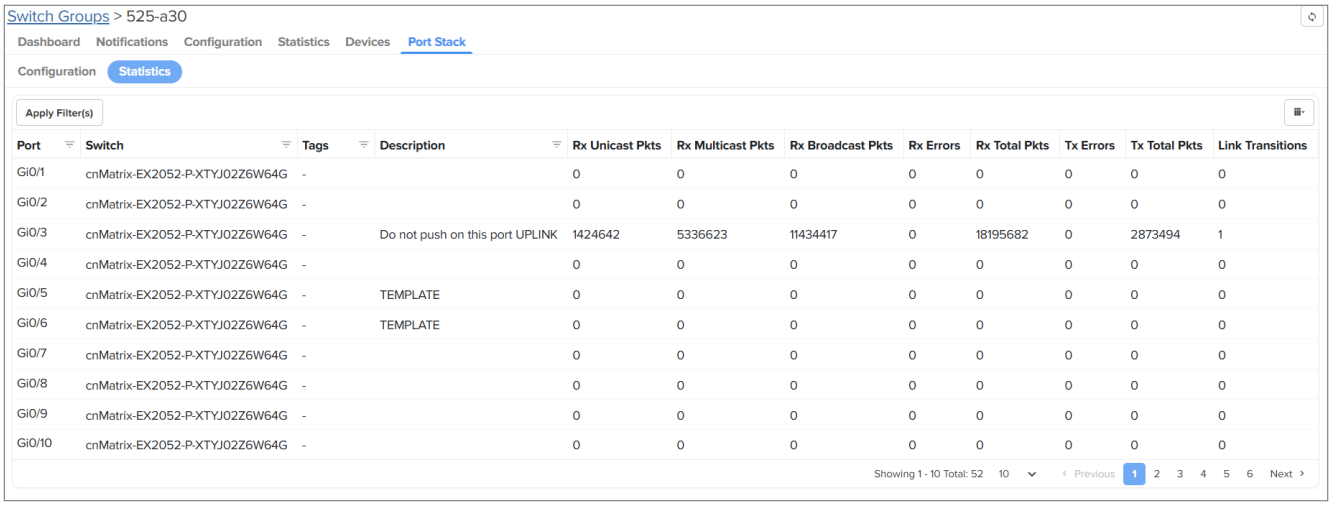
User can click on top bar to include additional fields in **Port Channel** Detail view.



Statistics

The **Statistics** page displays the latest data and statistics of each Port Stack. Port Stack statistics match the Client statistics and generate the Client View.

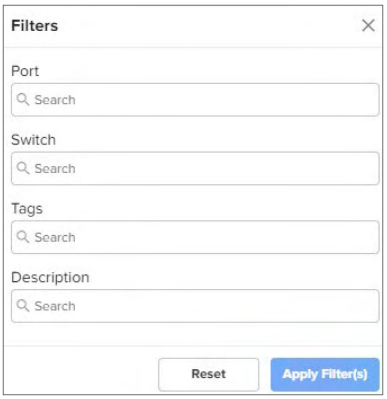
To view the Switch Ports statistics navigate to **Configuration** > **Switch Groups** > **Port Stack** > **Statistics**.



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	cnMatrix-EX2052-P-XTYJ02Z6W64G	-		0	0	0	0	0	0	0	0
Gi0/2	cnMatrix-EX2052-P-XTYJ02Z6W64G	-		0	0	0	0	0	0	0	0
Gi0/3	cnMatrix-EX2052-P-XTYJ02Z6W64G	-	Do not push on this port UPLINK	1424642	5336623	11434417	0	18195682	0	2873494	1
Gi0/4	cnMatrix-EX2052-P-XTYJ02Z6W64G	-		0	0	0	0	0	0	0	0
Gi0/5	cnMatrix-EX2052-P-XTYJ02Z6W64G	-	TEMPLATE	0	0	0	0	0	0	0	0
Gi0/6	cnMatrix-EX2052-P-XTYJ02Z6W64G	-	TEMPLATE	0	0	0	0	0	0	0	0
Gi0/7	cnMatrix-EX2052-P-XTYJ02Z6W64G	-		0	0	0	0	0	0	0	0
Gi0/8	cnMatrix-EX2052-P-XTYJ02Z6W64G	-		0	0	0	0	0	0	0	0
Gi0/9	cnMatrix-EX2052-P-XTYJ02Z6W64G	-		0	0	0	0	0	0	0	0
Gi0/10	cnMatrix-EX2052-P-XTYJ02Z6W64G	-		0	0	0	0	0	0	0	0

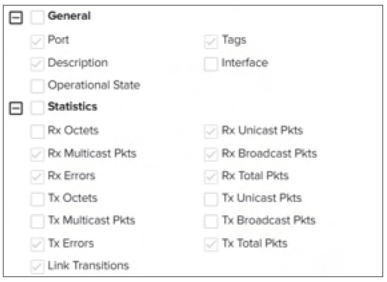
To apply filters, follow the steps below:

1. Click on the **Apply Filter(s)** tab.
2. A new window titled **Filters** appears.



3. Enter information in any field based on your filtering needs.
4. Click on **Apply Filter(s)**.

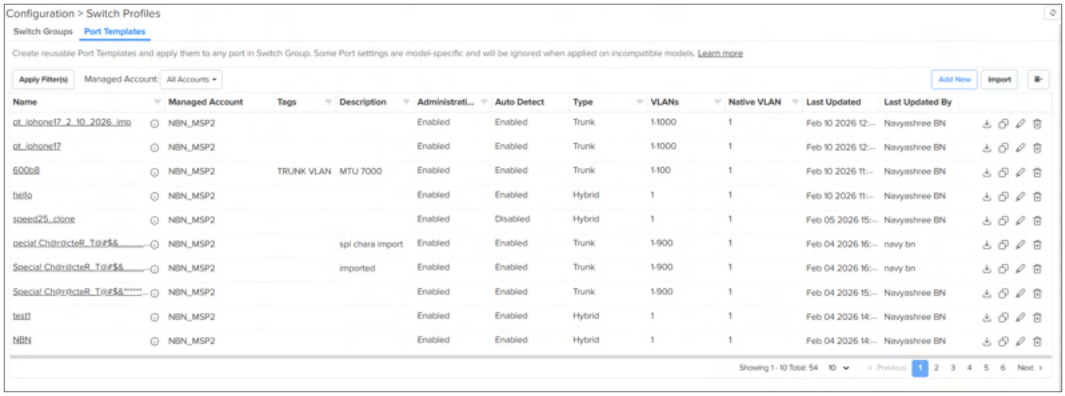
   User can click on top bar to include additional fields in **Statistics** Detail view.



Port Templates

Port Templates allow users to create predefined configurations and apply them to one or more ports in a ports settings of a Switch Group. When a template includes model-specific settings, the system automatically skips them for switch models that do not support them.

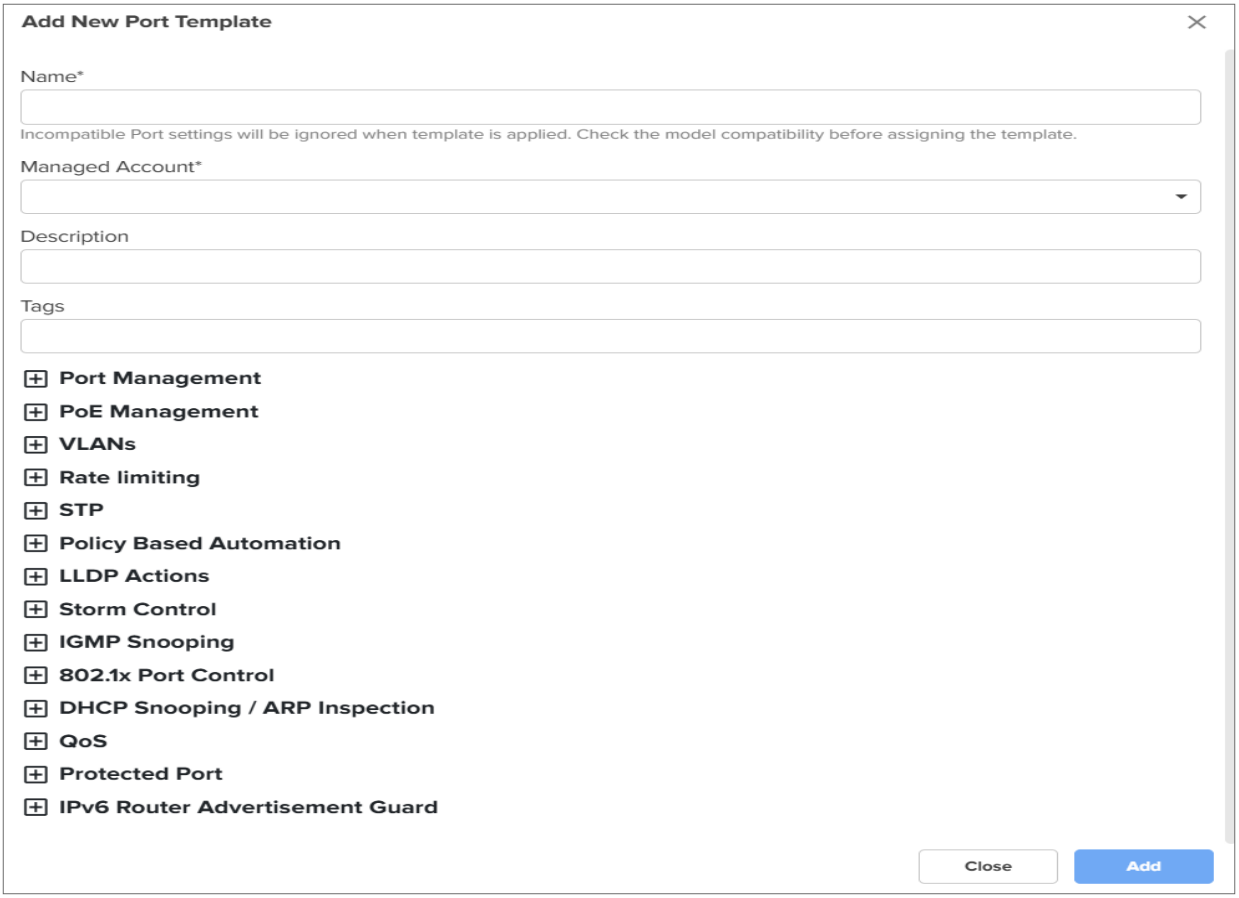
This can be used on ports section of switch group as well as **Port Stack** tab



To add a new port template, perform the following steps:

1. Navigate to **Configuration** > **Switch Profiles** > **Port Templates** tab.
2. Click **Add New**.

Add New Port Template window appears.



3. Set the required parameters shown in Table 81.

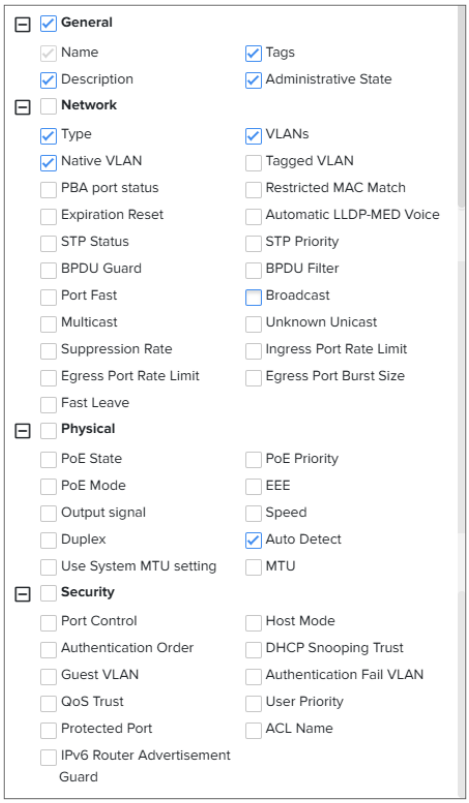
Table 81 *Add New Port Template parameters*

Parameter	Description
Name	Specifies a unique name for the Port Template.
Managed Account	Defines the range or applicability of the template.
Description	Describes the additional details about the template.
Tags	Allows user to assign keywords or labels to easily identify and group templates.
Port Management	Allows to enable/disable administrative state and configure the settings such as speed, Enable Auto Detect, MTU, and enable or disable the EEE.
PoE Management	Allows to enable/disable administrative state and set PoE Priority and PoE Mode.
VLANs	Allows to select the type, VLAN, and Native VLAN.
Rate Limiting	Allows to enter the Ingress Port Rate Limit, Egress Port Rate Limit, and Egress Port Burst Size.
STP	Allows to configure the STP State, Priority, BPDU Guard, BPDU Filter, and Port Fast
Policy Based Automation	Allows to enable/disable the PBA port status and Restricted MAC Match.
LLDP Actions	Allows to enable/disable the Expiration Reset and Automatic LLDP-MED Voice.
Storm Control	Allows to enter the Suppression Rate and allows to enable/disable broadcast,

Parameter	Description
	multicast, and unknown unicast traffic to prevent network storms.
IGMP Snooping	Allows to enable/disable the fast leave.
802.1x Port Control	Allows to configure the Port Control, Host Mode, Authentication Order, Guest VLAN, and Authentication Fail VLAN.
DHCP Snooping / ARP Inspection	Allows to configure the Port Trusted State.
QoS	Allows to configure the Trust and User Priority.
Protected Port	Allows to enable/disable the State.
IPv6 Router Advertisement Guard	Allows to configure the Policy.

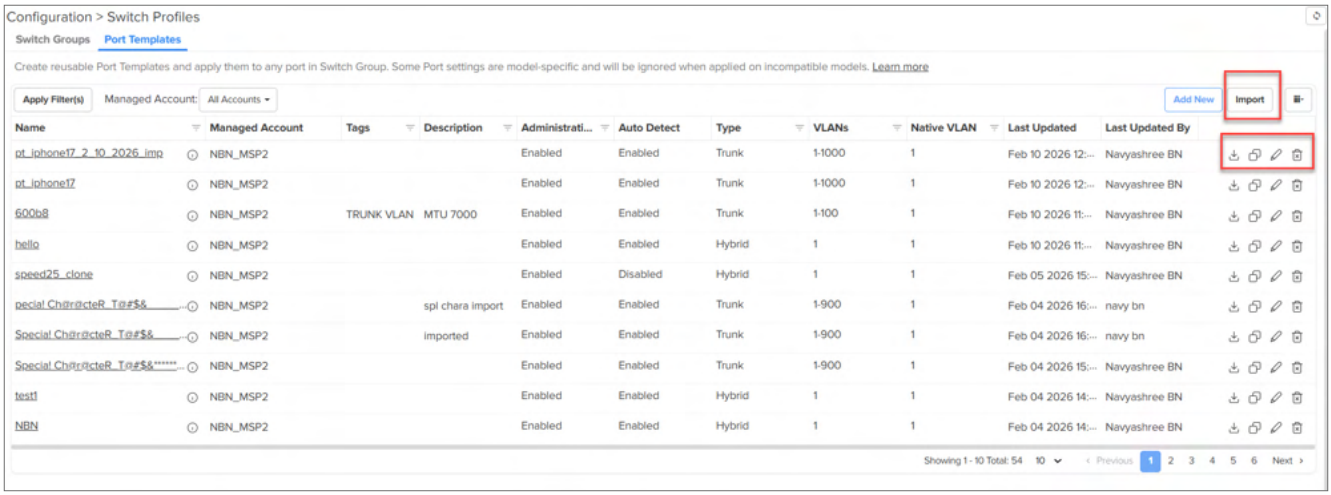
4. Click **Add**.

User can click on top bar to include additional fields in **Port Templates** Detail view.



Port Templates Operations

Port Templates can be Exported, Imported, Cloned, and Deleted.

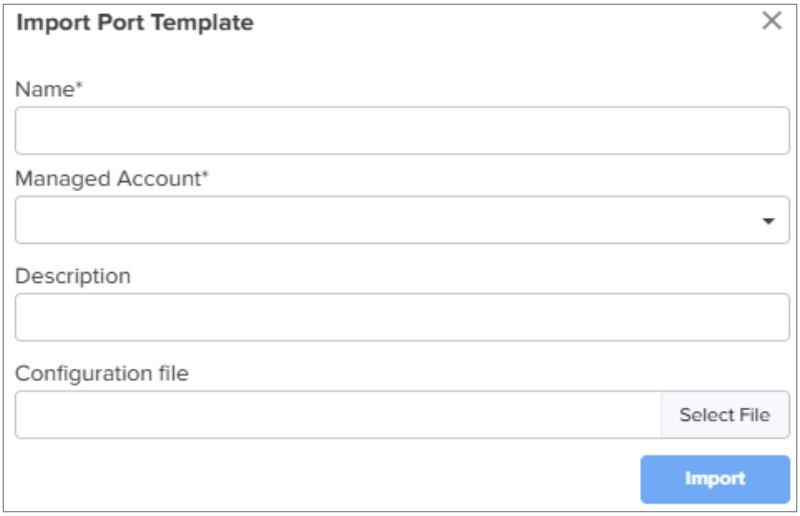


Export Port Templates

Click on the **Export** ( ) icon in the Port Templates Table to download the configuration as a JSON file.

Import Port Templates

1. Click **Import**. A dialogue box appears.
2. Enter the **Name**.
3. Select the **Managed Account** from the dropdown list.
4. Enter the **Description**.
5. Select **import.json** and import the file.



6. Click **Import.**

Clone Port Templates

Click on the **Clone** ( ) icon in the Port Templates Table to make a copy of the Port Templates.

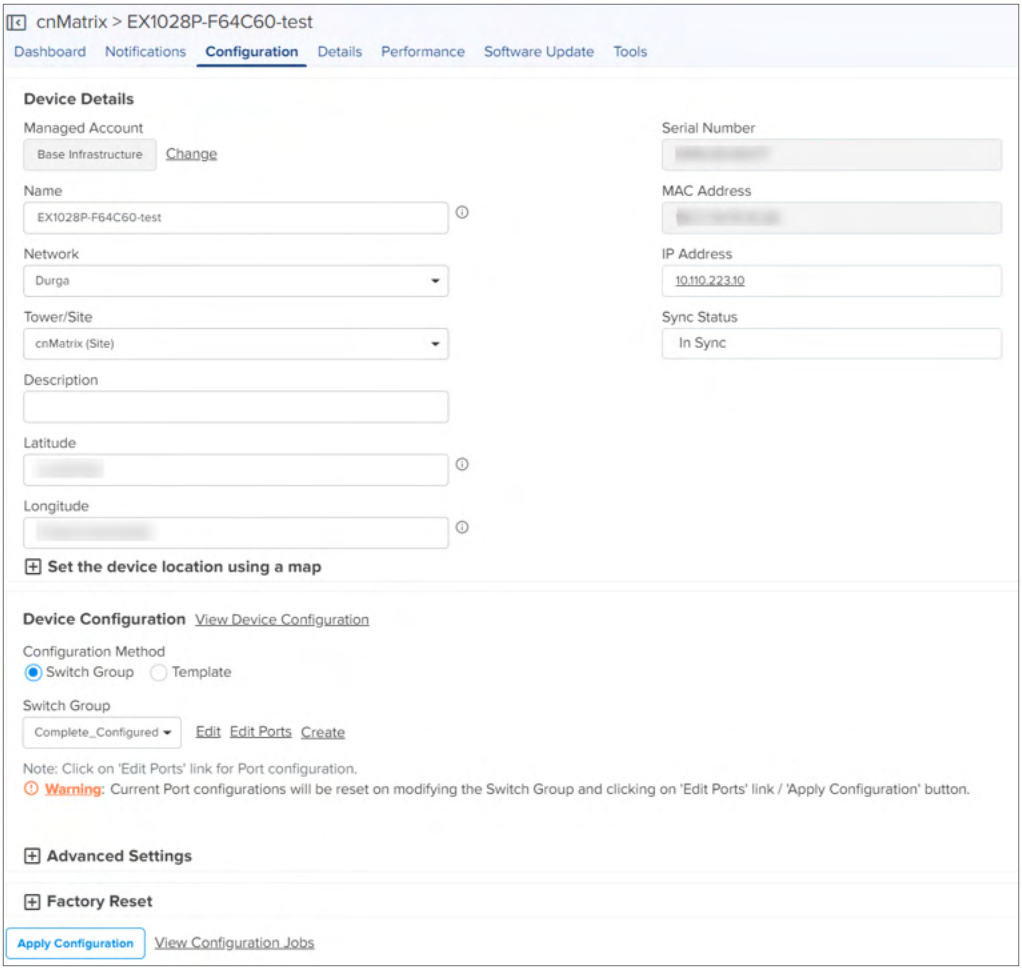
Delete Port Templates

To delete Port Templates from the list, click **Delete** icon of the specific device row.

Configuration

To configure the cnMatrix switches, perform the following:

1. Navigate to the Device **Configuration** page.
2. Enter the **Device Details, Set the service location**, and **Device Configuration.**



3. Click **Apply Configuration**.

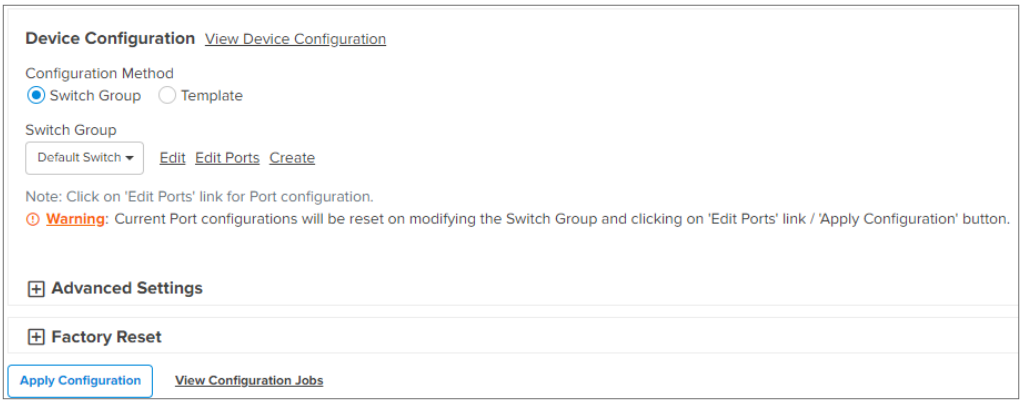
In the Configuration page, you can override the group configuration with device-specific configuration:

- cnMatrix Switch Profiles
- cnMatrix Switch Profiles
- Factory Reset

SVI VLANs allow users to create or modify Layer 3 (routable) VLAN interfaces on a switch for IP-based communication; users can add a new SVI if required or edit an existing one, configure IP addressing and routing parameters, and apply device-level overrides.

Switch Group Configuration Method

1. In **Configuration Method**, select **Switch Group** option.
2. Select a **Switch Group** from the dropdown.



   To **Edit** or **Create** a Switch Group, refer to the Switch Groups Configuration.

3. Click plus (+) sign next to **Advanced Settings** and configure for the Switch device-specific parameters.

The following are the parameters to configure:

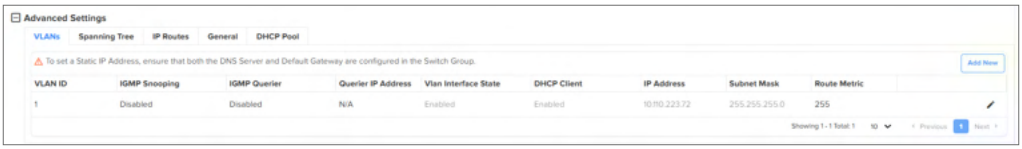
- VLANs
- Spanning Tree
- IP Routes
- General

VLANs

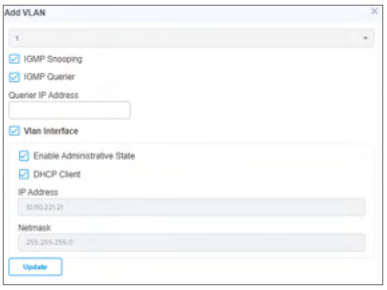
VLAN Interface allows to edit or add VLAN details such as **VLAN ID, IGMP Snooping, IGMP Querier, Querier IP Address, DHCP Client, IP Address**, and **Subnet Mask.**

Perform the following steps, to configure VLAN Interface:

1. In **Configuration** page, navigate to **VLAN Interface** tab.



2. Click **Add New** to add new LAN.
3. Click the edit (✎) icon to edit the VLAN details and click **Update.**



VLAN ID details will be displayed in the table.

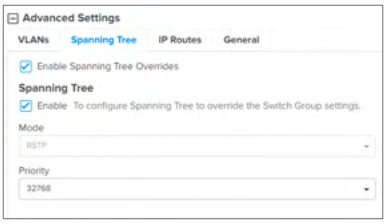
Spanning Tree

Enabling the spanning tree allows the user to configure Spanning Tree to override the Switch Group settings.

-

Perform the following to configure the Overrides:

1. In **Configuration** page, click plus (+) sign next to **Advanced Settings**.
2. Select **Enable Spanning Tree Overrides.**
3. Enter the **Spanning Tree** parameters.



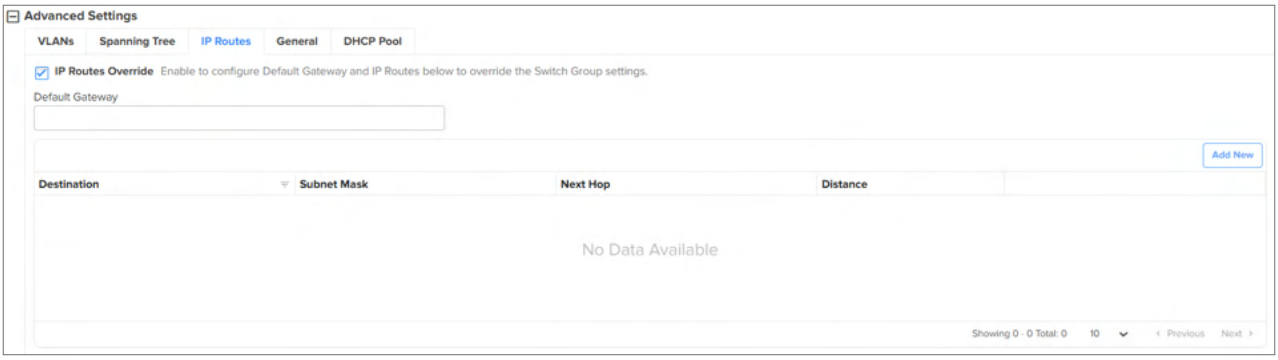
4. Select the **Priority** from the dropdown.

IP Routes

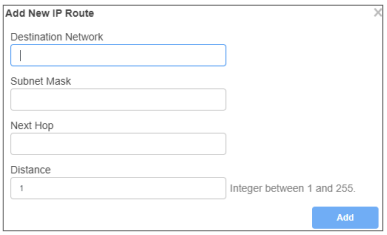
Enabling the IP Routes override allows the user to configure the Default Gateway and IP Routes to override the Switch Group.

If required, perform the following to configuration to Override:

- Configure the IP Route as follows:
- Enable the **IP Routes Override** and enter the **Default Gateway.**



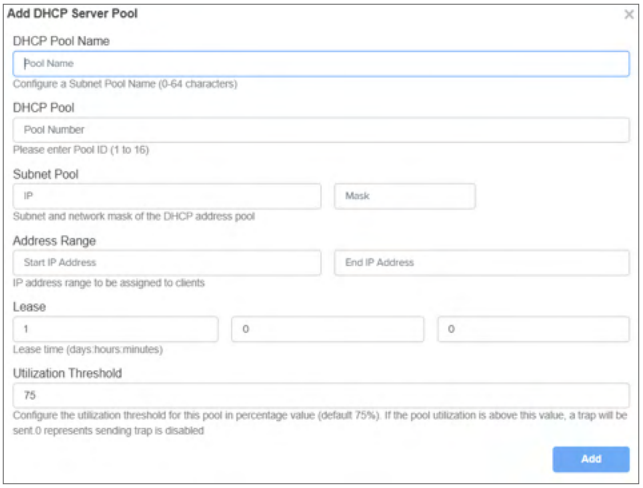
- Click **Add New**.
- Enter the parameters such as Destination Network, Subnet Mask, Next Hop, and Distance.
- Click **Add.**



Default gateway IP will override all the IPs of the Switch Groups.

General

DHCP Pool

- 

  - Enter the required parameters and click Add.

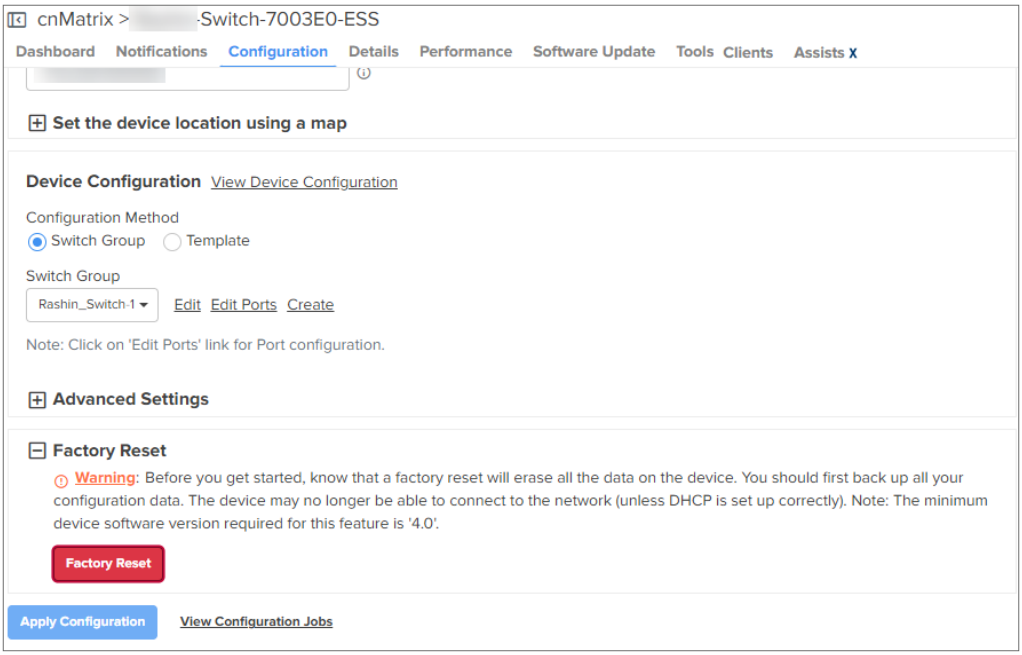
-

  - Enter the required parameters and click Add.

Factory Reset

To erase all the configuration on the device and bring the device back to the default factory configuration, complete the following steps:

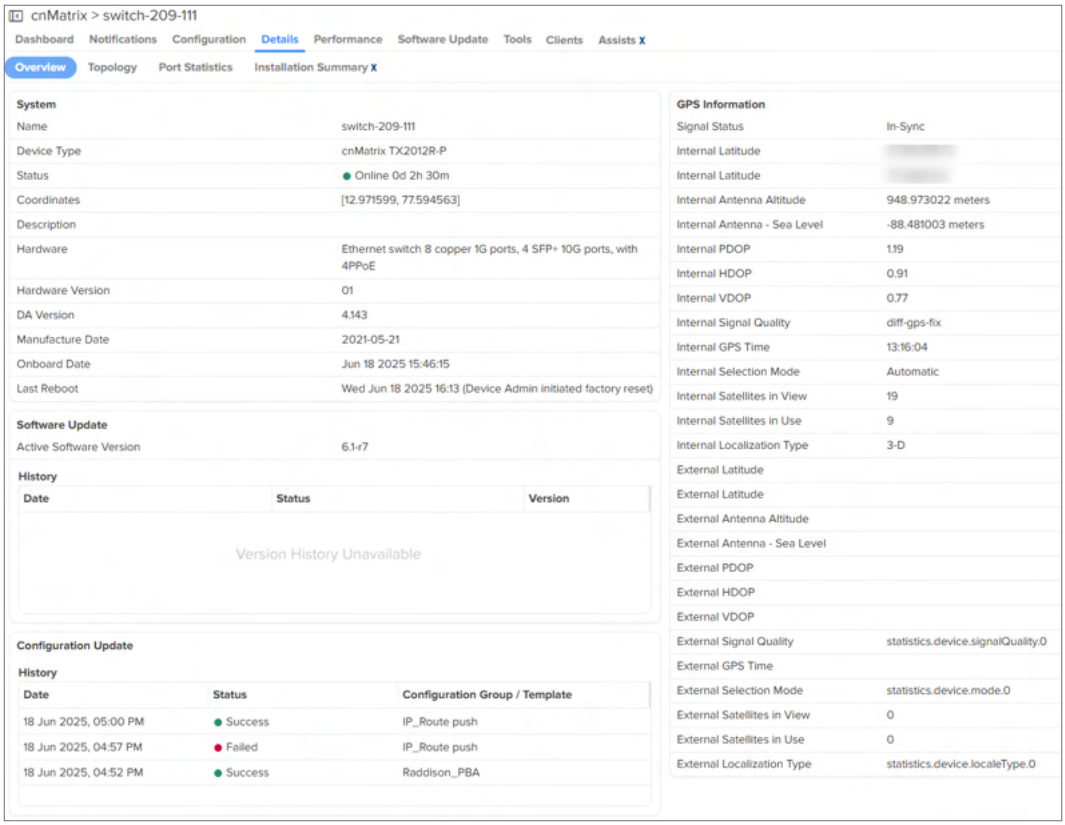
1. Navigate to the cnMatrix device **Configuration** page.
2. Expand the **Factory Reset** section and click **Factory Reset**.



3. In the pop-up window that appears, click **Yes, Factory reset**.

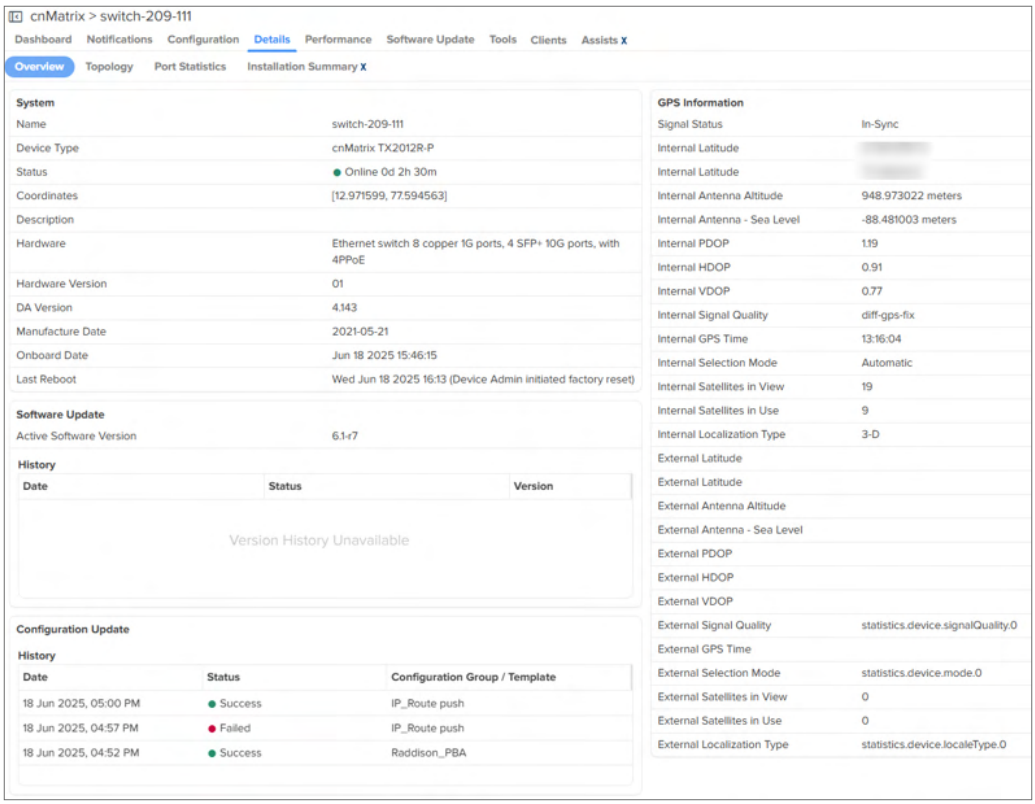
Device Details

Details page provides the information about the switches **Overview**, **Topology**, **Port Statistics**, and **Installation Summary**.



Details Overview

To view the details of the overview page, navigate to the **Details > Overview** tab.

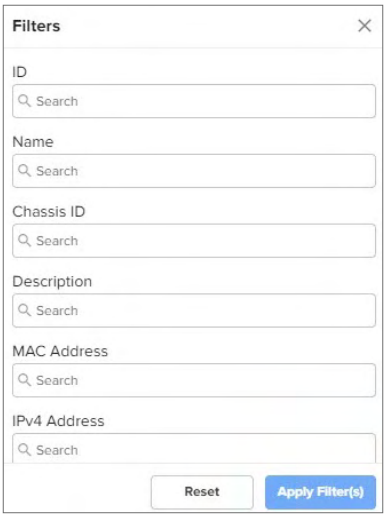


Topology

To view the details of the Topology page, navigate to the **Details** > **Topology** tab.

To apply filters, follow the steps below:

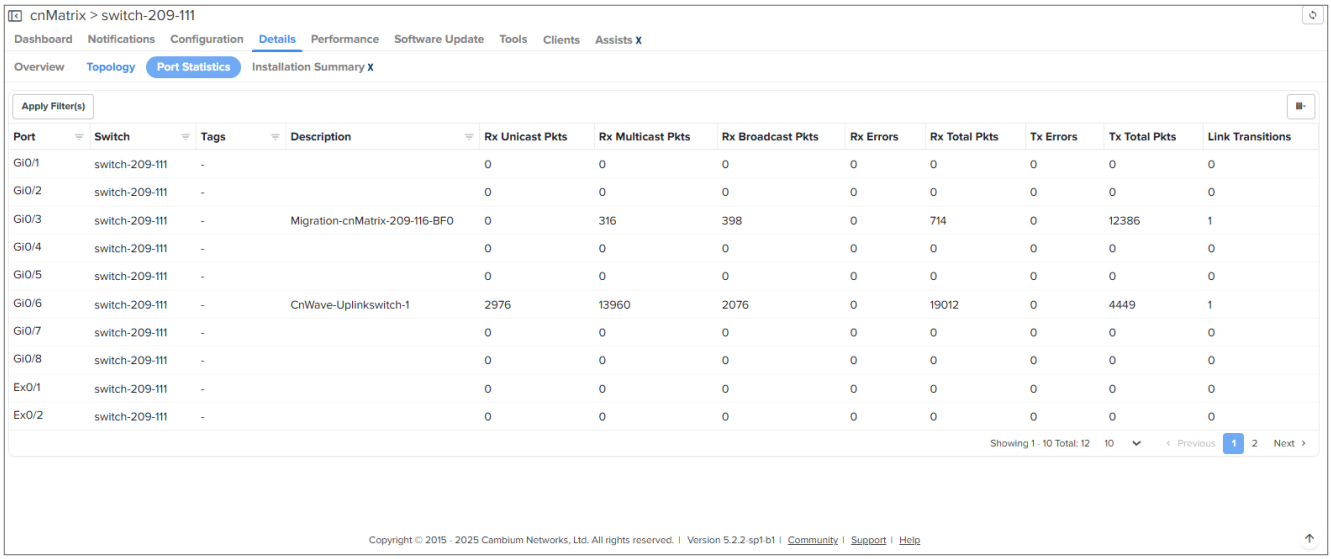
1. Click on the **Apply Filter(s)** tab.
2. A new window titled **Filters** appears.



3. Enter information in any field based on your filtering needs.
4. Click on **Apply Filter(s)**.

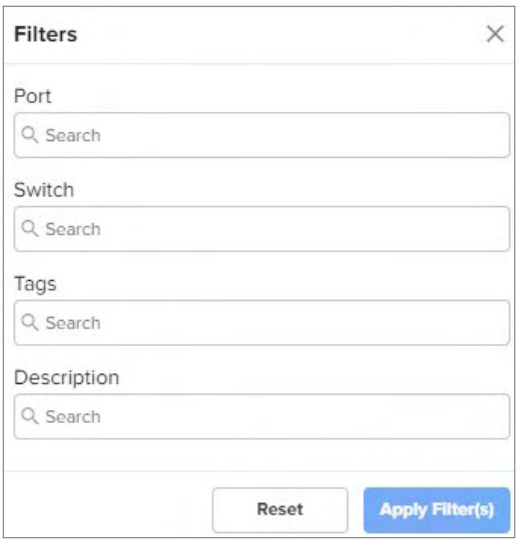
Port Statistics

To view the details of the Port Statistics page, navigate to the **Details** > **Port Statistics** tab.



To apply filters, follow the steps below:

1. Click on the **Apply Filter(s)** tab.
2. A new window titled **Filters** appears.



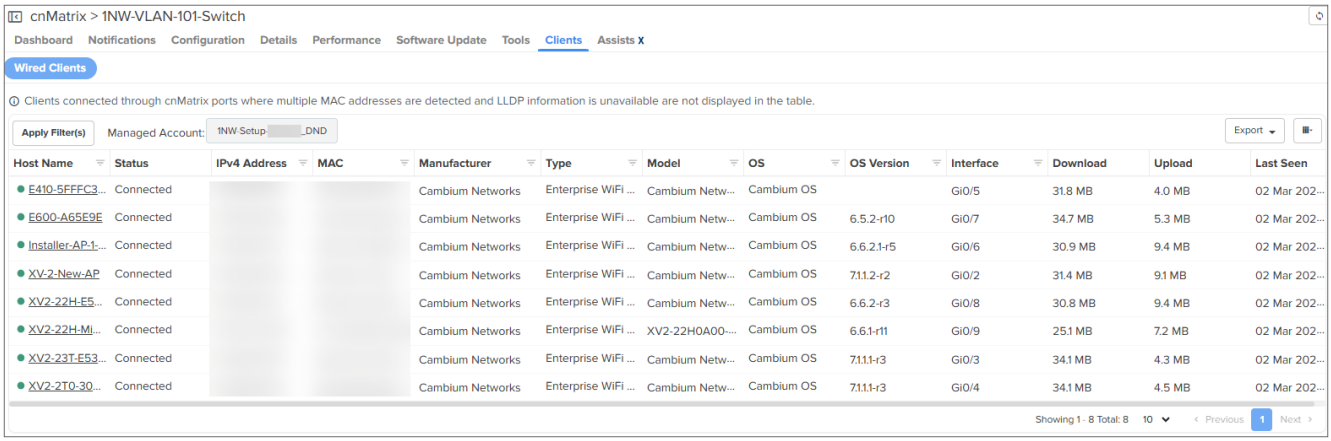
3. Enter information in any field based on your filtering needs.
4. Click on **Apply Filter(s)**.

Clients

Note

The Wired Clients feature is supported from cnMaestro version 5.0.3 or later.

The Wired Clients table displays real-time information about clients discovered through LLDP and related device.



The **Clients** > **Wired Clients** page at the Network- and Site-level displays the following details:

- **General**
  - Host Name
  - Manufacturer
  - Type
  - Model
  - OS
  - OS Version
  - Download
  - Upload
  - Status
  - Last Seen
- **Network**
  - IPv4 Address
  - MAC
  - Interface

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.

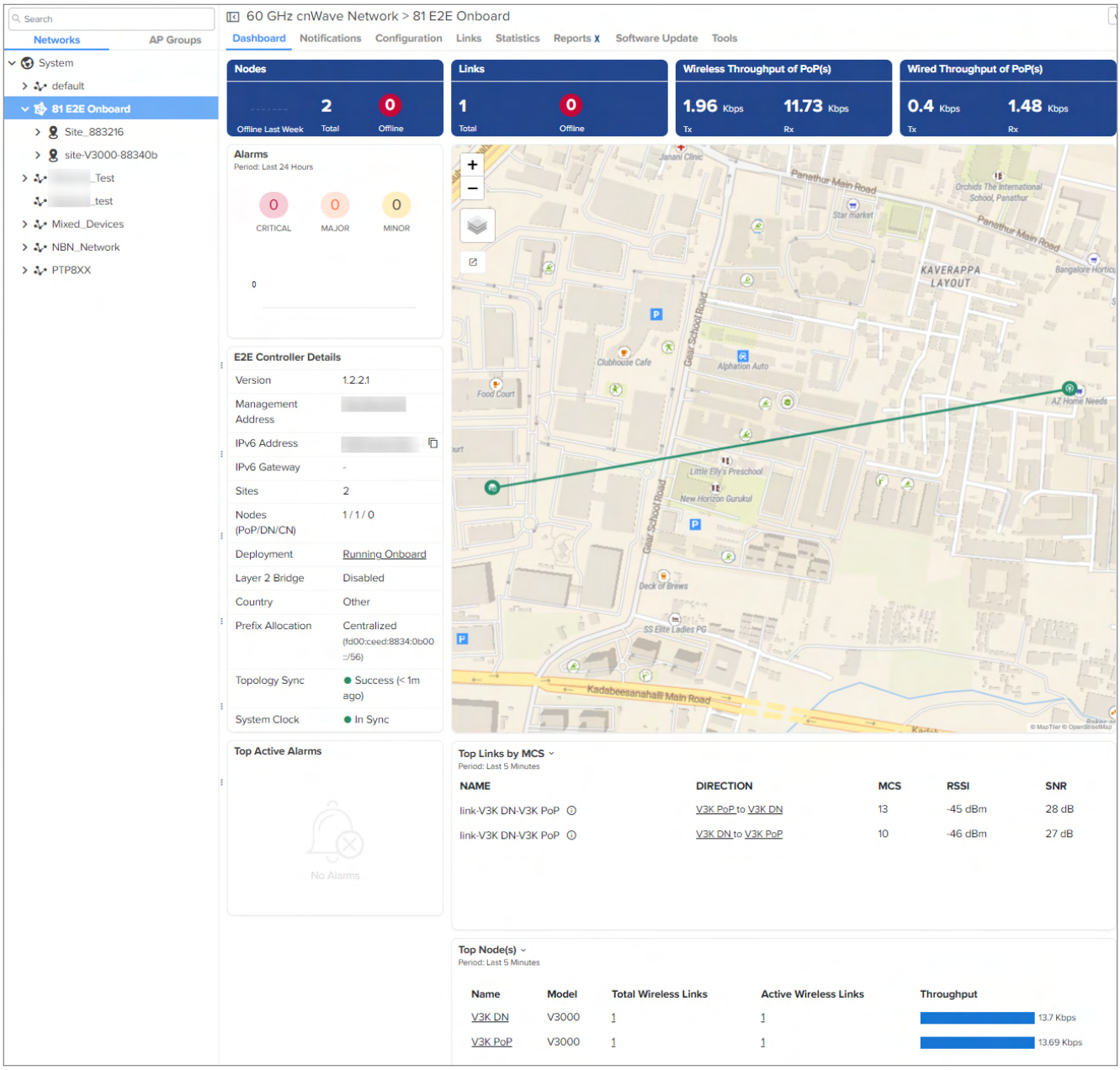
Managing E2E Network

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

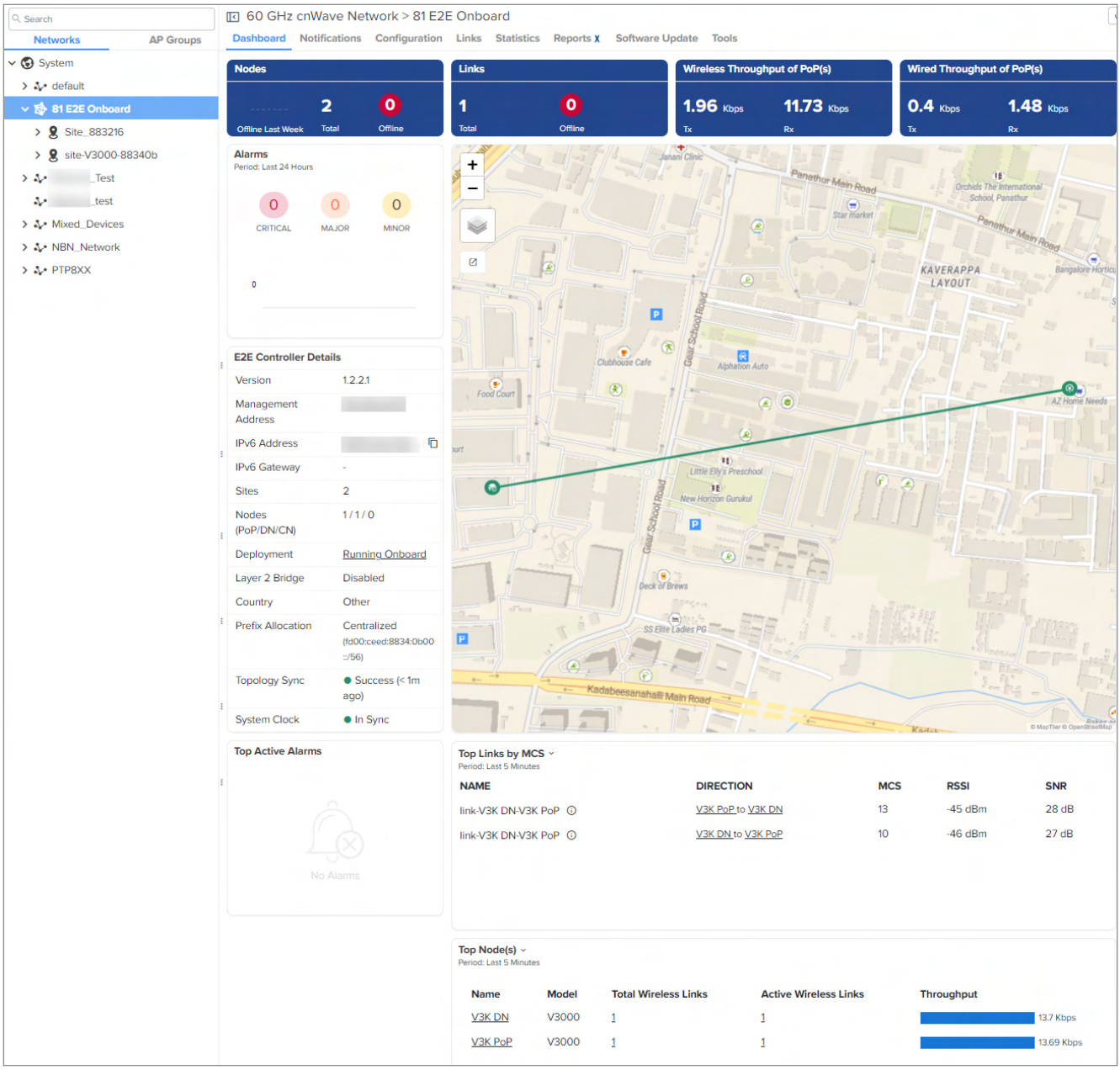
Dashboard pages are customized for each device type and aggregation level (such as E2E Network, Node, and Site). The dashboard section displays the **Nodes, Links, Auto Manage IPv6 Routes, Wireless Throughput of PoP (s), Wired Throughput of PoP(s), Alarms, E2E Controller Details, Top Active Alarms, Map, 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).**



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.



E2E Controller Details

E2E Controller Details displays the details such as **Version**, **Management Address, IPv6 Address, IPv6 Gateway, Sites, Nodes, Onboarding 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.**

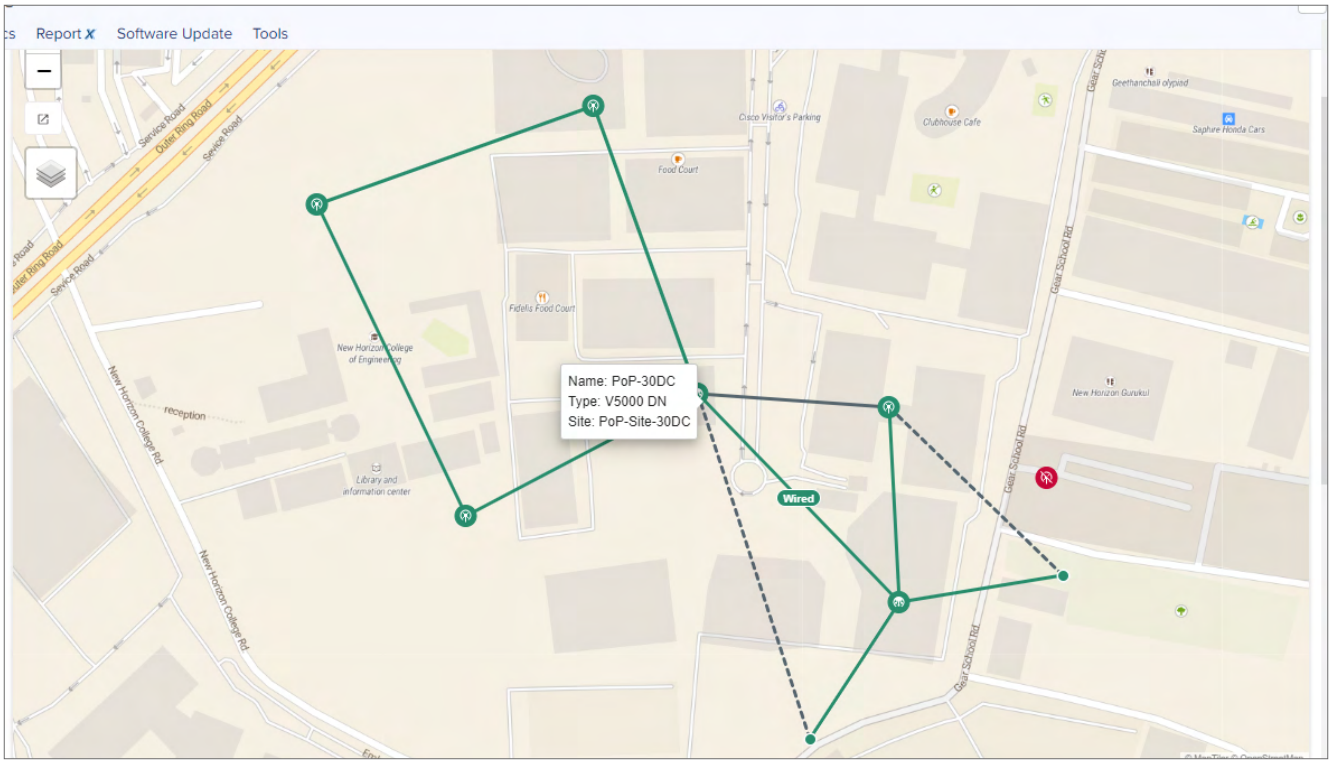
E2E Controller Details	
Version	1.1
Management Address	10.110.221.242
IPv6 Address	fd00:ba5e:88:3083::88:3...
IPv6 Gateway	-
Sites	4
Nodes (PoP/DN/CN)	1 / 0 / 1
Deployment	Running Onboard
Layer 2 Bridge	Disabled
Country	Belgium
Prefix Allocation	Deterministic (fd00:ceed:8830:8300::/56)
Topology Sync	Success (6m ago)
System Clock	In Sync

- If External E2E controller is managed by cnMaestro, it displays deployment as **External.**

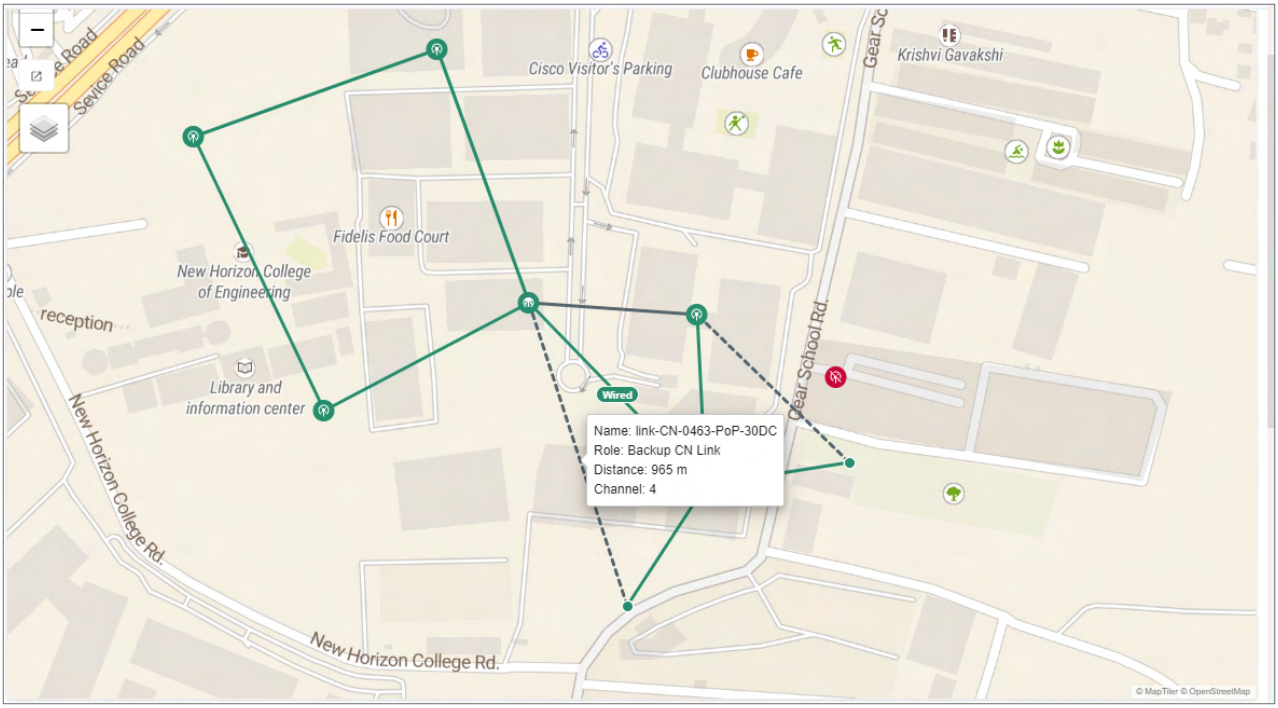
E2E Controller Details	
Version	1.1
Management Address	10.110.221.232
IPv6 Address	fd20:ba5e::100
IPv6 Gateway	fd20:ba5e::5
Sites	4
Nodes (PoP/DN/CN)	1 / 0 / 2
Deployment	External
Layer 2 Bridge	Disabled
Country	Other
Prefix Allocation	Centralized (fd00:ceed:17a1:1600::/56)
Topology Sync	Success (4m ago)
System Clock	In Sync

Dashboard Maps

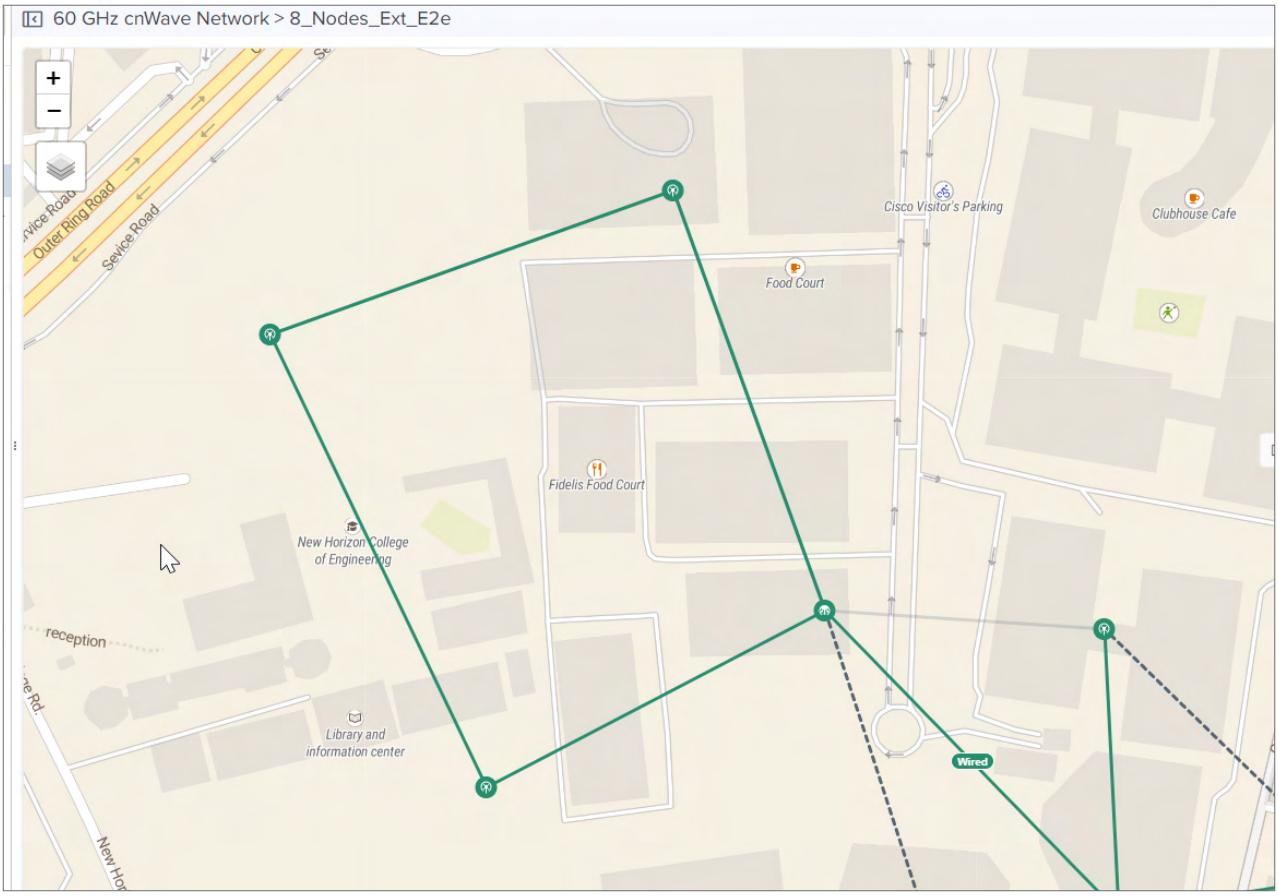
In the dashboard map, when user hovers on particular **PoP, DN** or **CN** it pops-up the device details. When user hovers on particular link it pops up the link details.



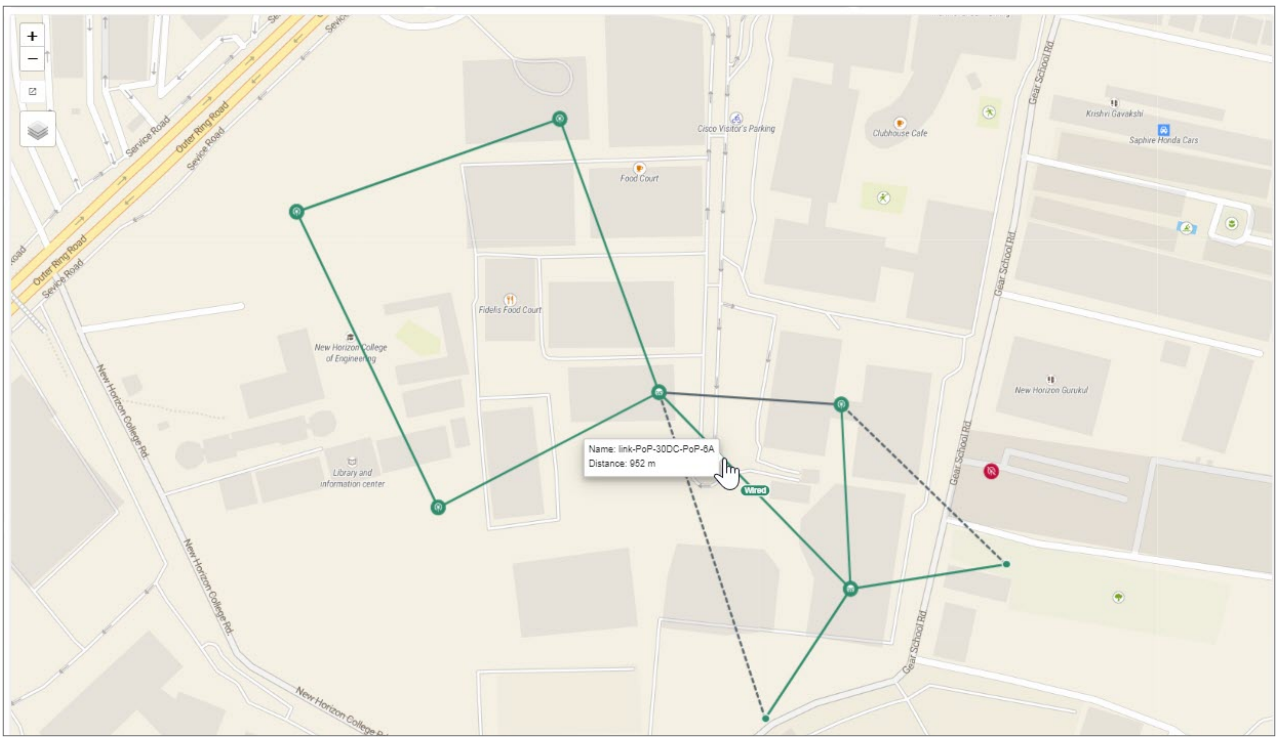
- Dotted line displays the Backup CN link between the DN and CN..



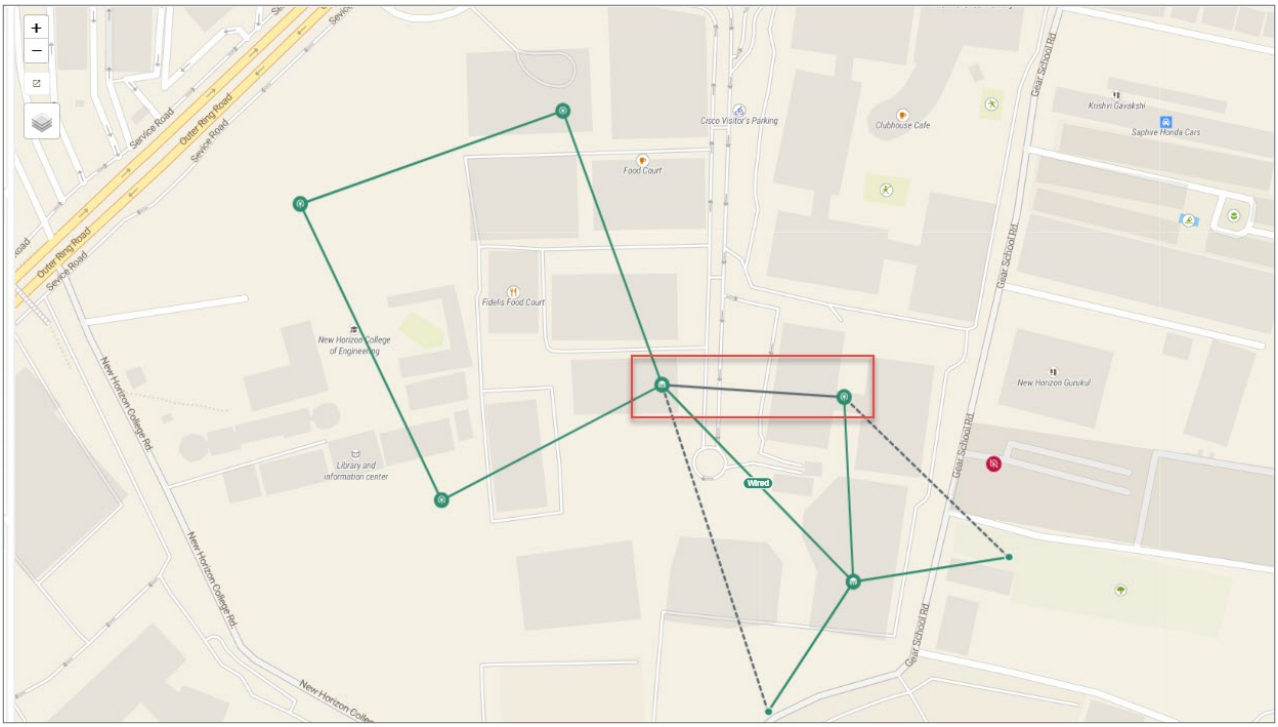
- Continuous line display the wireless link between PoP, DN, or CN..



- 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:

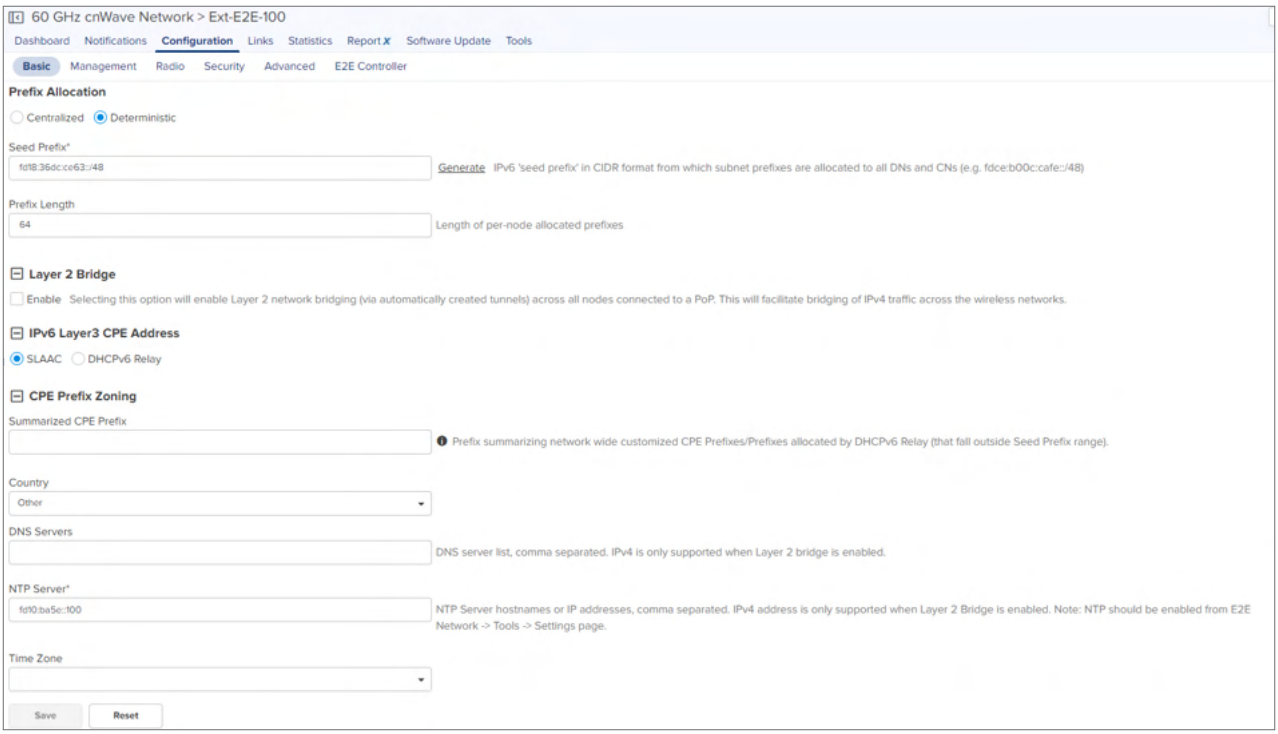
- Basic
- Management
- Radio
- Security
- Advanced
- E2E Controller
- High Availability X

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.



> **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 verison 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.

- If user selects **IPv6 Layer3 CPE Address** as **DHCPv6 Relay.**

  User can configure the DHCPv6 server address.

> **Note**
>
> - By default **Country** is **Other**, user can configure it.
> - By default **Enabled Radio Channels** is 2, user can configure channel if required.
> - Enter the **Hostnames** or **IP address** of NTP server.

2. In **CPE Prefix Zoning** enter **Summarized CPE Prefix**.
3. Select the **Country** from the dropdown.
4. Enter the channel number in **Enable Radio Channels.**
5. Enter the **DNS Server.**
6. Enter **NTP Server.**
7. Select the **Time Zone** from the dropdown.

> **Note**
>
> By default **Wireless Scans** will be disabled.

8. Click **Save.**

Management

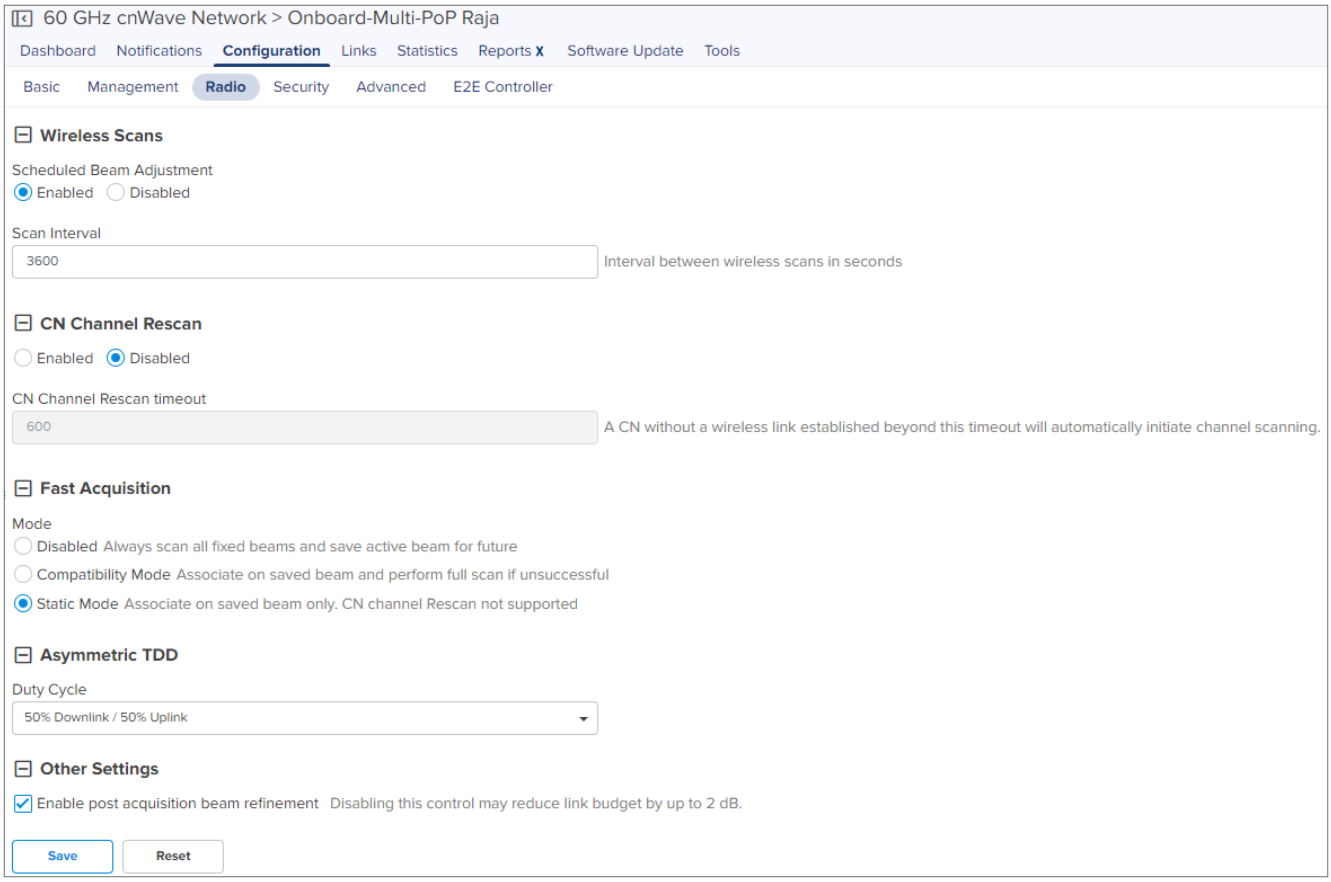
Management configuration allows user to configure and manage the credentials of the administrator and it allows enable **SNMP**.

1. Navigate to **Configuration** > **Management** to set the **Device GUI Passwords** and to enable the **SNMP**.

2. Click **Save.**

Radio

The Radio page manages the Radio related settings.



- **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.

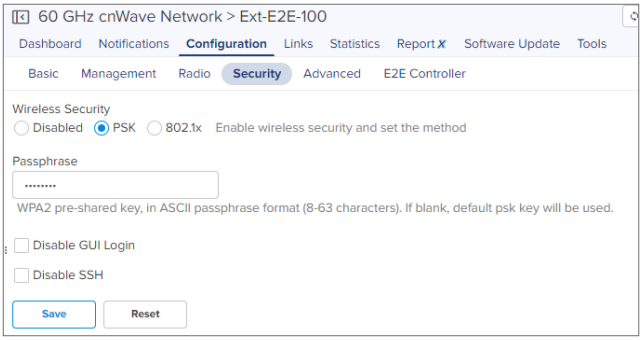
- **Asymmetric TDD**
  - **Duty Cycle**—Select a duty cycle from the dropdown list. For example:
    - **60% Downlink / 40% Uplink**—Set 60% of physical bandwidth for downloading and 40% of the physical bandwidth for uploading.
- **Other Settings**
  - **Enable post acquisition beam refinement**—Select 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**.



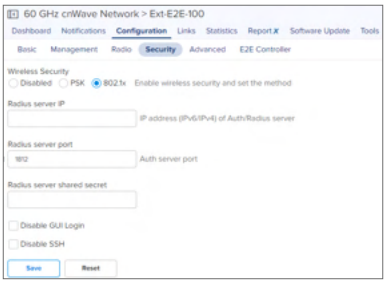
3. Enter the **Passphrase**.

> **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**.



3. Enter the **Radius server IP.**

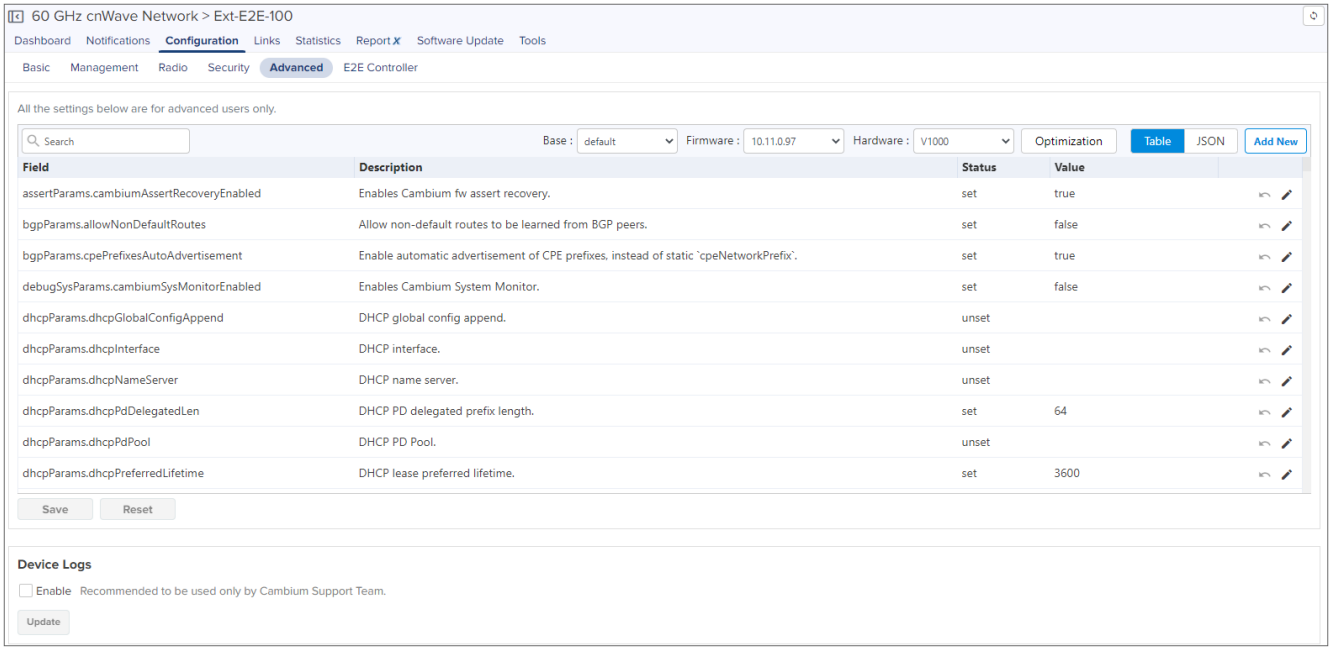
4. Enter the **Radius Server port.**
5. Enter the **Radius Server Shared Secret.**
6. Click **Save**.

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 polarity Allocation
- Optimize Control Superframe Allocation
- Optimize DPA Zone Allocation
- Clear Node Auto Configuration

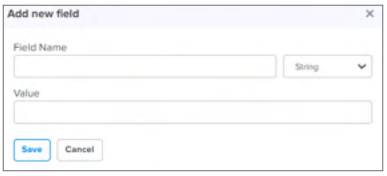


Table

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:

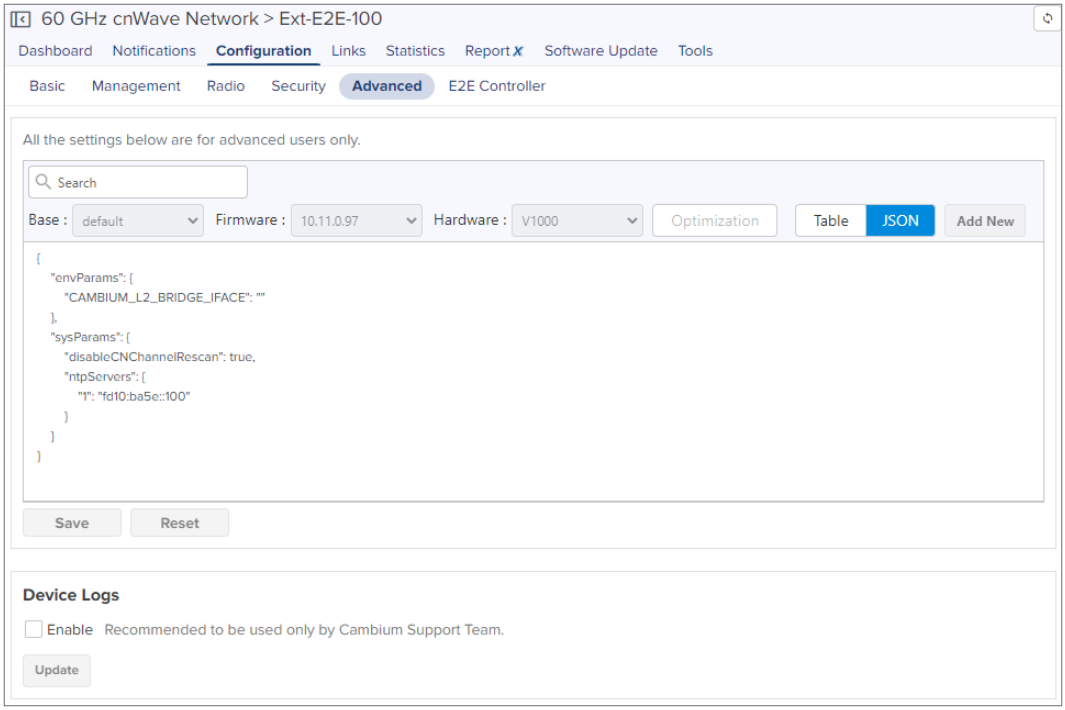
1. Navigate to **Configuration** > **Advanced.**
2. Click **Add New.**
3. Enter the **Field Name** and **Value.**



4. Click **Save.**

JSON

JSON allows Advanced user to download or view and edit in json format.



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.**

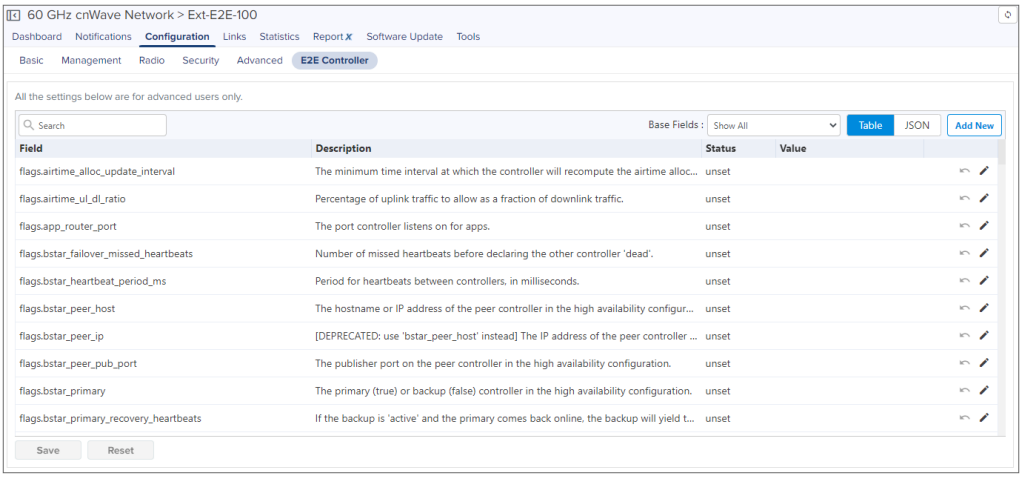
E2E Controller

Table

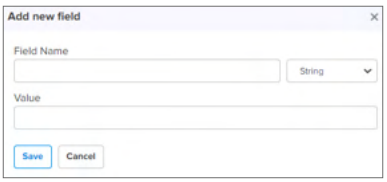
In **E2E Controller Table** user can edit or add **Field Name** and **Value.**

To Add Field:

1. Navigate to **Configuration** > **E2E Controller.**
2. Click **Add New.**



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.

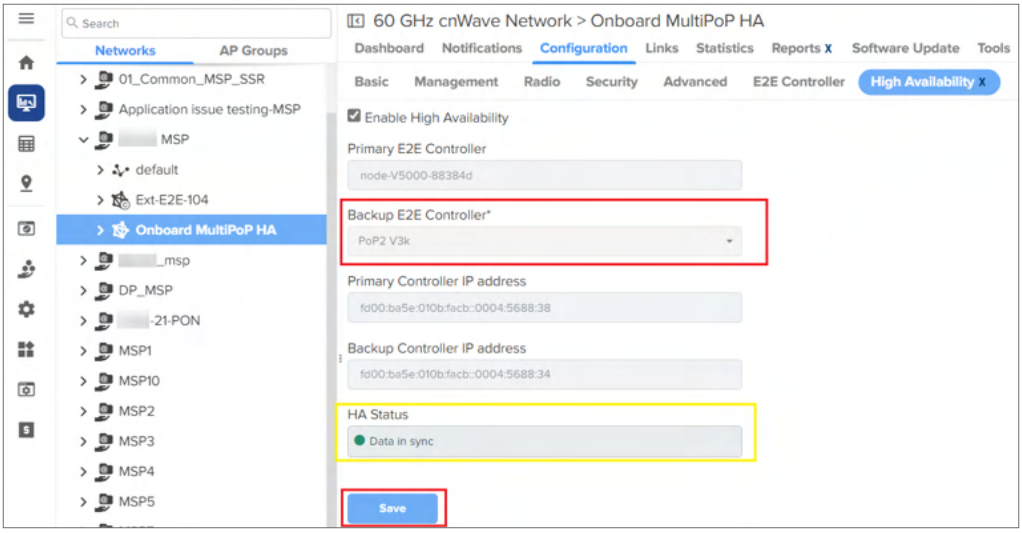
To enable the HA support for E2E Controller, complete the following steps:

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.



3. From the **Backup E2E Controller** dropdown list, select the required node that is connected to the complete network.

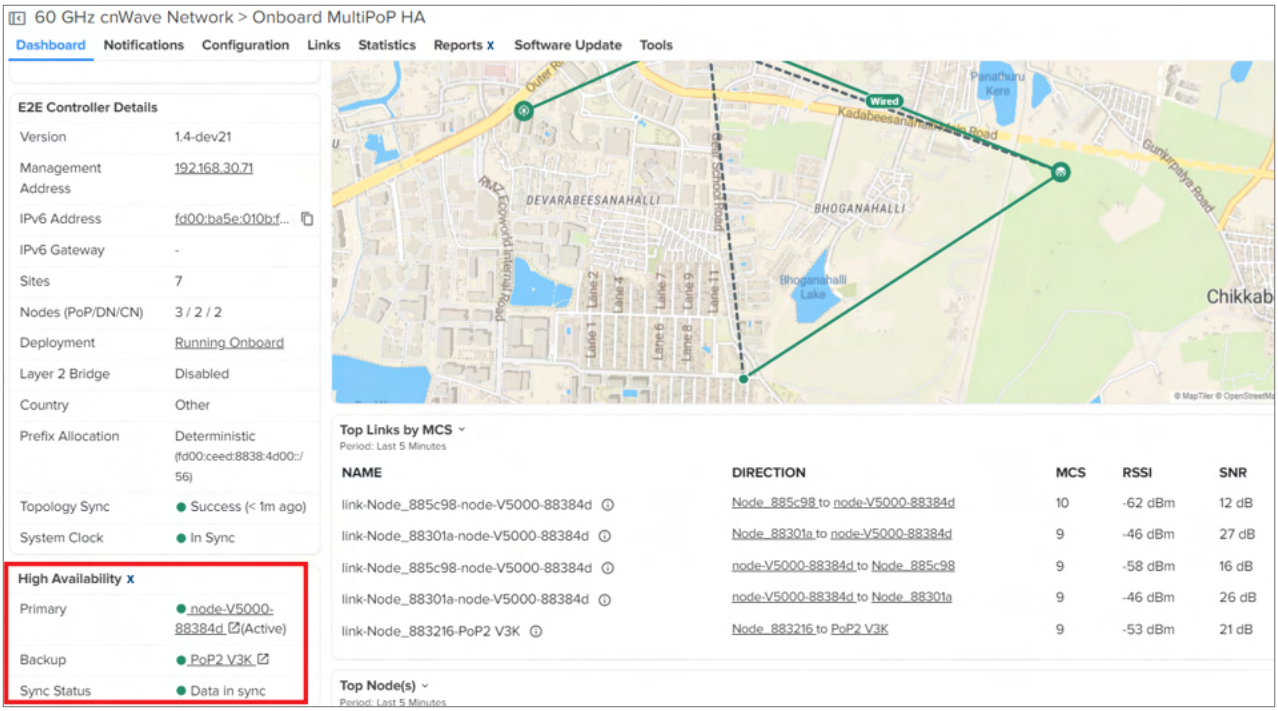
   You can check the IP addresses (read only) of primary and backup controllers.

4. Click **Save** to apply the changes.

5. 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 **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 82 *Caveats of HA configuration*

Configuration	Caveats
Configuration backup and restoration	• 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	• 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	• 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	• 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	• 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.

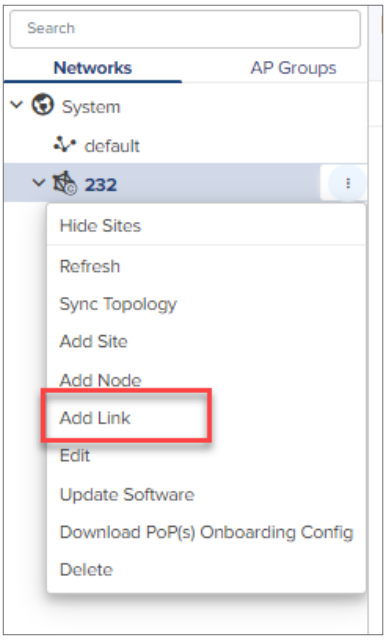
- List
- Statistics
- Events

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.

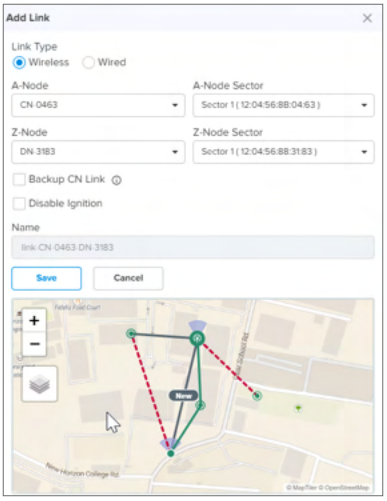
To add a link, perform the following steps:

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**.



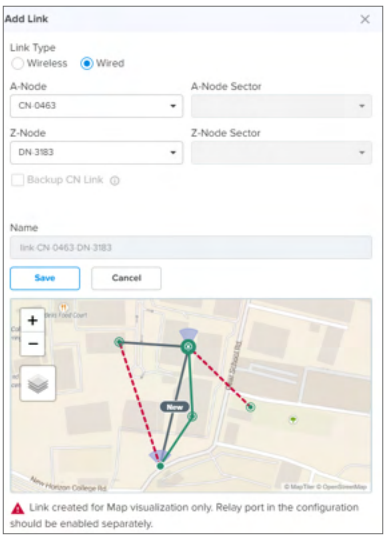
2. **Add Link** window pops-up.
3. Select **Link Type** Wireless or Wired.

Figure 304 *Wireless link*

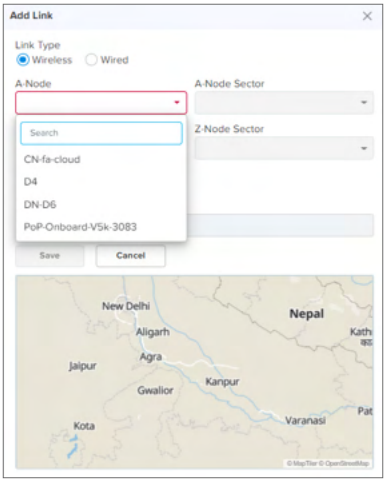


> **Note**
>
> In Wired Link Type, add Sector is disabled.

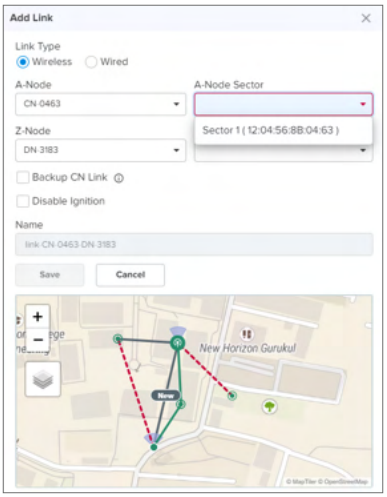
Figure 305 *Wired link*



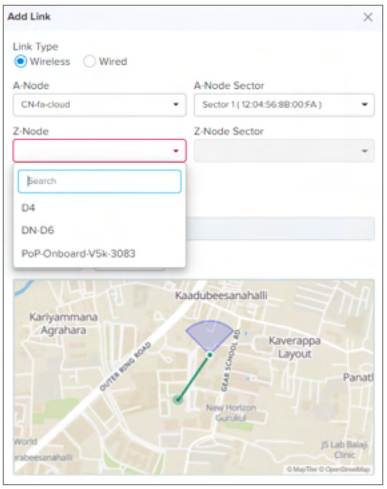
4. Select the **Node** from the dropdown in **A-Node.**



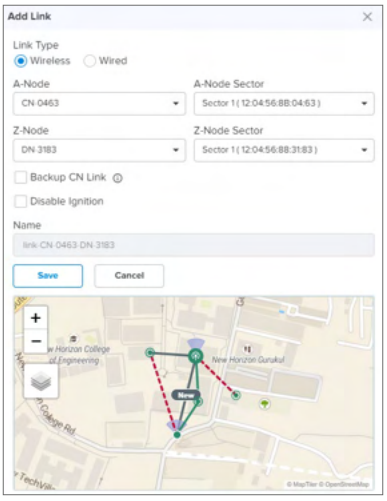
5. Select the **Sector** of the node from the dropdown in **A-Node Sector.**



6. Select the **Node** from the dropdown in **Z-Node.**

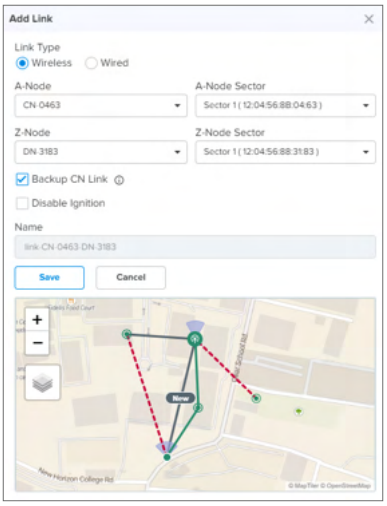


7. Select the **Sector** of the node from the dropdown in **Z-Node Sector.**

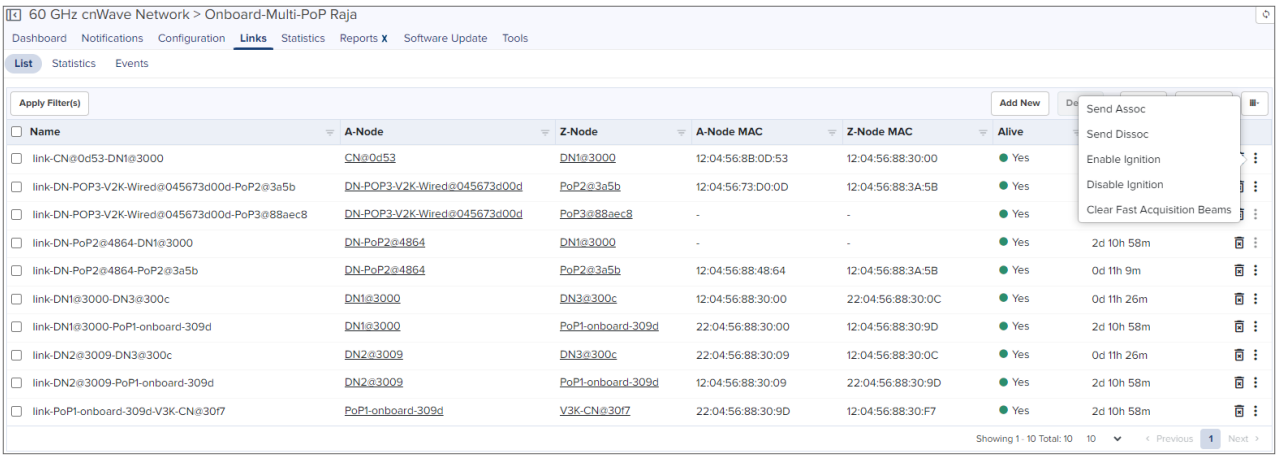


8. Enable the **Backup CN Link**.

   - 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.



9. Click **Save**.
10. Once the link is successful it displays the **Alive** status as **Yes**.



Available link options are:

- Send Assoc
- Send Dissoc
- Enable Ignition
- Disable Ignition
- Clear Fast Acquisition Beams

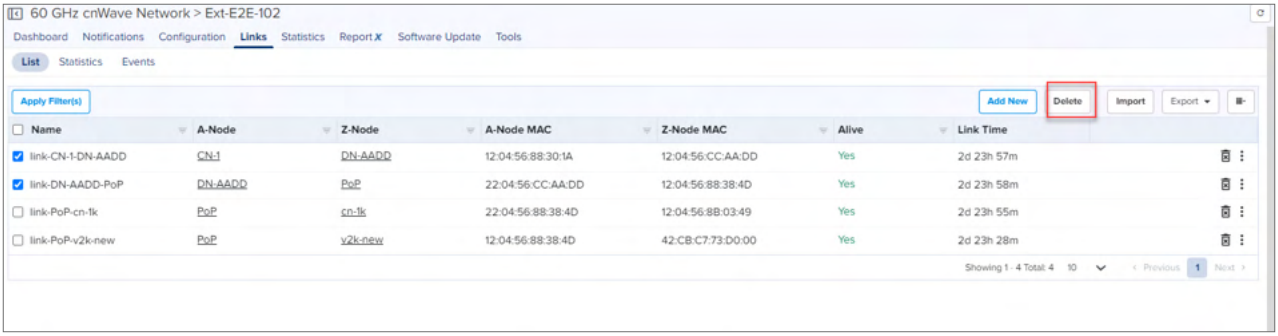
Delete Links

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.



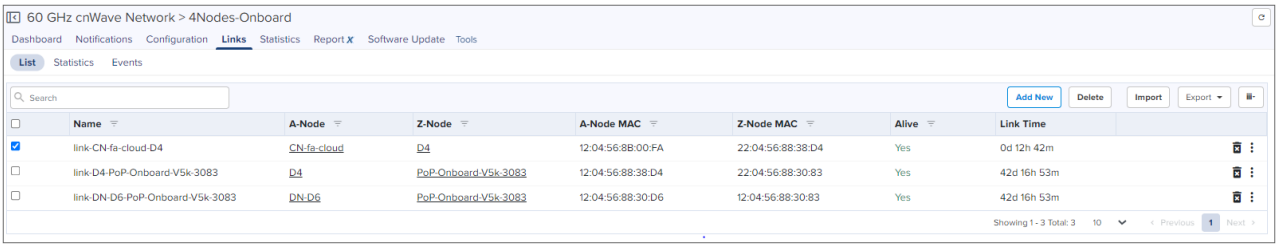
1. Click **Delete**.

Import List

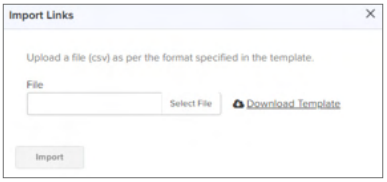
In **Links** tab you can import the E2E Controller Network Links.

To import the links:

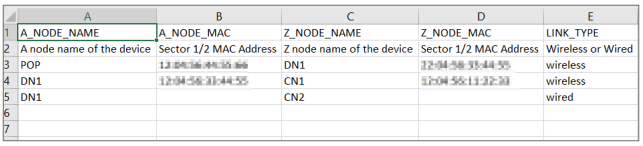
1. Navigate to **Links > List.**
2. Select **Import.**



3. **Import Links** pops-up.



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	[illegible]	DN1	12:04:56:31:44:55	wireless
4	DN1	12:04:56:31:44:55	CN1	[illegible]	wireless
5	DN1		CN2		wired
6					
7					

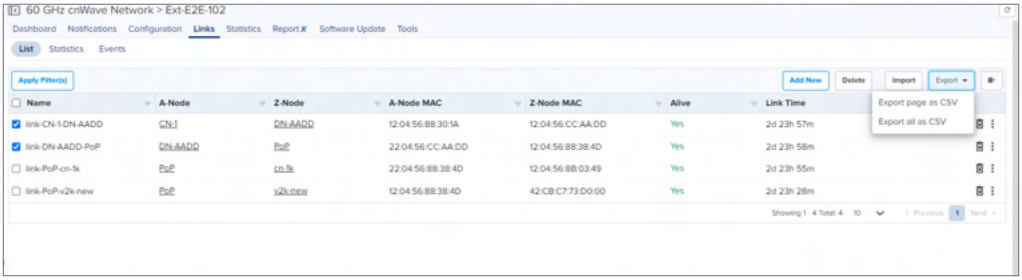
5. Select the file and click **Import**.

Export List

In **Links** tab you can export the E2E Controller Network Links.

To export the links:

1. Navigate to **Links** > **List** > select **Export.**

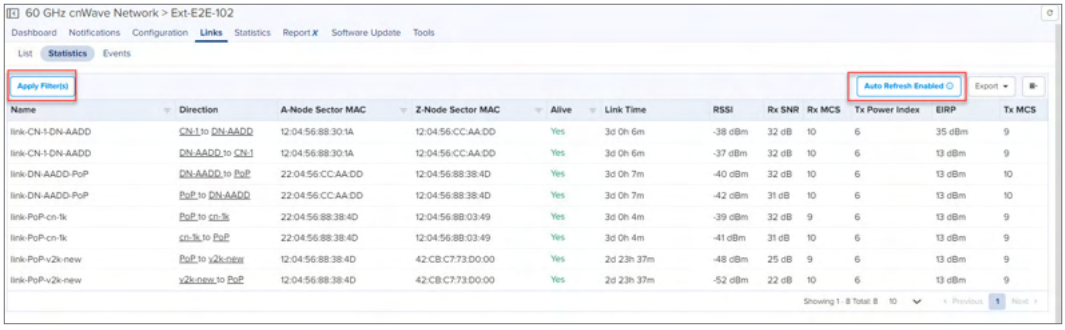


2. Data is exported in the.CSV file format as shown below.

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_N	Z_NODE_N	LINK_TYPE	ALIVE	IGNITION_	DISTANCE	AZIMUTH	BACKUP_C	IGNITION_	TIMESTAMP		
Link Name	A node nai	Sector 1/2	Z node nar	Sector 1/2	Wireless o	Yes/No	Ignition At	Distance b	Azimuth (D	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		

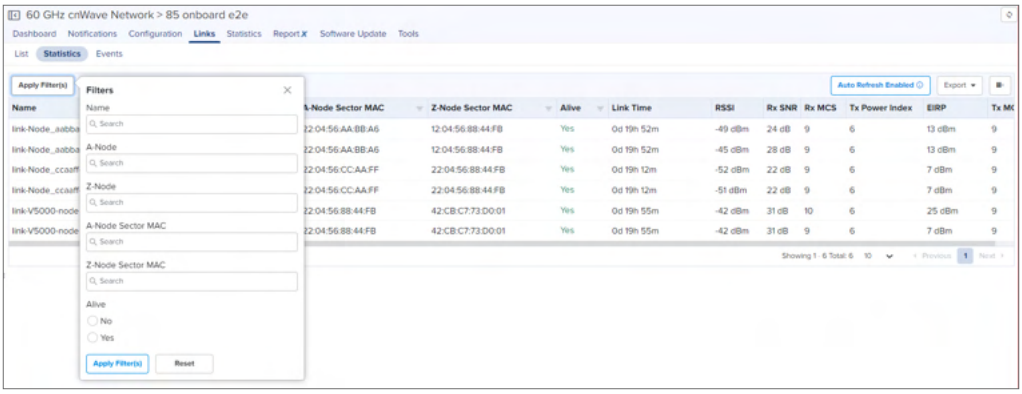
Statistics

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.

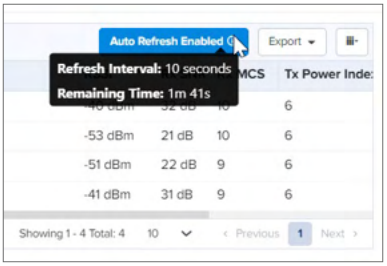


You can **Apply Filter(s)** for Name, A-Node, Z-Node, A-Node Sector MAC, Z-Node Sector MAC, and Alive. The **Auto Refresh** option allows to refresh data automatically as per Refresh Interval, which is configured for five minutes. By default, Refresh Interval is 10 seconds. This option gets disabled 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.**



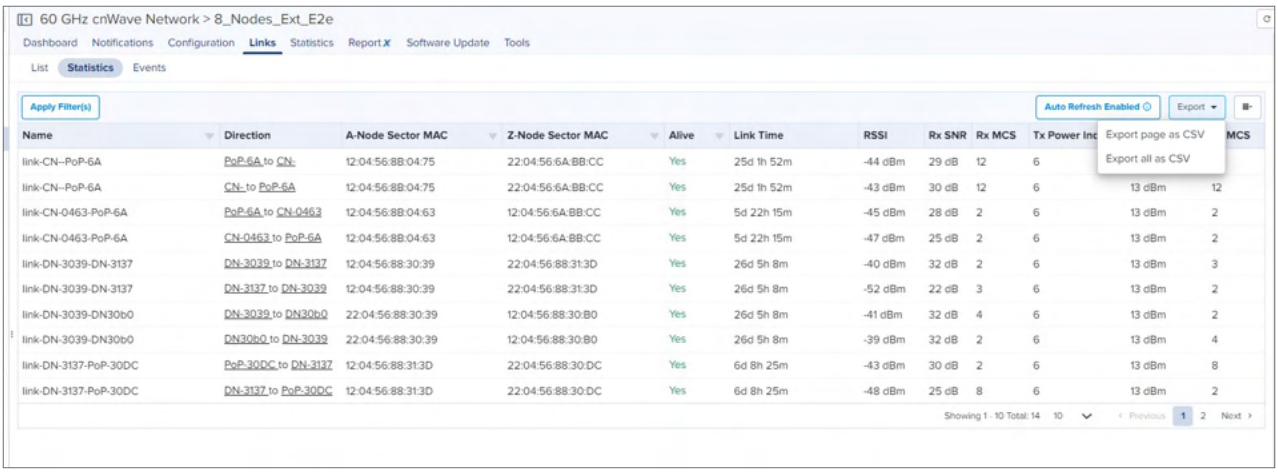
4. Click the info icon to view **Refresh Interval** and **Remaining Time**.



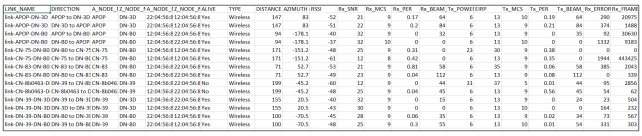
Export Statistics

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_LT	Z_NODE_LT	A_NODE_F	Z_NODE_F	ALIVE	TYPE	DISTANCE	AZIMUTH	RSSI	Rx_SNR	Rx_MCS	Rx_PER	Rx_BEAM_I	Tx_POWER	EIRP	Tx_MCS	Tx_PER	Tx_BEAM_I	Rx_ERROR	Rx_FRAME
link-APOP-DN-30	APOP to DN-30	APOP	DN-30	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	20875
link-APOP-DN-30	DN-30 to APOP	APOP	DN-30	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	10630
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	0.18	0	0	0
link-CN-75-DN-80	CN-75 to DN-80	CN-75	DN-80	12:04:56:8	12:04:56:8	Yes	Wireless	171	-151.2	-61	12	8	0.62	0	6	13	9	0.35	0	1944	443425
link-CN-83-DN-80	CN-83 to DN-80	CN-83	DN-80	12:04:56:8	22:04:56:8	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	22:04:56:8	Yes	Wireless	71	52.7	-49	23	9	0.04	112	6	13	9	0.08	112	0	339
link-CN-B0463-D	CN-B0463 to DN-39	CN-B0463	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-B0463-D	CN-B0463 to DN-39	CN-B0463	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-30	DN-30 to DN-39	DN-39	DN-30	22:04:56:8	22:04:56:8	Yes	Wireless	150	20.5	-40	32	9	0	15	6	13	9	0	24	23	504
link-DN-39-DN-30	DN-30 to DN-39	DN-30	DN-39	22:04:56:8	22:04:56:8	Yes	Wireless	150	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-80	DN-39	22:04:56:8	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-39	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 306 *Links > Events*

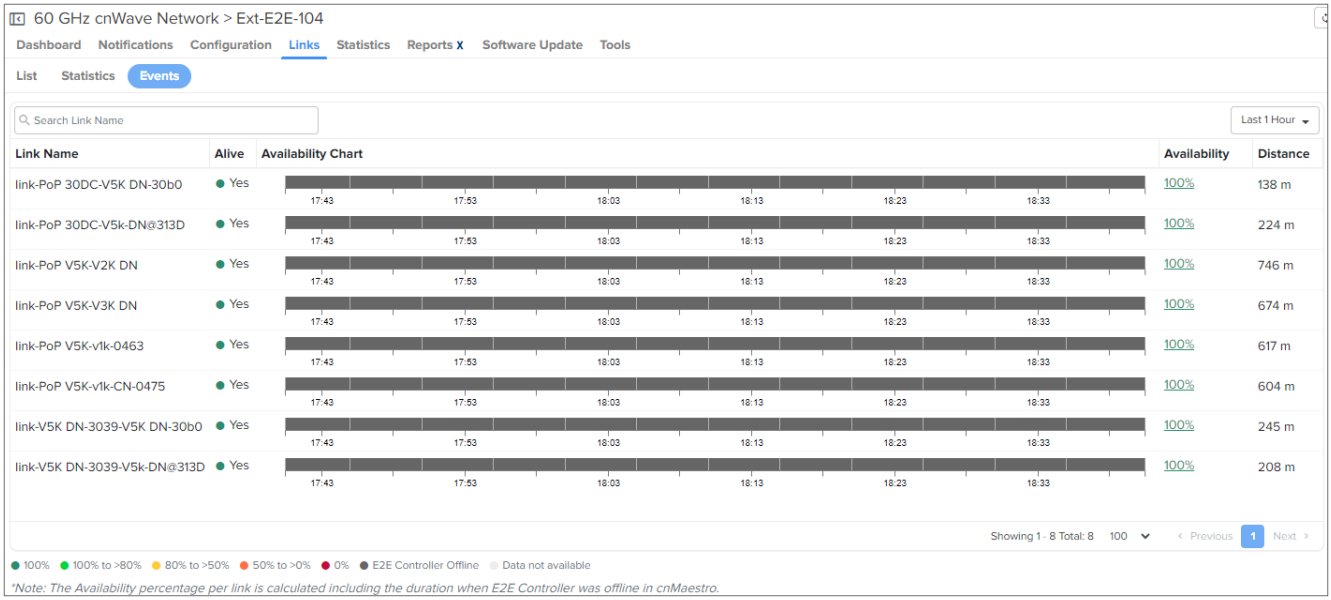
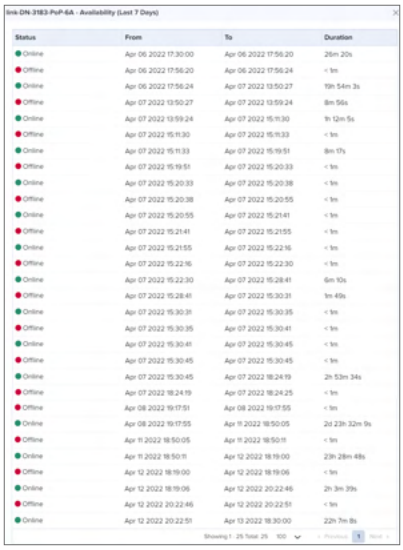


Table 83 *Events fields*

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: • 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. Hover on the link to see the hourly availability as shown in Figure 308. Clicking on percentage link availability displays pop-up window as shown in Figure 309 Link availability is presented in different colors in the chart as shown in Figure 307
Availability Percentage	Availability of link is shown in percentage in the Availability column as shown in Figure 308.
Distance	Distance of the link in meters.

Figure 307 *Link Availability in Percentage*



Availability percentage per link is calculated including the duration when E2E Controller was Offline in cnMaestro.

Figure 308 *Link Availability*

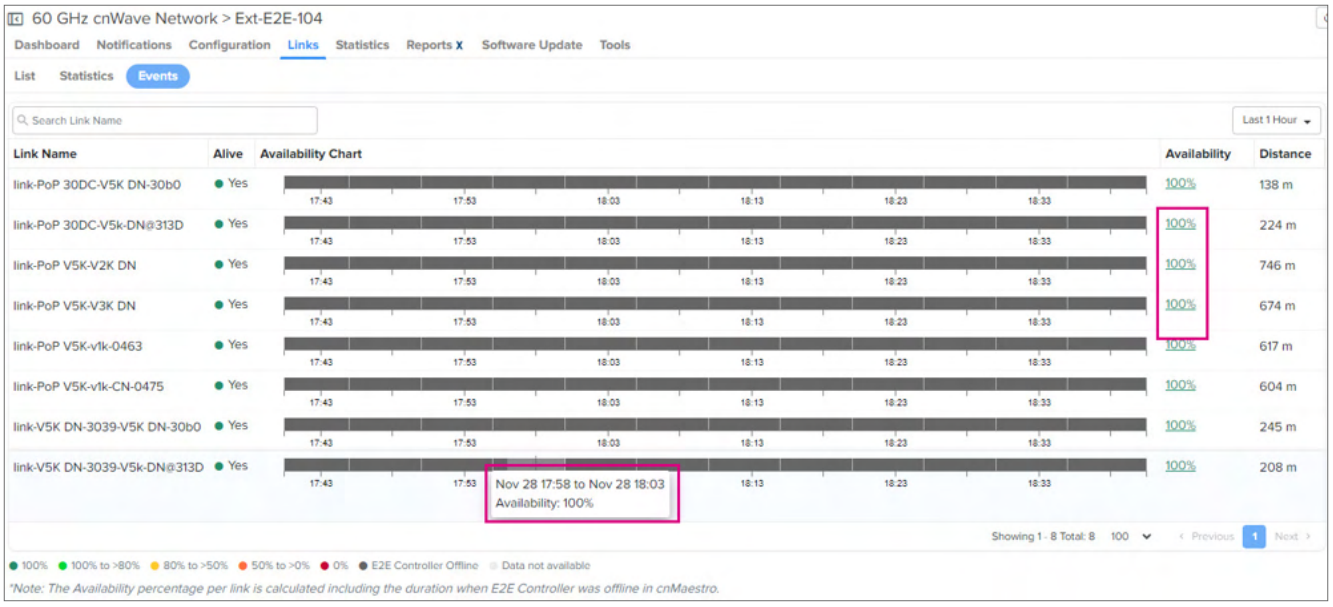
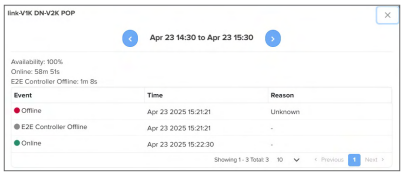


Figure 309 *Link Status*



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.

Statistics

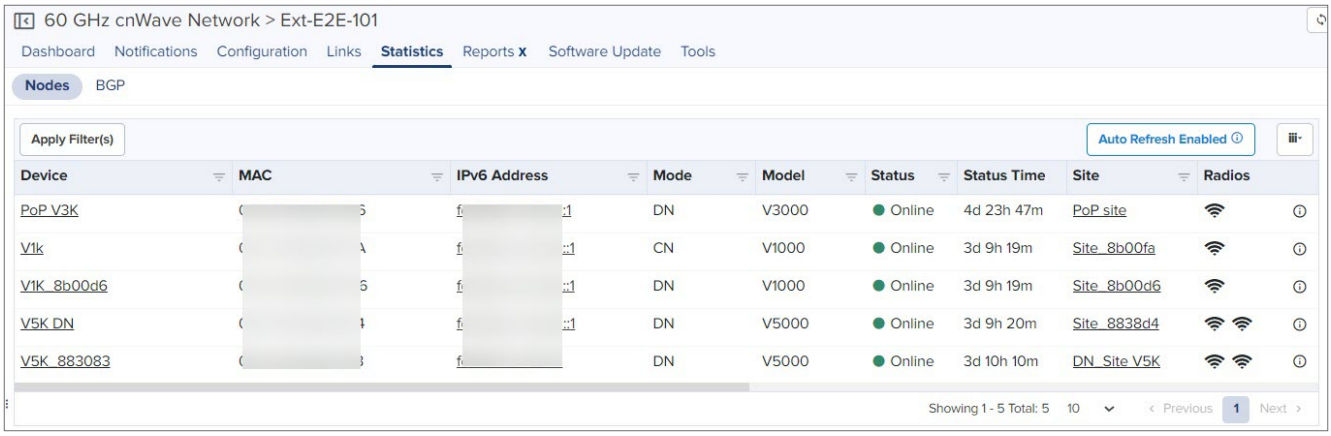
The E2E Network provides the following statistics:

- 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 310 *Nodes Statistics*

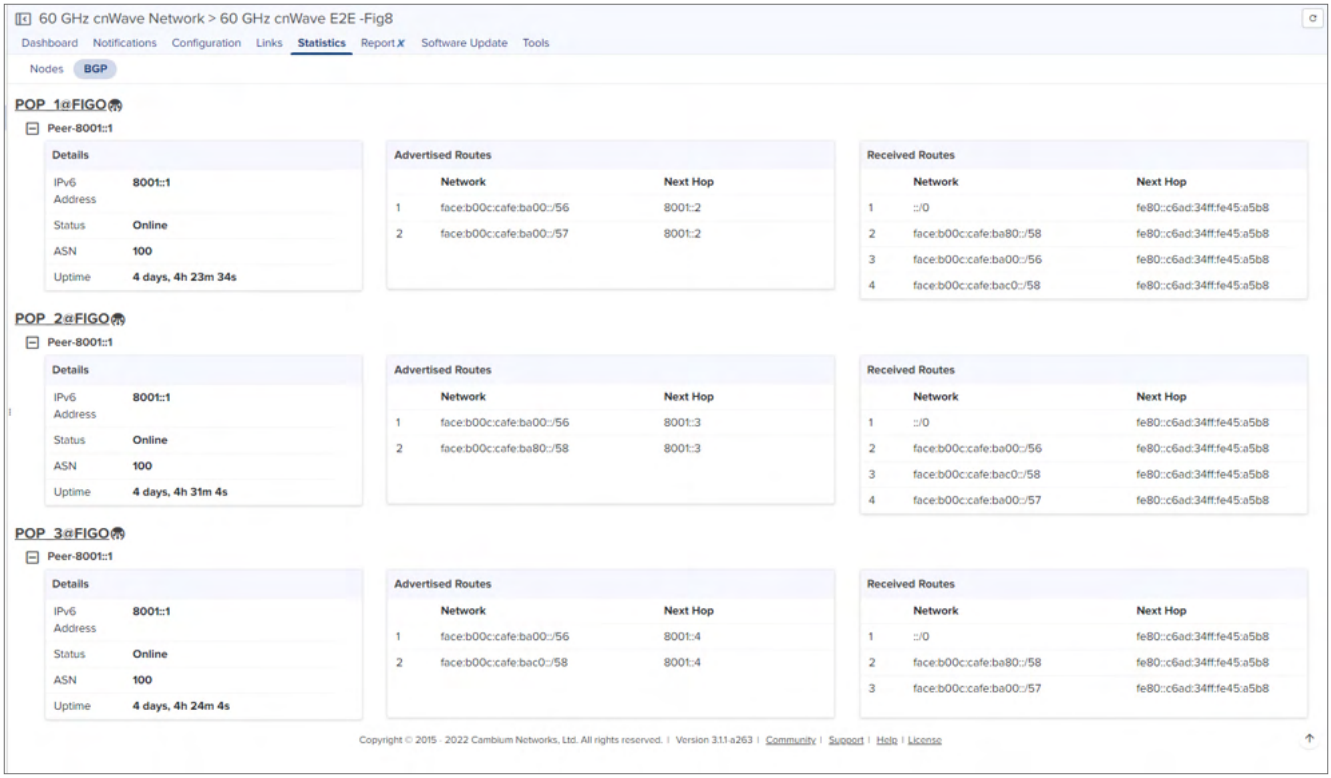


BGP

> **Note**
>
> BGP statistics displays only if BGP option is enabled in Routing in PoP configuration.

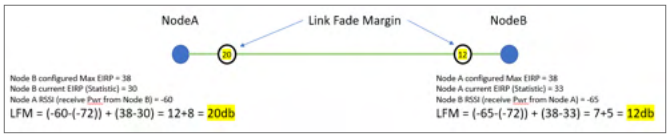
BGP provides the details of **Advertised Routes, Received Routes,** and **Peer** details.

Figure 311 *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 sensitively floor of -72 dBm. The LFM allows operators quicky 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 312 *Link Fade Margin*



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.

Software Update

The **Software Update** tab allows to update with the latest device software.

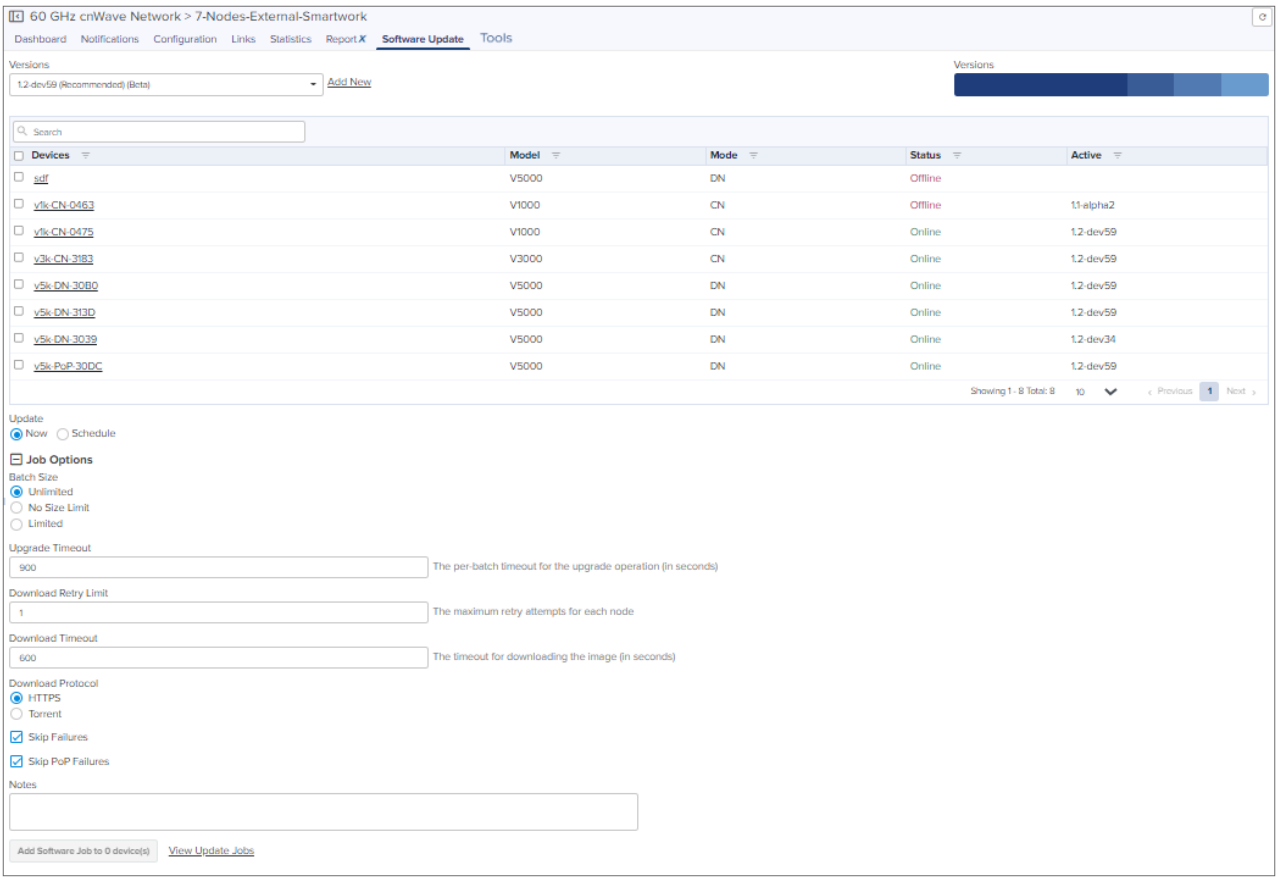
To update the software:

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.**

     Note

     If E2E Controller version is 1.2 or above, HTTPS or Torrent options will be available.

   - Enable the **Skip Failures** or **Skip PoP Failures**.
5. Click **Add Software Job to device.**



Note

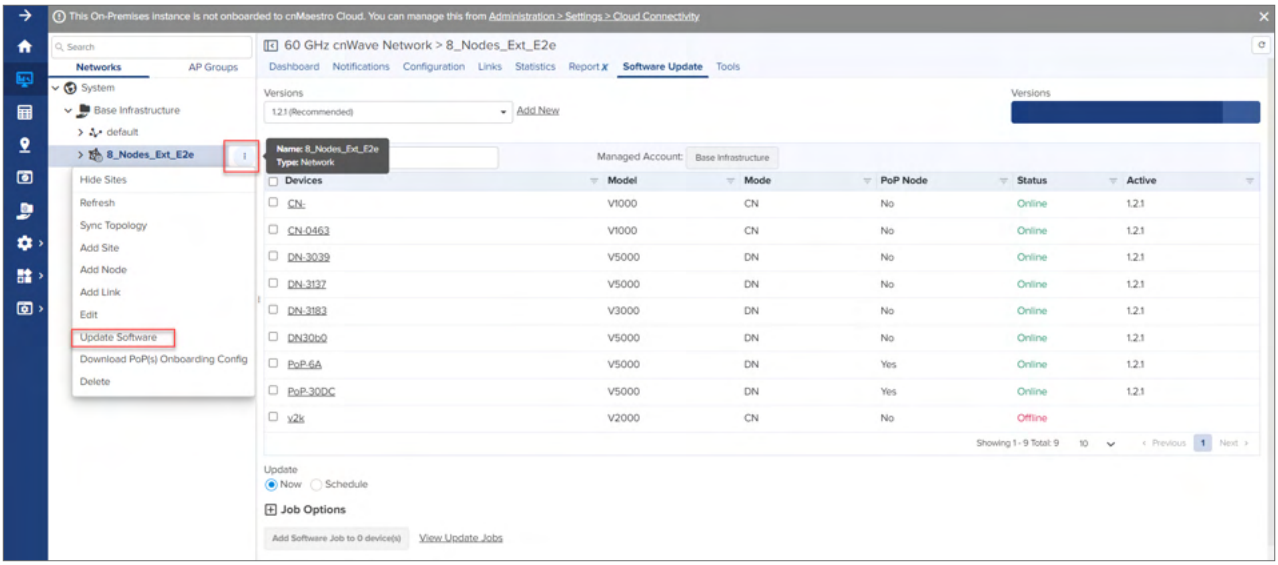
Onboard E2E controller will support only one synced image. If user needs to sync another image, select the image from **Versions** drop down and click **Sync Selected Image.**

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 84.

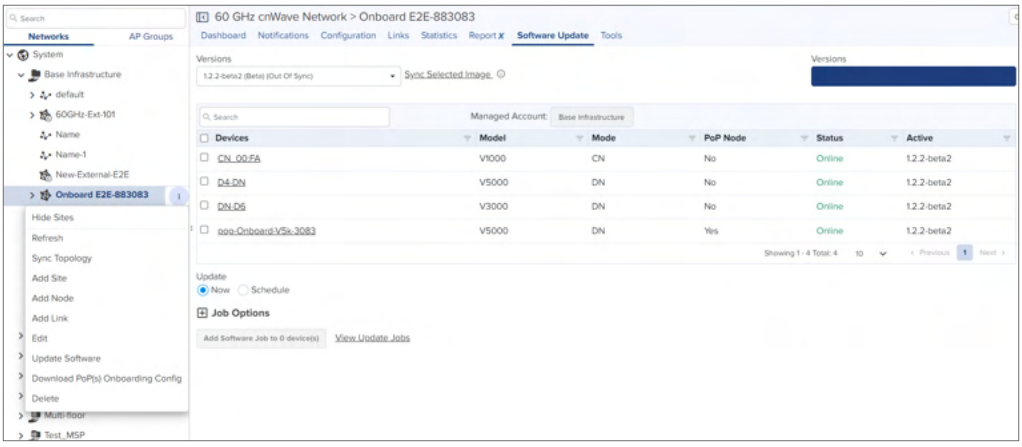
   Table 84 *Device Software Update: External E2E Controller*

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 85.

Table 85 *Device Software Upgrade: Onboard E2E Controller*

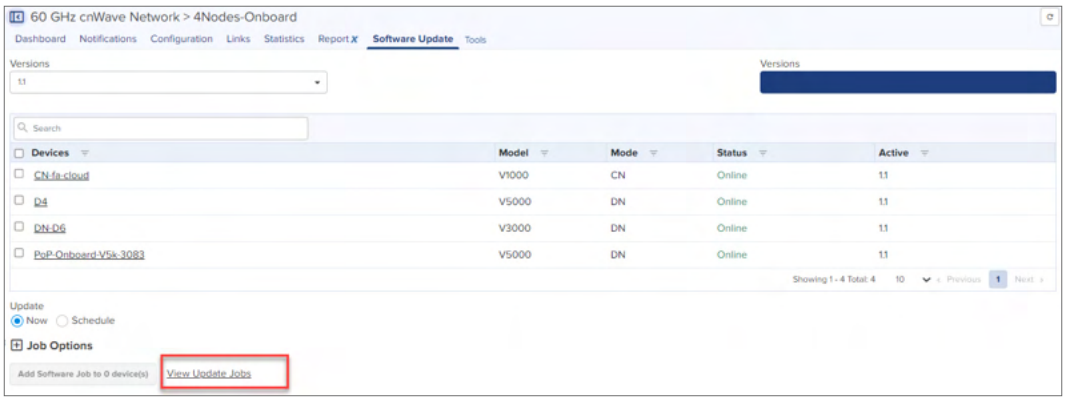
Software Upgrade	Example
If software version of Onboard PoP device is lower and upgraded to higher version then Software Upgrade is successful.	If the Onboard PoP device is running with 1.2, and selected software version is 1.2.1 or higher then Onboard PoP device is upgraded successfully.
If software 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 expect 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.

3. From the **Versions** dropdown, select the version and the devices in the network for software upgrade.

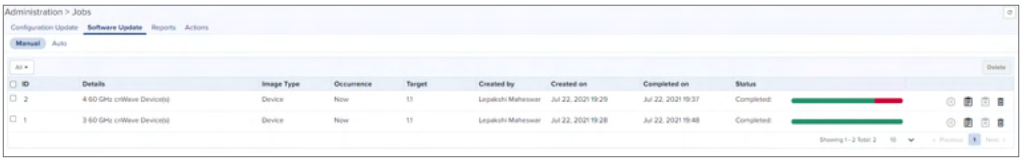
The Software Upgrade scenario for Onboard E2E Controller is explained in Table 85.

View Update Jobs

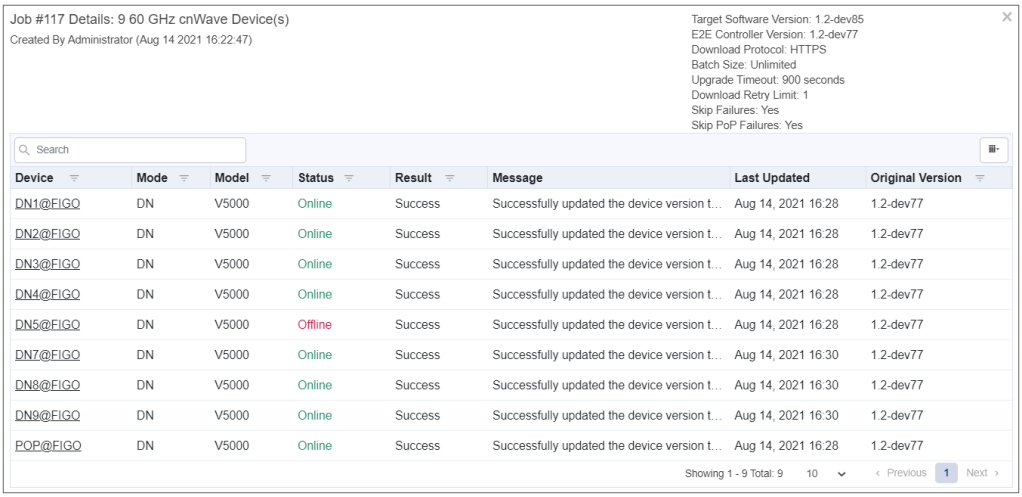
After adding the new Software Images, click **View Update Jobs.**



1. Navigate to the **Administration** > **Jobs** > **Software Update**.



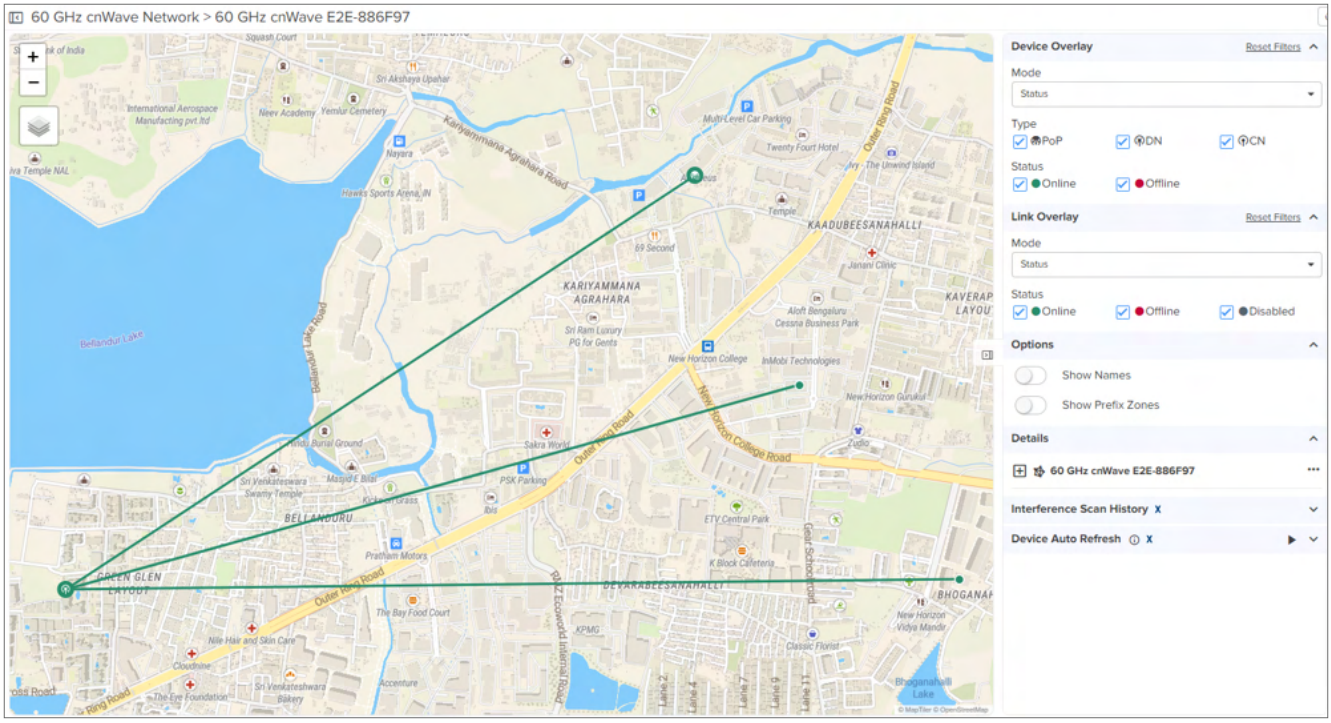
2. Click **Show More** to view the Job Details.



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 313).

Figure 313 *Viewing E2E Network*



Note

Gray color lines are unmanaged links and gray color nodes are unmanaged nodes.

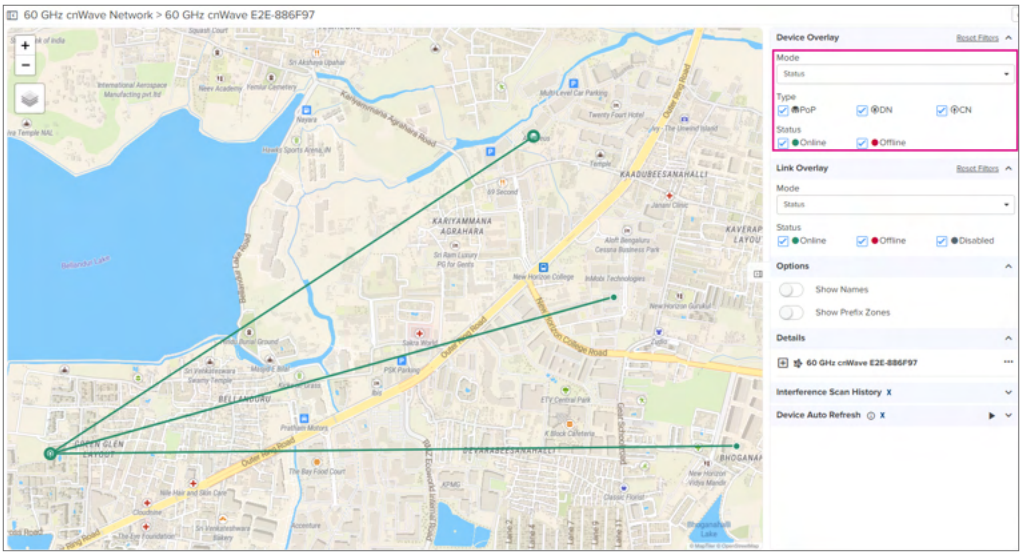
The following fields on the **Map** page provide details of the nodes and links:

- Device Overlay
- Link Overlay
- Options
- Details
- Interference Scan History X
- Device Auto Refresh

Device Overlay

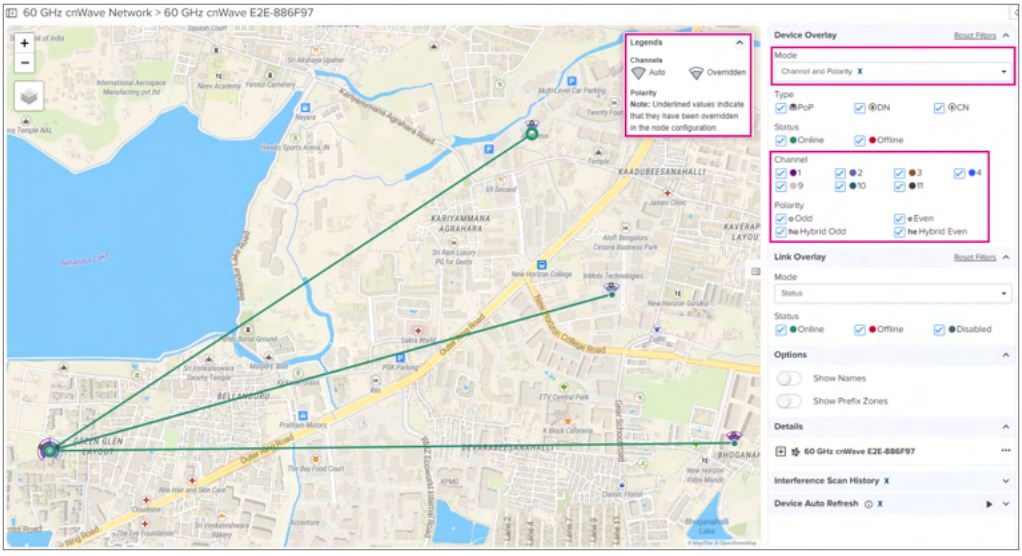
In the Device Overlay field section, complete the following steps:

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.



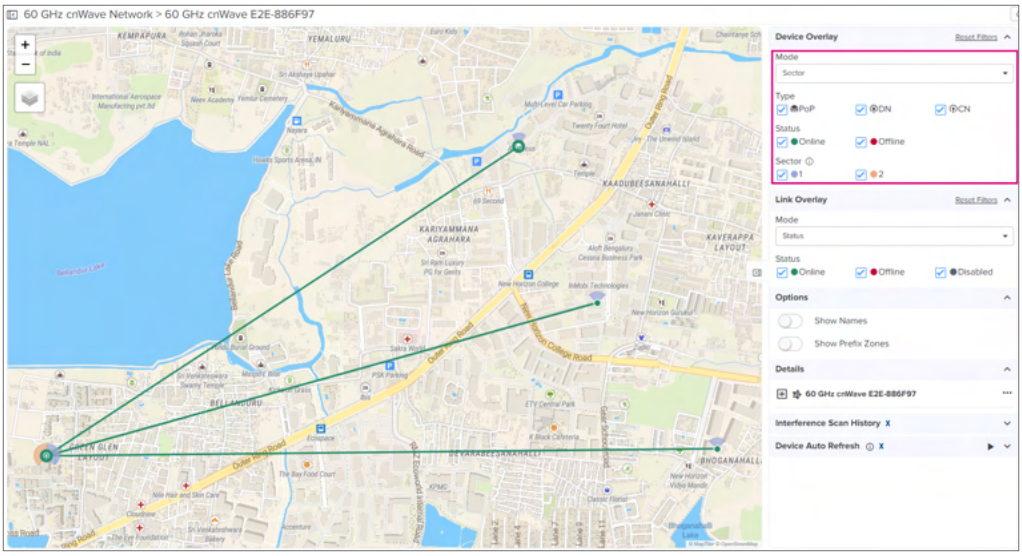
2. Select the **Mode** type as **Channel and Polarity** to view the following:

   - 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.



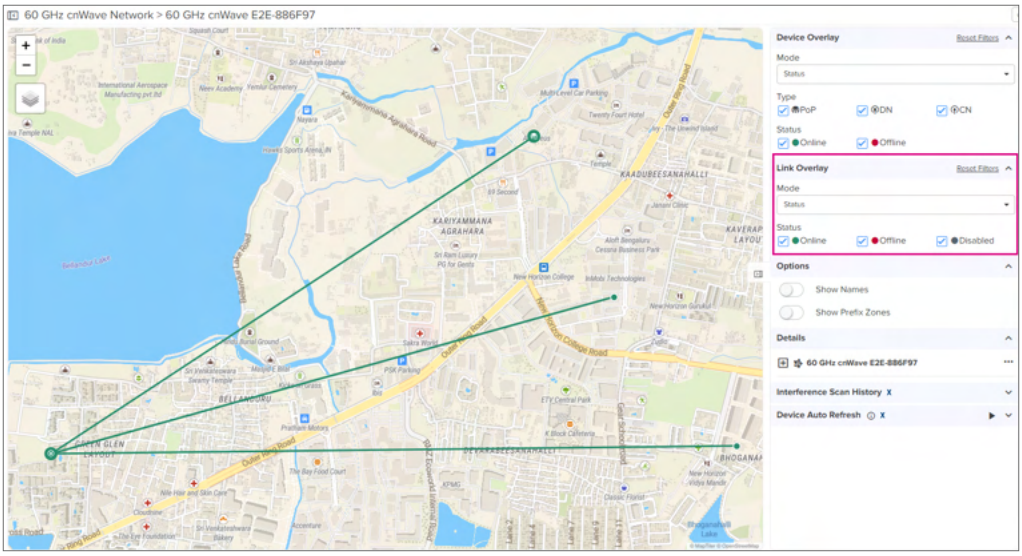
V5000 Sectors is shown below:

Link Overlay

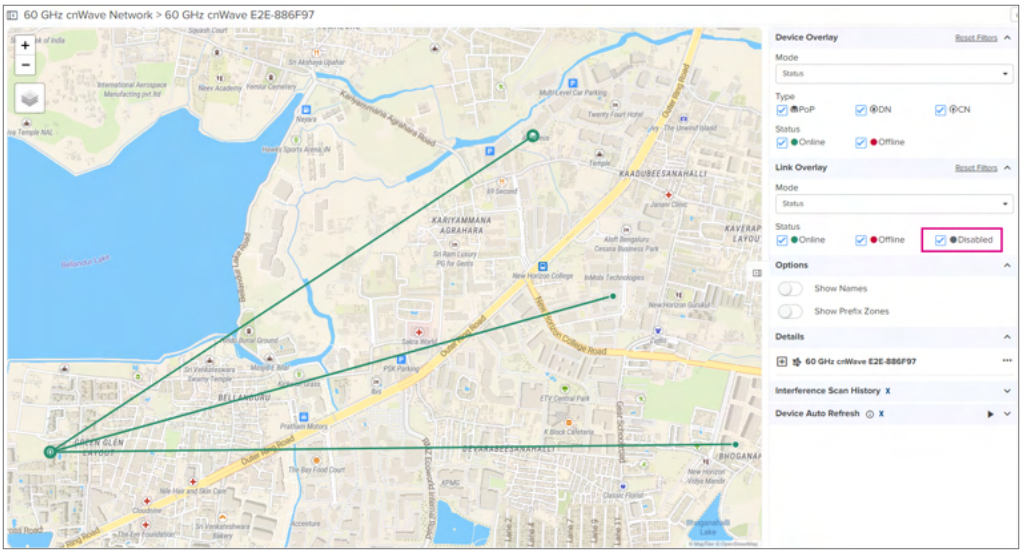
In the Link Overlay field section, complete the following steps:

1. Select the **Mode** type as **Status** to view the following:

   Status: The link status is Online or Offline.

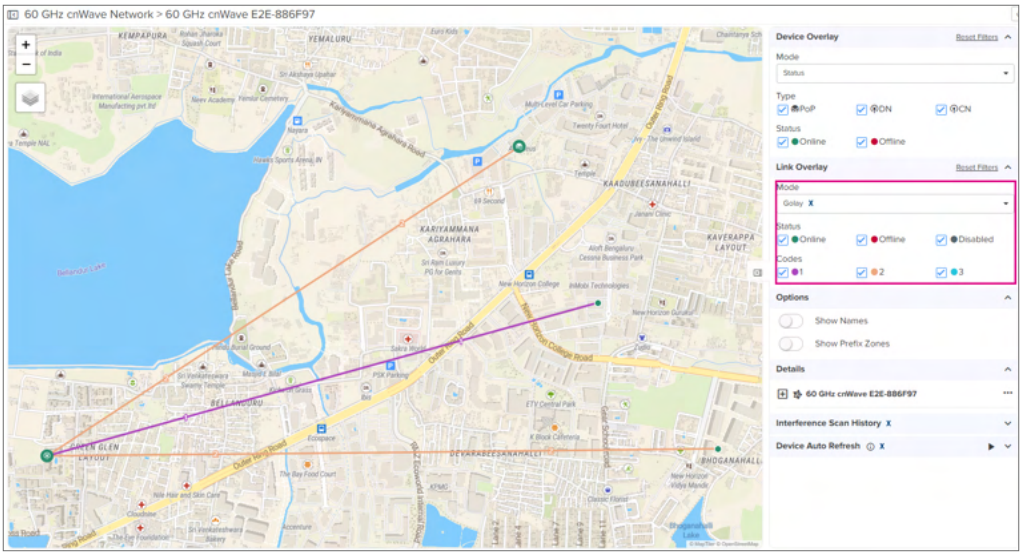


   By default the **Disabled** option is selected, which appears in light gray.



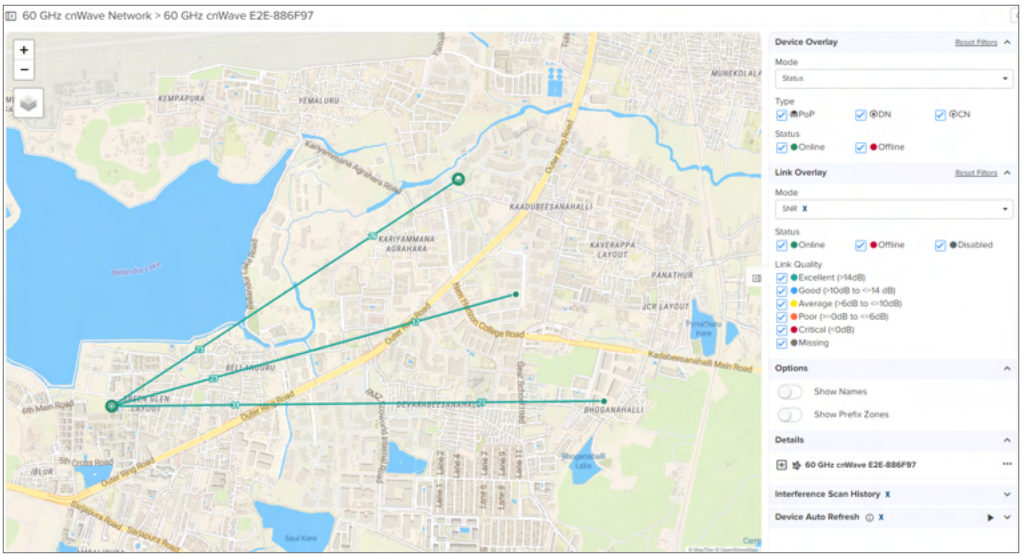
2. Select the **Mode** type as **Golay** to view codes.

   Golay: The Golay mode is represented in color codes, as shown below:



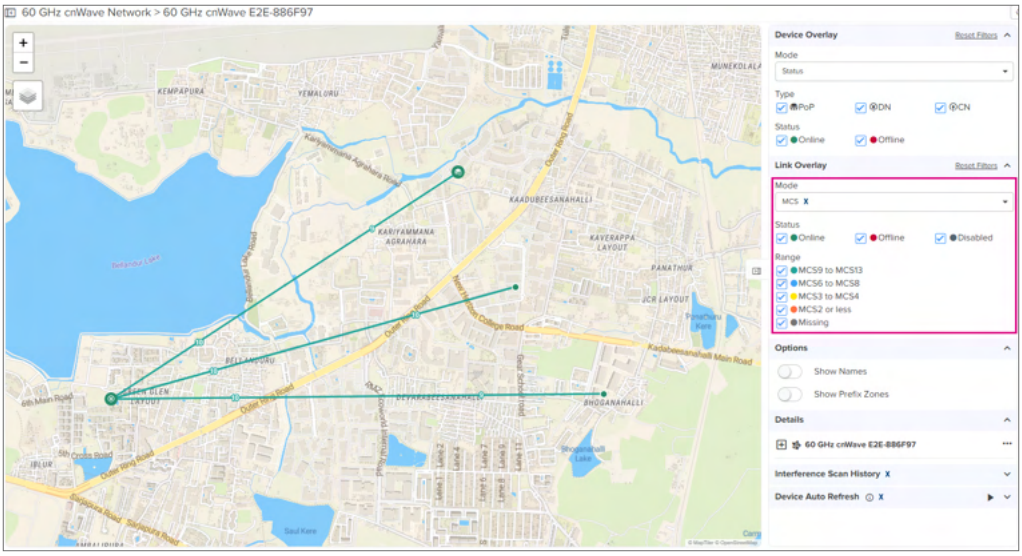
3. Select the **Mode** type as **SNR** to view link qualities.

   SNR: Shows various SNR link qualities and is represented in different colors.



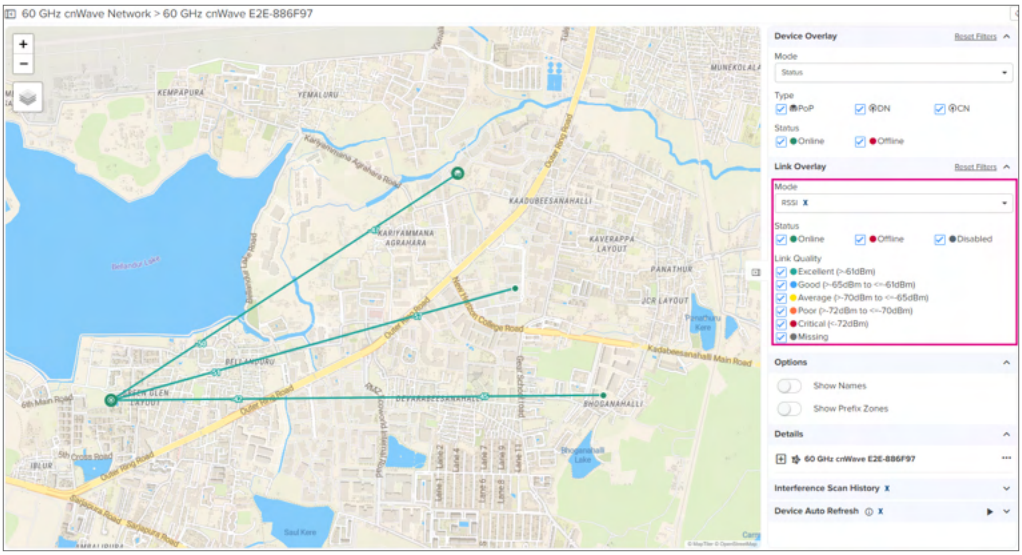
4. Select the **Mode** type as **MCS** to view link range.

   MCS: Shows the link status and various link ranges represented in different colors.



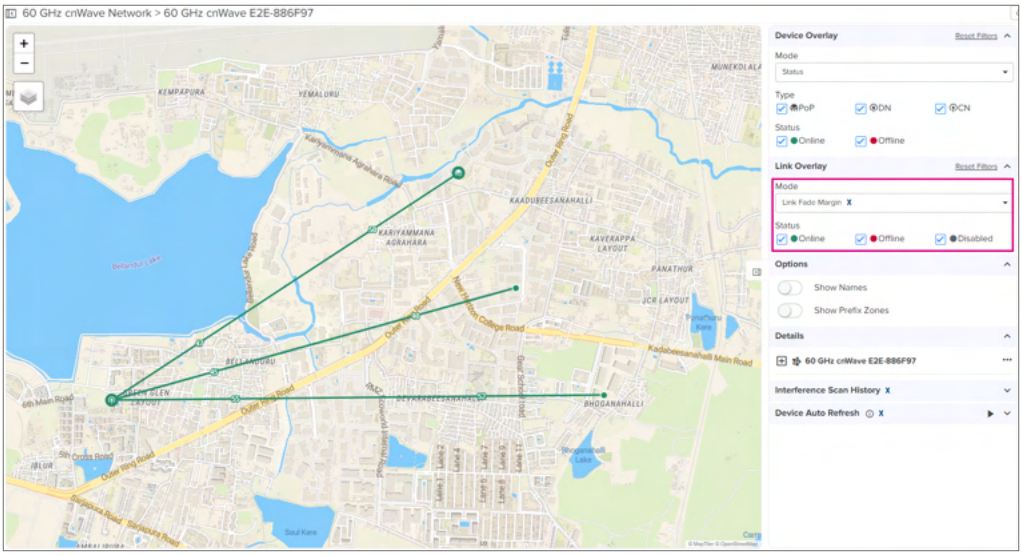
5. Select the **Mode** type as **RSSI** to view link qualities.

   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 312.



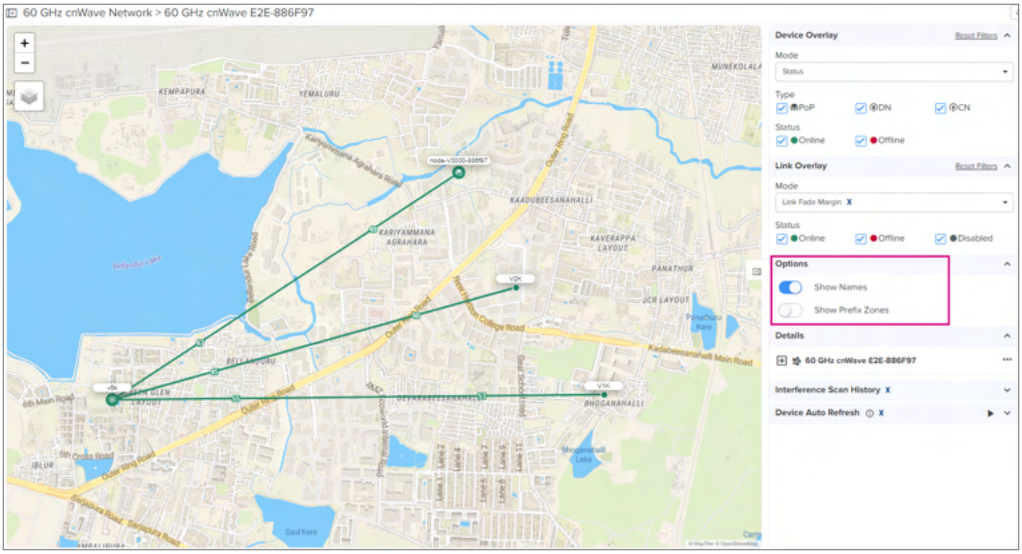
   Note: Link Fade Margin is applicable only when E2E Controller and Device version are 1.2.2.

   - Airtime%
   - Throughput (Mbps)

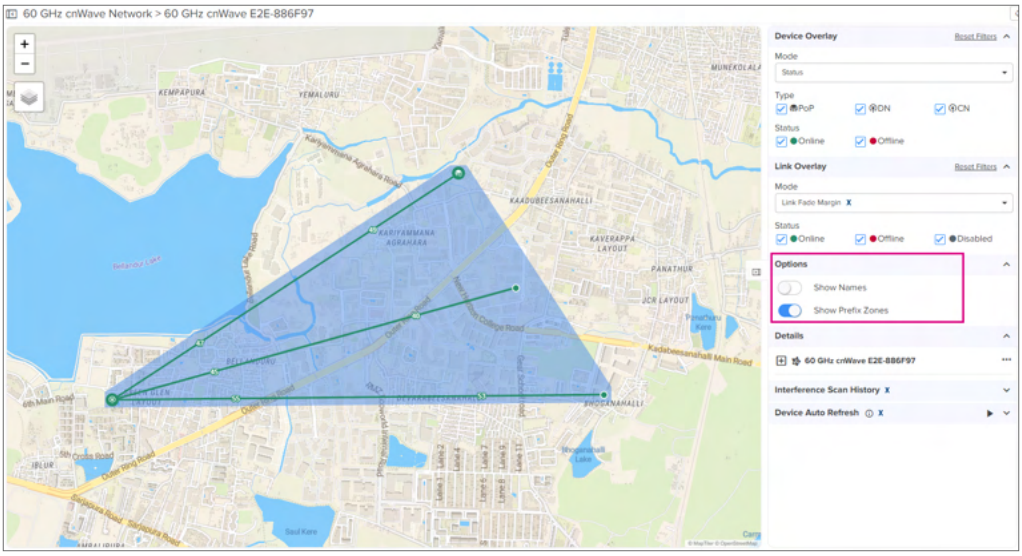
Options

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.



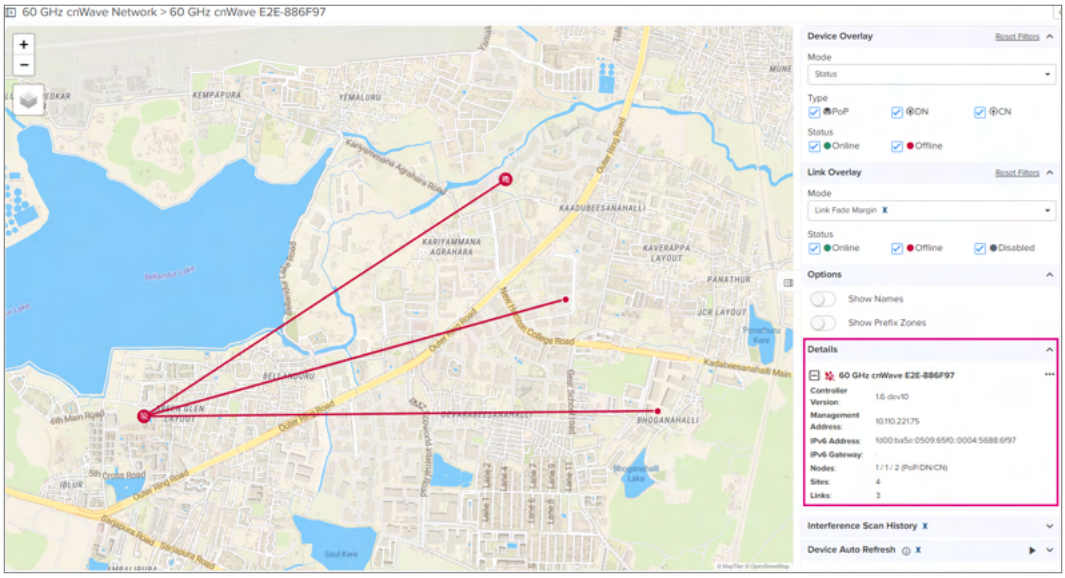
- **Show Prefix Zones**: shows the prefix zone of each PoP that is communicating with each other.



> **Note**
>
> **Show Prefix Zones** is enabled only if **Prefix Allocation** is set to **Deterministic**.

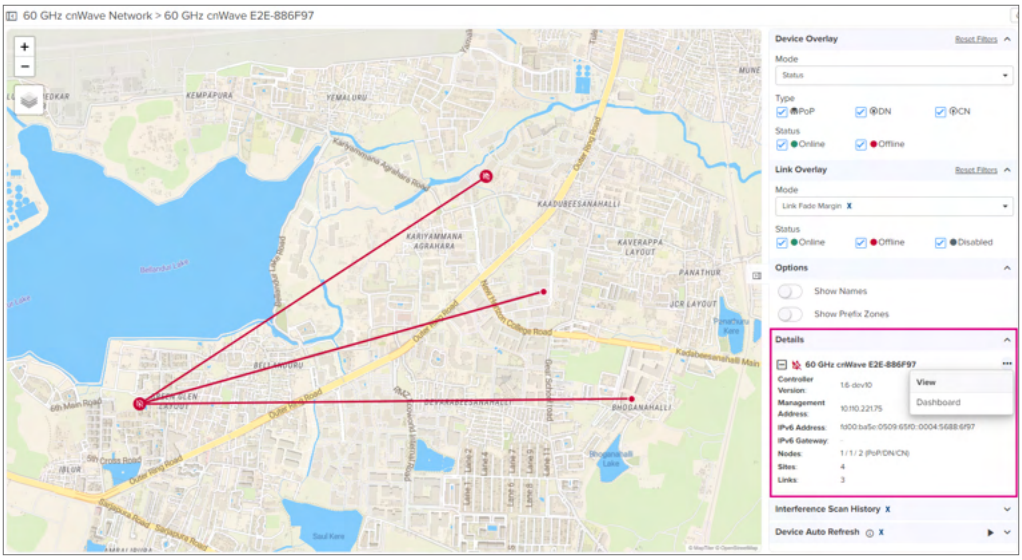
Details

The **Details** field displays the basic details of E2E Network when E2E Network is selected from the tree.



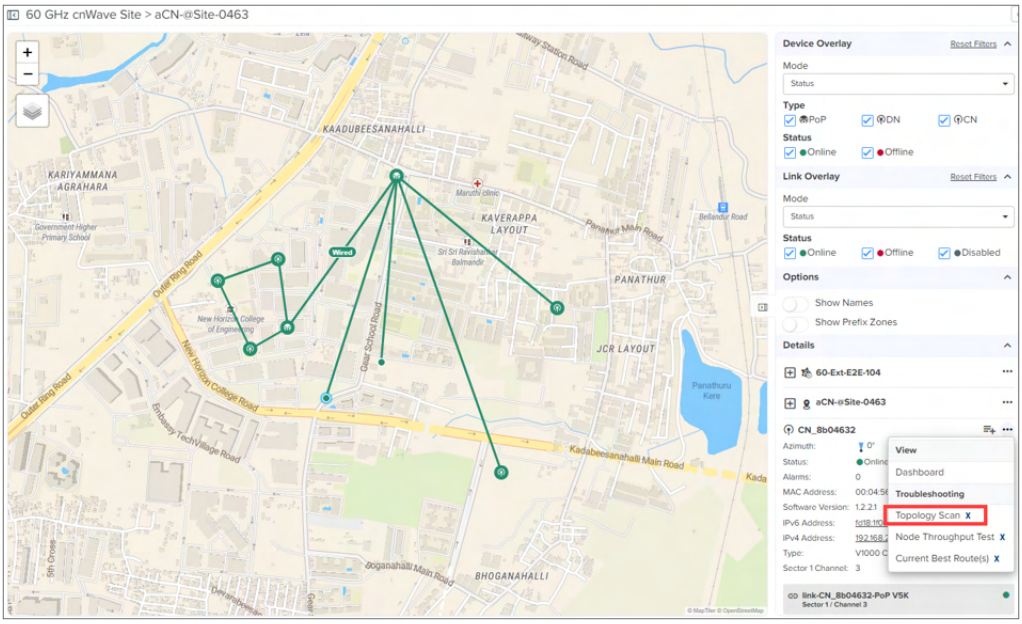
To view the details of nodes and links, complete the following steps:

1. Click the (•••) icon in the **Details** section to view E2E Network Dashboard.



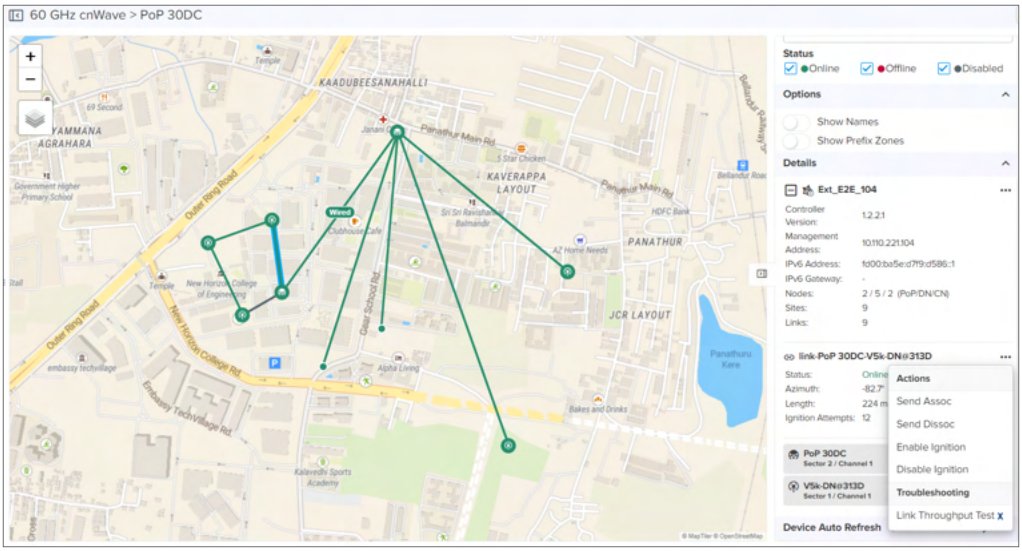
When a device is selected from the map, the device details are displayed.

2. Click the ••• icon next to the device to view the device **Dashboard**



Refer to Node Throughput Test and Current Best Routes in the Troubleshooting section.

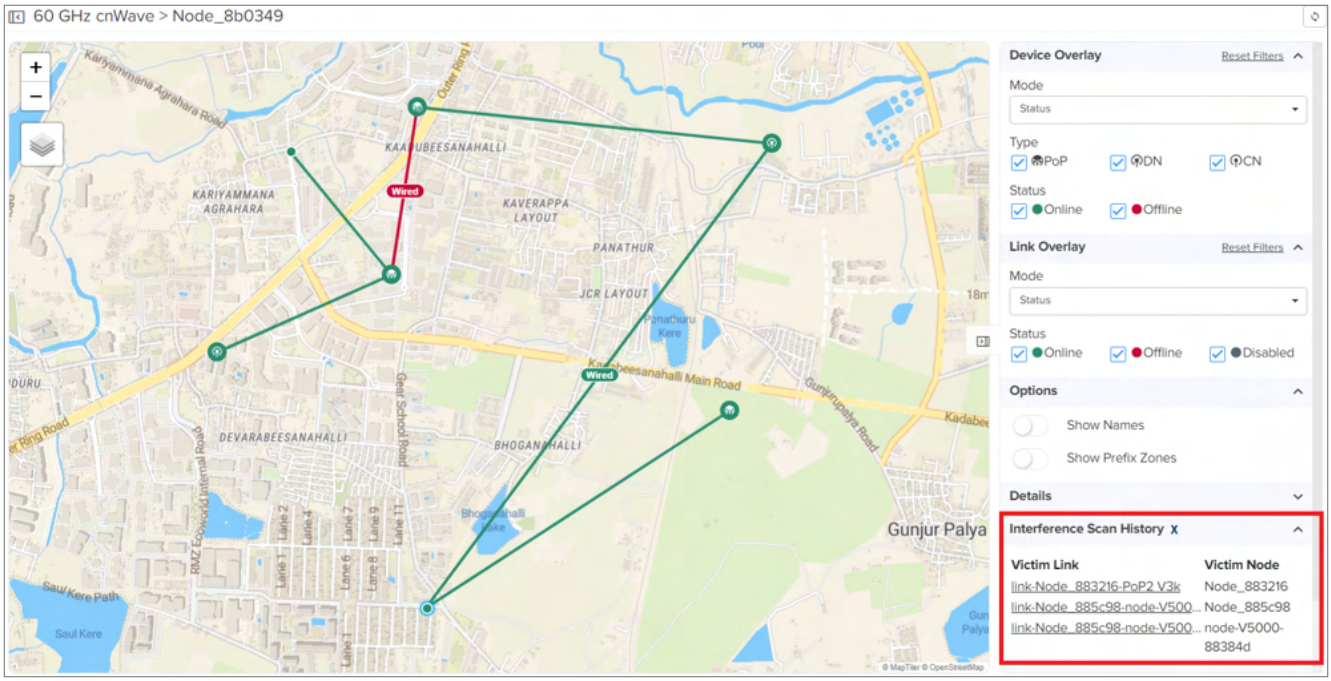
3. When a link is selected from the map, link details are displayed. Click ellipsis (•••) icon next to link to view the **Actions** details for the links.



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**. It is applicable only for cnMaestro X.
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

Toposcan Discovery tool allows a user to select a DN and scan for nodes on the same channel sector. Each sector will display list of nodes found and allows them to add into existing topology if they do not exist already.

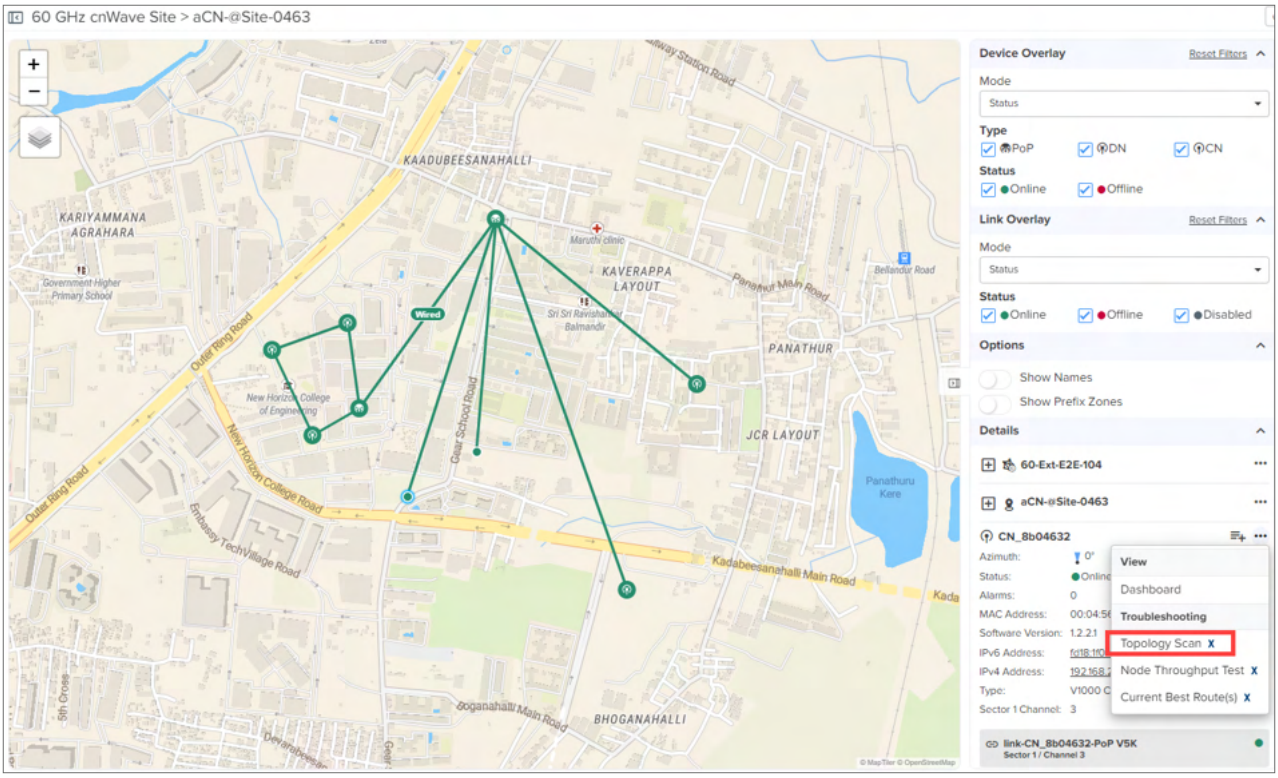
> **Note**
>
> .Topology Scan X is applicable only for cnMaestro X.

The scan will not detect any CN node with an existing wireless link or any DN node with an existing wireless link with the current scanning DN node.

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.

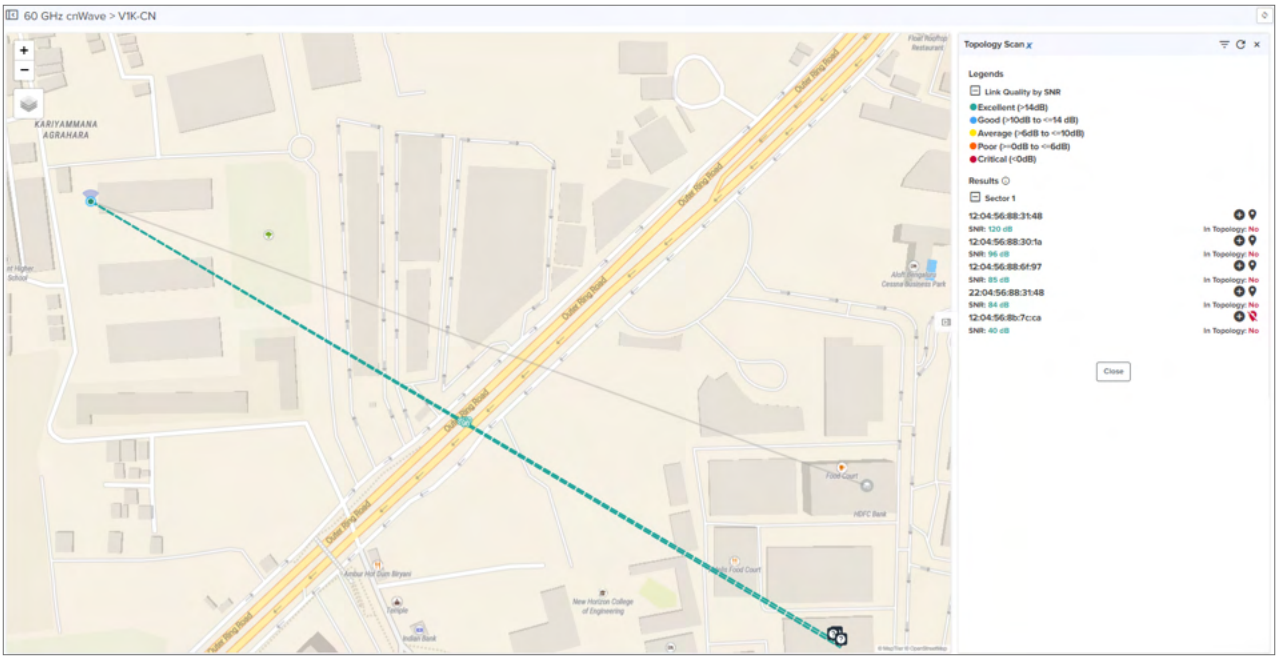
> **Note**
>
> Disable the auto-ignition of wireless links on the scanning DN which are actively running. Topology Scan will cause a momentary throughput reduction in nearby links.

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.

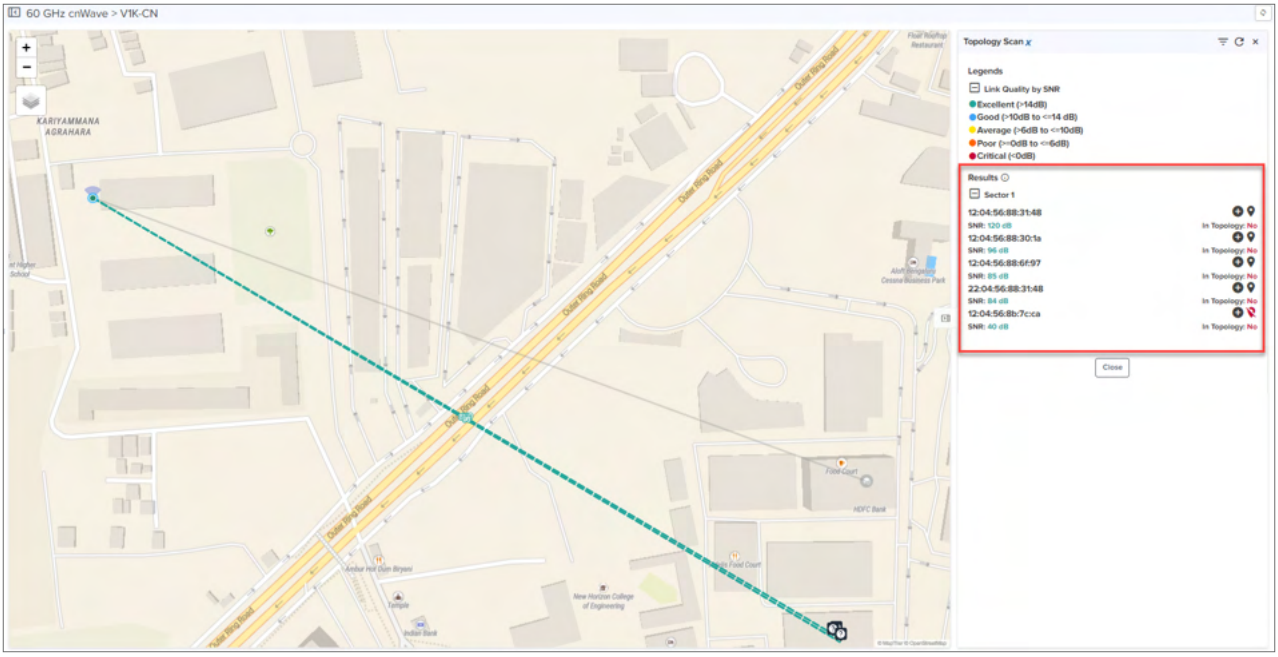
3. Click **Start Topology Scan**. Topology Scan begins as shown in the following figure.



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.

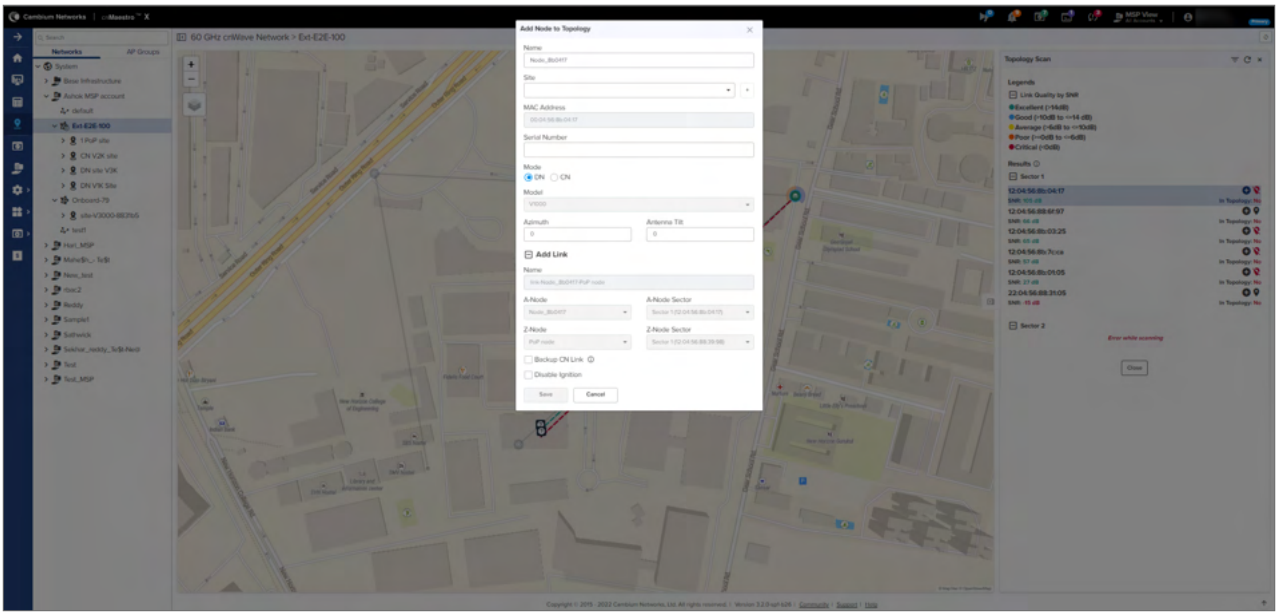
5. Click ( ) refresh icon to scan again.

   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.



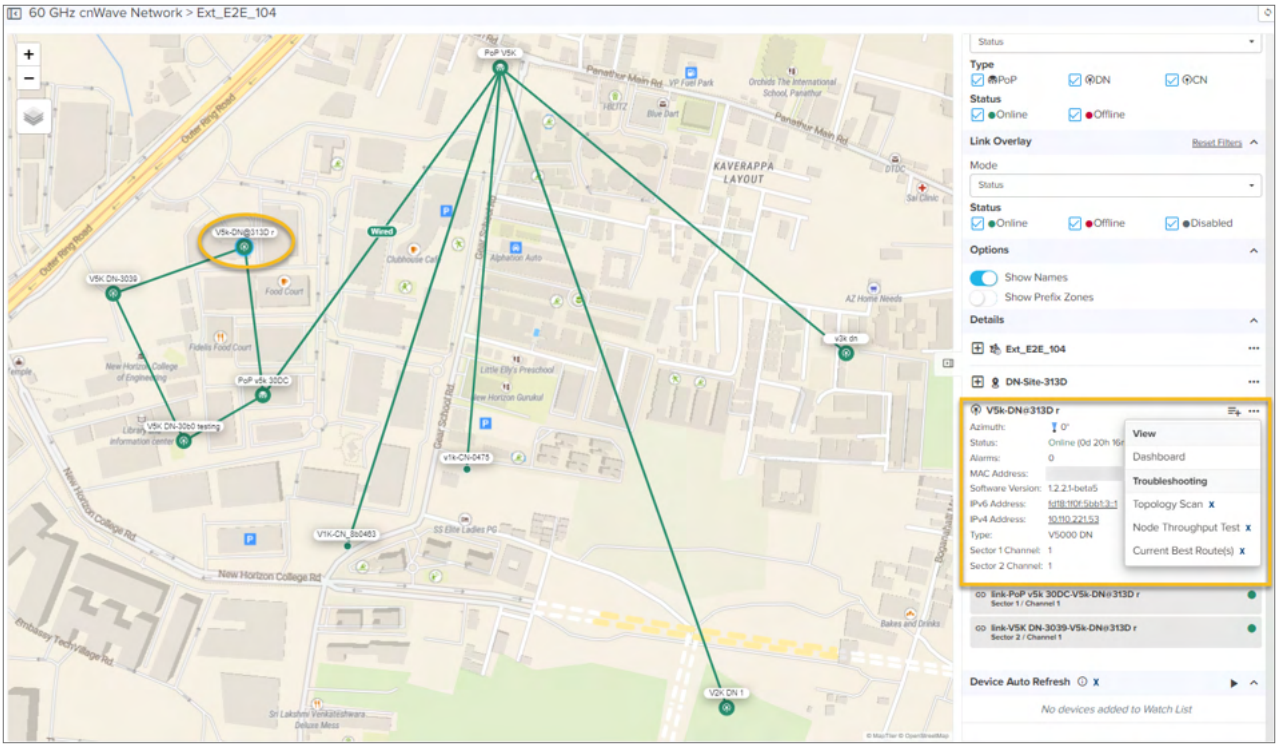
7. Enter the node and link details and click **Save**.

Node Throughput Test X

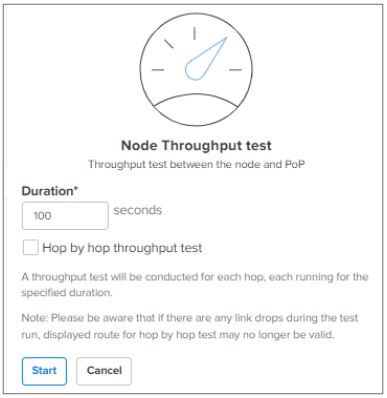
The **Node Throughput Test X** option allows you to test the throughput between a node and PoP. Using this option, you can conduct a throughput test for each hop seamlessly.

To run a node throughput test, complete the following steps:

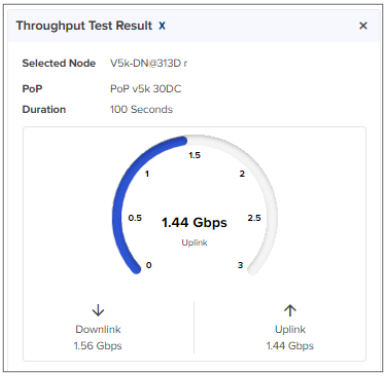
1. Select a device except the POP Node from the Map.

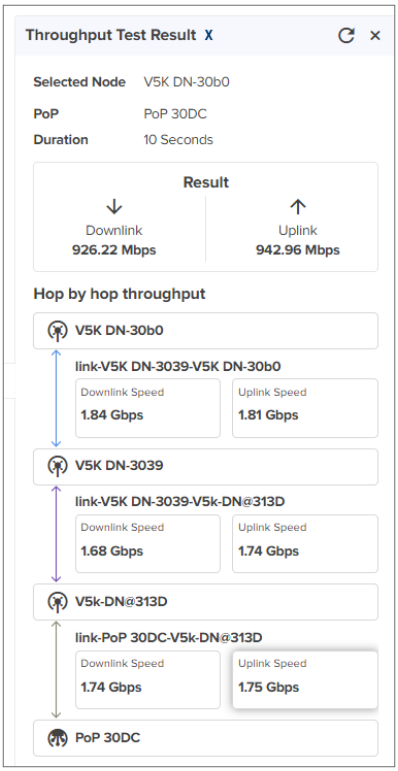


2. Click ellipsis (•••) icon next to the device name in the right pane, and select **Troubleshooting** >**Node Throughput Test X**



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

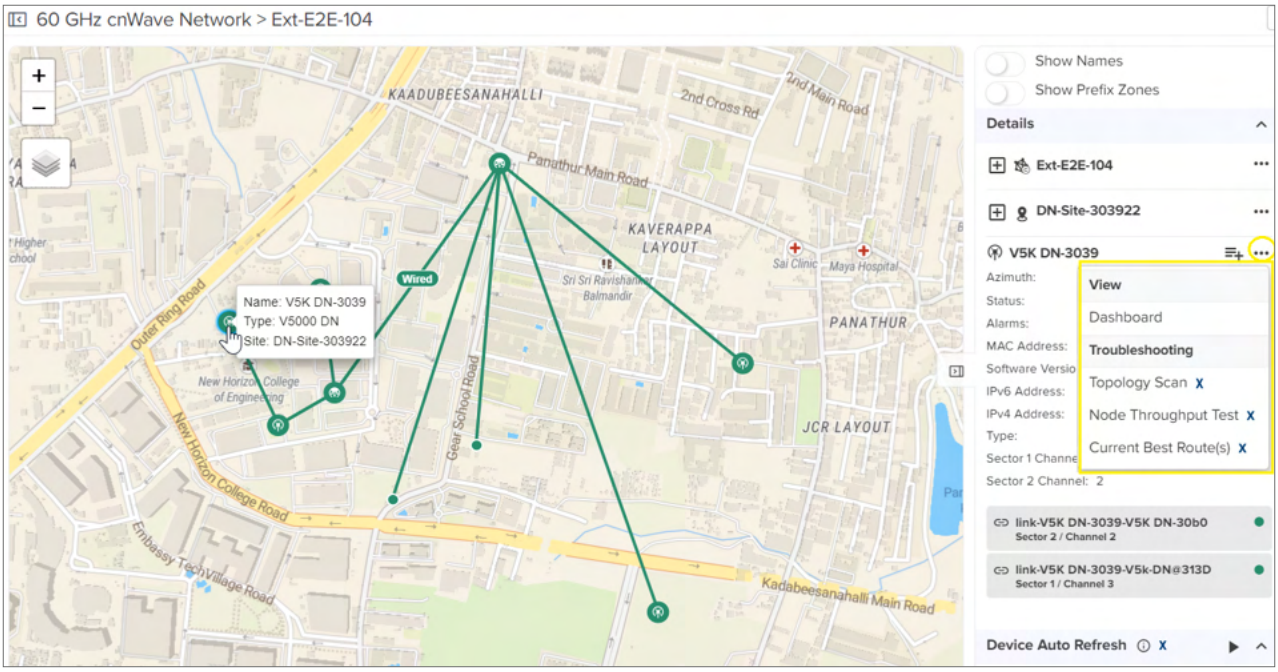
The Current Best Route(s) X feature is used to view the best route from a CN/DN to PoP. The **Current Best Route (s) X** map view displays statistics of the following parameters for uplink and downlink of wireless link of a node:

- Golay
- SNR
- MCS
- RSSI
- Throughput (Mbps)
- Airtime (%)
- Link Fade Margin (LFM)

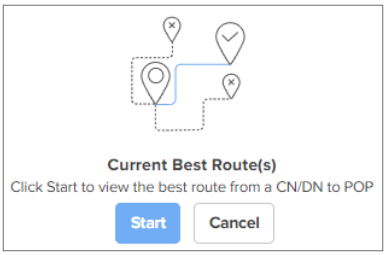
> **Note**
>
> The **Current Best Route(s) X** feature is applicable only to X accounts. In addition, this feature is supported only on the E2E Controller (Onboard or external) running with software version 1.2.2.1 or later.

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.

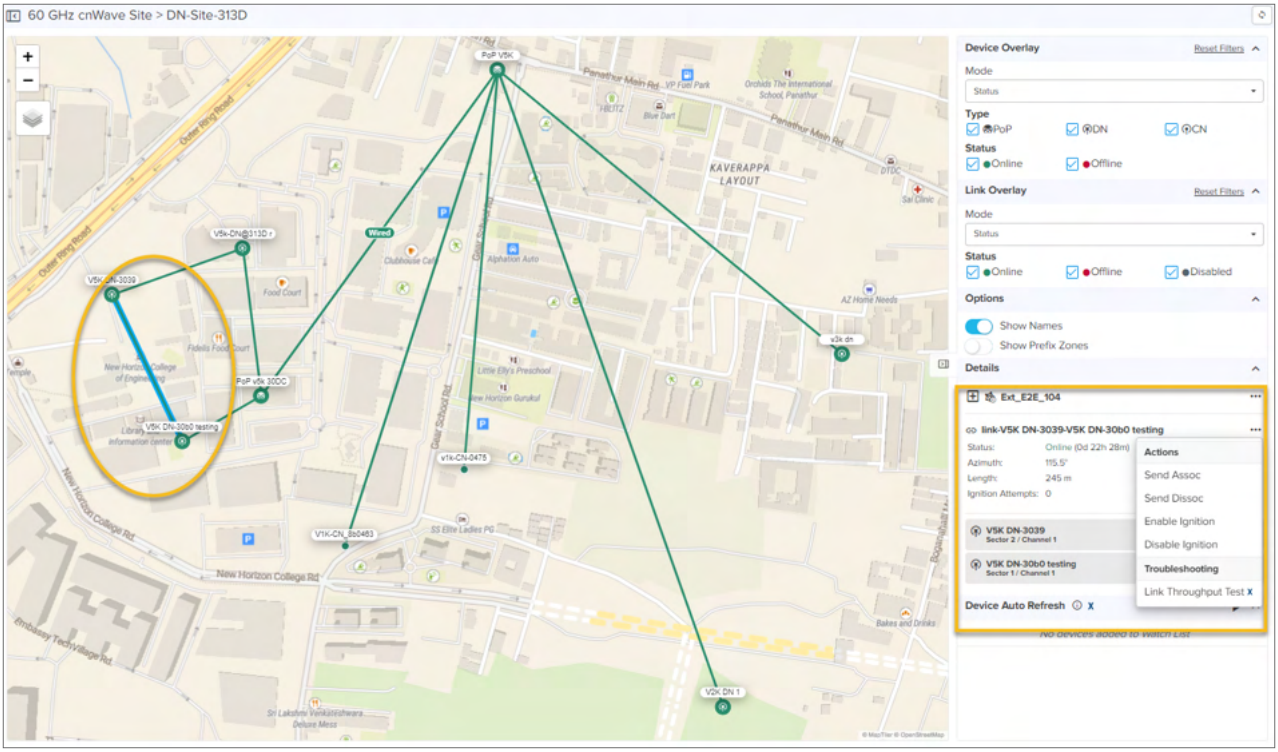


3. Click **Start**. The **Current Best Routes(s) X** section displays route details for the selected node.

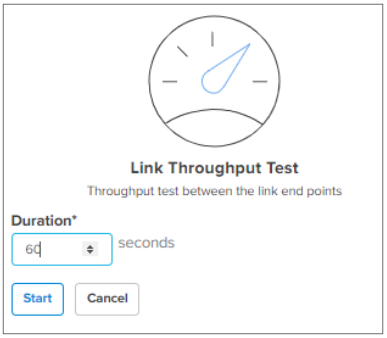
Link Throughput Test X

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:

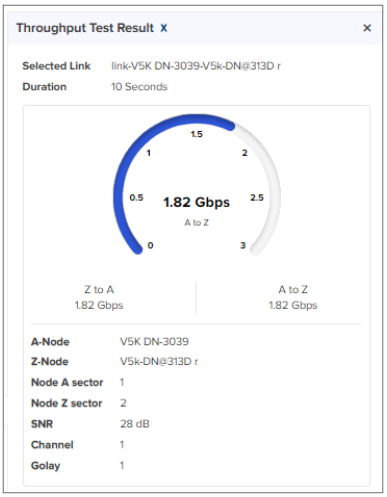
1. Select a Link from the Map.



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.

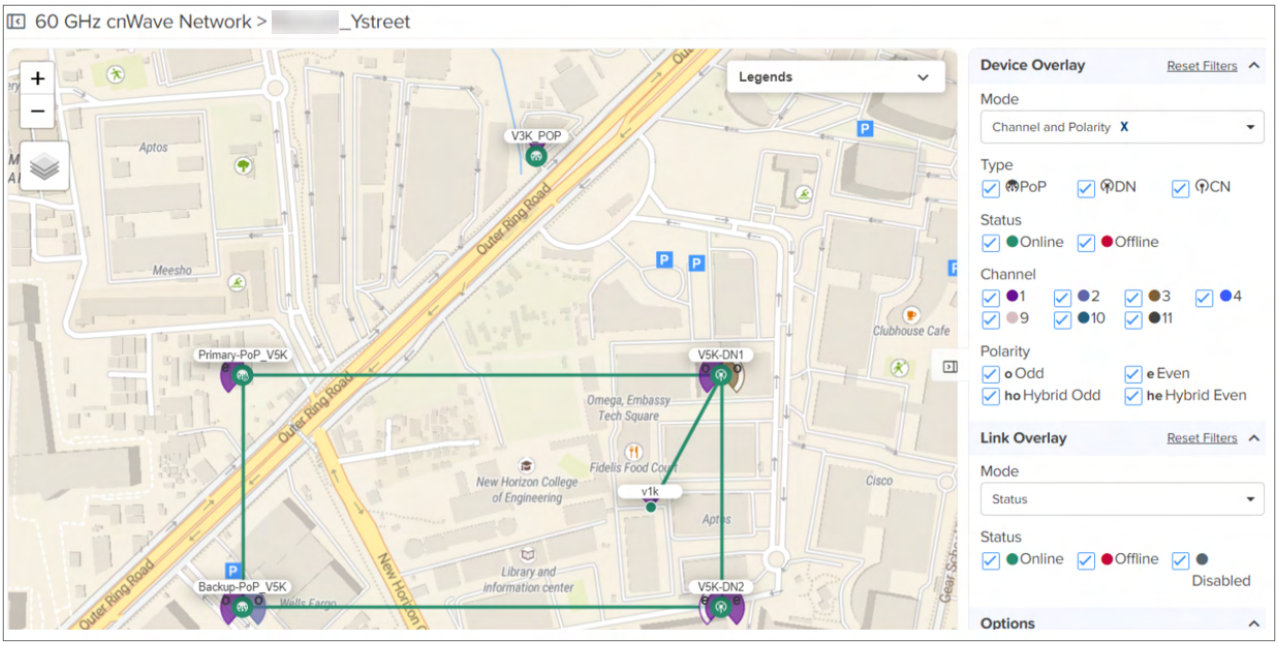
Running the Interference Scan tool

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:

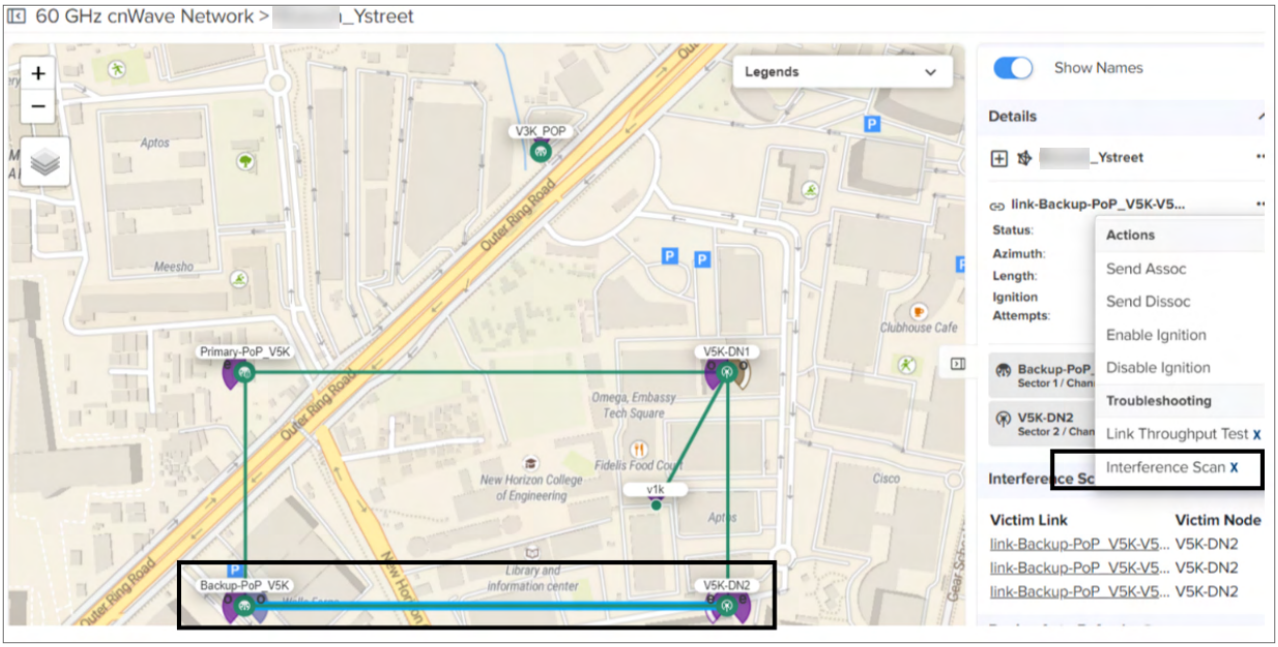
1. On the **Map** page, select a cnWave network and click on the link for which you want to run the interference Scan tool.

   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.

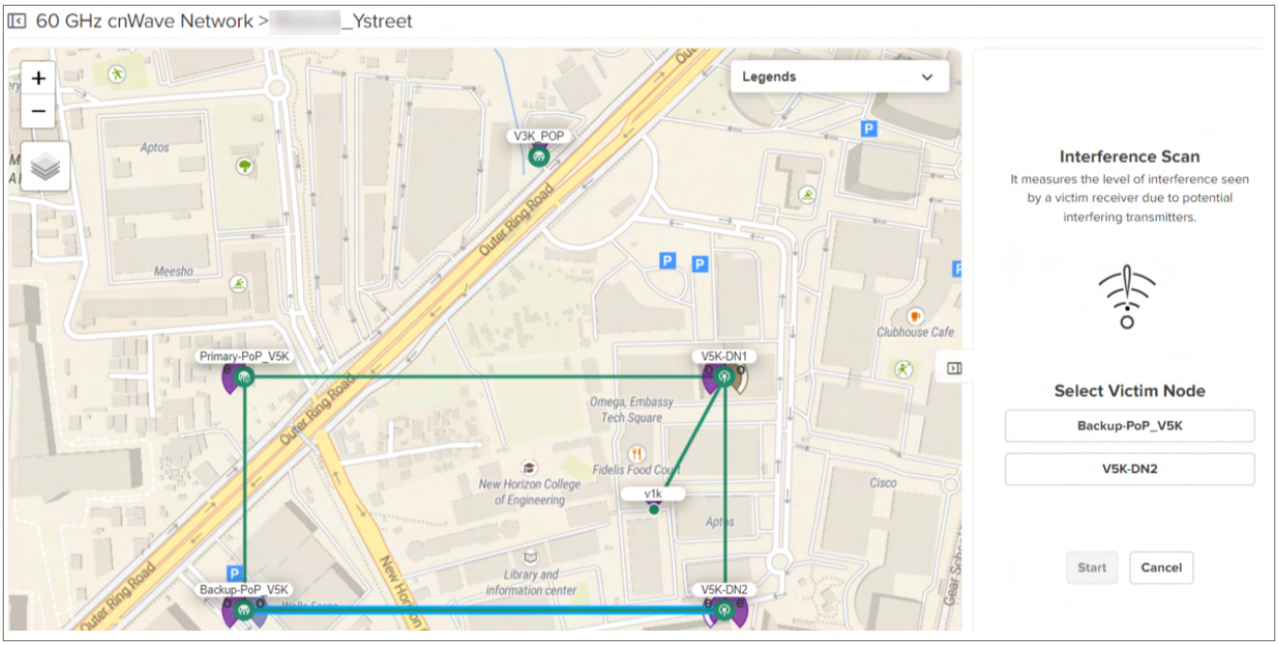


2. Click the ••• icon next to the link name and select **Interference Scan X** from the dropdown list.

   For example, Interference Scan is used for the link highlighted between Backup-POP_V5K linked to V5K-DN2 in the figure shown below.

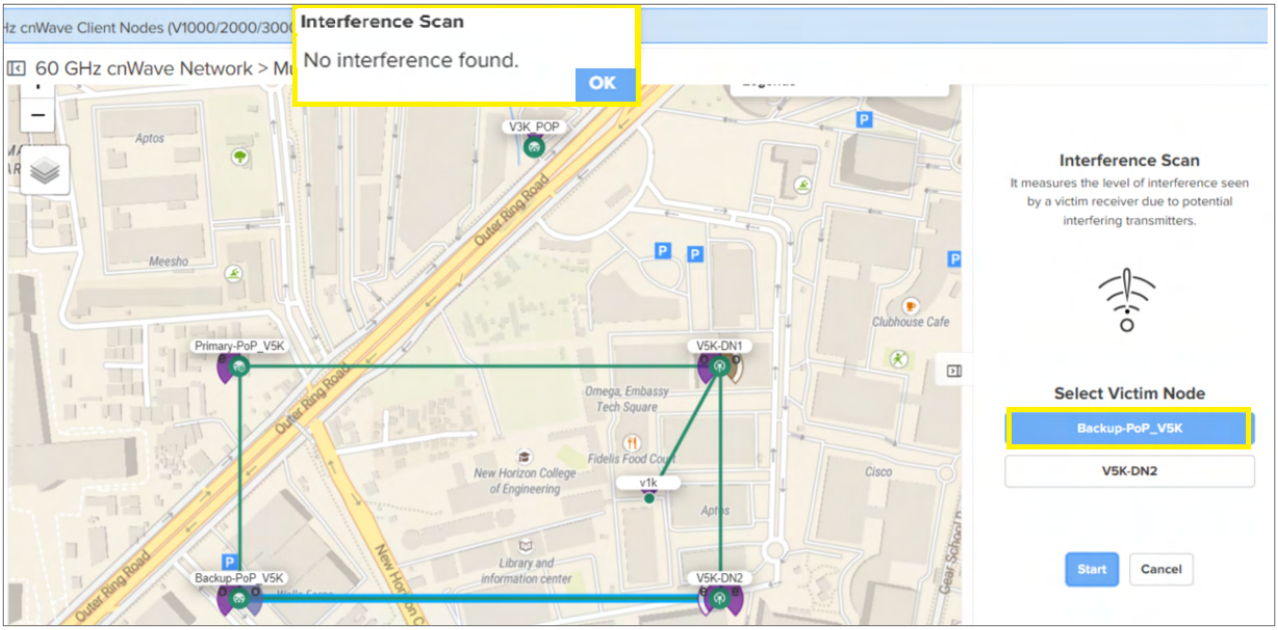


   When **Interference Scan X** is selected, the **Interference Scan** section appears with the victim node names on the right side of the Map page (as shown in the figure below).



3. Select the required victim node and click **Start**.

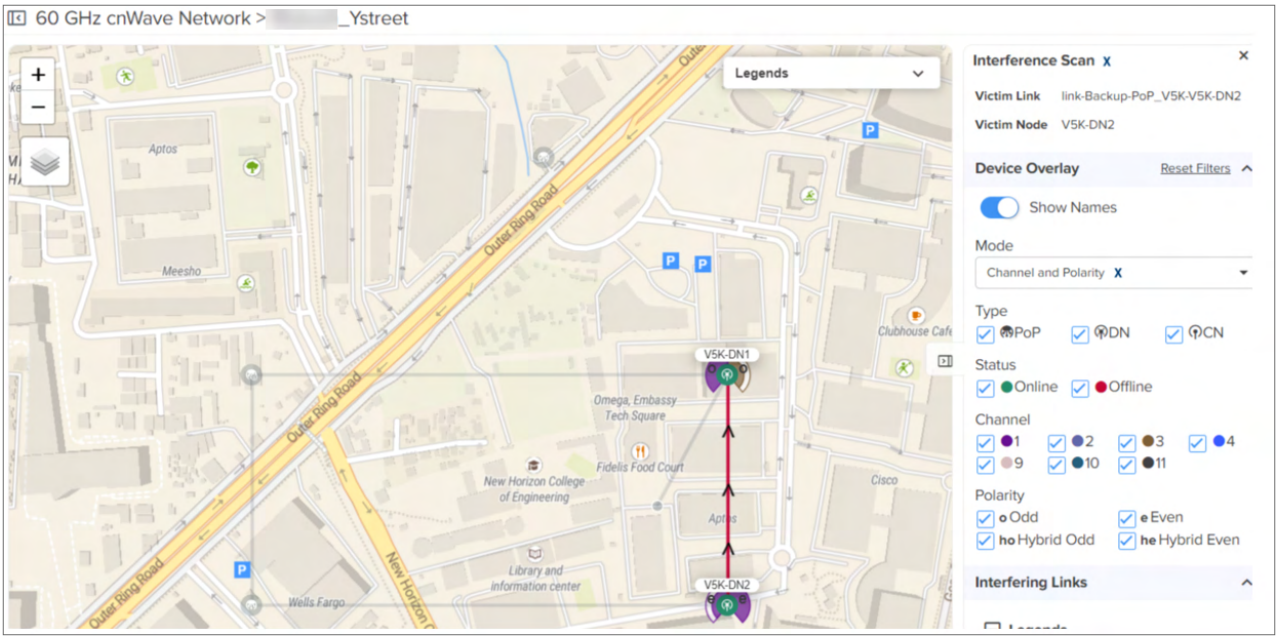
   The Interference Scan tool detects neighboring interfering links with wireless settings that may affect your network. The Interference Scan tool can be executed on any of the victim nodes. In the figure below, Interference Scan is executed on the first victim node Backup-POP_V5K. If no aggressor is found, 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

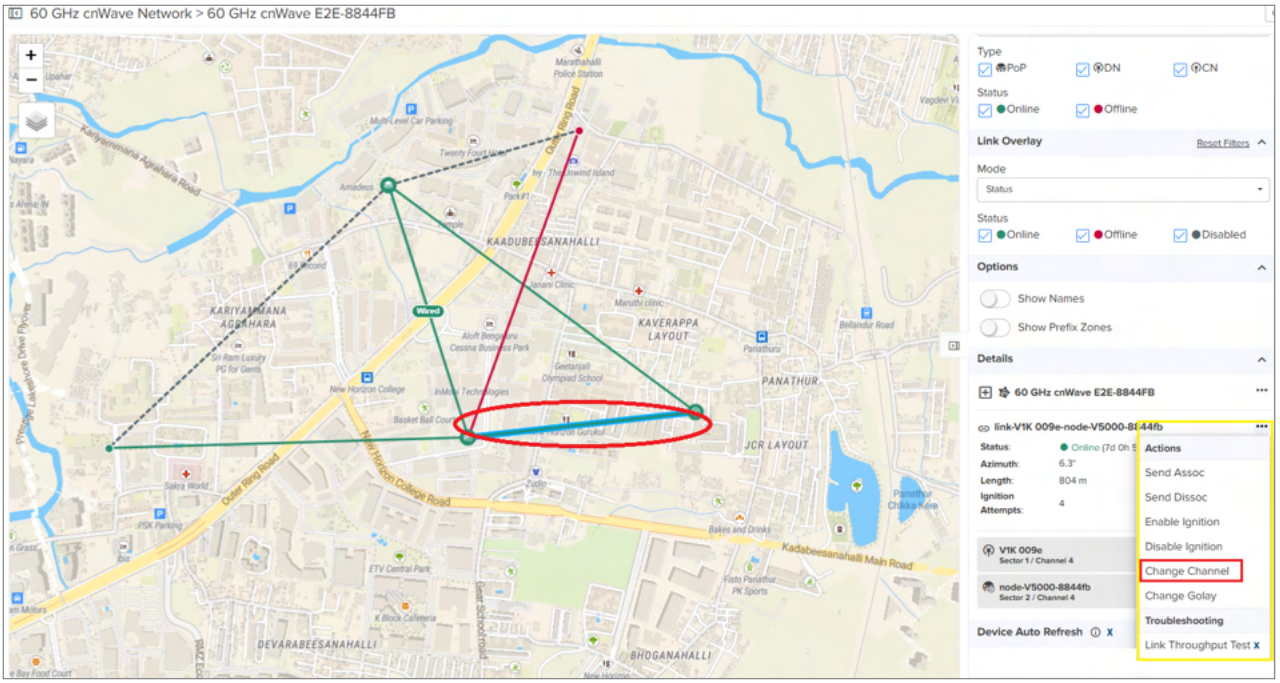
There may be an interference issue found when all the 60 GHz cnWave links in a **particular sector** have the same channel. In such a scenario, you can update or change the channel for all the links of a particular sector using the **Maps** page in cnMaestro UI.

Complete the following steps to change the channel:

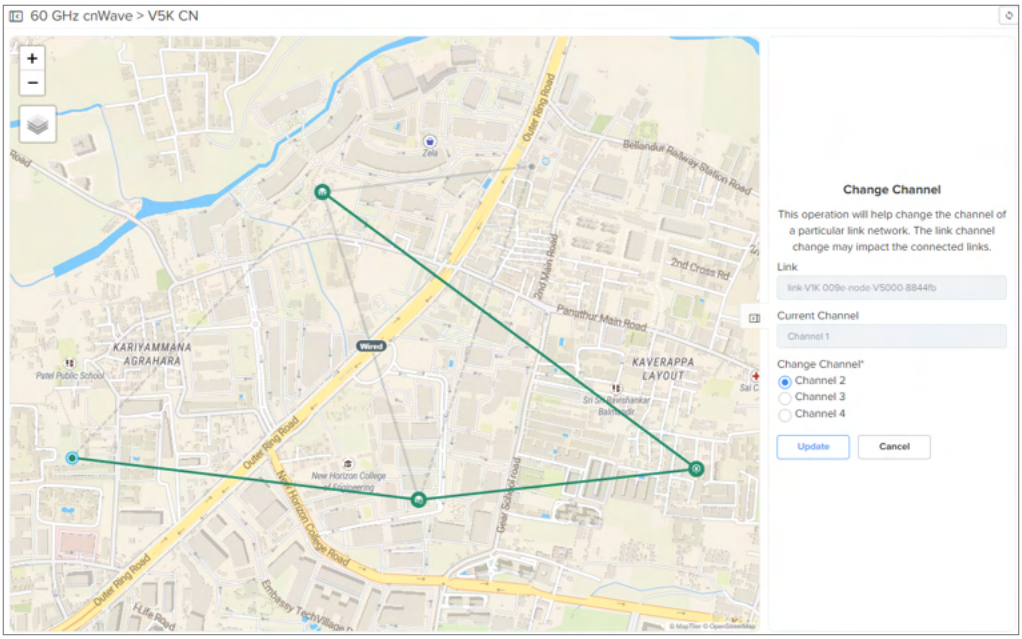
1. On the **Map** page, select a cnWave network and click on the link for which you want to change the channel.

   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

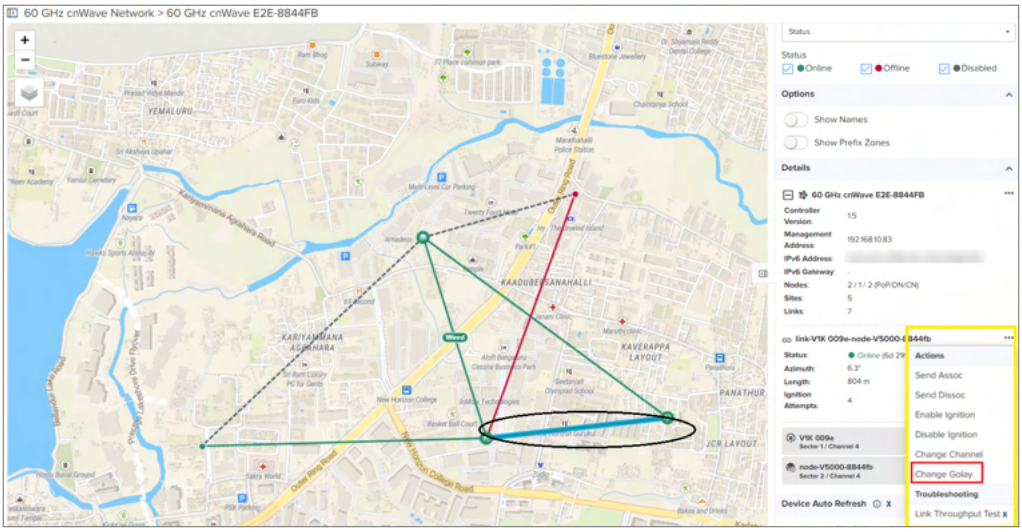
Using the **Maps** page in cnMaestro UI, you can change the Golay code for a **particular 60 GHz cnWave link** established between two nodes (not a sector) to avoid interference. Complete the following steps to change the

Golay:

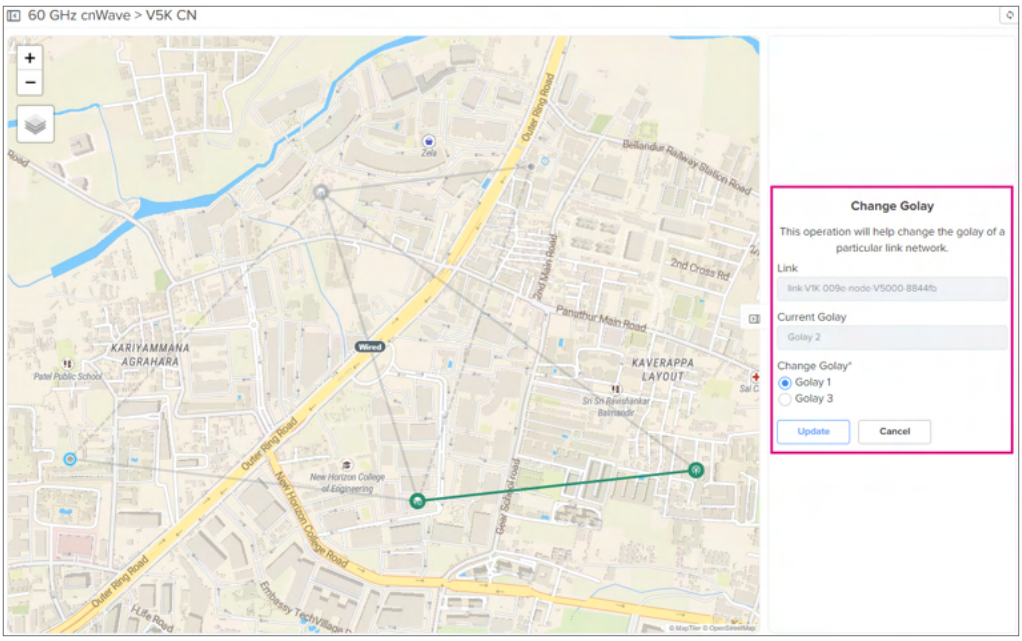
1. On the **Map** page, select a cnWave network and click on the link for which you want to change the Golay code.

   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.

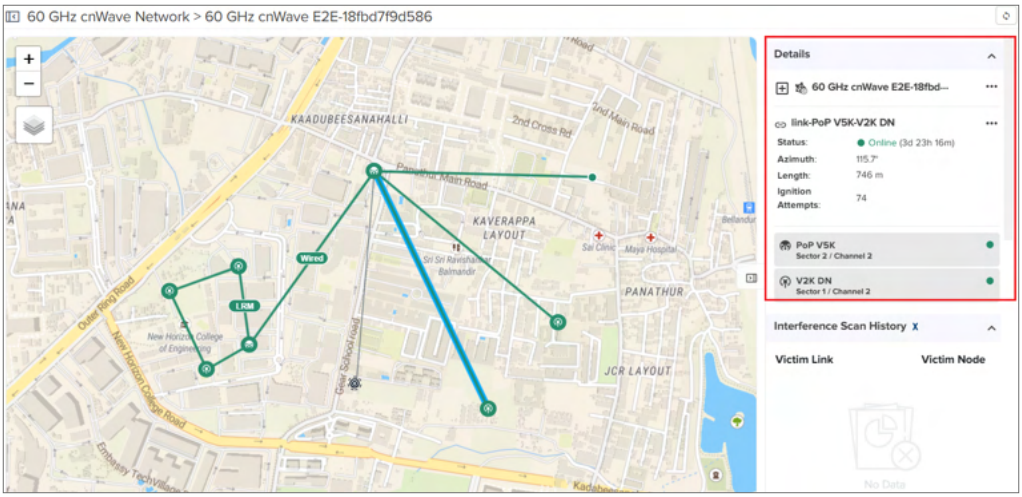
Setting the Last Resort Metric (LRM) for a cnWave 60 GHz link

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:

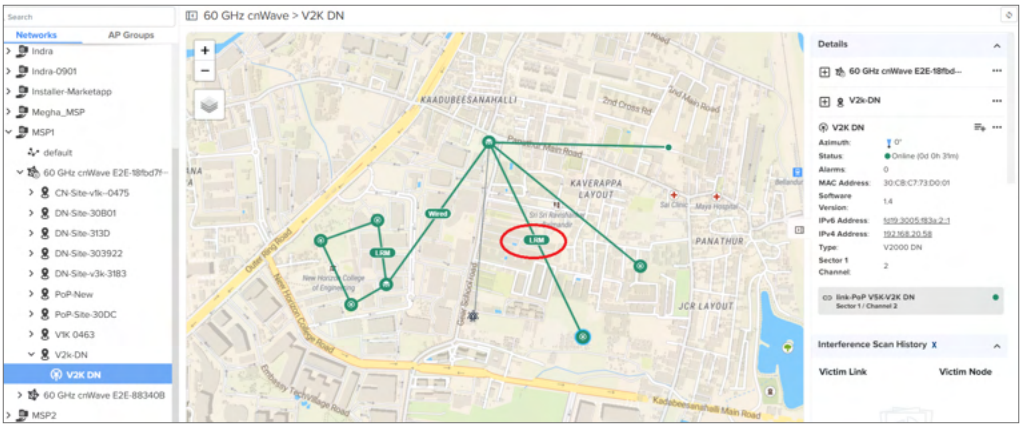
1. On the **Map** page, select a cnWave network and click on the link for which you want to set the last resort metric.

   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.

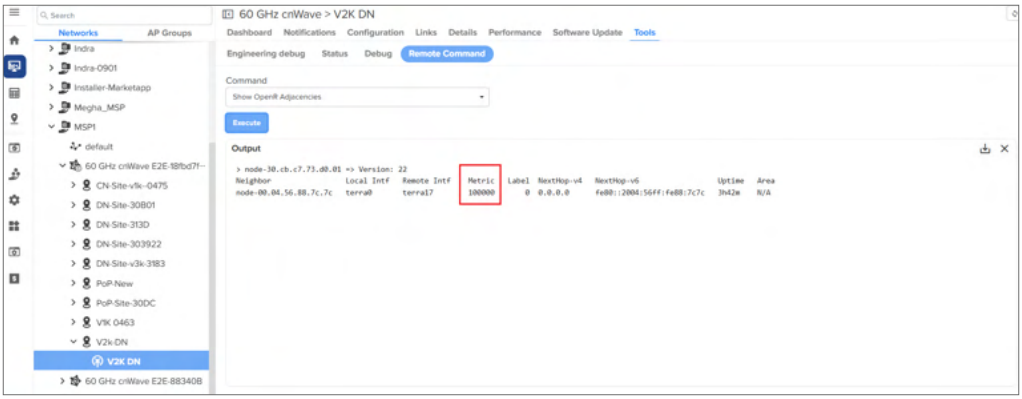
   When you select the **Set Last Resort Metric** option, a message appears indicating that the last resort metric is set successfully. You can see an **LRM** indicator on the selected link, as shown in the figure below.



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**.

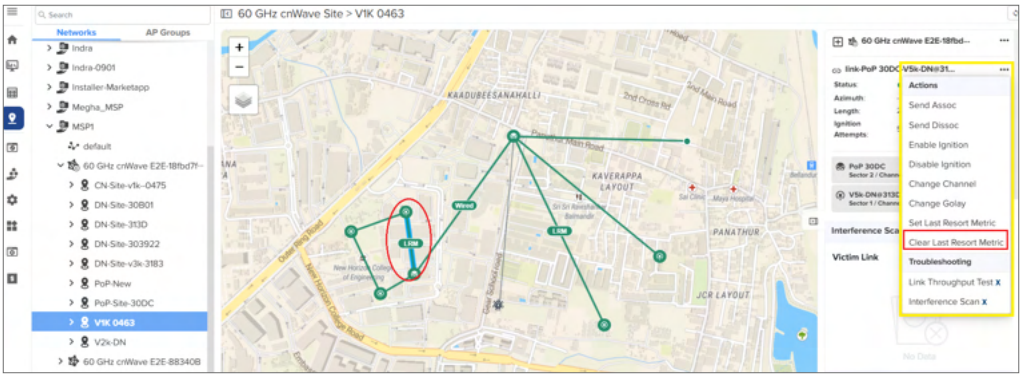
   The **Remote Command** page displays the output, indicating the last resort metric value (which is 100000). This mechanism also indicates that the link with the highest metric value is the last preferred link for routing traffic when other links are unavailable.



   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:

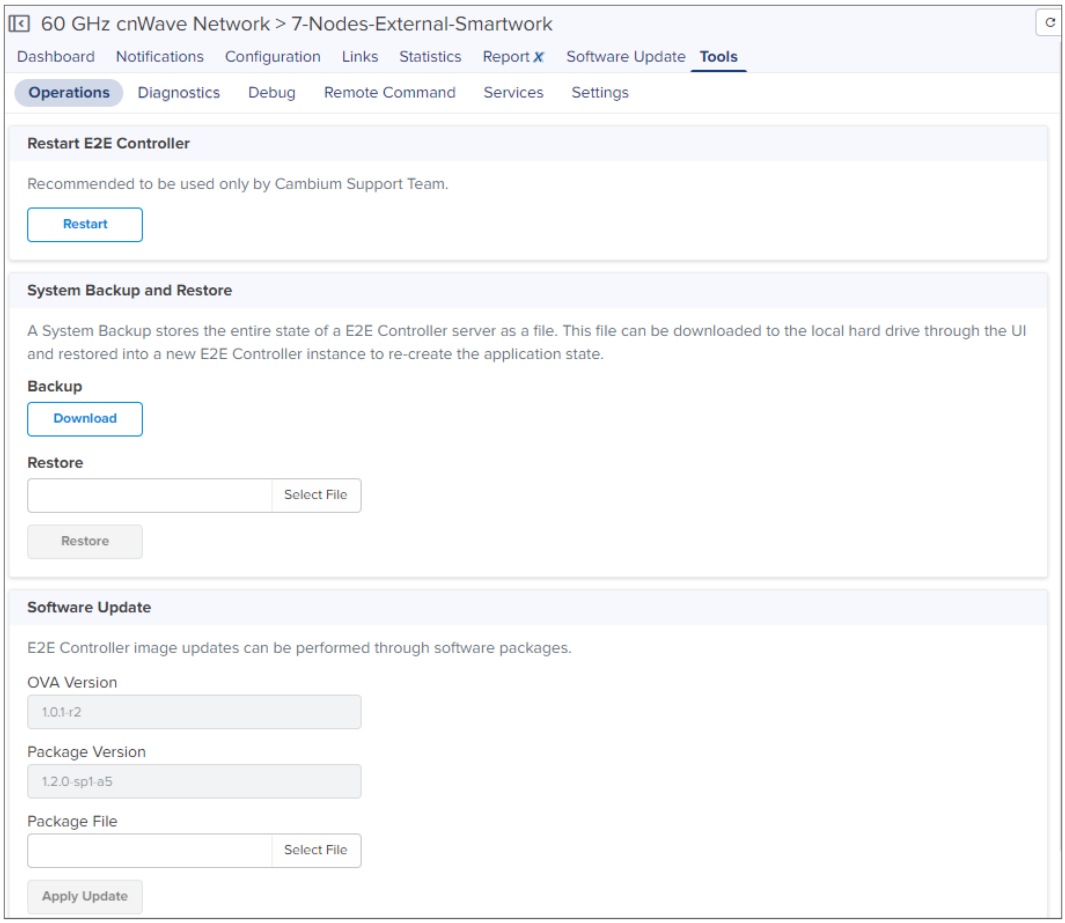
- Operations
- Diagnostics
- Debug
- Remote Command
- Services
- Settings

Operations

External E2E Controller deployment

If the device is deployed through **External E2E Controller** it displays the operations page as follows:

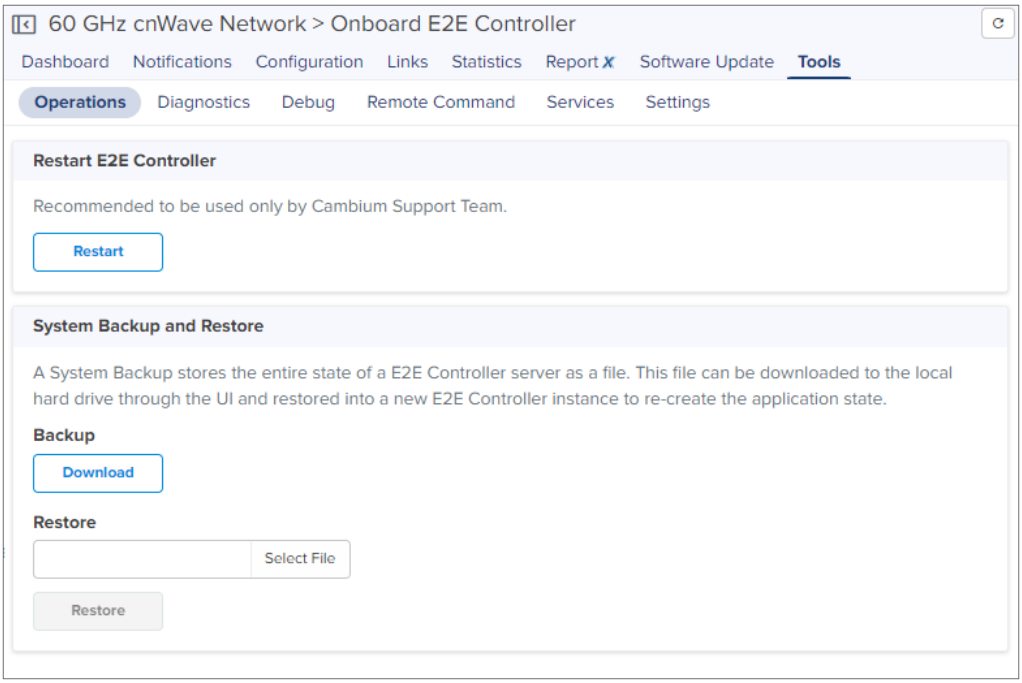
- **Restart E2E Controller** performs the **Restart.**
- A **System Backup and Restore** the entire state of a E2E Controller server as a file and file can be used to transfer data between two E2E Controller instances. It can be saved in local hard drive through the UI and restored into a new E2E Controller instance to re-create.
- The **Software Upgrade** is to upgrade E2E controller and can be done through E2E controller package.



Onboard E2E Controller deployment

Onboard 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.

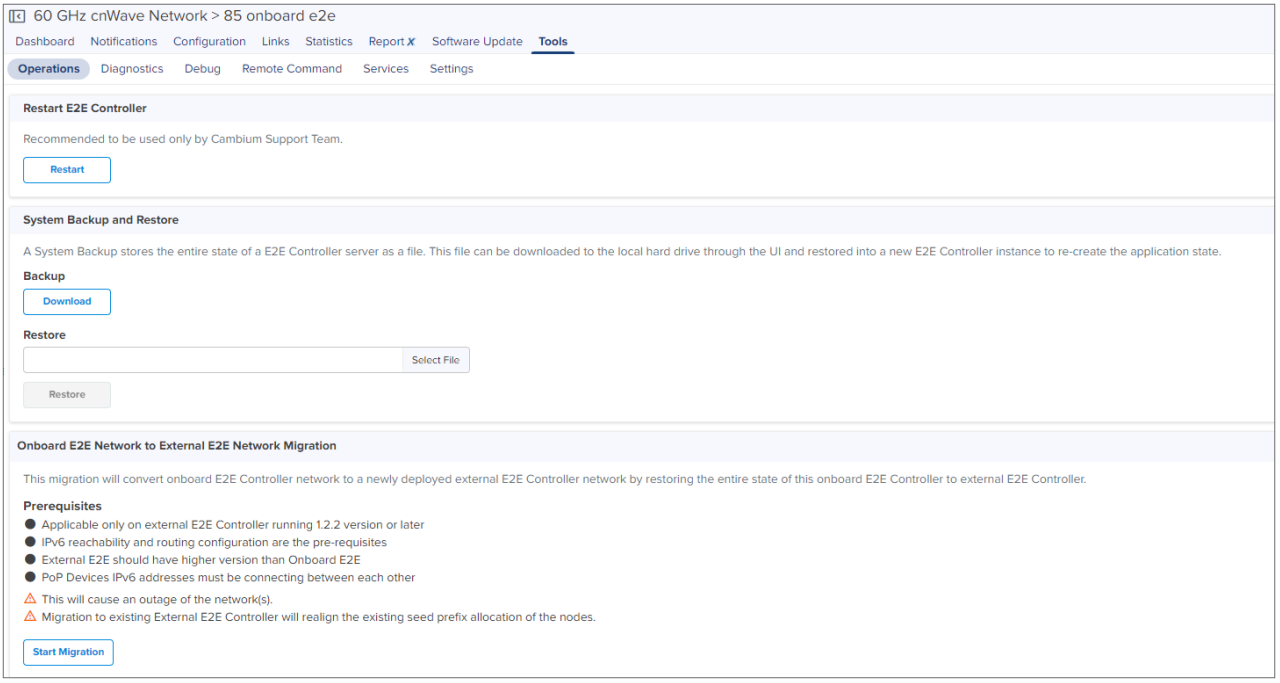


Onboard E2E Controller deployment

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.



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:

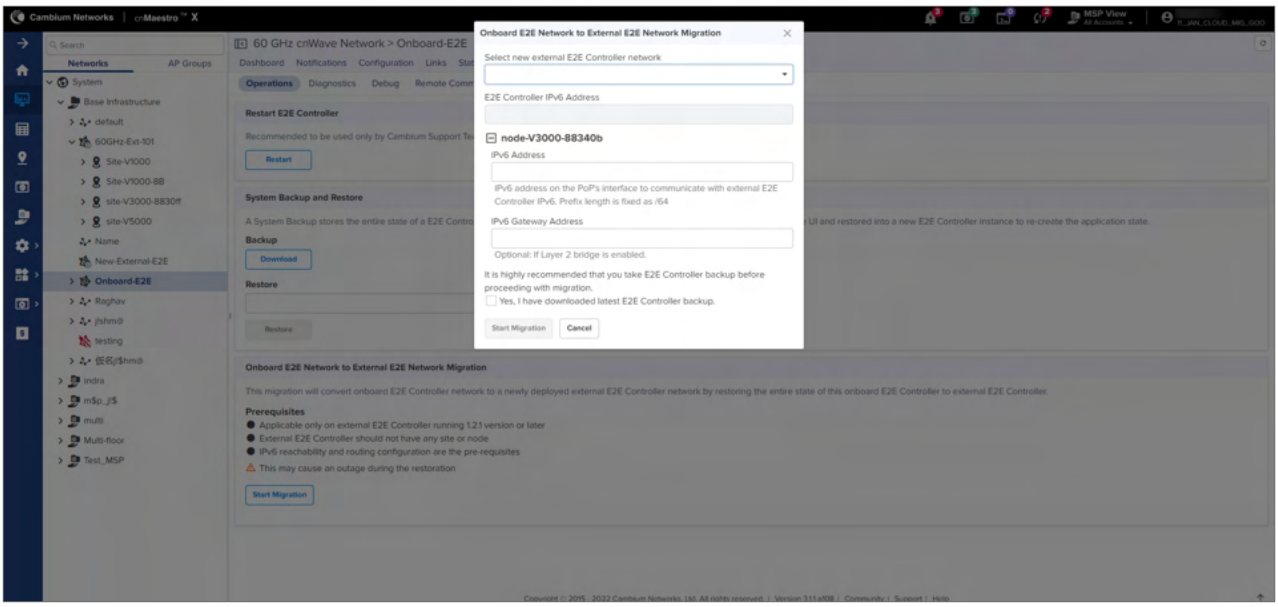
- Multi-PoP / Relay Port should be updated with the interface as in PoP interface configuration if not already done, to allow the connection between PoPs.
- If the existing E2E Network if configured with BGP, migrated PoP BGP Configuration must be updated in cnMaestro and then in POP GUI
- If the PoPs 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.

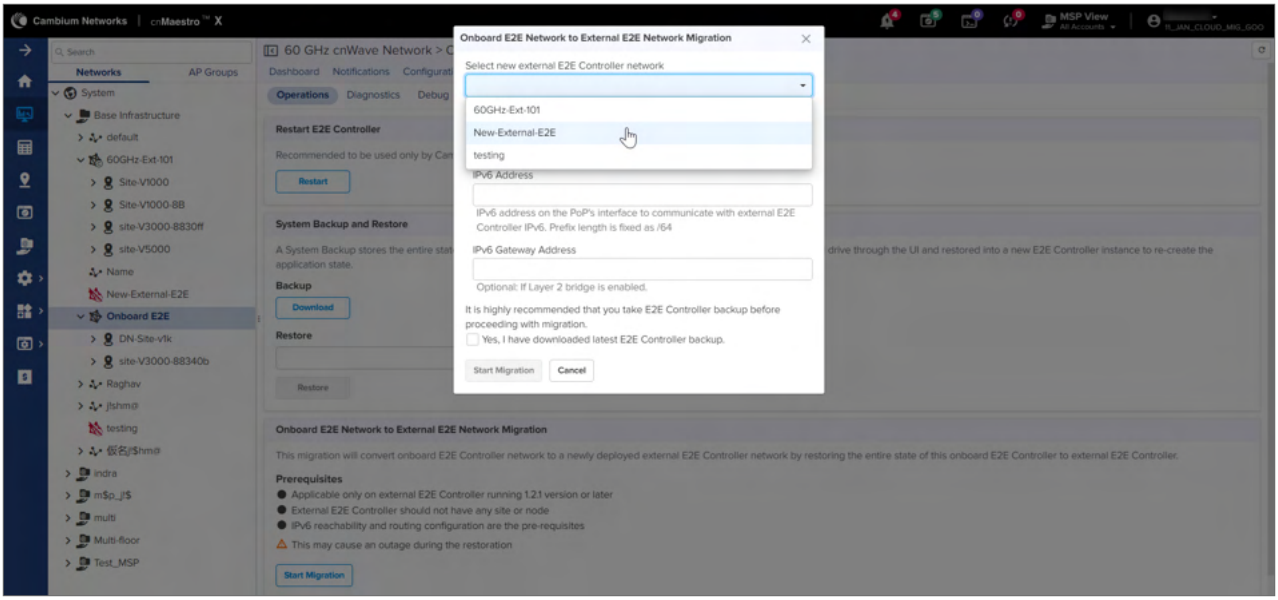
Perform the following steps to migrate Onboard E2E Controller to External E2E Controller:

1. Select Onboard E2E Network > **Tools** > **Operations.**
2. Click **Start Migration**.

   The **Onboard E2E Controller to External E2E Migration** window appears.

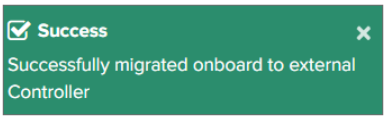


3. Select a new external E2E Controller network from the dropdown.

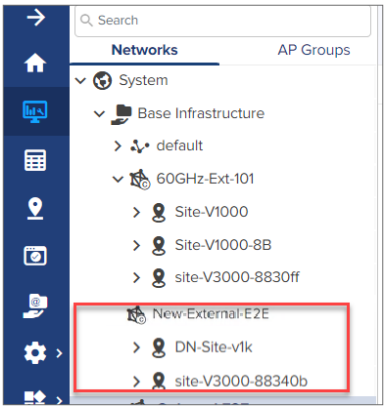


4. Enter **IPv6 Address**.
5. Enter **IPv6 Gateway Address** of PoP node, which is optional.
6. Select the checkbox next to **Yes, I have downloaded latest E2E Controller backup**.
7. Click **Start Migration**.

   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.

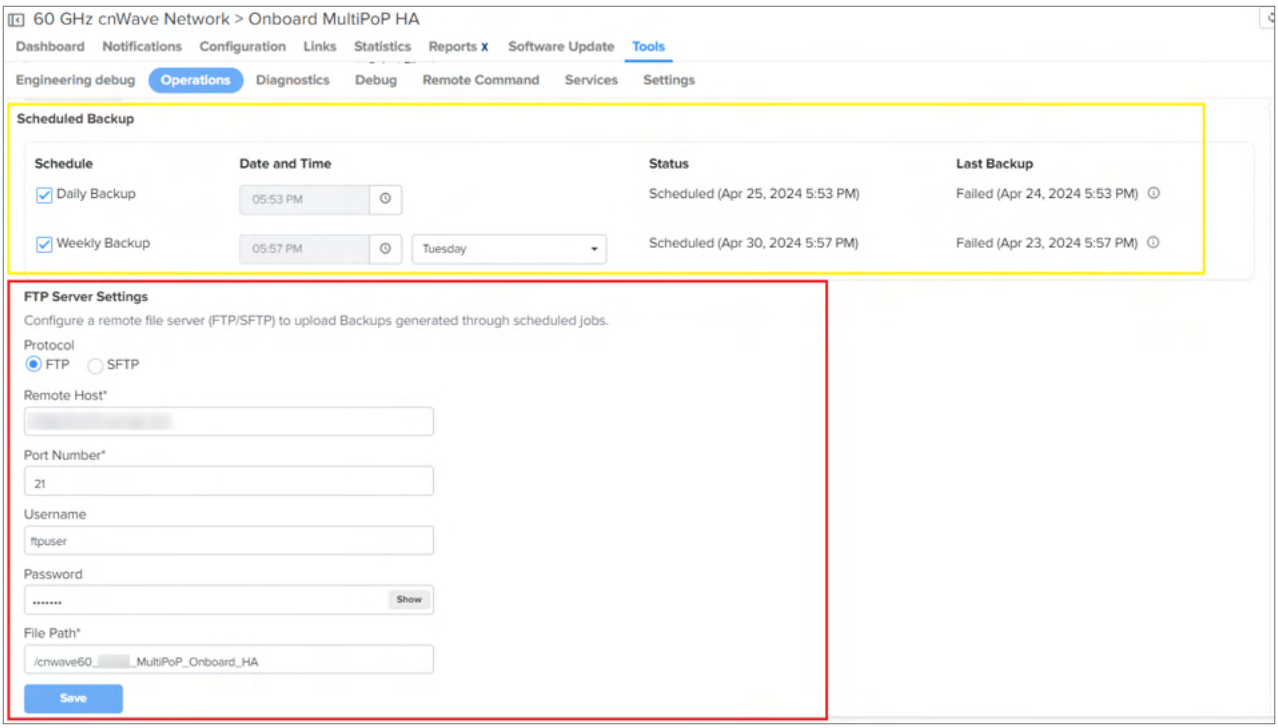


   Table 86 lists the parameters required for configuring the remote FTP or sFTP server.

   Table 86 *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.
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.

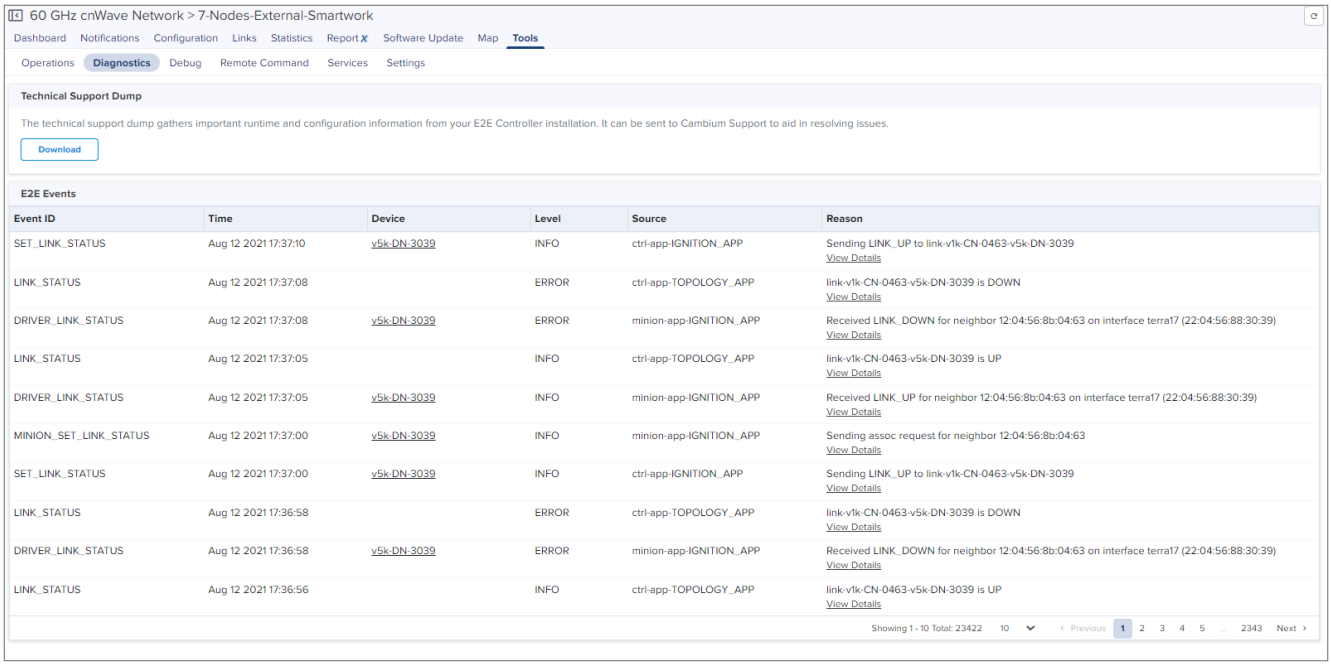
     The **Status** field in the **Scheduled Backup** section displays date and time of the scheduled job. Similarly, the **Last Backup** field displays date and time of the last failed job.

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 314 *Diagnostics*



Debug

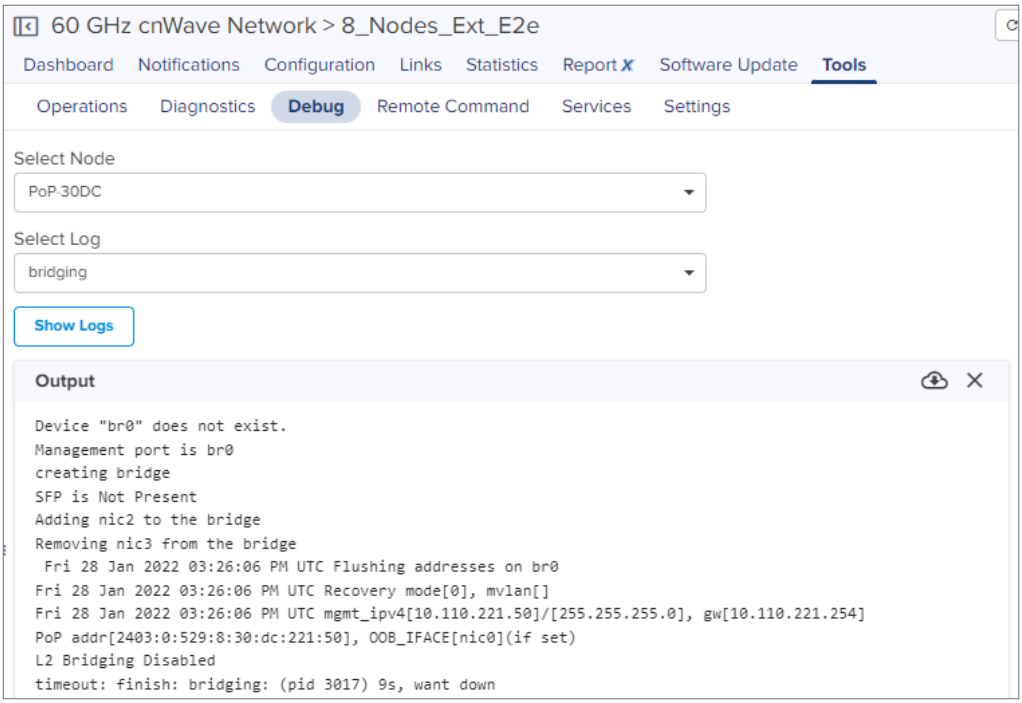
In **Debug** tab, you can view and download the Node logs by executing the following log:

- 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

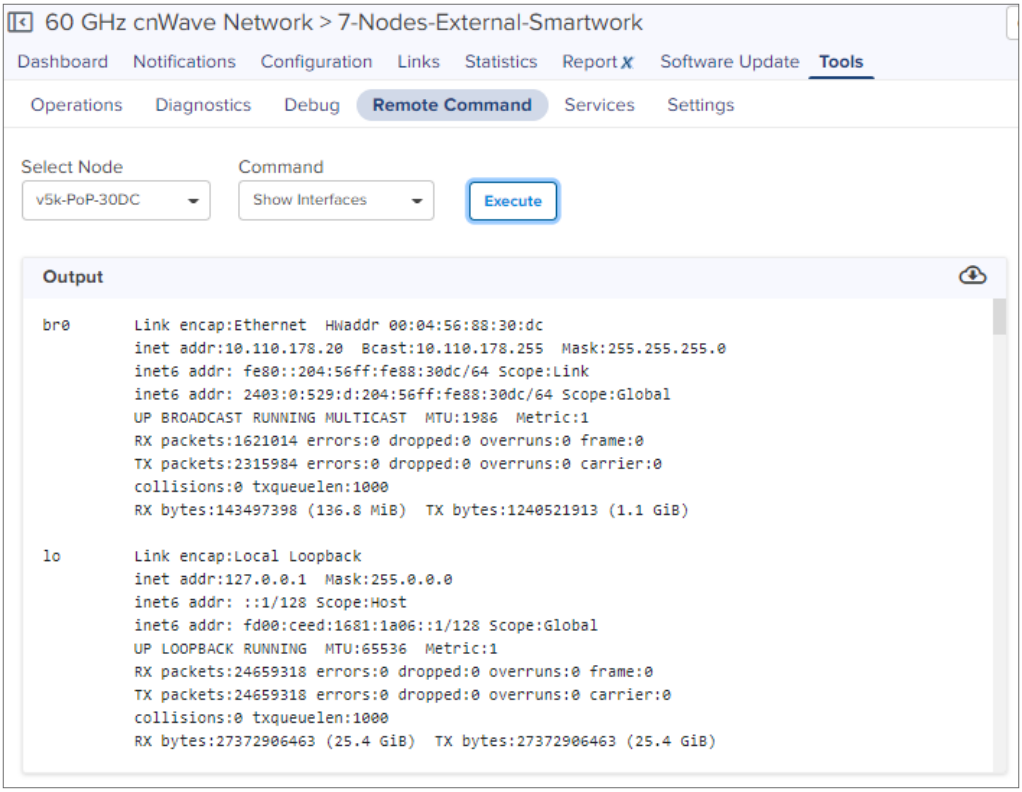
In **Remote Command** tab, user can view or download command logs by executing the following command:

- 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:



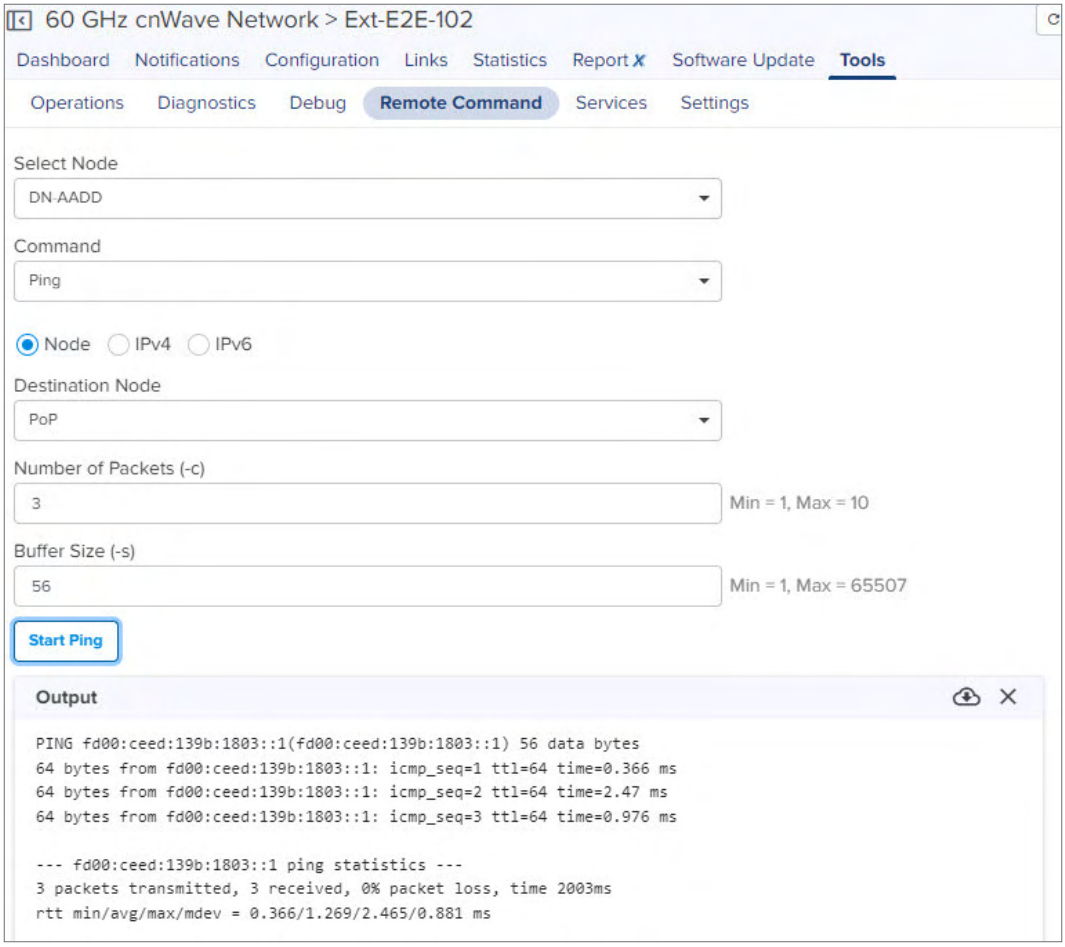
5. Click the download ( ) icon to download the generated output.
6. Click the clear (×) icon to clear the generated output.

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 315.

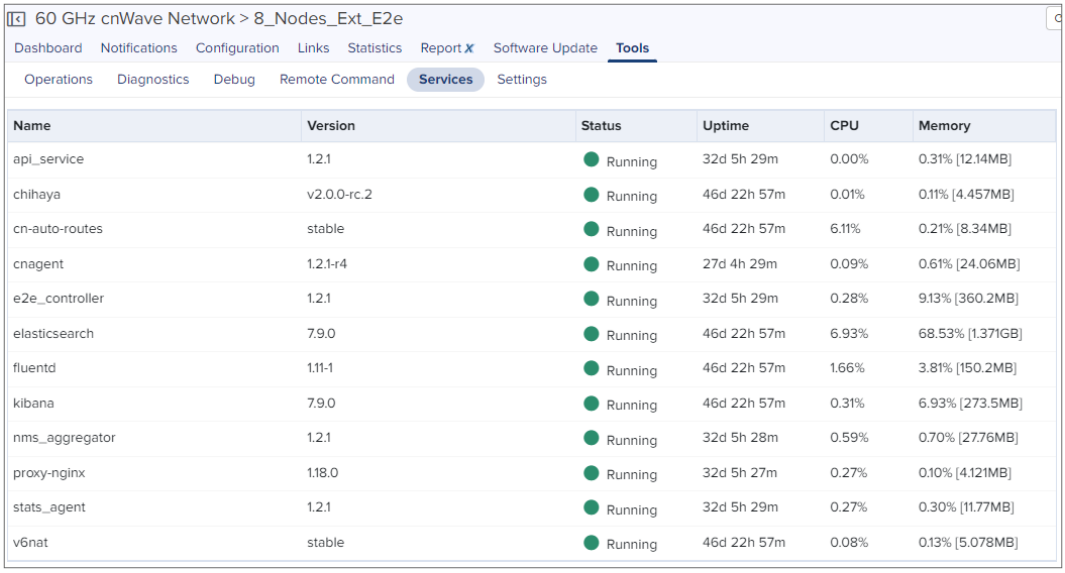
Figure 315 *Remote Command: Ping*



Services

In **Services** page user can view the services running in E2E Controller.

Figure 316 *Services*



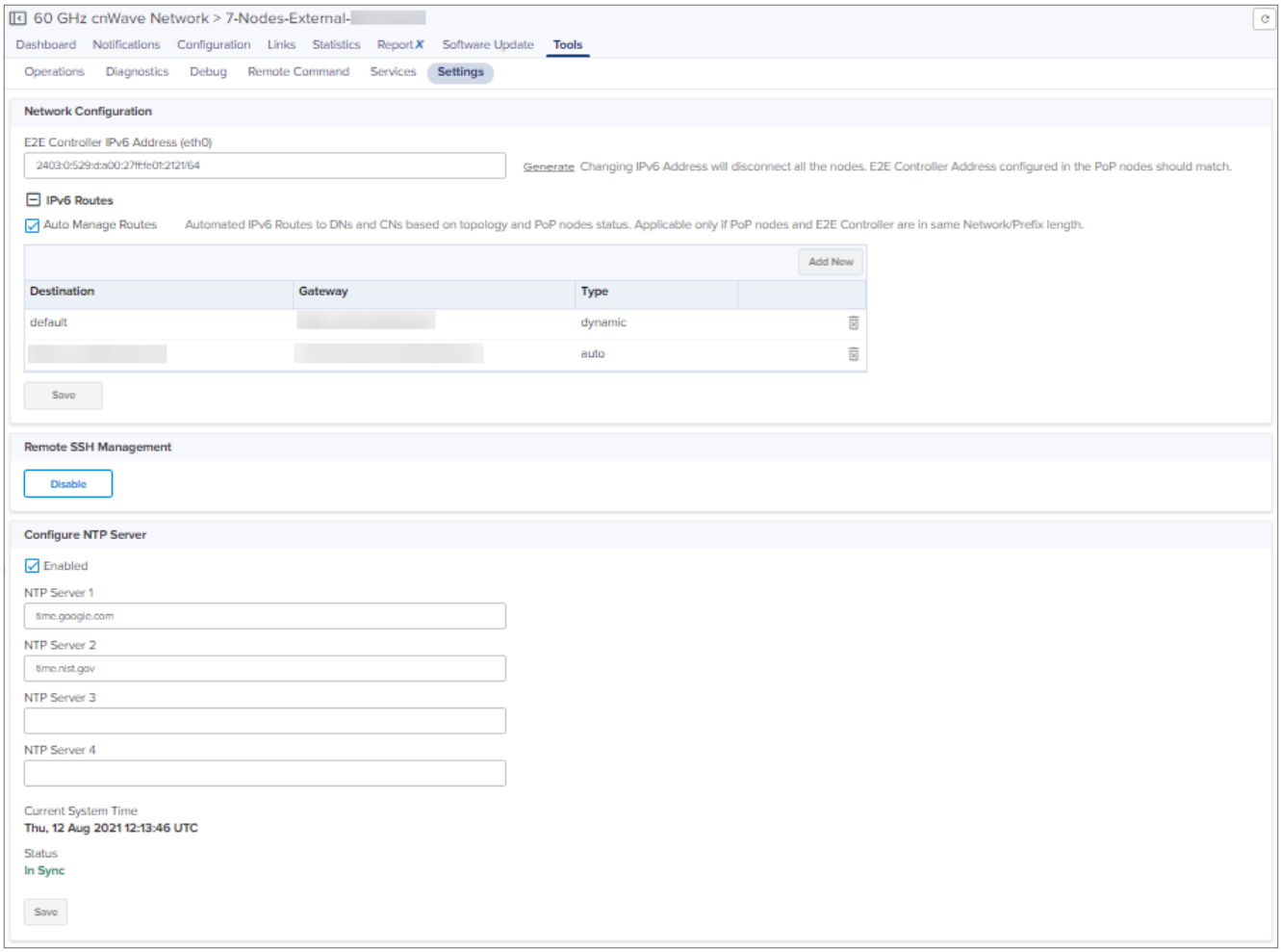
Name	Version	Status	Uptime	CPU	Memory
api_service	1.2.1	Running	32d 5h 29m	0.00%	0.31% [12.14MB]
chihaya	v2.0.0-rc.2	Running	46d 22h 57m	0.01%	0.11% [4.457MB]
cn-auto-routes	stable	Running	46d 22h 57m	6.11%	0.21% [8.34MB]
cnagent	1.2.1-r4	Running	27d 4h 29m	0.09%	0.61% [24.06MB]
e2e_controller	1.2.1	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

In **External E2E ControllerSettings** page you can configure the **Network Configuration, IPv6 Routes, Remote SSH Management,** and **NTP Server**.



In **Network Configuration** user can configure the **E2E Controller IPv6 Address** and **IPv6 Routes**.

To change **E2E Controller IPv6 Address**, perform the following:

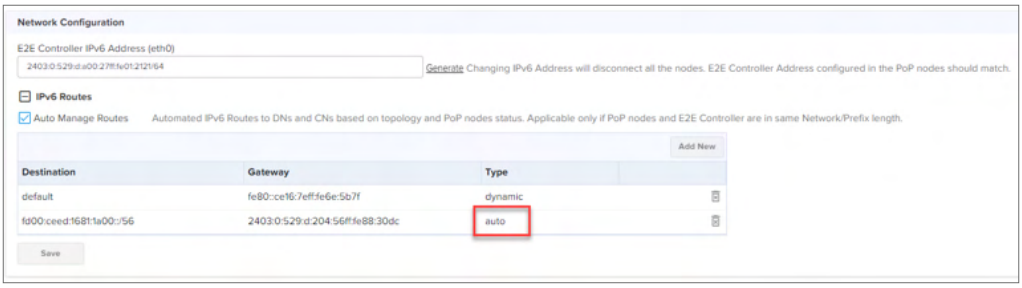
1. Navigate to **Tools** > **Settings** > **Network Configuration** tab.
2. Click **Generate** to automatically generate IPv6 address or manually change the IPv6 Address of E2E Controller.
3. Click **Save**.

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.

To Enable Auto Managed Routes:

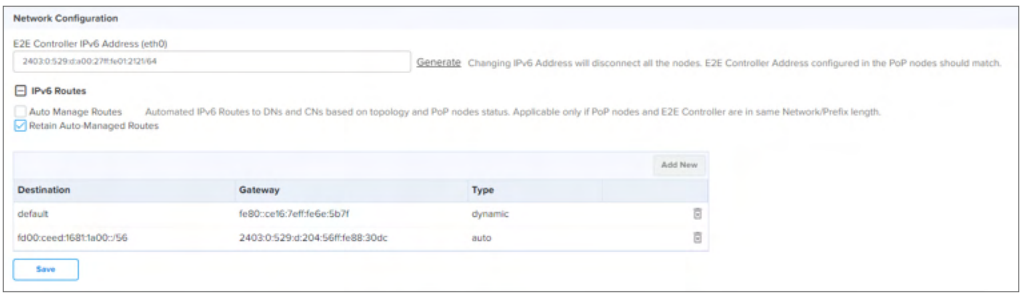
1. Navigate to **Tools** > **Settings** > **Network Configuration** tab.
2. Enable **Auto Manage Routes**.
3. Click **Save**.



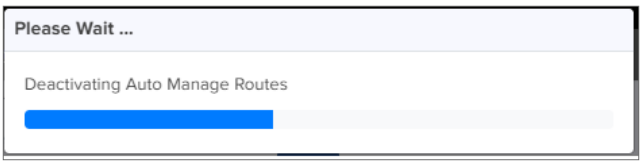
If IPv6 routes are managed through auto manage routes, the in the **Type** column the value is displayed as **Auto**.

To retain auto-managed routes, even after auto-managed routes is disabled, complete the following steps:

1. Navigate to **Tools** > **Settings** > **Network Configuration** tab.

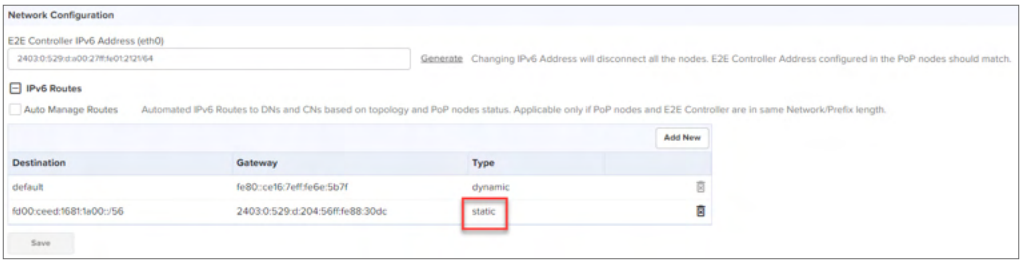


2. Enable **Retain Auto-Managed Routes.**
3. Click **Save.**



4. Please wait pops-up.

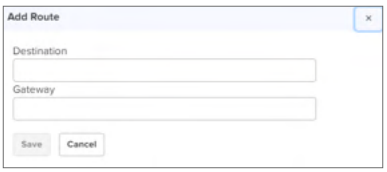
   Once the Auto Manage Routes is disabled, IPv6 routes can be managed through static routes and in type it displays as **Static**.



5. Click **Save**.

To add new static **IPv6 Routes**:

1. Click **Add New**.

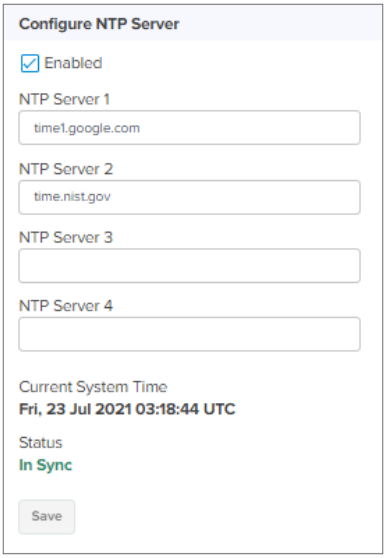


2. Enter **Destination** and **Gateway**.
3. Click **Save.**

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.

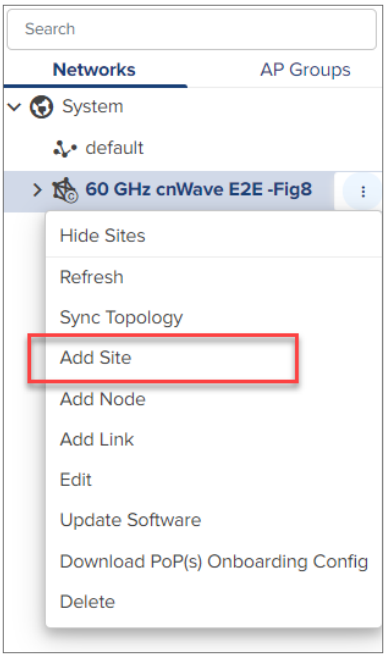


Site Configuration

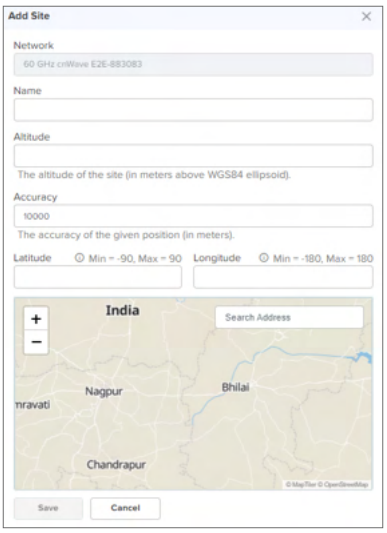
Sites are located within the networks and wireless access points attached to it.

To Add a Site

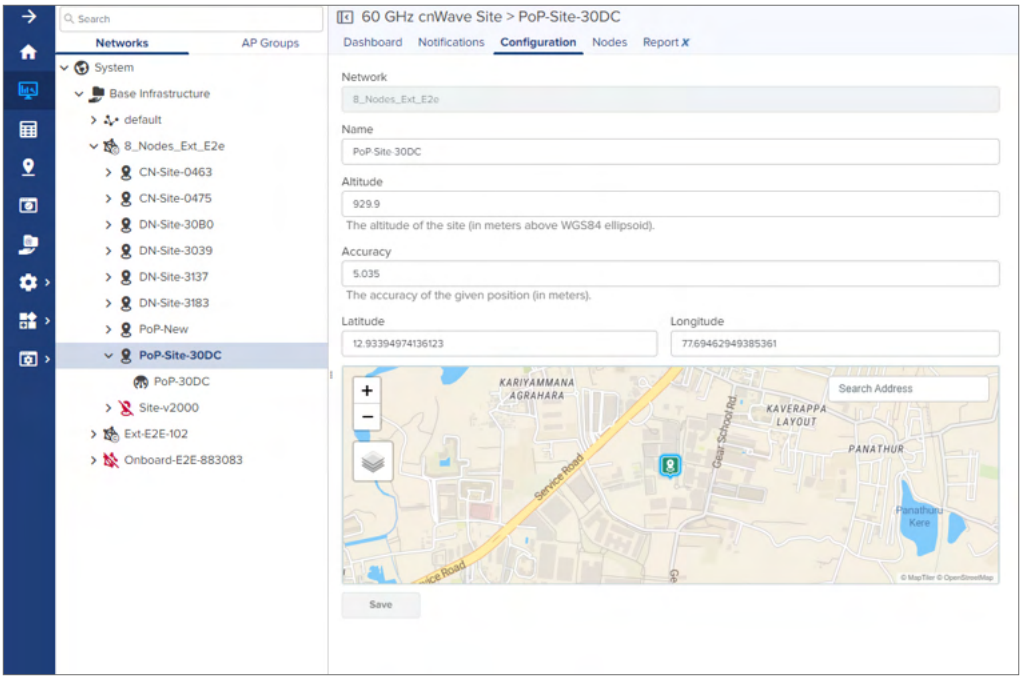
1. Navigate to **Network** and click ⋮ icon.
2. Select **Add Site** from the dropdown.



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.

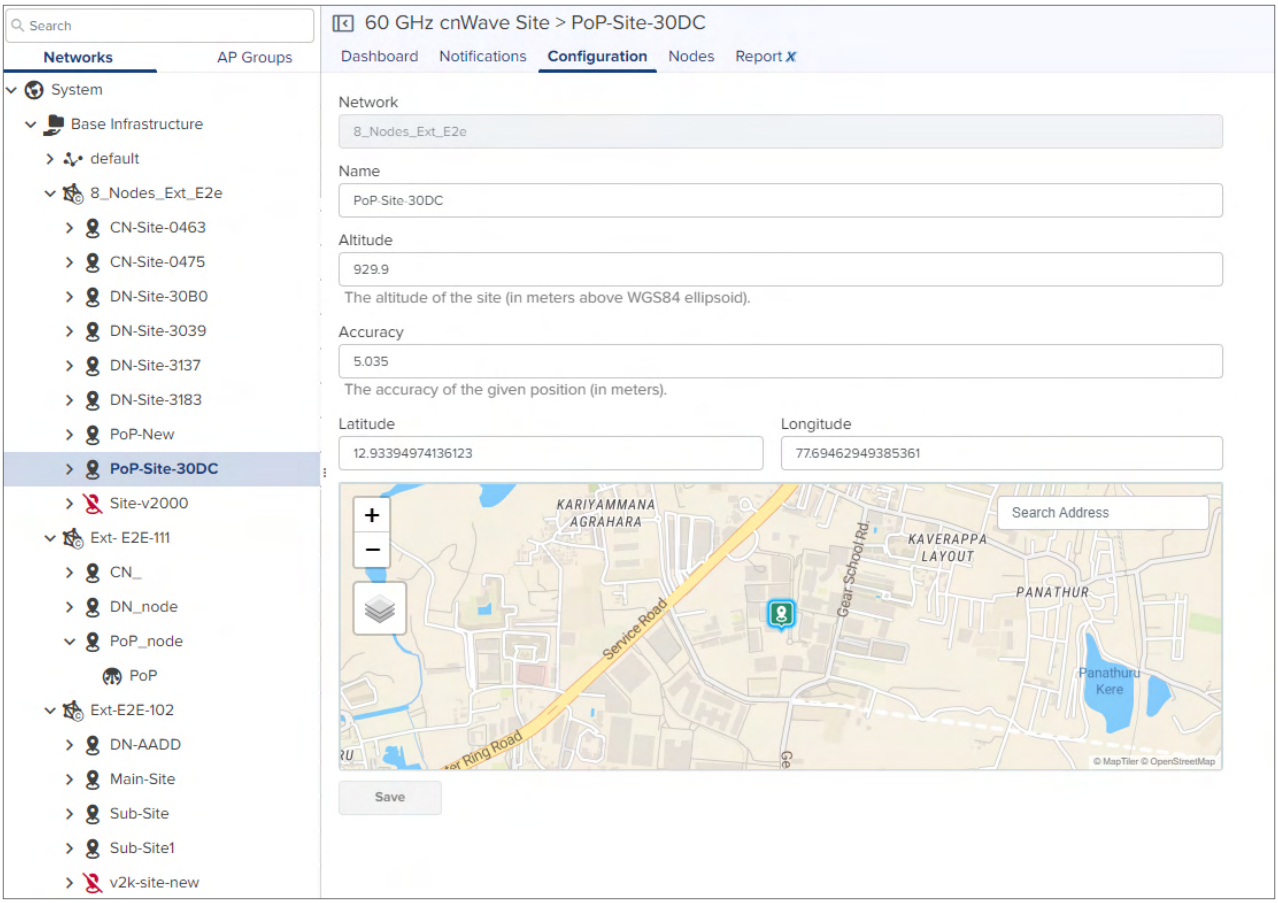


5. Click **Save**. When the Site is configured it gets added under the E2E Network.



To edit the **Site** perform the following:

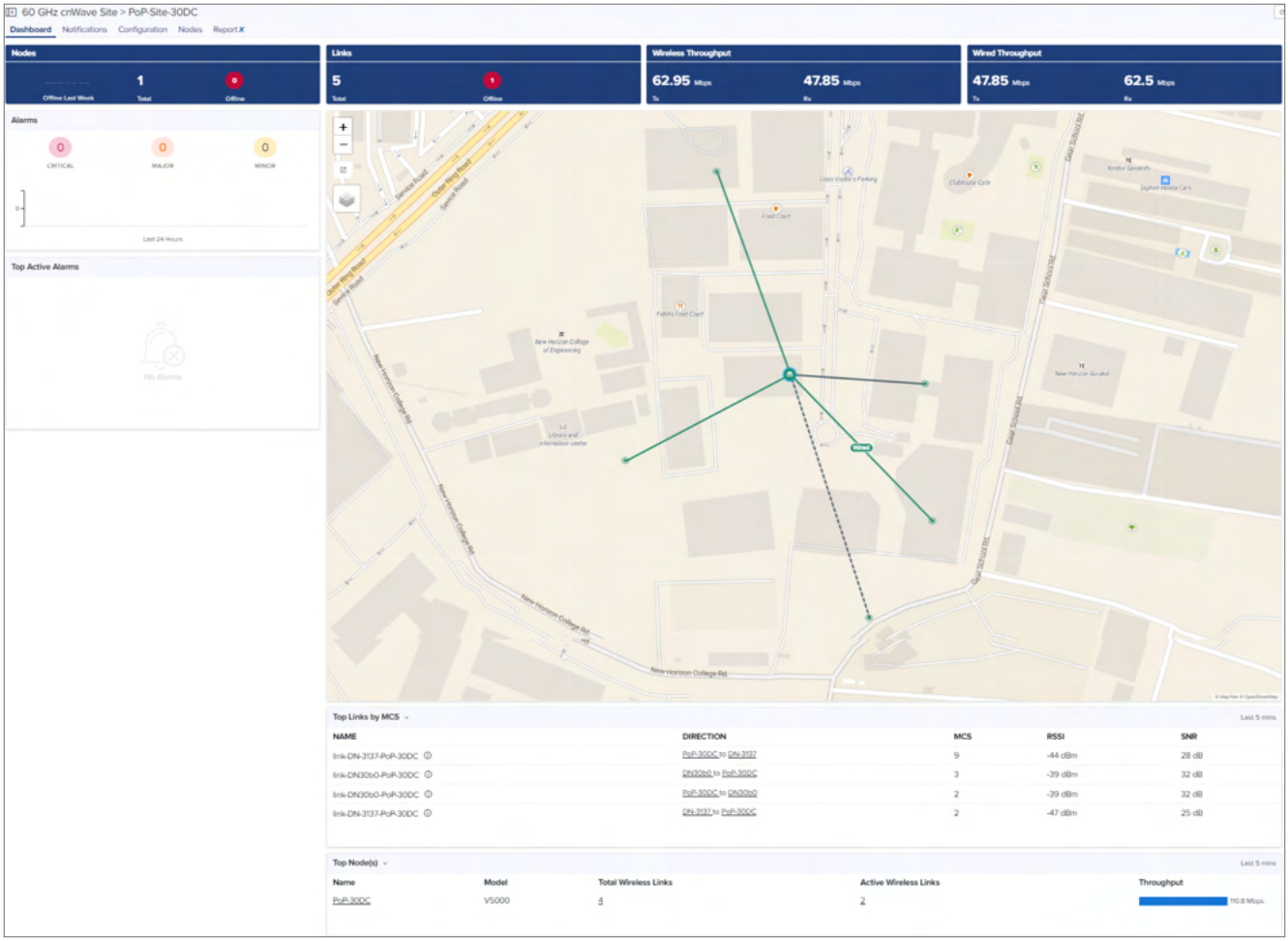
1. Navigate to **Network** > **Site** > **Configuration**.
2. Edit the details and click **Save.**



Site Dashboard

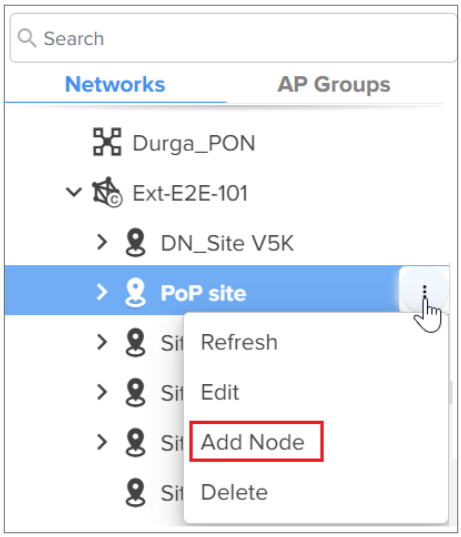
Dashboard pages are customized for each device type and aggregation level. The Site dashboard section displays the **Nodes, Links, Wireless Throughput, Wired Throughput, Alarms, Top Active Alarms, Top Links by MCS, Top Links by RSSI, Top Links by SNR, Top Node(s), Top PoP(s), Top DN(s), and Top CN(s).**

Figure 317 *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**.

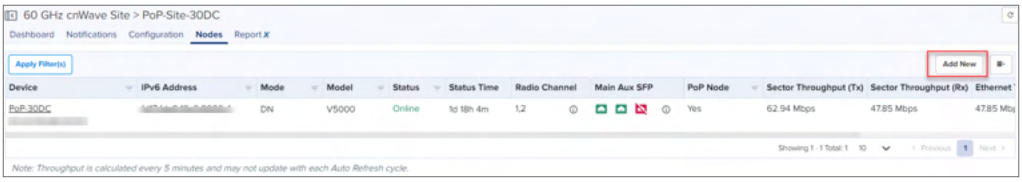


Note

From 3.1.1 release V2000 device (beta version) is supported.

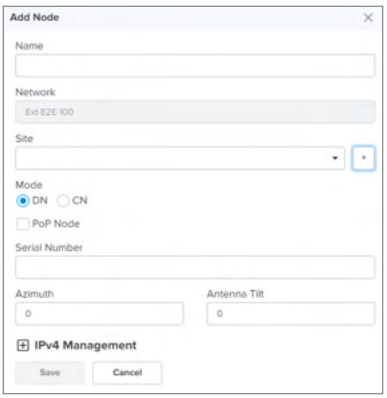
To Add a Node:

1. Navigate to the **Network** > **Site** > **Nodes.**



   Add Node window pops-up.

2. Click **Add new.**



3. Click to add site.

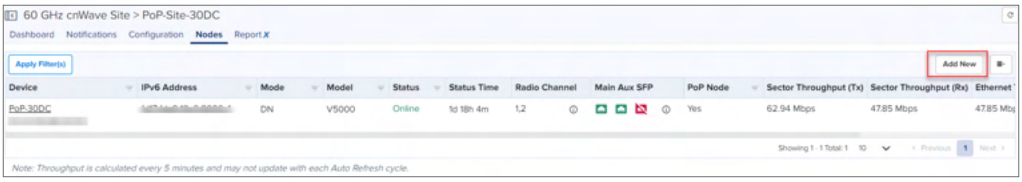
Adding the Node allows the user to create the different Nodes as shown below:

- PoP Node
- DN
- CN

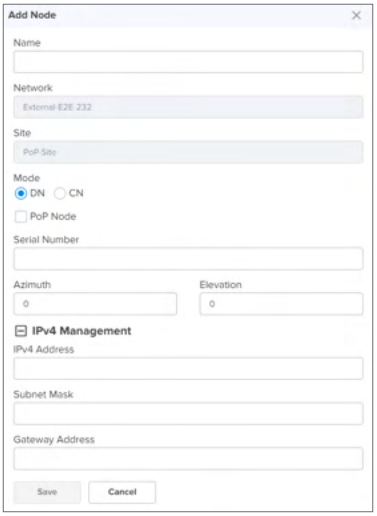
PoP Node configuration

To add a PoP Node:

1. Navigate to the **Network** > **Site** > **Nodes.**
2. Click **Add New.**



3. **Add Node** window pops-up.



4. Enter the **PoP Name**, select the Mode **DN.**
5. Enable **PoP Node**.

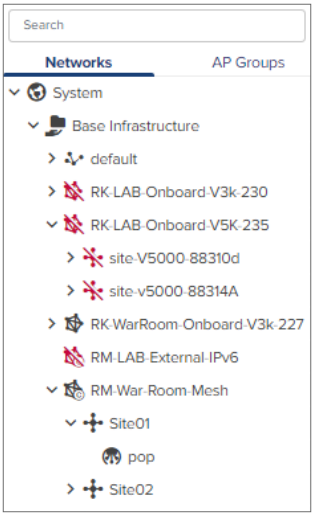
> **Note**
>
> Once the PoP Node is enabled user needs to select the **Routing** and **Interface** details**.**

6. Enter the **MAC Address**, and select the device **Model** from the dropdown.
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.**
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.

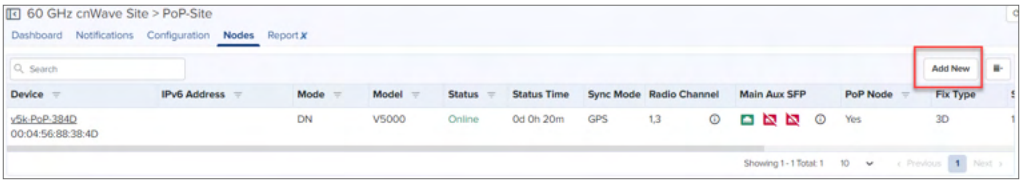
Once the **PoP** node is configured it gets listed under the **Site.**



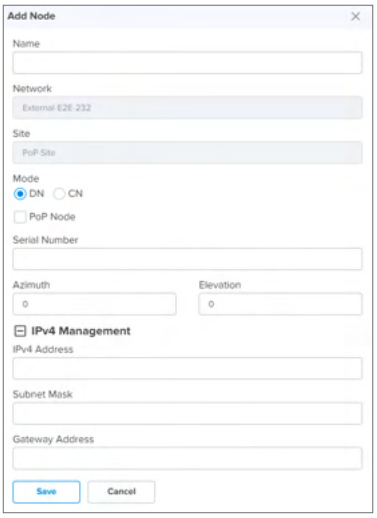
DN/CN Node configuration

To add DN/CN node:

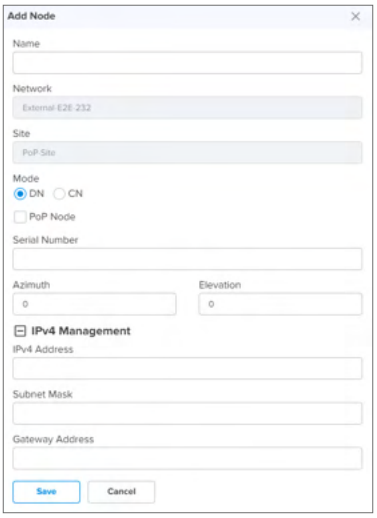
1. Navigate to the **Network** > **Site** > **Nodes.**
2. Click **Add New.**



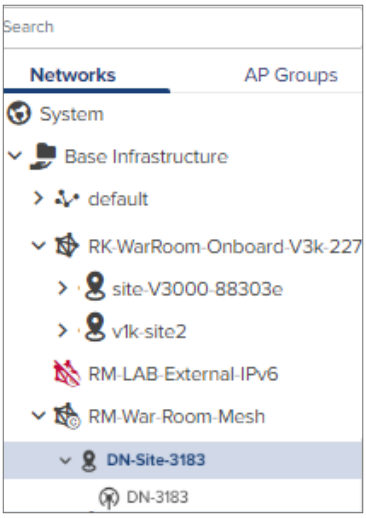
3. **Add Node** window pops-up.



4. Enter the **Node Name**, select the Mode **DN** or **CN.**
5. Enter the **MAC Address**, and select the device **Model** from the dropdown.
6. Enter the **Azimuth** and **Elevation**.



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

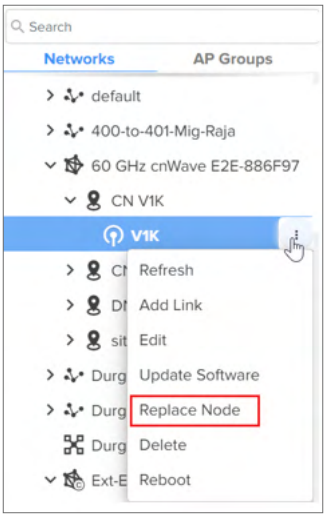
Replace Node allows to replace the existing faulty nodes with new nodes along with the configuration and links of existing faulty nodes.

Note

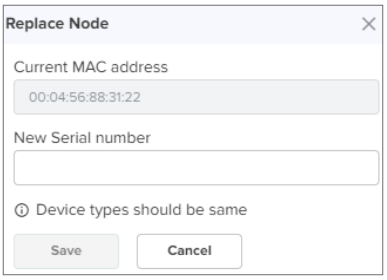
New node should be replaced with same model as existing node.

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.



4. Enter the **New MAC address**.
5. Click **Save**.

PoP Node

Once the PoP node is configured it displays the monitoring panel of the PoP node.

Dashboard

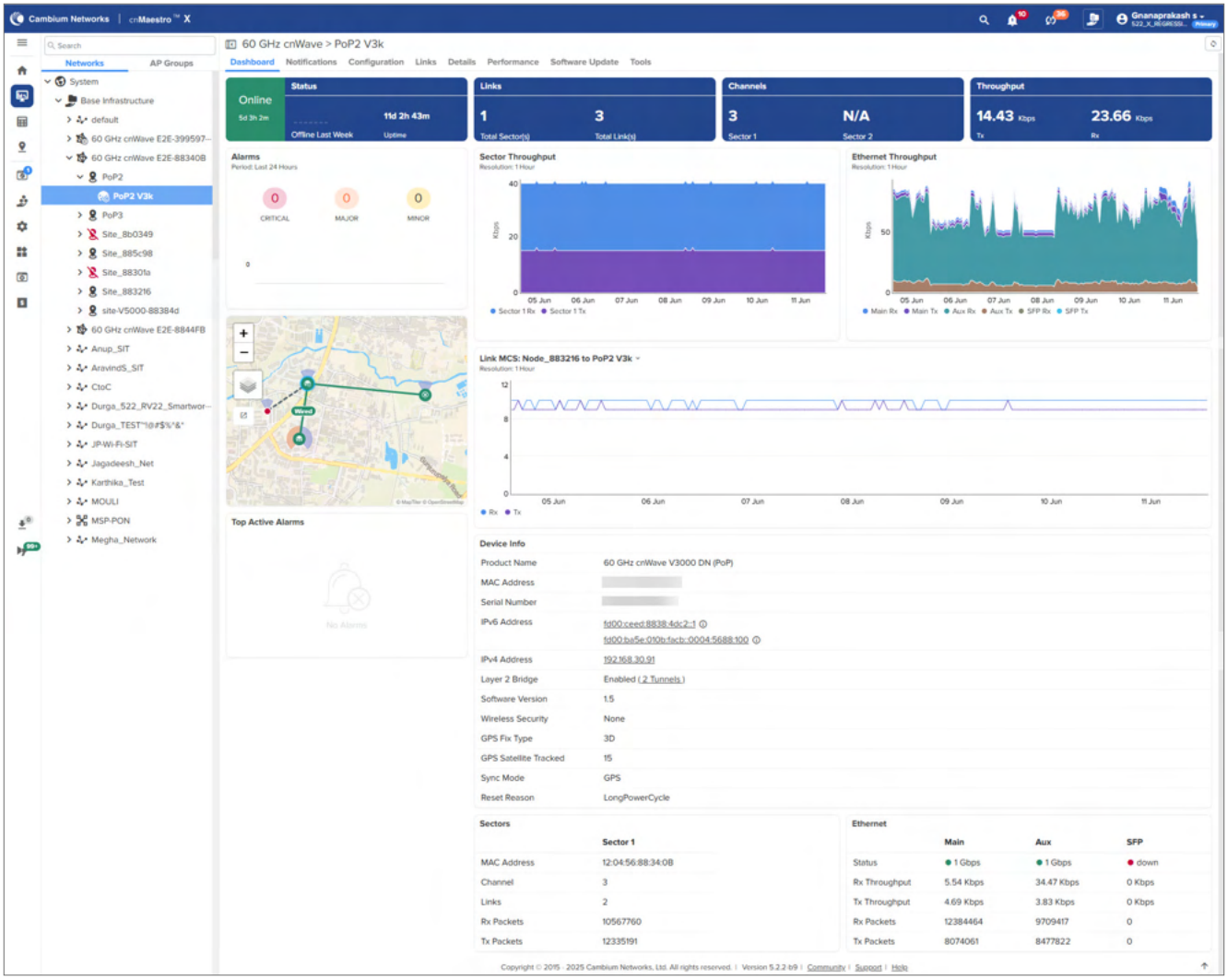
Dashboard pages can be customized for each device type and aggregation level. The PoP node dashboard section displays the **Status, Links, Channels, Throughput, Sector Throughput (Sector 1 and Sector 2), Ethernet Throughput (Main, Aux, SFP**), **Alarms, Top Active Alarms, Link MCS, Device Info, Sectors, and Ethernet**.

To view the Layer 2 Bridge details, click on **Tunnels** under **Device Info**. This navigates to **Details** > Network.

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 318 *PoP Node Dashboard*



Configuration

Basic

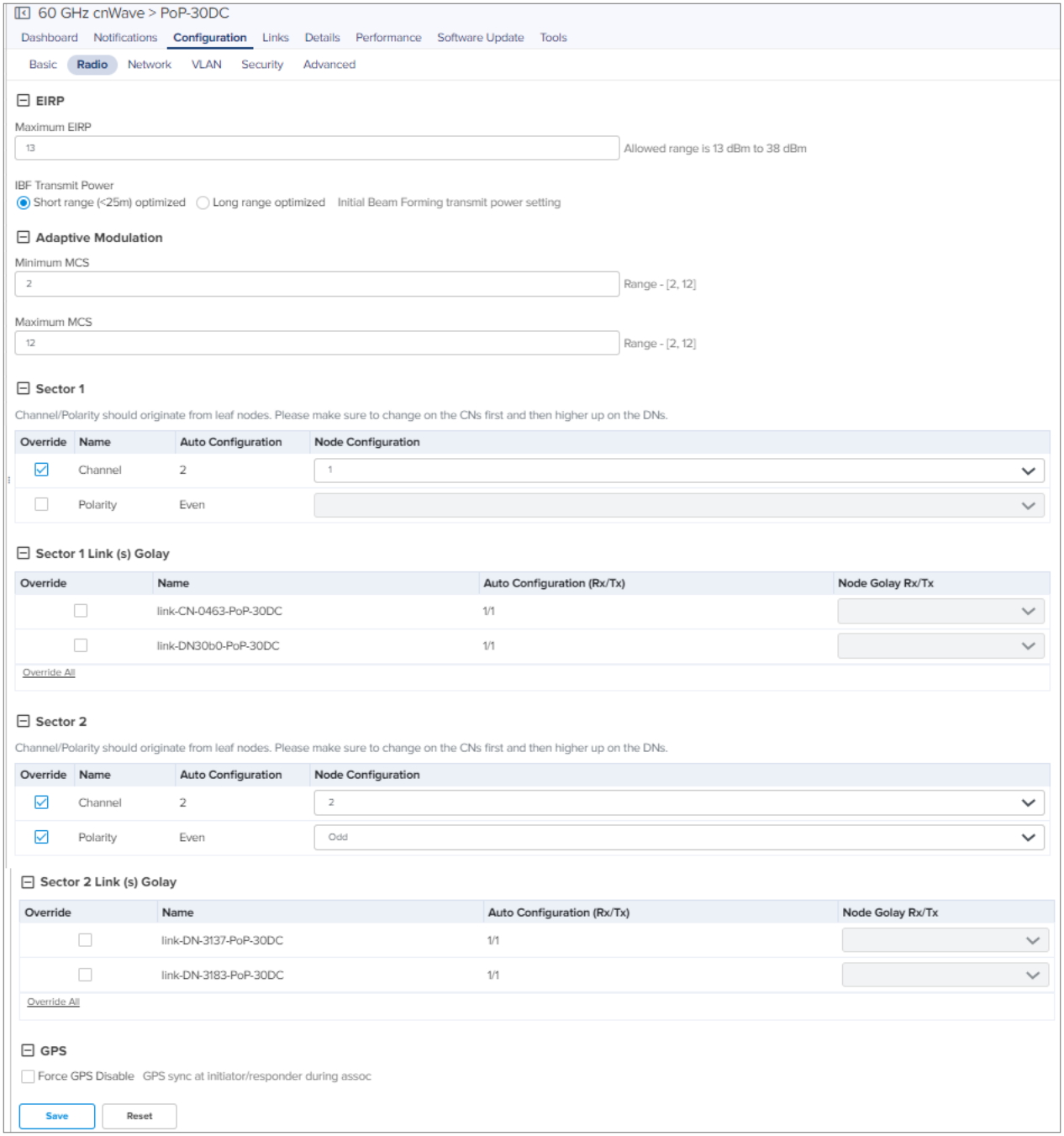
It displays the basic details of PoP node such as **Name, Description, MAC Address, Azimuth,** and **Elevation**. It also allows to edit the name of the node.

Figure 319 *Basic*

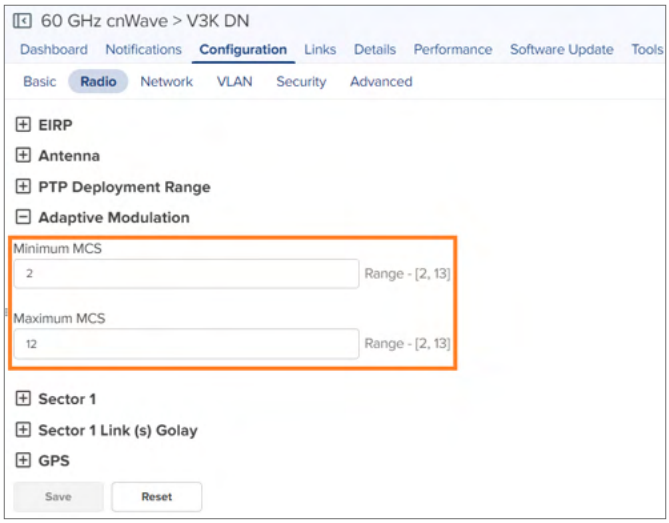
Radio

It allows the user to configure the **EIRP**, **Adaptive Modulation**, **Sectors (channels, Polarity and Link(s) Golay)**, and **GPS**.

Figure 320 *Radio*



For V3000, MCS 13 is supported as seen the following UI:

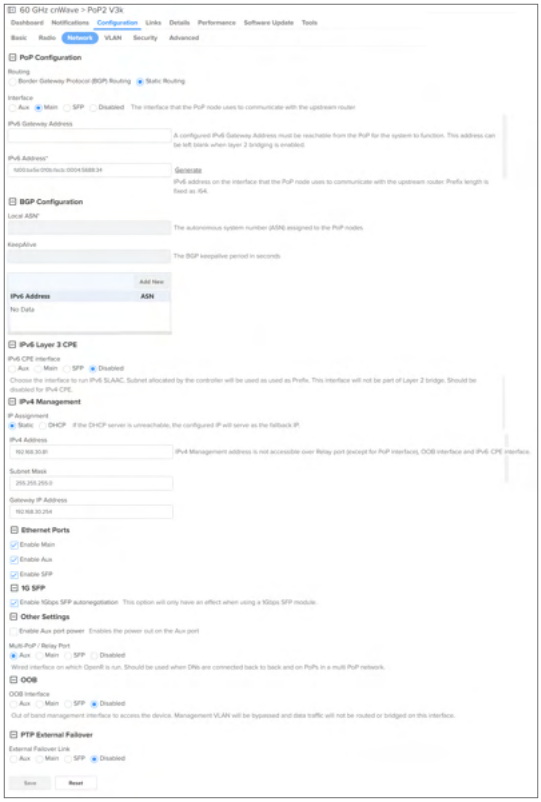


Network

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 321 *Network*

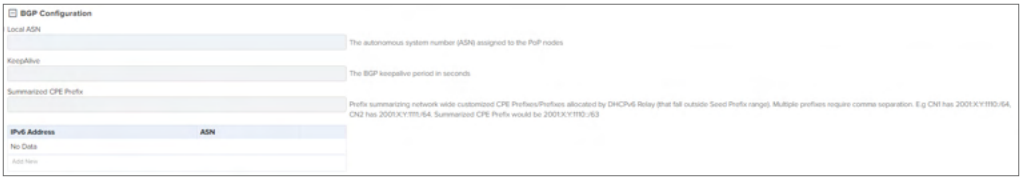


Configure the Network as shown below:

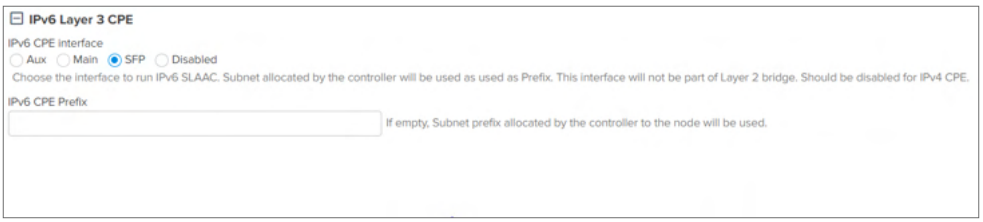
1. Navigate to the **Configuration** > **Network.**
2. In **PoP Configuration:**
   - Select the appropriate option in **Routing** and **Interface**.
   - Enter the **IPv6 Address.**
   - Enter **IPv6 Gateway Address** its optional.

3. In **E2E Controller Configuration**, enter the **IPv6 Address.**

4. In BGP Configuration add IPv6 Address.



5. In **IPv6 Layer 3 CPE**
   - Select **IPv6 CPE interface** as Aux, Main, or SFP.
   - Enter **IPv6 CPE Prefix.**

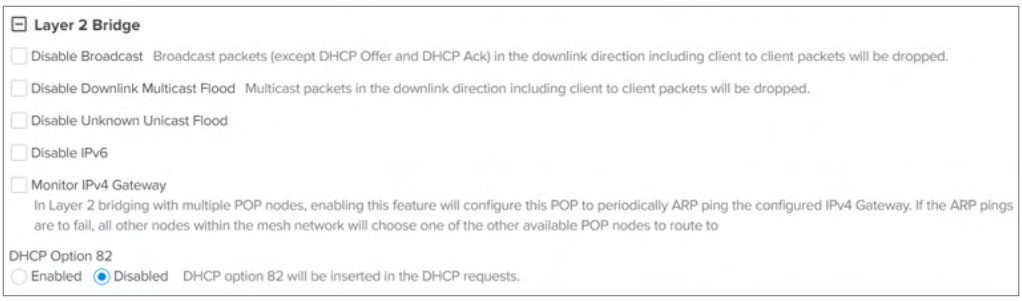


6. In the **IPv4 Management** section, the following options are supported:
   - **Static**: If you select Static, enter the IPv4 address, Subnet mask, and Gateway IP address manually.
   - **DHCP**: If you select DHCP, there is no need to set the IP address, Subnet mask, and Gateway IP address manually. 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.

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.

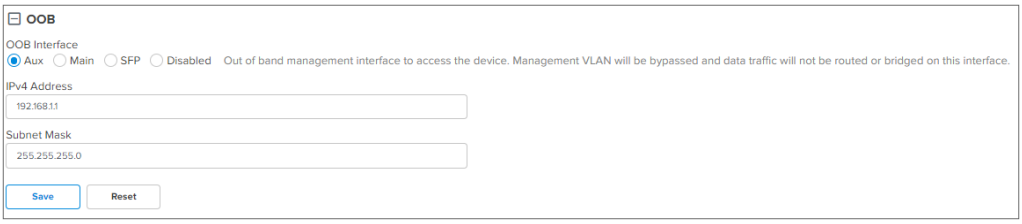
> **Note**
>
> The configuration is applicable only when static routing is used and IPv4 gateway is configured..

   - Insert DHCP Option 82



9. In **Other Settings** enable **Enable Aux port power** and **Multi-PoP / Relay Port**.

10. In **OOB Interface** enable the appropriate option **Main** or **Aux** or **SFP.**
    - Enter **IPv4 Address.**
    - Enter **Subnet Mask**.



11. 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

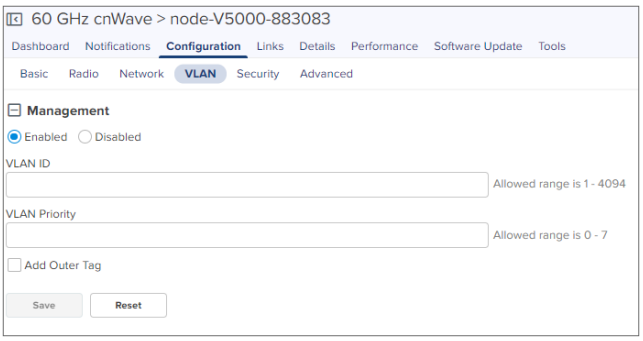
> **Note**
>
> From Software Update Version 1.1 of all nodes, supports configuration of the VLAN Management and Ports.

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.

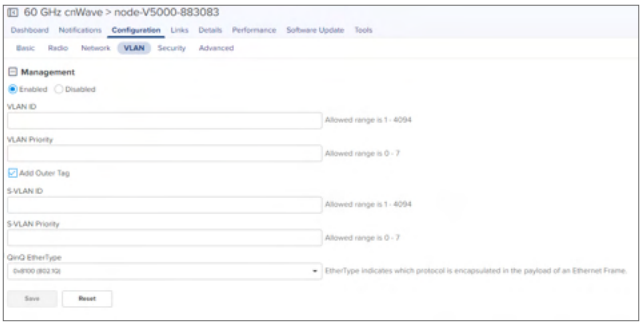
> **Note**
>
> Only PoP node Management VLAN can be configured, if Layer 2 Bridge is not enabled in **E2E Network** > **Configuration** > **Basic** page.
>
> Node running version 1.0.1:
>
> - When Layer2 bridge is disabled, Only PoP node Management VLAN ID can be configured.
> - When Layer2 bridge is 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.



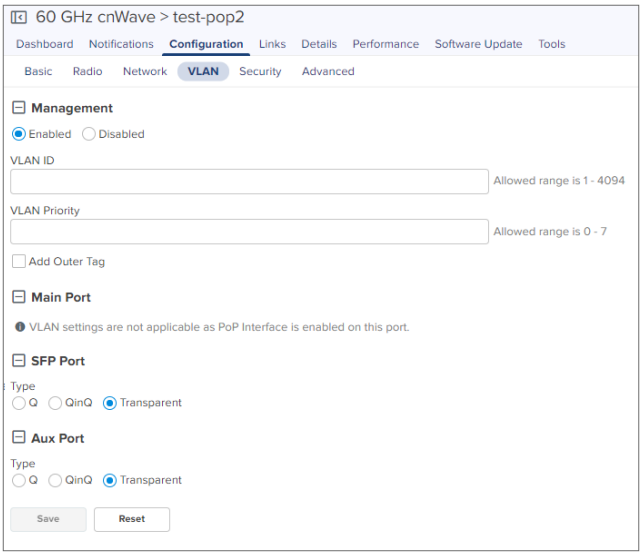
3. Enter the **VLAN ID** and **VLAN Priority**.
4. Enable **Add Outer Tag**.



5. Enter **S-VLAN ID**.
6. Enter **S-VLAN Priority.**
7. Enter **QinQ EtherType.**
8. Click **Save.**

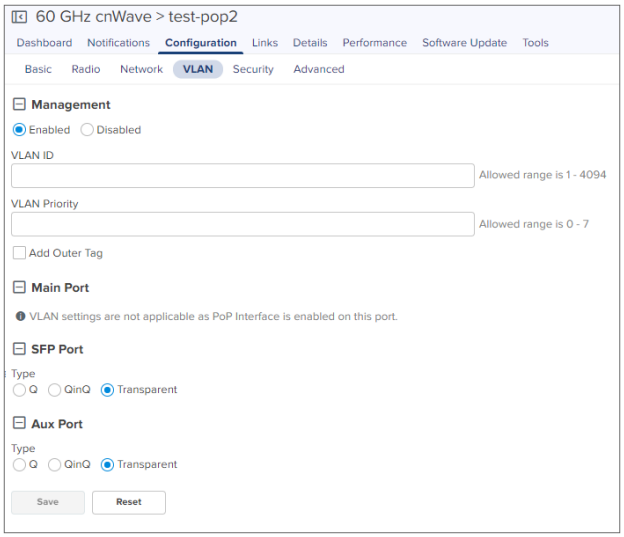
   If Layer 2 Bridge is enabled in **60 GHz cnWave Network** > **Configuration** > **Basic** page. User can configure Management VLAN and Ports of PoP node, DN and CN.

> **Note**
>
> VLAN settings are not applicable if Relay Port, SFP Port, or Aux Port is enabled on Network page.

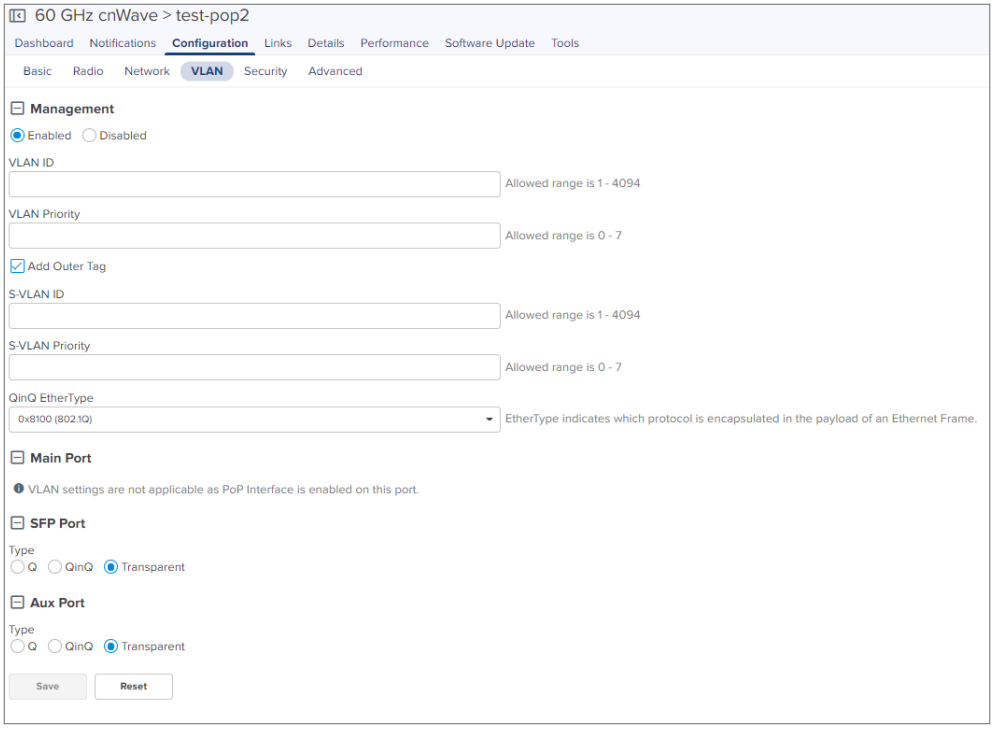


To add a VLAN:

1. Navigate to **Configuration** > **VLAN.**
2. Click Enabled.



3. Enter the **VLAN ID** and **VLAN Priority**.
4. Enable **Add Outer Tag**.

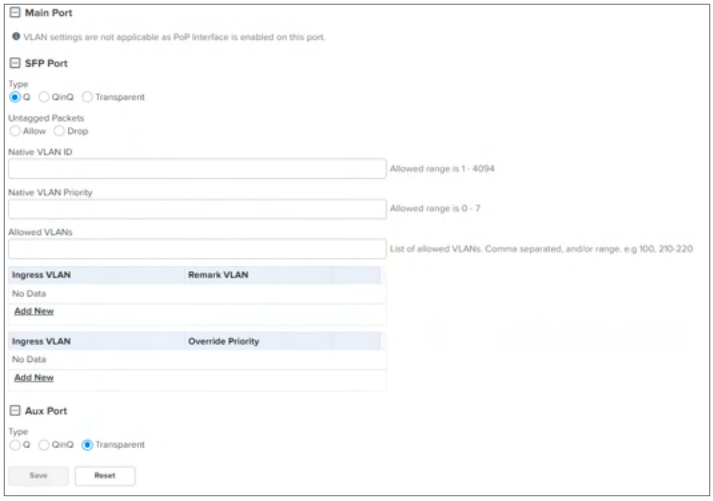


5. Enter **S-VLAN ID**.
6. Enter **S-VLAN Priority.**
7. Enter **QinQ EtherType.**

> **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:

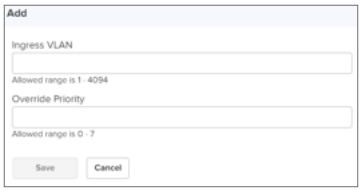


- Select **Untagged Packets** Allow or Drop.
- Enter **Native VLAN ID.**
- Enter **Native VLAN Priority**.
- Enter **Allowed VLANs**.
- To add new **VLAN Remarking.**

- Click Add New

  - Enter **Ingress VLAN** and **Remark VLAN**.
  - Click **Save**.
- To add new **VLAN Priority Override**.

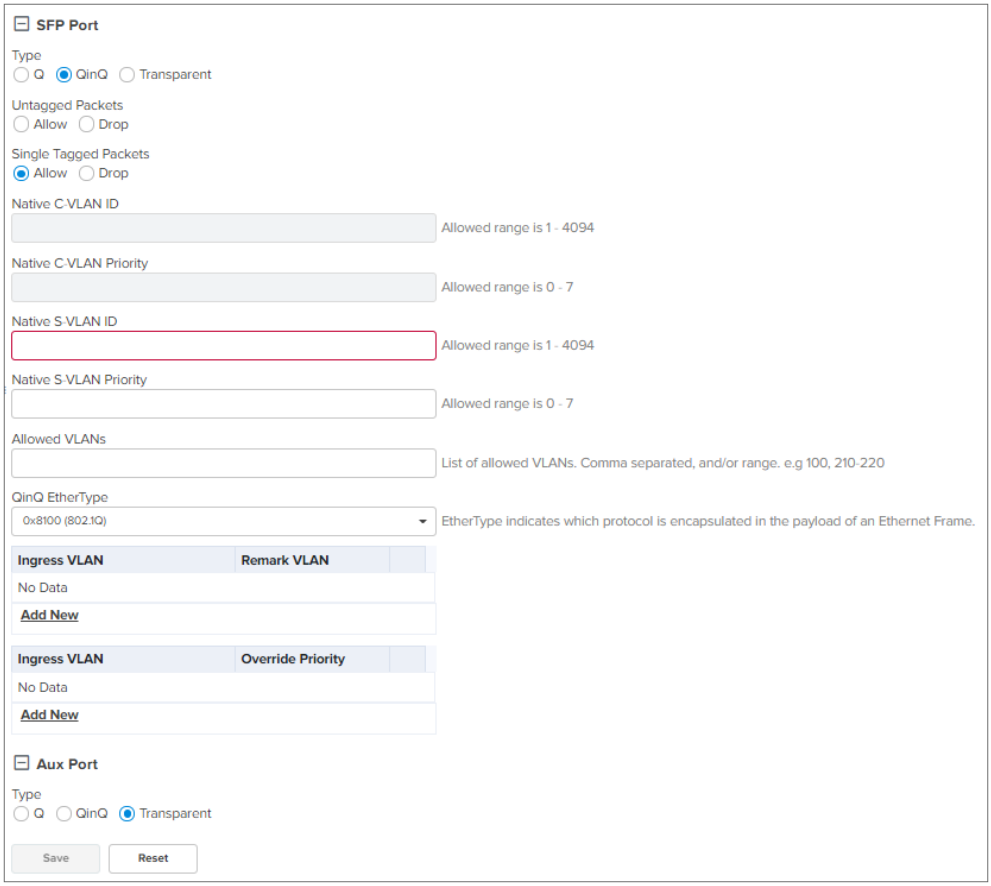
- Click **Add New**.



- Enter **Ingress VLAN** and **Remark VLAN**.
- Click **Save**.

- Click **Save**.

b. If user selects **QinQ** type perform as follows:



- 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.**

- Click **Add New**.

- Enter **Ingress VLAN** and **Remark VLAN**.
- Click **Save**.

- To add new **VLAN Priority Override**.

- Click **Add New**.

- 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 322 *Security*

Advanced

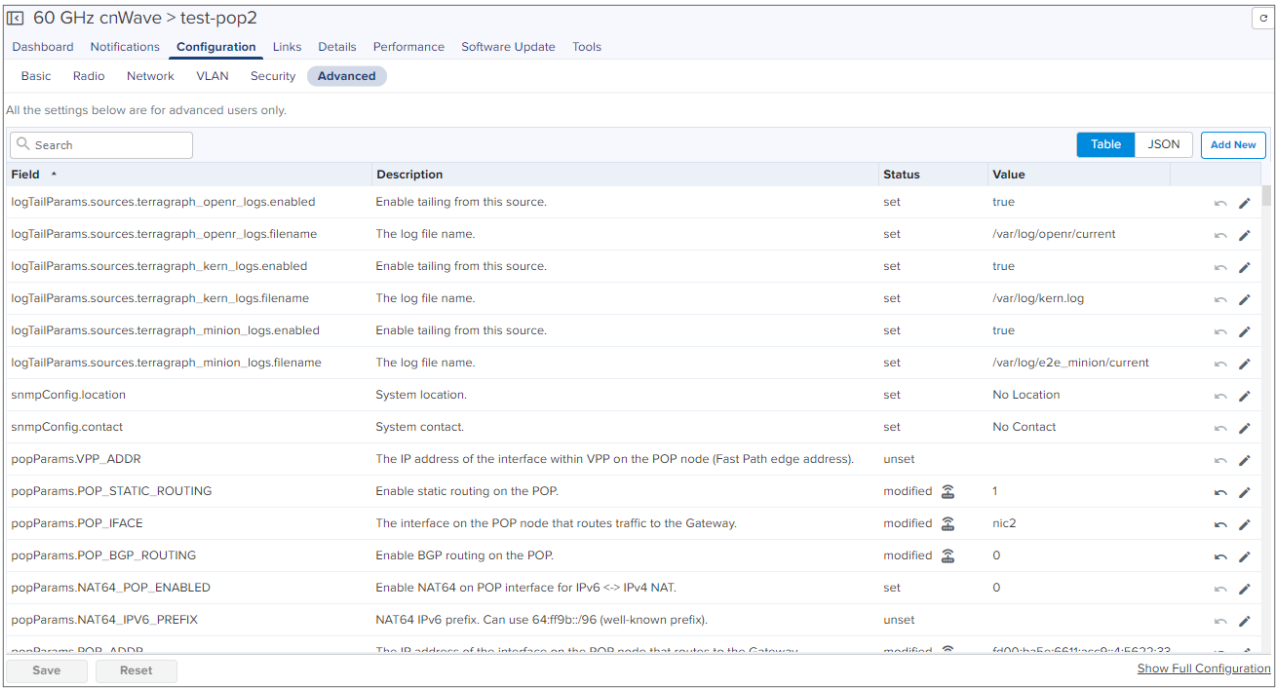
Advanced tab allows the advanced user to edit the settings of the Table and JSON format of the PoP Nodes.

Table

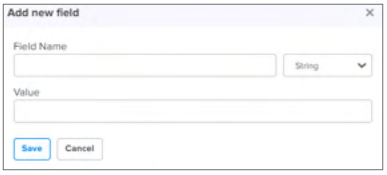
In the **Table** user can view and edit **Field Name** and **Value**. You can sort field name in alphabetical order.

To add a field:

1. Navigate to **Configuration** > **Advanced.**
2. Click **Add New.**



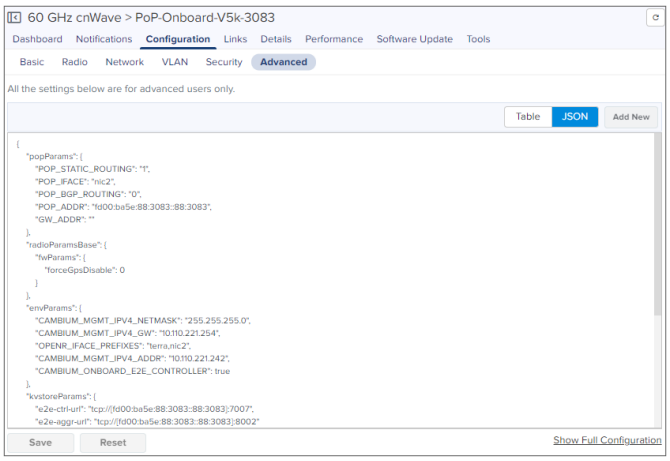
3. Enter the **Field Name** and **Value.**



4. Click **Save.**

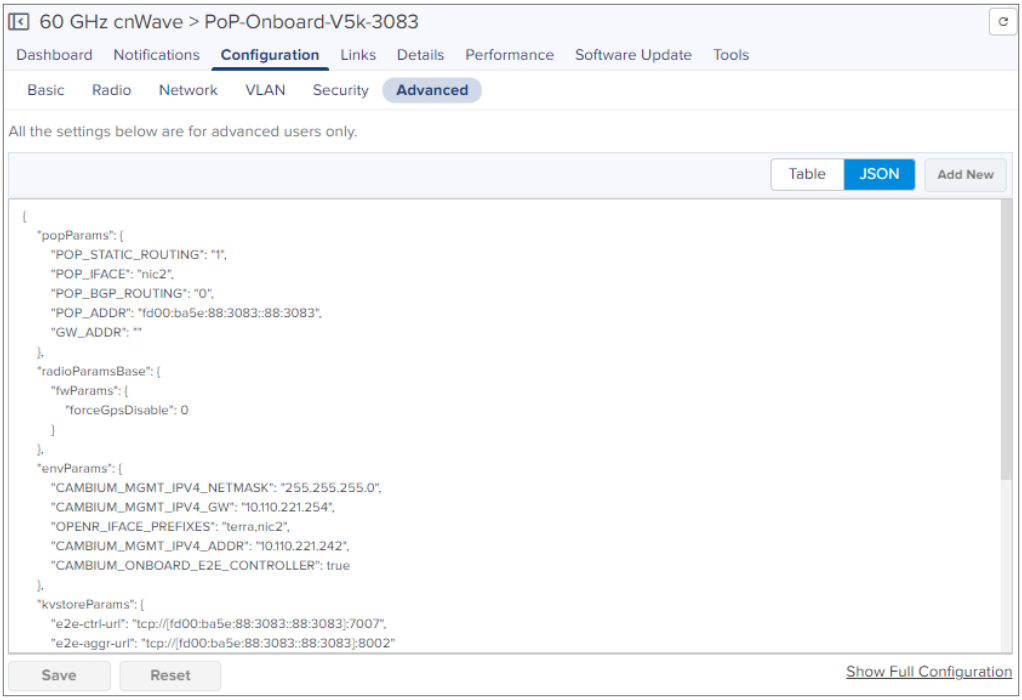
JSON

JSON allows advanced user to download or view the JSON format.



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**.

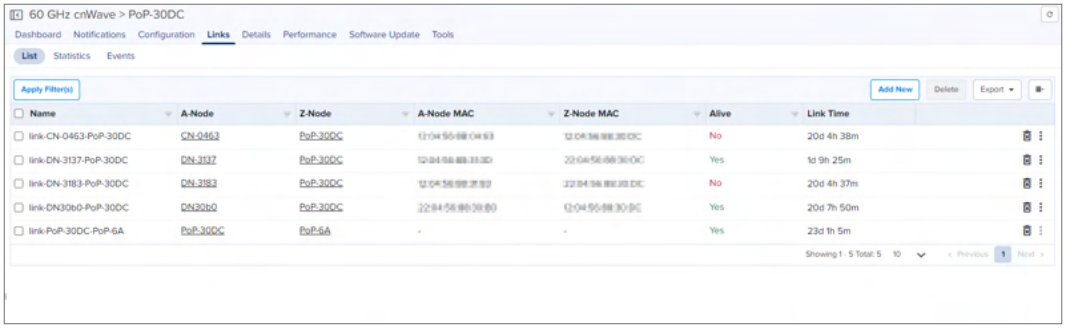
Links

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 323 *List*



For more details about adding a link and deleting a link in the network, refer the List section.

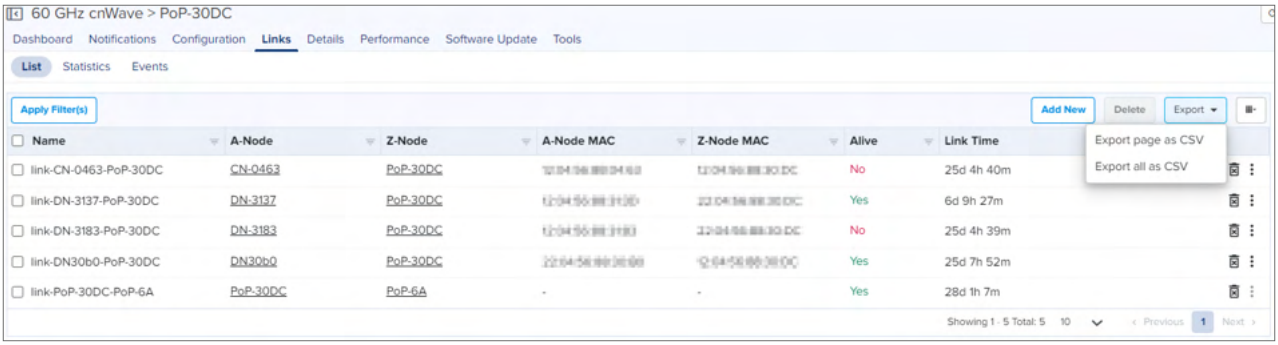
> **Note**
>
> By default A Node is selected as node, when adding new link in the network.

Export List

Export list allow the user to export the PoP links list.

To export the links :

1. Navigate to **Links** > **List** > select **Export.**

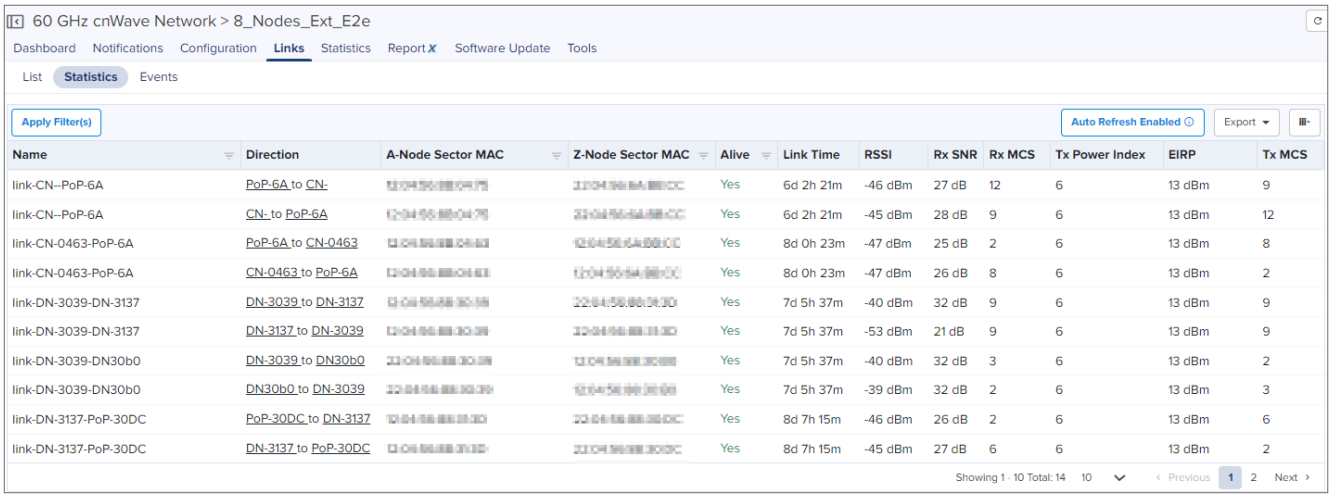


2. It exports .csv file format as shown below.

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_N	Z_NODE_N	LINK_TYPE	ALIVE	IGNITION_	DISTANCE	AZIMUTH	BACKUP_C	IGNITION_	TIMESTAMP		
Link Name	A node na	Sector 1/2	Z node nar	Sector 1/2	Wireless o	Yes/No	Ignition At	Distance b	Azimuth (D	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

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.



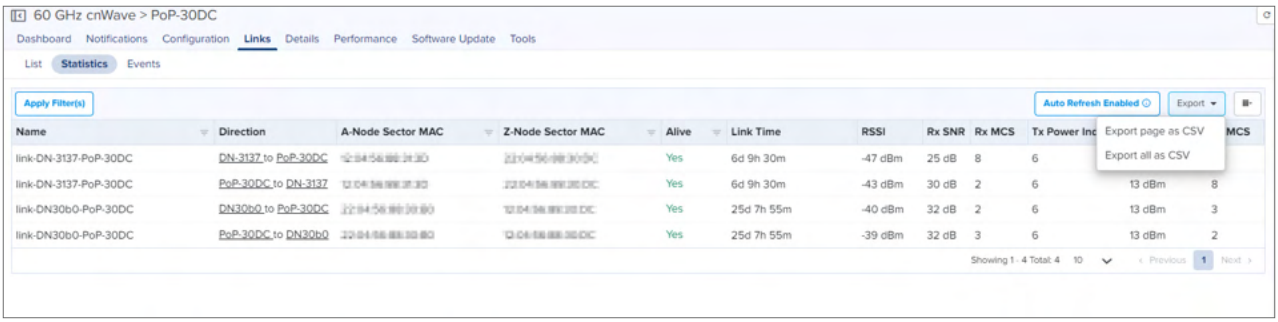
Name	Direction	A-Node Sector MAC	Z-Node Sector MAC	Alive	Link Time	RSSI	Rx SNR	Rx MCS	Tx Power Index	EIRP	Tx MCS
link-CN--PoP-6A	PoP-6A to CN-			Yes	6d 2h 21m	-46 dBm	27 dB	12	6	13 dBm	9
link-CN--PoP-6A	CN- to PoP-6A			Yes	6d 2h 21m	-45 dBm	28 dB	9	6	13 dBm	12
link-CN-0463-PoP-6A	PoP-6A to CN-0463			Yes	8d 0h 23m	-47 dBm	25 dB	2	6	13 dBm	8
link-CN-0463-PoP-6A	CN-0463 to PoP-6A			Yes	8d 0h 23m	-47 dBm	26 dB	8	6	13 dBm	2
link-DN-3039-DN-3137	DN-3039 to DN-3137			Yes	7d 5h 37m	-40 dBm	32 dB	9	6	13 dBm	9
link-DN-3039-DN-3137	DN-3137 to DN-3039			Yes	7d 5h 37m	-53 dBm	21 dB	9	6	13 dBm	9
link-DN-3039-DN30b0	DN-3039 to DN30b0			Yes	7d 5h 37m	-40 dBm	32 dB	3	6	13 dBm	2
link-DN-3039-DN30b0	DN30b0 to DN-3039			Yes	7d 5h 37m	-39 dBm	32 dB	2	6	13 dBm	3
link-DN-3137-PoP-30DC	PoP-30DC to DN-3137			Yes	8d 7h 15m	-46 dBm	26 dB	2	6	13 dBm	6
link-DN-3137-PoP-30DC	DN-3137 to PoP-30DC			Yes	8d 7h 15m	-45 dBm	27 dB	6	6	13 dBm	2

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			Yes	6d 9h 30m	-47 dBm	25 dB	8	6	
link-DN-3137-PoP-30DC	PoP-30DC to DN-3137			Yes	6d 9h 30m	-43 dBm	30 dB	2	6	13 dBm 8
link-DN30b0-PoP-30DC	DN30b0 to PoP-30DC			Yes	25d 7h 55m	-40 dBm	32 dB	2	6	13 dBm 3
link-DN30b0-PoP-30DC	PoP-30DC to DN30b0			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_I	Z_NODE_I	A_NODE_I	Z_NODE_I	ALIVE	TYPE	DISTANCE	AZIMUTH	RSSI	Rx_SNR	Rx_MCS	Rx_PER	Rx_BEAM_	Tx_POWEI	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-B0	APOP to DN-B0	APOP	DN-B0	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-B0	DN-B0 to APOP	APOP	DN-B0	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-B0	DN-B0 to CN-75	CN-75	DN-B0	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-B0	CN-75 to DN-B0	CN-75	DN-B0	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-B0	CN-83 to DN-B0	CN-83	DN-B0	12:04:56:8	22:04:56:8	Yes	Wireless	71	52.7	-53	21	9	0.81	58	6	35	9	0.06	58	385	2043
link-CN-83-DN-B0	DN-B0 to CN-83	CN-83	DN-B0	12:04:56:8	22:04:56:8	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-8b	CN-8b046	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 D	CN-8b046	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-3(	DN-39	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-3(	DN-39	DN-3D	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-B0	DN-B0 to DN-3(	DN-39	DN-B0	22:04:56:8	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-B0	DN-39 to DN-B(	DN-39	DN-B0	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 324 *Link Events*

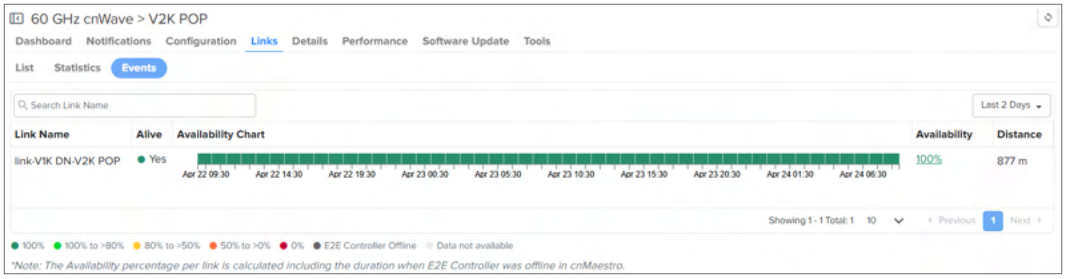


Table 87 *Link > Events fields*

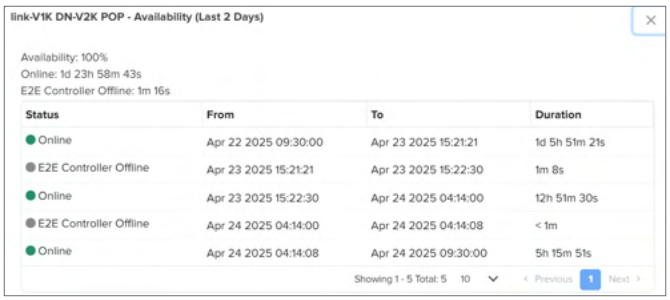
Field	Description
Link Name	Name of the link.
Alive	Status of the link (Yes or No).
Availability Chart	Displays the link availability duration (in chart format) based on time range selected from the dropdown list (located above the Distance field). This time range dropdown list supports the following 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 customize the time range using the Custom Range option from the dropdown list. **Note**: **Custom Range** and **Last 30 days X** are available only for cnMaestro X users. When you hover the mouse on the Availability Chart, the link availability is shown as described: 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 324.
Distance	Distance of the link in meters.

The **Availability Chart** field displays the ink availability in percentage and different colors, as shown below,

Figure 325 *Link Availability in Percentage*

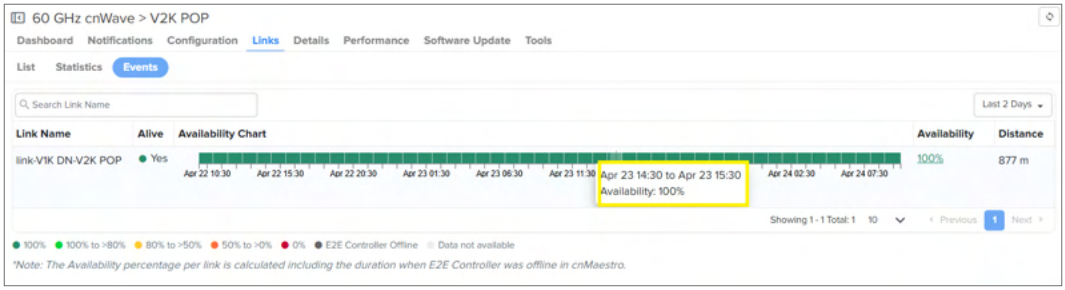
When you click on the percentage in the **Availability** column, you can view the detailed link availability information for the selected time range. Availability percentage per link is calculated, including the duration, when E2E Controller goes Offline in cnMaestro.

Figure 326 *Detailed link availability information*



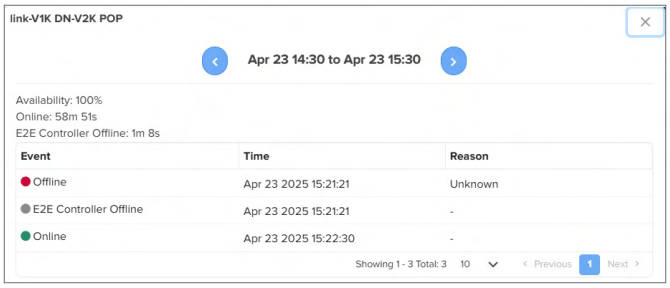
You can hover your mouse on the link to view the hourly availability of the link, as shown in the figure below.

Figure 327 *Viewing the hourly availability status*



When you click on the hourly availability time on the chart (for example, Apr 23 14.30 to Apr 23015.30 as shown in Figure 327), you can view the detailed link information for the selected one hour, including the link offline reason.

Figure 328 *Hourly details*



Details

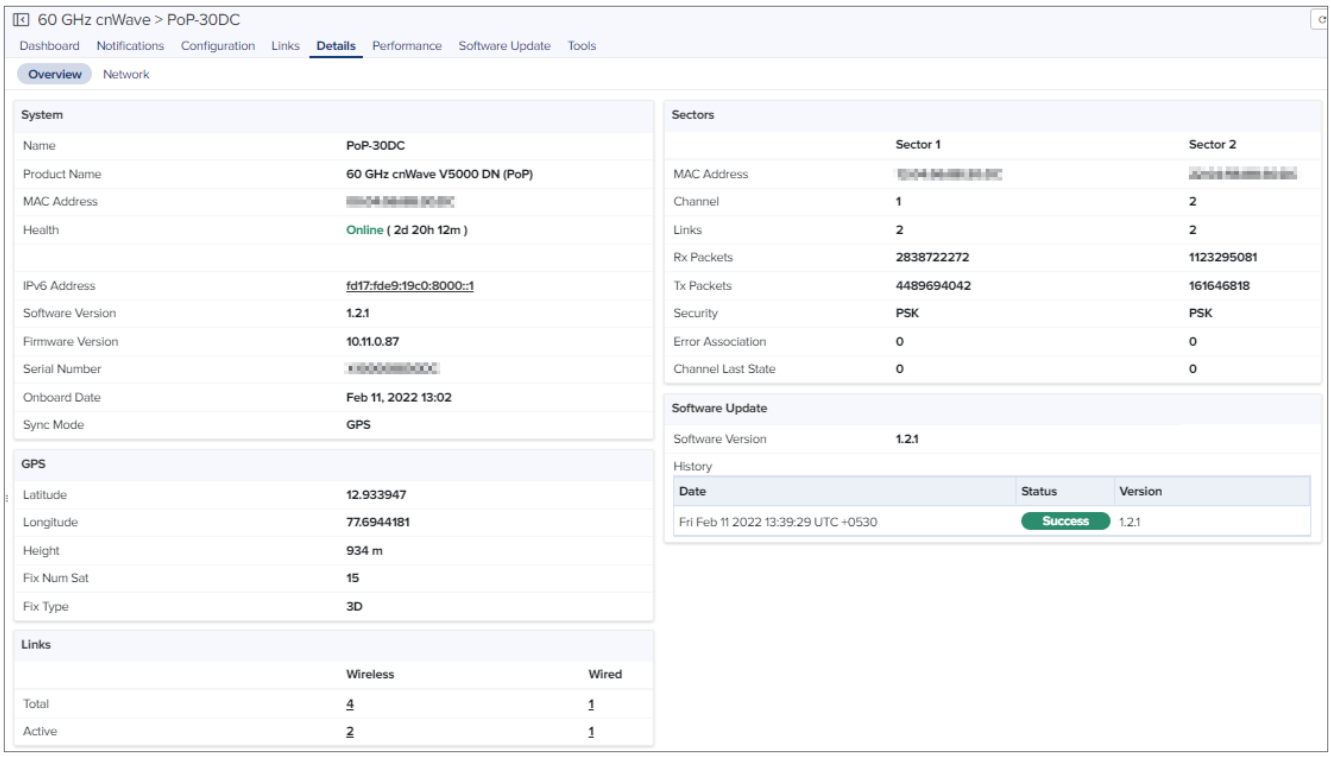
Details page provides the following device information:

- Overview
- Network

Overview

Overview page provides the device details and it also details of the last 3 software update history.

Figure 329 *Details Overview Page*

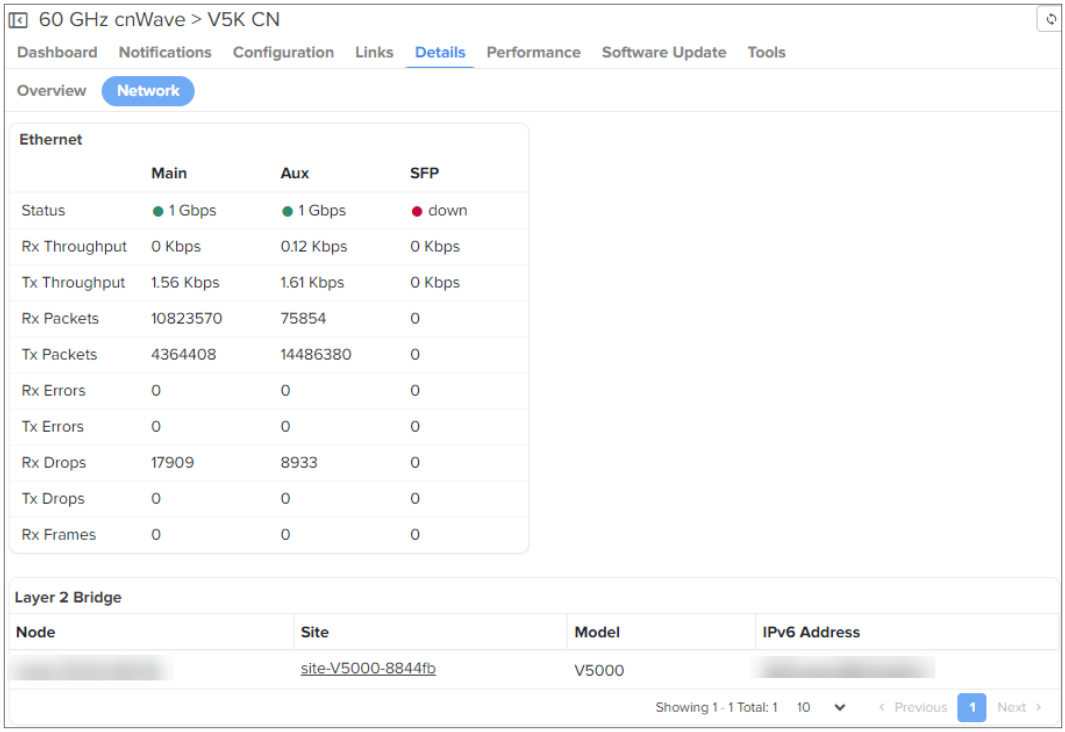


Network

In the **Network** page provides the following details:

- **Ethernet**: Displays Ethernet details, including **Main**, **Aux**, and **SFP** ports.
- **Layer 2 Bridge**: Displays Layer 2 Bridge details, including **Node**, **Site**, **Model**, and **IPv6 Address**.

Figure 330 *Details Network Page*



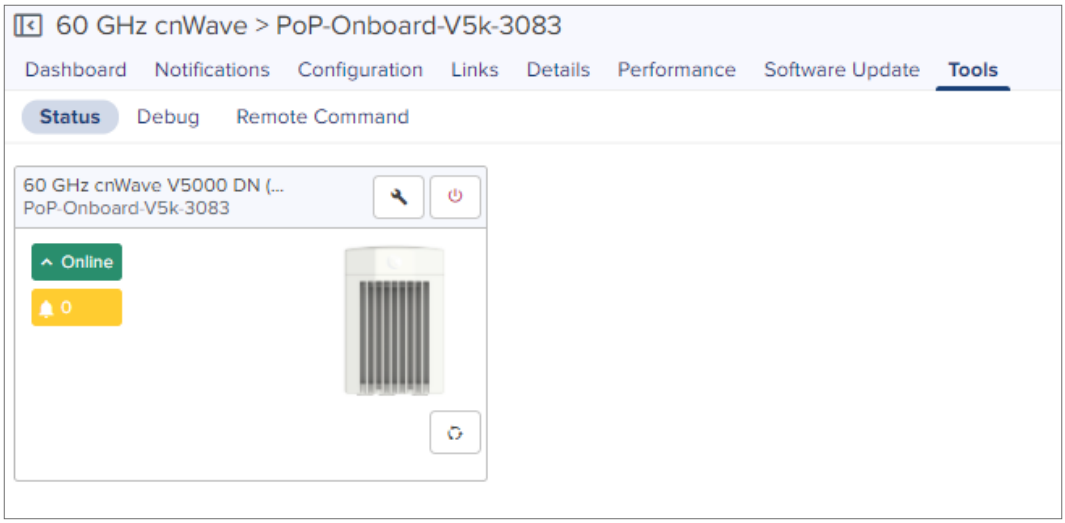
Tools

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.



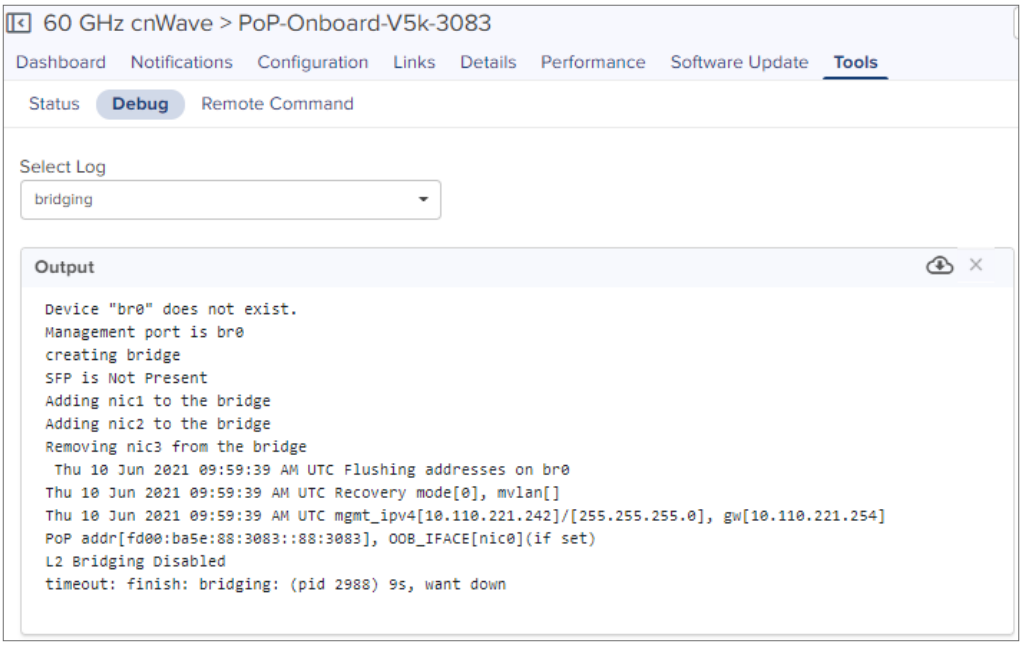
Debug

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)
- e2e_controller (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

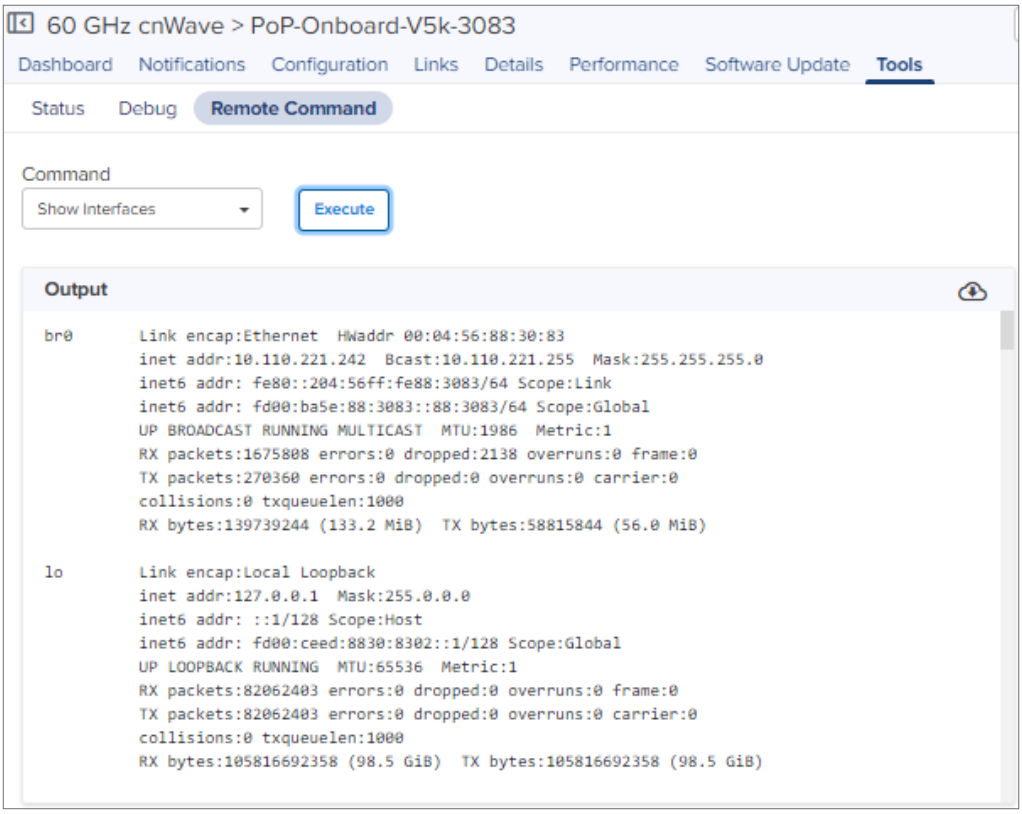
In **Remote command** tab, user can view or download Command logs by executing the following commands:

- 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
- Show GPS Stats

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 critera appears as shown:



- Click the download icon to download the generated output.
- Click the clear × icon to clear the generated output.

DN/CN Node

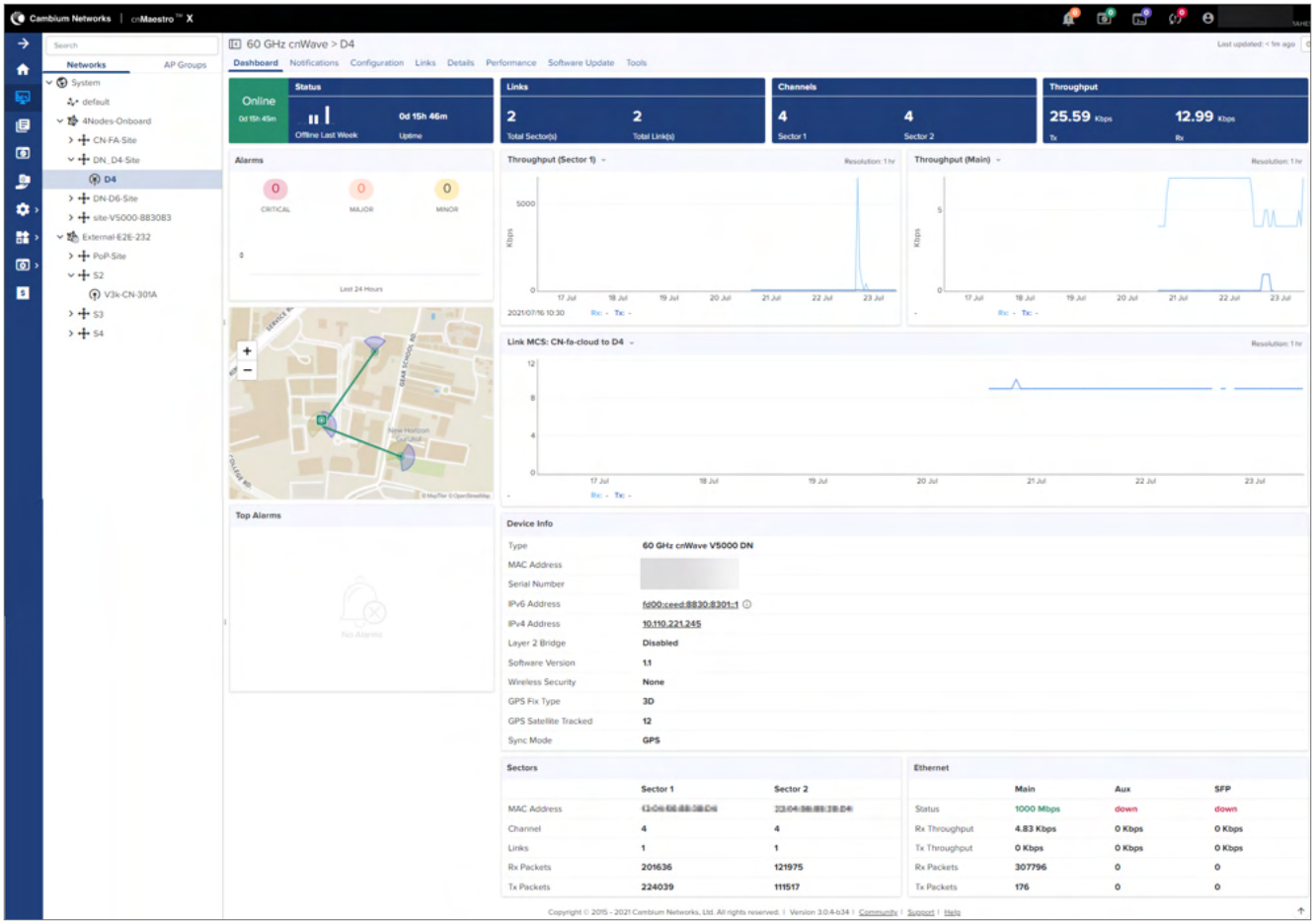
To create a new site, refer to Site.

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 331 *DN/CN Node Dashboard*



Configuration

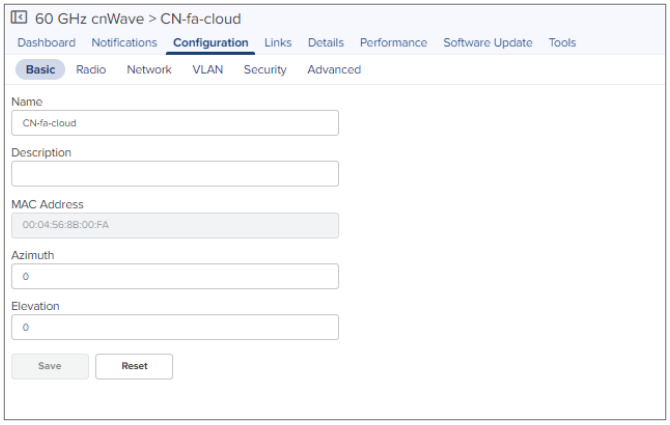
Configuration page allows the user to configure the following details of CN/DN:

- 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 332 *Basic*

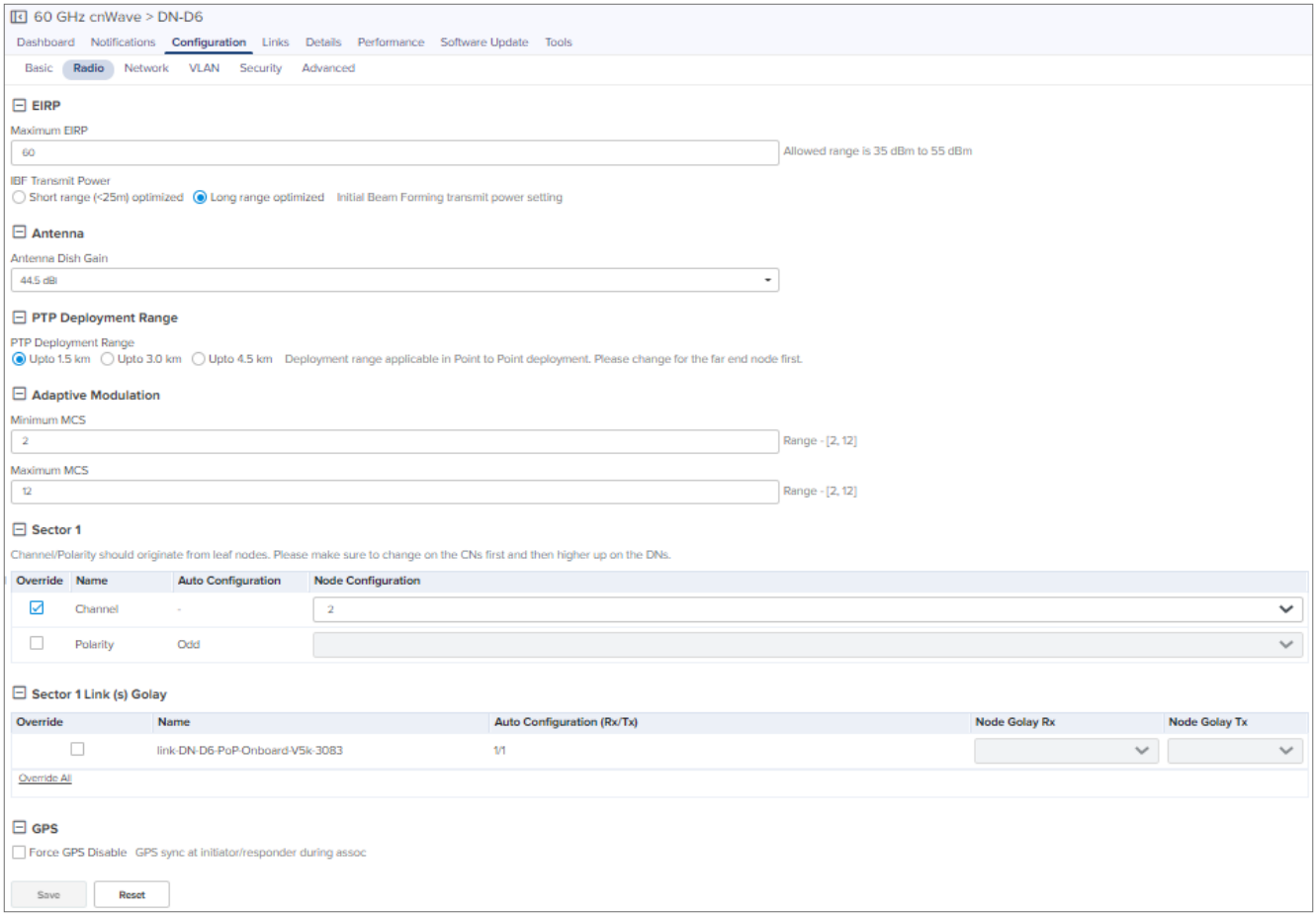


Radio

> **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**.

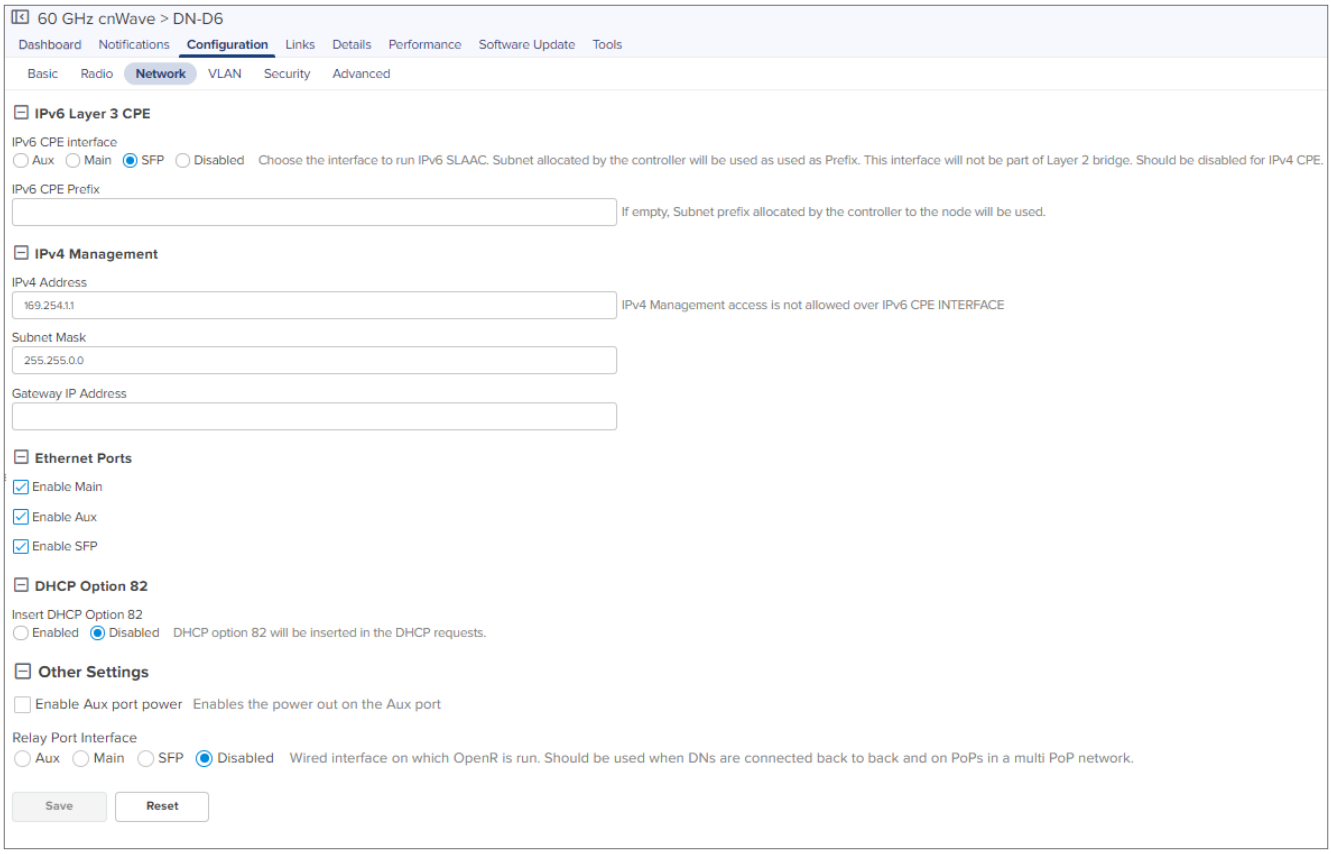
Figure 333 *Radio*



Network

Network tab allows the user to edit the **Layer 3 CPE, IPv4 Management**, **Ethernet Ports, PTP External Failover**, and **Other Settings.**

Figure 334 *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

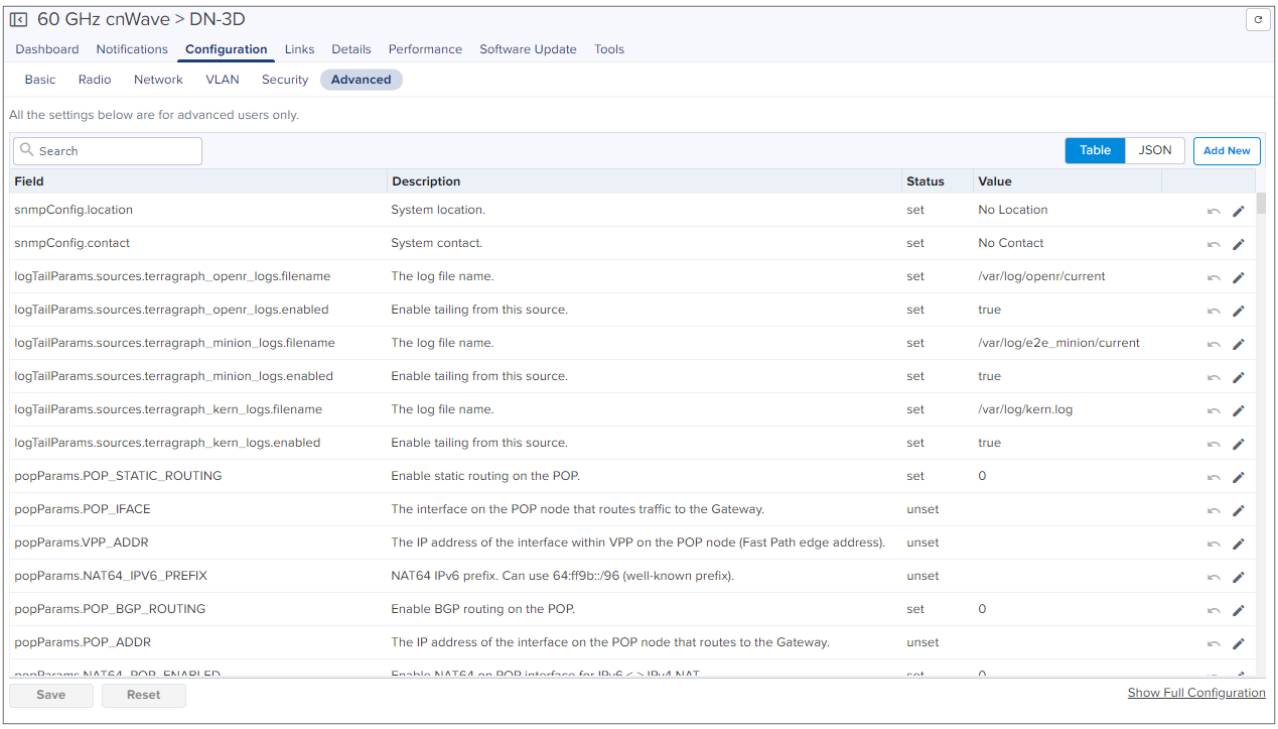
Security tab allows to reset the identity and password of the Radius user.

Figure 335 *Security*

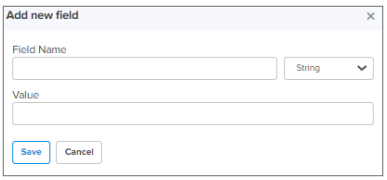
Advanced

Advanced tab allows the advanced user to set Field Name and Value.

1. Navigate to **Configuration** > **Advanced.**
2. Click **Add New.**



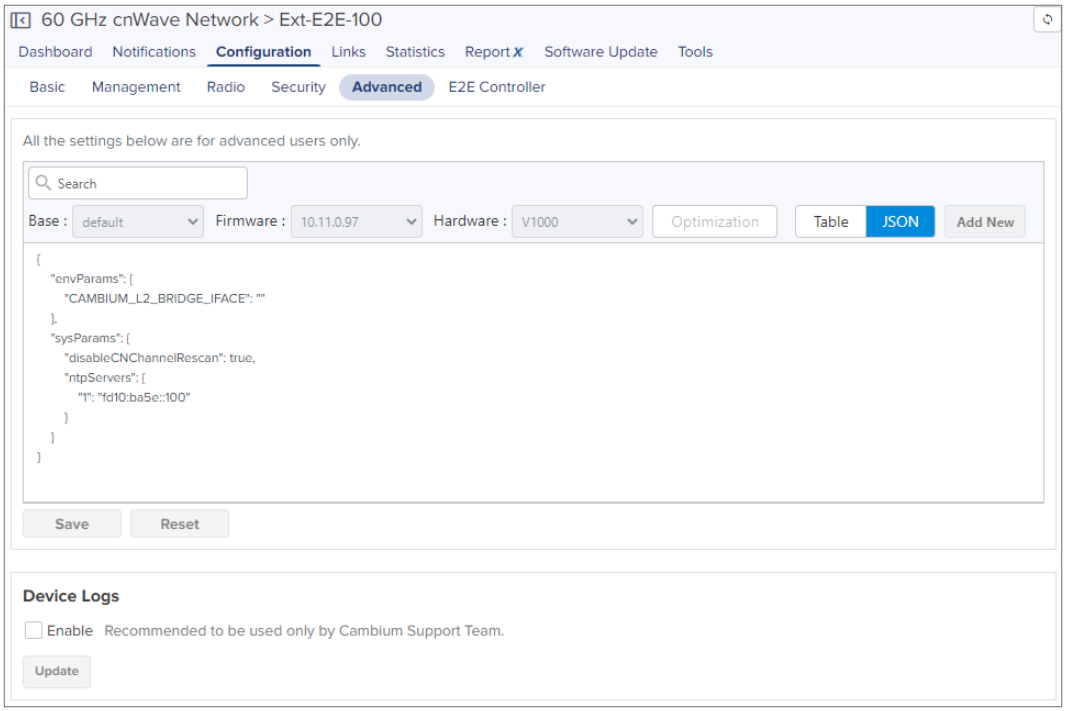
3. Enter the **Field Name** and **Value.**



4. Click **Save.**

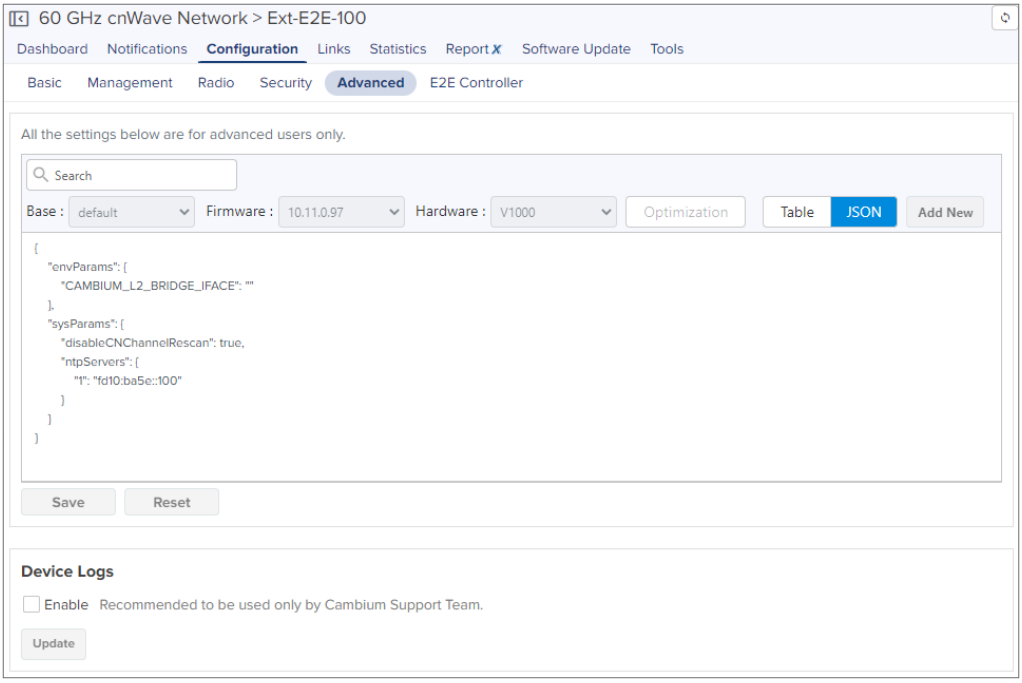
JSON

JSON allows Advanced users to view the JSON format.



To download the file, perform the following steps:

1. Navigate to **Configuration** > **Advanced** > **JSON.**



2. Click **Show Full Configuration.**
3. **View Device Existing Configuration** pops up.

4. Click **Download**.

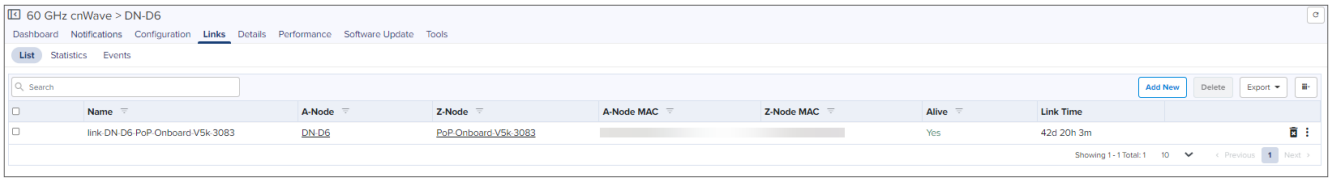
Links

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

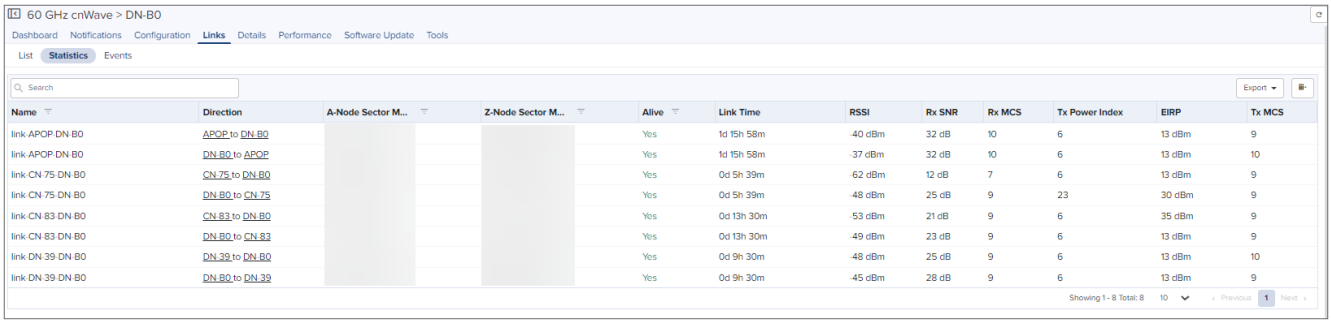
List provide the details about the links of the node and also provides the option to create a new link. User can delete the links in bulk by selecting the particular link.

Figure 336 *List*



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.



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 337 *Events*

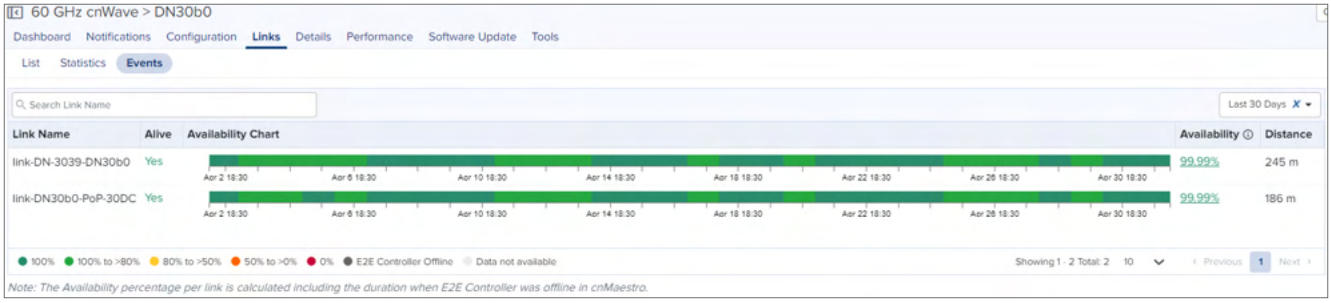


Table 88 *Events fields*

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: 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. • Hover on the link to see the hourly availability as shown in Figure 308. • Clicking on percentage link availability displays pop-up window as shown in Figure 309 • Link availability is presented in different colors in the chart as shown in Figure 307
Availability Percentage	• Clicking on percentage for the complete timeline link availability displays pop-up window as shown in Figure 339. • Availability of link is shown in percentage in the Availability column as shown in Figure 308.
Distance	Distance of the link in meters.

Figure 338 *Link Availability in Percentage*

Figure 339 *Link Availability details*

Availability percentage per link is calculated including the duration when E2E Controller was Offline in cnMaestro.

Figure 340 *Link Availability*

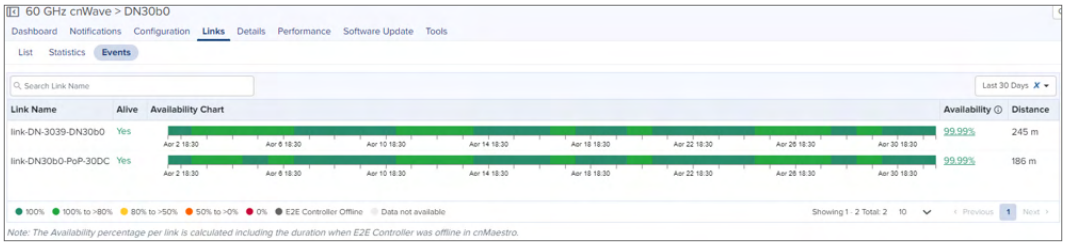
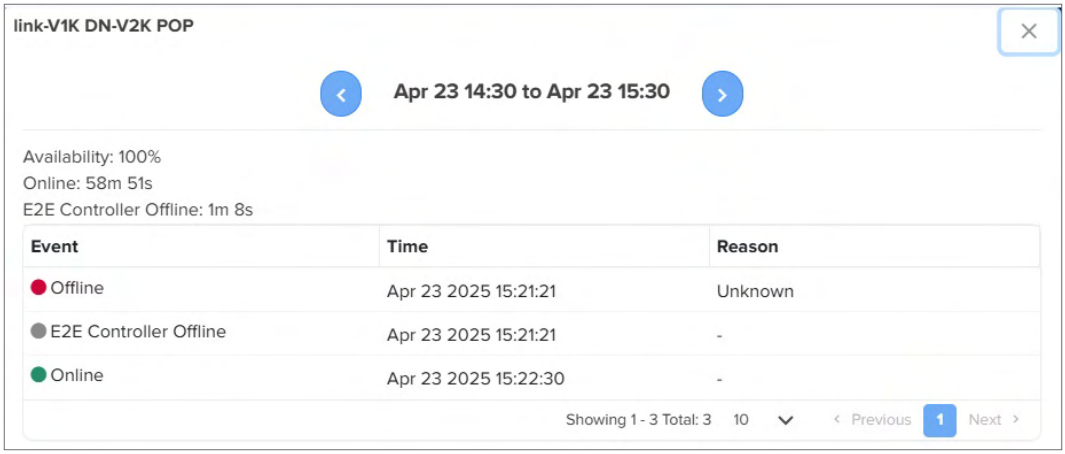


Figure 341 *Link Status*



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

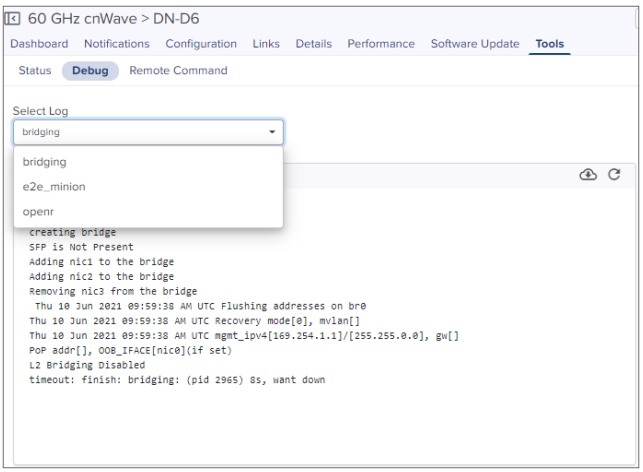
In **Debug** tab, you can view or download the DN or CN logs by executing the following log commands:

- 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 critera 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:

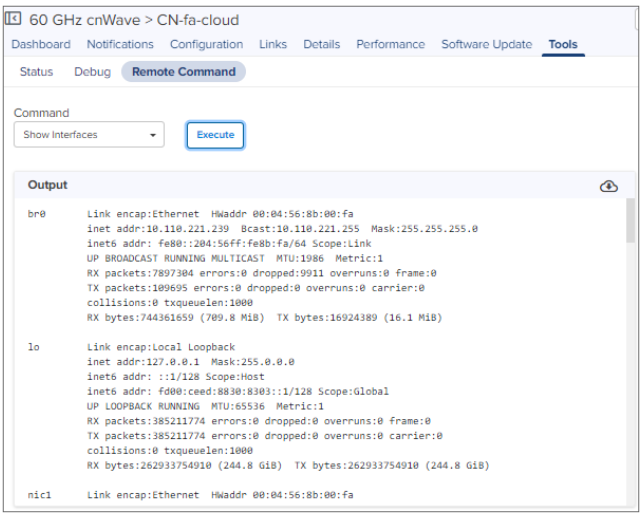
- Ping
- Show IGMP Membership Table
- Show Interfaces
- Show IPv4 Neighbors

- 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.**

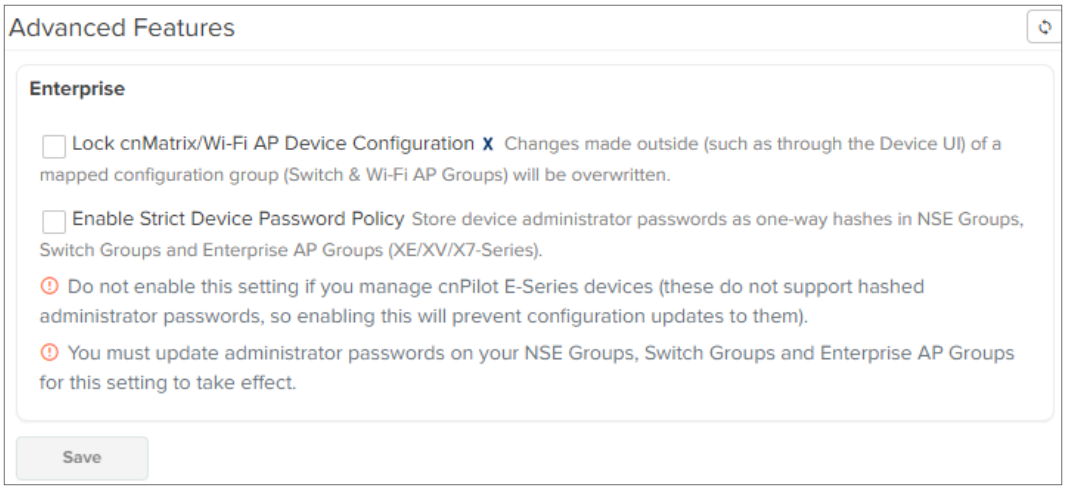
   The output for the selected critera appears as shown:



   - Click the download icon to download the generated output.
   - Click the clear ✕ icon to clear the generated output.

Configuring Advanced Features

To configure advanced features, navigate to **Configuration** > **Advanced Features** page.



Lock Device Configuration

To lock 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 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 Switch Groups and Enterprise AP Groups (XE/XV/X7-series).
- The administrator password has to be updated for all Switch Groups and Enterprise AP Groups under **Configuration** > **Switch Groups** > **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 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 Switch Groups and Enterprise AP Groups under the respective **Management** pages for this setting to take effect.

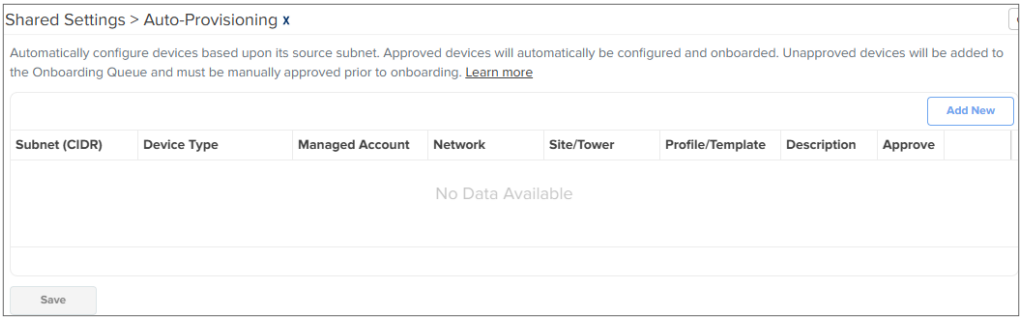
Auto-Provisioning

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 **Shared Settings** > **Auto-Provisioning** page.



2. Click **Add New** and following window appears.

Figure 342 *Auto-Provisioning for cnPilot Home (R-Series) devices*

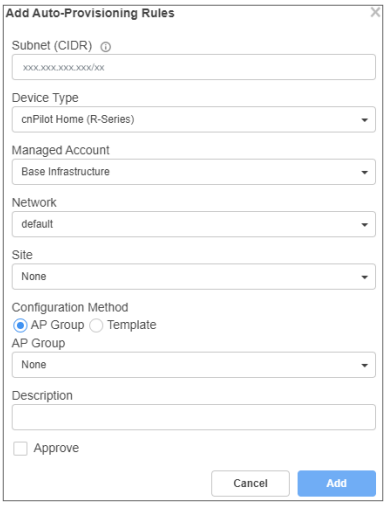
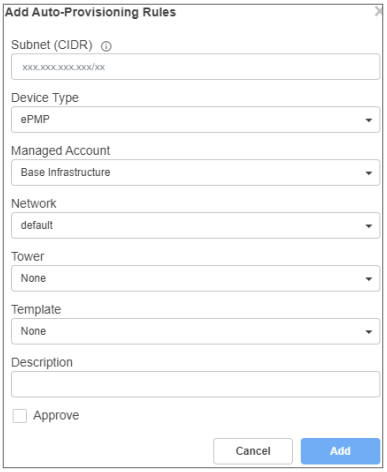


Figure 343 *Auto-Provisioning for all other devices*



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**.

Managed Services

This section includes the following topics:

- Managed Accounts

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

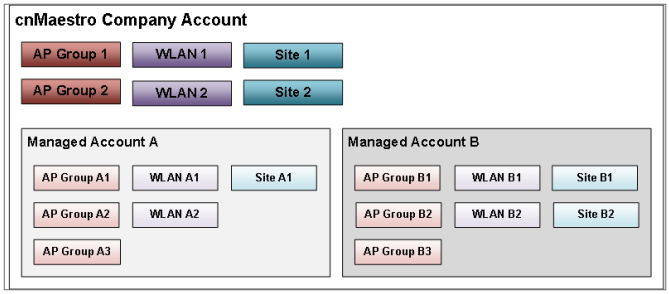
The Managed Accounts feature combines Accounts with Account Services.

Managed Accounts	=	Accounts	+	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 344 *Accounts*



Scope

The following scopes are available in a cnMaestro deployment::

- Global Scope for entities (Devices, Networks, Sites, etc.) that exist outside of Managed Accounts and are only available to Global cnMaestro Administrators.
- Account Scope for entities in Managed Accounts and accessible to Global Administrators and Account Administrators.
- Shared Scope objects can be used across all Managed Accounts but not modified by them, though they can be copied into the Account and then changed. Shared Scope applies to management objects such as AP Groups, WLANs, and Switch Groups.

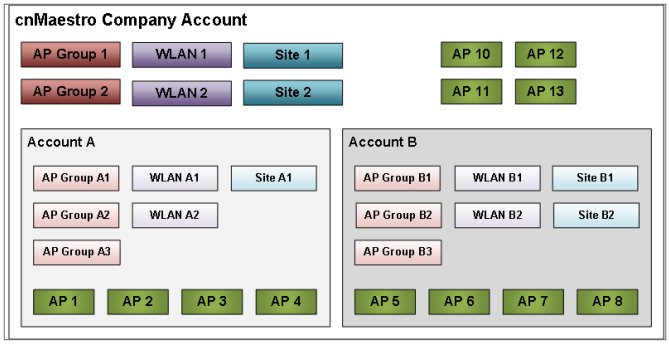
Access Points

Access Points exist in the Global cnMaestro application, or they can be added to a single Managed Account.

Note

The Managed Accounts feature supports all device types available within cnMaestro.

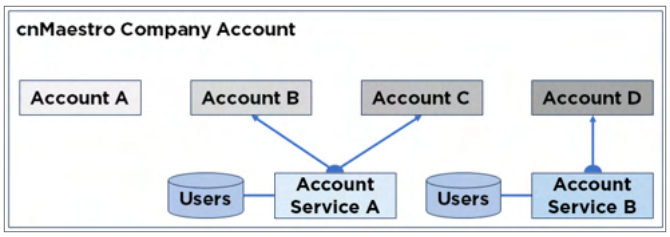
Figure 345 *Access Points*



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 346 *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 347 *Account UI - Sample 1*

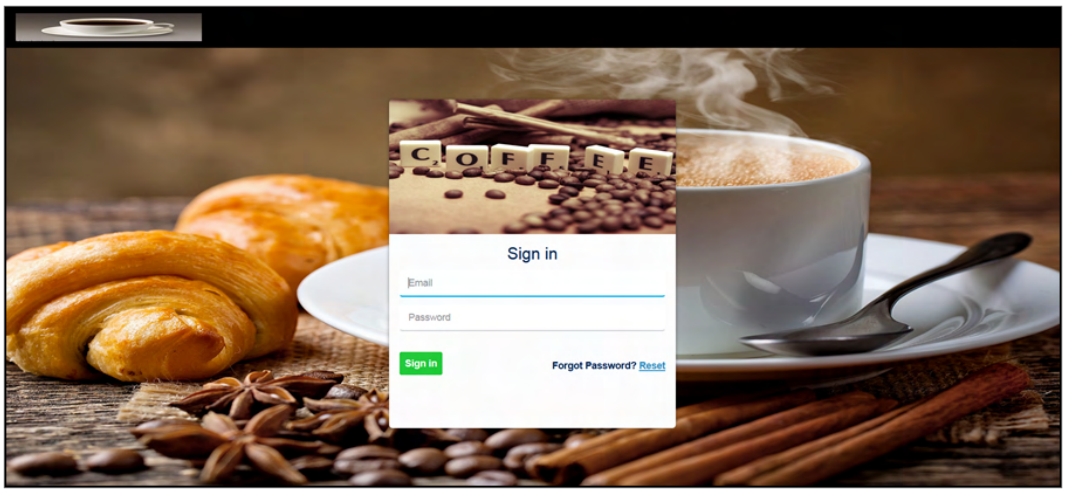
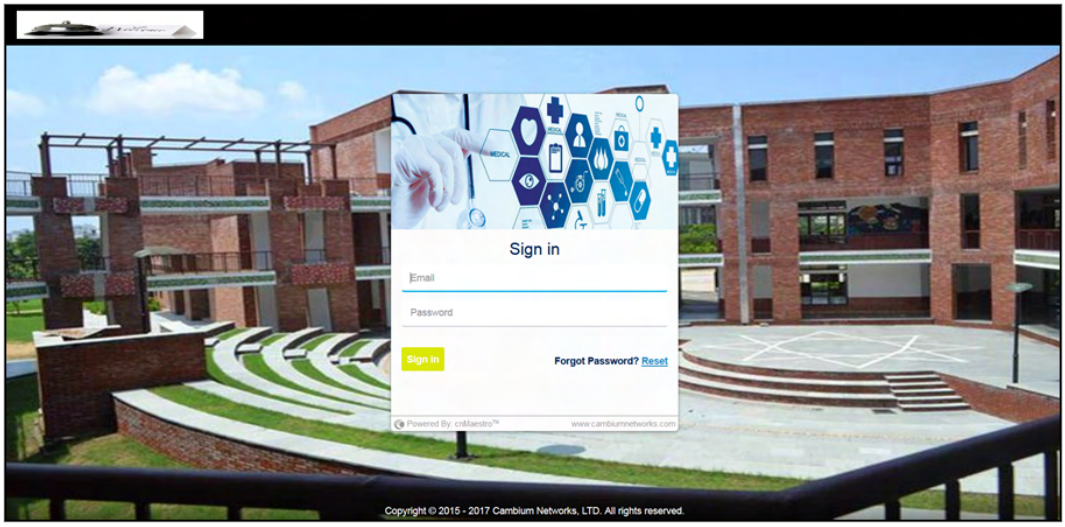


Figure 348 *Account UI - Sample 2*



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 89 *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	Create API clients	None	None	None

Table 89 *Tenant Administrator Roles*

Feature	Description	Administrator	Operator	Monitor
(Global cnMaestro administrator only)				
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
Data Tunnel (Global cnMaestro Administrator only)	Configure Data Tunnels	None	None	None
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 Groups	All	View	View
Guest Access Portal	Guest Access	All	View	View (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	None (Except	None (Except

Table 89 *Tenant Administrator Roles*

Feature	Description	Administrator	Operator	Monitor
		Monitoring)	System Monitoring)	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

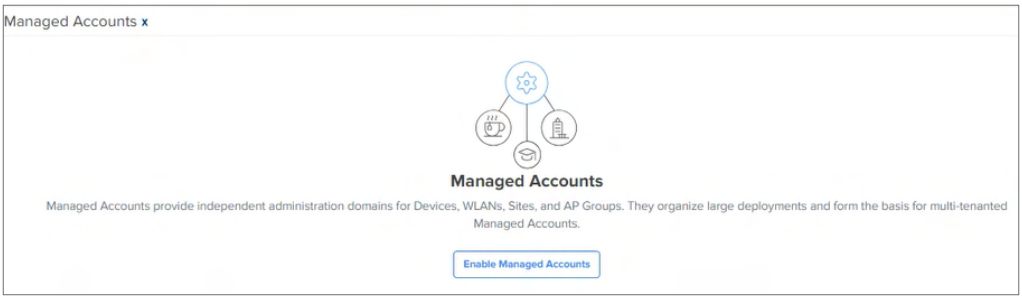
Enable Managed Accounts

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.**

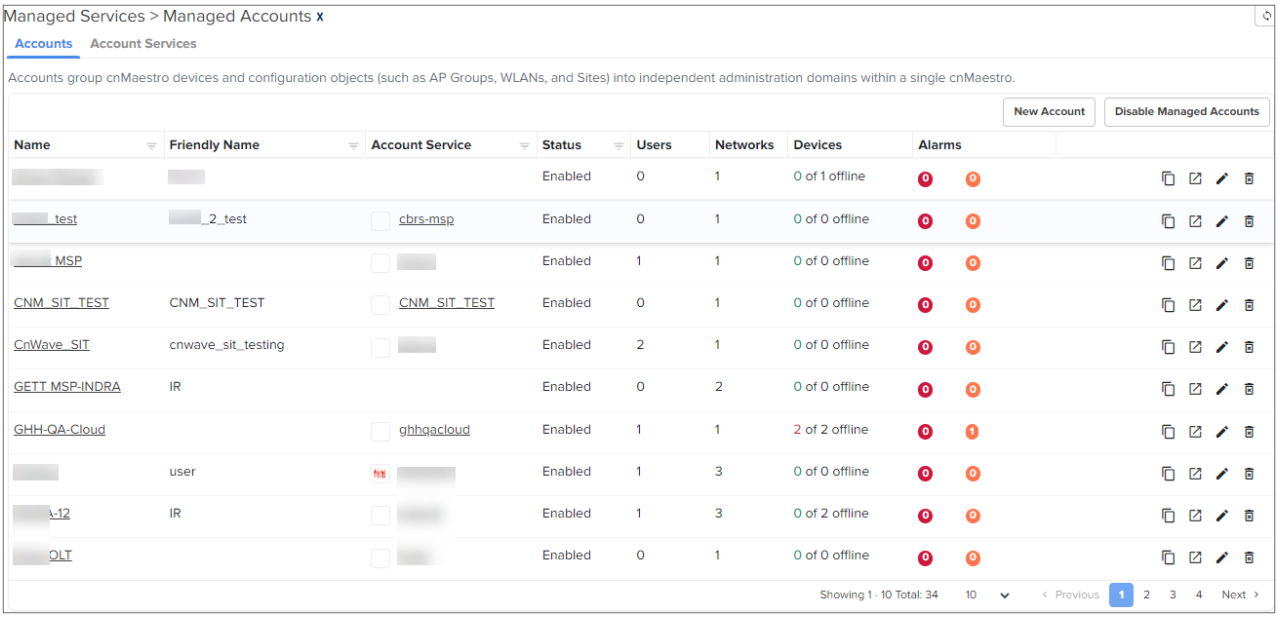
Figure 349 *Enabling Managed Accounts*



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 350 *Accounts and Account Services tabs*

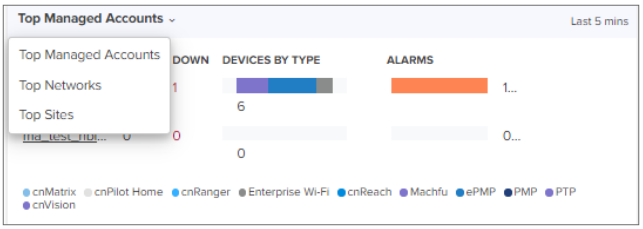


- The Header adds a select box that allows the Global Administrator to enter the context of Account selected.

  Figure 351 *Managed Accounts Component in Header*

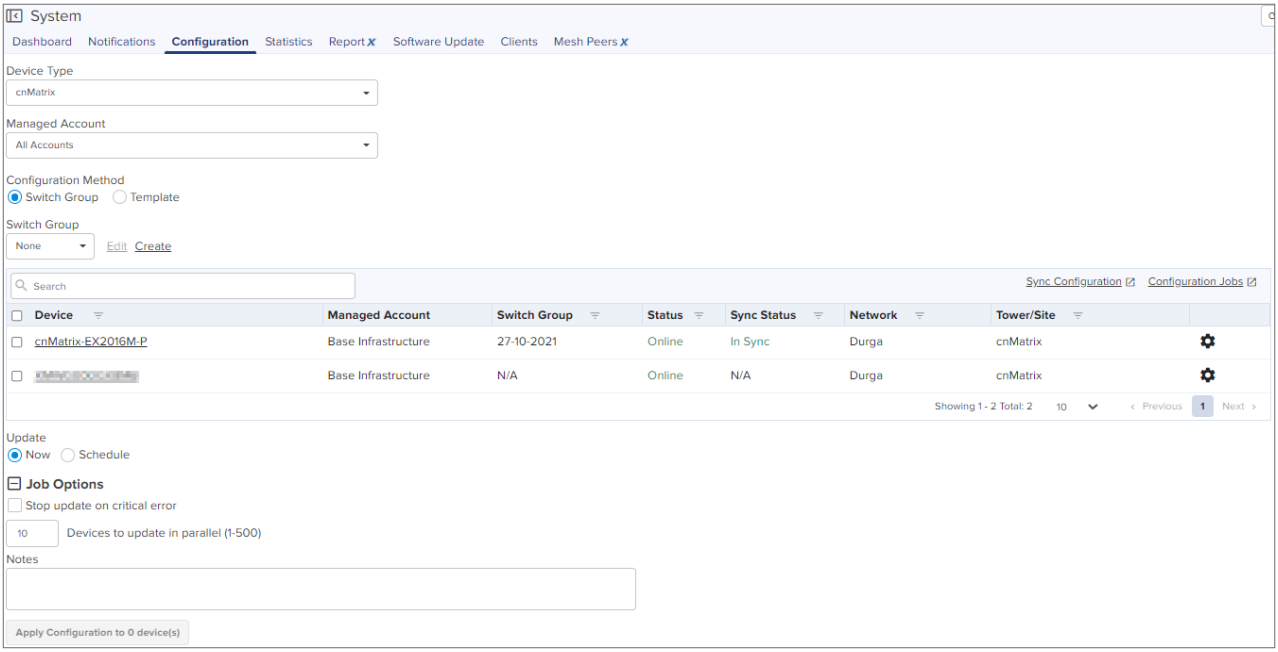
- The System Dashboard adds a Health component for Top Managed Accounts.

  Figure 352 *Dashboard > Top Managed Accounts*



- Global tabs in the UI are updated with a Managed Account column.

Figure 353 *Managed Account Column*



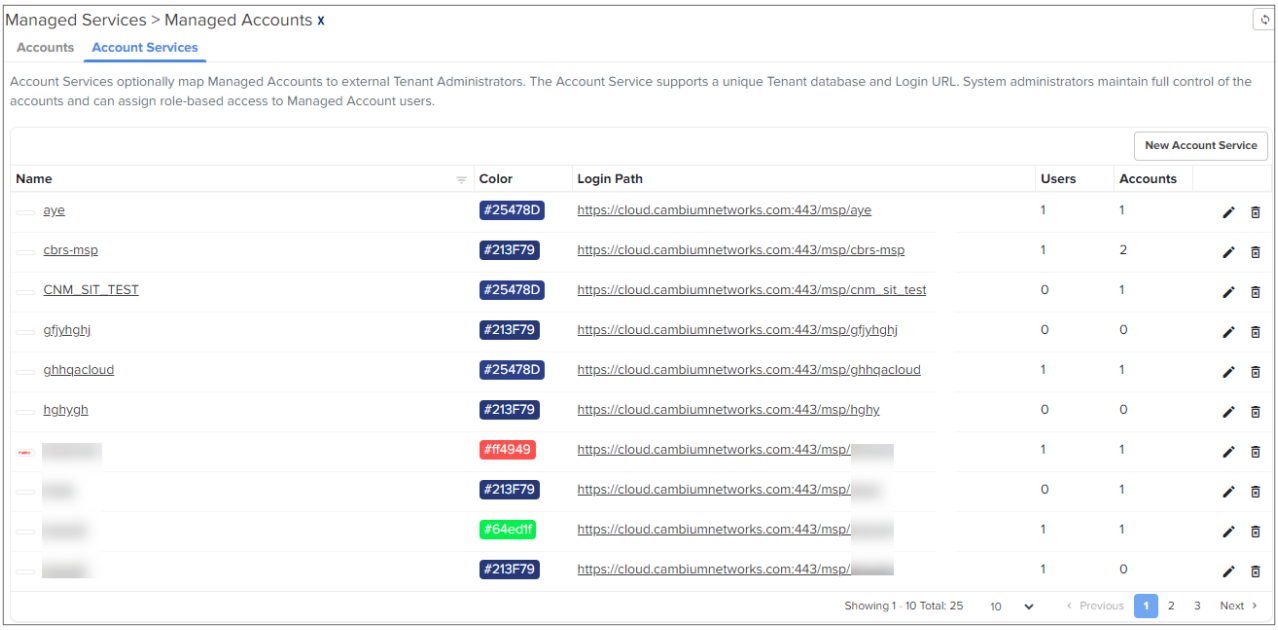
Creating Managed Account Services

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.

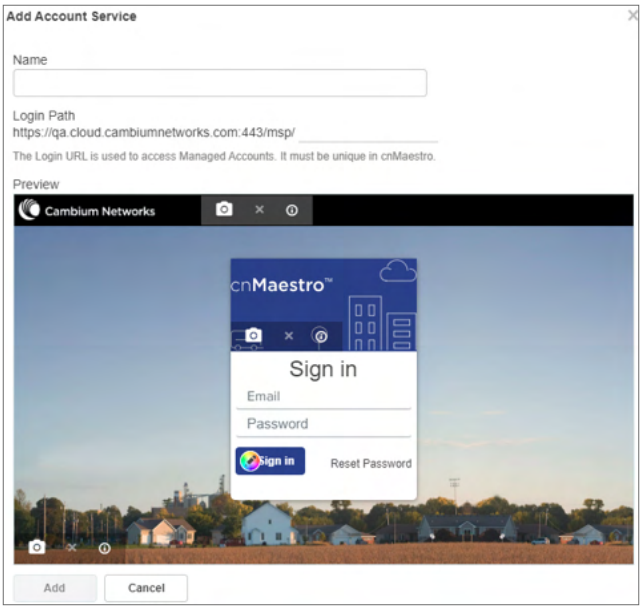
   Account Services Tab



2. Click **New Account Service.**

The **Add Account Service** window is displayed.

Add Account Service Window



3. Enter the following details:

Table 90 *Parameters in the Add Account Service Window*

Parameter	Description
Name	Name of the service. This name is visible to Account Administrators. A maximum of 64 characters are supported for the name.
Login Path	Account Administrators log into cnMaestro using a standard URL with an additional Path that defines the Account Service. For example, https://<cnmaestro cloud URL>/msp/<branded_service_path> **Note** • 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.

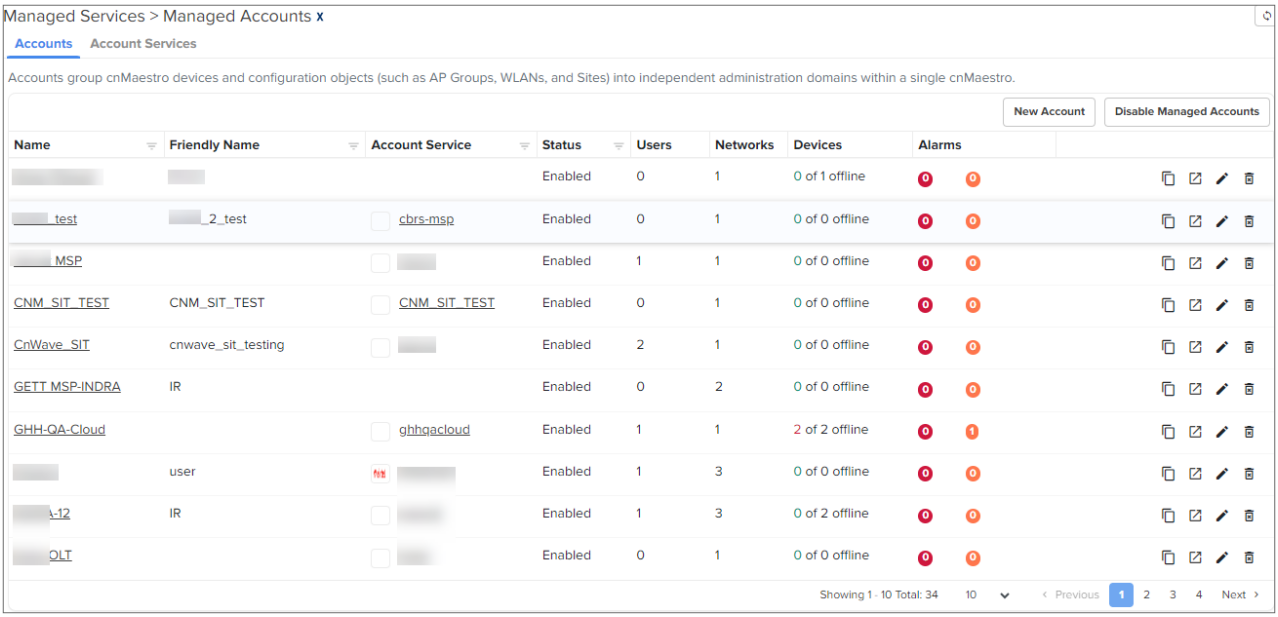
4. Click **Add**.

Creating Account

To create an Account:

1. Navigate to **Managed Accounts** > **Accounts** tab.

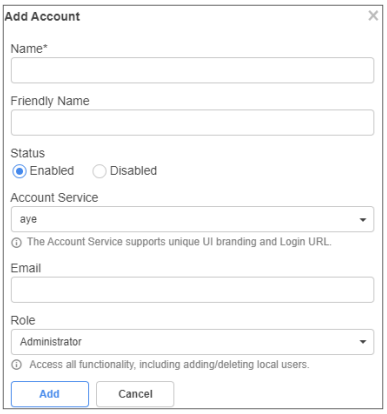
Figure 354 *Accounts Tab*



2. Click **New Account**.

   The **Add Account** window is displayed.

Figure 355 *Add Account window*



3. Enter the following details:

Table 91 *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

Table 91 *Parameters in the Add Account Window*

Parameter	Description
	has been created.
Role	The **Role** of the Account User (Administrator, Operator, or Monitor).

4. Click **Add**.

> **Note**
>
> Users are allowed to edit the existing name of the Account before validating the account.

Validating Account Users

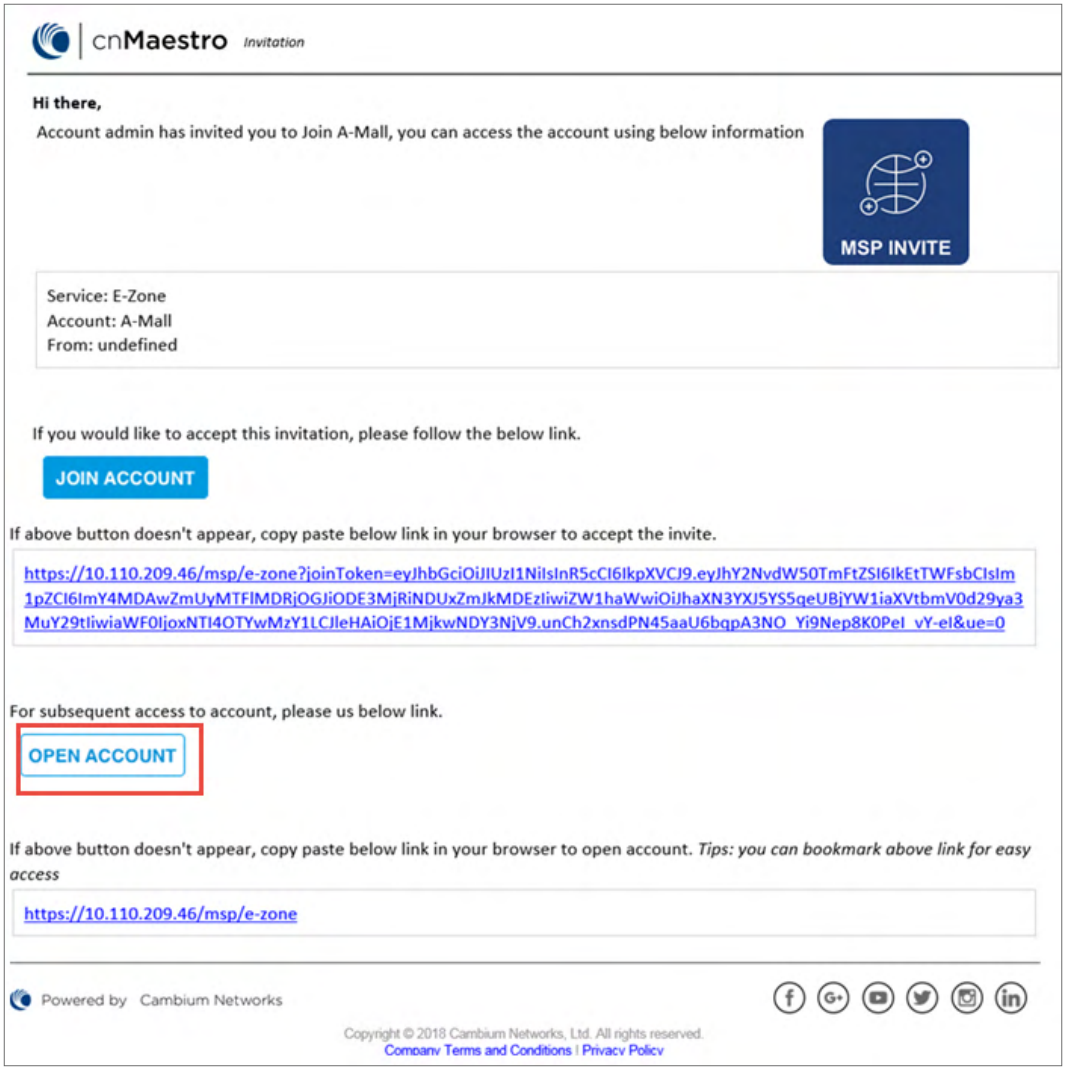
Once an Account is created, the Account User is sent an email invitation. The email provides directions on how to access the Account UI and set their password.

Figure 356 *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 357 *Checking Account Administrator User Email*



Create Account in Account Service

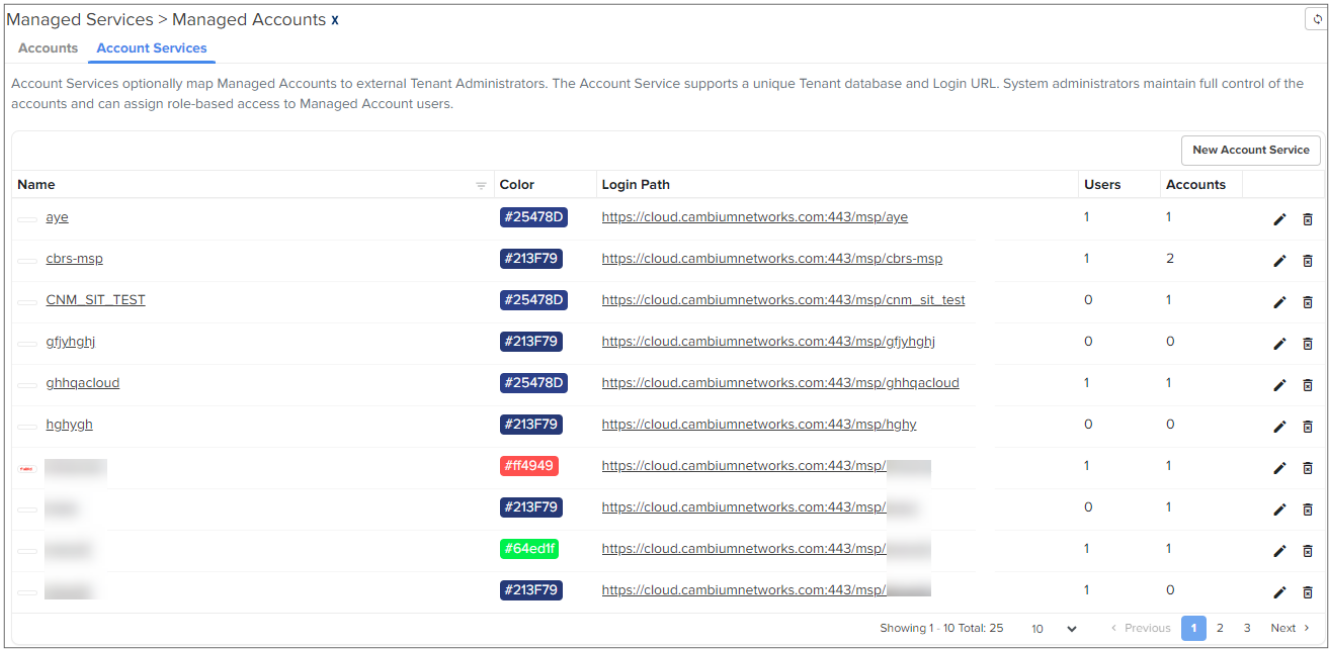
Clicking the link prompts the user to create a new Account or use an existing Account.

> **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 358 *A Sample Login URL*



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

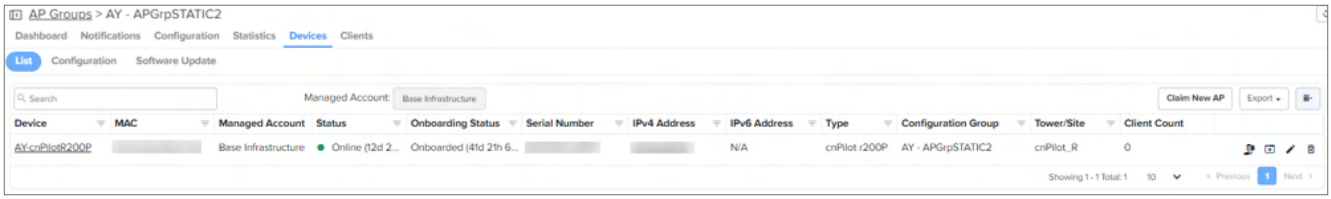
Global Super Administrator view along with respective Job IDs enrolled in the respective Accounts.

- 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 359 *System View*



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.

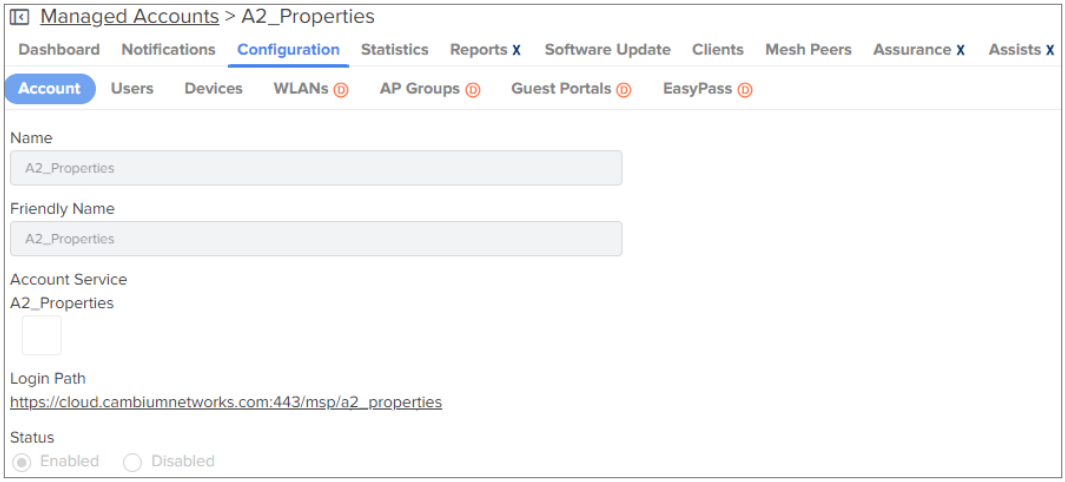
Note

The following configuration options have been deprecated from the Managed Accounts > Configuration page from release 5.2.5 onwards.

- WLANs—Navigate to the Wi-Fi Profiles page for configuring WLANs.
- AP Groups—Navigate to the Wi-Fi Profiles page for configuring AP Groups.
- Guest Portals—This is no longer supported in cnMaestro. Cambium recommends to use EasyPass portals.
- EasyPass—Navigate to the EasyPass page for configuring guest access portals.

These will be fully removed from the UI in a future release.

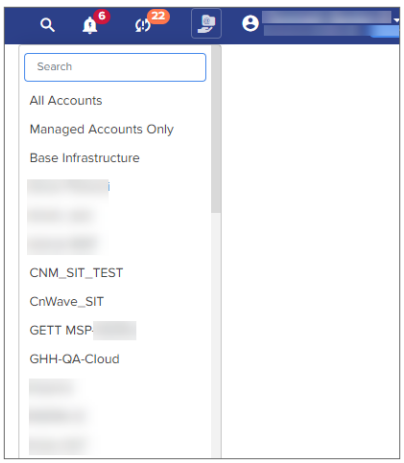
Figure 360 *Account View*



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 361 *Managed Account Administrator (User) View*



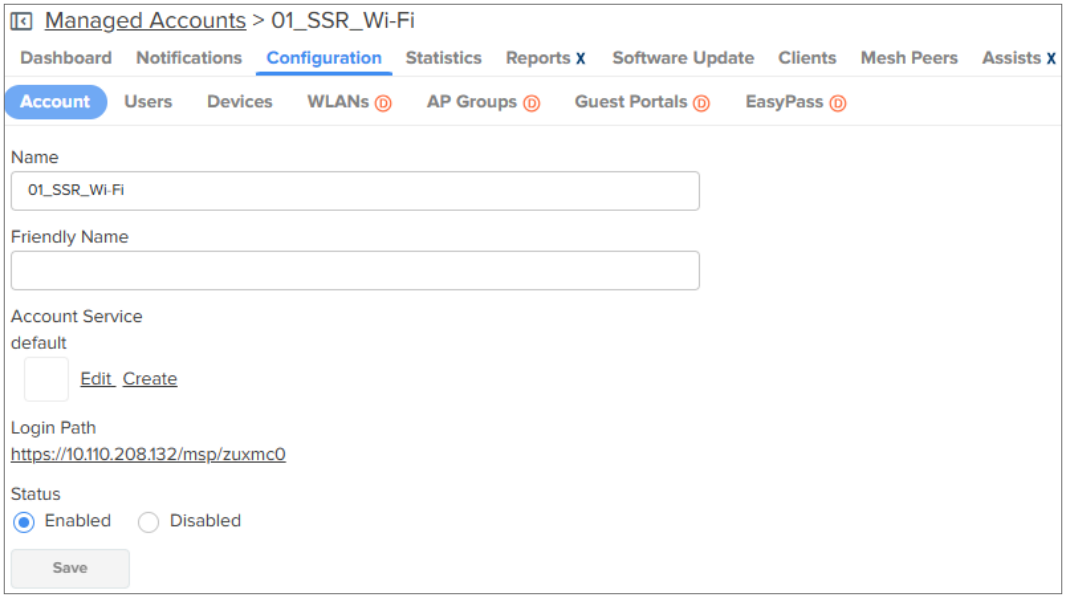
Users View

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.

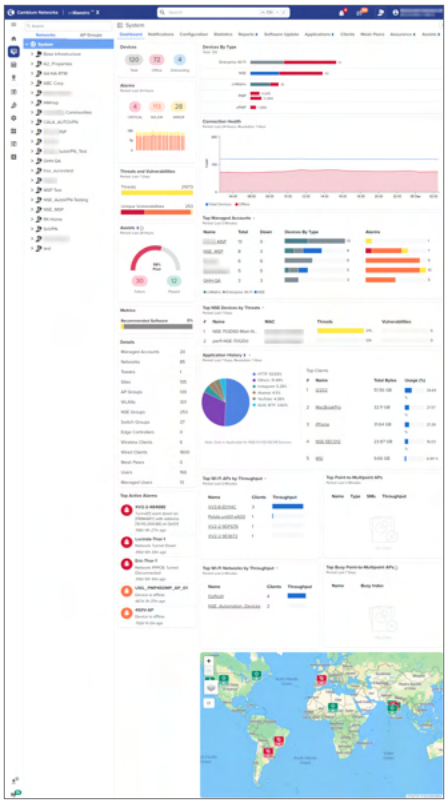
Figure 362 *Users*



System Dashboard

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

Figure 363 *System Dashboard*



Account Administration

AP Groups, WLANs, and Switch Groups have the following types of accessibility as shown below:

Table 92 *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.

> **Note**
>
> Once the Managed Account has been configured on an object, it cannot be changed.

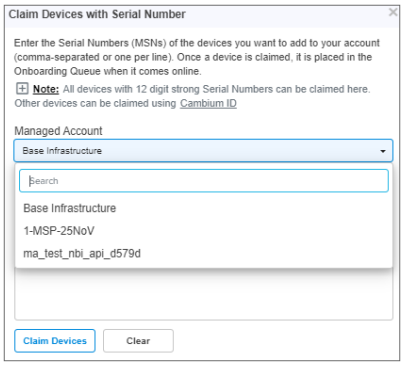
Device Management

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 364 *System Onboarding*



Device Onboarding

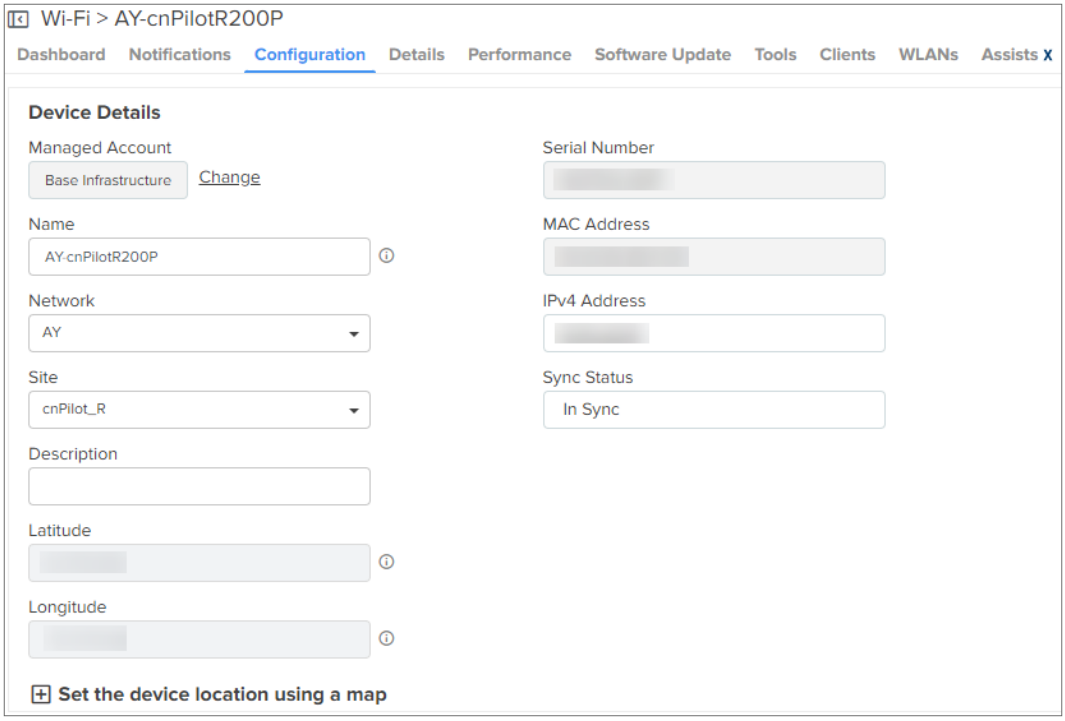
Onboarding devices through the Managed Account UI automatically places the devices in the Account.

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

Moving a Device Between Accounts

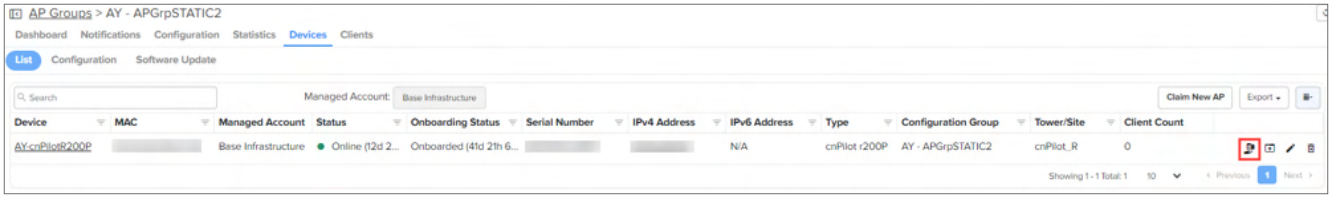
You can move a device from one Managed Account to another by using the **Change** option in the device configuration page.

Figure 365 *Moving a Device Between Accounts*



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

Figure 366 *Moving a device between Accounts in Enterprise View*



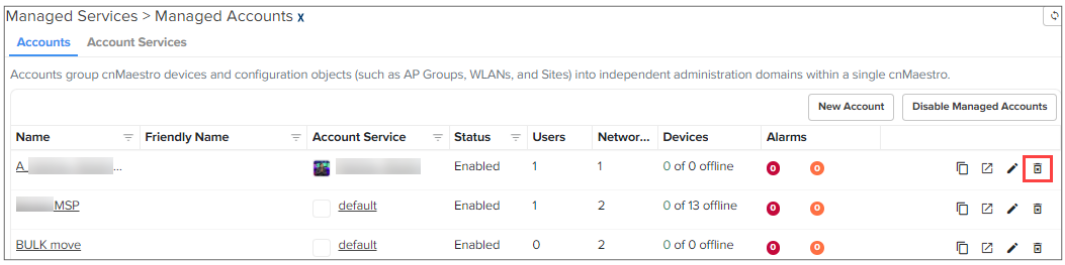
Account Deletion

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 367 *Account Deletion*

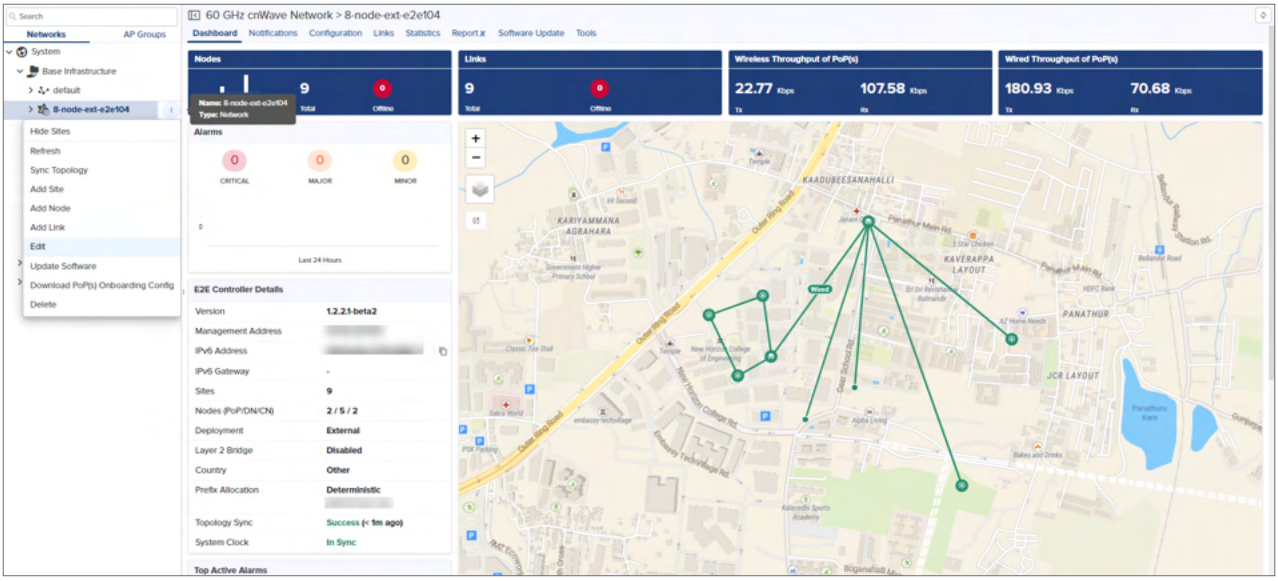


Swap 60 GHz cnWave Accounts

60 GHz cnWave Managed Accounts allow you to swap the Network from one Account to another.

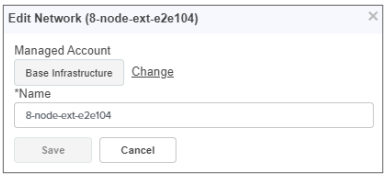
To swap the Account, perform the following steps:

1. Navigate to **System** tree > select **Accounts** > Select the **Network** to be Swapped.
2. Click **Action** (⋮) Icon.

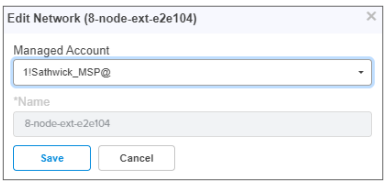


3. Click **Edit**.

   Edit Network window pops up.

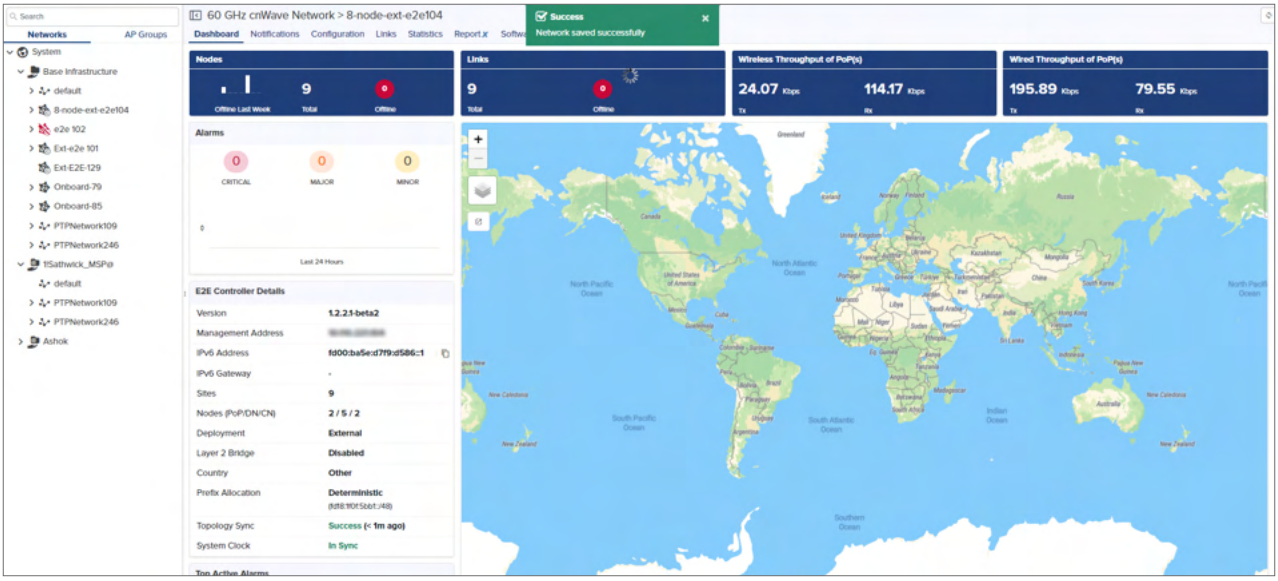


4. Click **Change**.
5. In **Edit Network** window, select the **Managed Account** from dropdown.



6. Click **Save**.

Success window pops up, when the **Network** is swapped from one **Account** to another **Account**.



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.

Note

Only the global administrator of On-Premises account has control on the following features:

- Association ACL
- Auto-Provisioning
- Scheduled Backup
- Server Settings
- SMTP Server
- SNMP Configuration

Network Services

This section includes the following topics:

- API Client
- RESTful API
- EasyPass
- SNMP
- RADIUS Proxy
- LTE
- Managing Edge Controller
- Installation Summary
- Spectrum Analyzer

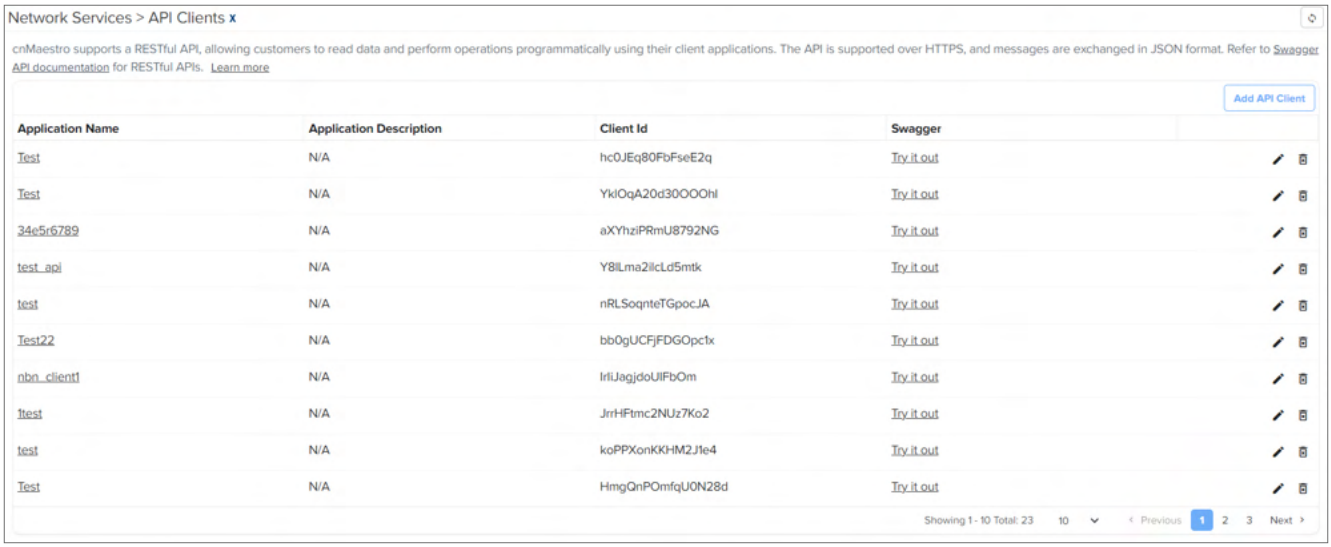
API Client

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.

API Clients

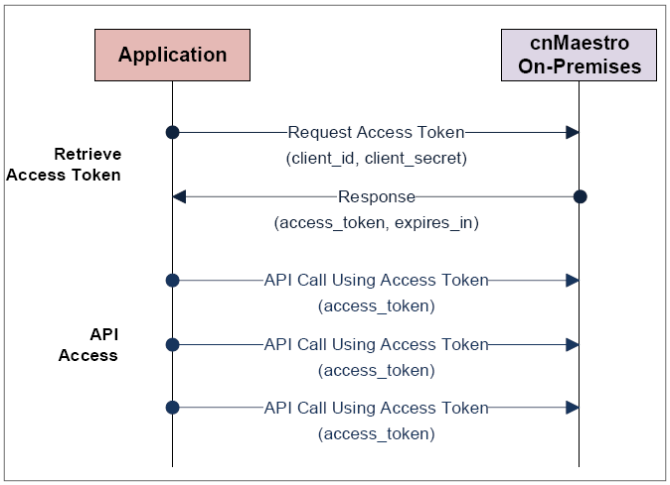
API Clients are external applications that access the RESTful API over HTTPS using OAuth 2.0 Authentication. They require a Client ID and Client Secret for access, both of which are detailed later in this chapter. For more information, refer to RESTful API Specification.



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.

Concurrent Access

Each client supports a single Access Token or multiple Access Tokens. Multiple Access Tokens allow concurrent access.

Single Access Token

If only one Access Token is enabled, whenever a new Access Token is generated from the Client ID and Client Secret, the previous Token expires immediately.

Multiple Access Tokens

If multiple access tokens are supported, then many clients can concurrently access the API. If another Access Token is created, the previous remains valid until their original expiration.

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.

The following table displays the approximate limit calculated by the system based on the number of CPUs.

Devices	GET	POST/Others
2 CPU	429	43
4 CPU	715	72
8 CPU	1429	143
12 CPU	2143	215
16 CPU	2715	272

Example of a Python client:

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

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

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

```
    return r.json()['access_token'], r.json()['expires_in']

def call_api(method, host, path, access_token):
    """
    Makes HTTP call to an API with given method.
    Parameters:
        `method` -
 method for the new Request object: GET, OPTIONS, HEAD, POST, PUT, PATCH, or DELETE\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()
```

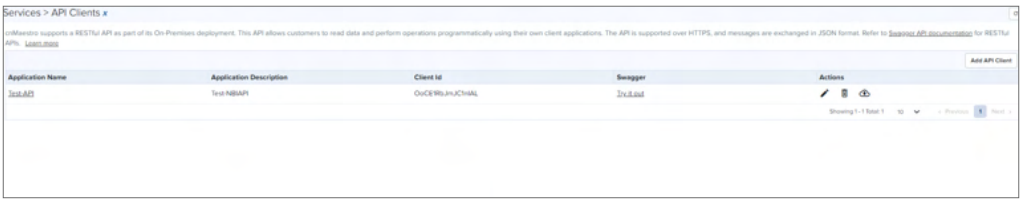
Swagger API

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.

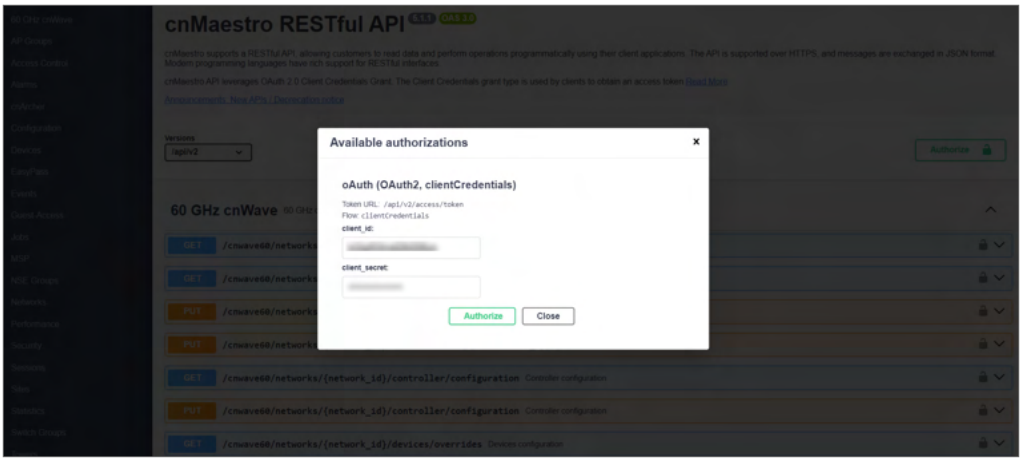
To access Swagger API, perform the following steps:

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



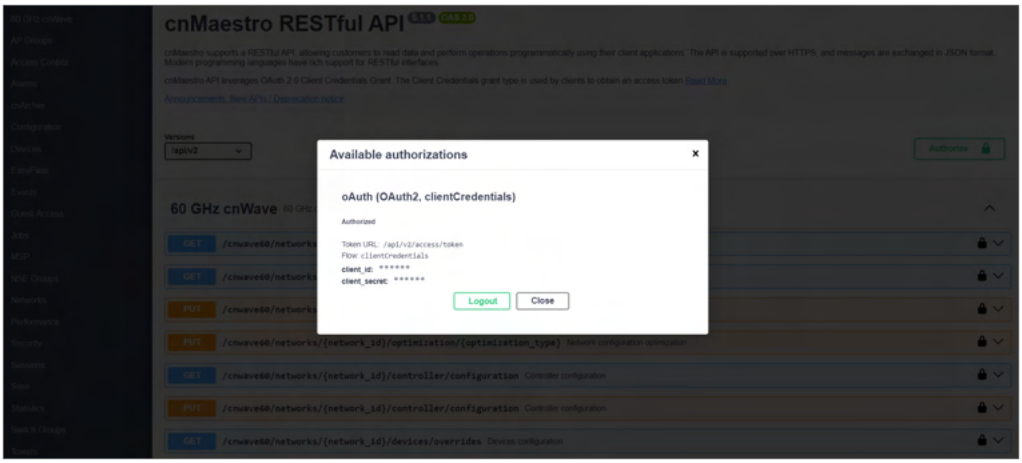
2. Click **Try it out**to open the Swagger UI.

   The **Available authorizations** window appears.



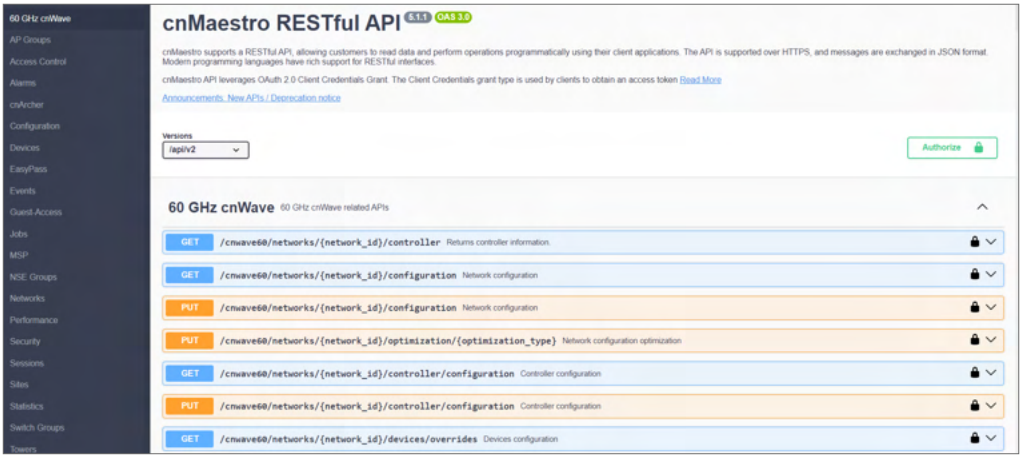
3. Enter **client_secret**.
4. Click **Authorize**.

   On successful authorization, an **Authorized** message appears in the **Available Authorization** window.



5. Click **Close**.

   The authorized **cnMaestro RESTful API** page appears.



API Session

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.

This section contains the following topics:

- Retrieving access token
  - Access Token Request (RFC 6749, section 4.4.2)
  - Access Token Response (RFC 6749, section 4.4.3)
  - Error Response (RFC 6749, section 5.2)
- Renewing access tokens
- Retrieving access token

Retrieving 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":"2YotnFZFEjr1zCsicMWpAA",
  "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 93 *Error Responce*

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"
}
```

Renewing access tokens

When a client requests an access token while a previous token is still valid, the system determines whether to return the existing token or generate a new one based on a renewal threshold.

cnMaestro pre-defines the renewal threshold as 50% of the token lifetime OR 15 minutes, whichever is lesser.

cnMaestro processes the renewal requests in the following ways:

- If the request is made before the renewal threshold:
  - No new token is generated.
  - The existing token is returned.
  - The token retains its remaining expiry time.
- If the request is made after the renewal threshold:
  - A new token is generated.
  - The new token gets a full expiry duration.
  - All previously issued tokens are immediately invalidated.

The following example scenarios explain how cnMeastro processes the renewal requests:

Scenario 1

- Token expiry: 300 seconds (5 minutes)
- Renewal threshold: 150 seconds (50% of token expiry)
- For requests received before 150 seconds—existing token is returned (with remaining expiry).
- For requests received after 150 seconds—new token is generated (valid for 300 seconds) and the previous token is invalidated immediately.

Scenario 2

- Token expiry: 3600 seconds (1 hour)
- Renewal threshold : 900 seconds (15 minutes, which is lesser than 50% of token expiry, in this case 1800 seconds).
- For requests received before 15 minutes—existing token is returned (with remaining expiry).
- For requests received after 15 minutes—new token is generated (valid for 3600 seconds) and the previous token is invalidated immediately.

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 94 lists the response codes that are supported in cnMaestro and may be returned through the HTTP protocol.

Table 94 *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 95 lists the HTTP request codes supported in cnMaestro.

Table 95 *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 96 *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 97 *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.

Context	Details
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 98 *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 99 describes the standard filtering parameters as shown below:

Table 99 *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, 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 100 are not specified, then the start or stop times will be open-ended.

Table 100 *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 101 *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 102 *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 103 *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 104 describes about the header and its values as shown below:

Table 104 ***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.

Name	Details
token_type	This will always be bearer.

```
{
   "access_token":"2YotnFZFEjr1zCsicMWpAA",
   "token_type":"bearer",
   "expires_in":3600
}
```

Example

Request

curl https://10.110.134.12/api/v2/access/token \

```
 -X POST -k \
 -u 8YKCxq72qpjnYmXQ:pcX5BmdJ2f4QLM5RfgsS4jOtxAdTRF \
 -d grant_type=client_credentials
```

Response

```
{"access_token":"d587538f445d30eb2d48e1b7f7a6c9657d32068e","token_type":"
 bearer","expires_in":86400}
```

Token (alternate request)

POST

`/api/v2/access/token`

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

Request

Headers

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

Body

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

Response

The response to both forms is the same.

Body

Name	Details
access_token	Access token to return with each API request.

Name	Details
expires_in	Time in seconds that the API session will remain active.
token_type	This will always be bearer.

```
{
   "access_token":"2YotnFZFEjr1zCsicMWpAA",
   "token_type":"bearer",
   "expires_in":3600
}
```

Example

Request

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
```

Response

```
{"access_token":"ee4e077cf457196eb4d27cf6f02686dc07763059","token_type":"
bearer","expires_in":86400}
```

Validate Token

GET

`/api/v2/access/validate_token`

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

Request

HTTP Headers

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

Response

Body

Name	Details
expires_in	Time in seconds that the API session will remain active.

```
{
   'expires_in': 86399
}
```

Example

Request

curl https://10.110.134.12/api/v2/access/validate_token \
`-X GET -k \`
`-H "Authorization: Beareree4e077cf457196eb4d27cf6f02686dc07763059"`

Response
`{"expires_in":85643}`

API Changes

For information about new APIs added, updates to existing APIs, and deprecations, see cnMaestro 6.0.0 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	ePMP	PMP	Wi-Fi	cnReach	cnVision	PTP	PTP 8xx	cnMatrix	60 GHz cnWave	cnWave 5G Fixed
azimuth	Azimuth of the device	✔	✔								
beam_width	Beam width of the device	✔	✔								
cbrs_state	CBRS state		✔								
cbrs_status	CBRS status		✔								
config.sync_reason	Configuration synchronization reason	✔	✔	✔	✔	✔	✔	✔	✔		
config.sync_status	Configuration synchronization status	✔	✔	✔	✔	✔	✔	✔	✔		
config.variables	Device is mapped to configuration variables	✔	✔	✔	✔	✔	✔	✔	✔		
config.version	Current configuration version	✔	✔	✔	✔	✔	✔	✔	✔		
country	Country	✔	✔	✔		✔					
country_code	Regulatory band						✔				
description	Description	✔	✔	✔	✔	✔	✔		✔	✔	
elevation	Elevation of the device	✔	✔								
hardware_version	Hardware version	✔	✔	✔	✔	✔	✔	✔	✔	✔	
height	Height of the device	✔	✔								
height_unit	Units of the device	✔	✔								
inactive_software_version	Inactive software version	✔	✔	✔	✔	✔	✔	✔	✔		✔
ip	IP address	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔

Name	Details	ePMP	PMP	Wi-Fi	cnReach	cnVision	PTP	PTP 8xx	cnMatrix	60 GHz cnWave	cnWave 5G Fixed
`ipv6`	IPv6	✔		✔		✔				✔	✔
`is_pop`	Determines whether PoP or not									✔	
`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	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
`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	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔

Name	Details	ePMP	PMP	Wi-Fi	cnReach	cnVision	PTP	PTP 8xx	cnMatrix	60 GHz cnWave	cnWave 5G Fixed
`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/down time interval (seconds)	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
`temperature`	Temperature							✔			
`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_`	Device is waiting for cnMaestro cloud sync process to acquire a subscription slot.

Onboarding State	Details
CLOUD_SYNC	
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
- 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.

Error Codes	Details
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
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

cnMatrix

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

cnReach

General

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

Networks

Name	Details	Mode
ip	IP address	All

Radios (Array format)

Name	Details	Mode
radios[].device_id	Device ID	Radios
radios[].id	Radio Id	Radios
radios[].linked_with	Linked with	Radios
radios[].mac	Radio MAC	Radios
radios[].margin	Margin	Radios
radios[].mode	Radio mode [ap, ep, rep]	Radios
radios[].neighbors	Radio neighbors	Radios
radios[].network_address	Network address	Radios
radios[].noise	Average noise (dB)	Radios
radios[].power	Transmit power	Radios

Name	Details	Mode
radios[].rssi	RSSI value (dB)	Radios
radios[].rx_bytes	Receive bytes	Radios
radios[].software_version	Current software version.	Radios
radios[].temperature	Radio temperature	Radios
radios[].type	Radio type [ptp, ptmp]	Radios
radios[].tx_bytes	Transmit bytes	Radios

Fixed Wireless (cnVision, ePMP and PMP)

General

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

Name	Details	cnVision	ePMP	PMP
ip_wan	WAN IP	AP/SM	AP/SM	
lan_mode_status	LAN mode status [no-data, half, full]	AP/SM	AP/SM	
lan_mtu	MTU size	SM	SM	
lan_speed_status	LAN speed status	AP/SM	AP/SM	
lan_status	LAN status [down, up]	AP/SM	AP/SM	AP/SM
netmask	Network mask	AP/SM	AP/SM	AP/SM

Radios

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

Name	Details	cnVision	ePMP	PMP
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 [eptp-master, eptp- 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 MIMO-B)]			SM
radio.ul_lqi	Uplink Link Quality Indicator			SM
radio.ul_pkts	Uplink packet count	AP/SM	AP/SM	AP/SM
radio.ul_pkts_loss	Uplink packet loss			AP/SM
radio.ul_retransmits	Uplink Retransmission	SM	SM	
radio.ul_retransmits_pct	Uplink Retransmission percentage	AP/SM	AP/SM	
radio.ul_rssi	Uplink RSSI	SM	SM	SM
radio.ul_snr	Uplink SNR (dB)	SM	SM	
radio.ul_snr_h	Uplink SNR (dB) horizontal			SM
radio.ul_snr_v	Uplink SNR (dB) vertical			SM
radio.ul_throughput	Uplink throughput	AP/SM	AP/SM	AP/SM
radio.wlan_status	WLAN status [down, up]	AP/SM	AP/SM	

PTP 650/670/700

General

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

Networks

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

Ethernet Ports (Array format)

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

Radios

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

PTP 820/850

General

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

Radio

Name	Details	Mode
radios[].defective_blocks	Radio defective blocks	All
radios[].id	Radio Id	All
radios[].radio_location	Radio location	All
radios[].rx_bps	Receive bits/second	All
radios[].rx_level	Receive level	All
radios[].rx_frequency	Receive frequency	All
radios[].tx_bps	Transmit bits/second	All
radios[].tx_level	Transmit level	All

Name	Details	Mode
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[].interaface_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
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[].packet_error_rate	Packet error of the radio	All
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

Interfaces

Name	Details	Mode
interfaces[].admin_state	Admin state	All
interfaces[].auto_negotiation	Auto Negotiation	All
interfaces[].interaface_location	Interface location	All

Name	Details	Mode
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

Tunnels

Name	Details	Mode
tunnels[].auth_type	Authentication type of the tunnel	All
tunnels[].local_host	Local host of the tunnel	All
tunnels[].remote_host	Remote host of the tunnel	All
tunnels[].rx_bytes	Received bytes over the tunnel	All
tunnels[].server_type	Server type of the tunnel	All
tunnels[].status	Status of the tunnel	All
tunnels[].tx_bytes	Transmitted bytes over the tunnel	All
tunnels[].type	Type of tunnel	All
tunnels[].uptime	Tunnel Uptime	All

cnWave 5G Fixed

General

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

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

Boot

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

Shutdown (Array format)

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

Interface Config

Name	Details	Mode
sfp1_speed	SFP1 Speed	BTS
sfp2_speed	SFP2 Speed	BTS

Interfaces (Array format)

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

Radio

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

Wireless and Ethernet interfaces

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

Name	Details	Mode
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
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)

Name	Details
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
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
radio.dl_rssi_imbalance	Downlink RSSI imbalance			SM
radio.dl_snr	Downlink SNR	SM	SM	
radio.dl_snr_h	Downlink SNR (dB) horizontal			SM

Name	Details	cnVision	ePMP	PMP
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

Name	Details	Mode
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_max_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

Name	Details	Mode
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

Name	Details	Mode
`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	AP MAC address **Note** This field has been deprecated since release 5.0.0 and will be fully removed in release 5.3.0. Use the `device_mac` field instead.
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	Transmit bytes

Name	Details
	Note This field has been deprecated since release 5.0.0 and will be fully removed in release 5.3.0. Use the `tx_bytes` field instead.
radio.rx_bytes	Received bytes **Note** This field has been deprecated since release 5.0.0 and will be fully removed in release 5.3.0. Use the `rx_bytes` field instead.
tx_bytes	Transmit bytes
rx_bytes	Received bytes
total_quota	Total quota
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
e88916f5b663c1ea966af835c8a0a19c20d17686" -H "Content-Type: application/json"-d
```

Body

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

Response:

```
{
"data": {
         "mType": 3,
         "msgId":28,
         "status":<integer values>,
         "prefixQs":<true/false>,
```

```
            "expiry":<integer values>,
            "action":<integer values>,
            "cmac":<client mac>,
            "msg":<Radius Returned Message>,
            "extURL":<external url string>
            }
}
```

The status value description is provided in the table below.

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

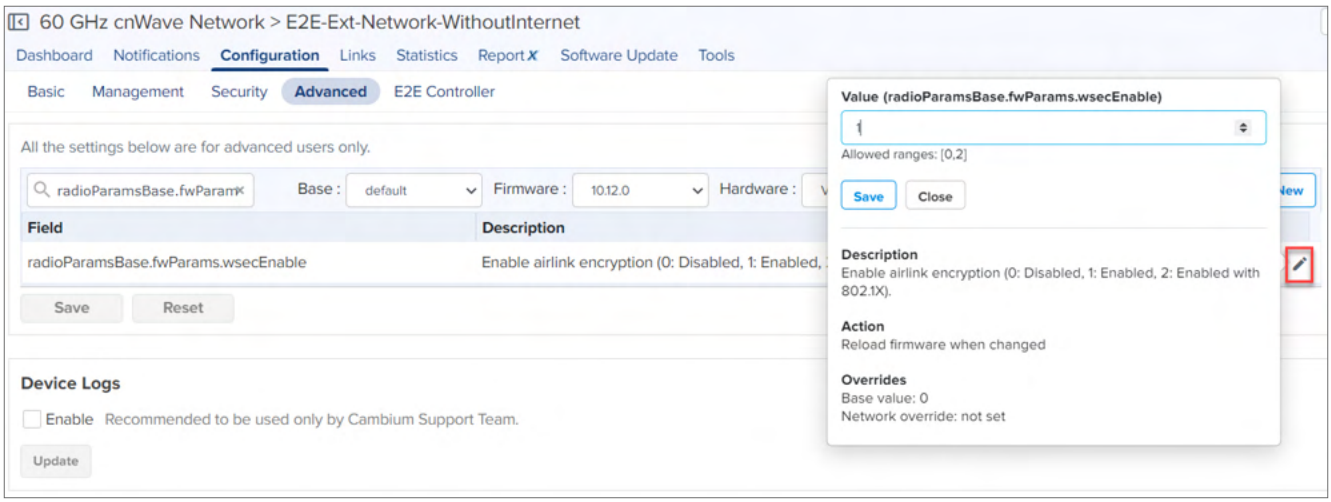
cnMaestro supports configuration overrides for 60 GHz cnWave E2E Network, E2E Controller, and Node(s) using the RESTful API.

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`



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

Example

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

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

Warning

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

Optimization

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

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

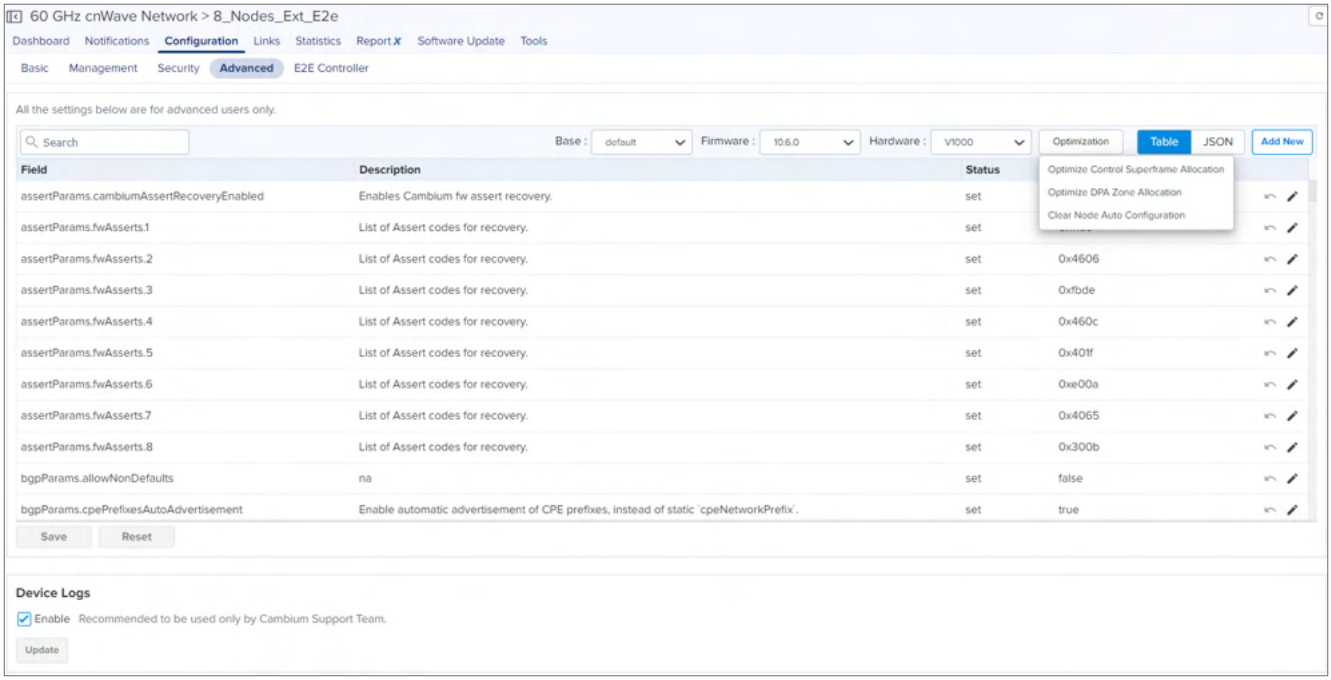
PUT `/api/v2/cnwave60/networks/{network_id}/optimization/{optimization_type}`

Available values :

`controlSuperframeAllocation`,

`dpaZoneAllocation`

`clearNodeAutoConfig`



Example

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

Device (Node) Configuration

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

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

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

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

Example

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

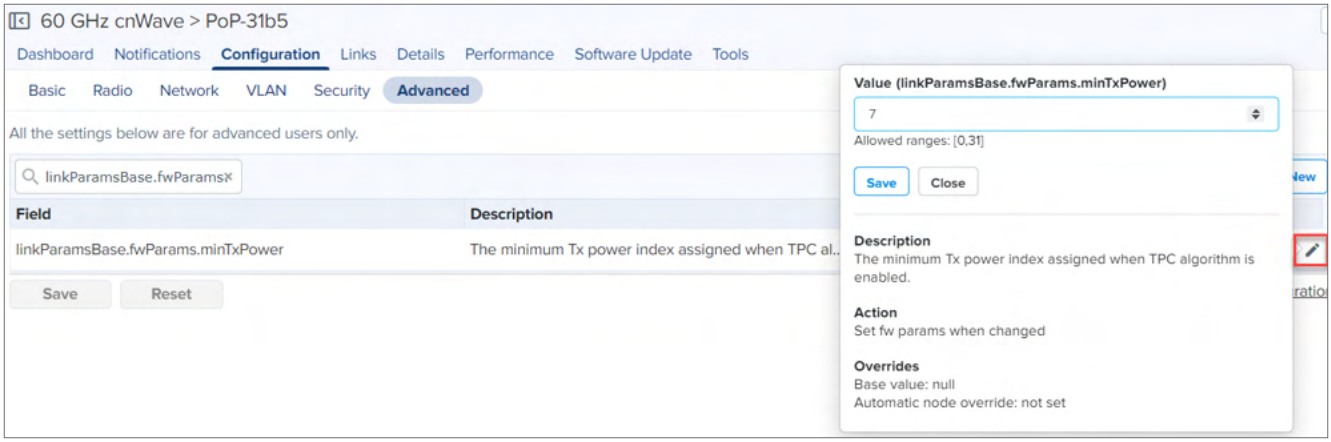
```
{
    "linkParamsBase": {
        "fwParams": {
            "minTxPower": 6
            "maxTxPower": 8
         }
      }
```

```
}
```

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

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

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



Warning

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

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

Example

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

Note

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

E2E Controller

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

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

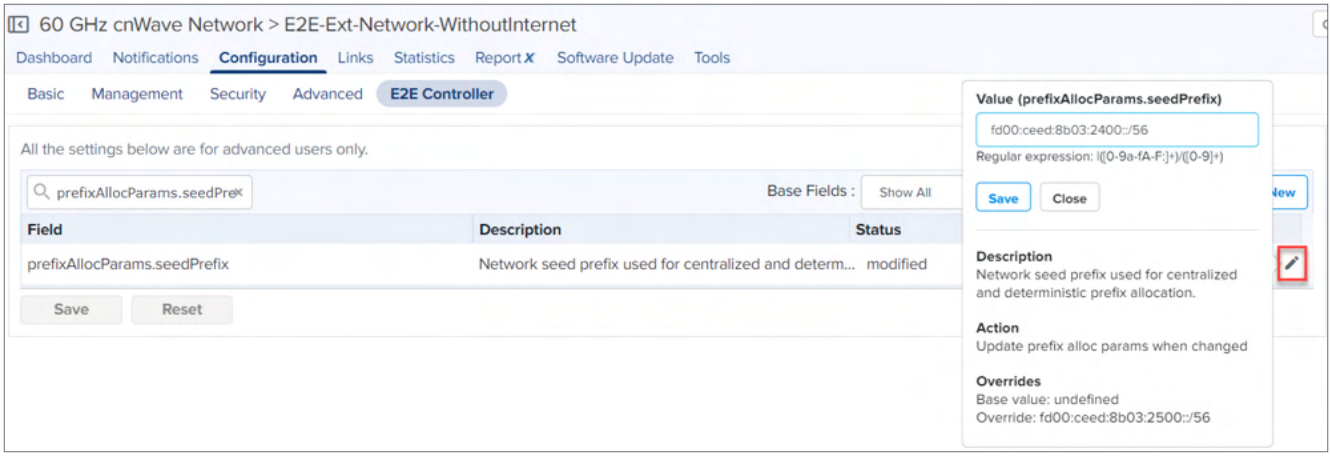
PUT `/api/v2/cnwave60/networks/{network_id}/controller/configuration`

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

Example

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

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



Warning

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

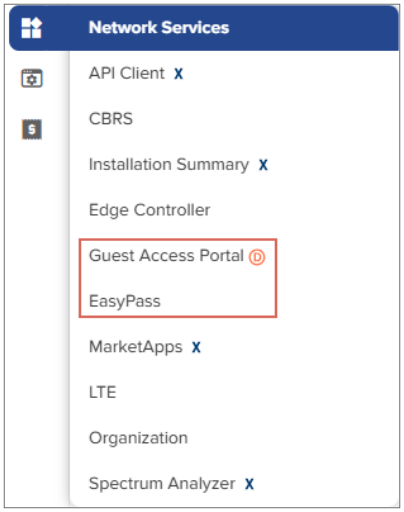
EasyPass

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

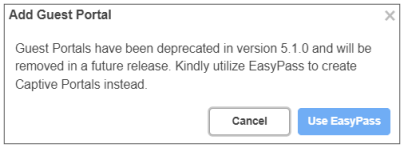
From cnMaestro 5.1.0 release onwards, the **Guest Access Portal** configuration wizard is deprecated and a new wizard, **EasyPass**, is introduced (as shown in Figure 368).

Figure 368 *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 369).

Figure 369 *The Add Guest Portal window*



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

Table 105 lists the supported devices and their compatibility with EasyPass.

Table 105 *List of supported devices - EasyPass*

Device	EasyPass support
Wi-Fi 5	Yes
Wi-Fi 6	Yes
Wi-Fi 7	Yes
Xirrus APs	No

EasyPass portal types are grouped into the following categories:

- Guest/Public 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.

> **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.
- Third-party Integration—Allows partners to integrate their external captive portals with cnMaestro by posting authentication and logout requests directly to cnMaestro.

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

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 106 *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	✔	✔
Paid **X**	✔	✔
WiFi4EU	✔	✔
Combined		
One Click + Voucher	✔	✔
One Click + Paid **X**	✔	✔
Voucher + Paid **X**	✔	✔

Implementation of EasyPass portals for various types of users

Table 107 lists the various types of users for whom the EasyPass portals can be implemented or best suited:

Table 107 *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										✔	

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 One Click + Voucher portal
  - Creating One Click + Paid X portal
  - Creating Voucher + Paid X portal
  - Creating a Third-Party Integration 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
  - EasyPass

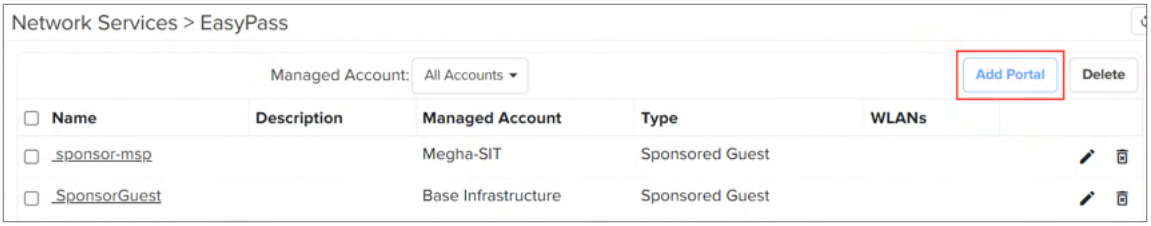
Creating a portal

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 370 *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 371 displays the options available for cnMaestro Essentials.

Figure 371 *The Select Portal Type window—cnMaestro Essentials*

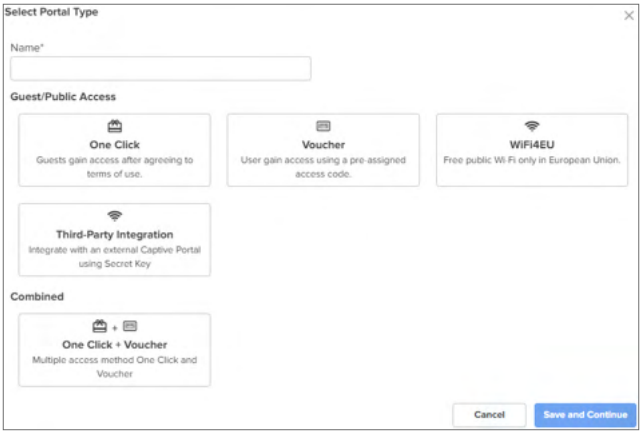
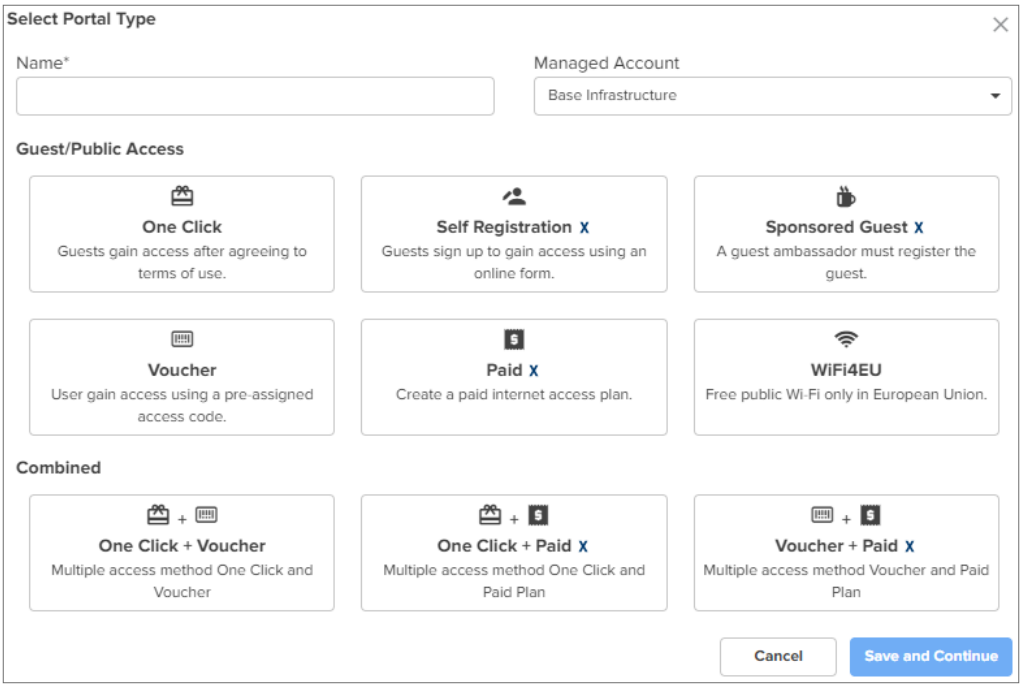


Figure 372 displays the options available for cnMaestro X.

Figure 372 *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.

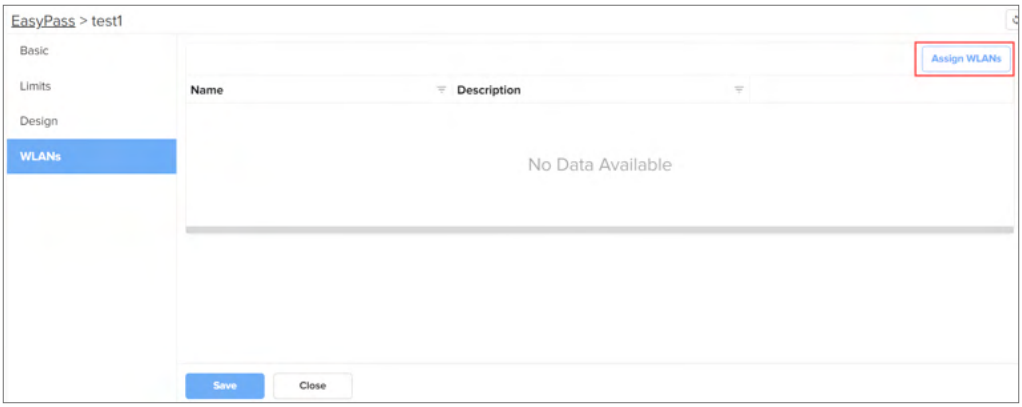
   - For the **Self Registration X** portal type, follow the additional steps described in Creating Self Registration X portal.
   - For the **Sponsored Guest X** portal type, follow the additional steps described in Creating Sponsored Guest X portal.
   - For the **Voucher** portal type, follow the additional 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 **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.

8. Configure the parameters of the **Limits** screen as described in The Limits screen parameters.
9. Click the **Design** tab and configure the parameters as described in The Design screen parameters.
10. Click the **WLANs** tab.

    The **WLANs** screen appears.

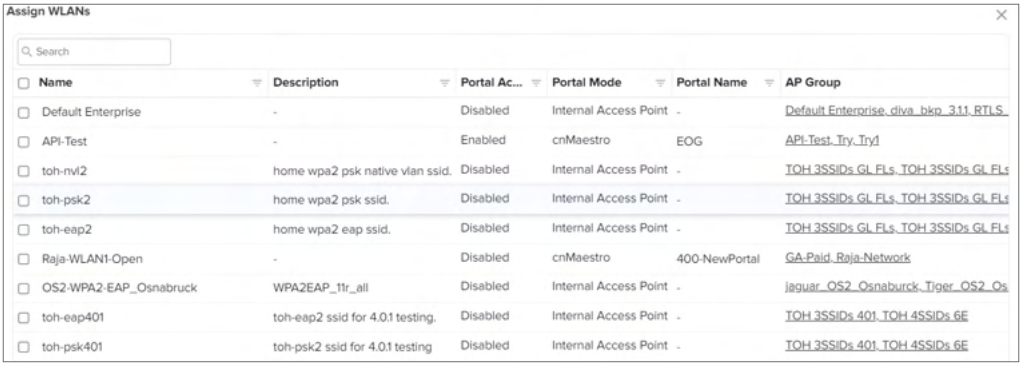
    Figure 373 *The WLANs screen*



11. Click **Assign WLANs**.

    The **Assign WLANs** window appears.

    Figure 374 *The Assign WLANs window*



12. Select the required WLANs and click **Assign**. For example, **testWLAN**.

    The selected WLAN is added to the WLANs page.

    Figure 375 *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 376 displays the **Basic** screen parameters.

Figure 376 *The Basic screen*

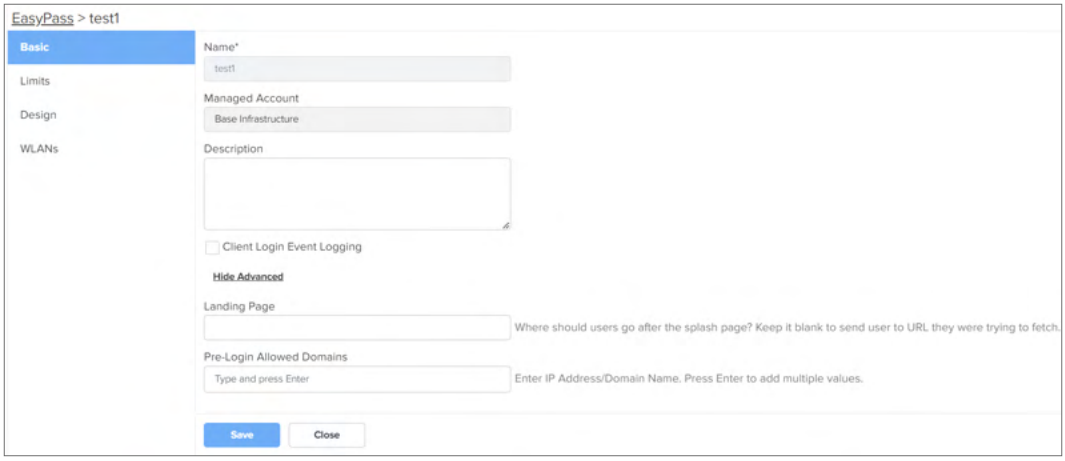


Table 108 describes the **Basic** screen parameters that appear across all portal types on their respective **Basic** screens.

Table 108 *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.

Table 108 *The Basic screen parameters*

Parameter	Description
	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 377 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 377 *The Limits screen*

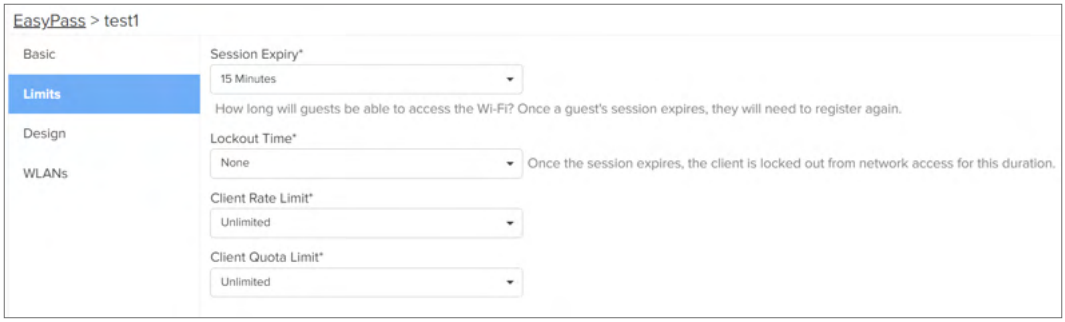


Table 109 describes the **Limits** screen parameters that appear across all portal types on their respective **Limits** screens.

Table 109 *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: • 15 Minutes • 1 Hour • 1 Day • 1 Month • End of Day (Midnight)

Table 109 *The Limits screen parameters*

Parameter	Description
	• End of week (Saturday) • Custom By default, **15 Minutes** is selected. Select the required option from the dropdown list. **Note**: When you select the **Custom** option, you can configure the minimum duration value to 1 for Days, Hours, and Minutes.
Lockout Time	The lockout time restricts the ability to create a new session for the specified duration when a session expires. The following options are supported: • None • 15 Minutes • 1 Hour • 1 Day • 1 Month • End of Day (Midnight) • End of week (Saturday) • Custom By default, **None** is selected. Select the required option from the dropdown list. **Note**: The **Lockout Time** parameter is not available for Self Registration X, Sponsored Guest X, Voucher, and Paid X portal types.
Client Rate Limit	Indicates the client rate limit. The following options are supported: • Limited—When the **Limited** option is selected, the **Downlink** and **Uplink** parameters appear. • Unlimited By default, **Unlimited** is selected. You can configure the client rate limit per user.
Downlink	This parameter is applicable only when **Client Rate Limit** is set to **Limited**. Downlink of client rate limit in Kbps. Maximum value: 1000000
Uplink	This parameter is applicable only when **Client Rate Limit** is set to **Limited**. Uplink of client rate limit in Kbps. Maximum value: 1000000
Client Quota Limit	Indicates the client quota limit.

Table 109 *The Limits screen parameters*

Parameter	Description
	The following options are supported: • Limited—When the **Limited** option is selected, the **Total** parameter appears. • Unlimited By default, **Unlimited** is selected. You can configure the client quota limit per user.
Total	The total client quota in MB or GB. You can either select **MB** or **GB** option from the dropdown list. By default, **MB** option is selected. **Note**: This parameter supports: • A minimum of 1 MB and a maximum of 8000000 MB. • A minimum of 1 GB and a maximum of 8000 GB.
Note: An additional parameter, **Device Limit**, must be configured for the following portal types in the **Limits** screen: • Self Registration X The **Device Limit** parameter must also be configured for the following portal types: • 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	Specifies the number of devices that the guest can connect to the wireless network. Minimum value: 1 Maximum value: 200 You can configure the device limit per user.

Note

After configuring the **Limits** screen parameters, proceed to step 9 described in the Creating a portal process.

The Design screen parameters

Figure 378 displays the **Design** screen parameters.

Note

The layout of the preview window differs based on the portal type you select.

Figure 378 *The Design screen*

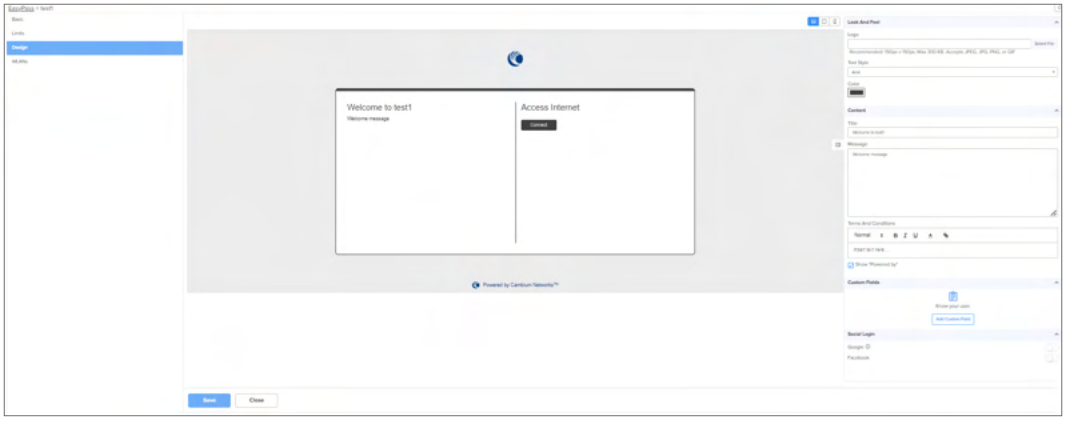


Table 110 describes the common **Design** screen parameters that appear across all portal types on their respective **Design** screens.

Table 110 *The Design screen parameters*

Parameter	Description
Logo	Logo for the portal. Recommended size: 150 x 150 pixels Maximum file size: 3 MB Supported formats: JPEG, JPG, PNG, or GIF
Page Background Image	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. The **Page Background Image** option is disabled by default. Enable the **Page Background Image** option and select an image file to upload.
Upload Image	This parameter is applicable only when the **Page Background Image** option is enabled. Select an image file to upload. Recommended size: 1024 x 768 pixels Maximum file size: 5 MB Supported formats: JPEG, JPG, PNG, or GIF
Background Placement	Background placement for the selected image. Select the required background placement option from the **Background Placement** dropdown list. The following options are supported: • Left Top • Left Center • Left Bottom • Right Top • Right Center • Right Bottom

Table 110 *The Design screen parameters*

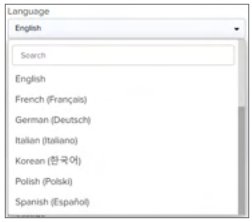
Parameter	Description
	• Center Top • Center Center • Center Bottom By default, the **Center Center** option is selected.
Repeat Background	This parameter is applicable only when the **Page Background Image** option is enabled. Enable the **Repeat Background** option to repeat the selected background. The **Repeat Background** option allows you to repeat a small image or pattern across your portal, creating a continuous background. **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.
Theme Color	Theme color for the design page.
Content Background Opacity	A value to increase or decrease the background opacity on the portal. Default value: 100 Minimum value: 0 Maximum value: 100
Text Color	Color of the text on the portal.
Language	Language for the content displayed on the EasyPass portal. The following languages are supported: • English • French • German • Italian • Korean • Polish • Spanish  Default is English. 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

Table 110 *The Design screen parameters*

Parameter	Description
	added. You must manually enter these contents in the selected language.
Font Face	Type of font to be used for the portal. The following options are supported: • 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	Indicates that a service is provided by an organization. You can disable this parameter. By default, this parameter is enabled.
Custom fields	Select the required fields to include in the design page by clicking **Add Custom Field**. The following options are supported: • Text • Number • Email • Phone • Date • Name
Connect	An option to provide access for users to the internet. Click **Connect** to access the internet. This is the default option available on the design page.
Custom Styling (CSS)	Enable the **Custom Styling (CSS)** option and select a CSS file to upload. You also have an option to download a sample CSS file.
Device-specific view options of the design page 	The view options on the design page are tailored for various devices. The following options are supported: • Desktop View • Tablet/iPad View • Mobile View By default, desktop view is selected. **Note:** The device-specific view options are available across all portal

Table 110 *The Design screen parameters*

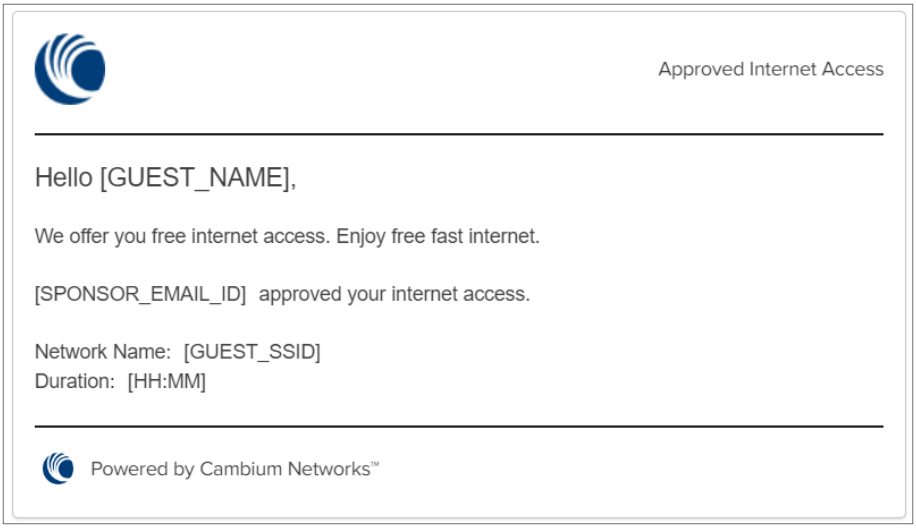
Parameter	Description
	types on their respective **Design** screens.
View in new tab and **Copy to clipboard** options of the design page	The following options are available across all portal types on their respective **Design** screens once you save the **Design** page. • View in new tab • Copy to clipboard
Collapse/Expand details panel	An option to collapse or expand the details panel.
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:	

Table 110 *The Design screen parameters*

Parameter	Description
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. Enter the payment code.
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 111 displays the **Voucher** screen parameters that appear across **Voucher**, **One Click** + **Voucher**, and **Voucher** + **Paid X** portal types on their respective **Voucher** screens.

Table 111 *The Voucher screen parameters*

Parameter	Description
Voucher Plan Name	Name of the voucher plan. **Note**: This parameter supports: • A minimum of one and maximum of 64 characters. • Only alphanumeric, underscore (_), and dashes (-). This parameter is mandatory.
Quantity	Quantity (in integers) of the voucher. Minimum value: 1 Maximum value: 2000
Voucher Message	Message for the voucher. This parameter supports a minimum of one and maximum of 128 characters.

Table 111 *The Voucher screen parameters*

Parameter	Description
Session Expiry	For information on this parameter, see Table 109.
Voucher Expiry	The expiry time of the voucher. The following options are supported: • 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 109.
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 379 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 379 *The One Click screen*

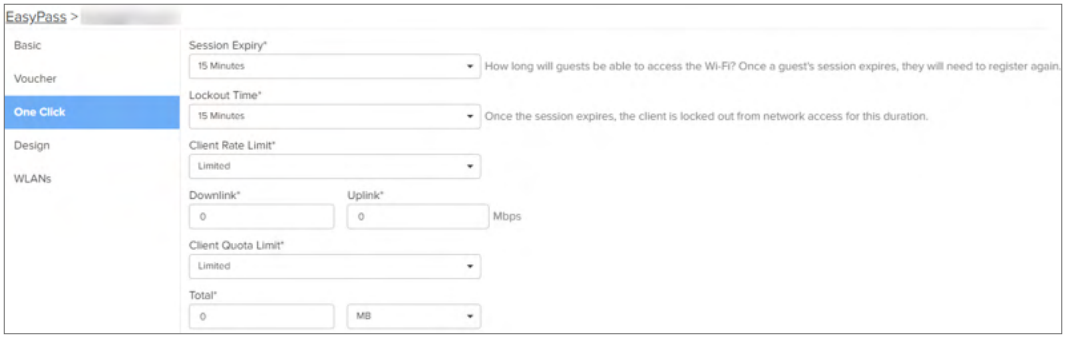


Table 109 describes the parameters that appear only for **One Click** + **Voucher** or **One Click** + **Paid X** portal types on the respective **One Click** screens.

Table 112 *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: • 15 Minutes • 1 Hour • 1 Day • 1 Month • End of Day (Midnight) • End of week (Saturday) • Custom By default, **15 Minutes** is selected. Select the required option from the dropdown list.
Lockout Time	The lockout time restricts the ability to create a new session for the specified duration when a session expires. The following options are supported: • None • 15 Minutes • 1 Hour • 1 Day • 1 Month • End of Day (Midnight) • End of week (Saturday) • Custom By default, **None** is selected. Select the required option from the dropdown list.

Table 112 *The Limits screen parameters*

Parameter	Description
Client Rate Limit	Indicates the client rate limit. The following options are supported: • Limited—When the **Limited** option is selected, the **Downlink** and **Uplink** parameters appear. • Unlimited By default, **Unlimited** is selected.
Downlink	This parameter is applicable only when **Client Rate Limit** is set to **Limited**. Downlink of client rate limit in Kbps. Maximum value: 1000000
Uplink	This parameter is applicable only when **Client Rate Limit** is set to **Limited**. Uplink of client rate limit in Kbps. Maximum value: 1000000
Client Quota Limit	Indicates the client quota limit. The following options are supported: • Limited—When the **Limited** option is selected, the **Total** parameter appears. • Unlimited By default, **Unlimited** is selected.
Total	The total client quota in MB or GB. You can either select **MB** or **GB** option from the dropdown list. By default, **MB** option is selected. **Note**: This parameter supports: • A minimum of 1 MB and a maximum of 8000000 MB. • A minimum of 1 GB and a maximum of 8000 GB.

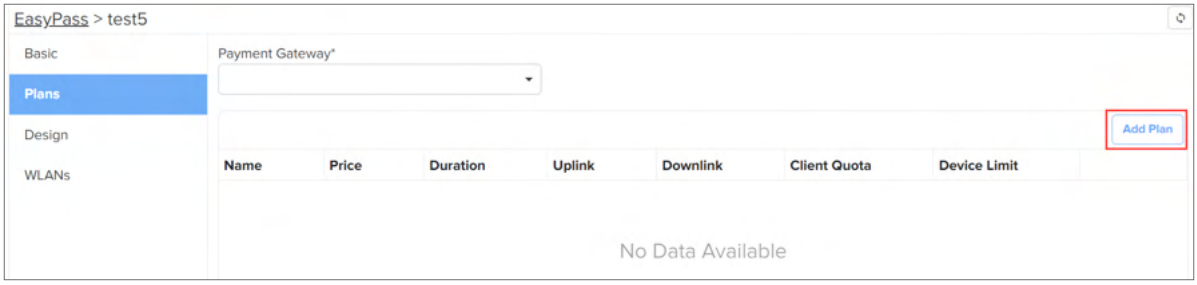
Note

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 380 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 380 *The Plans screen*



> **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 380).

   The **Add New Plan** window appears.

   Figure 381 *The Add New Plan window*

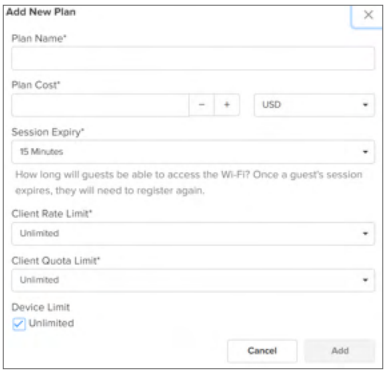


   Table 113 describes the common **Plans** screen parameters that appear across **Paid X**, **One Click + Paid X**, and **Voucher + Paid X** portal types on their respective **Plans** screens.

   Table 113 *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 109.
Client Rate Limit	
Downlink	
Uplink	
Client Quota Limit	
Total	
Device Limit	
Unlimited	Enable or disable the parameter.

Table 113 *The Add New Plan window parameters*

Parameter	Description
	If you disable the checkbox, you must specify the device limit. If you enable the checkbox, you can connect unlimited number of devices.

2. Click **Add** (as shown in Figure 381).

   The plan is added.

   Figure 382 *Plan added*

> **Note**
>
> Use the edit ( ) icon to modify a plan.

3. Select the required payment gateway option from the **Payment Gateway** dropdown list (as shown in Figure 383) and configure corresponding parameters as described in the following sections..

   Figure 383 *Payment gateway options*

   The following options are supported:

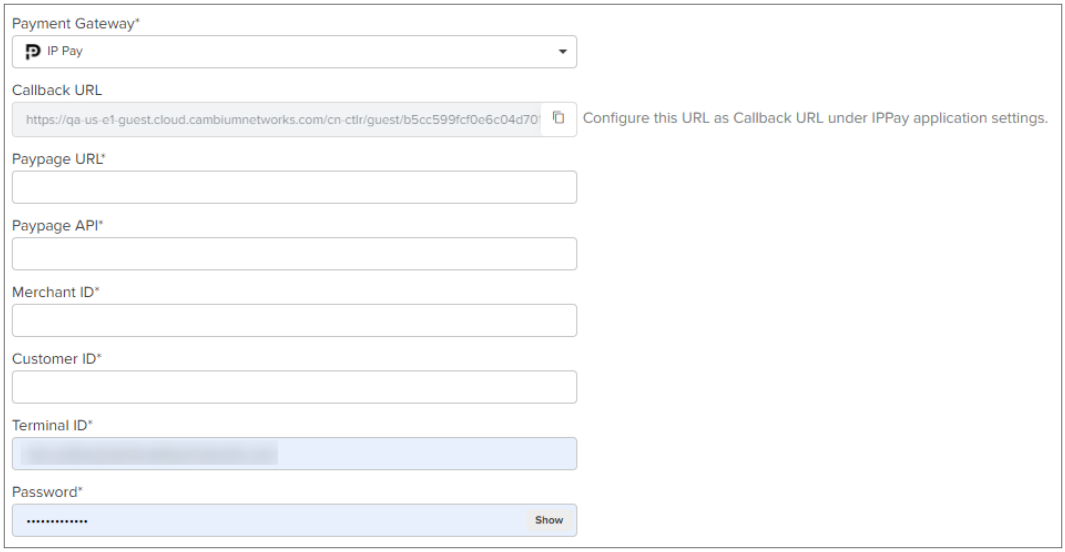
   - IP Pay
   - Quickpay
   - PayPal

> **Note**
>
> Set the mandatory fields for the selected payment gateway options.

IP Pay

Figure 384 displays the parameters available for the **IP Pay** payment gateway.

Figure 384 *IP Pay payment gateway*



Configure the IP Pay parameters described in Table 114.

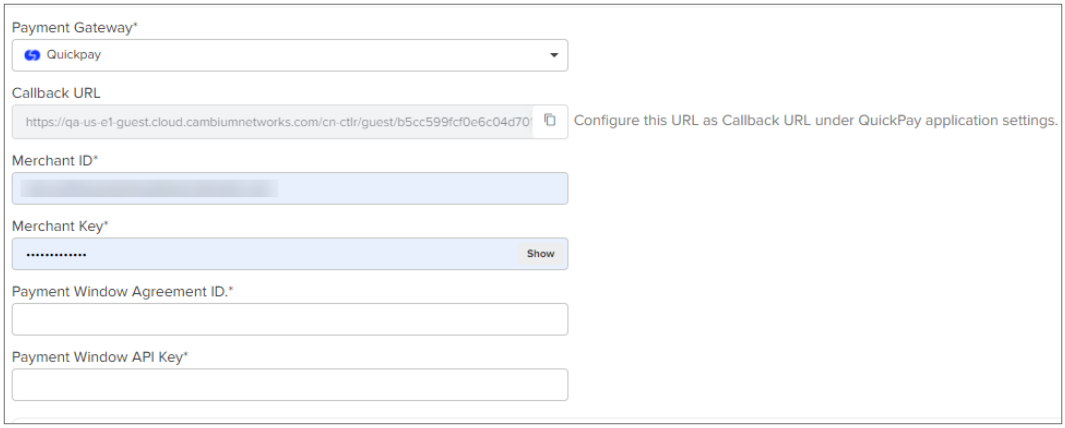
Table 114 *IP Pay parameters description*

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 385 displays the parameters available for the **Quickpay** payment gateway.

Figure 385 *Quickpay payment gateway*



Configure the Quickpay parameters described in Table 115.

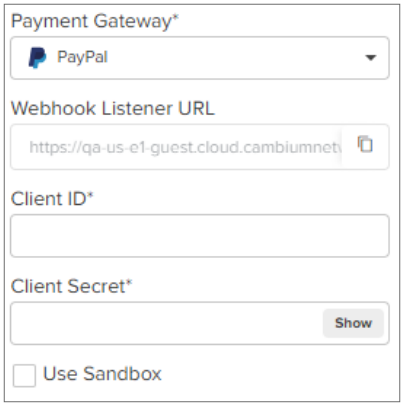
Table 115 *Quickpay parameters description*

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 386 displays the PayPal payment gateway screen.

Figure 386 *PayPal payment gateway*



Configure the PayPal parameters described in Table 115.

Table 116 *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

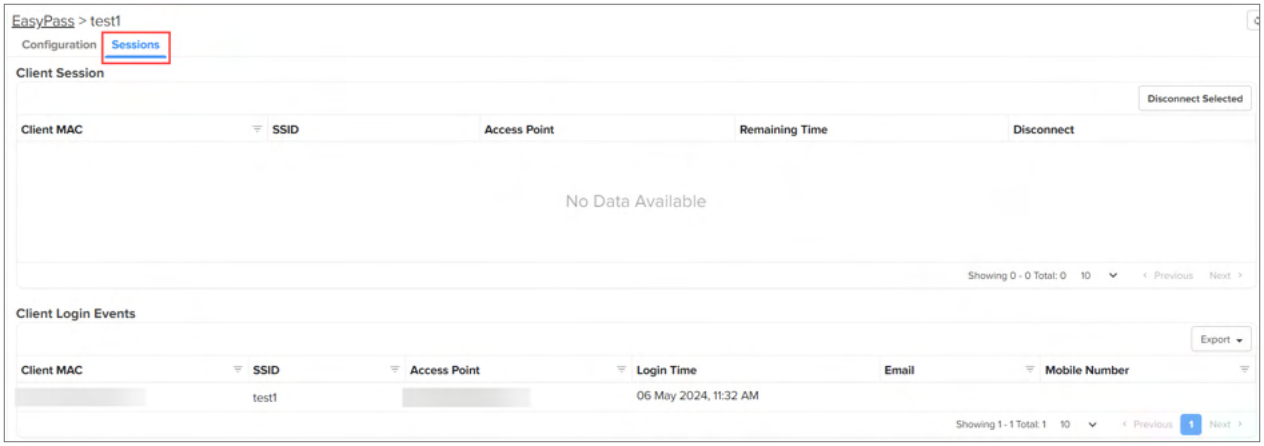
The following common tabs are available for various portal types in EasyPass:

- Sessions
- Guests
  - Adding a new guest user
- Vouchers
  - EasyPass
- Paid Transactions X
- EasyPass

Sessions

You can access the **Sessions** page using the **Sessions** tab from, as shown in Figure 387, from any of the portals.

Figure 387 *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:

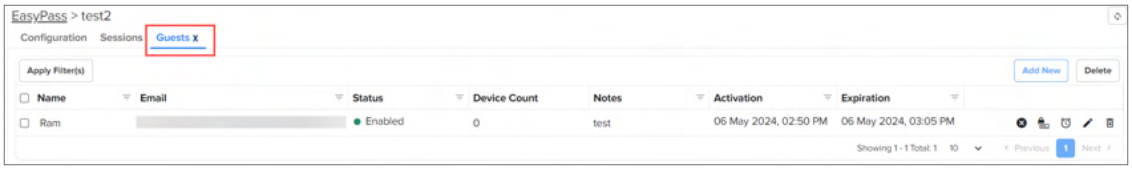
- Export page as CSV
- Export all as CSV

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 388).

Figure 388 *The Guests page*



Note

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

Adding a new guest user

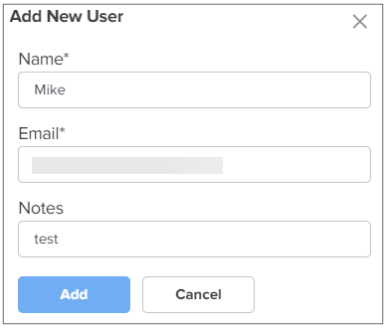
You can also add a new guest user from the **Guests** page.

Complete the following steps to add a new user:

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

   The **Add New User** window appears.

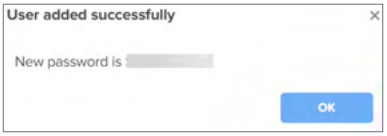
   Figure 389 *The Add New User window*

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 390).

   Figure 390 *The User added successfully window*

6. Click **OK**.

   A new guest user is added (as shown in Figure 391).

   Figure 391 *The new guest user details*

   You can view the details of the self registered guest connected to the Wi-Fi network (as shown in Figure 391).

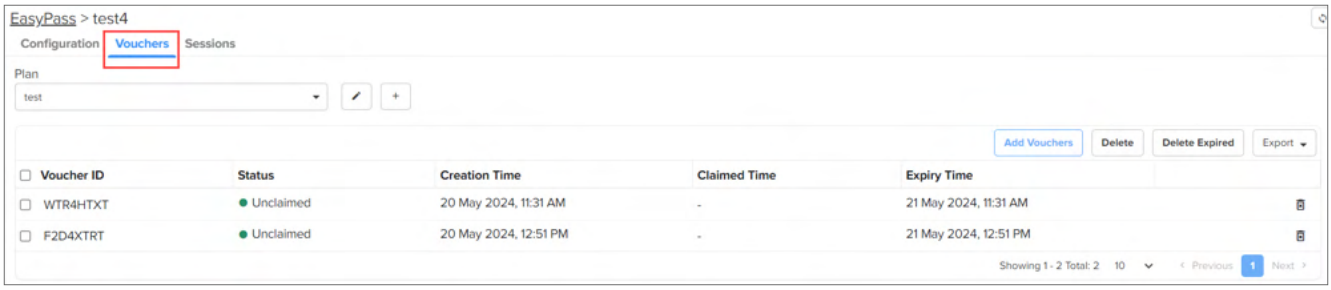
   - Use the disable access ( ) icon to disable access.
   - Use the reset password ( ) icon to reset a password.
   - Use the extend session ( ) icon to extend a session.
   - Use the edit ( ) icon to edit the user details.
   - Use the delete ( ) icon to delete a user.

Vouchers

You can access the **Vouchers** page using the **Vouchers** tab (as shown in Figure 392).

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 392 *The Vouchers tab*



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.

Note

Operator users can perform the following actions:

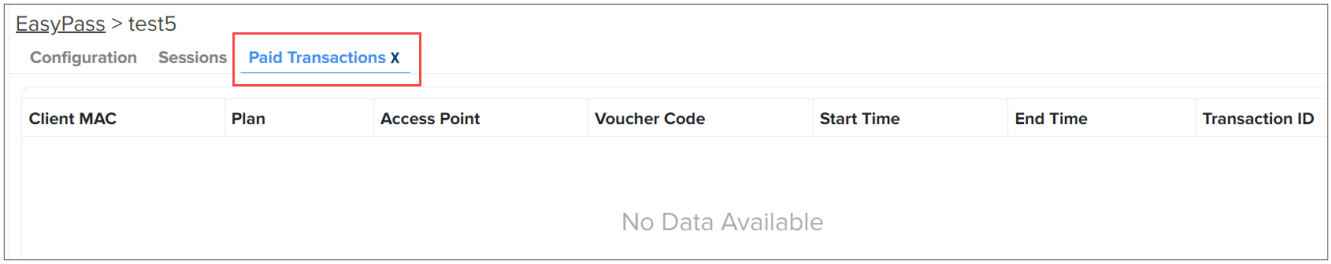
- Add new vouchers
- Delete the existing or expired vouchers
- Export voucher data
- View session details
- Disconnect users at the session-level

However, designing the vouchers and editing the voucher plans can be performed only by Super Administrator users.

Paid Transactions X

You can access the **Paid Transactions X** page using the **Paid Transactions X** tab (as shown in Figure 393).

Figure 393 *The Paid Transactions X tab*



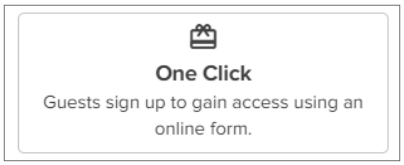
Note

The **Paid Transactions X** tab appears only for the **Paid X, One Click + Paid,** and **Voucher + Paid 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 394 *The One Click option*



Note

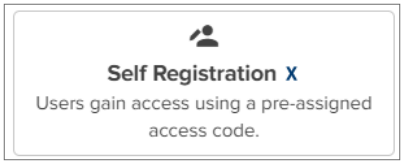
To create a One Click portal, complete the initial steps described in Creating a portal and continue with the next steps to configure the parameters of the **Basic** screen, **Limits** screen, **Design** screen, and **WLANs** screen.

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 395 *The Self Registration X option*



Note

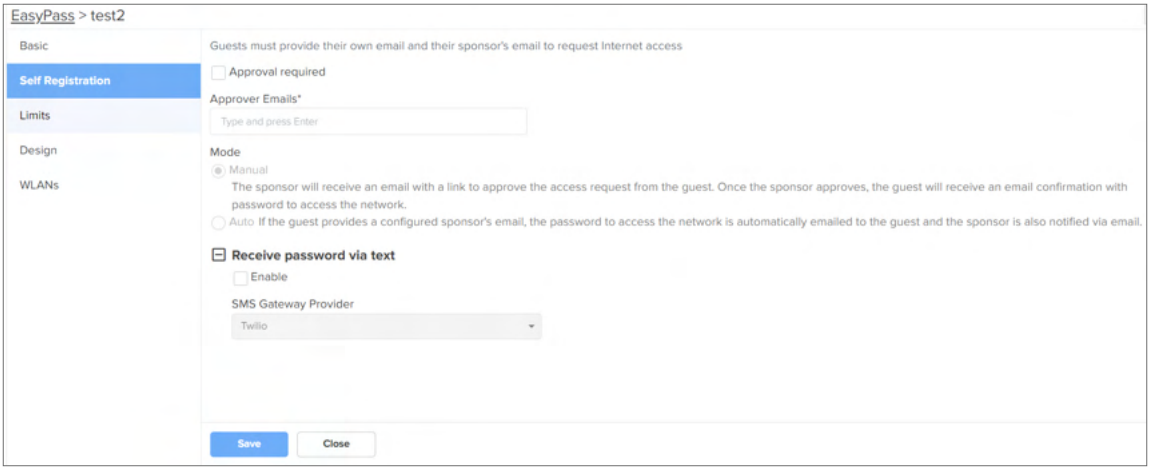
To create a Self Registration X portal, complete the initial steps described in Creating a portal and continue with the next steps to configure the parameters of the **Basic** screen, **Self Registration** screen, **Limits** screen, **Design** screen, and **WLANs** screen.

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

1. Click the **Self Registration** tab.

   The **Self Registration** screen appears.

Figure 396 *The Self Registration screen*



2. Configure the parameters described in Table 117.

Table 117 *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. This parameter is mandatory.
Mode	This parameter is applicable when the **Approval required** checkbox is selected. The following options are supported: • 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	Select the **Enable** checkbox. This parameter is disabled by default. When you select the **Enable** checkbox, the **SMS Gateway Provider** option is enabled.
SMS Gateway Provider	Select the required SMS gateway option to be used to send the OTP to the guest's mobile device. By default, the **Twilio** option is selected. The following gateway options are supported:

Table 117 *The Self Registration screen parameters*

Parameter	Description
	• Fast SMS • Generic SMS API • SMS Country • SMS Gupshup • SMSAPI • Twilio • Victory Link SMS Each of these gateway options can be configured with their respective parameters. For more information on the gateway options, see **SMS Gateway Providers** section.

SMS Gateway Providers

This section describes the different types of SMS gateway providers.

Figure 397 displays the parameters available for the **Twilio** option.

Figure 397 *Twilio option*

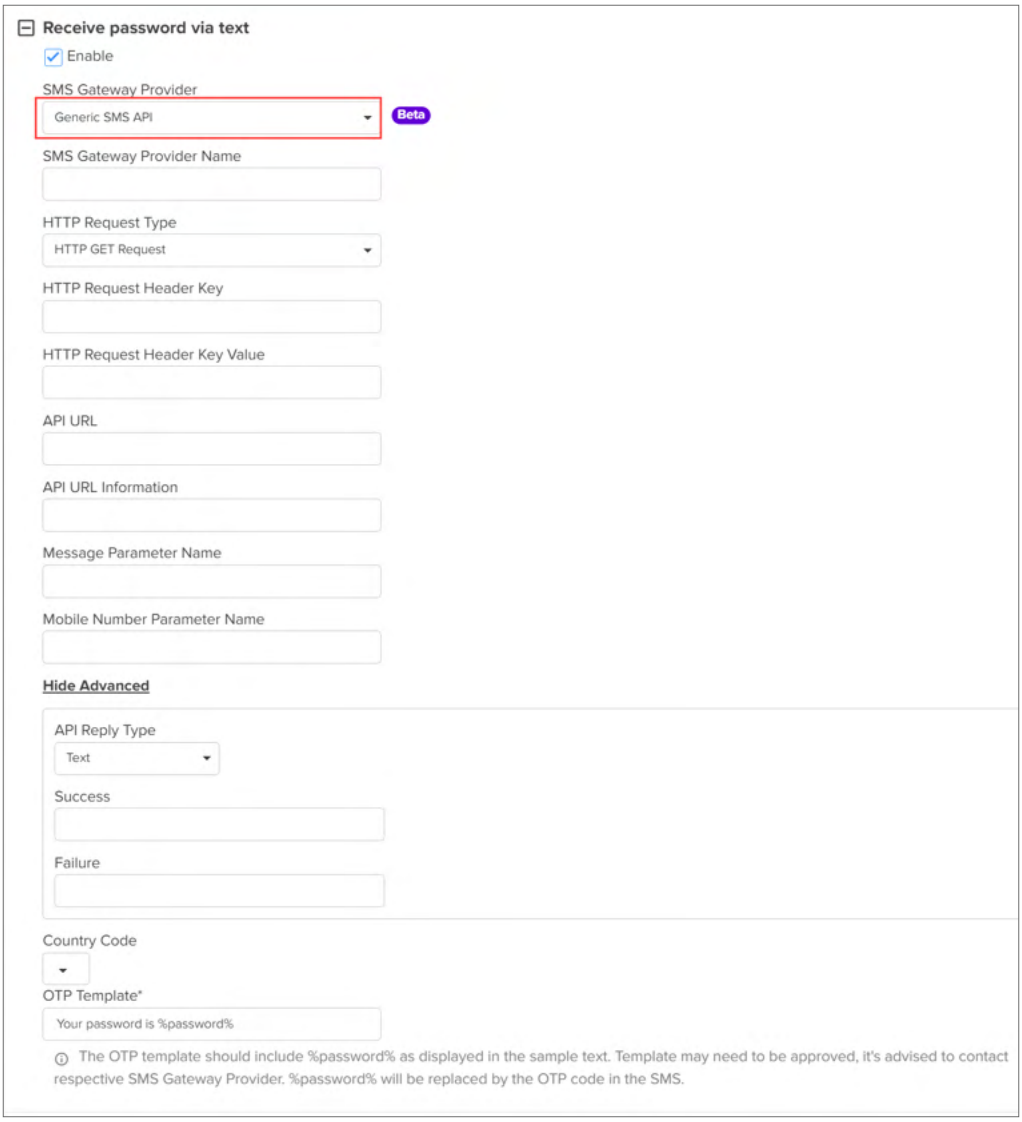
When you select the **Twilio** option, you must configure the parameters described in Table 118.

Table 118 *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 398 displays the parameters available for the **Generic SMS API** option.

Figure 398 *Generic SMS API option*



When you select the **Generic SMS API** option, you must configure the parameters described in Table 119.

Table 119 *Parameters of Generic SMS API*

Parameter	Description
SMS Gateway Provider Name	SMS gateway provider name. Enter a name for the SMS gateway provider. Enter the user name.
HTTP Request Type	HTTP request type. The following options are supported: • HTTP GET Request • HTTP POST Request

Table 119 *Parameters of Generic SMS API*

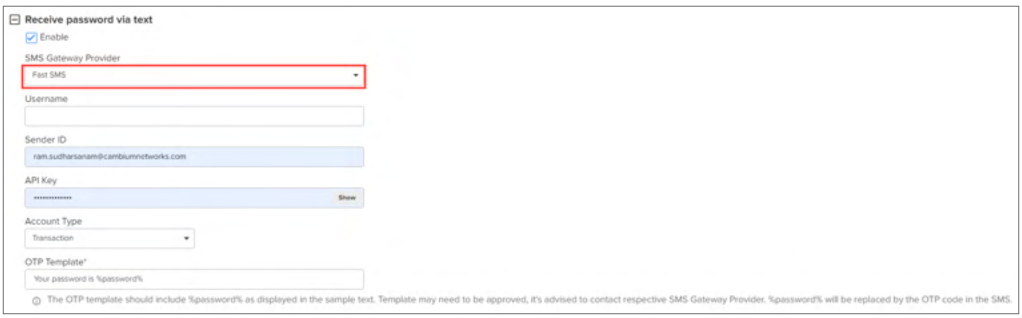
Parameter	Description
HTTP Request Header Key	HTTP request header key
HTTP Request Header Key Value	HTTP request header key value
API URL	API URL Enter the API URL.
API URL Information	API URL information. Enter the API URL information.
Message Parameter Name	Message parameter name. Enter the message 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: • 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.

Table 119 *Parameters of Generic SMS API*

Parameter	Description
XML Reply Success Element Value	XML reply success element value. Enter the reply success element value.
XML Reply Failure Element	XML reply failure element. Enter the XML reply failure element.
XMl 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 399 displays the parameters available for the **Fast SMS** option.

Figure 399 *Fast SMS option*



When you select the **Fast SMS** option, you must configure the parameters described in Table 120.

Table 120 *Parameters of Fast SMS*

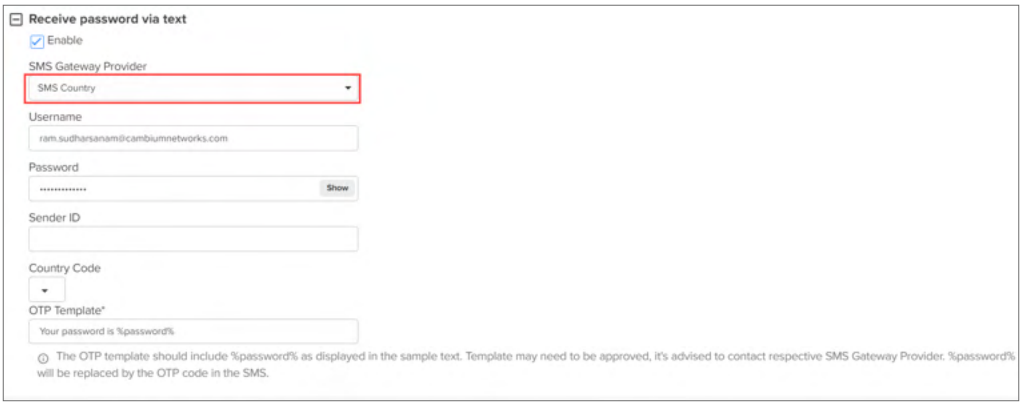
Parameter	Description
Username	User name. Enter the user name. This field is optional.
Note: The **Sender ID** and **API key** fields are populated, by default.	
Account Type	Account type. Select the required option from the dropdown list. The following options are supported: • Transaction • Promotional • International

Table 120 *Parameters of Fast SMS*

Parameter	Description
	• OTP • Other
OTP Template	OTP template. Enter the password in the **OTP Template** field. This parameter is mandatory.

Figure 400 displays the parameters available for the **SMS Country** option.

Figure 400 *SMS Country option*



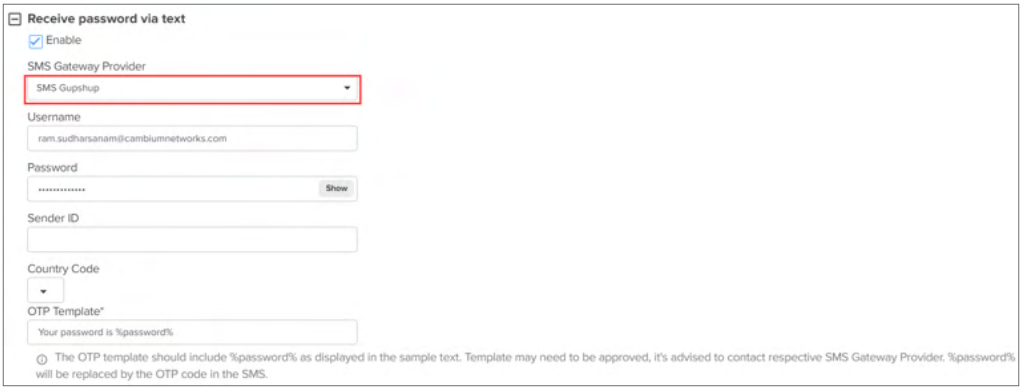
When you select the **SMS Country** option, you must configure the parameters described in Table 121.

Table 121 *Parameters of SMS Country*

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 401 displays the parameters available for the **SMS Gupshup** option.

Figure 401 *SMS Gupshup option*



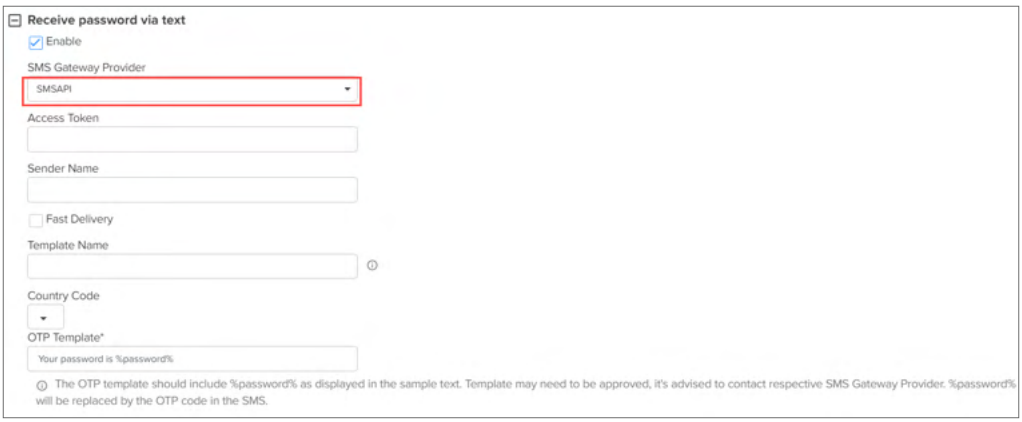
When you select the **SMS Gupshup** option, you must configure the parameters described in Table 122.

Table 122 *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 402 displays the parameters available for the **SMS API** option.

Figure 402 *SMS API option*



When you select the **SMS API** option, you must configure the parameters described in Table 123.

Table 123 *Parameters of SMS API*

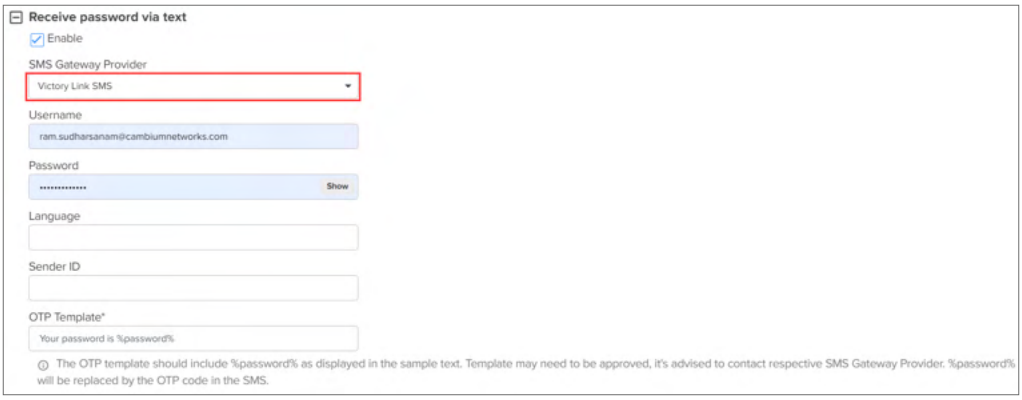
Parameter	Description
Note: The **Username** and **Password** fields are populated, by default.	

Table 123 *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 403 displays the parameters available for the **Victory Link SMS** option.

Figure 403 *Victory Link SMS option*



When you select the **Victory Link SMS** option, you must configure the parameters described in Table 124.

Table 124 *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.

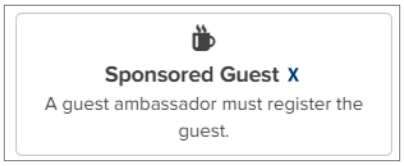
> **Note**
>
> After configuring the parameters in the Self-Registration window, continue to step 8 to configure the parameters in the **Limits**, **Design**, and **WLANs** screens.

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 404 *The Sponsored Guest X option*



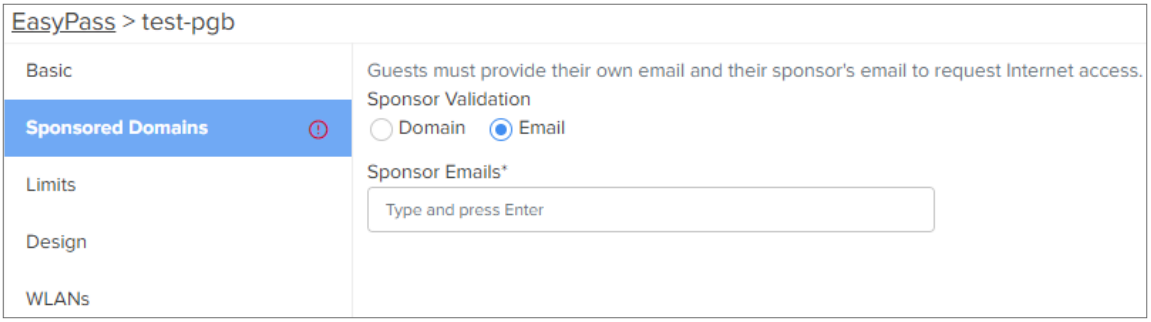
> **Note**
>
> To create a Sponsored Guest X portal, complete the initial steps described in Creating a portal and continue with the next steps to configure the parameters of the **Basic** screen, **Sponsored Domains** screen, **Limits** screen, **Design** screen, and **WLANs** screen.

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

1. Click the **Sponsored Domains** tab.

   The **Sponsored Domains** screen appears.

   Figure 405 *The Sponsored Domains screen*



2. Configure the parameters described in Table 125.

   Table 125 *The Sponsored Domains screen parameters*

Parameter	Description
Sponsor Validation	Type of validation to be used for this portal. The following options are available: • 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 125 *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

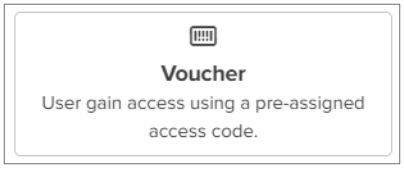
After configuring the parameters in the **Sponsored Domains** window, continue to step 8 to configure parameters in the **Limits**, **Design**, and **WLANs** screens.

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 406 *The Voucher option*



Note

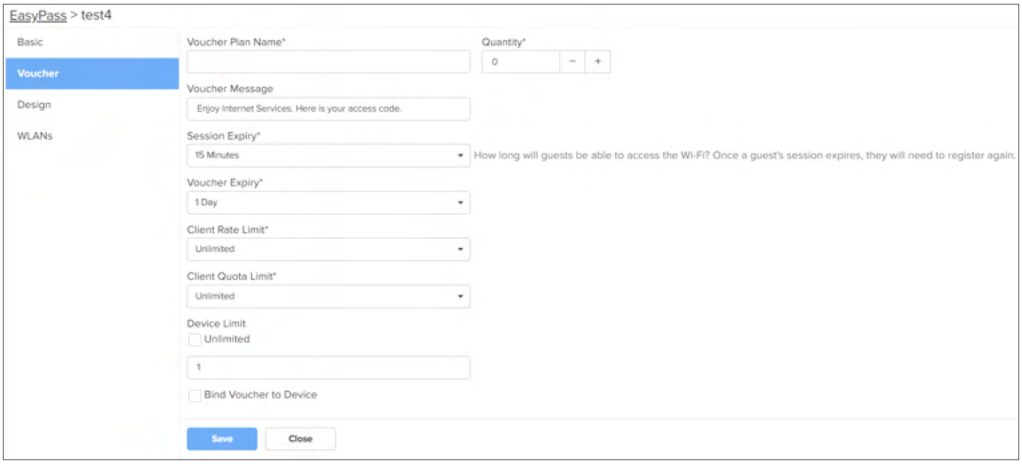
To create a Voucher portal, complete the initial steps described in Creating a portal and continue with the next steps to configure the parameters of the **Basic** screen, **Voucher** screen, **Design** screen, and **WLANs** screen.

Follow these additional steps to create a Voucher portal:

1. Click the **Voucher** tab.

   The **Voucher** screen appears.

Figure 407 *The Voucher screen*



2. Configure the parameters described in Table 111.

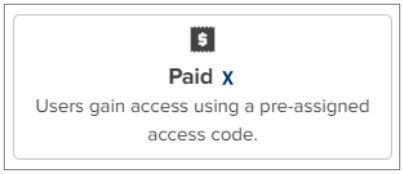
Note

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 408 *The Paid X option*



Note

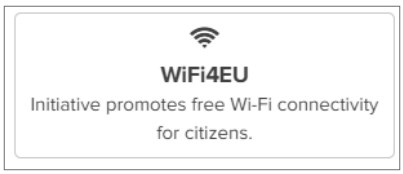
To create a Paid X portal, complete the initial steps described in Creating a portal and continue with the steps to configure the parameters of the **Basic** screen, **Plans** screen, **Design** screen, and **WLANs** screen.

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 409 *The WiFi4EU option*



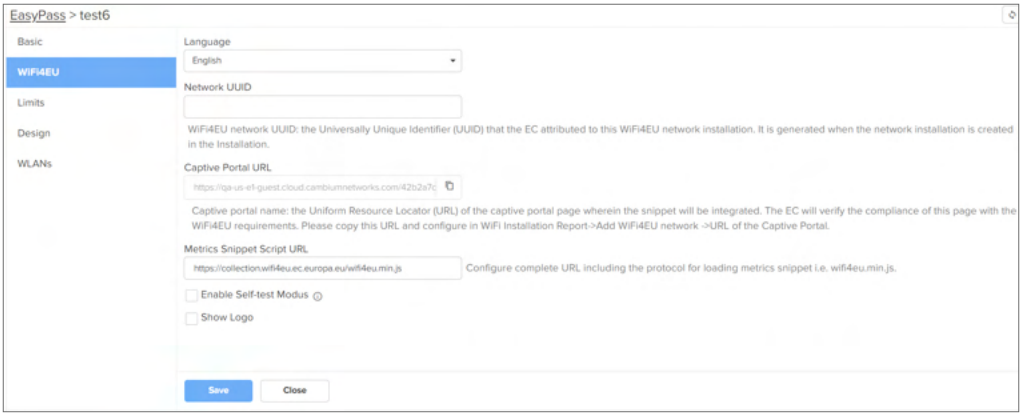
> **Note**
>
> To create a WiFi4EU portal, complete the initial steps described in Creating a portal and continue with the next steps to configure the parameters of the **Basic** screen, **WiFi4EU** screen, **Limits** screen, **Design** screen, and **WLANs** screen.

Follow these additional steps to create a WiFi4EU portal:

1. Click the **WiFi4EU** tab.

   The **WiFi4EU** screen appears.

   Figure 410 *General parameters*



2. Configure the parameters described in Table 126.

   Table 126 *General parameters - WiFi4EU*

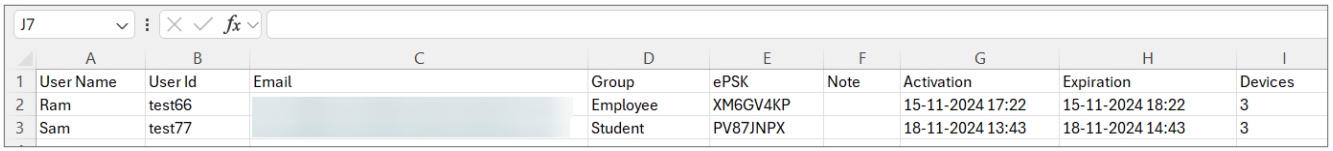
Parameter	Description
Language	Select the preferred language from the dropdown list.
Network UUID	Universally Unique Identifier (UUID) that the EC attributed to the WiFi4EU network installation.
Enable Self-test Modus	Allows the browsers background script verification.
Show Logo	Displays the WiFi4EU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

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 411 *List of users with their associated data*



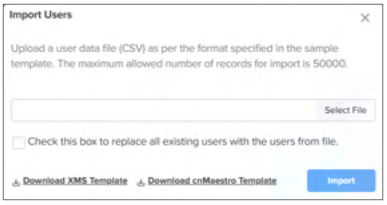
	A	B	C	D	E	F	G	H	I
1	User Name	User Id	Email	Group	ePSK	Note	Activation	Expiration	Devices
2	Ram	test66		Employee	XM6GV4KP		15-11-2024 17:22	15-11-2024 18:22	3
3	Sam	test77		Student	PV87JNPX		18-11-2024 13:43	18-11-2024 14:43	3

Complete the following steps to import user data using a CSV file:

1. Click the **Import** button (as shown in).

   The **Import Users** page appears.

   Figure 412 *The Import Users page*



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 413 *Confirmation dialog box to regenerate ePSKs for selected users*

  When you click **Yes** (as shown in Figure 413), 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 414 *Confirmation dialog box to send ePSKs for selected users*

When you click **Yes** (as shown in Figure 414), ePSKs are sent for selected users.

- Click the **Extend session** button to extend a session for selected users.

  A confirmation dialog box appears.

  Figure 415 *Confirmation dialog box to extend session for selected users*

  When you click **Yes** (as shown in Figure 415), the session is extended for selected users.

  You can also use the Extend session ( ) icon to extend the session for a selected user.

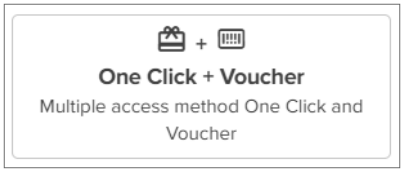
> **Note**
>
> The session is extended based on the **Session Expiry** duration set in the **Limits** screen.

- 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 416 *The One Click + Voucher option*



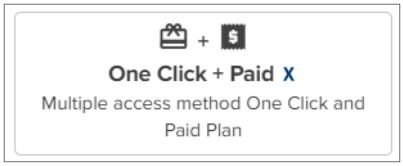
> **Note**
>
> To create a One Click + Voucher portal, complete the initial steps described in Creating a portal and continue with the next steps to configure the parameters of the **Basic** screen, **Voucher** screen, **One Click** screen, **Design** screen, and **WLANs** screen.

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 417 *The One Click + Paid X option*



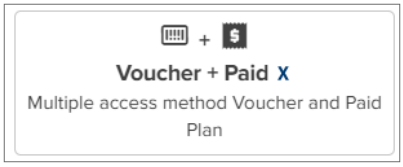
> **Note**
>
> To create a One Click + Paid X portal, complete the initial steps described in Creating a portal and continue with the next steps to configure the parameters of the **Basic** screen, **Plans** screen, **One Click** screen, **Design** screen, and **WLANs** screen.

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 418 *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.

Creating a Third-Party Integration portal

The EasyPass **Third-party Integration** portal type allows partners to integrate their external captive portals with cnMaestro by posting authentication and logout requests directly to cnMaestro. To enable secure and region-specific communication, each **Third-Party Integration** portal provides a unique base URL (which may differ by account and region) and a secret key for authentication. These credentials allow the third-party application to securely interact with the captive portal integration APIs.

The following API endpoints are supported:

- **Login**—Allows an external captive portal to authenticate a user and grant network access through a Cambium AP.
- **Logout—**Allows the external captive portal to disconnect a user from the network.

To use these integration APIs, the external captive portal must authenticate every request using a secret key and the base URL provided in the EasyPass **Third-Party Integration** portal within cnMaestro. cnMaestro will validate

the secret key and grant access to the requested resource if authentication is successful. If the Base URL is incorrect, or if the secret key is missing, invalid, or expired, the request is rejected with an authentication error.

Note

When configuring third-party integration EasyPass portal, you must enable the following option in cnMaestro **Wi-Fi Profiles** > **WLANs** > **Guest Access** page > **Basic Settings** tab> **External Hotspot**.

- **External Portal Post Through cnMaestro**—This option enables the EasyPass portal to correctly route the guest access requests through cnMaestro.

This section provides details on the following topics:

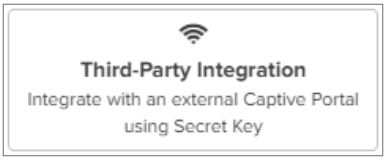
- Creating a portal and secret key
- Revoking and generating the secret key
- Using the Secret Key in API Requests

Creating a portal and secret key

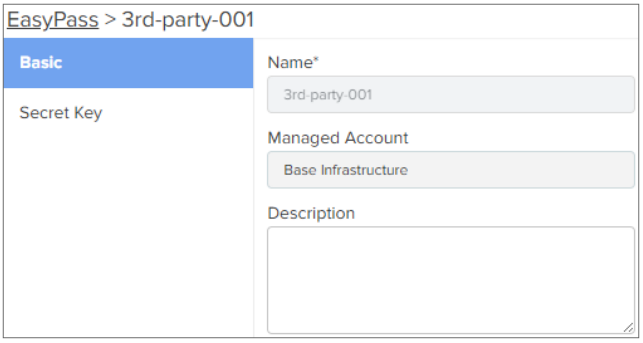
This section is targeted at the cnMaestro administrator to create the EasyPass Third-Party Integration portal, generate the integration Base URL and secret keys, and deliver them to the captive portal developer partner.

Complete the following steps:

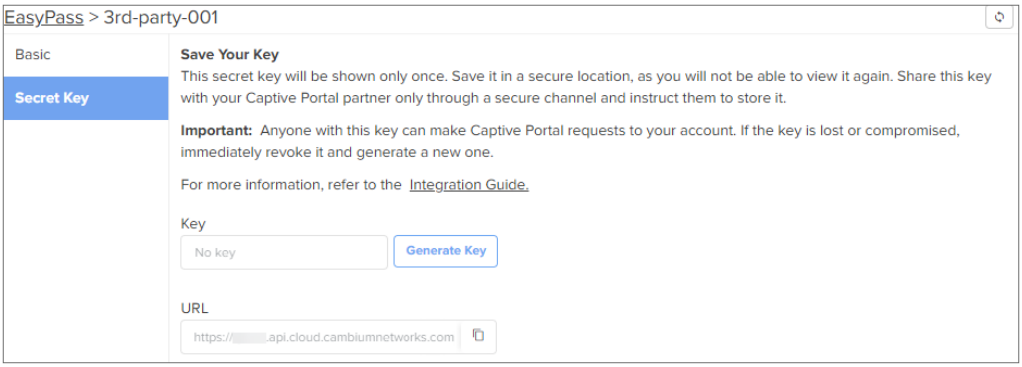
1. From the cnMaestro home page, navigate to **Network Services** > **EasyPass**.
2. Click **Add Portal** and select **Third-Party Integration** as the portal type.



3. Click **Save** and **Continue**.



4. Inside the portal, select the **Secret Key** tab.



5. Copy the base URL from the **URL** field.

   The URL for API requests is always visible on this page and is unique to your portal and region.

6. To generate the secret key, click **Generate Key**.

   A successful key generation message is displayed and the secret key is displayed in the **Key** field.

> **Note**
>
> The secret key is displayed only at the time of generation. Cambium recommends that you immediately copy and store the key securely. If you navigate away from the **Secret Key** page, you will be unable to retrieve the key.

7. Click **Save**.
8. Communicate the secret key and base URL to your external captive portal developer partner in a secure way.

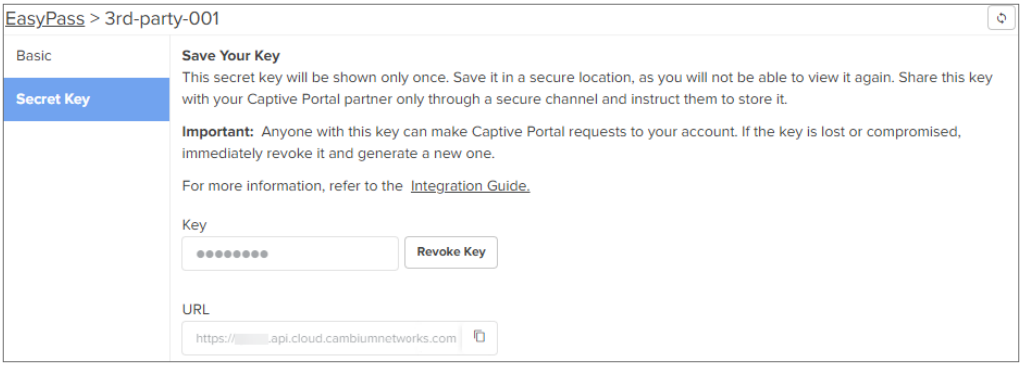
Revoking and generating the secret key

This section is targeted at both the cnMaestro admin and the Captive Portal developer partner.

If you believe that your secret key is compromised or has been misplaced, you can revoke the existing key and generate a new key.

To revoke and generate a new key:

1. On the **Secret Key** page, first click **Revoke Key**, to revoke the existing key.



2. Click **Generate Key** to generate a new secret key.

   Copy and store the new secret key.

Using the Secret Key in API Requests

For information on how to use the integration APIs, secret key and base URL, refer to the cnMaestro External Captive Portal Integration Guide on the Cambium Support site.

SNMP Configuration X

This chapter provides the following information:

- Overview
- Enable SNMP
- Configure SNMP parameters
- cnMaestro MIB (Management Information Base)

Overview

cnMaestro supports SNMPv2c for basic monitoring and traps.

Note

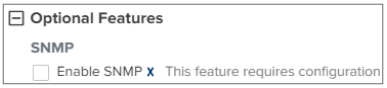
SNMP uses UDP port 161 for GET requests and UDP port 162 for TRAPs.

Enable SNMP

To enable SNMPv2c, perform the following:

1. Navigate to **Administration** > **Settings** > **Optional Features.**
2. Enable **SNMP management.**

Figure 419 *Enable SNMP*



Enabling SNMP turns on the functionality within the UI; however, the server does not start until the SNMP configuration is completed.

Note

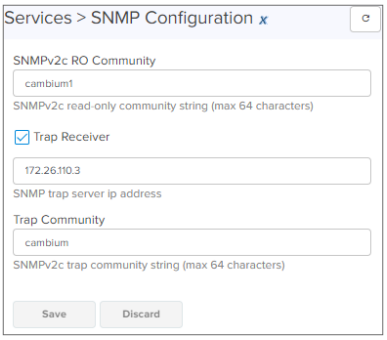
SNMP services do not start until a valid configuration exists.

Configure SNMP parameters

To configure SNMP parameters, perform the following:

1. Navigate to **Services > SNMP Configuration** (this tab is only visible if SNMP is enabled).

   Figure 420 *Configure SNMP*

2. Enter the **SNMPv2c RO Community String** name (maximum limit is 64 characters).
3. Enable the **Trap Receiver** checkbox and enter the IP Address.

   Note

   You can configure the desired Trap Community string in the cnMaestro **SNMP configuration** page.

4. Enter the **SNMPv2c Trap Community** string name (maximum limit is 64 characters).
5. Click **Save**.

   Note

   If there are thousands of devices in your cnMaestro account, you should set your **MIB** browser or `snmpget` command to use a minimum timeout of 20 minutes.

cnMaestro MIB (Management Information Base)

The cnMaestro MIB can be downloaded from Cambium Support Center.

By default, the following OIDs are available when SNMPv2 is enabled in cnMaestro:

- .1.3.6.1.2.1 (mib-2)
- .1.3.6.1.4.1.2021 (UCD)
- .1.3.6.1.6.3.1.1 (snmpV2 - snmpMIB)
- .1.3.6.1.6.3.1.2 (snmpV2 - snmpMIBConformance)
- .1.3.6.1.4.1.17713.23 (CAMBIUM - cnMaestro)

RADIUS Proxy

Note

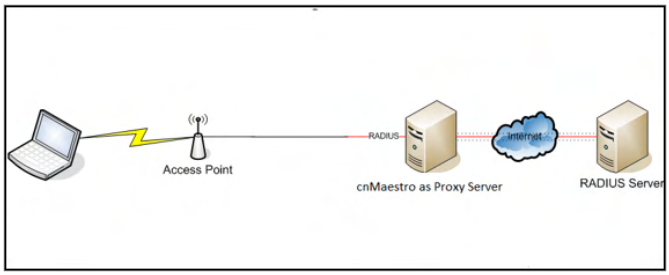
- RADIUS Proxy is not supported on cnMaestro Cloud.

Overview

cnMaestro can act as a proxy server to authenticate RADIUS requests for cnPilot Wi-Fi devices. In this scenario, cnMaestro acts as a Network Access Server (NAS) for the RADIUS server.

The APs send RADIUS packets to cnMaestro, and cnMaestro, in turn, forwards them to the RADIUS server. cnMaestro can act as a proxy for either authentication or accounting messages, as show in Figure 421.

Figure 421 *RADIUS Proxy on cnMaestro On-Premises*



Minimum version requirements are as follows:

- Minimum cnPilot AP release version supported is 3.3.

RADIUS Proxy Configuration

To configure RADIUS Proxy on cnMaestro, complete the following steps:

1. Navigate to **Shared Settings** > **Wi-Fi Profiles** > **WLANs** page.
2. Click **Add** to create a new WLAN.

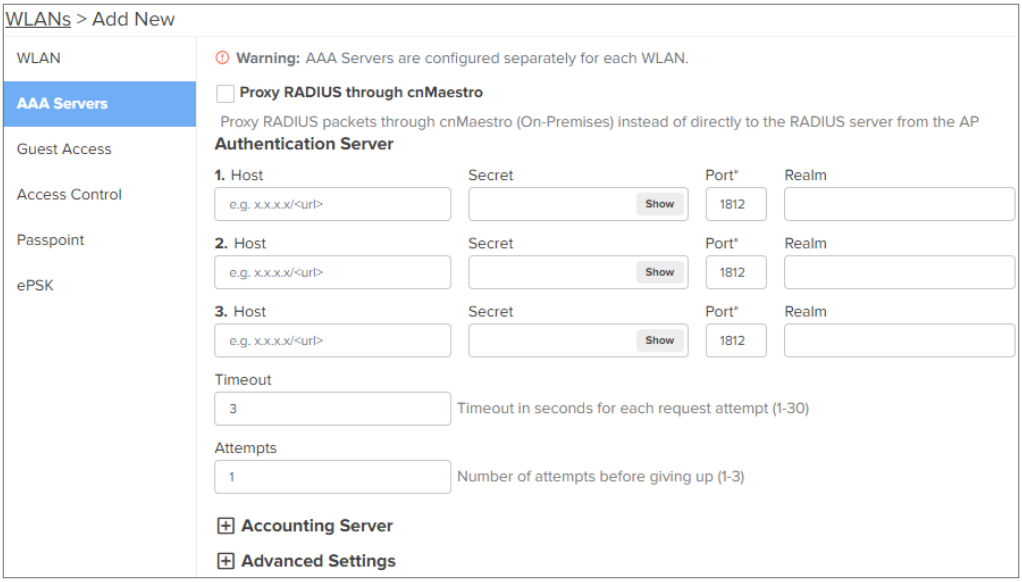
   OR

   Click an existing WLAN from the table to edit (or click the edit (✎) icon).
3. Click the **AAA Servers** section on the left navigation menu.
4. Select the **Proxy RADIUS through cnMaestro** checkbox.
5. Configure **Authentication Server** details.
6. Configure **Accounting Server** details.
7. Configure **NAS-Identifier**.

   Note

   Include **NAS-Identifier** attribute to use the RADIUS request packets and default the system name.
8. Push the configuration from cnMaestro to AP.

Figure 422 *RADIUS Proxy Configuration*



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).

Note

Users must have a cnMaestro Cloud Anchor account prior to enabling CBRS services in On-Premises.

This topic describes the following sections:

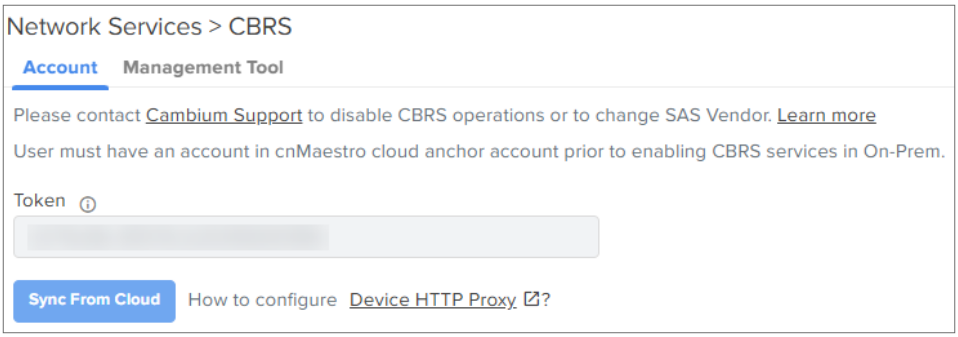
- Enabling CBRS in On-Premises
- Share CBRS configuration to the On-Premises Instance
- Management Tool
- Domain Proxy View

Enabling CBRS in On-Premises

Perform the following to enable CBRS:

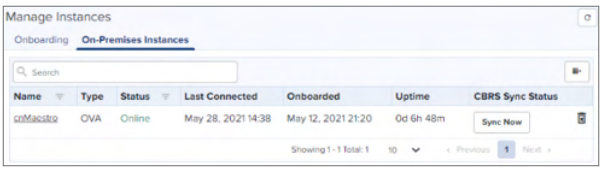
1. On successful activation of the CBRS service in the Cloud Anchor account, cnMaestro generates a Token.
2. Onboard the On-Premises instance to the Anchor account.
3. User can synchronize the CBRS token from the On-Premises or Anchor account.
    a. In the On-Premises instance, navigate to **Network Services** > **CBRS** > **Account** page, click **Sync From Cloud** to synchronize the CBRS token.

The token is synched from the Cloud instance and CBRS is enabled.



> **Note**
>
> To disable CBRS or to edit the SAS vendor, contact Cambium Support team.

b. Navigate to the **Anchor Account** > **Manage Instances** > **On-Premises Instances** and click **Sync Now** on CBRS sync status.



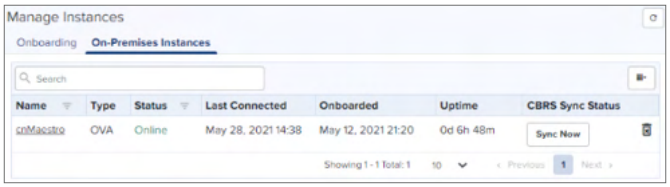
c. You must configure an HTTP proxy to access CBRS-related services.

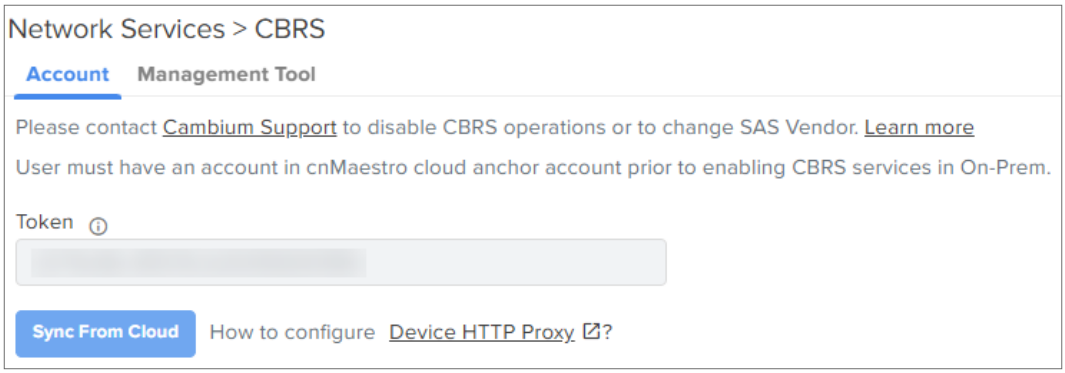
For information, see Configuring HTTP Proxy Server for CBRS and AFC Connectivity.

Share CBRS configuration to the On-Premises Instance

> **Note**
>
> From version 3.0.3, cnMaestro supports Synchronize CBRS Configuration to On-Premises instance.

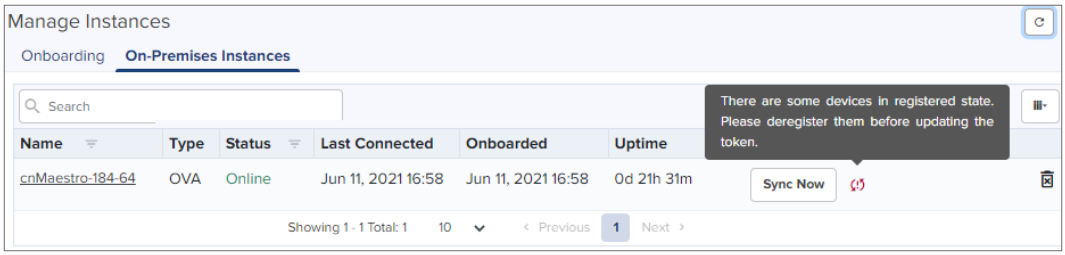
Once On-Premises is connected to the Anchor Account, the user can synchronize CBRS details (SAS ID, Token) to the cnMaestro On-Premises instance to register CBRS devices.





If the user shares (synchronizes) the CBRS details that are configured on the Anchor account with the connected On-Premises instance, and if any devices are registered in On-Premises with a different CBRS token or SAS ID, then it displays the deregister error as shown in Figure 423. The deregister and synchronize error message will be displayed in On-Premises account also.

Figure 423 *Deregister error*



Management Tool

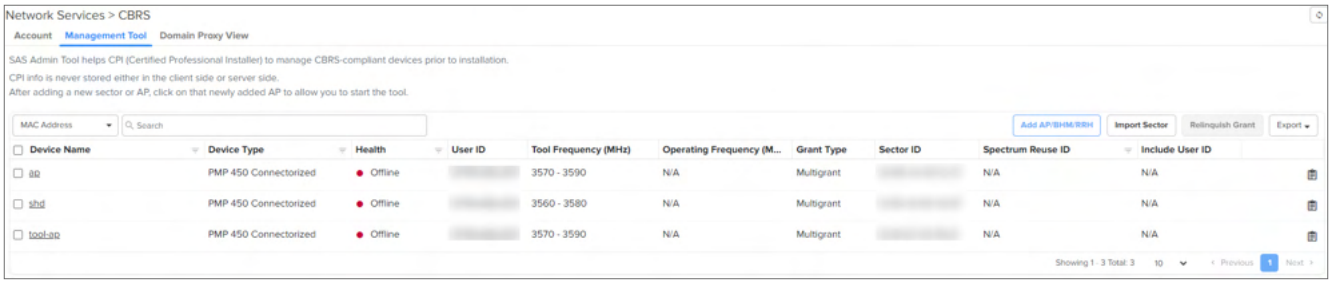
The Management Tool allows one to register CBRS devices to the SAS provider before physically connecting CBRS-complaint devices to the network. The following Cambium CBRS-compliant devices operate in 3.6 GHz band frequency, ranging from 3550 to 3700 MHz:

> **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

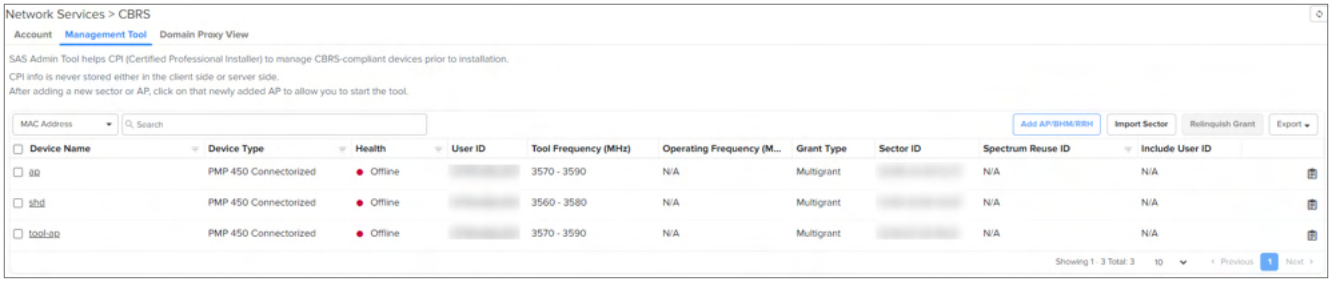
The CBRS procedure can be performed by an authorized CPI (Certified Professional Installer). CPIs are required to enter necessary credentials to update the CBRS parameters.

A CBRS sector view is shown below:



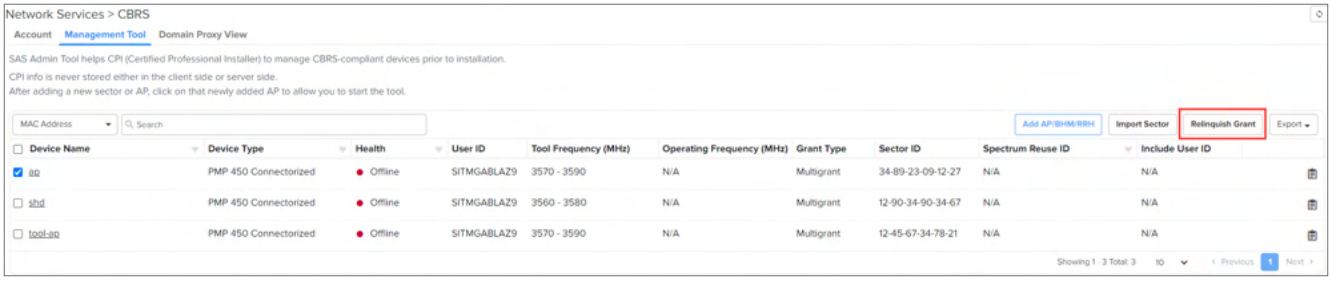
Export

The **Export** button allows one to export multiple device reports in the **CSV** format.



Relinquish Grant

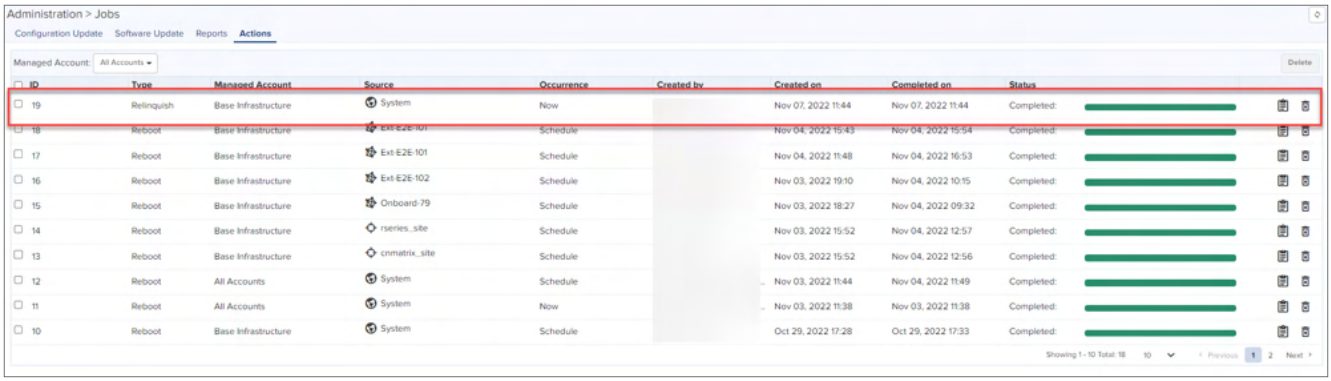
The Relinquish Grant button relinquishes all grants of selected sector and places devices in the Registered state. The device will start the Multi-Grant procedure if the Multi-Grant feature is enabled on the device.



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.



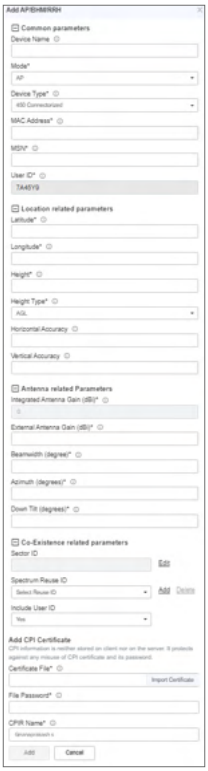
Creating a Management Tool Sector

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

1. Navigate to **Services** > **CBRS** > **Management Tools** and click **Add AP/BHM/RRH**.
2. 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.
   - **Add CPI Certificate**: Certificate File, File Password, CPIR Name.

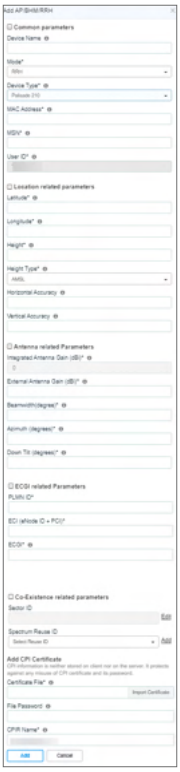


3. Click **Add** to add a sector.

Add RRH

1. Navigate to **Services** > **CBRS** > **Management Tools** and click **Add AP/BHM/RRH.**
2. Enter all parameters under the following categories when the user selects the **Mode** as **RRH**:

- **Common Parameters**: Device Name, Mode, Device Type, MAC Address, and MSN.
- **Location Related Parameters:** Latitude, Longitude, Height and Height Type, Horizontal Accuracy, and Vertical Accuracy.
- **Antenna Related Parameters**: External Antenna Gain, Beamwidth, Azimuth, and Down Tilt.
- **ECGI Related Parameters**: PLMN ID, ECI (eNode ID + PCI), and ECGI.
- **Co-Existence Related Parameters:** Sector ID and Spectrum Reuse ID.
- **Add CPI Certificate**: Certificate File, File Password, CPIR Name.



3. Click **Add** to add a sector.

> **Note**
>
> Refer to CBRS Device Parameters for additional details.

Import Management Tool Sector

To import a sector:

1. Navigate to **Services** > **CBRS** > **Management Tool** and click **Import Sector** button.

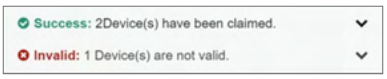
1. Click **Download Template** if user does not have an Import Sector template. Users can download two different template formats:
   a. PMP: Excel or ODS
   b. LTE: Excel or ODS
2. Click **Import Excel** to select **Import Sector** template file. File must be Microsoft Excel format (.xlsx) or OpenDocument Spreadsheet (ods) format.
3. Enter CPI credentials:
   a. Upload CPI Certificate File by clicking **Import Certificate**.
   b. Enter CPI File Password.
   c. Enter CPI Registered Name.
4. Enter the **Sector ID.**
5. Select **Spectrum Reuse ID** from the 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.

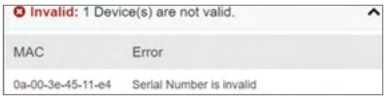
   Note
   - **Include User ID** is applicable only for PMP devices, when SAS is selected as **Federated Wireless**.
   - See the CBRS Consolidated Procedures Guide and the Cambium PMP Release 20.3 training slides for more details on when to select **Yes** or **No.**

7. Click **Import.**

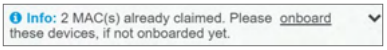
   Import status is displayed as **Success, Info**, and **Invalid**.



8. Details of **Success**, **Info,** and **Invalid** section can be seen by clicking expand ( ) arrow.



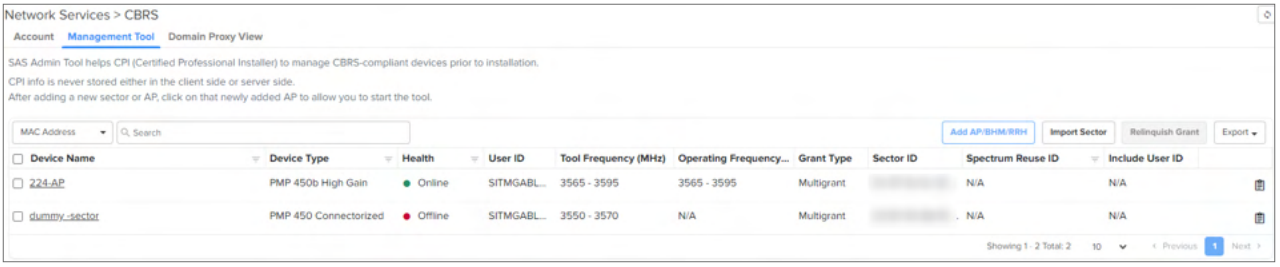
9. If the device is already claimed, it can be onboarded by clicking the onboard link.



Management Tool Sector Statistics

To view Sector Statistics:

1. Navigate to **Services** > **CBRS** > **Management Tool.**
2. Click **View Sector Statistics** under **Status**.



3. **Sector Statistics** window pops up.

> **Note**
>
> Refer to the CBRS State Diagram for additional details.

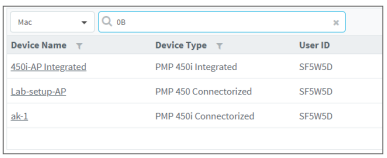
Search Management Tool Sector

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.

> **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.



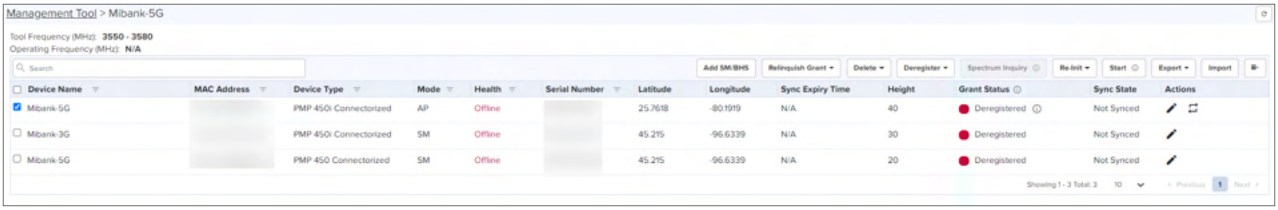
1. Filter AP or sectors can be cleared by clicking ⊗ or **Clear** button.

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.



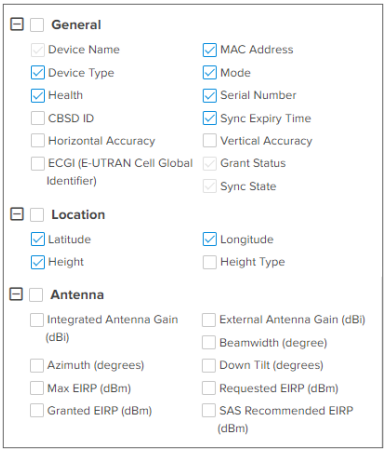
Sector Details View

- 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.

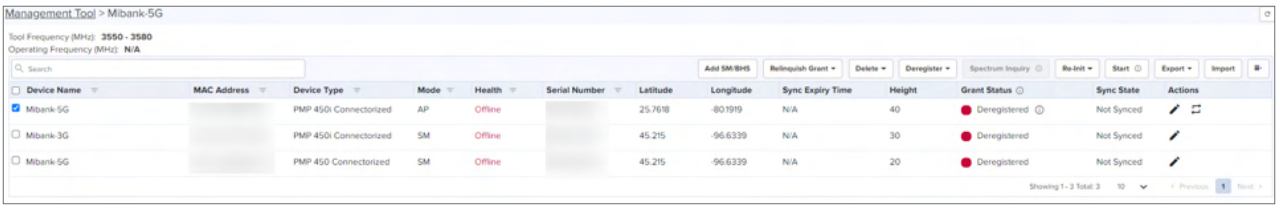
> **Note**
>
> If the device is **Config_Synced**, the CBSD state of the device will be updated from the device in real-time.

- 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( ).



- User can use following button to control the CBRS procedure:

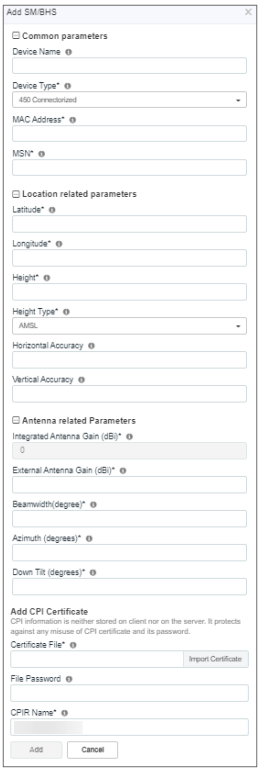


  - **Start** and **Stop**: manage to start and stop CBRS procedure of a sector.
  - **Reinitialize**: restarts the CBRS procedure and reinitializes the devices.
  - **Deregister:** deregisters the device (single or multiple).
  - **Spectrum Inquiry**: checks the availability of frequencies.
  - **Delete**: deletes the device (single or multiple).
  - **Unblock**: clears the de-registered state on an LTE, allowing a registration or reregistration request.
  - **Export**: exports the sector data in .xlsx format.
  - **Import:** imports the SM in the sector.
  - **Relinquish Grant:** relinquishes grants generated in Wide-Grant mode.

- Once the sector is authorized (AUTHORIZED state), button transfers grant details from the Management Tool to real devices.

Add SM or BHS

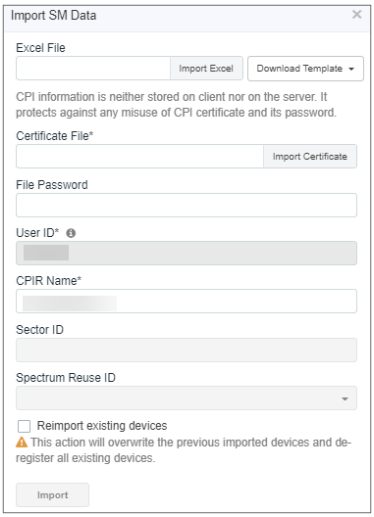
1. Navigate to **Services** > **CBRS** > **Management Tool** > select a sector.
2. Click **Add SM** or **BHS** to add SM in a sector.



3. Enter all parameters under following categories:
   - **Common parameters:** Device Name, Device Type, MAC Address, and MSN.
   - **Location related parameters**: Latitude, Longitude, Height and Height Type, Horizontal Accuracy, and Vertical Accuracy.
   - **Antenna related parameters**: Integrated Antenna Gain, Beam width, Azimuth, and Down Tilt.
   - **Add CPI Certificate**: Certificate File, File Password, and CPIR Name.
4. Click **Add** to add an SM.

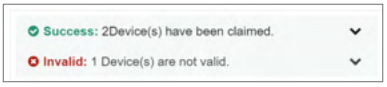
Import SMs

1. Navigate to **Services** > **CBRS** > **Management Tool** and select a sector**.**
2. Click **Import** button to import SMs into a sector.
3. Enable the **ReImport Devices** to overwrite the previous imported data and deregister all existing devices.

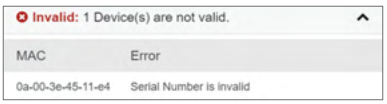


4. Click **Download Template** if user does not have Import Sector template. Users can download two different template formats:
   - PMP: Excel or ODS
   - LTE: Excel or ODS
5. Click **Import Excel** to select Import Sector template file. File must be Microsoft Excel format (.xlsx) or Open Document Spreadsheet (ods) formats.
6. Enter the following CPI credentials:
   - Upload CPI Certificate File by clicking **Import Certificate** button.
   - Enter CPI File Password.
   - Enter CPI Registered Name.
7. Click **Import**.

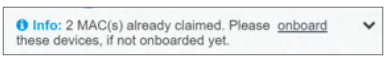
   Import status will be shown under **Success, Info,** and **Invalid** sections.



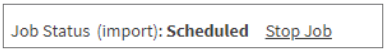
8. Details of **Success**, **Info** and **Invalid** can be seen by clicking ⌄.



9. If the devices is already claimed, it can be onboarded by clicking the **onboard** link.



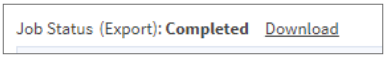
10. Once the user clicks **Import**, a job is scheduled.



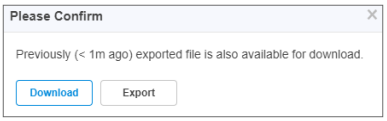
Export Sector

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.

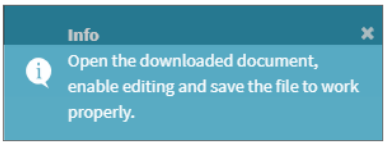


4. Once the Job status is Completed, **Download** the Sector xlxs.



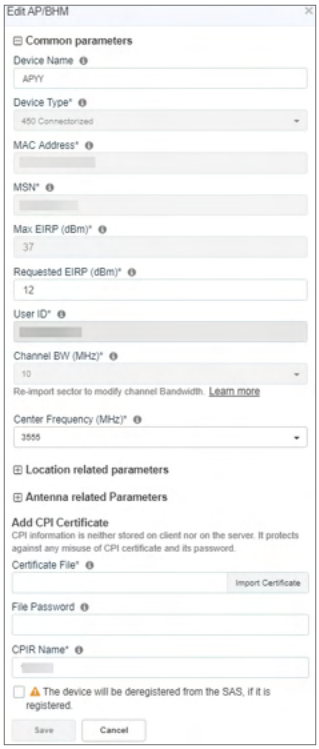
> **Note**
>
> **Download** button is enabled only for two hours after the export job completes.

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

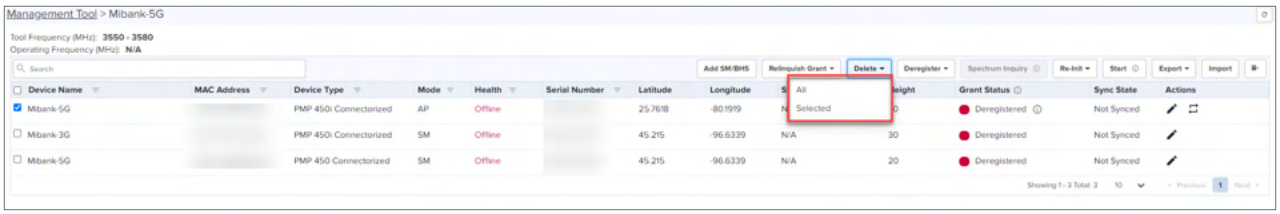
1. Navigate to **Services** > **CBRS** > **Management Tool** and select a sector**.**
2. Click **Stop** button if the CBRS procedure is running.
3. Click **Edit** button to edit device parameters.
4. Enter CPI credentials:
   - Upload CPI Certificate File by clicking **Import Certificate** button.
   - Enter CPI File Password.
   - Enter CPI Registered Name.
5. After editing the device. The device should go to derigestered state.



6. Click **Save**.

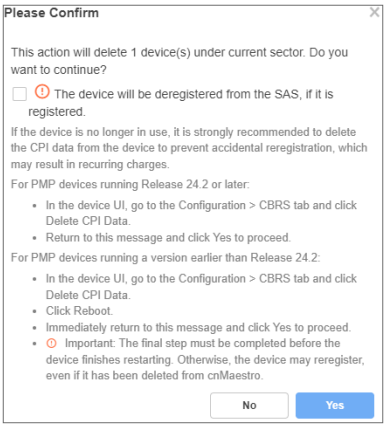
Delete Device

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.



5. Click **Yes** to confirm.

   The following confirmation message is displayed when you select the **Selected** option from the **Delete** dropdown list.



6. After confirmation, a job is scheduled.

7. Deleting AP:

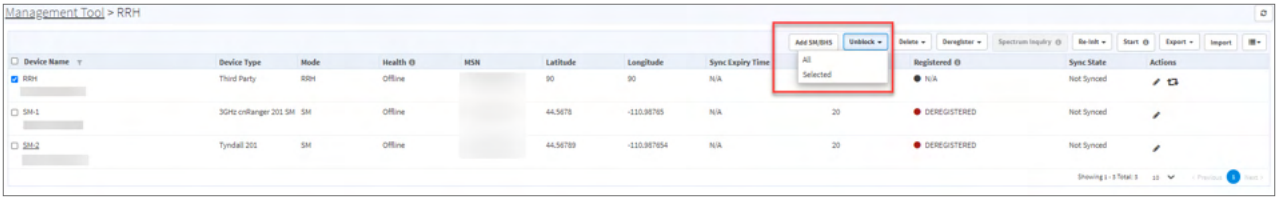
   All SMs of the sector must be deregistered and deleted before deleting the AP. Refer to the Deregistration procedure to deregister all SM devices.

8. Select the AP of the sector to delete.
9. Click **Delete**.

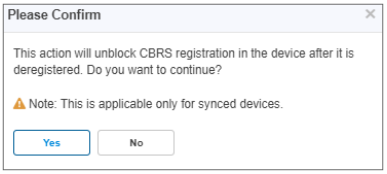
> **Note**
>
> If the procedure is started for the device and it is registered, then, while deleting the device, you must select the **Deregister** checkbox, otherwise the deletion will fail.

Unblock Device

1. Navigate to **Services** > **CBRS** > **Management Tool** and select a sector.
2. If LTE device is **Config Synced**, and if device deregister flag is enabled, unblock removes the deregistartion flag on the device.
3. 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.



4. Click **Selected** display the **Please Confirm** window.

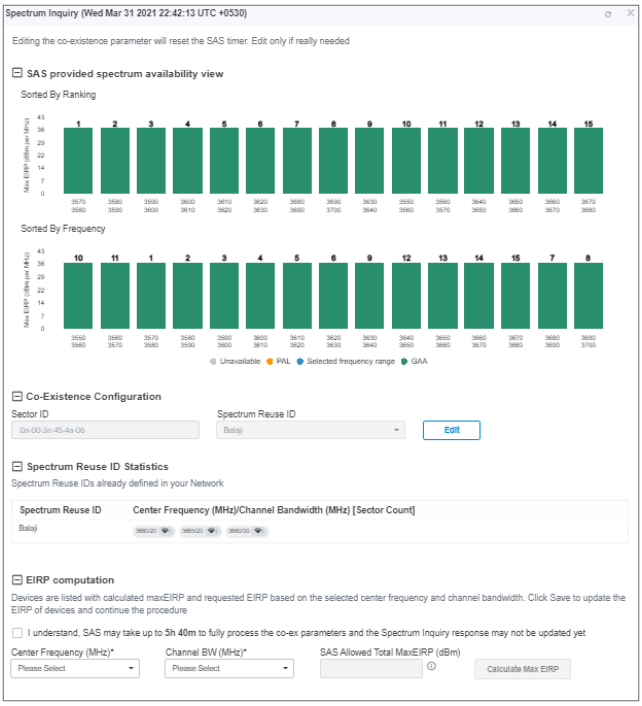


5. Click **Yes** to confirm the action.

Start CBRS Procedure

The Start button starts the CBRS procedure for a sector.

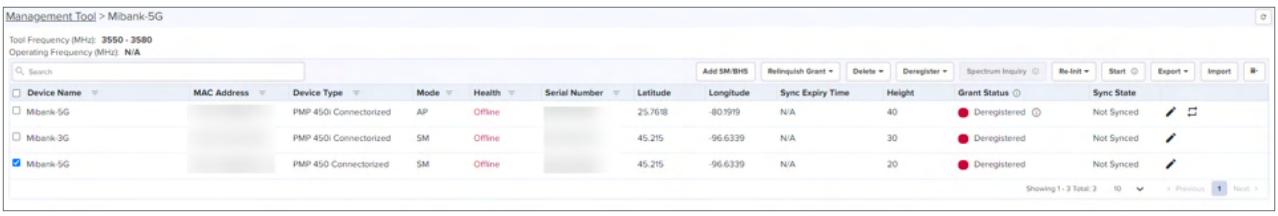
1. Navigate to **Services** > **CBRS** > **Management Tool** and select a sector.
2. Click **Start** to start CBRS procedure of a sector.
3. Once the user clicks start, the **Spectrum Inquiry** window pops up.



> **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:



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).

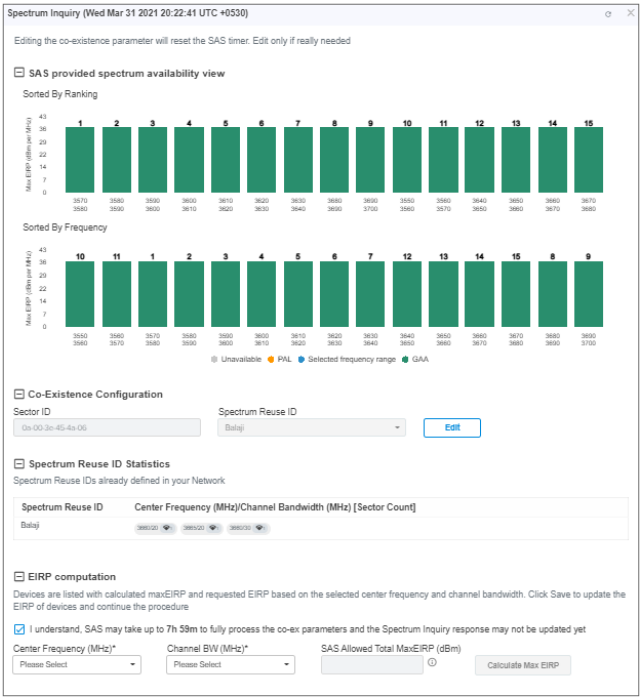
Multi-Grant

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.

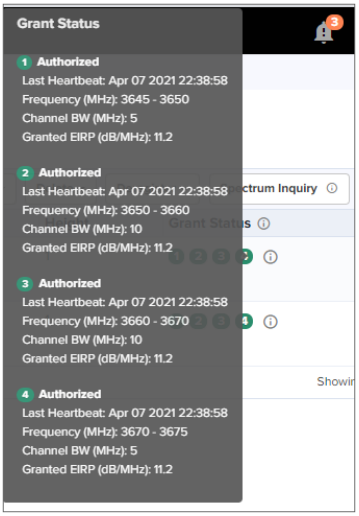
5. Accept the checkbox process of the Co-Existence parameters.

> **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:

7. To view the Grant Status click the info (ⓘ) icon.

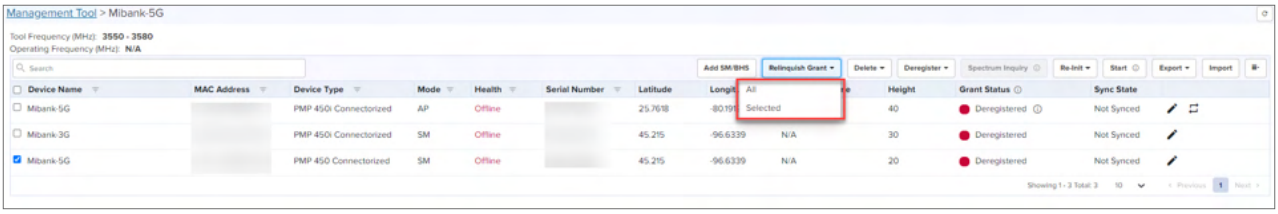


Relinquish Grant

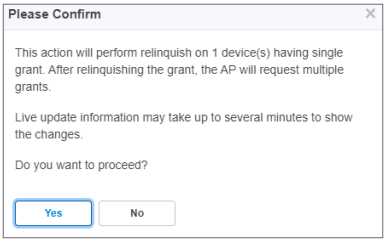
Relinquish Grant relinquishes all grants of selected sector. This will make devices enter the Registered state. The device will start Multi-Grant procedure if Multi-Grant feature is enabled on it.

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.

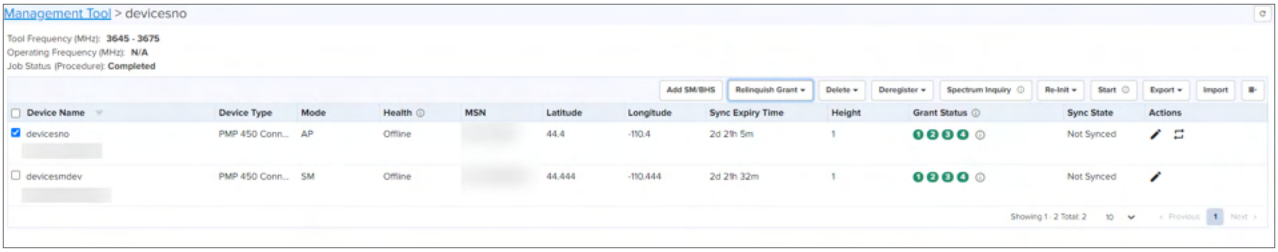


3. Click **Yes** to confirm the action.



> **Note**
>
> Live update information may take upto several minutes to display the changes of reflected relinquish status.

4. Once the user clicks **Yes**, **Wider Grant** gets converted to the **Multiple Grants** as shown below:



Stop CBRS Procedure

The **Stop** button stops the CBRS procedure for a sector.

1. Navigate to **Services** > **CBRS** > **Management Tool** and select a sector**.**
2. Click **Stop** button to stop CBRS procedure.

> **Note**
>
> - If the device is already synced with the Management Tool, the CBRS Start and Stop procedures are not applicable to the synced devices.
> - If user does not see the **Stop** button, it means the CBRS procedure is already in stopped state, **Start** and **Stop** are toggles.
> - If all devices of the sector are in AUTHORIZED state, the CBRS procedure will automatically stop.

Reinitialize CBRS Procedure

The **Re-init** button allows the user to start the CBRS procedure for a sector and reinitialize selected devices (Reinitialize = Start of sector + Reinitialization of user selected devices). At least one device must be selected in order to enable the **Re-init** button. Clicking **Re-init** reinitializes selected devices to UNREGISTERED (irrespective of previous CBRS state).

1. Navigate to **Services** > **CBRS** > **Management Tool** and select a sector.
2. Click **Stop** if the CBRS procedure is already running.
3. Select one or more devices to be reinitialized.

> **Note**
>
> You might notice some delay in enabling **Re-init** button after pressing **Stop.** It is due to a delay in properly stopping the CBRS procedure.

4. Click **Re-init** to start the reinitialization procedure
5. Confirmation window pops up:
   - Click **Continue** or
   - Select **Spectrum Inquiry** to edit the **EIRP values** as shown in Start procedure.

> **Note**
>
> - Synced devices cannot be reinitialized.
> - Reinitialize modifies or corrects the parameters. For example, if a device is in HALT state due to a parameter error, the user can stop the CBRS procedure and reinitialize the device after modifying device parameters.

Deregistration

The deregistration procedure allows user to deregister the devices from the DomainProxy.

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.

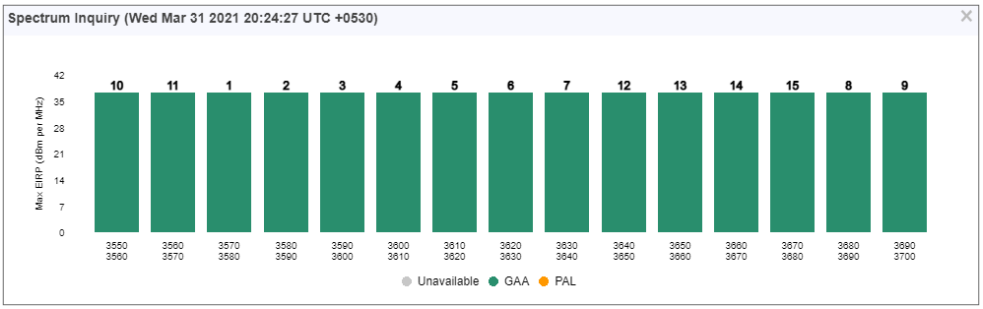
   Once the user clicks **Deregister**, a job is scheduled**.**

   Job Status (Deregistration): **Completed**

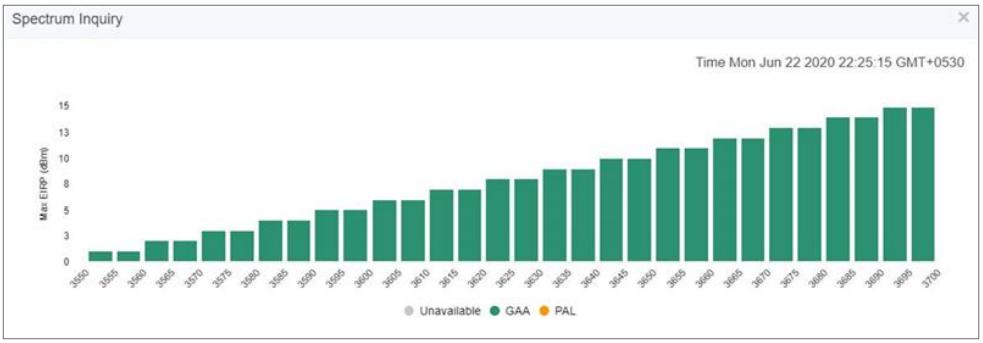
5. If the deregistration fails, the reasons will be indicated under ⓘ.

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.

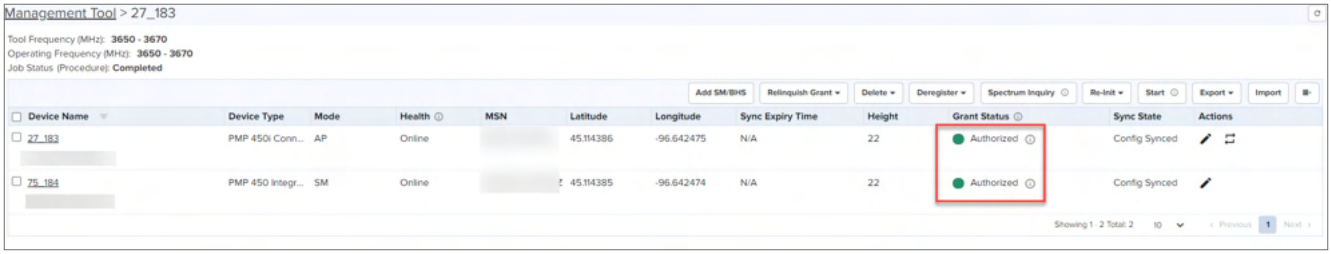
Once **Yes** is clicked, the Management Tool will check the accessibility of AP/BHM before proceeding with sync.

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.



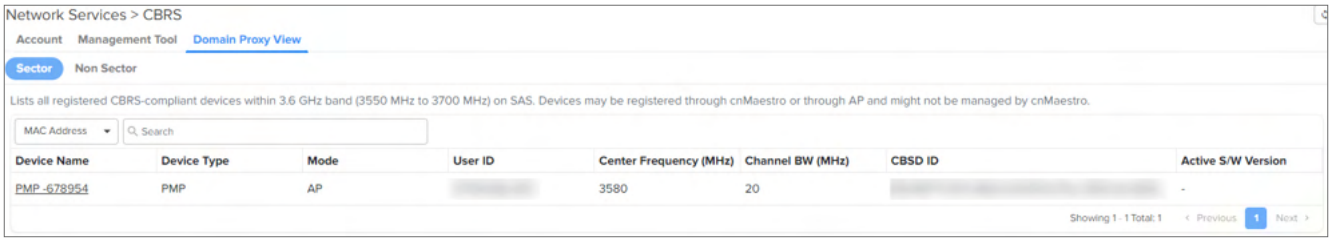
It displays the possible single Grant state such as:

- 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.

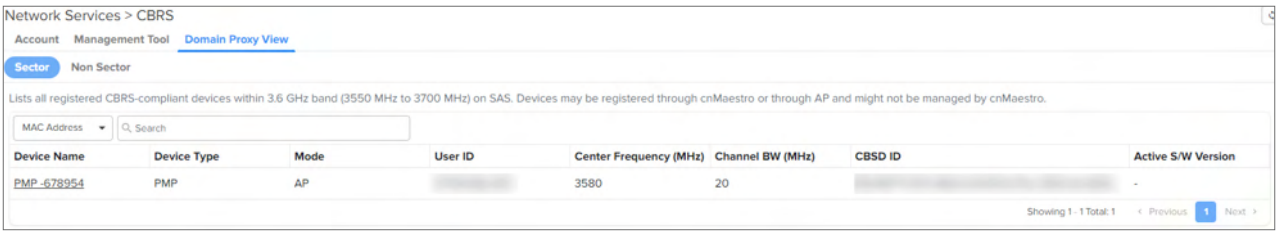


- **Sectors Page**: displays the devices according to the parenting AP list.
- **Non-Sector Page**: displays each individual AP and SM of **LTE** and **PMP**.

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.



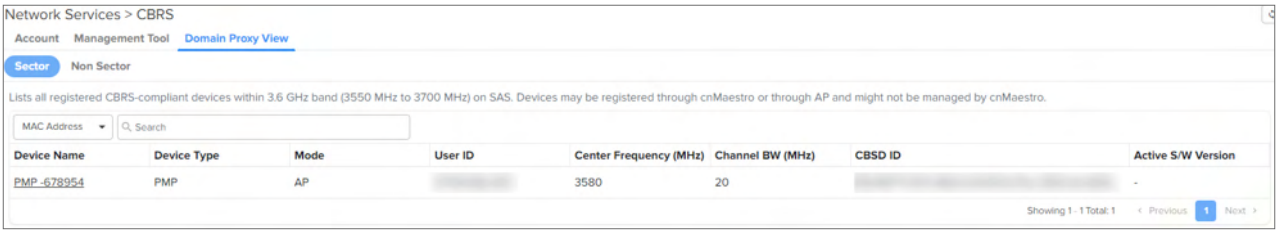
3. Enter text in search box.

> **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.



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 **Hearbeat 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

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.

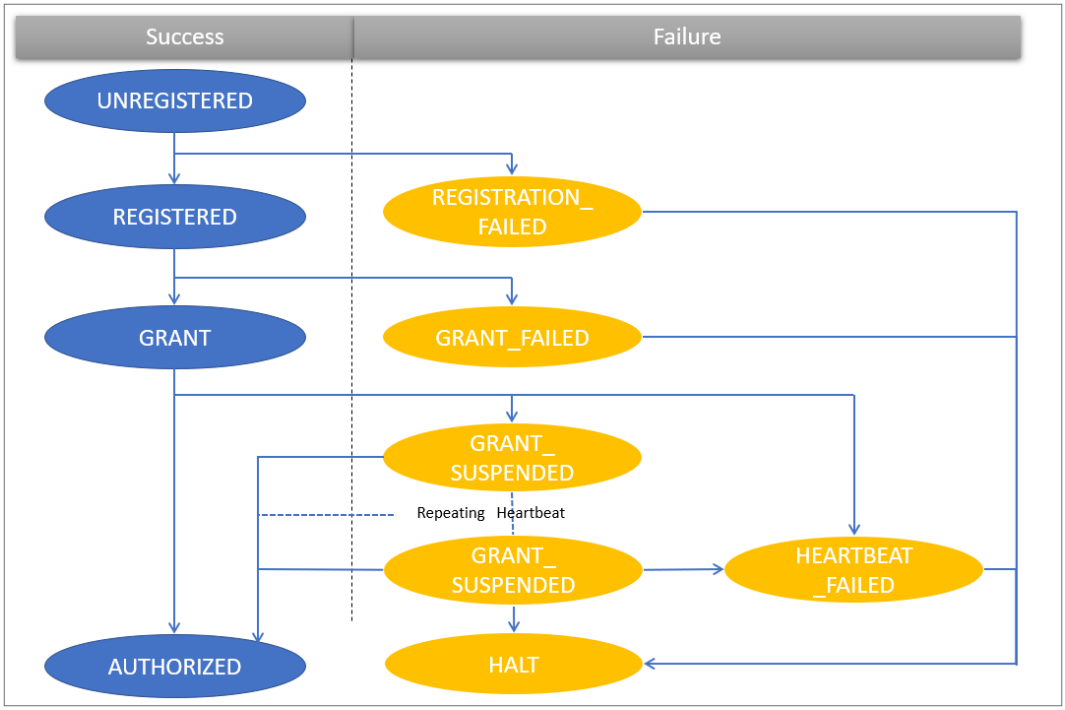
Management Tool Sync

The Sync procedure allows the user to transfer grant information from the Management Tool to a real device. The Sync action can only be performed on an AP or BHM. The SM and BHS are synced automatically when they come online. Once the AP/BHM/SM/BHS are synced, no further action is taken from Management Tool.

1. Navigate to **Services** > **CBRS** > **Management Tool** and select a sector**.**
2. Click **Sync** to perform the synchronization procedure.
3. Click **Yes** to enable CBRS on AP/BHM after successful sync or click **No** to cancel synchronization procedure.

   Once **Yes** is clicked, the Management Tool checks the accessibility of AP/BHM and proceeds with sync.

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: • 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.

Configuring HTTP Proxy Server for CBRS and AFC Connectivity

For CBRS- and AFC-complaint devices to communicate with the SAS and AFC server, respectively, an HTTP proxy server is required. It may be an internal proxy, the cnMaestro Cloud proxy, or an external HTTP proxy.

- External Proxy Requirements
- Squid as an External Proxy
- High Availability for Squid External Proxy
- Configuring HTTP Proxy for CBRS and AFC

External Proxy Requirements

If you are using a forward proxy in your network, continue to use it rather than setting up a new one. Connections are established using HTTP CONNECT with the following CBRS and AFC URLs, which is required by the proxy.

- CBRS SAS server URL: sas.cbrs.cambiumnetworks.com
- AFC server URLs:
  - api.qcs.qualcomm.com
  - afcapi.qcs.qualcomm.com
  - afcapi.canada.qcs.qualcomm.com

A TLS intercepting proxy (such as a security gateway) may break the connectivity.

Squid as an External Proxy

The below versions support external proxy configuration, but does not offer high availability and may not be inline with your network standards. This configuration is tested for the below new versions:

- Ubuntu 20.04 / Squid Cache: Version 4.10
- Centos 7 / Squid Cache: Version 3.5.20

Note

This example contains URLs that are allowed for CBRS and AFC for both US and Canada regions. Operators may remove the unneeded URLs, if they prefer. For example, an operator in Canada using AFC but not CBRS can remove the CBRS entries and the US AFC entries. However, this is not mandatory.

```
## WARNING:
## While this config may work for your use case,
we encourage you to follow your own best practices and modify this file for your network.
##This ACL limits connections to CBRS and AFC.
acl afc_prod_reg dstdomain api.qcs.qualcomm.com
acl afc_us_si dstdomain afcapi.qcs.qualcomm.com
acl afc_canada_si dstdomain afcapi.canada.qcs.qualcomm.com
acl cbrs dstdomain sas.cbrs.cambiumnetworks.com
acl cloud dstdomain cloud.cambiumnetworks.com

acl SSL_Ports port 443
acl CONNECT method CONNECT

##Deny CONNECT to other than secure SSL ports.
http_access deny CONNECT !SSL_Ports

##Allow access only for specific domains.
http_access allow CONNECT afc_prod_reg
```

```
http_access allow CONNECT afc_us_si
http_access allow CONNECT afc_canada_si
http_access allow CONNECT cbrs
http_access allow CONNECT cloud

##Deny access for all other requests.
http_access deny all

##We do not need any cache for proxying cache deny all.

##Squid normally listens to port 3128.
http_port 3128
```

High Availability for Squid External Proxy

Since a standalone proxy is a single point of failure, it is recommended to use an high availability (HA) setup for Squid. This can be done using Pacemaker or DRDB.

Configuring HTTP Proxy for CBRS and AFC

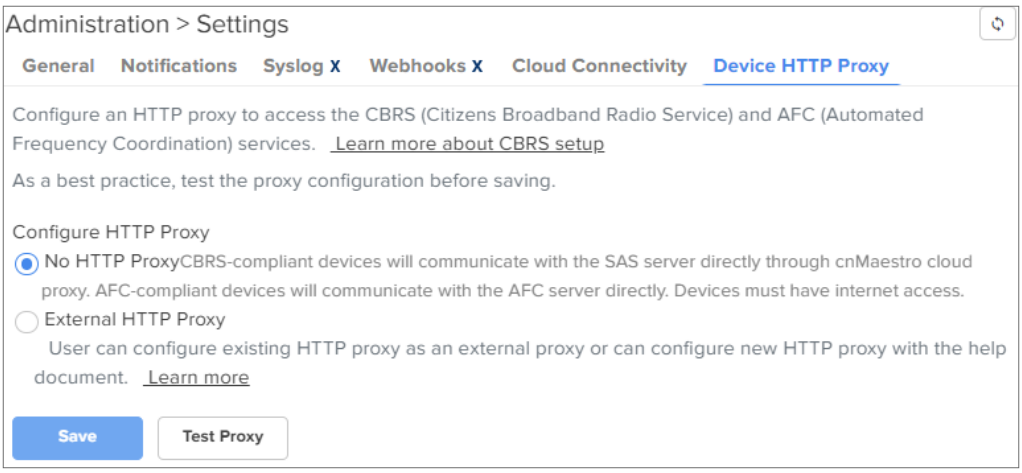
To configure HTTP proxy for CBRS and AFC services, complete the following steps:

Note

Cambium recommends to test the configured HTTP proxy server before proceeding to implement the same for CBRS and AFC connectivity.

1. Navigate to the **Administration** > **Settings** > **Device HTTP Proxy** page.

   Figure 424 *Device HTTP Proxy page*

2. Select from one of the following options in the **Configure HTTP Proxy** section:

   - **No HTTP Proxy**: This option is selected, by default.

     Here, CBRS- and AFC-compliant devices directly communicate with the SAS and AFC servers, respectively, through the Cambium domain proxy.

     Note

     The On-Premises server, CBRS-complaint devices, and AFC-complaint devices must have internet access to communicate directly with the Cambium domain proxy.

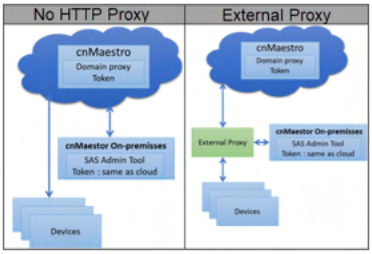
- **Eternal HTTP Proxy:**

  Additionally, configure the proxy server address in the Proxy field in the `http://<IPv4-address>:<Port-Number>` format.

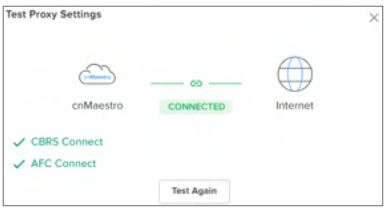
  For example, `http://11.110.0.101:9090`

  > **Note**
  >
  > The **External HTTP Proxy** method is preferred, because upgrades to cnMaestro could result in proxy server downtime and in turn result in loss of CBRS and AFC connectivity.

  Figure 425 *Proxy server configurations*

3. Click **Test Proxy** to test domain proxy connectivity. If the test is successful, it will display the following message:

4. Click **Save**.

LTE

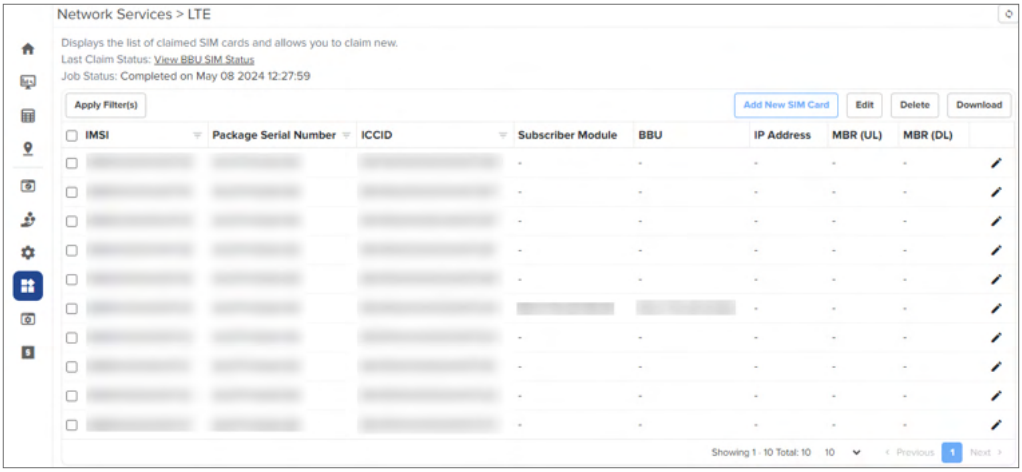
cnMaestro supports LTE as part of its cnMaestro deployment. LTE allows customers to onboard the SM with IMSI into cnMaestro.

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).

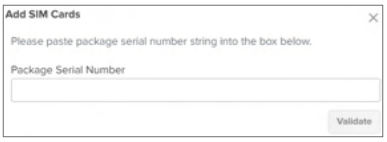
Adding SIM Cards

To add a SIM card, complete the following steps:

1. Navigate to **Network Services > LTE**.



2. Click **Add New SIM Card**. The following window appears.

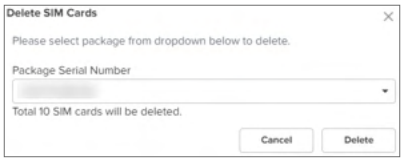


3. Enter appropriate **Serial Number** of SIM package and click **Validate**.
4. After successful validation of the serial number, click **Add**.

> **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.

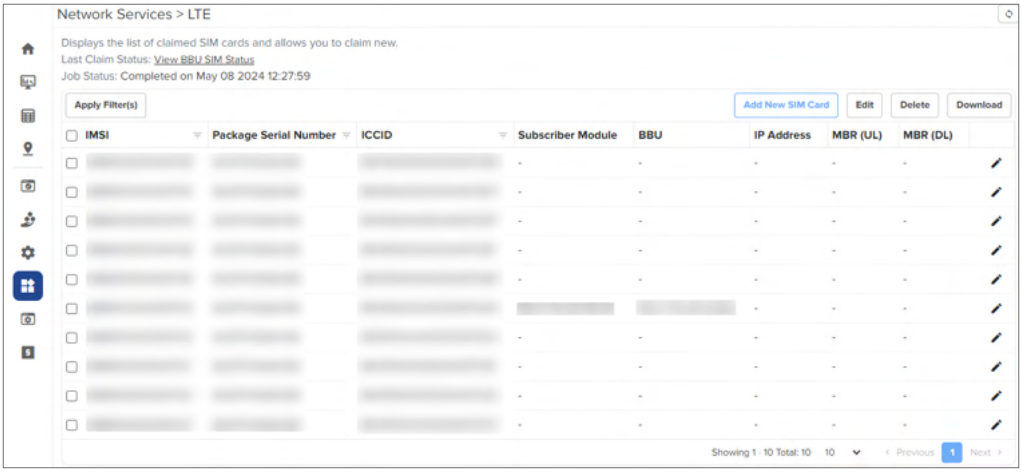


> **Note**
>
> IMSI numbers get deleted with the mapped Serial Number.

Update SIM Details

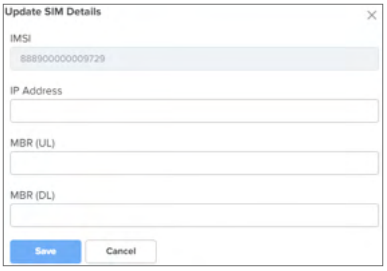
User can edit the SIM details as follows.

1. Navigate to **Network Services > LTE**.



2. Click the edit ( ) icon for the IMSI that you want to edit.

   The **Update SIM Details** window pops-up.

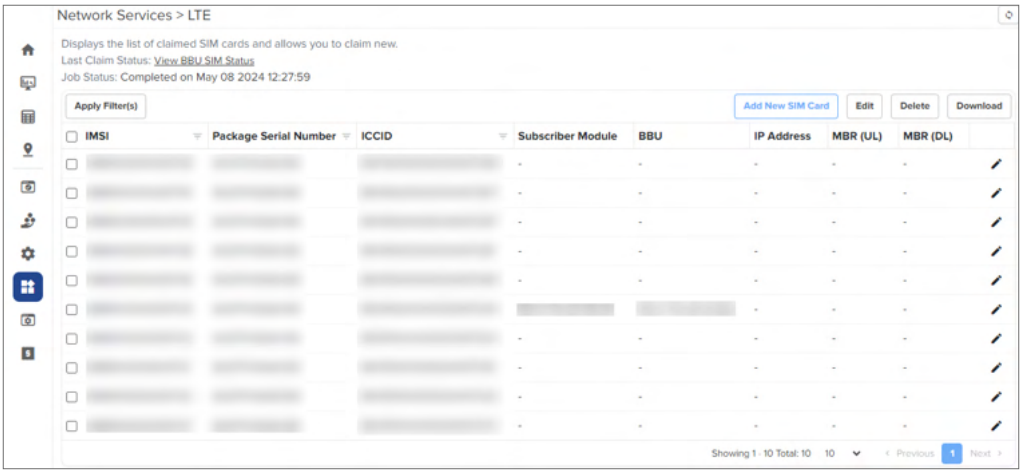


3. Enter a valid **IP Address**.
4. Enter the **MBR (UL)** and **MBR (DL)**.
5. Click **Save**.

Viewing BBU SIM Status

Allows the users to view the status of the SIM connected to the BBU.

1. Navigate to **Network Services > LTE.**



2. Click **View BBU SIM Status.**

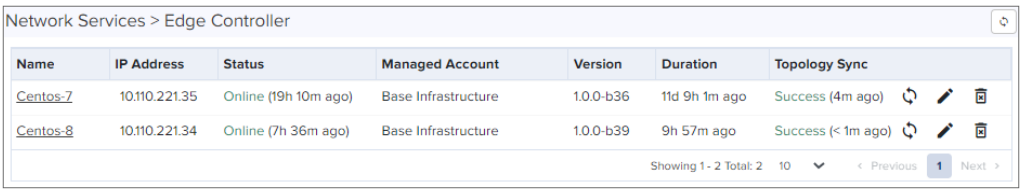
Managing Edge Controller

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 426.

   Figure 426 *Edge Controllers*



   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

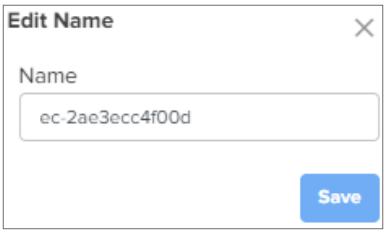
Topology Sync

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.



2. Click **Save**.

Delete

1. Click the delete (🗑) icon in the Edge Controller page.

   The delete confirmation window appears.

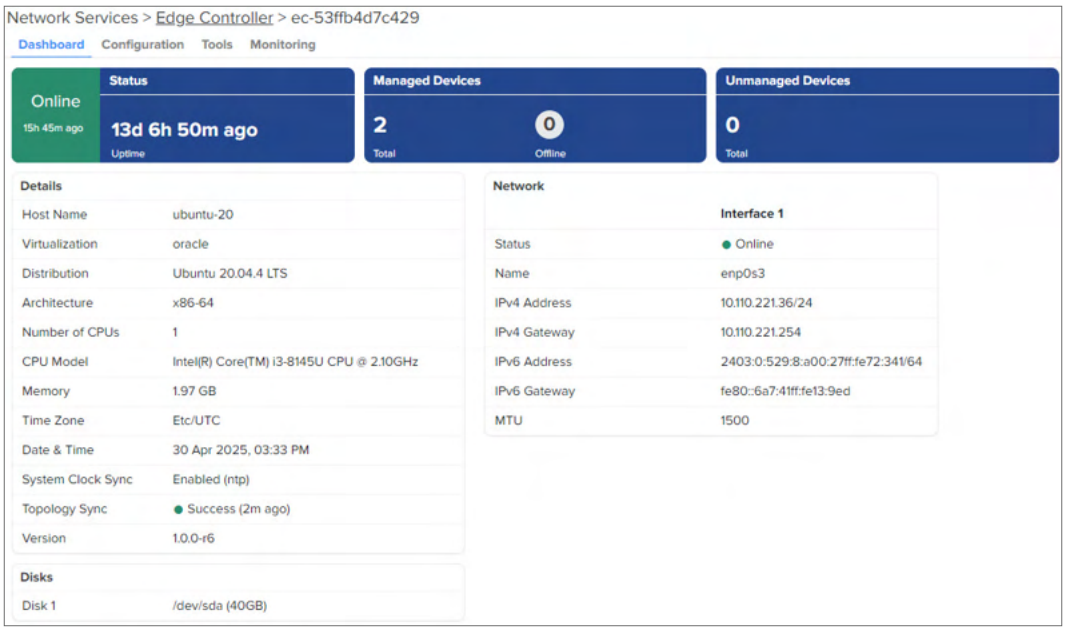
2. Click **Yes**.

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 427.

Figure 427 *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 127.

Figure 428 *Edge Controller and PTP 820/850 devices status*

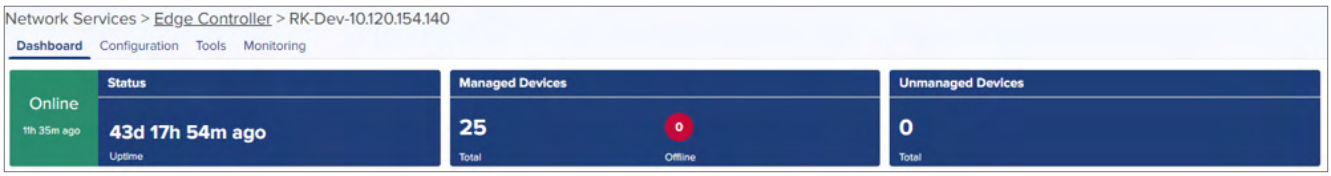


Table 127 *Fields in the Edge Controller dashboard*

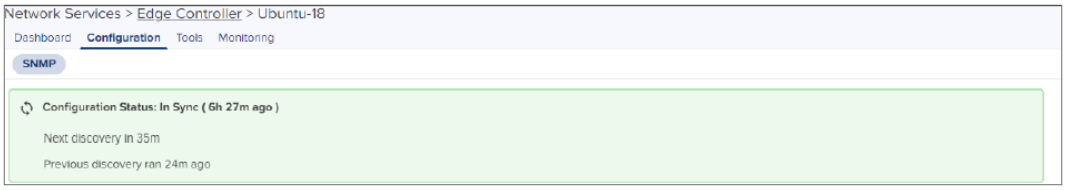
Field	Description
Host name	Name of the host.
Virtualization	Type of virtualization such as VMware or Oracle.
Distribution	Type of distribution such as Ubuntu and CentOS versions.
Architecture	CPU and Operating System installed.
Number of CPUs	Total number of CPUs utilized.
CPU Model	Type of CPU model.
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.
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 429.

Figure 429 *Configuration Status*

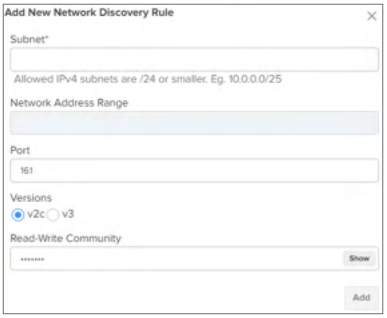


Rules

To add a new rule, perform the following steps:

1. Click **Add New**.

The **Add New Network Discovery Rule** window appears.



2. Type **Subnet** range in CIDR format (for example, 10.204.88.0/28) to discover PTP 820/850 devices.

   The range of IP addresses in the **Network Address Range** field is displayed.

3. Type **Port** number.
4. Choose SNMP **Version**:

   For SNMP version **v2c**, perform the following:

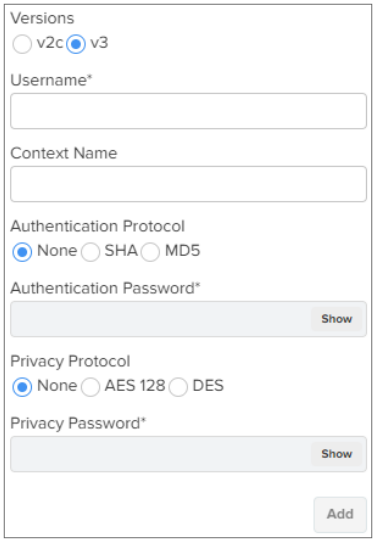
   a. Enter preferred community string when you create a SNMP discovery rule.

   b. Click **Add.**

> **Note**
>
> Default community string is private.

For SNMP Version **v3,** perform the following:

a. Choosing SNMP v3 version allows you to enter the parameters as shown in the following figure.



b. Enter the following fields:

- **Username**.
- **Context Name** field is optional.

c. Choose any one of the **Authentication Protocol.**

- None
- SHA
- MD5

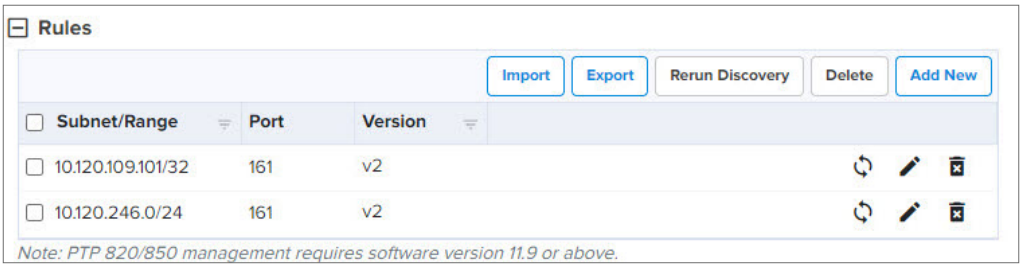
d. Choose any one of the **Privacy Protocol**.

- None
- AES128
- DES

e. Type **Privacy Password**.

f. Click **Add**.

SNMP Rules added are listed in the Rules table as shown in the following figure.



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.

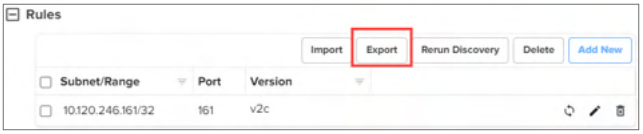
2. Browse to **Select File** or **Download Sample Template** to change or configure the SNMP as per the requirements in **Downloaded Sample Template.**

3. Click **Import**.

Export

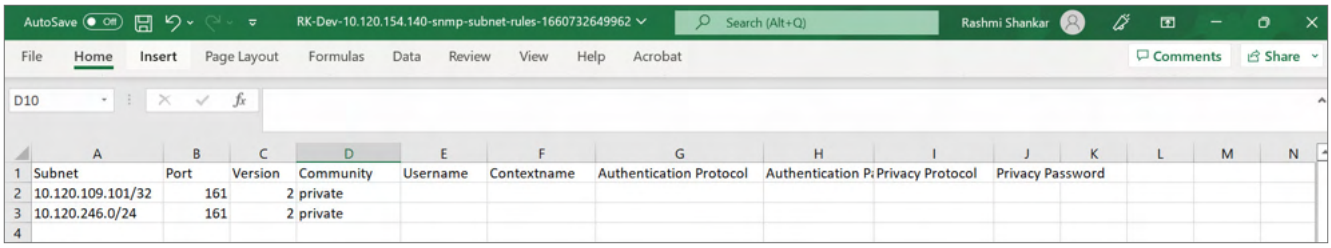
To export SNMP rules, perform the following steps:

1. Select one or more SNMP rules required to export.
2. Click **Export**.



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.



Delete

To delete SNMP rules in the table, perform the following steps:

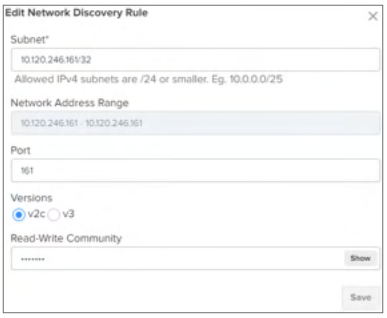
1. Select one or more SNMP rules in the table.
2. Click **Delete**, to delete one or more entries in the table or click **Delete** (🗑) icon to delete specific rule in the table.

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.



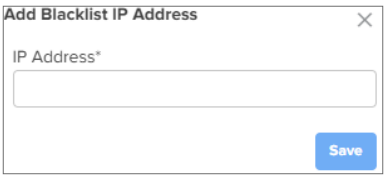
2. Click **Save**.

Blacklist

To blacklist PTP 820/850 devices, perform the following steps:

1. Click **Add New.**

Add Blacklist IP Address window appears.



2. Type **IP Address.**
3. Click **Save.**

Blacklisted IP Addresses are displayed in the table.

4. Select one or more blacklisted IP addresses in the table.
5. Click **Delete**, to delete one or more entries in the table or click **Delete** (🗑) icon to delete specific blacklist entry in the table.

Advanced Settings

In **Advanced Settings** section, configure the following parameters:

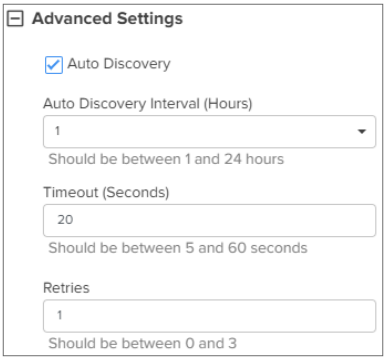
Note

- By default, **Auto Discovery** option is disabled.

- By default, **Auto Discovery Interval** option is 24 hours, when enabled and fields are auto-filled.

Enable **Auto Discovery** if you want to run SNMP discovery rules manually and perform the following steps:

1. Select **Auto Discovery Interval** option from the dropdown.
2. Enter **Timeout** in seconds between 5 to 60 seconds.
3. Enter **Retries** values between 0 and 3.



4. Click **Save**.

Tools

The Tools page allows you to perform the following actions:

- Diagnostics
- Operations
- Services

Diagnostics

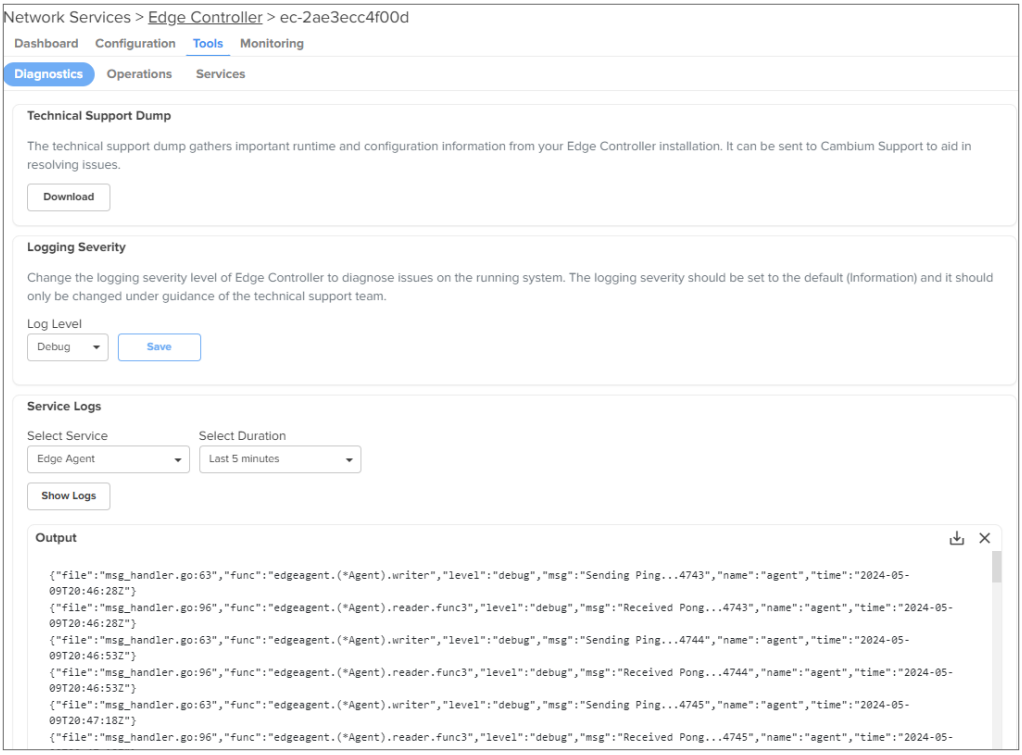
Diagnostics page allows you to gather technical support dump which can be downloaded and sent to Cambium Networks support team.

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

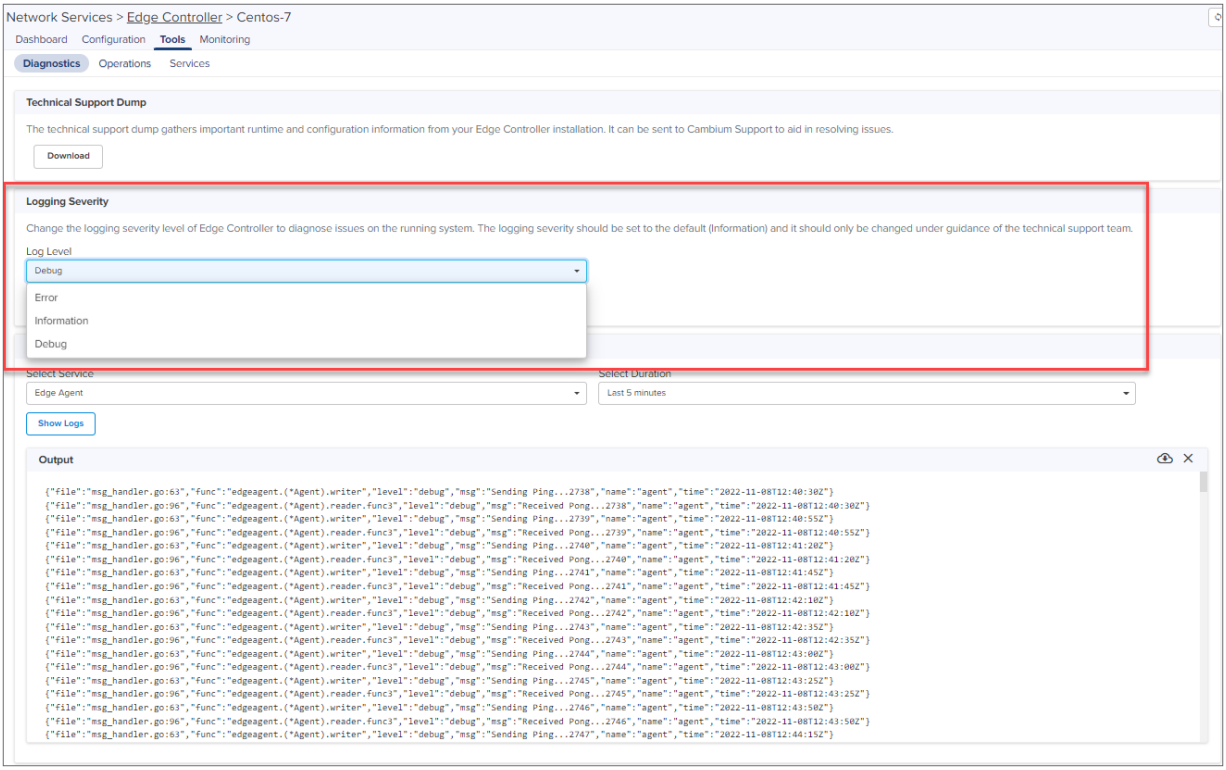


Logging Severity

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.

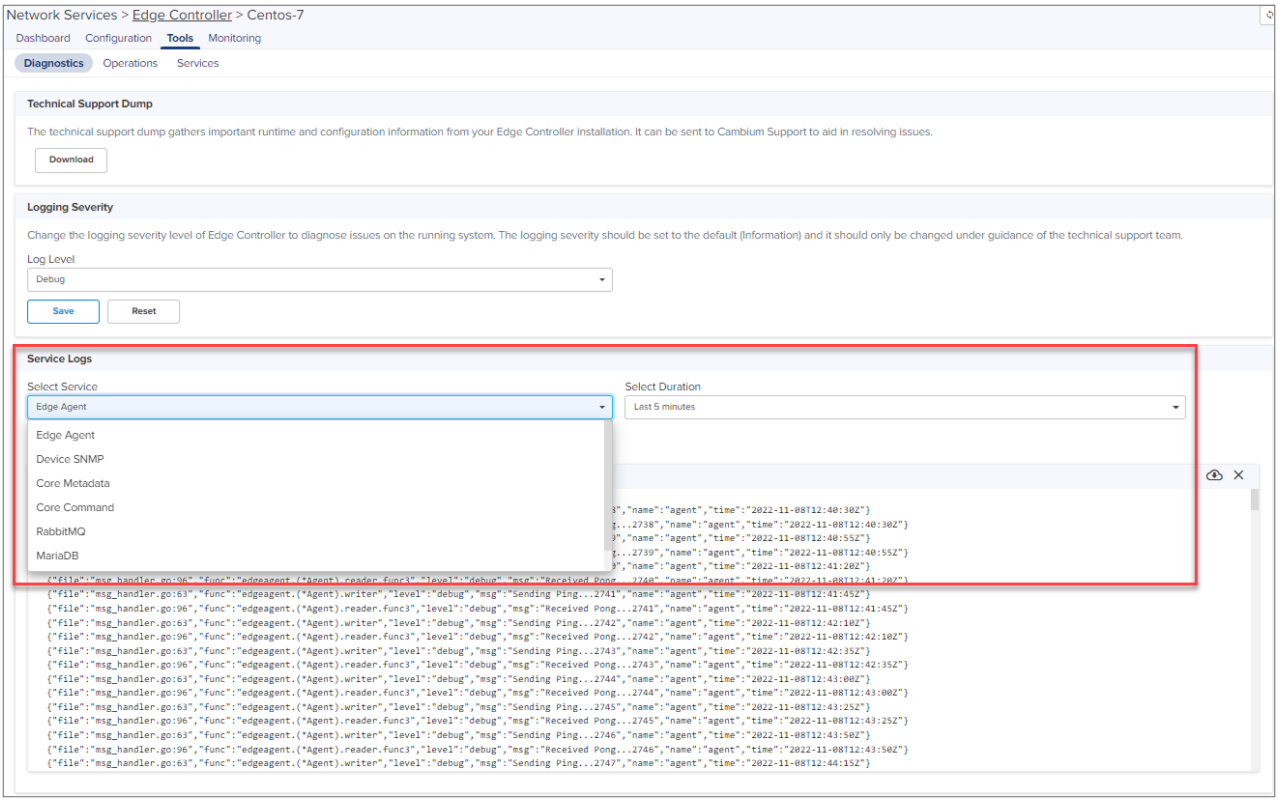
1. Select **Service** and **Duration** from the dropdown.

   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:

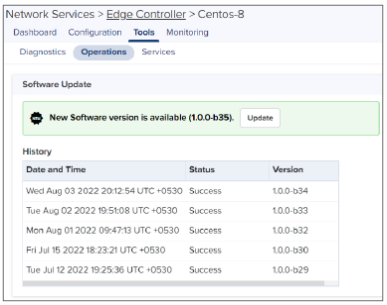


3. Click download ( ) icon to download the generated output.
4. Click clear (✕) icon to clear the output.

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.

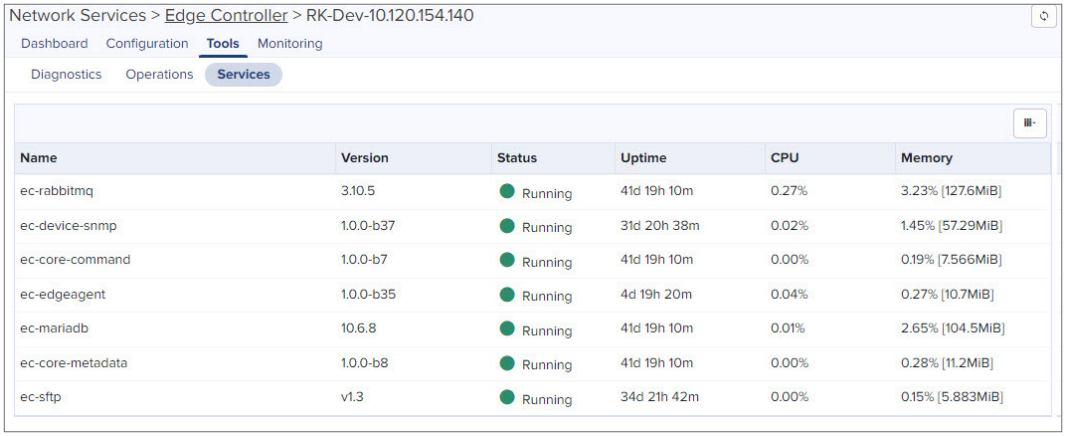
1. 1. Navigate to **Tools > Operations**.
2. 2. Click **Check for new software update**, checks for any new available software update.



Services

In **Services** page you can view the services running in the Edge Controller.

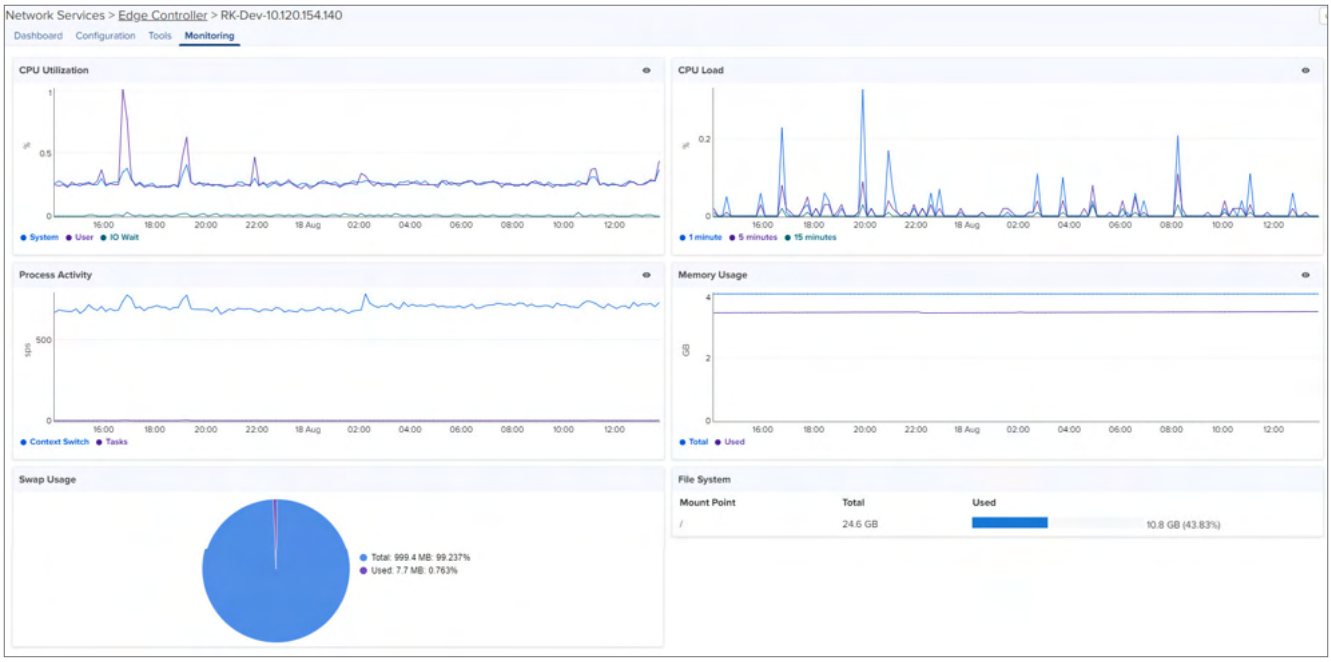
Figure 430 *Services*



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.**

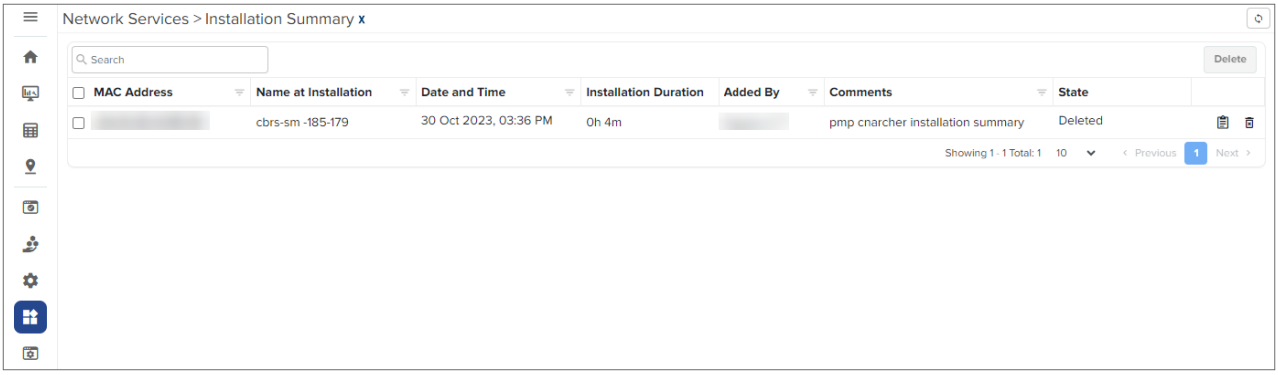


Table 128 *Fields in Installation Summary*

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.

3. Click **View Details** icon to view detailed Installation Summary.

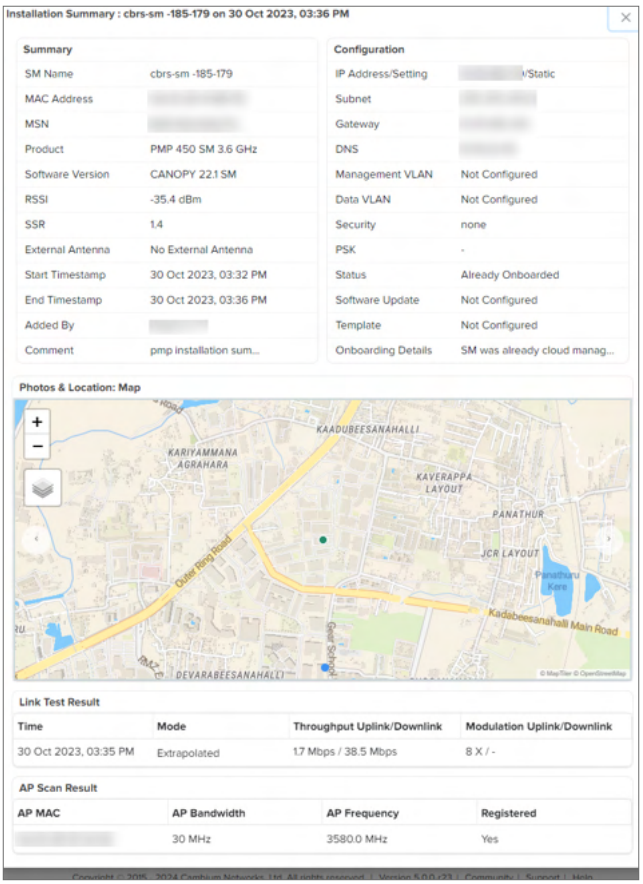


Table 129 *Summary fields in Installation Summary*

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.

Configuration

Table 130 *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 131 *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.

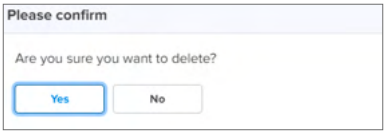
Table 132 *Fields in AP Scan Result*

Field	Description
AP MAC	MAC address of the AP.

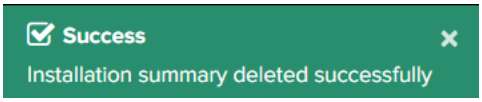
Table 132 *Fields in AP Scan Result*

Field	Description
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.



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**.

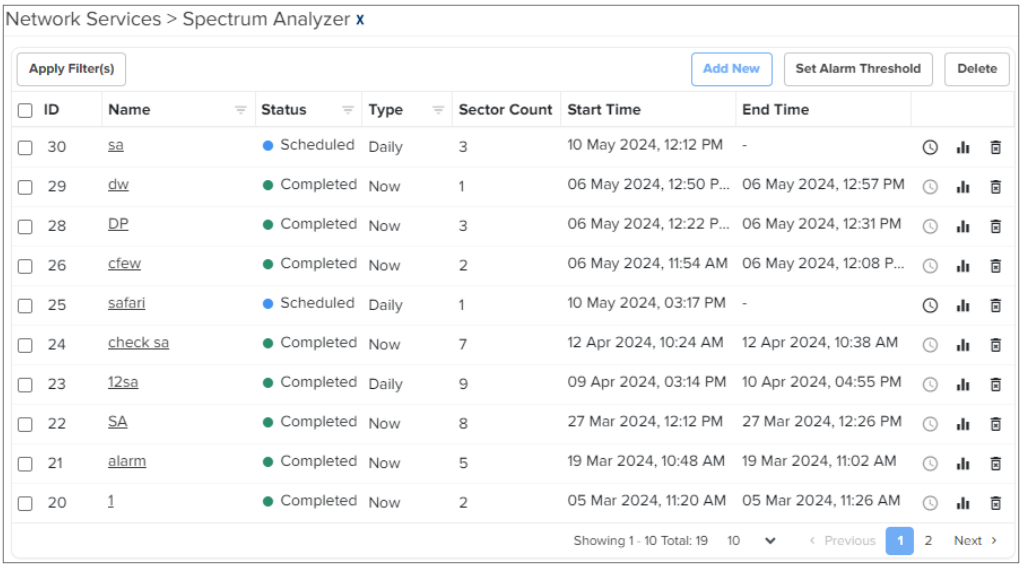


Table 133 *Fields in Spectrum Analyzer*

Field	Description
Name	The user-defined name for the spectrum analysis job or scan.
Status	The current status of the spectrum analysis.
Type	The type of analysis performed (for example, Now, Weekly).
Sector Count	The number of sectors or wireless areas analyzed in the spectrum scan.
Start Time	The scheduled start time for the spectrum analysis job.
End Time	The scheduled end time for the spectrum analysis job.

3. Click **View Result** icon on top right corner to view the detailed Spectrum Analyzer summary.

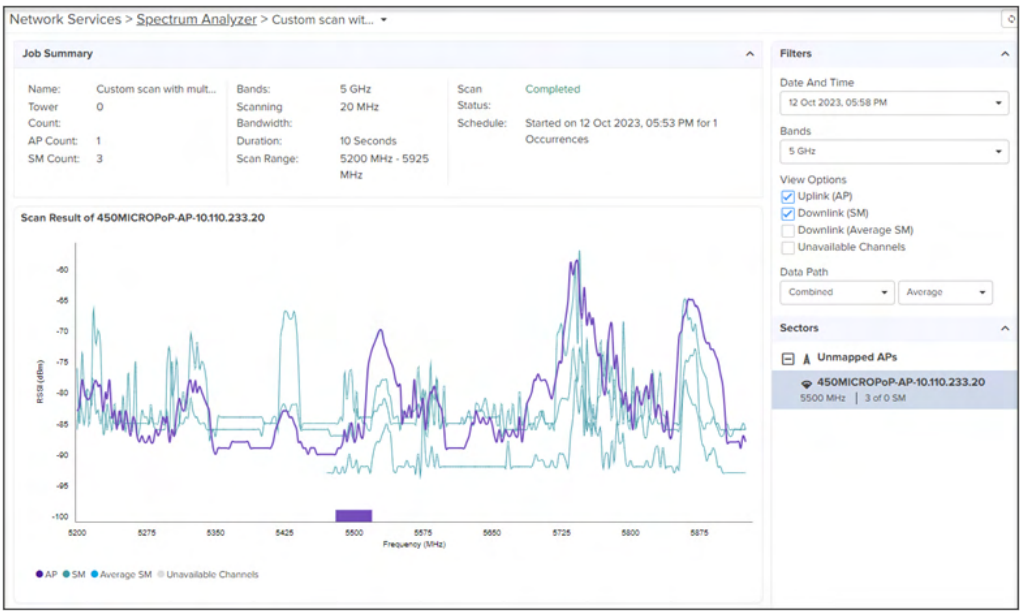


Table 134 *Job Summary parameters*

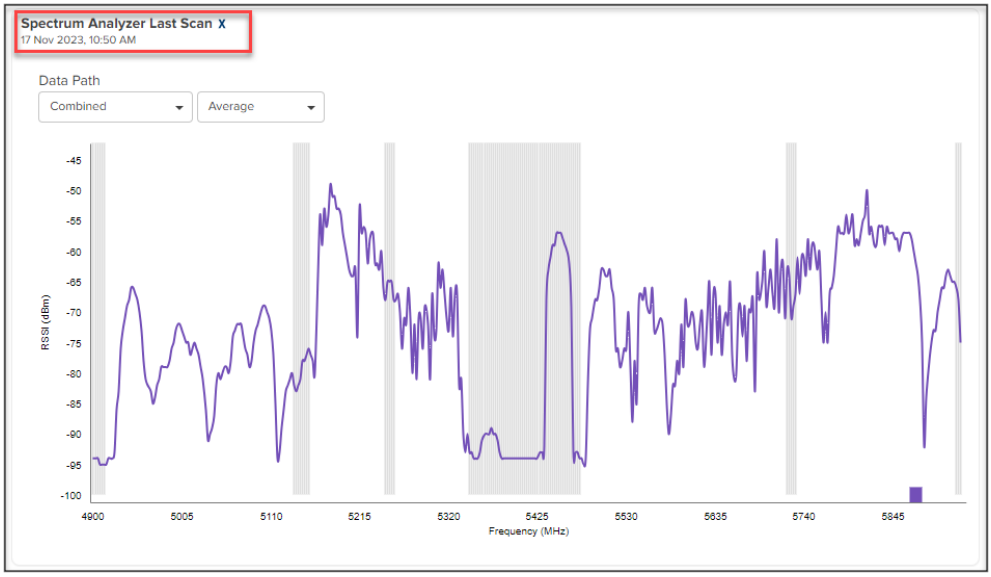
Field	Description
Name	The user-assigned name for the analysis job.
Tower Count	The number of towers included in the analysis.
AP Count	The number of APs in the analysis.
SM Count	The number of SMs in the analysis.
Bands	The frequency bands under analysis.
Scanning Bandwidth	The width of the frequency 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 135 *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	The viewing options for analyzing the spectrum. • Uplink (AP) • Downlink (SM) • Downlink (Average SM) • Unavailable Channels
Data Path	The data path used for the analysis. • **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:

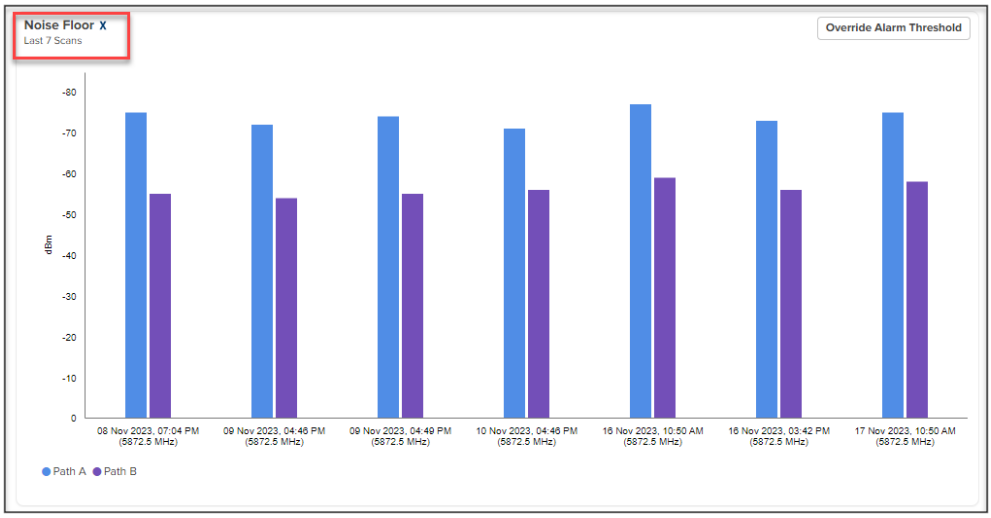
a. Navigate to PMP device **Dashboard** > **Spectrum Analyzer Last Scan**.



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.

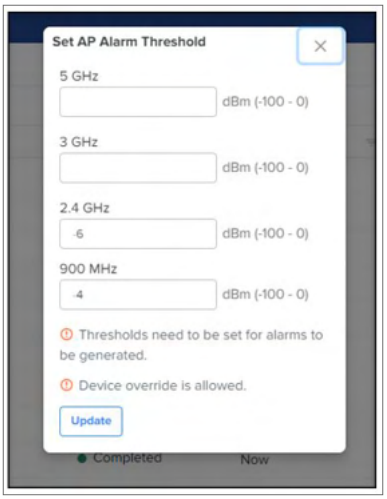


e. **Unmapped APs** display any APs that are not assigned to a tower.

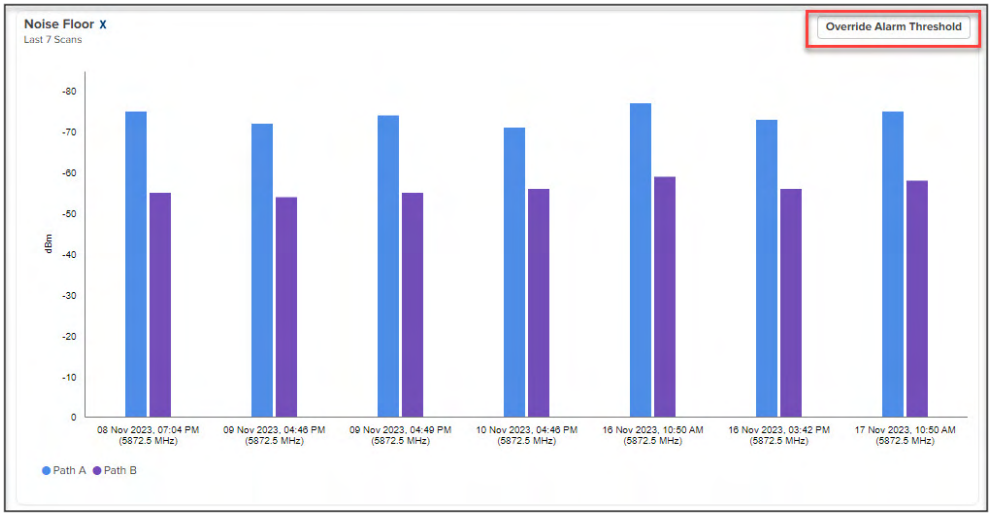
f. Click **Delete** icon on the top right corner to delete a job.

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.



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**.

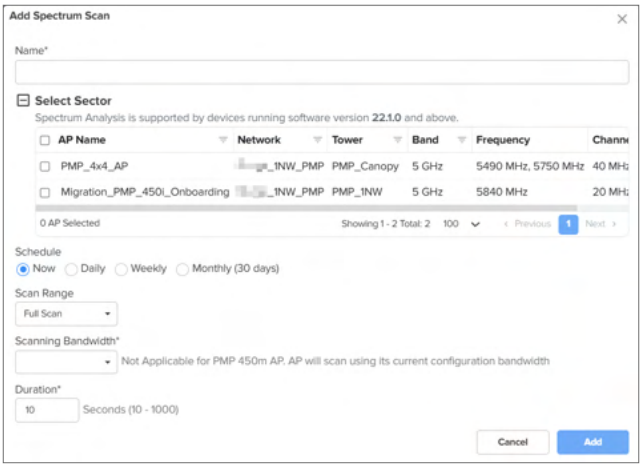


Table 136 *Add Spectrum Scan parameters*

Field	Description
Name	Job name to distinguish the analysis job within the Spectrum Analyzer.
Schedule	Scheduling options, including: • **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: • **Full Scan**: Performs a comprehensive analysis of the entire spectrum. • **Custom Scan**: Set the Min Frequency and Max Frequency to precisely choose the frequency range for a more accurate spectrum analysis.
Scanning Bandwidth	The specific scanning bandwidth from the available options to adjust the spectrum analysis. **Note** Scanning Bandwidth is not applicable for PMP 450m AP.
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:

- User Management
- Cloud Anchor Account
- Server Management
- Webhooks X
- Notifications
- Audit Logs
- Syslog
- Firewall

User Management

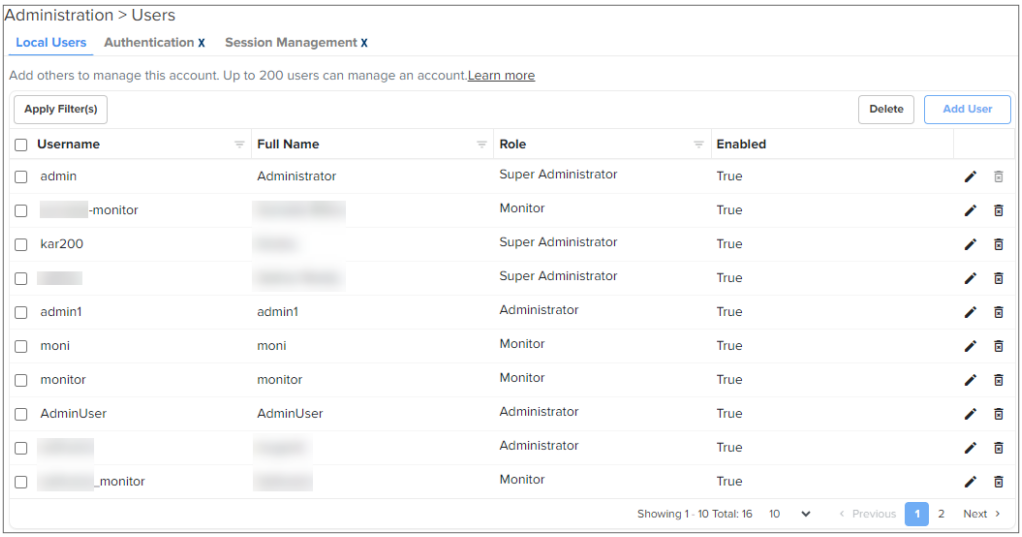
This chapter provides the following details:

- Local Users
- Authentication
- Session Management

Local Users

1. To add Local Users, navigate to **Administration > User.**

   Figure 431 *Add User*



2. Click **Add**.

For more details refer to Creating Users and Configuring User Roles.

Role-Based Access

Each user is assigned a Role that defines their authorization. On successful authentication, every request from this user is processed in light of their Role.

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 view access.
- **CPI**: CPI can onboard devices using the CBRS tool.

Note

- cnMaestro On-Premises allows the user to limit the number of concurrent sessions for each Role and display current active user sessions.
- CPI role is authorized only when **CBRS** is enabled.

Role-Mappings

The table below defines how Roles are authorized to access specific features.

Table 137 *Role-Mappings*

Feature	Description	Super Administrator	Administrator	Operator	Monitor	CPI
Authentication Services	Create and configure Authentication servers	All	None	None	None	None
API Management	API Client. administration	All	None	None	None	None
Application Operations	Application level operations such as to create, update and delete operations for Networks, Towers/Sites. Bulk device configuration	All	All	None	None	None
Application Settings	Change global application configuration and onboarding key	All	All	None	None	None
Configuration/Software Update and	Manage configuration/softwar	All	All	All	None	None

Table 137 *Role-Mappings*

Feature	Description	Super Administrator	Administrator	Operator	Monitor	CPI
Scheduled Report Jobs	e update and scheduled report related jobs					
Data Tunnel	Data Tunnel configuration	All	All	View	View (Statistics tab only)	View (Statistics tab only)
Device Operations	Device operations such as reboot device, link test, connectivity test, technical support file download, and Wi-Fi performance test	All	All	All	None (except Wi-Fi Performance test which is supported in On-Premises only)	None (except Wi-Fi Performance test which is supported in On-Premises only)
Device Overrides	Per-device configuration, including updating AP Group and applying configuration	All	All	All	None	None
Global Configuration	The ability to create and apply configuration for global features such as Templates, WLANs, AP Groups, auto-provisioning, and bulk sync configuration	All	All	View	None	None
Guest Portal	Guest Portal configuration	All	All	View	View (sessions only)	View (sessions only)
Managed Service Provider (MSP)	MSP operations such as modification of branded service, managed account and user invitations	All	View	None	None	None
	Note: Operator/Monitor users are not permitted to move devices across managed accounts.					
Monitoring	Display of monitoring data at all levels, VM Monitoring	All	All	All	View	View

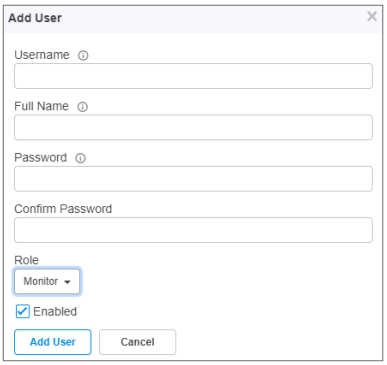
Table 137 *Role-Mappings*

Feature	Description	Super Administrator	Administrator	Operator	Monitor	CPI
Notifications	Alarms and Events management	All	All	All	View	None
Onboarding	Device approval, modifying individual device configuration, and performing software update	All	All	All	None	All
Reporting	Report generation	All	All	All	All	All
Session Management	Capability to view and logout other users sessions	All	All	None	None	None
SNMP Configuration	SNMPv2c configuration parameters	All	All	View	None	None
Software Images	Upload and delete device software images	All	All	View	None	None
Software Upgrade	Upgrade the device with the latest software	All	All	All	None	None
System Operations	System operations such as Reboot VM, change log level, system upgrade, system monitoring, uploading SSL certificate, import/export server data and server tech dump, and upload/delete device software images	All	All	None	None	None
User Management	User management operations such as manage users and roles	All	View	None	None	None

Creating Users and Configuring User Roles

To add a user:

1. Navigate to **Administration** > **Users**.
2. Click **Add User**. The following window is displayed:



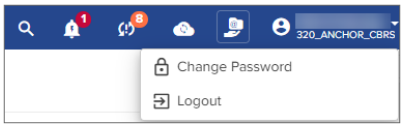
3. Enter the **Username**.
4. Enter the **Full Name**.
5. Enter the **Password**.
6. Confirm the Password by entering the same password.
7. To configure user roles, select any role for the user from the **Role** dropdown list:
   - Super Administrator
   - Administrator
   - Operator
   - Monitor
   - CPI
8. Select or clear the checkbox to enable or disable the user.
9. Click **Save**.

To edit or delete a user, click the Edit icon or the Delete icon against the user in the **Administration** > **Users** page.

Changing Password

Change Password option is available only for local users.

Figure 432 *Changing Password*



Ensure Primary Authentication is Local Users to **Change Password** option. After changing the password, the current session will get logged out.

Also, ensure there are no parallel sessions with the same users before selecting **Change Password** option.

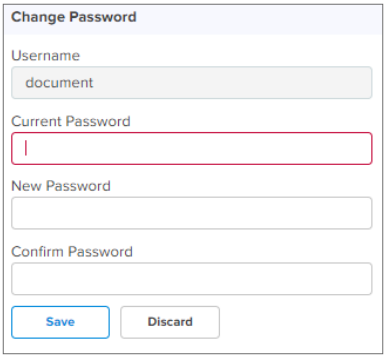
To change password:

1. From the user name dropdown in the top right corner of the UI, select **Change Password**.
2. Enter the following details:
   a. The Current Password.
   b. A new Password for this user.

c. Confirm the Password by entering the same password.

3. Click **Save**.

Figure 433 *Changing Password Parameters*



Authentication

cnMaestro On-Premises supports a Primary mode of authentication and an optional Secondary mode. If the Primary mode is Local Users (users specified in cnMaestro in the Users tab), no Secondary mode is available. If the Primary mode is an Authentication Server, then the Secondary mode will be set to Users and cannot be changed.

cnMaestro supports authentication and authorization with TACACS+, RADIUS, LDAP, and Active Directory servers, and is a cnMaestro X feature.

Authentication Server

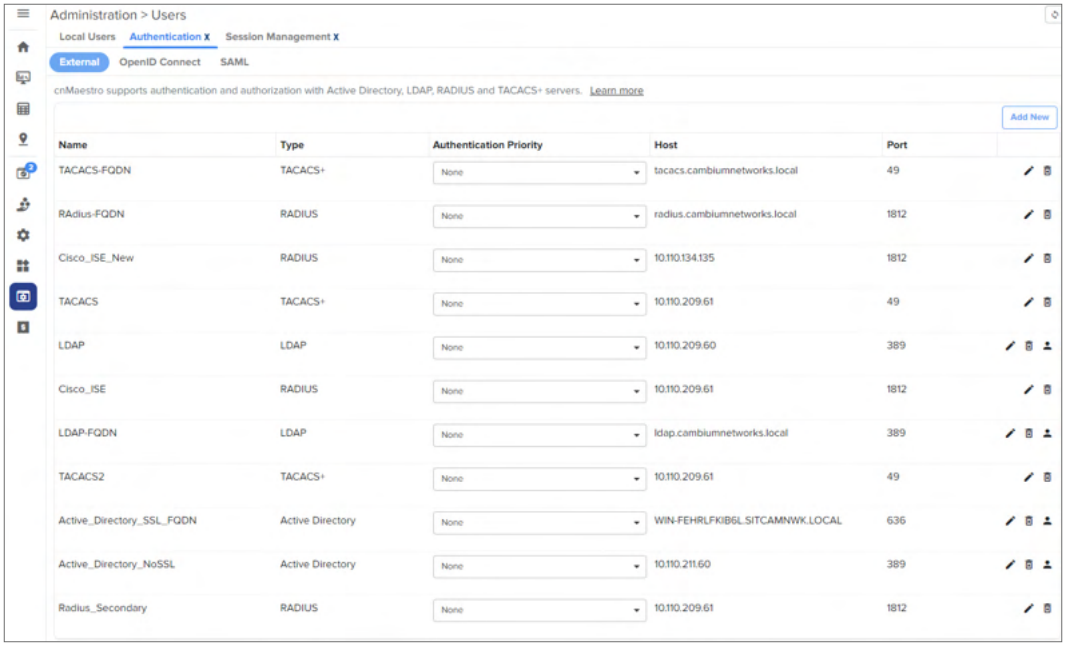
Authentication Servers can be configured only by cnMaestro Super Administrators. The following operations are available:

- Authentication Priority
- Create New Authentication Server Configuration
- Verifying the Role of the User
- Show User Groups for Active Directory

Viewing Authentication Servers

To view External Authentication which are configured in cnMaestro, navigate to **Administration** > **Users** > **Authentication**.

Figure 434 *Authentication: External*



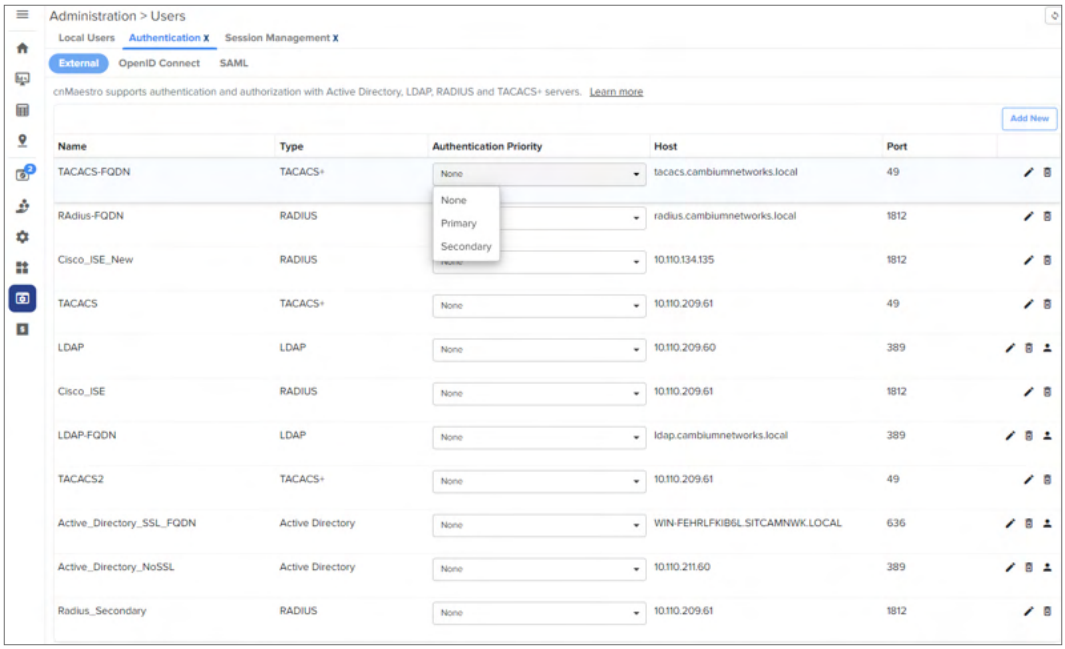
Authentication Priority

In addition to the primary server authentication, cnMaestro On-Premises now supports configuration for secondary external server for authentication. Secondary authentication and primary authentication servers should be different.

Note

The same authentication mechanism cannot be used twice. For example, If we select primary as Test-TAC-IP, then we cannot select the same in secondary authentication.

Tertiary authentication is always default to Local Users. Local Users logs in only when primary and secondary are not reachable or when the services are not being run on authentication server. If the primary server is not reachable then fallback happens to the secondary authentication server. If the secondary authentication server is not reachable then fallback happens to tertiary authentication. If primary authentication server is running properly, users belonging to primary authentication server can only be logged in. If secondary authentication server is running properly, users belonging to secondary authentication server can only be logged in.



Create New Authentication Server Configuration

1. Navigate to **Administration** > **Users** > **Authentication** > **External** > **Add New.**

   Add Authentication Server window pops up.

2. Enter authentication parameter details as shown in Table 138.

   Figure 435 *Add Authentication Server*

3. Click **Add**.

Table 138 *Authentication parameters*

Parameter	Description
Server Settings	
Authentication Server Name	Global name of the server.
Authentication Server Type	Select the type of Authentication Server from the dropdown. • TACACS+ • Active Directory • RADIUS • LDAP To configure authentication server type for Active Directory, refer to Table 139 and for LDAP, refer to Table 140.
IP Address/Host name	Enter the FQDN (Fully Qualified Domain Name) of the server or the IP address of the server.
Port	TCP port of the server. (Default value is 49).
Shared Secret	Shared secret key for communicating with the server.
Service Name	Name defined in the service configuration table configured by TACACS+ server administrator. This is used to configure service and corresponding user groups.
Role Mappings	Each of the Authentication Server user groups should be mapped to one or more cnMaestro Roles. Refer Role-Based Access section to view the supported Roles on cnMaestro. Enter the role strings that are configured in the type of authentication server. Atleast one mapping must be completed for this feature to work correctly.

Note

- TACACS+ server administrator should setup the service name and corresponding user group as per the configuration.
- The RADIUS administrator should setup user group as per configuration. The RADIUS administrator can choose a user group and the same should be configured on cnMaestro Authentication server configuration.

Table 139 *Active Directory Parameters*

Parameter	Description
BASE DN	Distinguished Name for Active Directory.
Certificate	Browse and update with certificate chain in .PEM format.
IP Address	IP address of the server.
Port	TCP port of the server (default 389). When SSL/TLS option is enabled, the port will automatically change to 636.
SSL/TLS	Select this checkbox if Active Directory connection should be secured over SSL/ TLS as LDAPS. Browse and select the Root certificate of the Active Directory server in .PEM format.

Note

The Active Directory administrator should setup user group as per configuration. The Active Directory administrator can choose a user group and the same should be configured on cnMaestro

Authentication server configuration. Examples: CN=super-admin CN=admin CN=network CN=operator

Note

If Role is not configured in TACACS+/RADIUS server or if the group is not configured in Active Directory, you cannot login to cnMaestro.

Note

A user with valid credentials will not be to able to login if:

- cnMaestro role to Authentication server's user group mapping is missing in Authentication server configuration.
- User group of the user is not configured in Authentication server.

Table 140 *LDAP Parameters*

Base DN	Base DN is generally the Admin DN used to log in to LDAP server. For example: cn=admin,dc=xyz,dc=com.
Certificate	Browse and update with certificate chain in .PEM format.
IP Address/Hostname	Provide IP address for LDAP and hostname of server if SSL/TLS is enabled.
LDAP Password	LDAP Password is the admin password used by Admin DN to log in.
Port	TCP port of the server. (Default for LDAP is 389 and for LDAPS is 636)
Suffix	Suffix is the DNS name. For example: dc= xyz, dc=com.
SSL/TSL Security	Select this checkbox if you want the LDAP connection to be secured over SSL/TLS as LDAPS. Browse and select the Root certificate of the Active Directory server in the .PEM format. **Note** • If you select the **SSL/TSL Security** checkbox, the default port will appear as **636** in the **Port** text box. • If you clear the **SSL/TSL Security** checkbox, the default port will appear as **389** in the **Port** text box.

You can perform the following action on **Authentication** page:

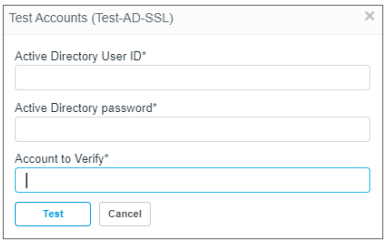
- **Edit**: Click edit (✎) icon of the specific row.
- **Delete**: Click delete (🗑) icon of the specific row.

Primary authentication order will change as Local Authentication if this server is setup as Primary Authentication under **Manage Authentication Server Authentication** section.

Verifying the Role of the User

To know and verify the role of the **Active Directory** user:

1. Navigate to **List all Authentication Servers** page.
2. Click the test (👤) icon next to any of the Active Directory type. The following window appears:



3. Provide the following details:
   - Active Directory User ID
   - Active Directory Password
   - Account to Verify
4. Click **Test**.

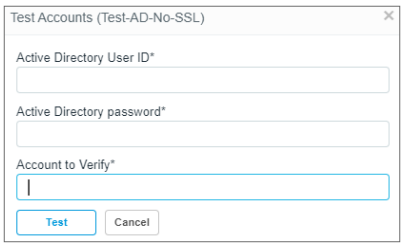
To know and verify the role of the **LDAP** user:

1. Navigate to **Administration** > **Users** > **Authentication** > **External**.
2. Click the test (👤) icon next to any of the LDAP type. The following window appears:

3. Enter the name of the **Account to Verify**.
4. Click **Test**.

Show User Groups for Active Directory

cnMaestro administrator can view user groups for Active Directory server type configuration by providing valid user credentials to login to Active Directory. The user details can then be viewed as shown below:



1. Enter **Active Directory User ID**. The User ID should be a valid string (example: user@example.com).
2. Enter **Active Directory password**.
3. Enter **Account to Verify**.

For searching the group of the user, the Users ID should follow the user@example.com format.

OpenID Connect

OpenID Connect allows users to authenticate using a third-party identity provider (IDP) service. OpenID Connect (OIDC) is an authentication protocol built on OAuth 2.0 used to securely sign in users to cnMaestro.

To authenticate user using OpenID Connect, perform the following steps:

1. Navigate to **Administration** > **Users** > **Authentication** > **OpenID Connect** tab.
2. Click **Add New**. A pop-up window is displayed.

3. Enter the parameter details as required.
4. Enable **SSL/TLS Security** option, browse and select the SSL/TLS Security certificates if available.
5. Click the (+) plus sign next to **Field Mappings**, **Role Mappings**, and **Login Experience Customization** and add the parameter details as described in Table 141.

Table 141 *OpenID Connect fields*

Parameter	Description
Connection Name	Unique identifier of the connection.
Issuer URL	Enter the URL of the OpenID Connect provider.
Client ID	Client ID provided by providers.
Client Secret	Client Secret for authentication from provider.
Callback URL	Configure the OpenID Connect provider with the Callback URL.
Field Mappings	
Role Key Name	Key name for role taken from userInfo endpoint.
Role Mappings	Map OpenID Connect provider roles to cnMaestro roles. The following roles are available: • Super Administrator • Administrator • Operator • Monitor • CPI

Table 141 *OpenID Connect fields*

Parameter	Description
	Note Atleast one mapping must be completed in order for this feature to work correctly. Refer Role-Based Access section to view the supported Roles on cnMaestro.
Login Experience Customization	
Button Display Name	Display name of the login button shown on login screen.
Button Icon URL	Destination URL of the icon. Default dimension of the icon—22 x 22 pixels (px) You can preview the login screen before adding the new connection.

6. Click **Add**.

SAML

cnMaestro supports authentication and authorization with SAML Identity Providers (IdP). It is an XML-based open-standard for transferring identity data between two parties: an Identity Provider (IdP) and a Service Provider (SP).

To authenticate users using SAML perform the following steps:

1. Navigate to **Administration** > **Users** > **Authentication** > **SAML** tab.

   SAML page is displayed.

2. Enter the parameter details as shown in Table 142.

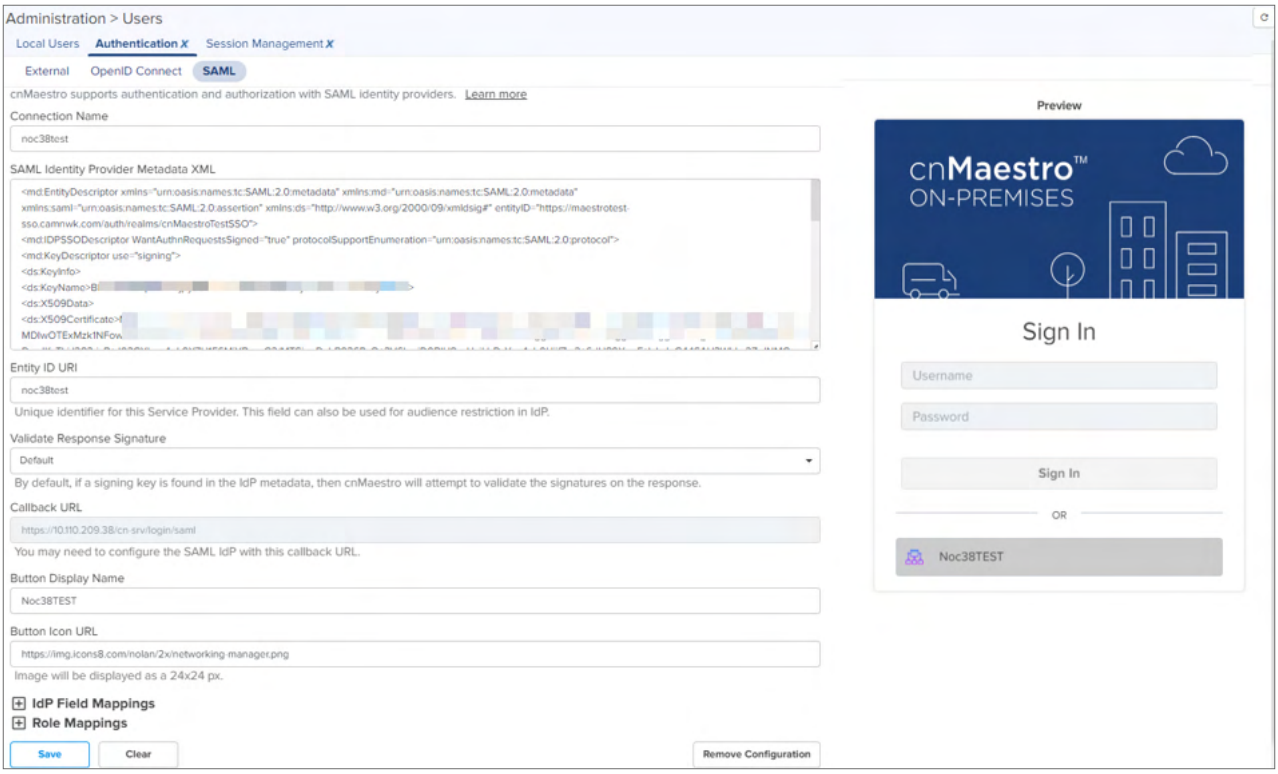


Table 142 *SAML fields*

Parameter	Description
Connection Name	Unique identifier of the connection.
SAML Identity Provider Metadata XML	Enter SAML ID Metadata in XML format.
Entity ID URI	Unique identifier for this Service Provider. This field can also be used for audience restriction in IdP.
Validate Response Signature	Validates signature on SAML response from IdP. By default, if a signing key is found in the IdP metadata, cnMaestro will attempt to validate the signatures on the response.
Callback URL	Configure the SAML IdP with this callback URL.
Button Display Name	Display name of the login button shown on login screen.
Button Icon URL	Image will be displayed as a 22x22 px.
IdP Field Mappings	Map IdP Fields/Attributes to cnMaestro fields. Username: User name of the IdP mapped field. Roles/Groups: Role taken from userInfo endpoint.
Role Mappings	Map IdP roles to cnMaestro roles. Atleast one mapping must be completed in order for this feature to work correctly. Super Administrator Administrator Operator

3. Click **Save.**

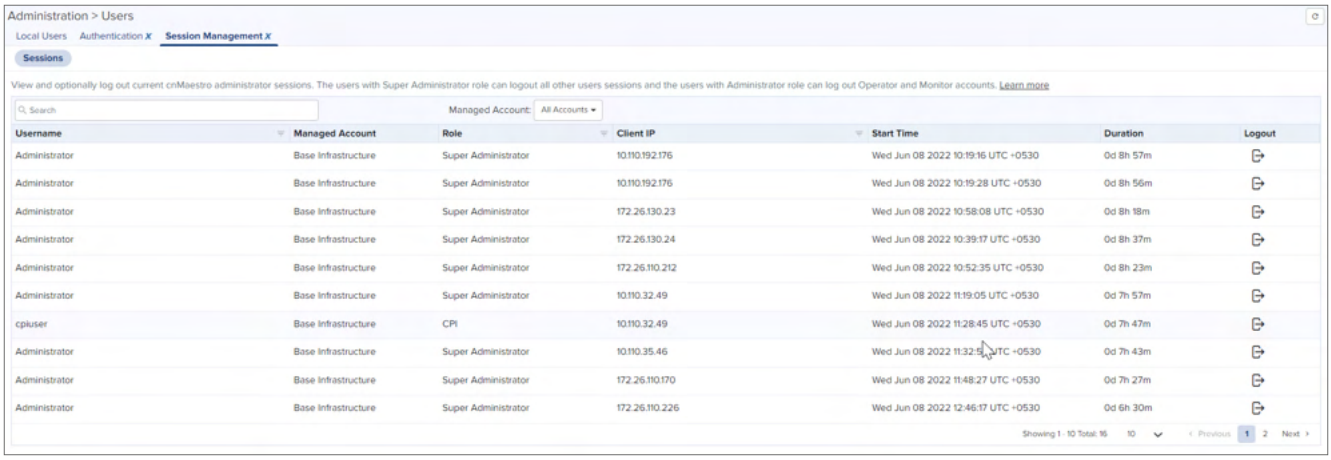
Session Management

View and optionally log out current cnMaestro administrator sessions. Users with Super Administrator Role can logout all other users sessions and users with Administrator Roles can log out Operator and Monitor accounts.

Sessions

Displays the detailed information on user sessions.

Figure 436 *Session Management > Sessions*



Note

Users, who are logged in using **OpenID Connect** and **SAML** authentication methods, are automatically logged out after 24 hours.

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.

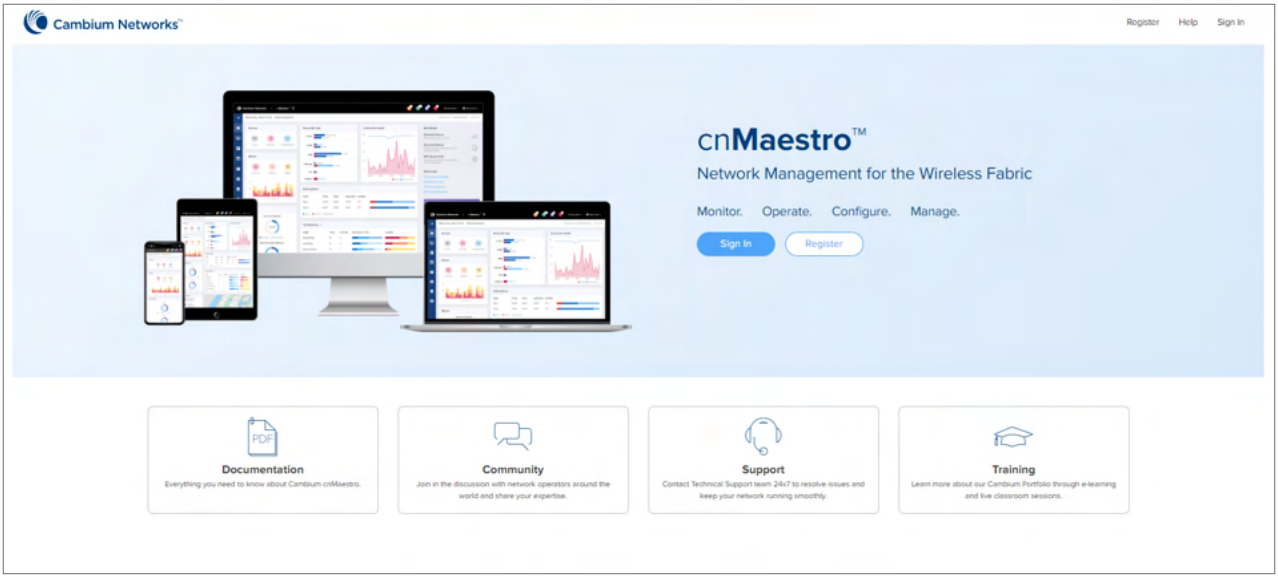
Manage Instances describes the following topics:

- 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:

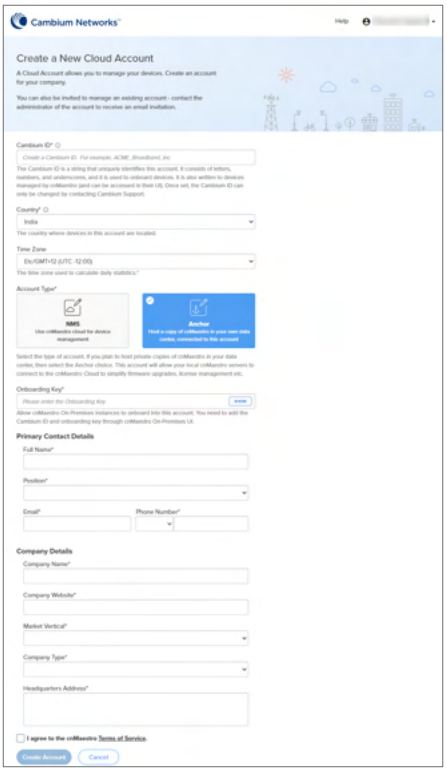
1. Log in to the cnMaestro UI, https://cloud.cambiumnetworks.com.



2. Click **Add New Account**.

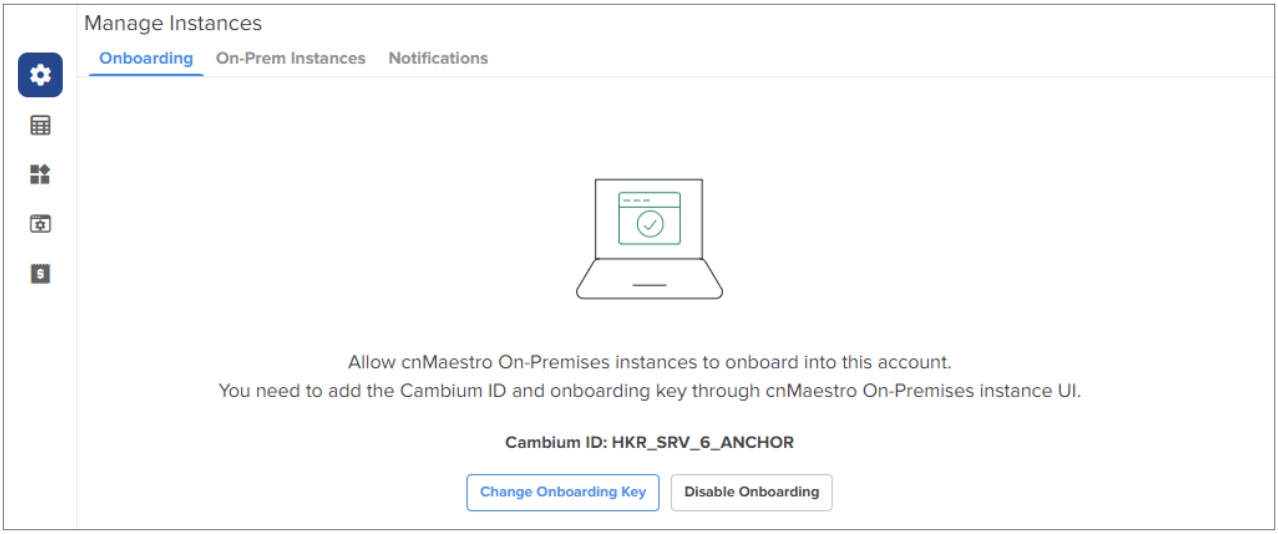
   The **Create a New Cloud Account** page is displayed.

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



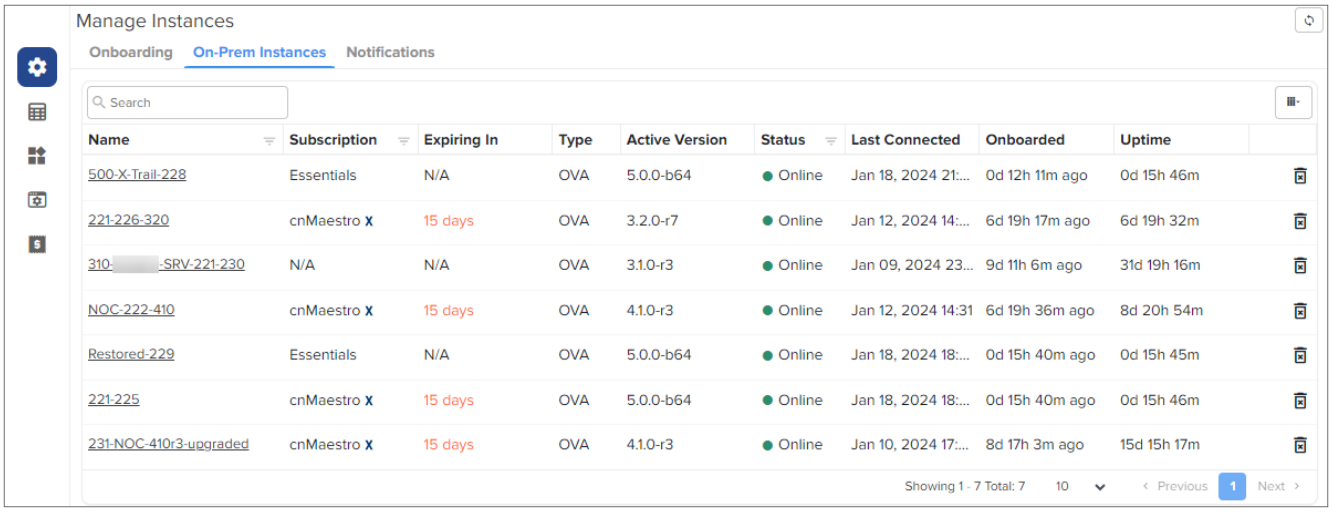
4. Enter the On-Premises **Onboarding Key**.
5. Configure the parameters under the **Primary Contact Details** and **Company Details** sections.
6. Read the cnMaestro Terms of Service and select the **I agree to the cnMaestro Terms of Service** checkbox.
7. Click **Create Account**.
8. When the Anchor Account is created, an Onboarding Key must be set to allow On-Premises instances to connect.
9. Navigate to the **Manage Instances** page as shown below, where you can change the onboarding key and/or disable onboarding.

   This key must be entered in the cnMaestro On-Premises UI to connect to the Anchor Account.

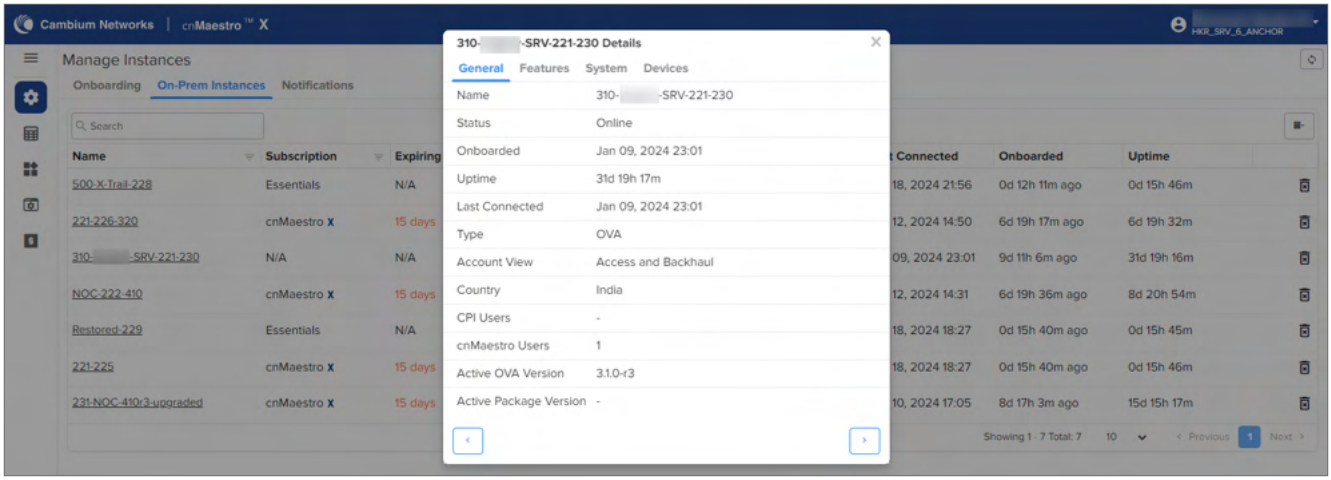


On-Premises Instances

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.

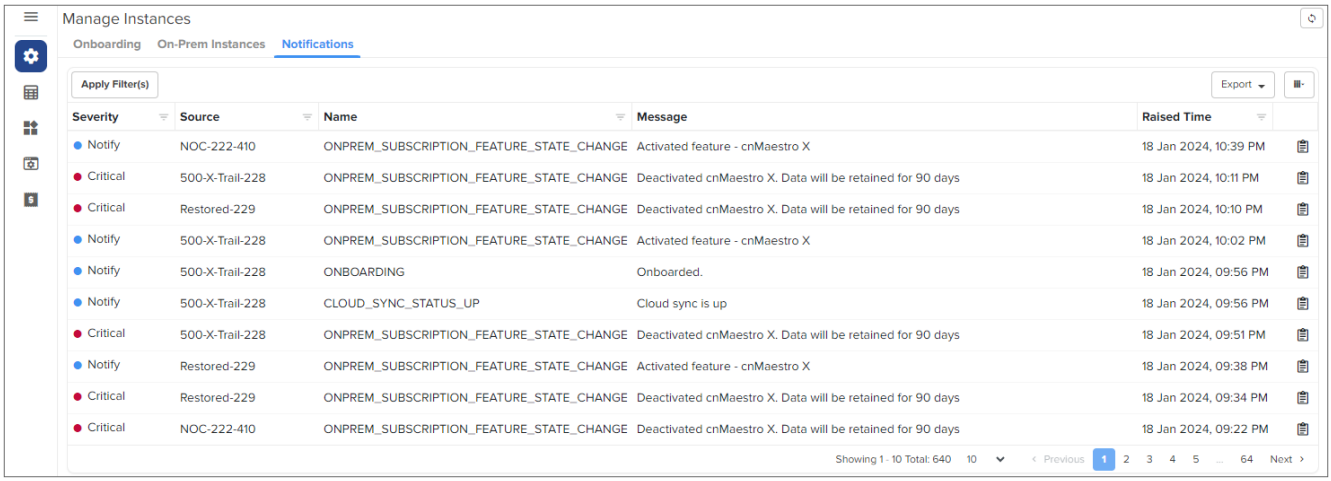


By clicking the instance host name, you can see the On-Premises server details such as General, Features, System, and CBRS:



Notifications

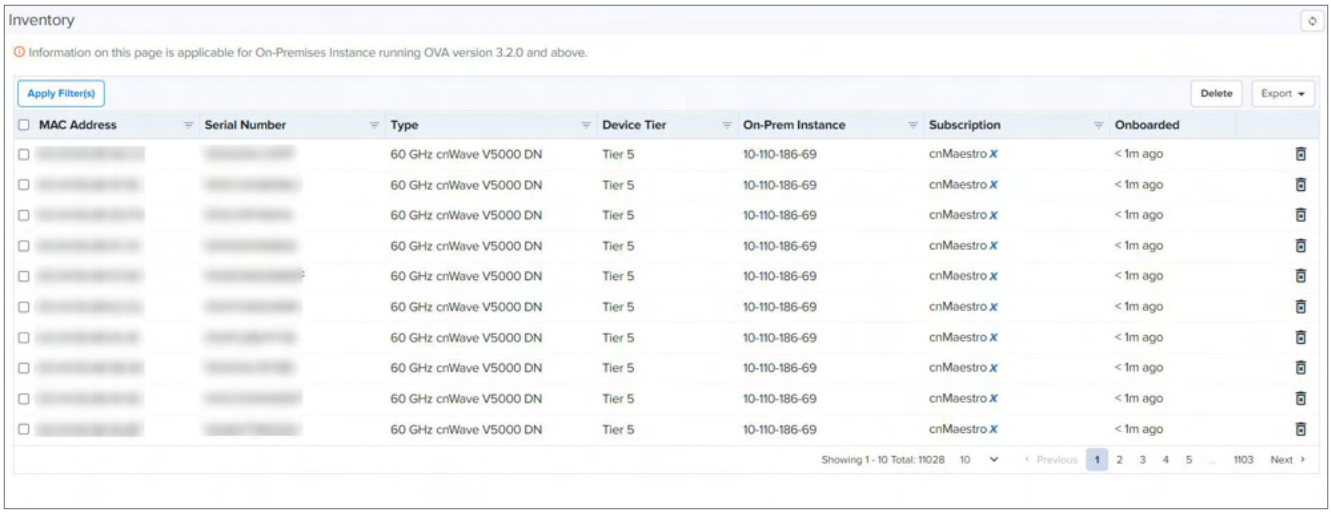
Notification page displays the history of the most recent events notification of On-Premises instances with **Severity**, **Source**, **Name**, **Raised Time**, and **Message**.



Click View Details to view the Event Details as shown below:

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.



Administration

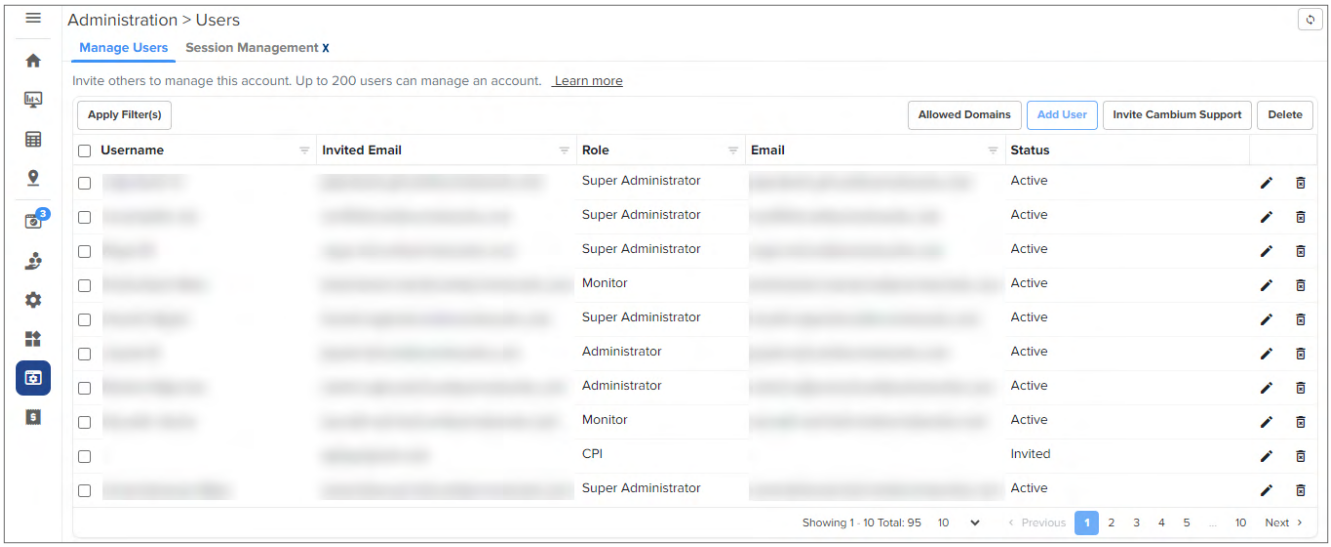
Administration provides the following details:

- 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 437 *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 Add User window is displayed.

3. Enter the email addresses in the **Email** text box.

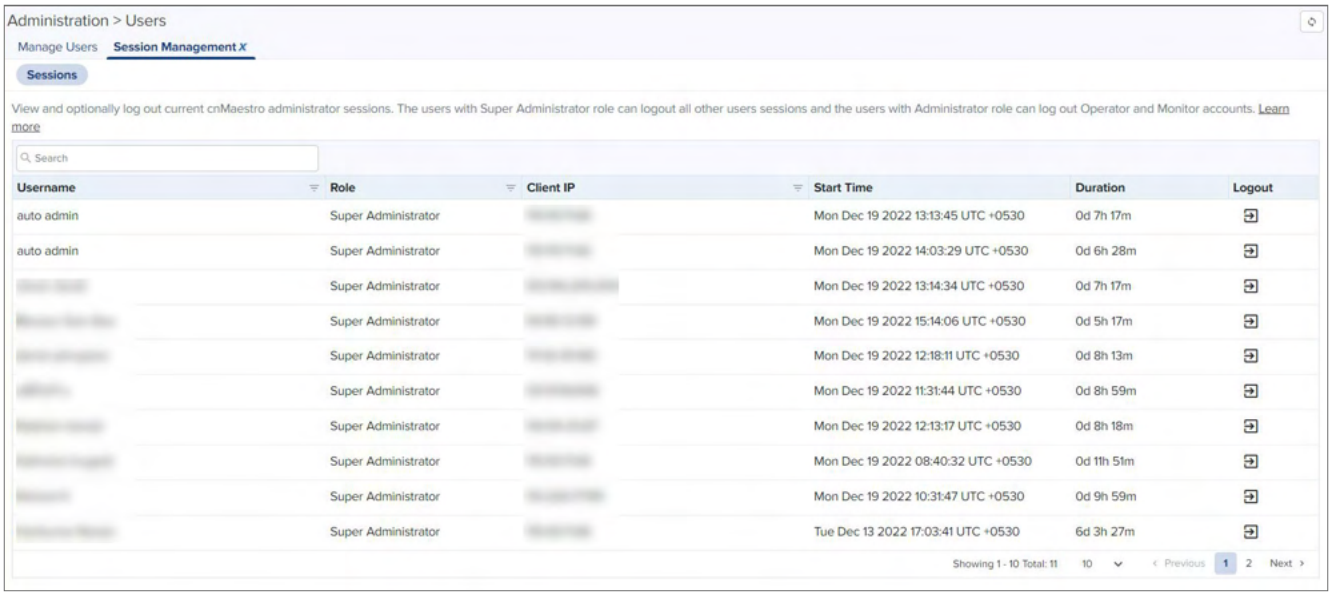
You can invite multiple users simultaneously by entering their email IDs in the Email text box or copy and paste the multiple email IDs as a comma-separated input.

4. Click **Send** 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.



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	

Network Services

Network Services provide the following details:

- CBRS

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.

Manage Subscriptions

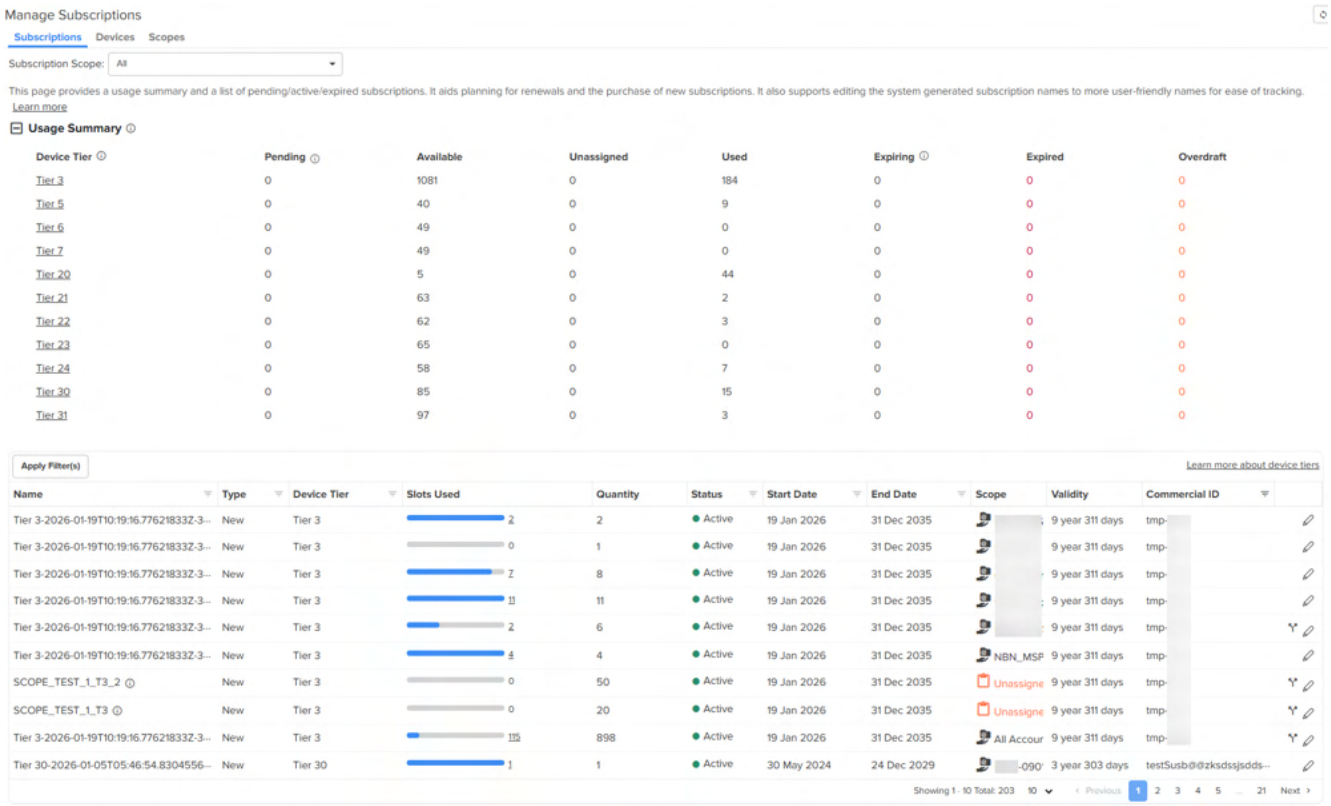
Manage Subscriptions provide the following details:

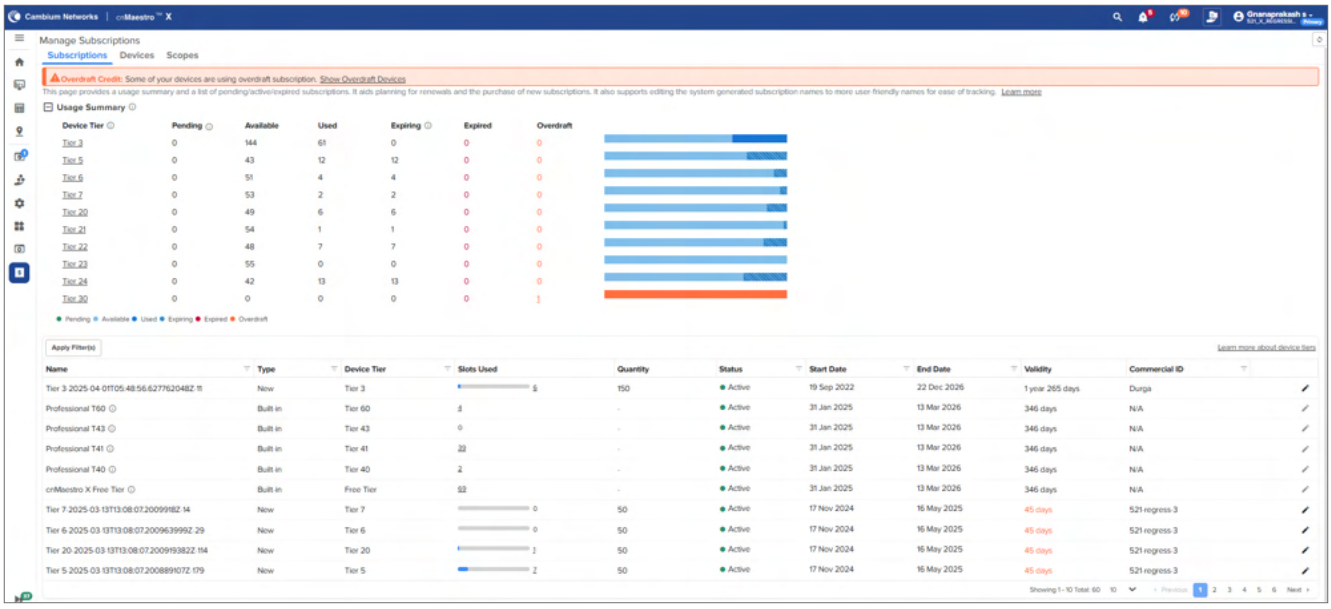
- Subscriptions
- Devices

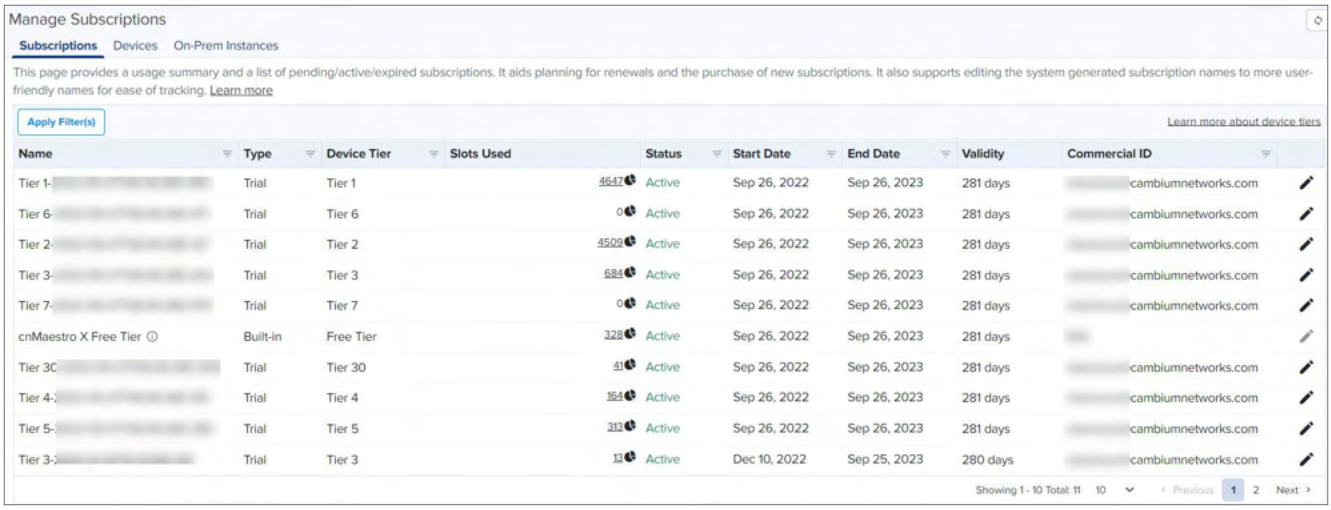
- On-Premises Instances

Subscriptions

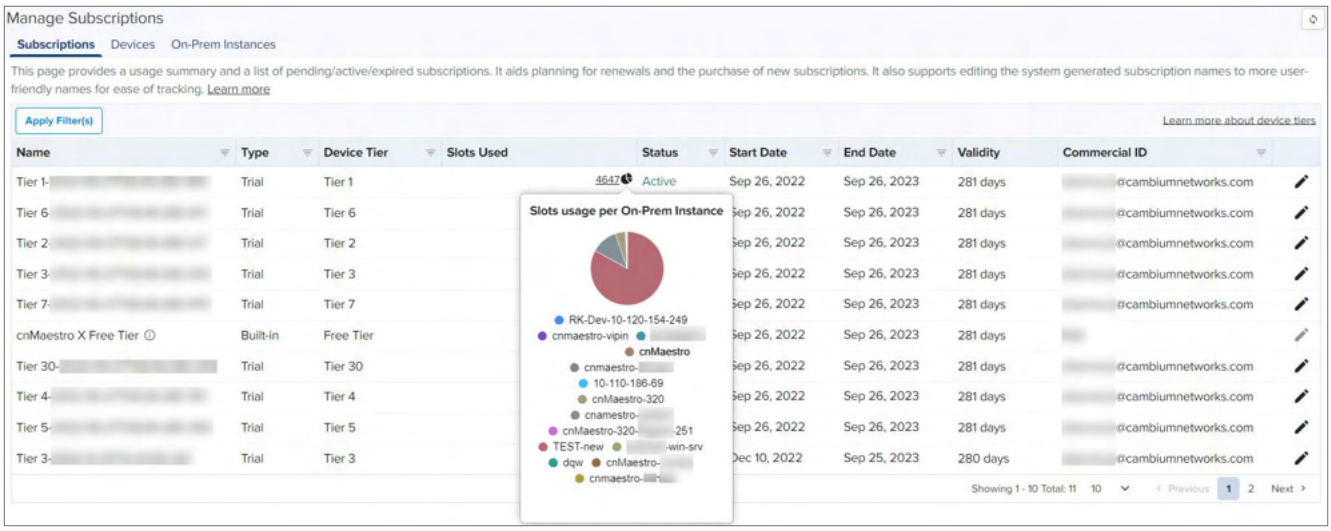
Subscriptions page describes about the usage summary and a list of pending, active, and expired subscriptions. It aids planning for renewals and the purchase of new subscriptions.







By clicking the slot ( ) icon, you can view the Slot usage per On-Premises Instance as shown below:

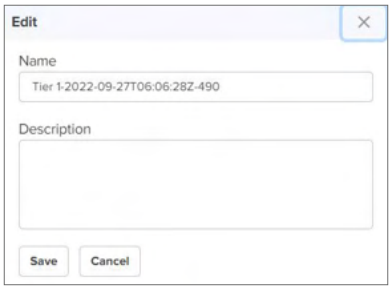


It also supports editing the system generated subscription names to more user-friendly names for ease of tracking.

To edit the **Subscriptions** perform the following steps:

1. click edit ( ) icon.

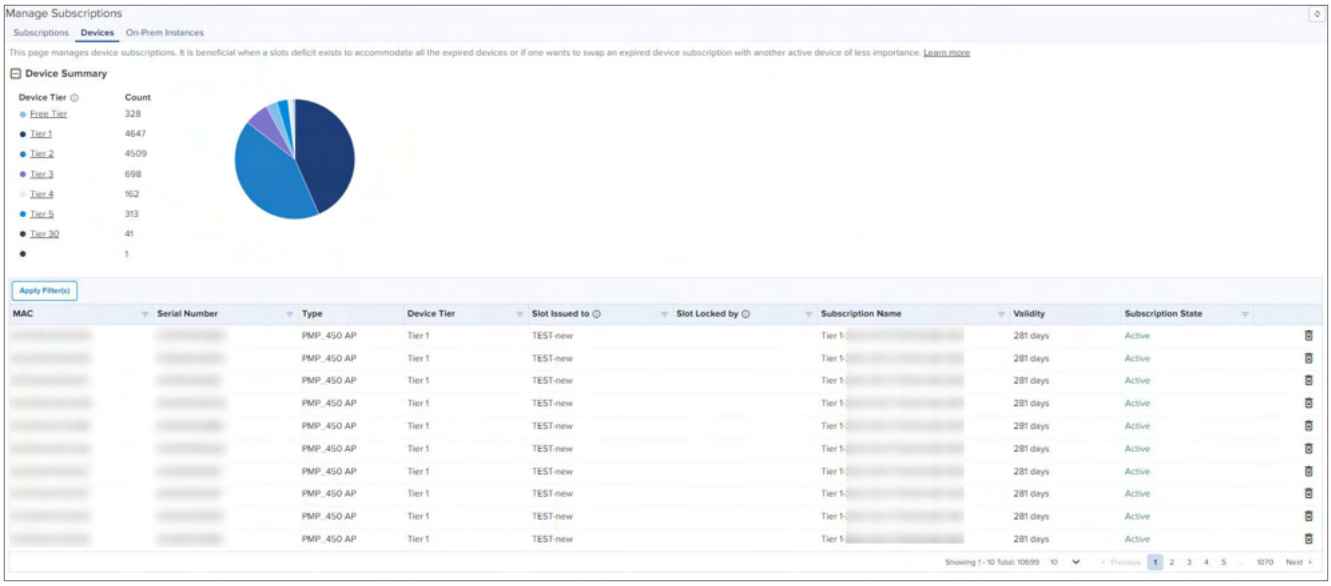
   Edit window pops up as shown below.



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.

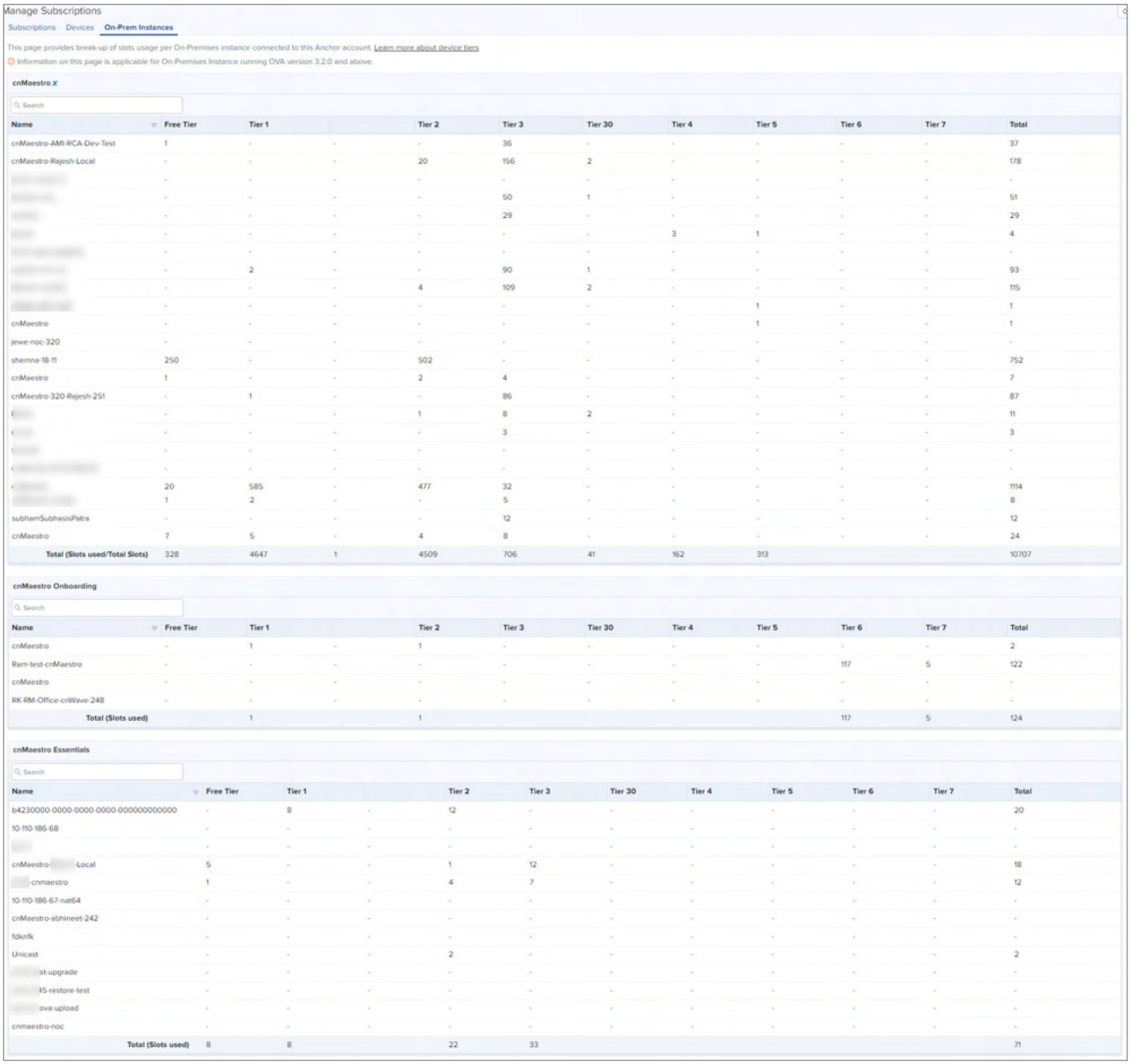


On-Prem Instances

Note

On-Prem Instances page is applicable for On-Premises instances running OVA version 3.2.0 and above.

On-Prem Instances page provides break-up of slots usage per On-Premises instance connected to this Anchor account such as cnMaestro X, Onboarding, and Essentials.



Manage Subscriptions

Subscriptions | Devices | On-Prem Instances

This page provides break-up of slots usage per On-Premises instance connected to this Anchor account. Learn more about device tiers

Information on this page is applicable for On-Premises Instance running OVA version 3.2.0 and above.

cnMaestro X

Name	Free Tier	Tier 1		Tier 2	Tier 3	Tier 30	Tier 4	Tier 5	Tier 6	Tier 7	Total
cnMaestro-AMI-RCA-Dev-Test	1	-	-	-	36	-	-	-	-	-	37
cnMaestro-Rajesh-Local	-	-	-	20	156	2	-	-	-	-	178
[illegible]	-	-	-	-	-	-	-	-	-	-	-
[illegible]	-	-	-	-	50	1	-	-	-	-	51
[illegible]	-	-	-	-	29	-	-	-	-	-	29
[illegible]	-	-	-	-	-	-	3	1	-	-	4
[illegible]	-	-	-	-	-	-	-	-	-	-	-
[illegible]	-	2	-	-	90	1	-	-	-	-	93
[illegible]	-	-	-	4	109	2	-	-	-	-	115
[illegible]	-	-	-	-	-	-	-	1	-	-	1
cnMaestro	-	-	-	-	-	-	-	1	-	-	1
jewe-noc-320	-	-	-	-	-	-	-	-	-	-	-
shemna-18-11	250	-	-	502	-	-	-	-	-	-	752
cnMaestro	1	-	-	2	4	-	-	-	-	-	7
cnMaestro-320-Rajesh-251	-	1	-	-	86	-	-	-	-	-	87
[illegible]	-	-	-	1	8	2	-	-	-	-	11
[illegible]	-	-	-	-	3	-	-	-	-	-	3
[illegible]	-	-	-	-	-	-	-	-	-	-	-
[illegible]	-	-	-	-	-	-	-	-	-	-	-
[illegible]	20	585	-	477	32	-	-	-	-	-	1114
[illegible]	1	2	-	-	5	-	-	-	-	-	8
subhamSubhasisPatra	-	-	-	-	12	-	-	-	-	-	12
cnMaestro	7	5	-	4	8	-	-	-	-	-	24
Total (Slots used/Total Slots)	328	4647	1	4509	706	41	162	313			10707

cnMaestro Onboarding

Name	Free Tier	Tier 1		Tier 2	Tier 3	Tier 30	Tier 4	Tier 5	Tier 6	Tier 7	Total
cnMaestro	-	1	-	1	-	-	-	-	-	-	2
Ram-test-cnMaestro	-	-	-	-	-	-	-	-	117	5	122
cnMaestro	-	-	-	-	-	-	-	-	-	-	-
RK-RM-Office-cnWave-248	-	-	-	-	-	-	-	-	-	-	-
Total (Slots used)		1		1					117	5	124

cnMaestro Essentials

Name	Free Tier	Tier 1		Tier 2	Tier 3	Tier 30	Tier 4	Tier 5	Tier 6	Tier 7	Total
b4230000-0000-0000-0000-000000000000	-	8	-	12	-	-	-	-	-	-	20
10-110-186-68	-	-	-	-	-	-	-	-	-	-	-
[illegible]	-	-	-	-	-	-	-	-	-	-	-
cnMaestro-[illegible]-Local	5	-	-	1	12	-	-	-	-	-	18
[illegible]-cnmaestro	1	-	-	4	7	-	-	-	-	-	12
10-110-186-67-nat64	-	-	-	-	-	-	-	-	-	-	-
cnMaestro-abhineet-242	-	-	-	-	-	-	-	-	-	-	-
fdknfk	-	-	-	-	-	-	-	-	-	-	-
Unicast	-	-	-	2	-	-	-	-	-	-	2
[illegible]st-upgrade	-	-	-	-	-	-	-	-	-	-	-
[illegible]15-restore-test	-	-	-	-	-	-	-	-	-	-	-
[illegible]ova-upload	-	-	-	-	-	-	-	-	-	-	-
cnmaestro-noc	-	-	-	-	-	-	-	-	-	-	-
Total (Slots used)	8	8		22	33						71

cnMaestro X - lists the devices that are subscribed and upgraded to cnMaestro X.

Onboarding - lists the devices that are upgraded from On-Premises 3.1.0 and in cnMaestro Trial period.

Essentials - lists the devices that are in the Essentials.

Server Management

This chapter provides the following details:

- Monitoring
- Settings
- Operations
- Update cnMaestro Software

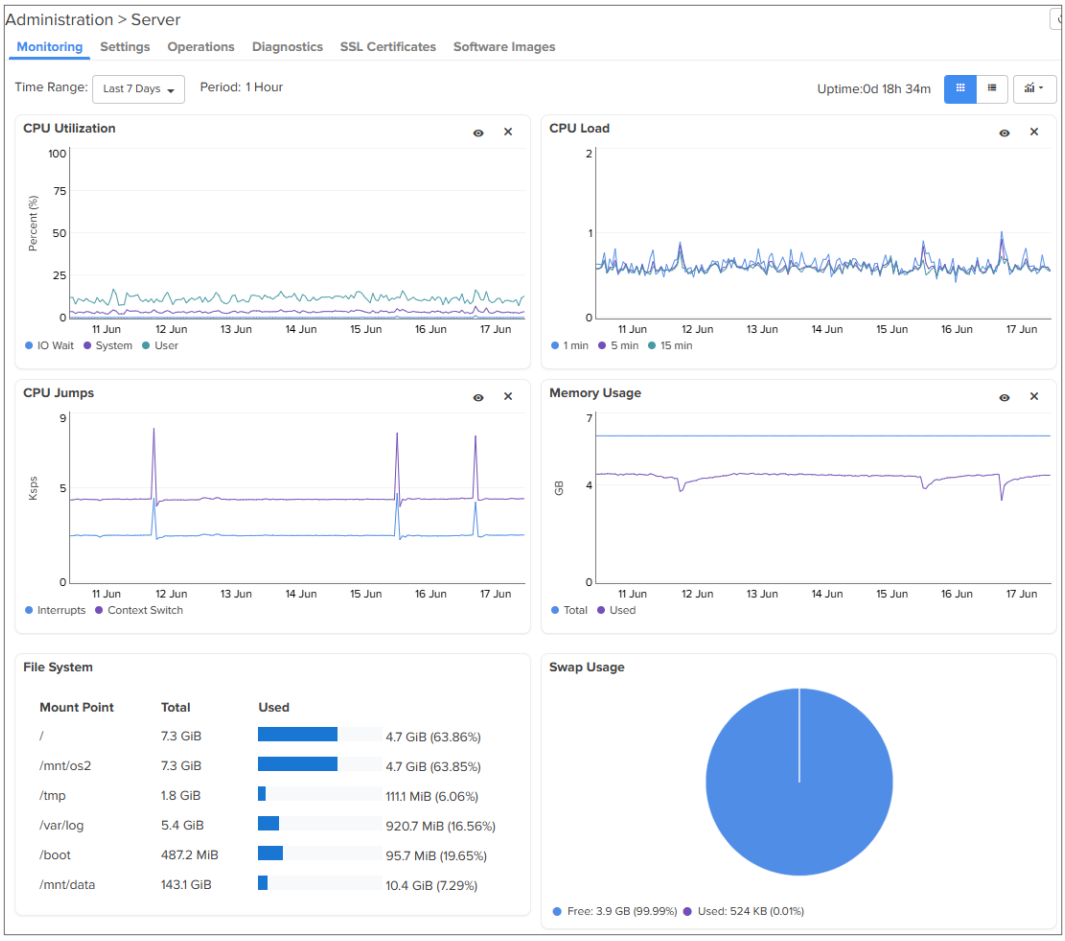
- System Backup
- In-System Upgrade
- Diagnostics
- Certificate Management
- Managing Software Images

Monitoring

The **Server** tab provides monitoring and operations for the virtual machine instance.

Navigate to **Administration > Server.**

Figure 438 *Monitoring cnMaestro Server Instance*



Settings

This section provides the following details:

- Basic
- Configure NTP Server
- Configure Email Server
- Login Security Banner

Basic

The user can enter the **System Name** and enable **SSH access to cnMaestro server**.

> **Note**
>
> - In High Availability (HA) enabled environment, SSH access is enabled only for the primary server.
> - Enabling SSH access is unnecessary for regular operations and can increase the attack surface, posing potential security risks. It should only be enabled when required for specific troubleshooting or configuration tasks.

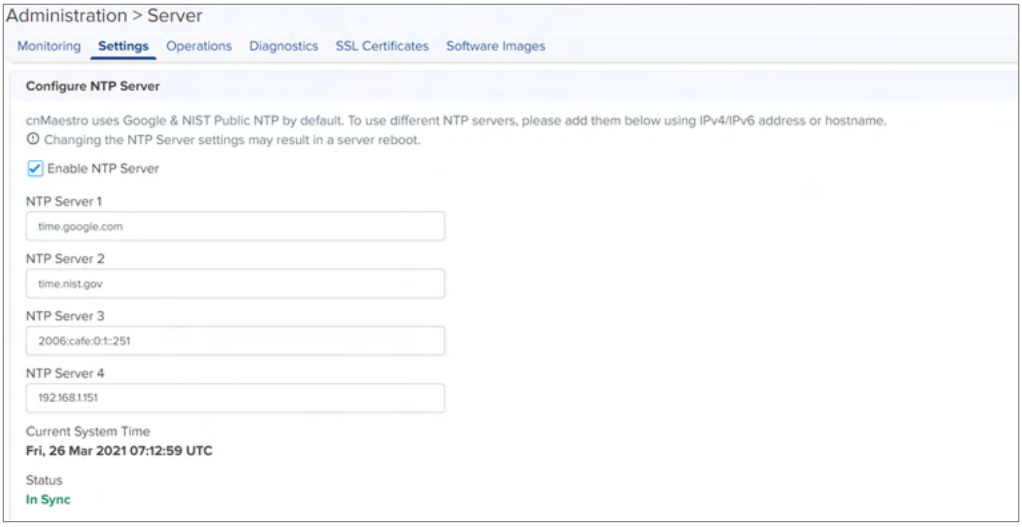
Figure 439 *System Name*

Configure NTP Server

The user can configure the NTP Server with hostname or IP address.

To configure the NTP server:

1. Navigate to **Administration** > **Server** > **Settings** > **Configure NTP Server** tab.
2. Select **Enable the NTP Server**.
3. Enter **Host Name** or **IP Address**. It displays **Current System Time** and **Status** of the server.



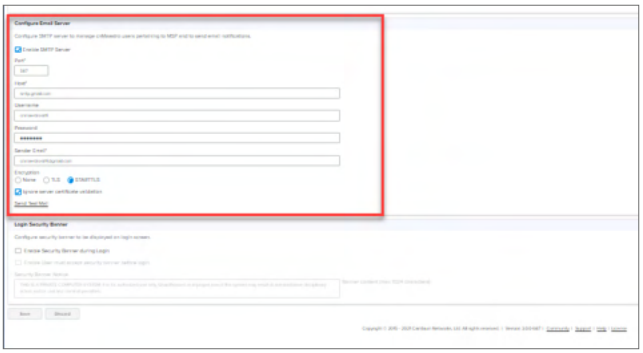
Configure Email Server

The user can configure the email server to send and receive email messages.

To configure the email server:

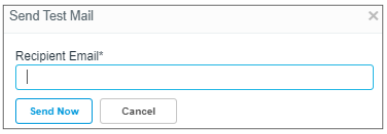
1. Navigate to **Administration** > **Server** > **Settings** > **Configure Email Server** tab.

   Figure 440 *Email Server*

2. Select the **Enable SMTP Server**.
3. Enter the **Port** number.
4. Enter name of the **Host**.
5. Enter the **Username**.
6. Enter the **Password**.
7. Enter the **Sender Email**.
8. To send the email in an encrypted format, select any one of the following:
   - **None:** Uses port number 587 for communication which is not secured.
   - **TLS:** Uses port number 465 for encrypted communication. When this option is selected, you must upload the CA certificate in the **CA Certificate** field.
   - **STARTTLS**: For encrypted communication on port number 587, choose STARTTLS option. When this option is selected, upload the CA certificate in the **CA Certificate** field.
9. If no certificate validation is required, select the **Ignore Server Certificate Validation** checkbox.
10. Click **Send Test Email**.

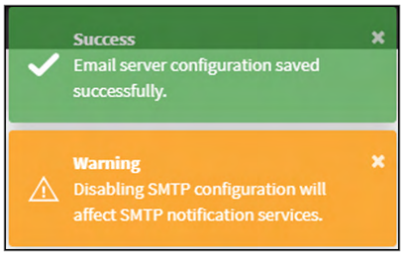
    Figure 441 *Specifying email address*

11. Enter the **Recipient Email**.
12. Click **Send Now**.

Note

When user tries to disable SMTP configuration a warning message pops up.



Notifications

The Email Notifications feature allows the Super Administrator and the Administrator to add subscribers (Email IDs) for receiving different types of Email alerts.

For information and steps about configuring notifications in cnMaestro On-Premises, see Notifications.

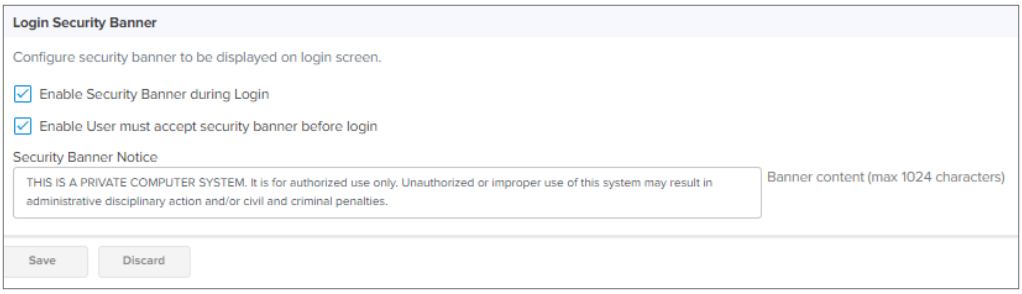
Login Security Banner

For security purpose, a banner can be displayed before the login window appears in cnMaestro On-Premises.

To enable the security banner, perform the following steps:

1. Navigate to **Administration** > **Server** > **Settings** > **Security Banner**.

   Figure 442 *Enabling Security Banner*

2. Enable Security Banner during Login

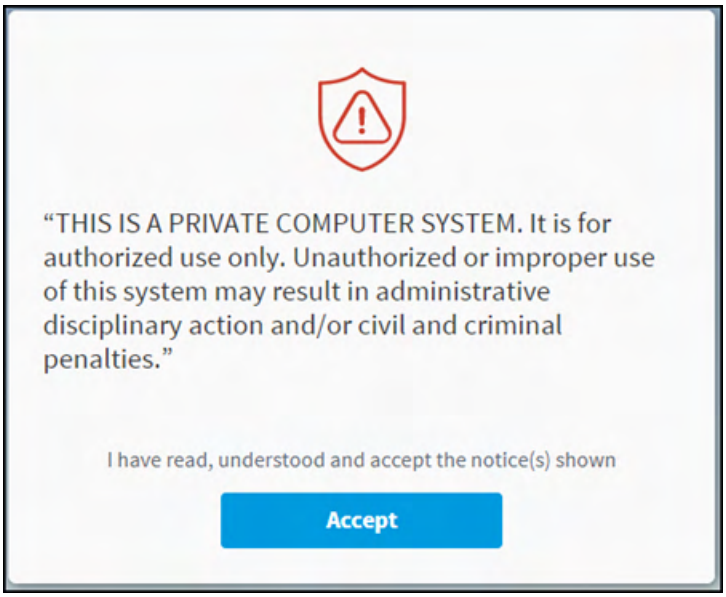
   User must accept Security Banner before login.

3. Enter the **Security Banner Notice**.

4. Click **Save.**

   A sample security banner window is shown below:

   Figure 443 *Security Banner*

5. Click **Accept**.

The login window is displayed.

Operations

This section provides the following details:

- Reboot Virtual Machine
- Update cnMaestro Software
- System Backup
- In-System Upgrade

Reboot Virtual Machine

Warning:

All devices goes offline when the virtual devices is rebooted.

Update cnMaestro Software

Package Types

cnMaestro On-Premises software is released in two forms:

OVA Image

The OVA image contains all software needed to run the cnMaestro application. It is installed on a virtual machine and releases intermittently to update system software. Moving to a new OVA image requires an in-system upgrade of the current OVA (no import and export of data is required after the 2.0 release). The OVA is approximately 3.0 GB in size.

Package Upgrade

The package file is installed on top of an OVA image; and updates the cnMaestro application. Packages releases more frequently and provide a faster upgrade path for enhancements. Packages can be installed by downloading them from Cambium and uploading them through the UI (at **Administration** > **Server** > **Operations**).

Note

1. The general update flow will be an OVA file followed by package releases. For significant system-level updates, a new OVA file will be generated.
2. Refer to Cloud connectivity page for download of software from cnMaestro Cloud.

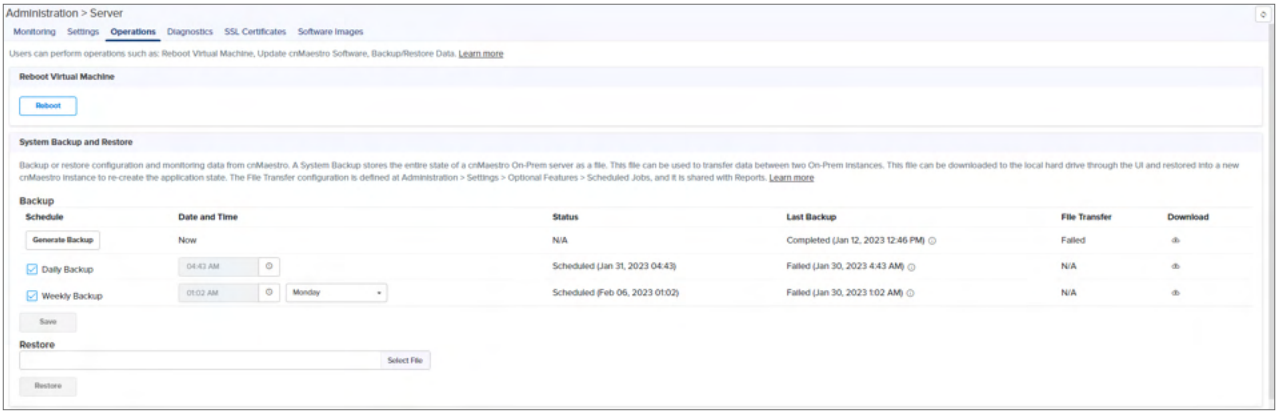
System Backup

Backup or restore configuration and monitoring data from cnMaestro. A System Backup stores the entire state of a cnMaestro On-Premises instances as a file. This file can be used to transfer data between two On-Premises instances. This file can be downloaded to the local hard drive through the UI and restored into a new On-Premises instance to re-create the application state.

The File Transfer configuration is defined at **Administration** > **Settings** > **General > Optional Features** > **Scheduled Jobs**, and it is shared with Reports

To generate the system backup job, perform the following steps:

1. Navigate to **Administration > Server > Operations> System Backup and Restore**.

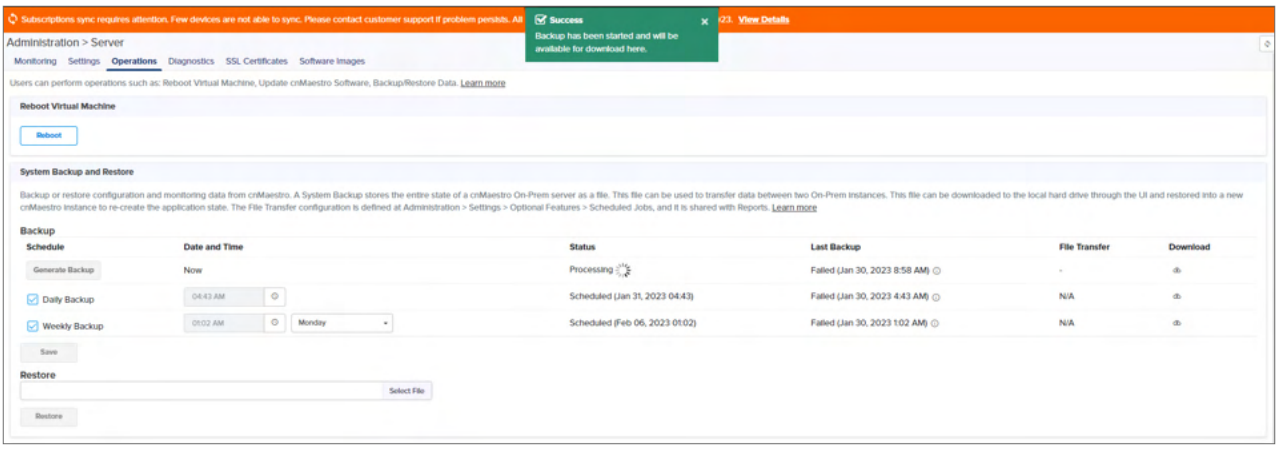


2. Select any one of the following options:
   - **Daily Backup:** Allow you to set a time not exceeding the current system time. The backup files will be generated every day at the scheduled time.
   - **Weekly Backup**: The backup files will be generated for a specified day and time weekly.
3. Click **Save**.

> **Note**
>
> When the new backup is generated the old backup will be deleted.

4. Click **Generate Backup**

   Success window pops up.



5. Click the download icon to download the last backup file.

Restore Backup

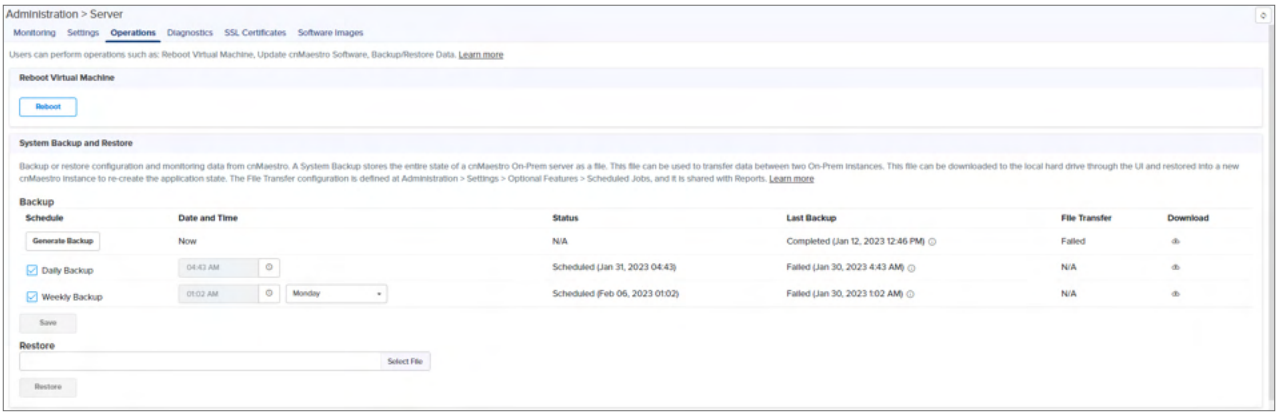
The user can now restore the downloaded system backup file to the new On-Premises instance to recreate the same application state

Before backup and restore user need to verify the following procedures:

- User need to ensure the target is in the same subscription mode as the source backup.
- If the source has active subscriptions with connected Cloud Anchor account. Then during the backup and restore the source and target will be sharing the same subscriptions. If the source/target is deleted, then the sharing is removed. Until the sharing is there, the source is marked as inactive and you cannot do any other restore on these instances. Both On-Premises must be online to delete any device. If user cannot make anyone of the instance online, contact the Cambium Networks support.
- If the source/target is in Onboarding X trial version, then restoring is not allowed.

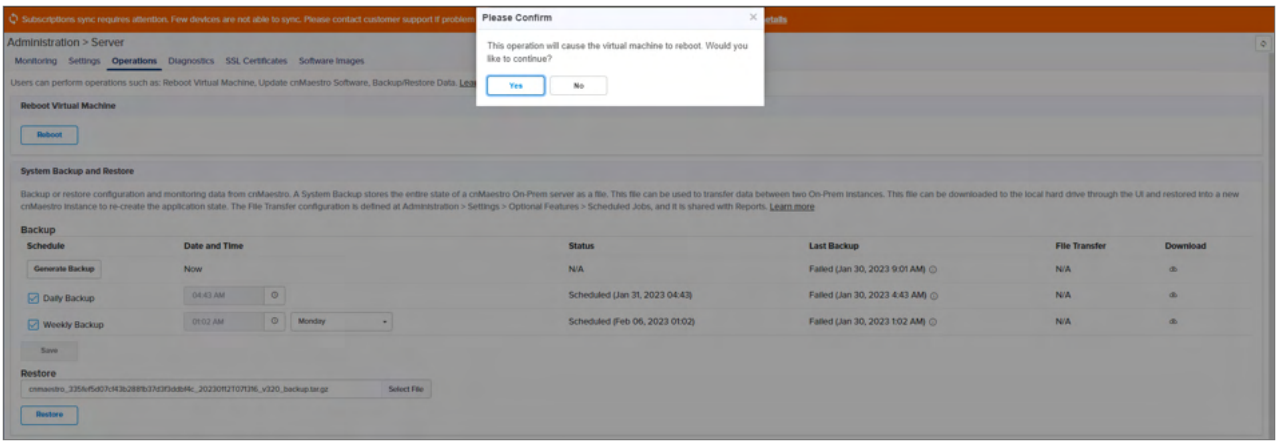
To restore the backup, perform the following steps:

1. Navigate to **Administration > Server** > **Operations** > **Restore**.



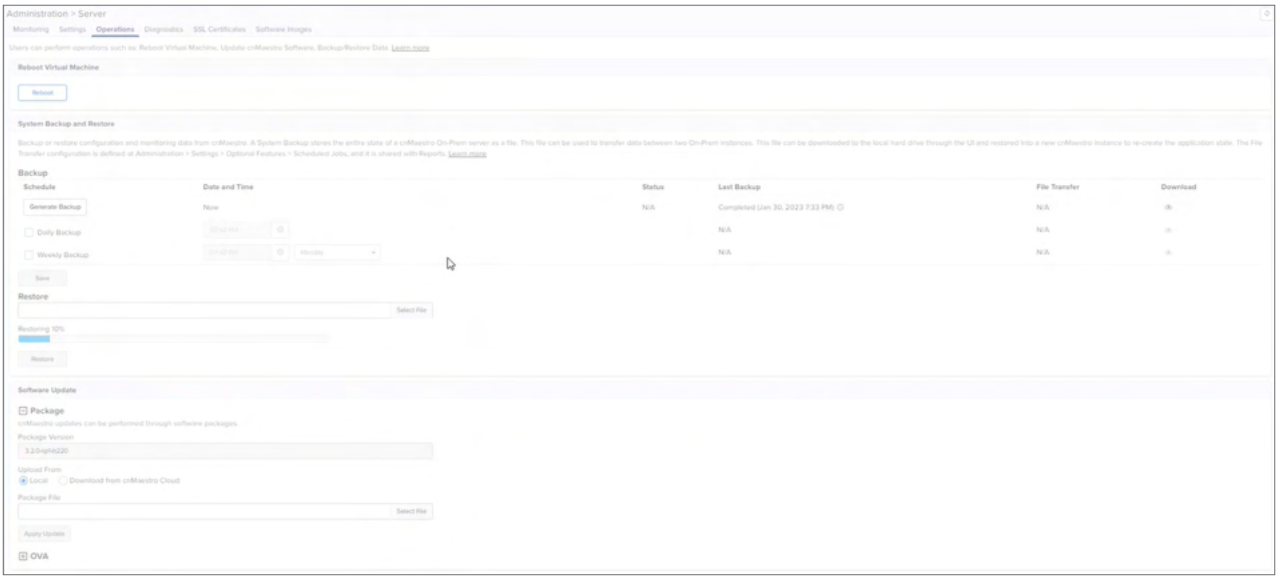
2. Click **Select File** to select the downloaded backup file.
3. Click **Restore**.

   Please Confirm window pops up.



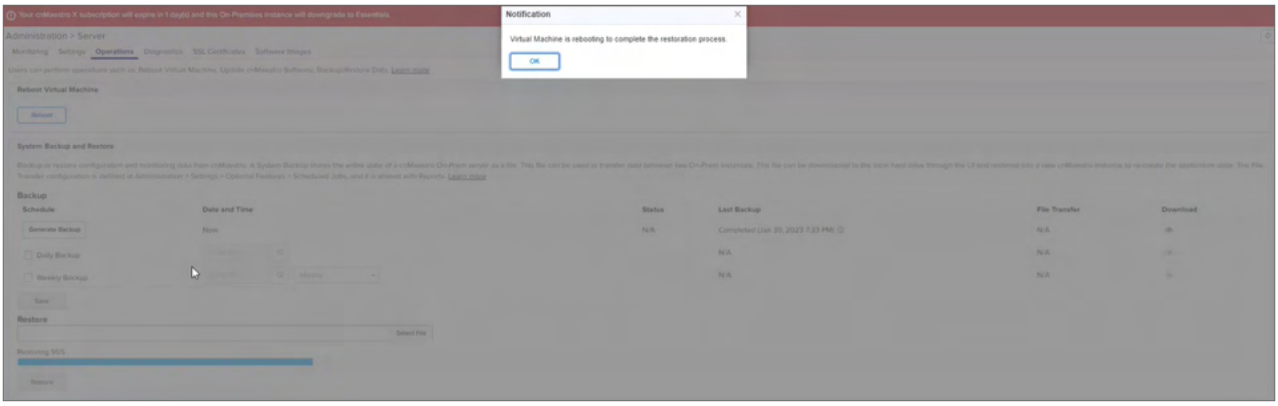
4. Click **Yes**.

   When the backup restore is initiated white overlay appears on the UI.



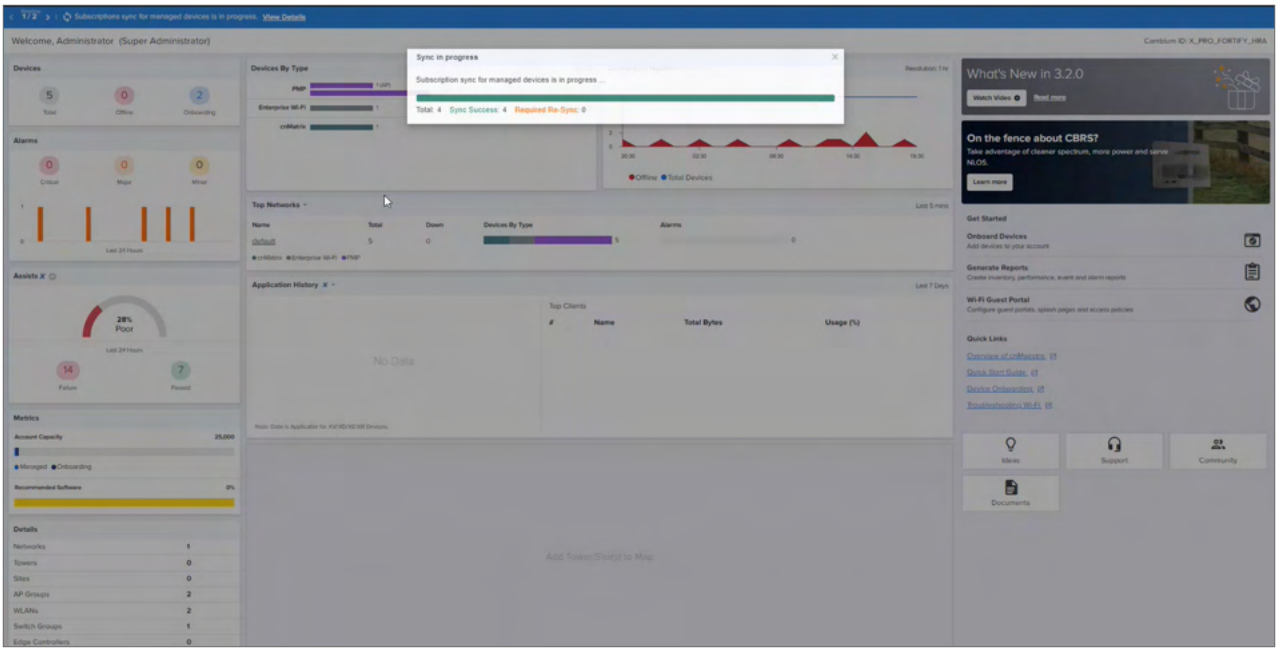
5. The **Notification** window pops up.
6. Click **OK** to complete the restoration process.

   System reboots automatically.



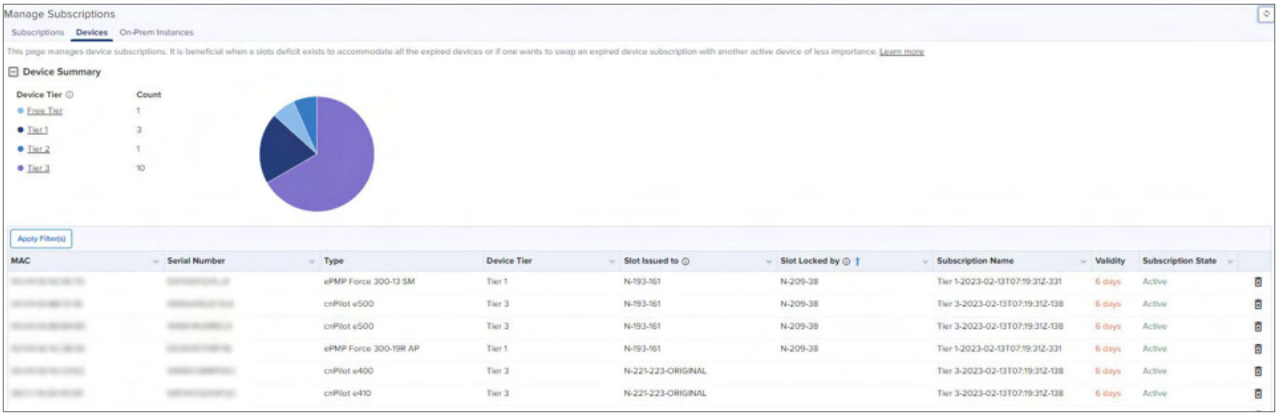
7. When **Sync in progress** notification banner is displayed.

   Click **View Details**, to view the **Sync in progress** details.

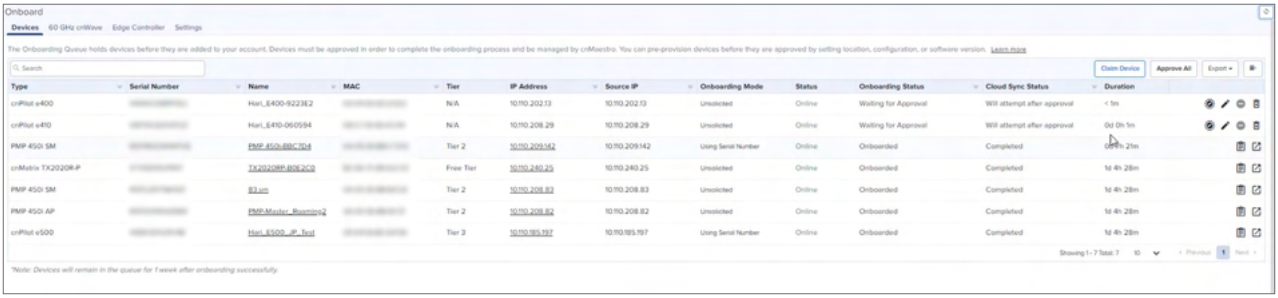


8. While restore is in progress on the anchor account devices page, you can view the Slot locked by and Slot Issued to status of the devices as shown in .

   Devices page

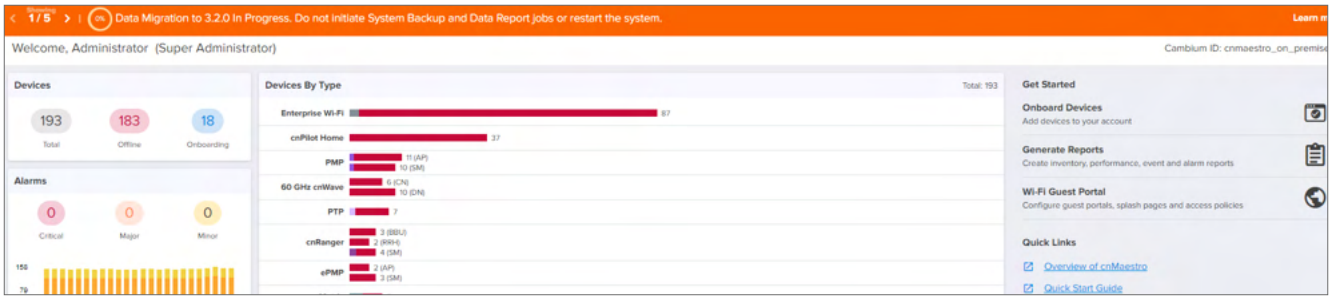


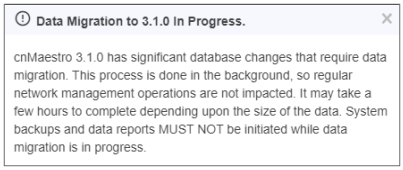
   When the restore is completed the devices will be onboarded into the **Onboard** page.



Data Migration

Data migration to 3.2.0 from a lower version takes time depending upon the size of backup file. During migration, the below banner is displayed:





In 3.2.0 release, when we import the backup data, the following banner displays in the top of cnMaestro On-Premises UI, and it will be there until the indexing completes.

Note

- The indexing occurs whenever the user navigates to different UI pages. For example, when the user navigates to WLAN-AP group page, the respective indexing will be created and the banner will be displayed in the top of the UI.
- Database indexing pauses during the database migration and emails once indexing the webhooks.
- Do not Import data or Export data when the Migration banner is running.

OVA Update Process

Updating an OVA image can be managed through the following process (which assumes the hardware has enough hard disk space for two instances of cnMaestro.

1. Export the cnMaestro Server data from the old instance.
2. Stop the old instance.
3. Start the new instance (using the directions presented above).
4. Import the data into the new instance.
5. Set the IP address of the new instance to that of the old instance.

Clone Virtual Machine

Cambium also recommends backing up (or cloning) the virtual machine prior to updating cnMaestro software.

In-System Upgrade

In-System Upgrade updates the cnMaestro software without performing a system export followed by an import. Essentially all updates are performed within a single VM image. In-System Upgrade works in both Standalone and High Availability environments. The mechanism of the upgrade is transparent to the user: specify to upgrade the

system on one instance, and the upgrade is propagated to both instances. The coordination happens automatically.

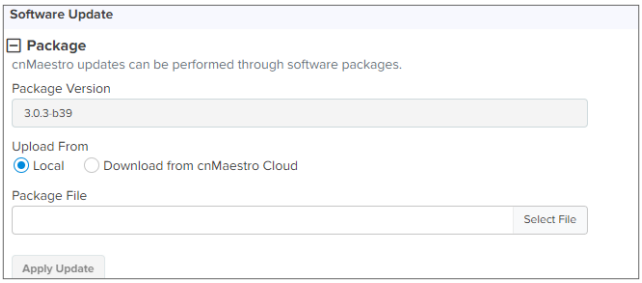
Software Update

The UI allows the user to upload a new OVA and install it. This process is used for both standalone and HA installations. The Software Upgrade can be done through OVA or package.

Package Upgrade

1. Navigate to **Administration** > **Server** > **Operations** > **Software Update**.
2. Click **Package**.
3. Browse and select the **cnmaestro-package_3.1.1-r63.tar.gz** file. You can upload the file from **Local** or **Download from cnMaestro Cloud.**
4. Click **Apply Update** or **Download and Apply.**

Figure 444 *Package Upgrade*

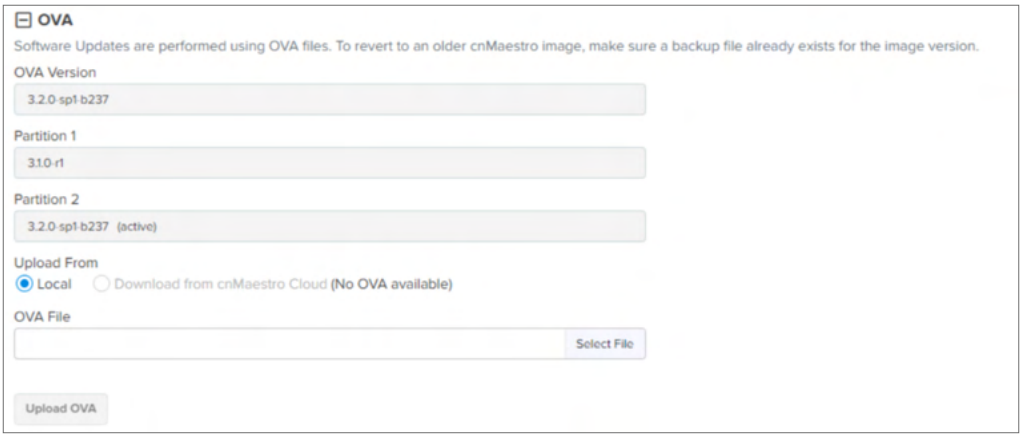


OVA Upgrade

Note

- Ensure a minimum of 1 GB free RAM in the cnMaestro On-Premises server for the OVA to upgrade successfully.
- To upgrade from 3.1.x to 3.2.0, refer to Upgrade of On-Premises from 3.1.x to 3.2.0.

1. Navigate to **Administration** > **Server** > **Operations** > **Software Update**.
2. Click **OVA**.
3. Browse and select the **cnmaestro-on-premises_3.2.0-r1_amd64.ova** file. You can upload the file from **Local** or **Download from cnMaestro Cloud.**



4. Click **Upload OVA** or **Download OVA**. After upload it will progress with Staging.

OVA Upgrade Using CLI

1. Copy the OVA file into the location /srv/storage/tmp.
2. Execute the command **sudo /srv/bin/cnmaestro-image stage /srv/storage/tmp/<OVA file name>.**
3. Staging Status can be verified in UI under **Server** > **Operation** > **OVA**.

In the CLI, it can be verified by executing the command sudo /srv/bin/cnmaestro-image status

If you are unable to apply the upgrade OVA using the UI, there is a command line mechanism that can be used as a failsafe. See **Appendix > Maintenance > Command Line Alternatives > Apply OVA Upgrade** for more details.

Diagnostics

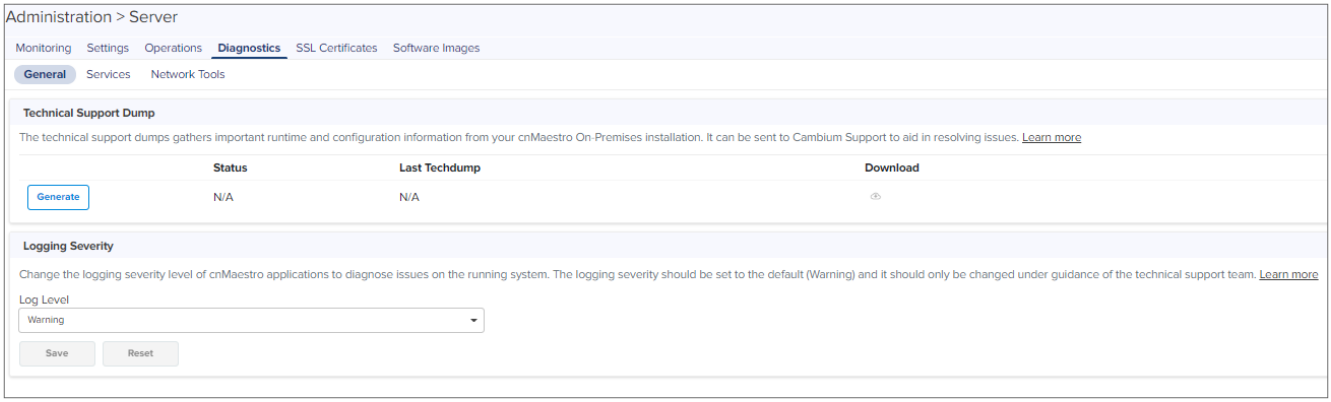
This section provides the following details:

- Server Technical Support Dump
- Logging Severity
- Services

Server Technical Support Dump

The Technical Support Dump gathers important runtime information on the cnMaestro instance. It is accessed at **Administration > Server > Diagnostics** and can be used by Cambium Networks Support to aid in resolving issues.

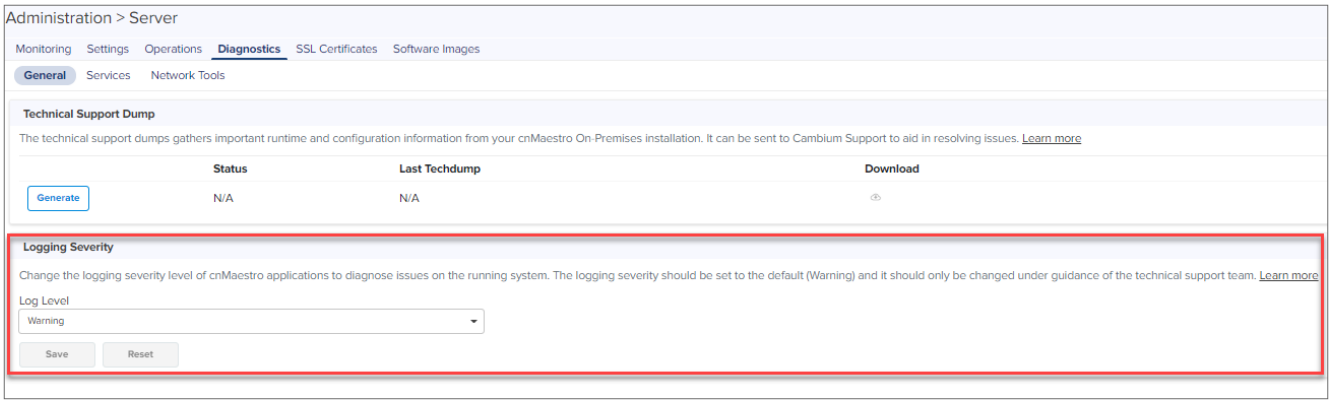
Figure 445 *Technical Support Dump*



Logging Severity

Change the severity level of the messages logged by the cnMaestro system. These messages are not accessible directly, but can be downloaded as part of the Technical Support Dump. The log level severity can be changed at runtime and it does not require reboot of server to take effect.

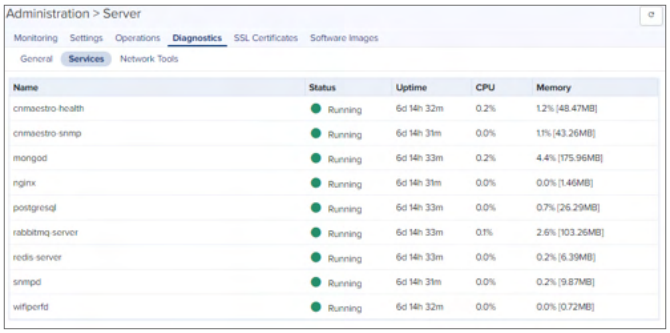
Figure 446 *Logging Level*



Services

Real time display of the status of critical cnMaestro services.

Figure 447 *Services*



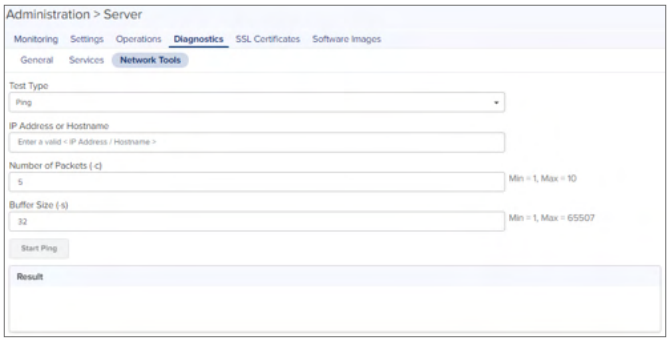
Network Tools

The Network Tools page consolidates a number of operations that can be performed on cnMaestro On-Premises. The operations are listed below:

Table 143 *Network Tools*

Tools	Description
DNS Lookup	Lists the DNS records for a domain in priority order.
Ping	Network ping to a hostname or IP address.
Traceroute	Lists the hosts or IP addresses showing the route of the test packets starting from the selected monitoring location to the destination Domain or IP.

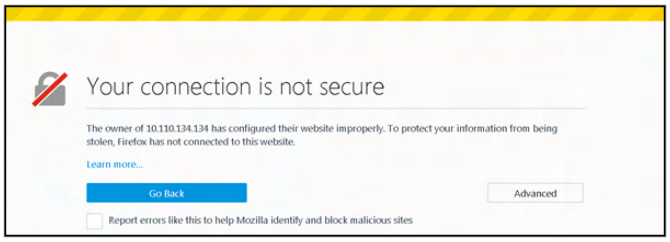
Figure 448 *Network Tools*



Certificate Management

cnMaestro On-Premises generates a self-signed certificate when it starts the first time. Because the root CA is not present in standard browsers, cnMaestro users (administrators or Captive Portal customers) receive an SSL error message as shown below:

Figure 449 *SSL Error Message*



To fix the browser error, cnMaestro must host a certificate from a trusted certificate authority, and map the FQDN (fully qualified domain name) used to access cnMaestro. This requires the administrator to export a CSR (Certificate Signing Request) and import the signed Certificate back into cnMaestro.

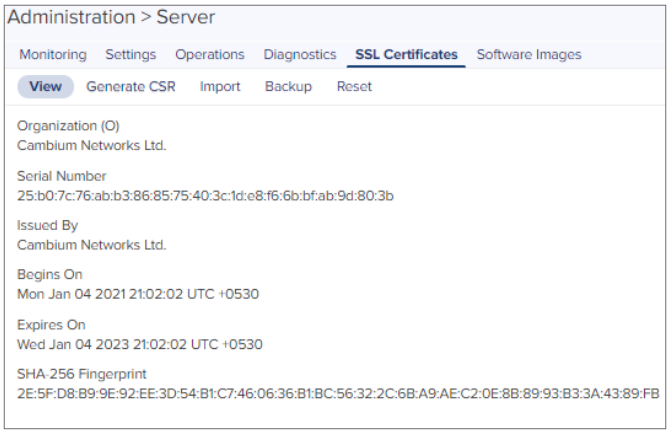
The following options are available to manage the certificates:

- View Certificate
- Generate a Certificate Signing Request (CSR)
- Import a Certificate

- Backup Management
- Reset

View Certificate

To view the certificate details, click **View** tab.

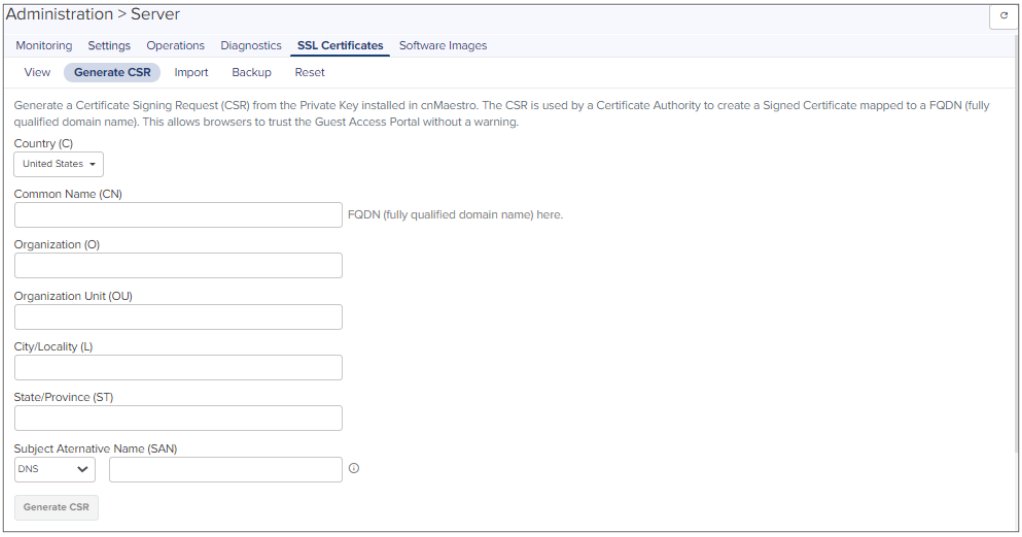


Generate a Certificate Signing Request (CSR)

A certificate-signing request leverages the current Private Key and exports a CSR that can be forwarded to any Certificate Authority.

To generate a CSR:

1. Navigate to **Administration** > **Server** > **SSL Certificates**.
2. Select **Generate CSR** tab.



3. Specify the parameters as in the below table:

Table 144 *Configuring CSR Parameters*

Parameter	Description
Common Name	Enter FQDN name of the cnMaestro server. This is either the Domain Name or the IP Address.
Organization (O)	Enter the name of the organization.
Organization Unit (OU)	Enter the name of the organization unit.
City/Locality (L)	Enter the name of the city.
State/Province (ST)	Enter the name of the state.
Subject Alternative Name (SAN)	Enter DNS or IP Address.
Country (C)	Select the name of the country from the dropdown list.

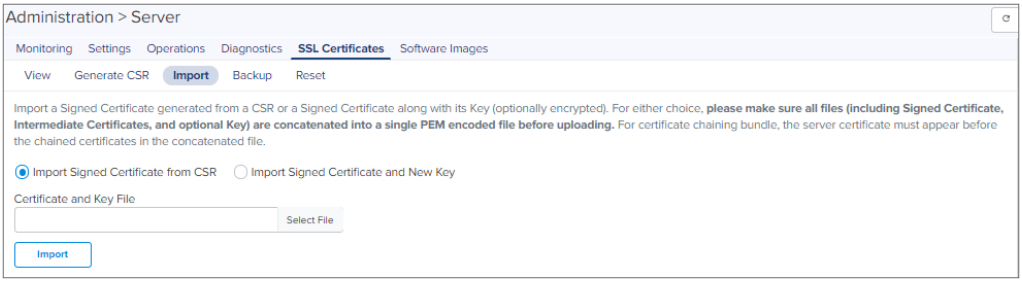
4. Click **Generate CSR**., the user is prompted to save a cnMaestro .csr file to their hard drive. The CSR can then be sent to a Certificate Authority and signed.

Import a Certificate

Once the CSR has been transferred to the Certificate Authority to create a certificate, it can be imported back into cnMaestro. cnMaestro will validate the certificate maps correctly to the stored Private Key, and disallow the import if incorrect. Alternatively, the user can append the Private Key to the Certificate file in PEM format and upload both if certificate and key is generated outside cnMaestro. User can also provide password optionally if key is generated with the password. This will replace both the Certificate and Key on cnMaestro.

To import a certificate:

1. Click **Import** tab.



2. Select any one of the below options:
   a. Import signed Certificate from CSR.
   b. Import signed Certificate and new Key.
3. Browse and upload the Certificate and Key file.
4. Click **Import**.

Note

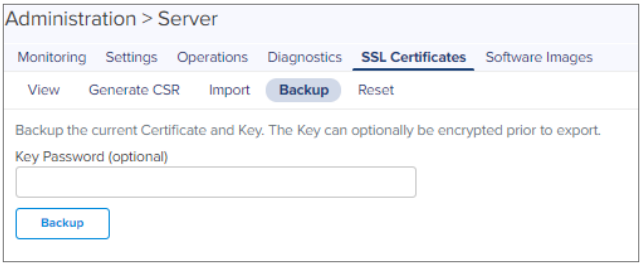
The Certificate and any optional intermediate certificates should be appended and stored in a single PEM-encoded file prior to submission. The signed Certificate should be positioned at the top of the file, followed by any intermediate certificates.

When importing a Certificate and Key, a single PEM-encoded file should be submitted with entries in the following order: Certificate, intermediate certificates, and Key. If the Key is encrypted, a password should be provided in the textbox on the UI at the time of import.

Backup Management

cnMaestro generates a 4096-bit Private Key when it boots up. This section allows the customer export this Key and current Certificate for backup. These will be exported as a single file, and the Key can optionally be encrypted with a password. To backup the certificate and the key:

1. Click **Backup** tab.



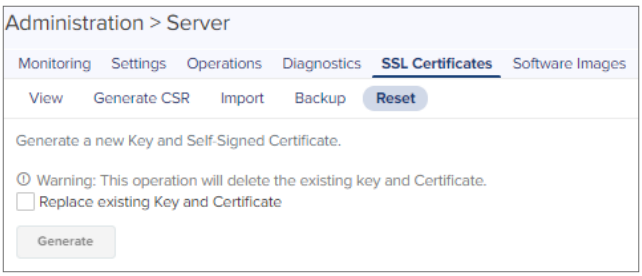
2. Enter the password for the key in the Key **Password** texbox.
3. Click **Backup**.

Reset

It replaces the current Private Key and Certificate and recreates them from scratch. The Certificate is self-signed, and it can be replaced using the Certificate import mechanism detailed above.

To generate a new private key:

1. Click **Reset** tab.



2. Select the **Replace the existing Key and Certificate** checkbox.
3. Click **Generate**.

Managing Software Images

This section provides the following details:

- Overview
- Automatically Update Device Software

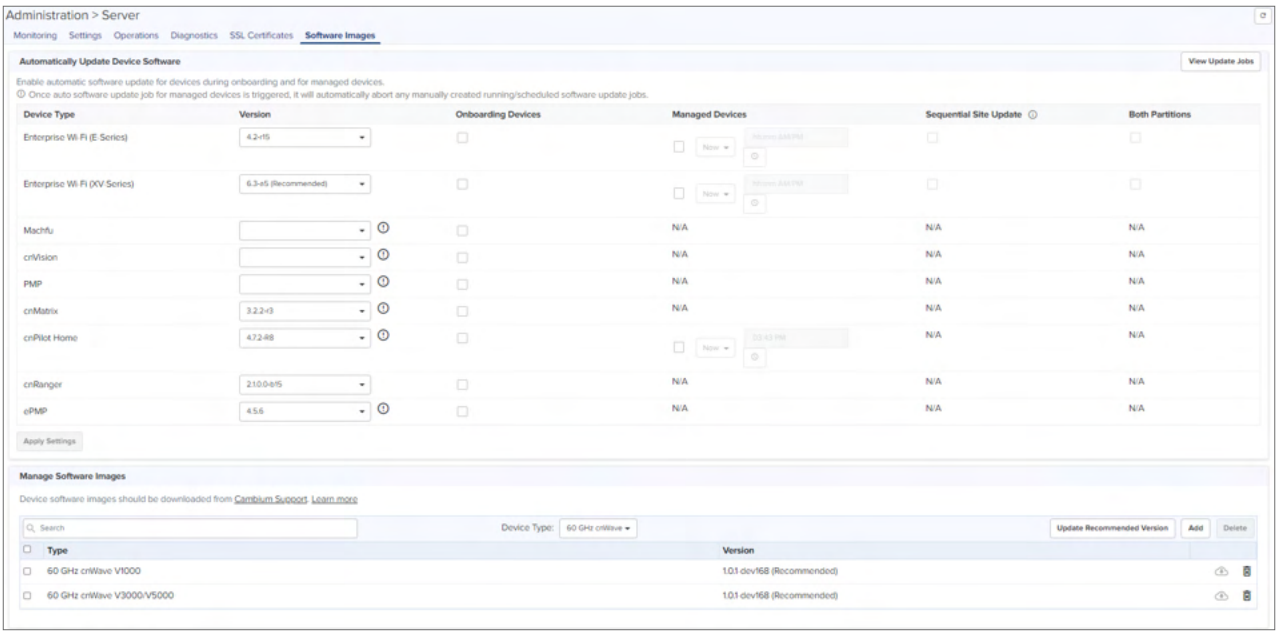
Overview

cnMaestro On-Premises allows one to add new device software images as they are released by the device teams. Adding new device software is a manual process: one needs to first download the images from the Cambium

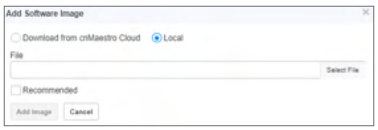
Support Center and then upload them into cnMaestro.

The steps are shown below for local upload:

1. Navigate to https://support.cambiumnetworks.com/files and download the device image to your locak desktop or laptop.
2. In the cnMaestro On-Premises UI, navigate to **Administration** > **Server** > **Software Images** tab.



3. Select the image file and then click **Add** button.
4. Add Software Image window pops up.



5. Once file is successfully uploaded to the server, it will appear in the grid.

Note

cnMaestro uses the name of the uploaded file to determine the version and device type. Please do not change the file name during the upload or download process.

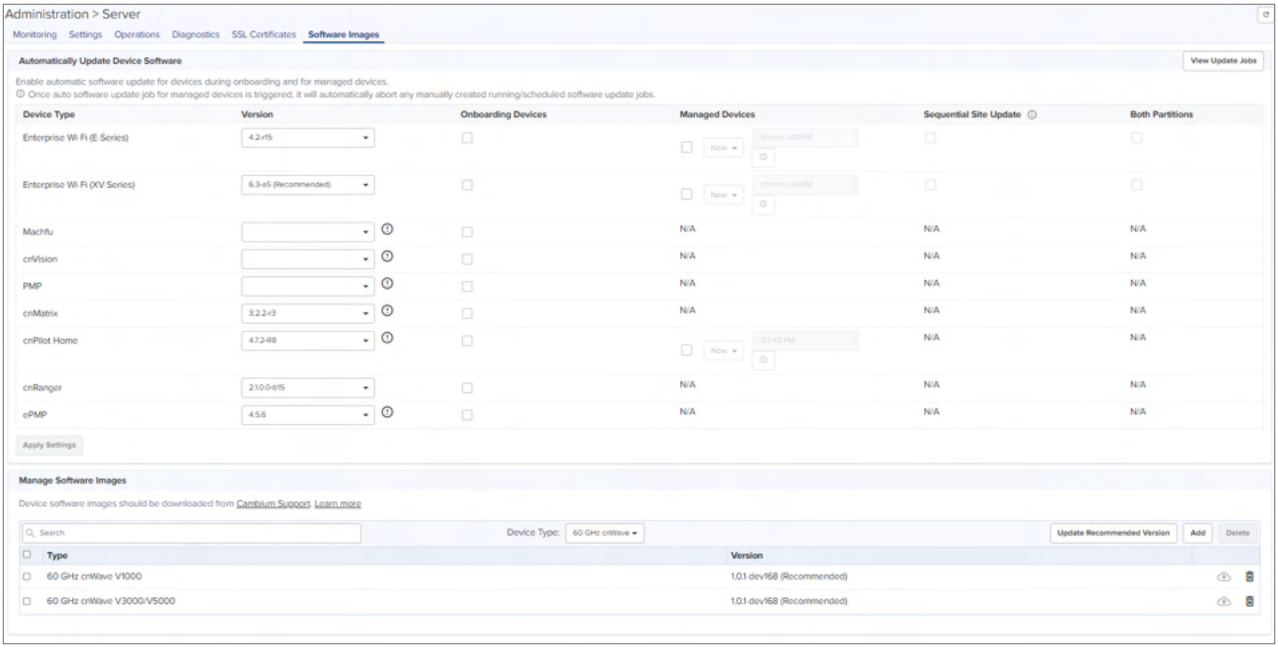
All the checkbox will be disabled by default.

Add Images

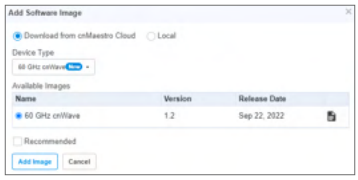
Once the On-Premises server is synced with the cloud, the user can upload the software images from cloud directly to the On-Premises.

To upload Software Image perform as follows:

1. Navigate to **Administration > Server > Software Images.**



2. Click **Add Image.**
3. **Add Software image** window appears.
   - If the On-Premises account has onboarded to any anchor account in cloud.
     a. Click **Download from cnMaestro Cloud.**
     b. Select **Device Type**.



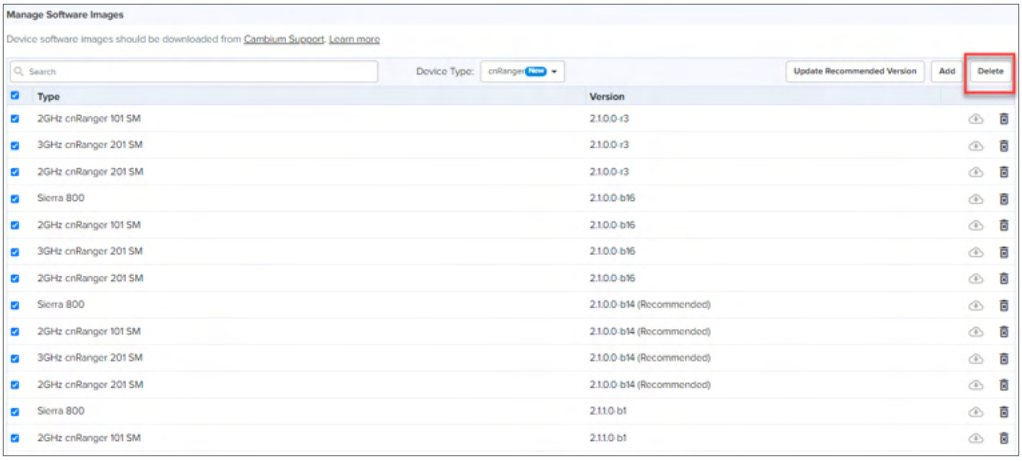
     c. Select the **Version**.
     d. Click **Add Image.**
   - If the On-Premises account is not onboarded to any anchor account in cloud.
     a. Click **Local**.

     b. **Select File** from the local desktop.
     c. Click **Add Image**.

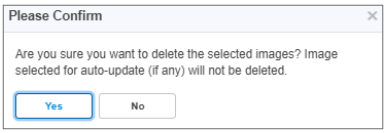
Delete Images

To delete Software Image perform as follows:

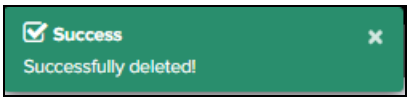
1. Navigate to **Administration** > **Server** > **Software Images.**



2. Select the images to be deleted and Click **Delete.**
3. Click **Yes** in Please confirm window to delete the images.



4. It will display the Success message as shown below:

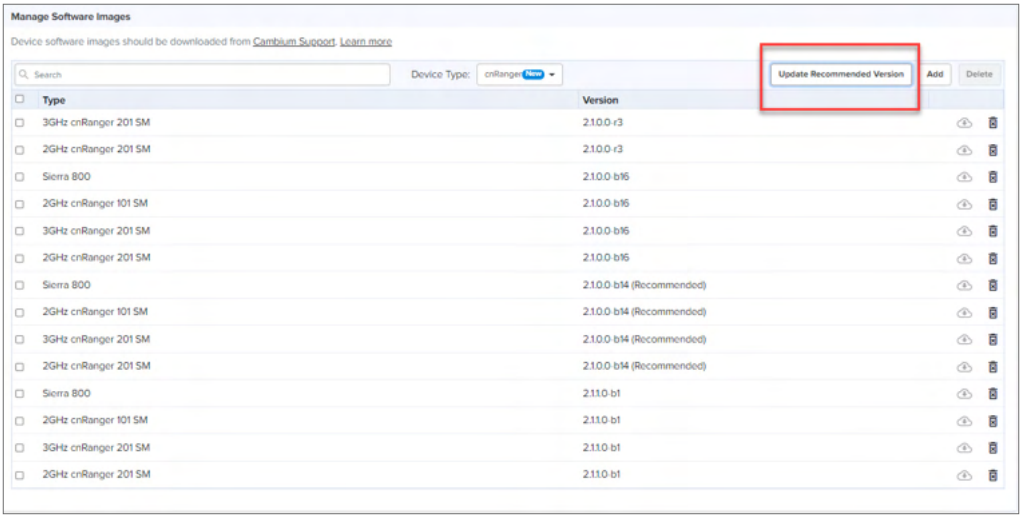


Update Recommended Version

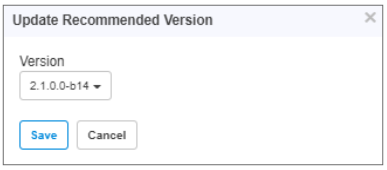
Update recommended version allows the user to update the Version with the recommended version available from the dropdown.

To update recommended version perform as follows:

1. Navigate to **Administration** > **Server** > **Software Images.**



2. Click **Update Recommended Version** and window pops up**.**



3. Select the **Version** from the dropdown and click **Save.**

Automatically Update Device Software

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:

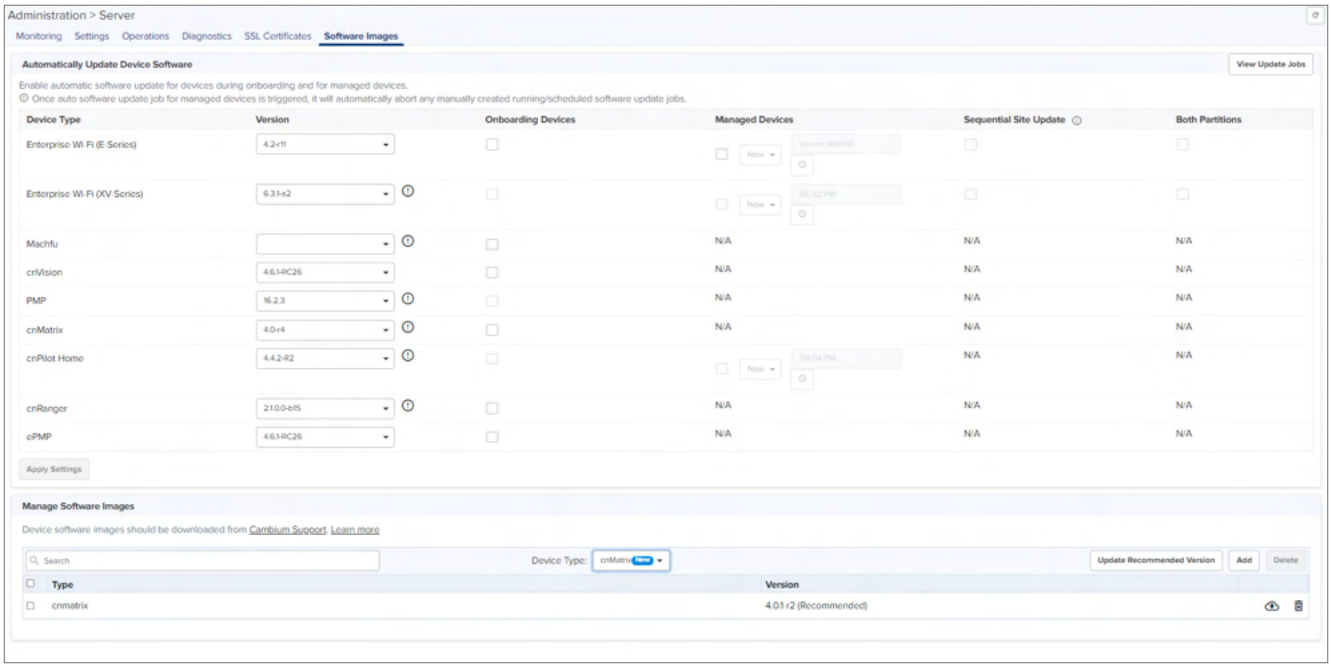
1. Navigate to **Administration** > **Server** > **Software Images** > **Automatically Update Device Software** tab.
2. Select the version file and then click **onboarding/Managed Devices**.

> **Note**
>
> Enable the onboarding checkbox, 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 and R series).
   - Enable **Sequential Site Update** and **Both Partitions** flag only for only E-Series and XV-Series devices.
4. Click **Apply Settings.**

> **Note**
>
> - Once auto software update job for managed devices is triggered, it will automatically abort any manually created running/scheduled software update jobs.
> - To avoid failures in onboarding devices having minimum supported version other than recommended version enable the onboarding checkbox.

Figure 450 *Automatically Update Device Software*



Webhooks X

Webhooks allow cnMaestro to post real-time alarm notifications to a configured third-party URL or application. cnMaestro uses HTTPS POST request to send notifications to the third-party URL or application. Webhooks enable the following benefits:

Benefit	Details
Cloud Friendly	Webhooks are a standard mechanism for Cloud alerts and inter-service asynchronous communication.
Firewall Friendly	HTTPS is generally amenable for outgoing and incoming firewall connections.
Real-Time	Alarms are sent to third-party services in real-time.
Security	All communication is over HTTPS, and the target domain is validated. Optional security parameters are available for client authentication.
TCP	Webhooks use TCP instead of UDP, so they can alert when the external system is down, or the event was not received.
Third-Party Support	Many Cloud and On-Premises services support Webhooks.

To configure Webhooks for cnMaestro, you must first configure a Webhooks template and then configure the notifications to be sent by cnMaestro to the Webhooks URL.

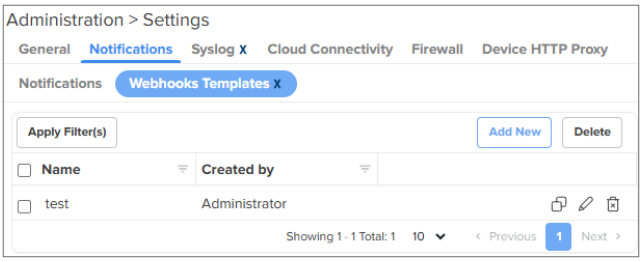
This topic describes the following:

- Configuring Webhooks template
- Supported variables
- Error and retransmission
- Notifications

Configuring Webhooks template

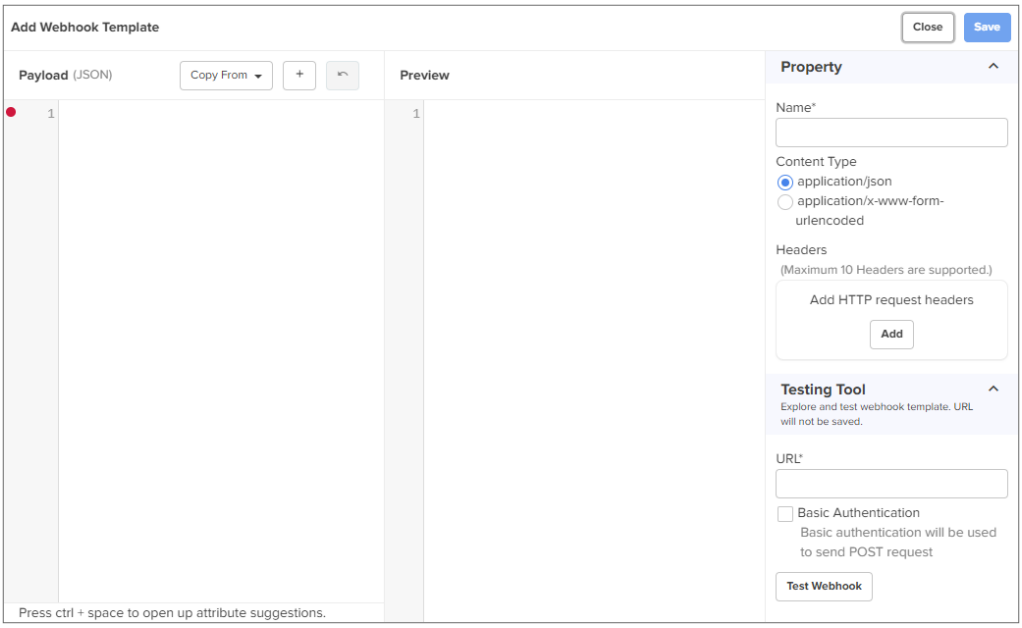
To configure the webhooks template, perform the following:

1. Navigate to **Administration** > **Settings** > **Notifications** > **Webhooks Templates X**.



2. Click **Add New**.

   The Add Webhook Template page appears.



3. Enter the parameters as shown in the below table.

Table 145 *Add Webhook Template parameters*

Parameter	Description
Payload (JSON)	Provide the Webhooks payload template in the JSON format in the left window. From the **Copy From** dropdown list, select **Default (Included)**. The Payload window populates the default JSON payload format. You can delete or add additional variables by clicking the add attributes (+) icon. The **Preview** window on the right displays a sample payload output with example values.
Property-related parameters	
Name	Webhooks label for display and filtering purposes. This will also be included in the default payload as `WEBHOOK_NAME`.
Content-Type	Indicates the type of payload content. This helps in the Webhooks receiving system to interpret and process the payload. The following types are supported: • **application/json** • **application/x-www-form-urlencoded**
Headers	Specifies the key and value pair for identifying the Webhooks. A maximum of 10 headers are supported. To add a header: 1. Click **Add**. 2. Specify the values in the **Key** and **Value** parameters. 3. Click **Add**.

Parameter	Description
	To delete a header, click the delete ( ) icon.
Testing Tool-related parameters Allows to test the connectivity of the Webhooks URL from cnMaestro UI.	
URL	Specify the Webhooks URL where you want to receive the notifications.
Basic Authentication	Indicates that the HTTPS basic authentication is added to the Webhooks POST request. By enabling basic authentication, you can configure the username and password associated with your endpoint. The Basic Authentication parameters are Base64 encoded and included in the header of the HTTPS request. **Note** • The username and password for Basic Authentication are different from cnMaestro user credentials. These credentials are used at your endpoint. • Basic Authentication is an HTTP standard which that adds an **Authorization: Basic <credentials>** header to the HTTPS POST request. Credentials are Base64 encoded username and password, encoded the following way: Base64 (username:password).
Test Webhook	Click to test the connectivity of the Webhooks URL. You can also test this connectivity while configuring the notifications. Refer to <>.

For example, a sample device offline alarm payload is shown below:

```
{
 "acknowledgedBy":
 "alarmDuration": "27127611898",
 "alarmld": "66e2854a6d49046d4b3425c5",
 "alarmMsg": "Device is offline.",
 "alarmName": "STATUS_DOWN",
 "alarmSeverity": "major",
 "alarmStatus": "true",
 "alarmCategory": "STATUS",
 "alarmType": "Status",
 "alarmRaisedTimelSO": "2024-09-12T06:03:10.472Z",
 "deviceName": "SmartSensor-Xl",
 "deviceMac": "F8:A1:65:3E:9B:4C",
 "deviceSerialNo": "SN123456789",
 "deviceType": "Sensor",
 "deviceModel": "SSX-2024",
 "deviceMode": "wi-fi",
 "deviceIPv4": "192.168.0.101",
 "deviceIPv6": "2001 :db8:85a3: :8a2e: 370:7334",
 "systemMac": "00:1A:2B:3C:4D:5E",
 "systemName": "Workstation-01",
 "systemIPv4": "192.168.1.10",
 "systemIPv6": "fe80::la2b:3c4d:5e6f:7g8h",
 "sourceType": "",
 "managedAccount": "Tally Managed Account",
 "networkName": "Global Network",
 "siteName": "Apartment Site",
 "siteld": "SITEID001",
 "towerName": "Apartment Tower",
 "webhookName": "WebhookSettingsName",
 "webhookRetryCount": "1",
 "webhookTimestamp": "1753248602370"
}
```

4. Click **Save**.

   The template is saved and listed on the **Webhooks Templates** page.

Supported variables

The following variables can be used to specify your own payload within a custom template. The variables will be replaced with actual values before sending to Webhooks endpoint.

Table 146 *Types of Variables*

Variable	Description
ALARM_ACK_BY	Name of the person who acknowledged the alarm.
ALARM_DURATION	Alarm duration (seconds)
ALARM_ID	Alarm ID (for example, 9bd4Gc313a4d1e8fie2482df7b77628)
ALARM_MSG	Alarm message (for example, “GPS Sync state changed to Synchronized”)
ALARM_NAME	Alarm name (for example, Configuration Sync)
ALARM_SEVERITY	Alarm severity (for example, critical, major, minor)
ALARM_STATUS	Alarm status (for example, true)
ALARM_CATEGORY	Alarm category (for example, STATUS)
ALARM_TYPE	Type of alarm (for example, status)

Variable	Description
ALARM_LAST_ UPDATED_TIME	Timestamp in the ISO 8601 format (`YYYY-MM-DDTHH:mm:ssZ`) when the alarm was last updated
ALARM_RAISED_TIME	Alarm raised timestamp in the ISO 8601 format (`YYYY-MM-DDTHH:mm:ssZ`)
ALARM_RAISED_ TIME_UTC	Alarm raised time in the 24 hour format along with the UTC offset standard time (`hh:mm` <UTC offset standard time>
CLIENT_MAC	Client MAC address (for example, AA:BB:CC:DD:EE:FF)
CLIENT_IPv4	Client IPv4 Address (for example, 192.168.0.1)
CLIENT_IPv6	Client IPv6 Address (for example, AF60::540:3CGD:DE33:8965)
DEVICE_NAME	Device name
DEVICE_MAC	Device MAC address (for example, AA:BB:CC:DD:EE:FF)
DEVICE_SN	Device serial number (for example, SN123456789)
DEVICE_TYPE	Device type (for example, Wi-Fi-enterprise)
DEVICE_MODEL	Device Model (for example, ePMP 1000, cnPilot r201)
DEVICE_MODE	Mode of the device depending on the device model. Following are the supported modes for various devices: • 60 GHz cnWave CN: "CN" • 60 GHz cnWave DN: "DN" • cnMatrix: "sw" • cnPilot Enterprise (ePMP Hotspot): "wi-fi" • cnPilot Home (R-Series)): "wi-fi" • cnRanger BBU: "bbu" • cnRanger RRH: "rrh" • cnRanger SM: "sm" • cnVision Client: "client" • cnVision Hub: "hub" • cnWave 5G Fixed BTS: "bts" • cnWave 5G Fixed CPE: "cpe" • Enterprise Wi-Fi (E-Series, XE/XV/X7-Series, Xirrus-Series): "wi-fi" • ePMP AP: "ap" • ePMP SM "sm" • PMP AP: "ap" • PMP SM: "sm" • PTP 650/670/700: "bhm", "bhs" • PTP 820/850: "ptp"
DEVICE_IPv4	Device IPv4 Address (for example, 192.168.0.1)
DEVICE_IPv6	Device IPv6 Address (for example, AF60::540:3CGD:DE33:8965)
SYSTEM_MAC	System MAC address (for example, AA:BB:CC:DD:EE:FF)

Variable	Description
SYSTEM_NAME	System name
SYSTEM_IPv4	System IPv4 Address (for example, 192.168.0.1)
SYSTEM_IPv6	System IPv6 Address (for example, AF60::540:3CGD:DE33:8965)
SOURCE_TYPE	Type of source
MANAGED_ACCOUNT	Managed account name (absent if not mapped to an account)
NETWORK_NAME	Network name
SITE_NAME	Site name (**Note**: Value will be blank if the device is not under a Site)
SITE_ID	Site ID (**Note**: Value will be blank if the device is not under a Site)
TOWER_NAME	Tower name (**Note**: Value will be blank if the device is not under a Tower)
WEBHOOK_NAME	Webhooks name
WEBHOOK_RETRY_COUNT	Webhooks retry count (**Note**: Value is present only if Webhooks is retried; default is 0)
WEBHOOK_TIMESTAMP	Timestamp, in the ISO 8601 format (`YYYY-MM-DDTHH:mm:ssZ`), when the Webhook was sent

Error and retransmission

cnMaestro expects an HTTP status code 2XX reply from the Webhooks URL to confirm the alarm notification sent via HTTPS POST that is successfully delivered. For any request, if status code 5XX is received, cnMaestro will keep retrying the same payload at the interval of 1, 2, 5, 10 and every 15 minutes thereafter until the request succeeds. 3XX or 4XX response will not be retried.

Note

If there are multiple Webhooks configured, a retry/error on the one Webhook will not affect the other. For example, if you have Zapier and Twilio, a retry/error on the Twilio will not affect the Zapier, any new alarm notification on Twilio will be discarded and a retry will happen only with the cached payload.

Notifications

The Notifications feature allows the Super Administrator and the Administrator users to configure how notifications of alerts are sent from cnMaestro to the users.

cnMaestro supports sending notifications either to configured email IDs or Webhooks URLs.

Note

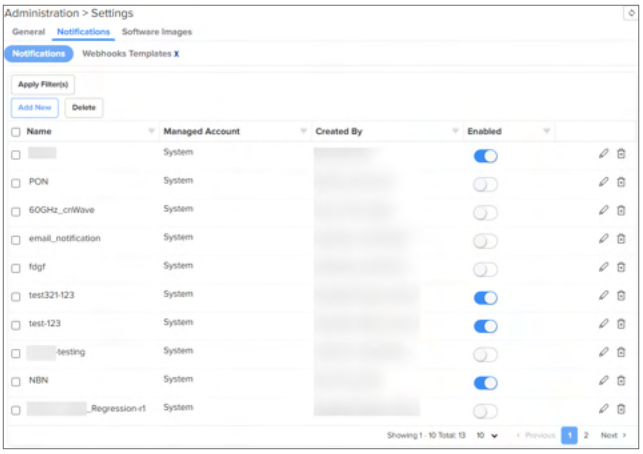
- Email delivery of notifications in the JSON format is being deprecated. Future releases of cnMaestro will support only HTML-based emails.
- A maximum of four email IDs and three webhooks are supported for each notification.

Adding a notification

1. Navigate to **Administration** > **Settings** > **Notifications** page.

   The Notifications page is displayed.

   All existing notifications are listed in a table.



2. Click **Add New**.

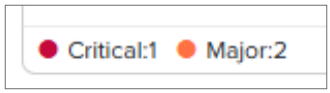
   The Add Notification page is displayed:

   Figure 451 *Add Notification page*

3. Configure the following parameters:

Table 147 *Notifications parameters*

Parameter	Description
Enable Notification	Enable the configured notification by selecting the checkbox. Default, it is disabled. You can also enable a notification on the **Notifications** page by toggling the switch ( ), located under the **Enable** column, to the on ( ) position.
Name	Name of the notification settings.
Managed Account	Specifies the level at which the notification is configured. The following options are available: • **System**—Notifications are sent for the alarms raised for the accounts at the system-level. Select the account for which you want to configure the notifications in the dropdown list. • **Network**—Notifications are sent for alarms raised at the selected networks. To add a network, click **Add**, and then select the network in the **Add Networks** window. • **Site**—Notifications are sent for alarms raised at the selected sites. To add a site, click **Add**, and then select the Managed Account, network, and the site in the **Add Sites** window. • **Tower**—Notifications are sent for alarms raised at the selected towers. To add a tower, click **Add**, and then select the Managed Account, network, and the tower in the **Add Towers** window.
Source Type	Indicates the source type from which the notifications are raised. For the list of supported source types, refer to Supported source types.
Alarms	Select the required alarm types to be notified. 1. To view the alarms available, select any source from the **Source Type** list. The source-specific alarms are listed in the **All Alarms** window. You can sort the listed alarms either by name of the alarm ID. 2. Select the alarms in one of the following ways: • Select the appropriate checkboxes and click the move ( ) icon to move the alarm to the **Selected Alarms** window. To remove any selected alarms to the All Alarms window, click the remove ( ) icon. • To select all the alarms, click the move all ( ) icon. To remove all alarms, click the remove all ( ) icon.

Parameter	Description
	Based on the alarms selected, the severity-wise count of alarms that are selected is displayed. 
Email	Specifies the email IDs to which the notifications are to be sent. A maximum of four email IDs are supported. Type the email ID in the text box, and press the Enter key to add the email ID.
Email Content Type	The notification content format to be used in the email body. The following options are supported: • HTML—HTML email example • JSON—JSON email example **Note** • Email delivery of notifications in the JSON format is being deprecated. Future releases of cnMaestro will support only HTML-based emails.
Webhooks	Specifies the webhooks details. A maximum of three webhooks are supported 1. To add a Webhooks URL, click **Add**. The **Add Webhook** window is displayed. 2. Specify the Webhooks URL in the **URL** field. 3. To add authentication credentials, select the **Basic Authentication** checkbox and specify the username and password. 4. Select the webhooks template from the **Templates** dropdown list. To add a new template, refer to Configuring Webhooks template. 5. To test the connectivity to the webhooks URL, click Test Webhook. A success or a failure message is displayed depending on whether the test results. 6. Click **Add**. The Webhooks is listed under the Webhooks table. 7. To edit a Webhooks, click the edit (✎) icon. 8. To delete a Webhooks, click the delete (🗑) icon.

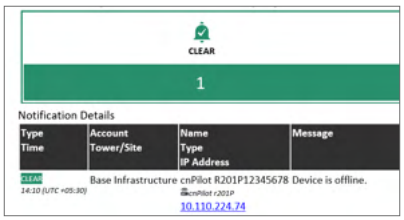
4. Click **Save**.

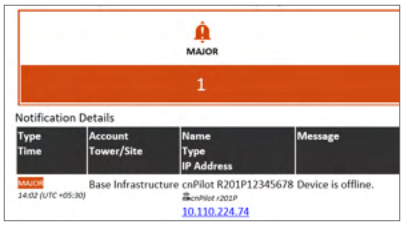
   The notification is listed in the **Notifications** page.

5. To edit a notification, click the edit (✎) icon.
6. To delete a notification, click the delete (🗑) icon.

   To delete notifications in bulk, select the notifications that you want to delete and click **Delete**.

HTML email example





JSON email example

Supported source types

The following table lists the source types supported at the system-, network-, site-, and tower-levels.

Source Type	Managed Account			
	System	Network	Site	Tower
All	✔	✔	✔	✔
cnMatrix	✔	✔	✔	✔
cnPilot Enterprise (ePMP 1000 Hotspot)	✔	✔		
Enterprise Wi-Fi (E-Series)	✔	✔	✔	✔
Enterprise Wi-Fi (XE/XV-Series)	✔	✔	✔	✔
Enterprise Wi-Fi (Xirrus-Series)	✔	✔	✔	✔
Enterprise Wi-Fi (X7-Series)	✔	✔	✔	✔
Light Speed	✔	✔	✔	

Source Type	Managed Account			
	System	Network	Site	Tower
PTP 820/850	✔	✔		✔
PTP 650/670/700	✔	✔		✔
60 GHz cnWave	✔	✔	✔	
cnRanger	✔	✔		✔
ePMP AP	✔	✔		✔
ePMP SM	✔	✔		✔
cnVision	✔	✔		✔
PMP AP	✔	✔		✔
PMP SM	✔	✔		✔
cnWave 5G Fixed	✔	✔		✔
cnReach	✔	✔		✔
cnPilot Home (R-Series)	✔	✔	✔	✔
System	✔			
Network	✔	✔		
Site	✔	✔	✔	
Tower	✔	✔		✔

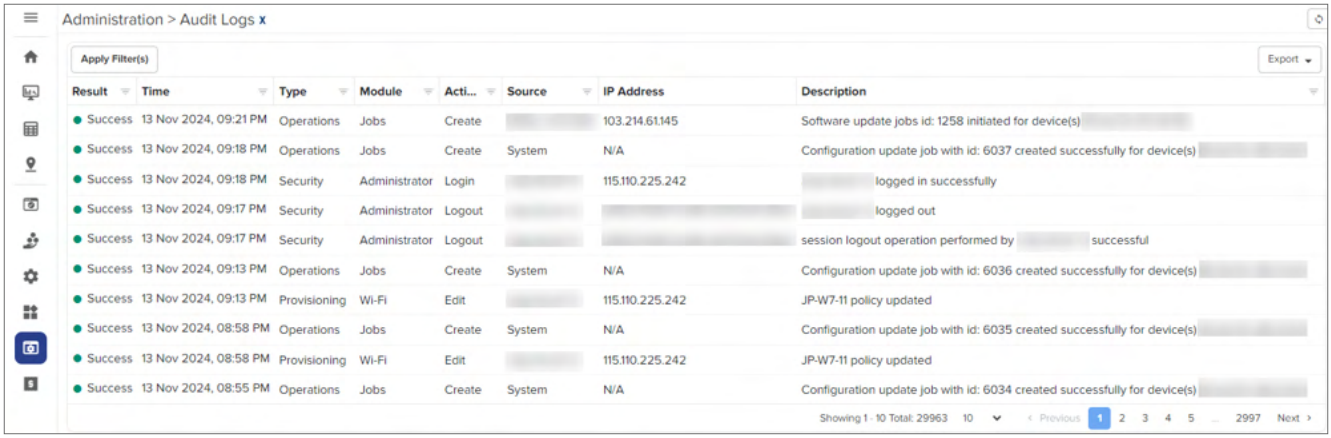
Audit Logs

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 452 *Audit Logs*



The following table describes the Audit Logs parameters and their descriptions.

Table 148 *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.
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 149 *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.
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.

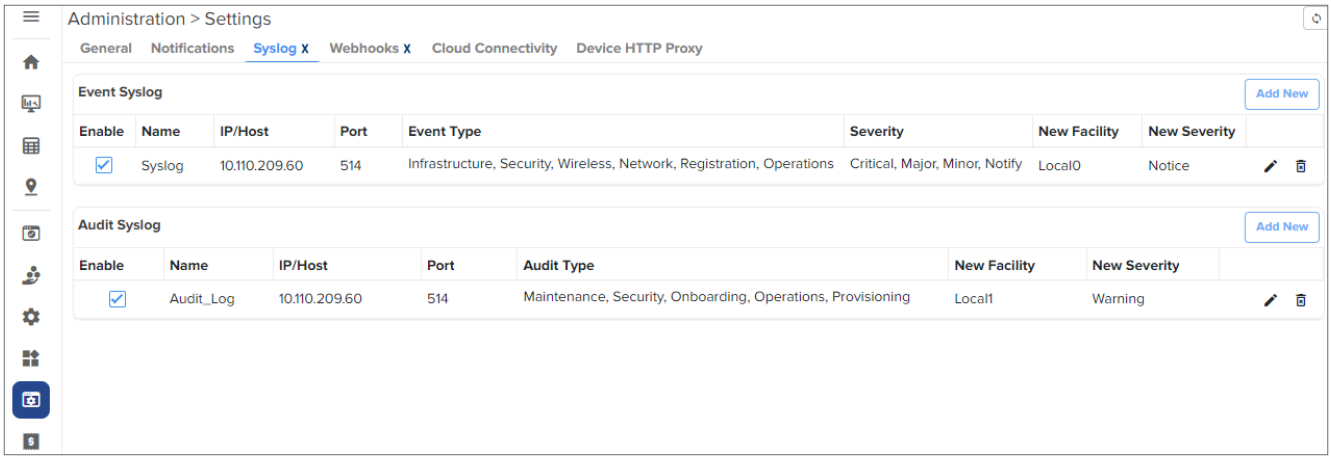
Module	Types	Description
ACL	Provisioning	Adding, editing, and removing the ACL entries.
Administrator	Provisioning Operations Security	User Management: Login, Users, Roles, Email.
Alarm	Provisioning	Alarms and Alarm History.
API	Provisioning	API Management: API Clients and Webhooks.
Auditing	Provisioning	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.
MSP	Operations	Operations covering Managed Services and Managed Account.
Onboard	Provisioning Operations	Onboarding Queue.
Profile	Provisioning	Create or update a profile.
Report	Provisioning Operations	Data Reports.
Software-Upgrade	Provisioning Operations	Software Upgrade: device image import/export, upgrade device.
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.

Module	Types	Description
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.

Syslog

cnMaestro supports Notification Syslog (Event Log) and Audit Syslog. The generated Event Logs and Audit Logs are sent to the syslog server configured under **Administration** > **Settings** page. Every syslog has a Facility and a Severity level. Maximum of five entries can be added in Notification syslog and Audit syslog.

Figure 453 *Syslog*



The following table describes the parameters in Syslog server:

Table 150 *Syslog Server Parameters*

Field	Description
Enable	Enable the notification syslog or audit syslog.
Event/Audit Type	The type of event (Infrastructure, Network, Operation, Security and Wireless). You can select one or multiple events.
IP/Host	The IP address provided to the server.
Name	The username provided to the server.
New Facility	The type of program logging the message. The allowed facilities are local 0 to local 7.
New Severity	The severity of the system log message.
Port	IP address or hostname provided to the server.
Severity	The initial severity of the generated syslog messages (i.e. Critical, Major, Minor or Notify).

Event Syslog

Notification messages are filtered based upon Type (which may be slightly different between Events and Alarms) and Severity.

Click **Add** to add a new Event Syslog.

Note

At least one Event Type or Severity must be selected.

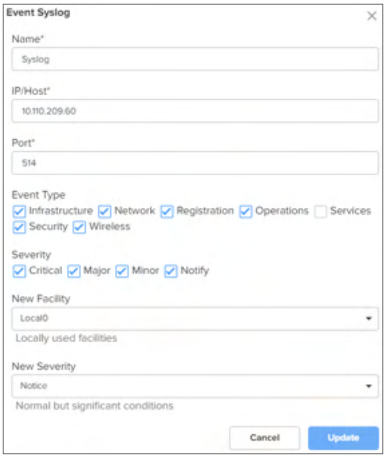
1. Enter **Name**.
2. Enter the **IP/Host** address.
3. Enter the **Port** number. Port 514 is the default for syslog.
4. Select **Event Type**.
5. Select **Severity Type**.
6. Select the **New Facility** from the dropdown**.**

Facility	Description
Local 0-Local 7	It is the locally used facilities.

7. In the **New Severity** dropdown, select the type of Severity. Please refer to the below Severity table:

Value	Severity	Description
0	Emergency	System is unusable.
1	Alert	Action must be taken immediately.
2	Critical	Critical conditions of hard device errors.
3	Error	Error conditions
4	Warning	Warning conditions.
5	Notice	Normal but significant conditions. Conditions that are not error conditions but may require special handling.
6	Informational	Informational messages.
7	Debug	Debug-level-messages.

8. Click the edit (✎) icon to edit the Event Syslog. The dialog box appears:

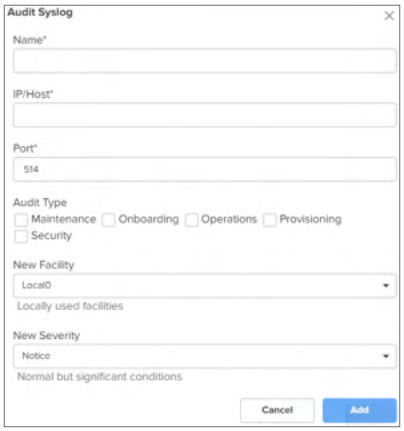


9. Repeat the above steps to update an existing Notification Syslog.

Audit Syslog

The Audit Syslog separates messages based upon Audit Type.

Click **Add** to add a new Audit Syslog.



Note

At least one Audit Type must be selected.

1. Enter **Name**.
2. Enter the **IP/Host** address.
3. Enter the **Port** number. The port number 514 is the standard syslog port.
4. Filter by **Audit Type**.
5. Select **New Facility** from the dropdown.

Facility	Description
Local 0-Local 7	Available facilities.

6. Select the type of **Severity**.
7. Click **Add**.

Firewall

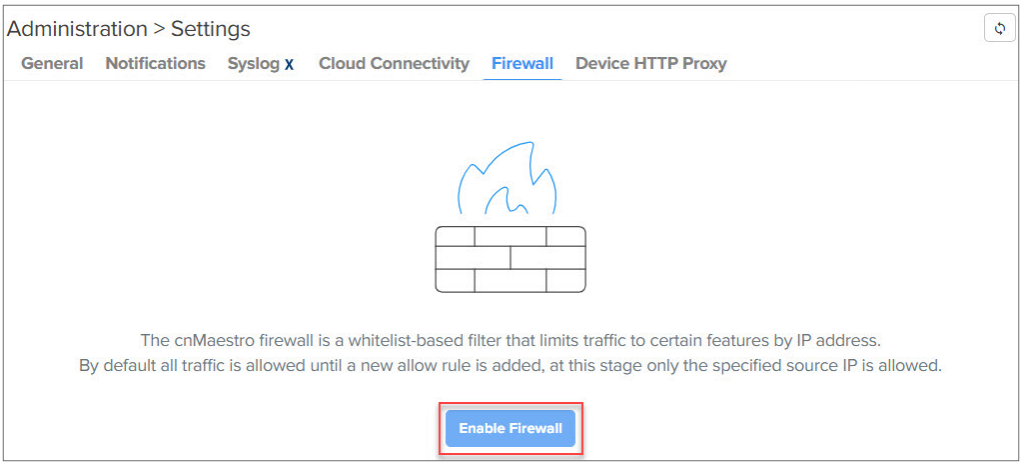
cnMaestro incorporates support for the Firewall in the On-Premises version. This feature enables administrators to manage and restrict incoming traffic by creating rules based on IP addresses. By default, all traffic is allowed until specific **Allow** rules are configured. Enabling the Firewall ensures that only the traffic from authorized IPs accesses management, APIs, captive portals, and other services. This feature provides administrators with greater control and security, protecting the system from unauthorized access.

Enabling Firewall

By default, the Firewall feature is disabled. To enable this feature, complete the following steps:

1. Navigate to the **Administration** > **Settings** > **Firewall** page.
2. To enable the feature, click **Enable Firewall** as shown in Figure 454.

   Figure 454 *To enable Firewall*

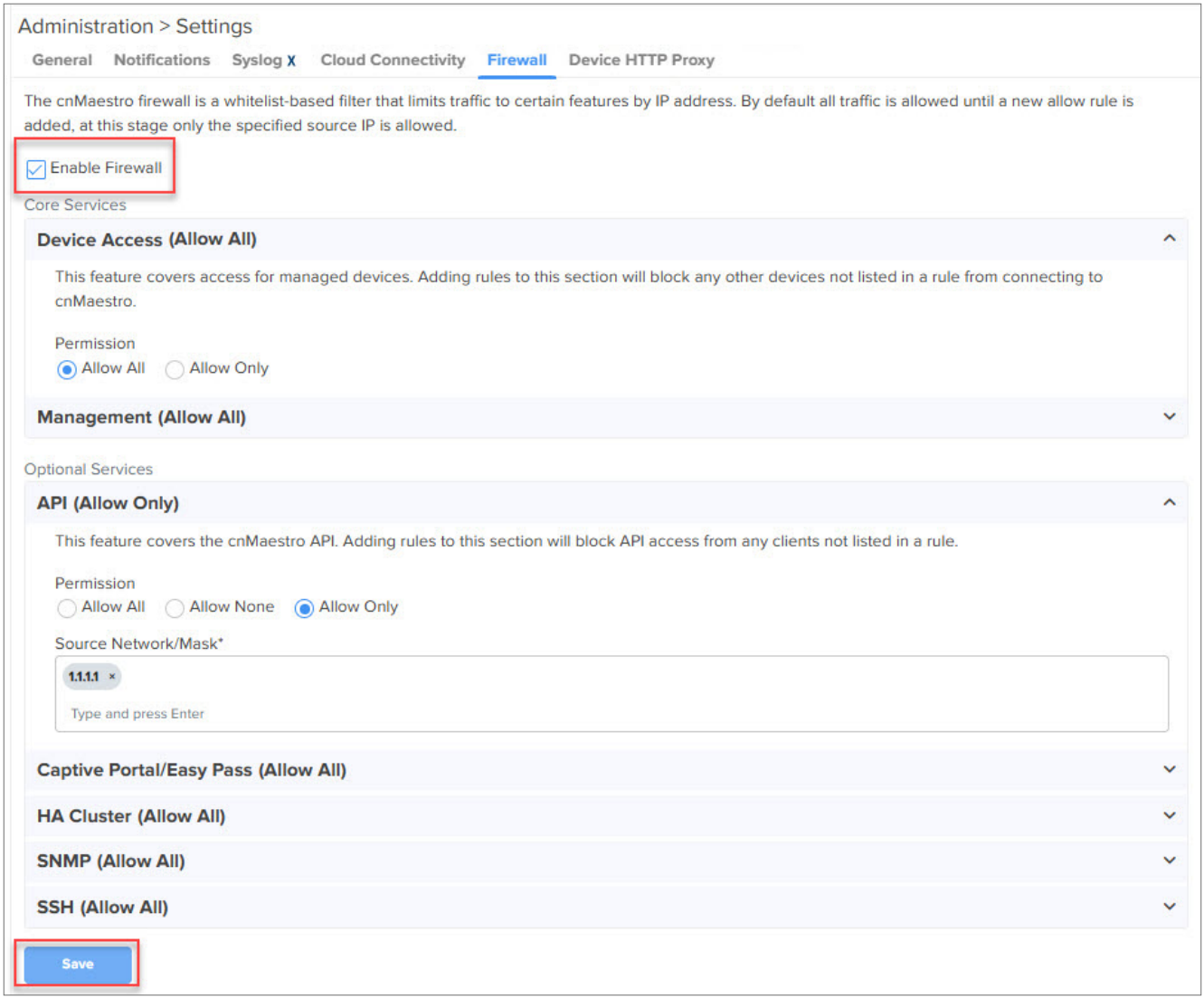
   

3. This setup page remains visible until a configuration is saved.

Configuring Firewall

Users can access Firewall from the **Administration** > **Settings** > **Firewall** page.

Figure 455 *Firewall page*



To configure the Firewall settings, complete the following steps:

1. Navigate to **Administration** > **Settings** > **Firewall**.
2. Click **Enable Firewall** to access the main configuration page as shown in Figure 454.
3. Select the **Enable Firewall** checkbox to activate the feature as shown in .
4. Select the service (for example, Management, API, SSH).
5. Choose the appropriate permission type:
   - **Allow All**: This option permits all incoming traffic without any restrictions.
   - **Allow None**: This option blocks all incoming traffic entirely.
   - **Allow Only**: This option restricts access, permitting traffic only from specified IP addresses. For Allow Only, enter the IP addresses or subnet ranges for the rule.
6. Click **Save** to apply changes.

Warning

When configuring Firewall rules for the **Management** service, ensure that the specified IP addresses or subnet ranges include your current IP address. Failure to include your current IP address may result in blocked access to cnMaestro from your current IP.

Warning

When configuring Firewall rules for the **SSH (Allow all)** service, it is best practice to keep SSH disabled unless specifically instructed by Cambium Support. If you enable SSH, adding rules to this section blocks access to any SSH clients not listed in a rule.

Note

If cnMaestro HA is either enabled or planned, ensure you add all HA peer IPs (primary, secondary, or cluster) to the allowed list. Failure to include these IPs may result in disruptions to HA communication and access issues.

Default state

If users remove all rules and set all permissions to **Allow All**, the Firewall returns to its default state. This configuration allows unrestricted traffic to all services.

Note

If users are unable to access the UI after configuring Firewall rules, they can log in to the CLI and use the cnMaestro WAF script to reset the Firewall settings. This option allows users to restore access to the cnMaestro system if the configured IP address becomes unavailable. To reset all configured rules and regain access, users can execute the following command in the CLI:

```
cnmaestro-waf --reset
```

Appendix

This section includes the following topics:

- Guest Access
- Maintenance
- Anchor Account Benefits
- Deployments
- Windows DHCP
- Hypervisor Installation
- Network Port Requirements
- XMS-Enterprise to cnMaestro X

Guest Access

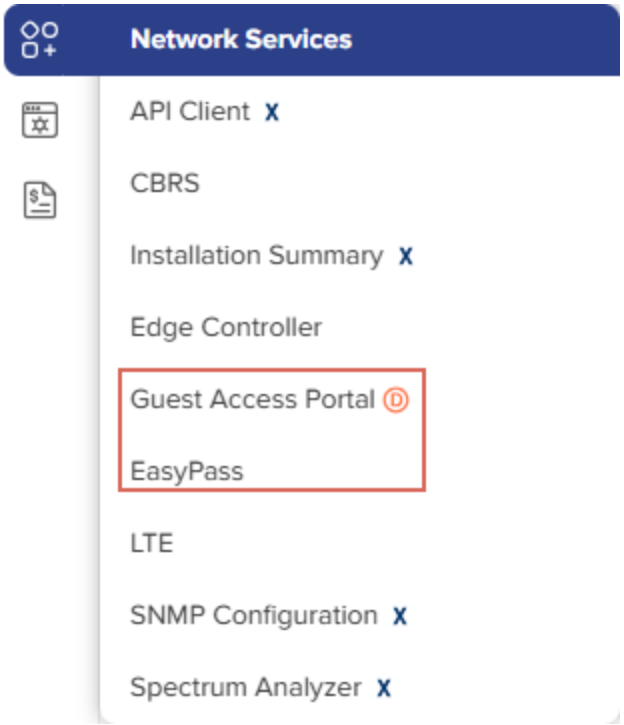
This section describes how to configure Guest Access using cnMaestro. This feature allows the clients to connect to the internet through Free Tier, Vouchers, or Paid Access types.

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 456.

To create captive portals on cnMaestro, use EasyPass. For information, see EasyPass.

Figure 456 *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 and ePMP 1000 Hotspot.

Configuration

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

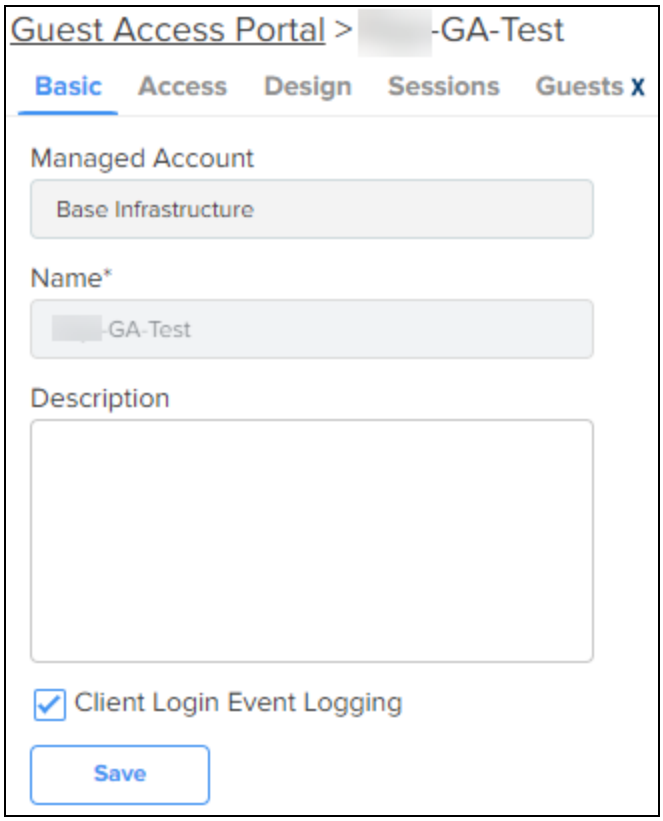
Creating the Guest Access Portal in cnMaestro

1. Basic Details
2. Access Portal
3. Design Page
4. Sessions
5. Guests

> **Note**
>
> In a HA installation, you must use the Floating Management IP to access the Guest Access Portal. For this you must map the DNS to the Floating Management IP and one of the unique IP addresses of the cnMaestro instances.

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:

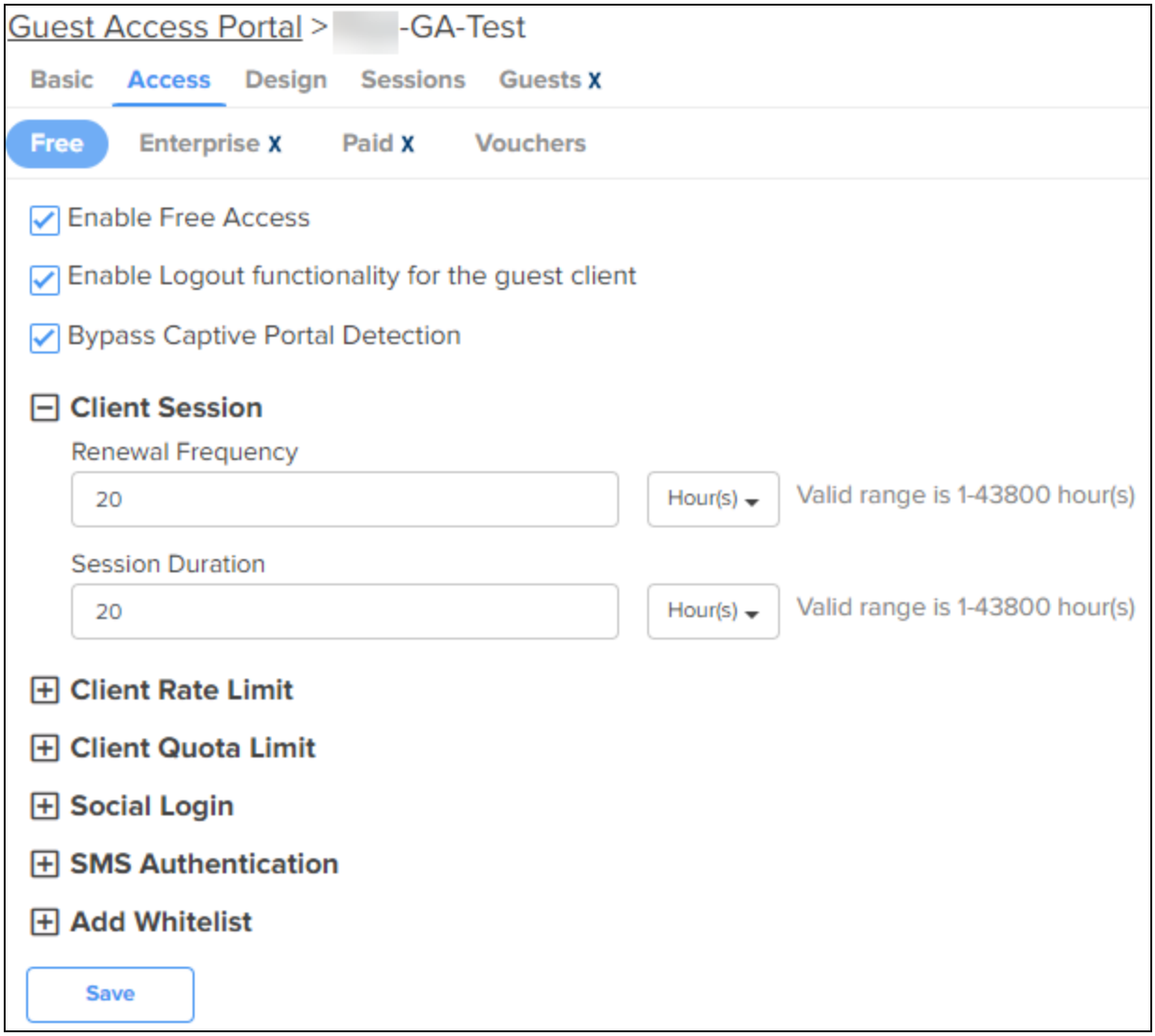
- Free
- **Enterprise** X access through one of the following options:
  - Microsoft Azure
  - Sponsored Guest
  - Self Registration
  - Google
- **Paid** X
- Vouchers

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



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 151 *Free Access Type Parameters*

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

Table 151 *Free Access Type Parameters*

Parameter	Description

Client Quota Limit	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.
	
	The similar behavior is supported through RADIUS attributes for RADIUS-based onboard guest access clients.
	
	`RADIUS_VENDOR_ID_CAMBIUM 9 (17713)`
	
	`RADIUS_VENDOR_ATTR_CAMBIUM_WIFI_QUOTA_UP (151)`
	
	`RADIUS_VENDOR_ATTR_CAMBIUM_WIFI_QUOTA_DOWN (152)`
	
	`RADIUS_VENDOR_ATTR_CAMBIUM_WIFI_QUOTA_UP_GIGWORDS (153)`
	
	`RADIUS_VENDOR_ATTR_CAMBIUM_WIFI_QUOTA_DOWN_GIGWORDS (154)`
	
	`RADIUS_VENDOR_ATTR_CAMBIUM_WIFI_QUOTA_TOTAL (155)`
	
	`RADIUS_VENDOR_ATTR_CAMBIUM_WIFI_QUOTA_TOTAL_GIGWORDS (156)`
	
	The `gigwords` attributes are used for supporting data quota limits above 4 GB when required.

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	Consists of the following options: • Domain URL: The redirected URL used by the client when trying to access the Internet. • Google: Consists of ID and Secret options to configure, which admin can create from https://console.cloud.google.com/. • Facebook: Consists of ID and Secret options to configure, which admin can create from https://developers.facebook.com/apps/. • Twitter: Consists of consumer key, consumer secret key, and callback URL. • Office 365: Consists of ID and Replyback URL.

Note

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

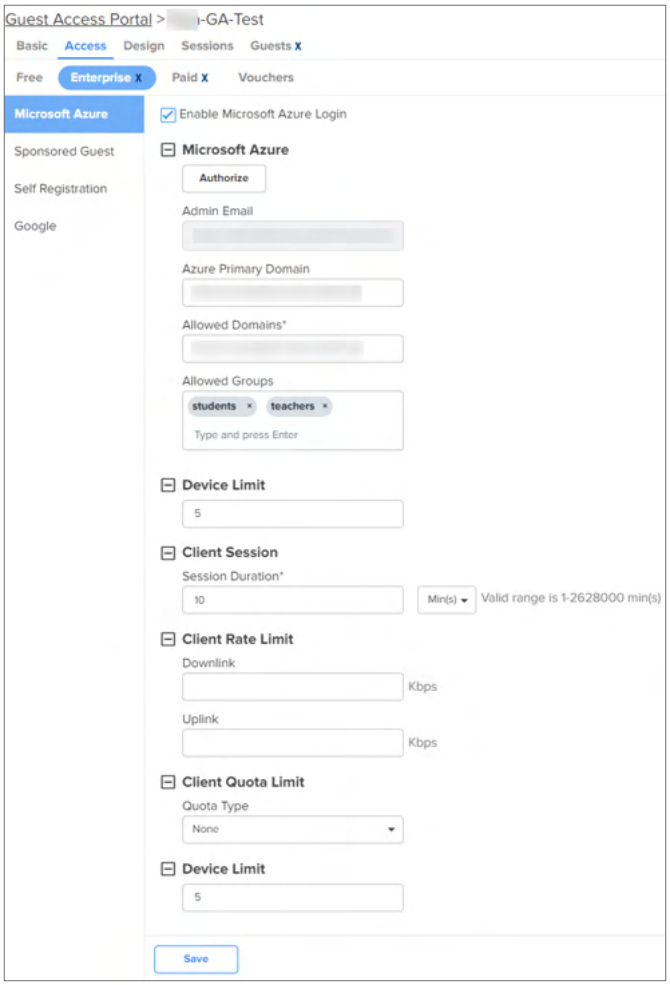
Enterprise Wi-Fi Access X using Microsoft Azure Login, Sponsored Guest, Self Registration, or Google

Note

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

Microsoft Azure

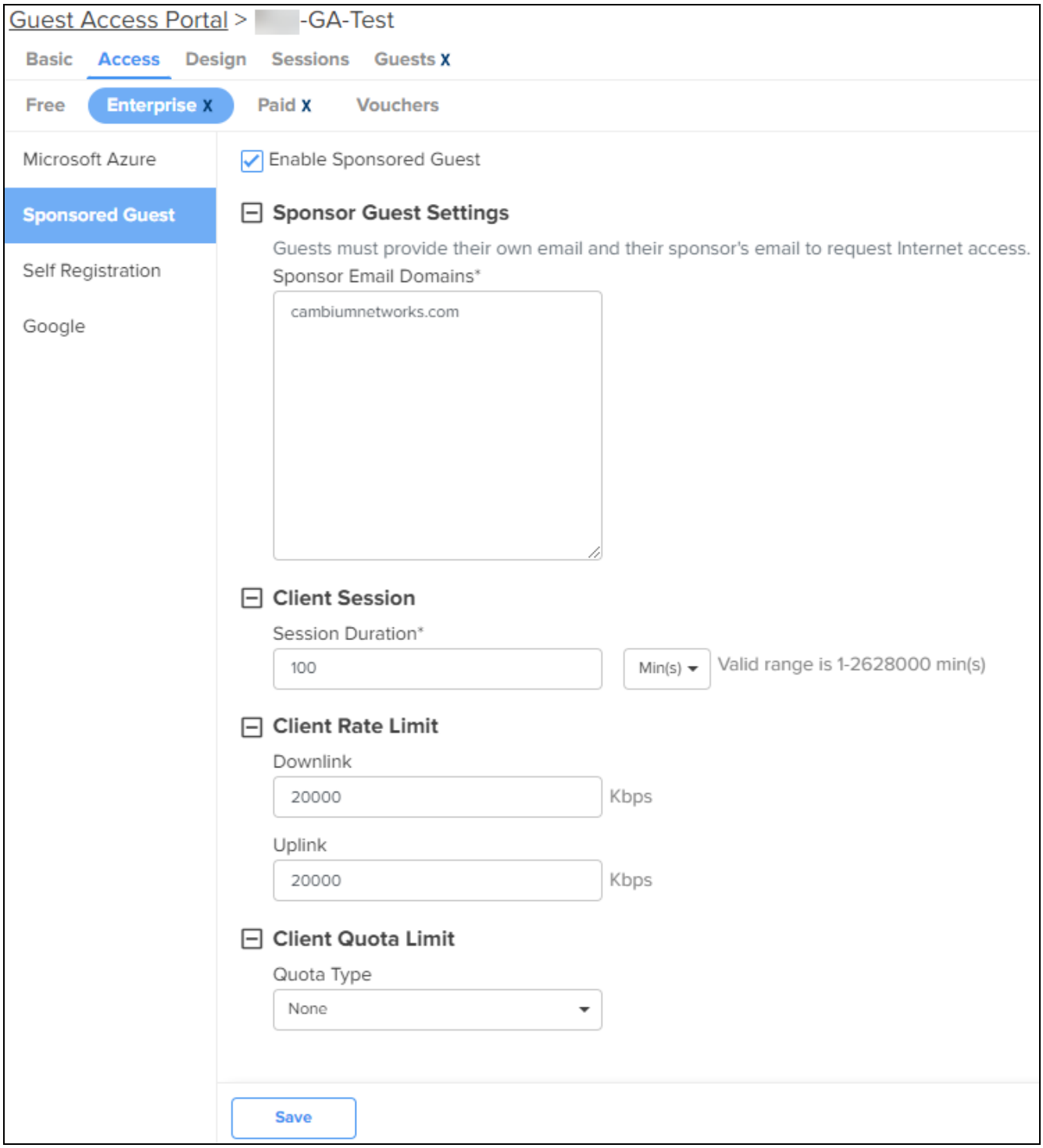
Enterprise Microsoft Azure access page enables Microsoft Azure users to log in to access the Enterprise Wi-Fi. To set up users to authenticate from Microsoft Azure, navigate to **Network Services** > **Guest Access Portal** > **Access** > **Enterprise X** > **Microsoft Azure**, complete the following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



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**:



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.

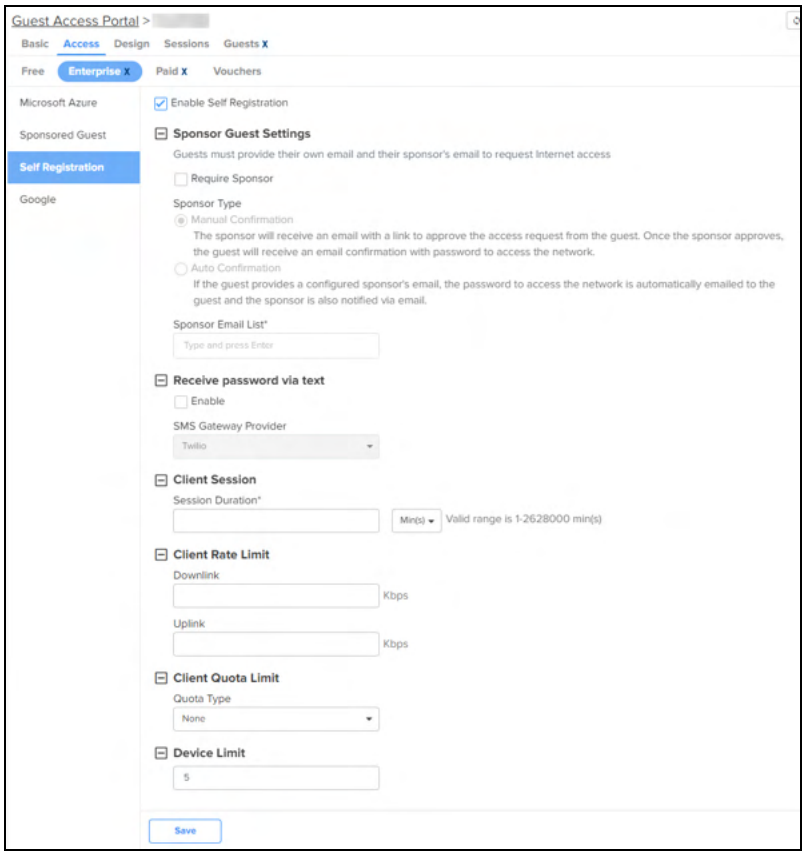


Table 152 *Self Registration Parameters*

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: • **Manual Confirmation**—The sponsor receives an email for approving the guest's access request. After approval, the guest receives an email confirmation along with the password to connect to the wireless network. • **Automatic Confirmation**—If the guest provides a configured sponsor's email address, the password to access the network is automatically emailed to the guest and the sponsor is also notified via email.
Sponsor Email List	Configure the list of sponsor email addresses for approving access

Table 152 *Self Registration Parameters*

Parameter	Description
	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): • 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: • 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.

Table 152 *Self Registration Parameters*

Parameter	Description
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.

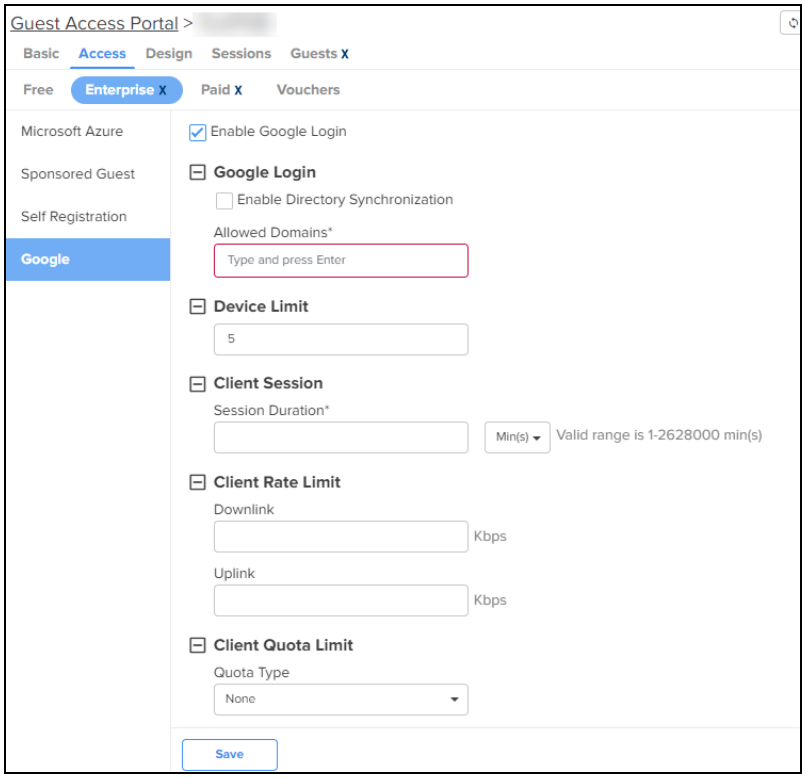


Table 153 *Google Parameters*

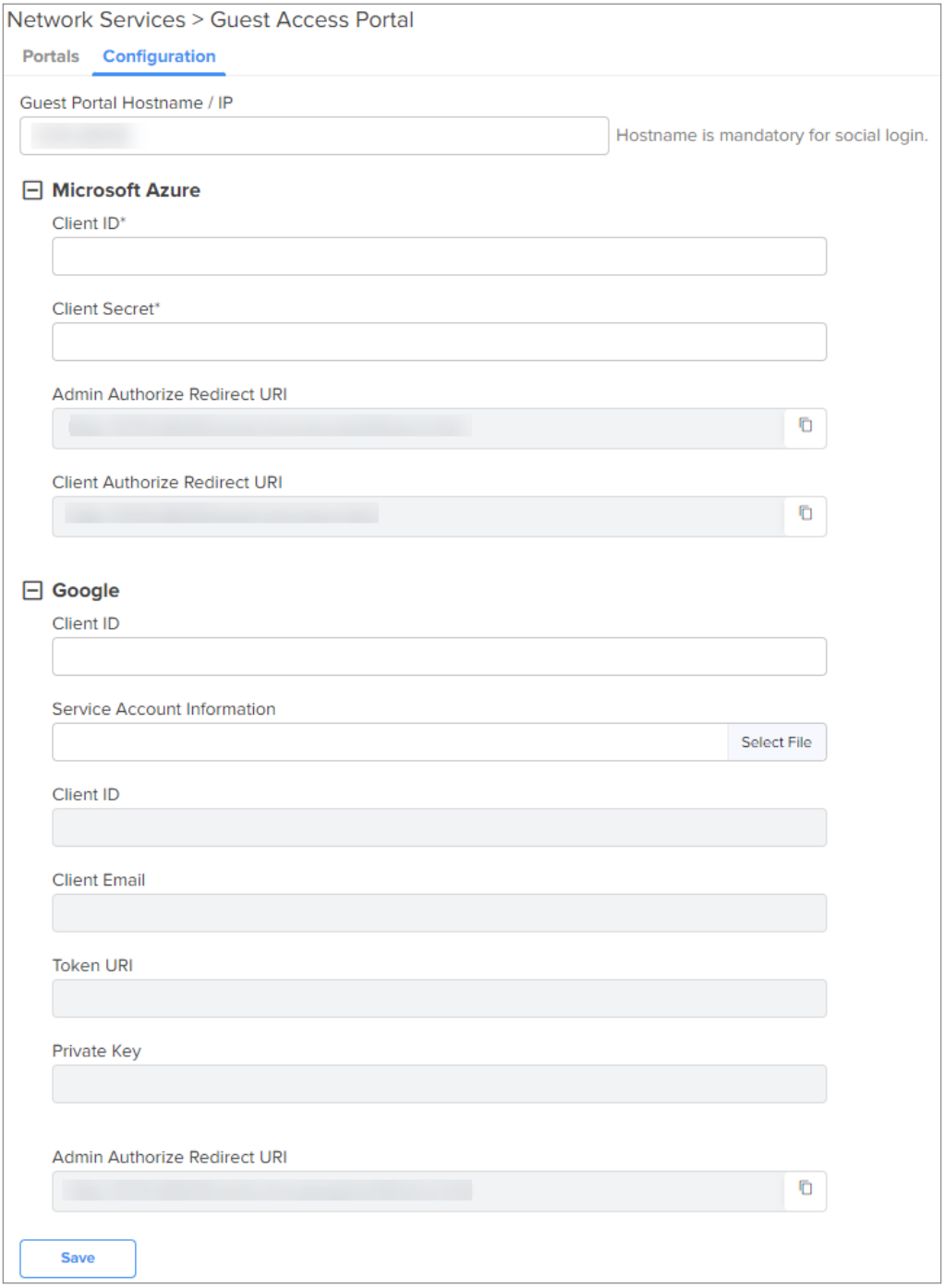
Parameter	Description
Enable Google Login	Select the checkbox to enable Google-based Wi-Fi access and configure the following parameters.
Device Limit	Specifies the number of devices that the guest can connect to the wireless network. Default: 5.
Google Login	
Enable Directory Synchronization	Select 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: • 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.

Configuring Additional Parameters for Guest Access Portal

In addition to the Guest Access portal configuration, you must configure certain additional parameters.

Complete the following steps:

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



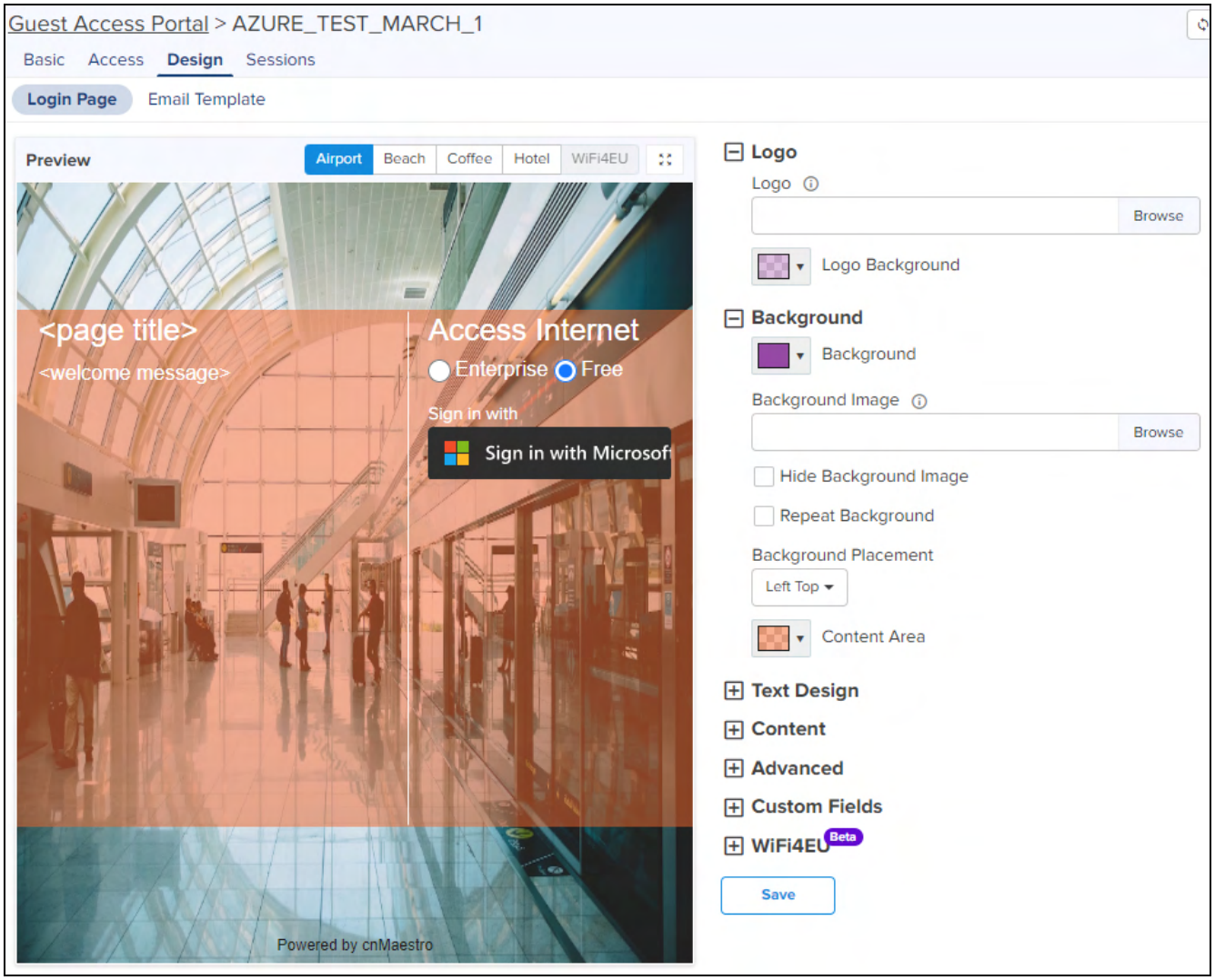
2. In the **Google** section, enter the **Client ID** that you generated in Google APIs. See API Key Generation-Google for more information.
3. In the **Service Account Information** field, click **Select File**.

   Search for the JSON file that you downloaded from the Google Service Account. See Creating Google Service Account for more information.

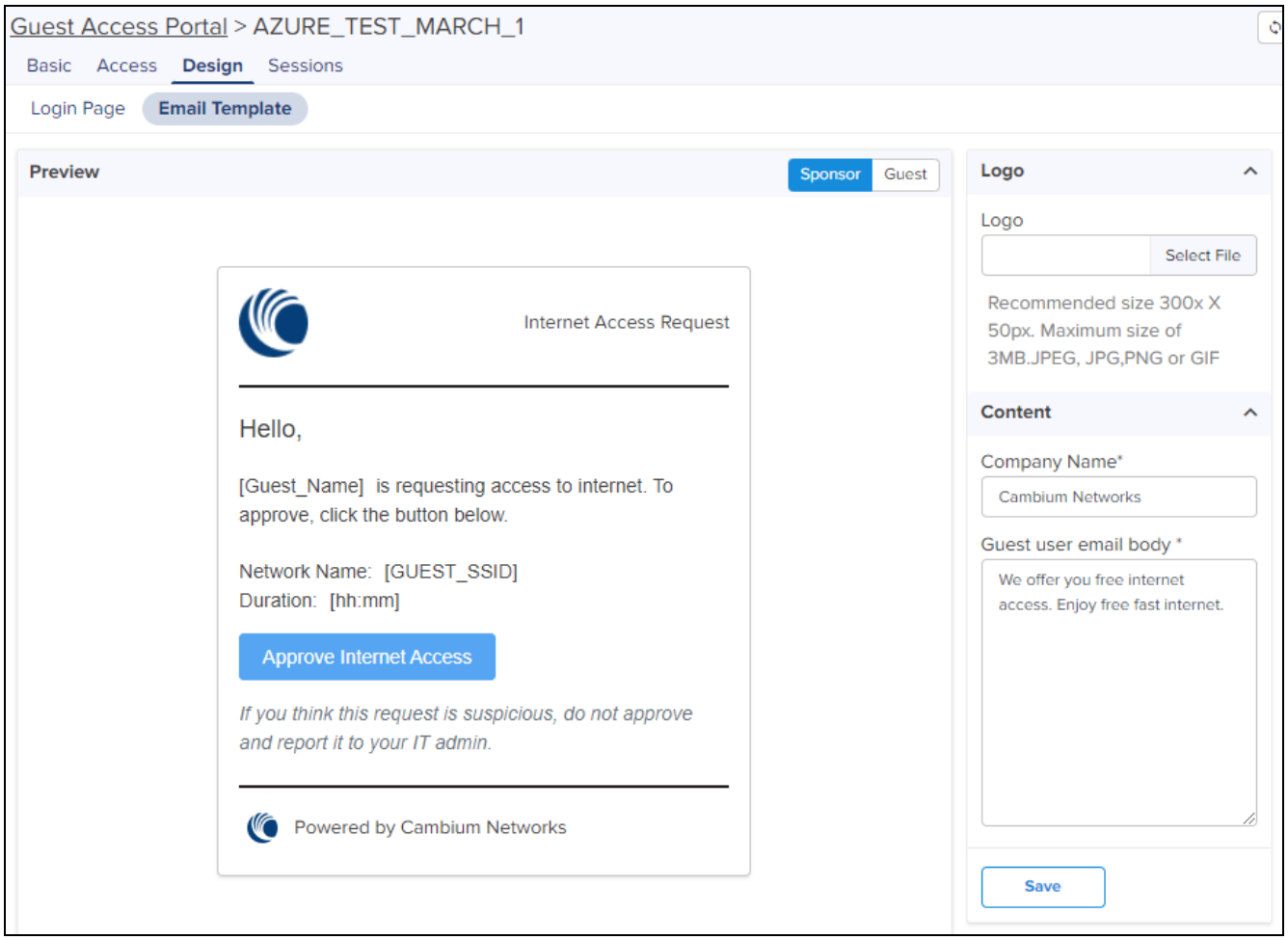
   The information is auto-populated.
4. Click **Save**.

Designing the Guest Access Login Page and Email Templates

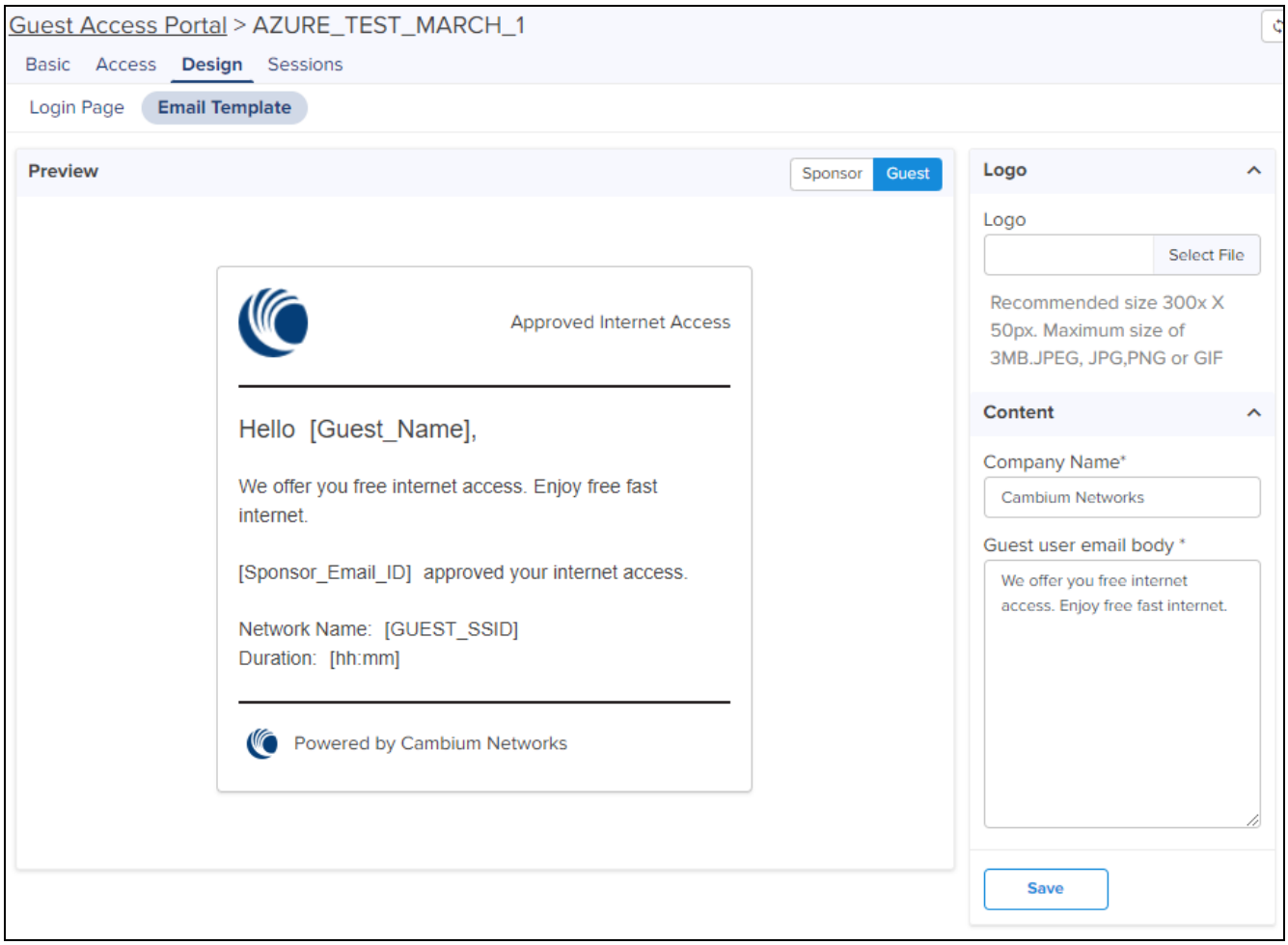
To design the guest login page for users to see when requesting access, navigate to **Network Services** > **Guest Access Portal** > **Design** > **Login Page**, complete the following parameters, and click **Save:**



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:**



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:**



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.

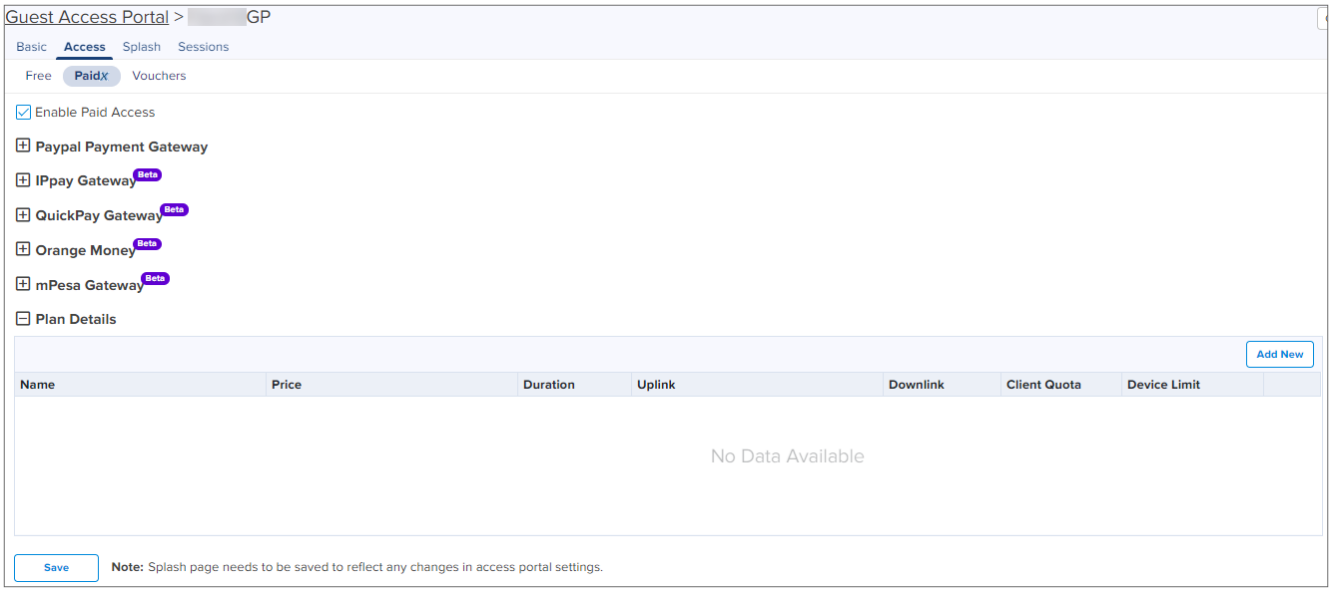
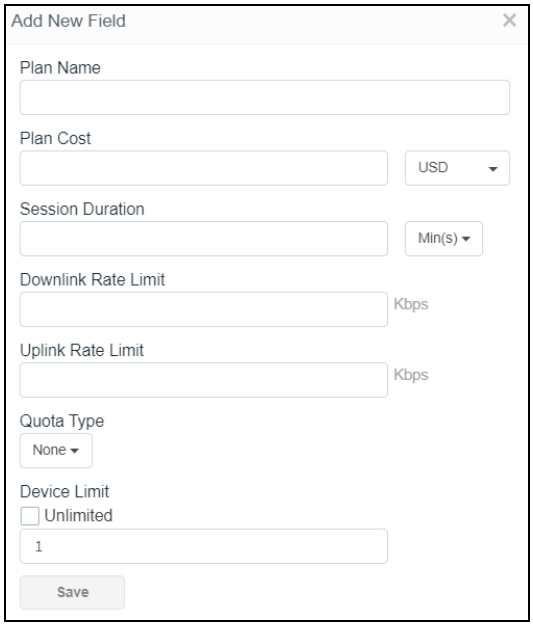


Table 154 *Paid Access Type Parameters*

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.



Voucher Access Type Configuration

Important Points to Remember

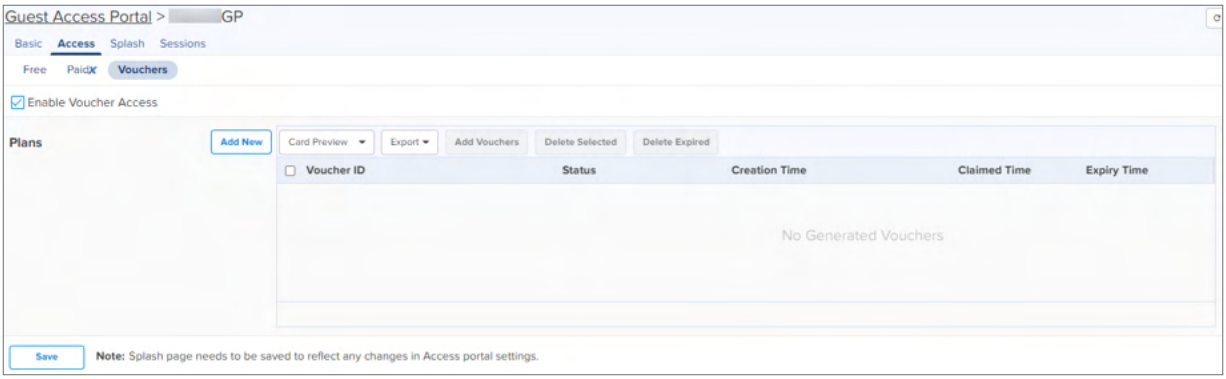
- Vouchers can only be generated after enabling Vouchers and creating at least one Voucher plan.
- The maximum number of vouchers that users are allowed to create per Voucher portal is as follows:
  - cnMaestro X—30,000

    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.



- Click **Add New**. The window with general and design parameters for the plan is displayed.

Table 155 *Voucher Access Type Parameters*

Parameter	Description
Design	• **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. With all the above parameters, administrators can create their own design for the card with text, color, and message to be displayed on card.
General	• **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.

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

Figure 457 ***Select a plan***

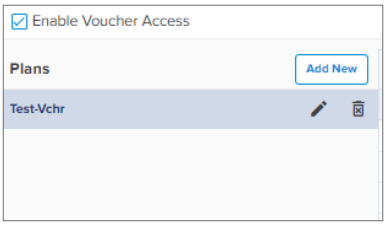
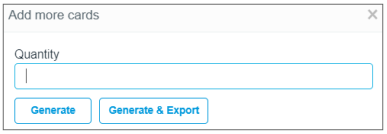


Figure 458 ***Add Vouchers***



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

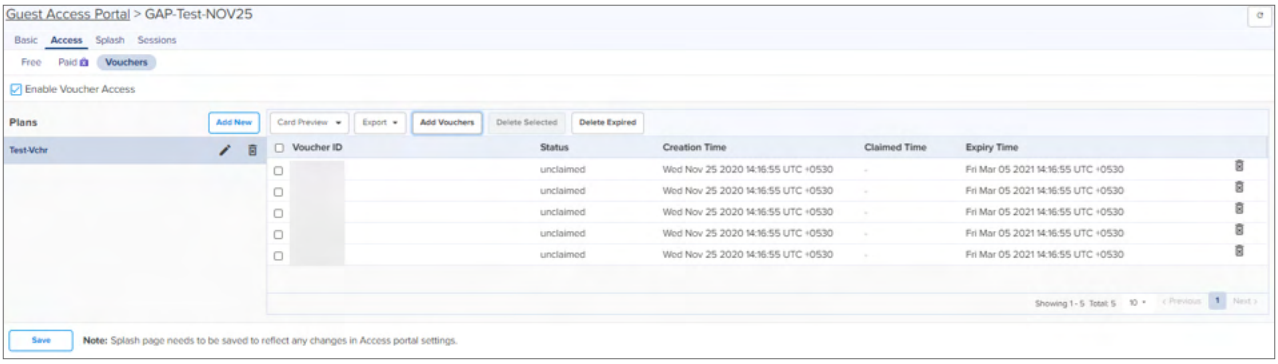


Figure 459 *Sample Voucher Code*

Note

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

Design Page

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

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

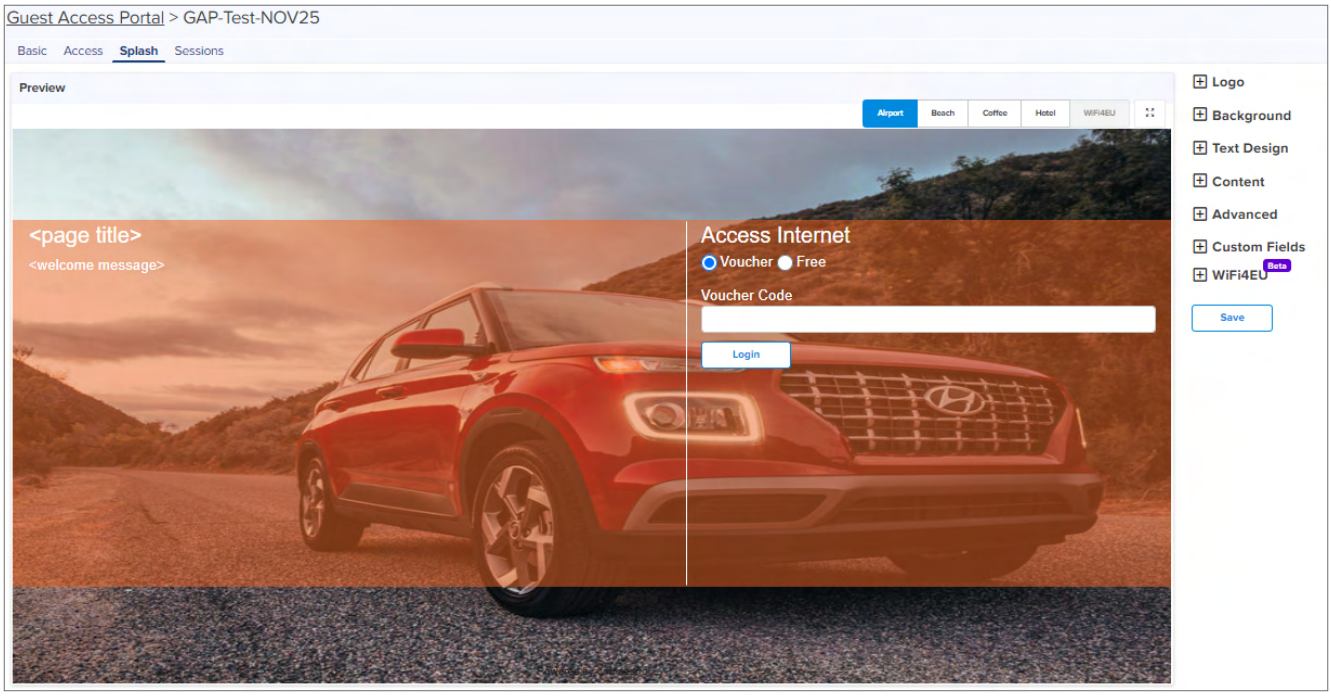


Table 156 *Design Page Parameters*

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. • 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. • Recommended image resolution—300 pixels × 50 pixels

Table 156 *Design Page Parameters*

Parameter	Description
	• 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.
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.

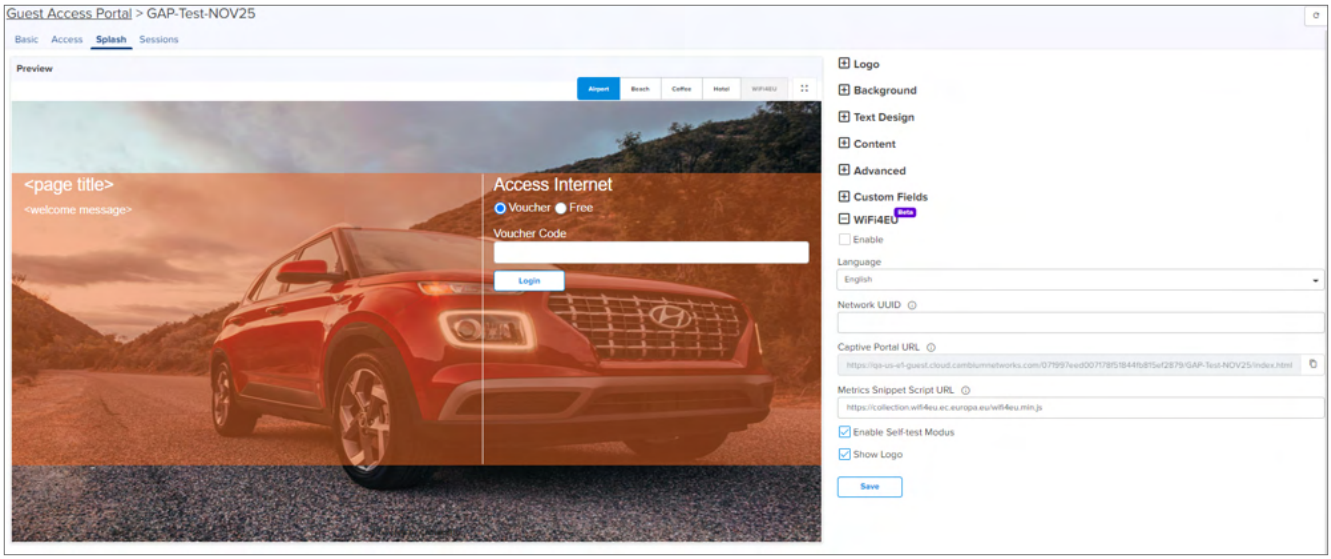


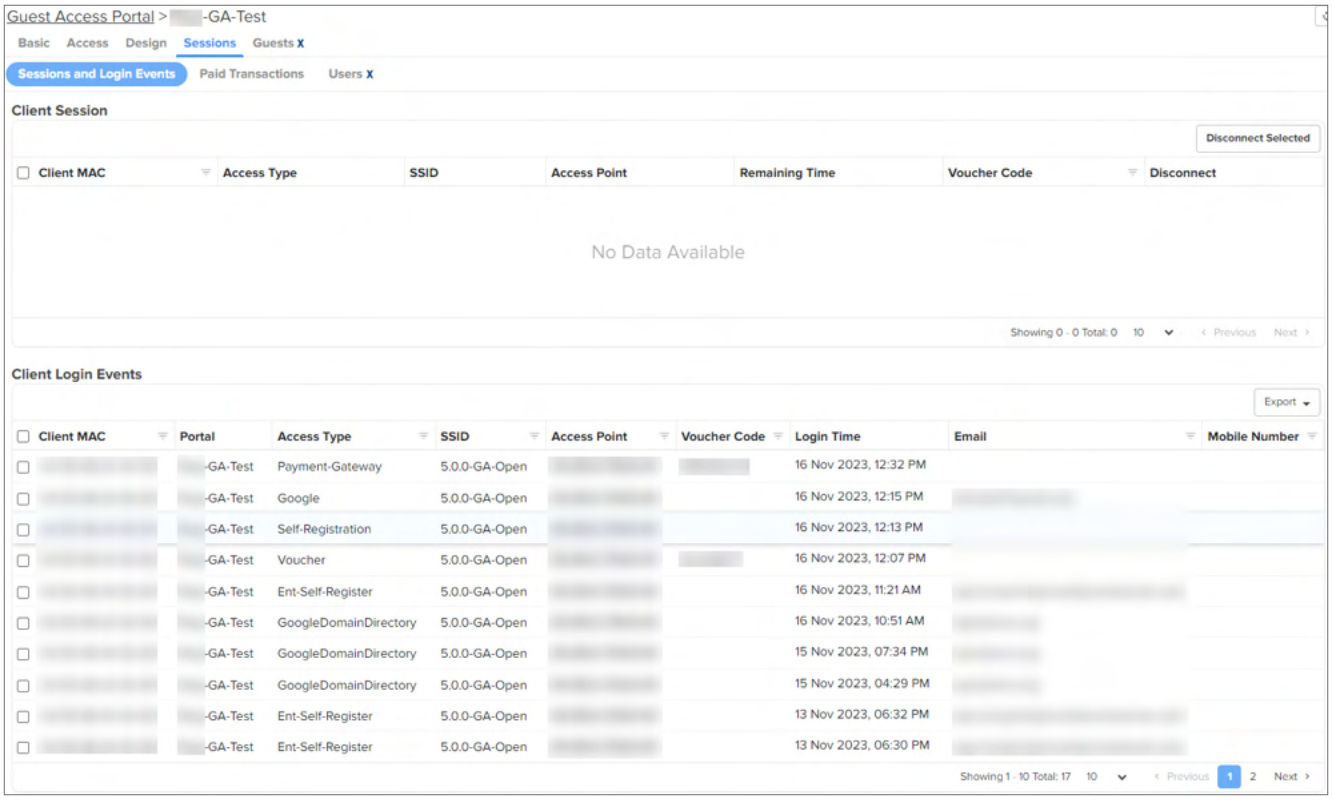
Table 157 *WiFi4EU Parameters*

Parameter	Description
General	• **Network UUID**: Universally Unique Identifier (UUID) that the EC attribute is generated when the network installation is created in the Installation. • **Language:** Allows to select the preferred language. • **Enable Self Test Mode**: Allows the browsers background script verification. • **Show Logo:** Displays the WiFi4EU logo provided by the European union.

Sessions

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

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



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.

Table 158 *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.

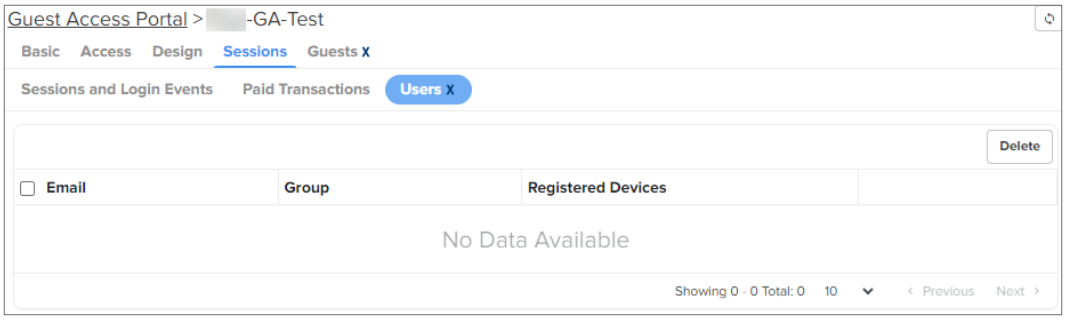


Table 159 *Users Table Parameters*

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.

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.

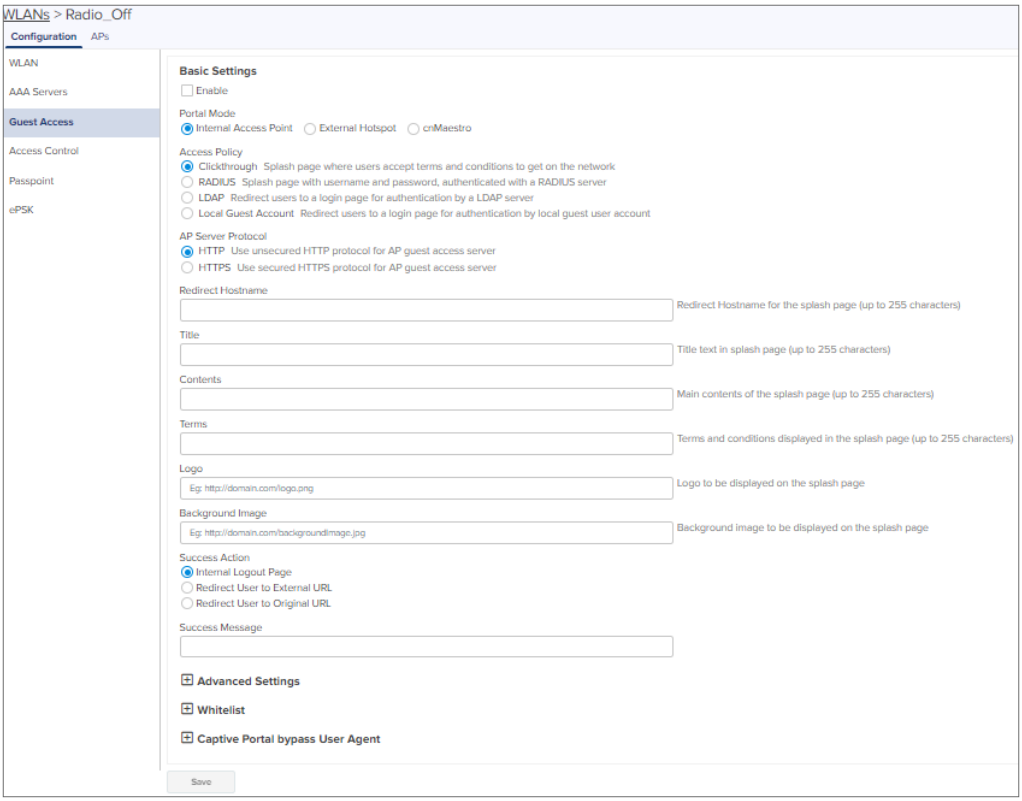
Note

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:

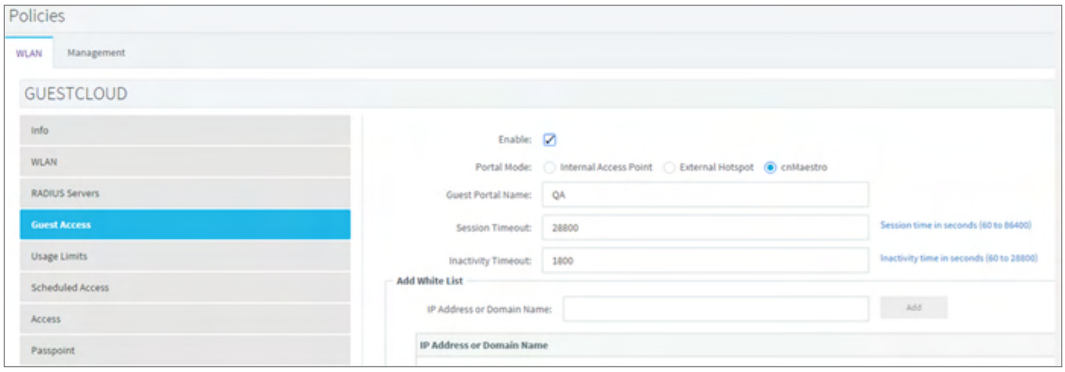
1. Login to the device.
2. Navigate to **Configuration** > **WLAN** > **Guest Access**.

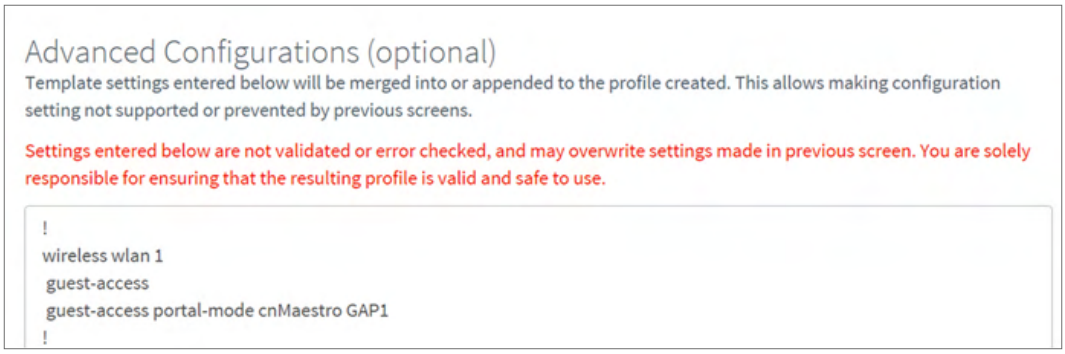


3. Enable the **Guest Access** checkbox.
4. Choose the **Portal Mode** radio as **cnMaestro**.
5. In the **Guest Portal Name** text box, select the name of the portal that was created in cnMaestro and enter the respective parameters.

Configuration at cnMaestro side

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

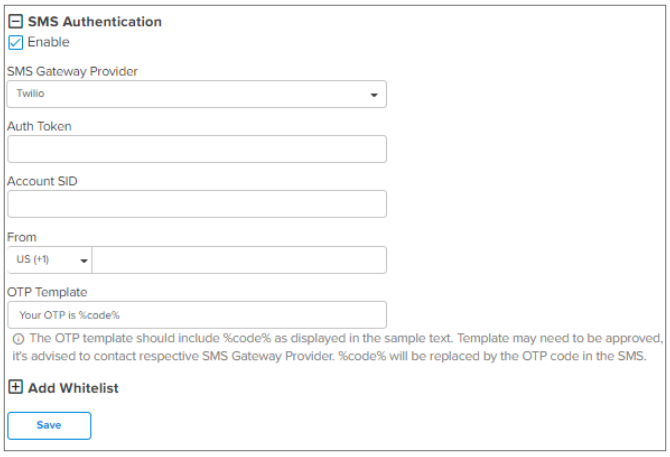




Access Types

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

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



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.

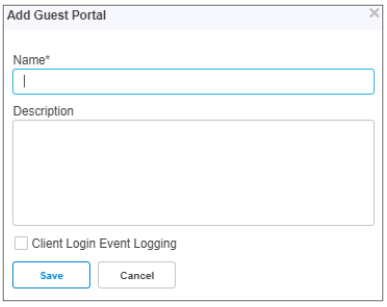
Guest Access using Social Login

Configuration

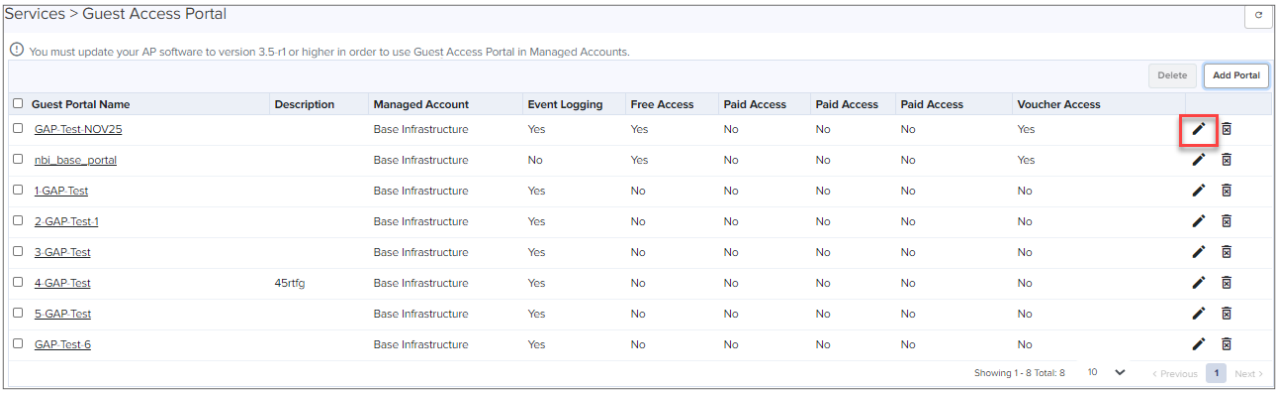
To achieve cnMaestro Guest Access using Social Logins like Google, Twitter, Facebook, and Office 365, perform the following steps:

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

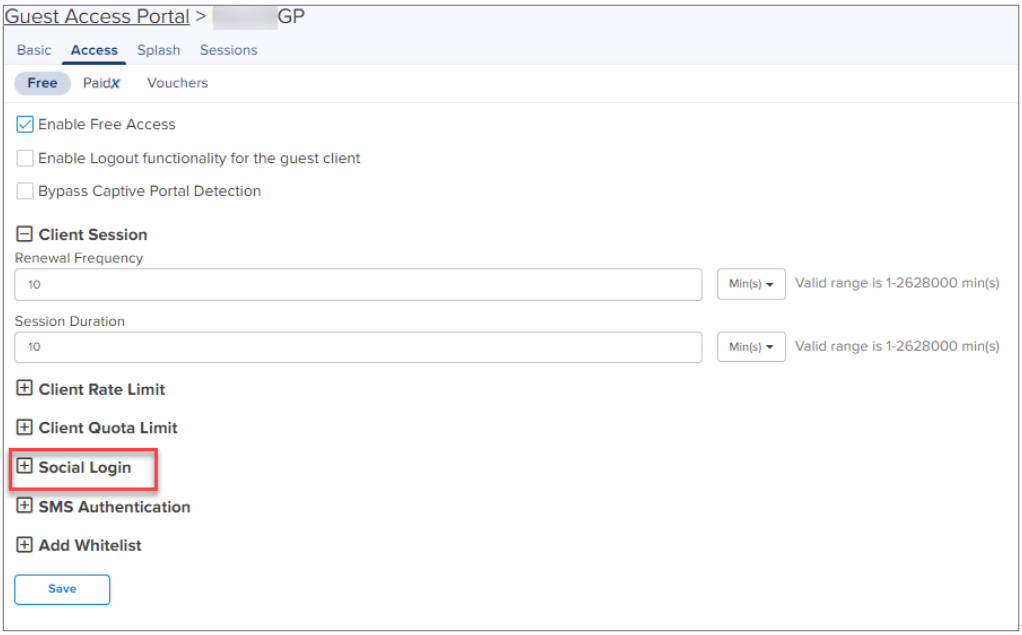
1. Login to cnMaestro and navigate to **Network Services** > **Guest Access Portal** > **Add Portal.**
2. Enter Portal Name, Description, enable logging for client login events.
3. Click **Save.**



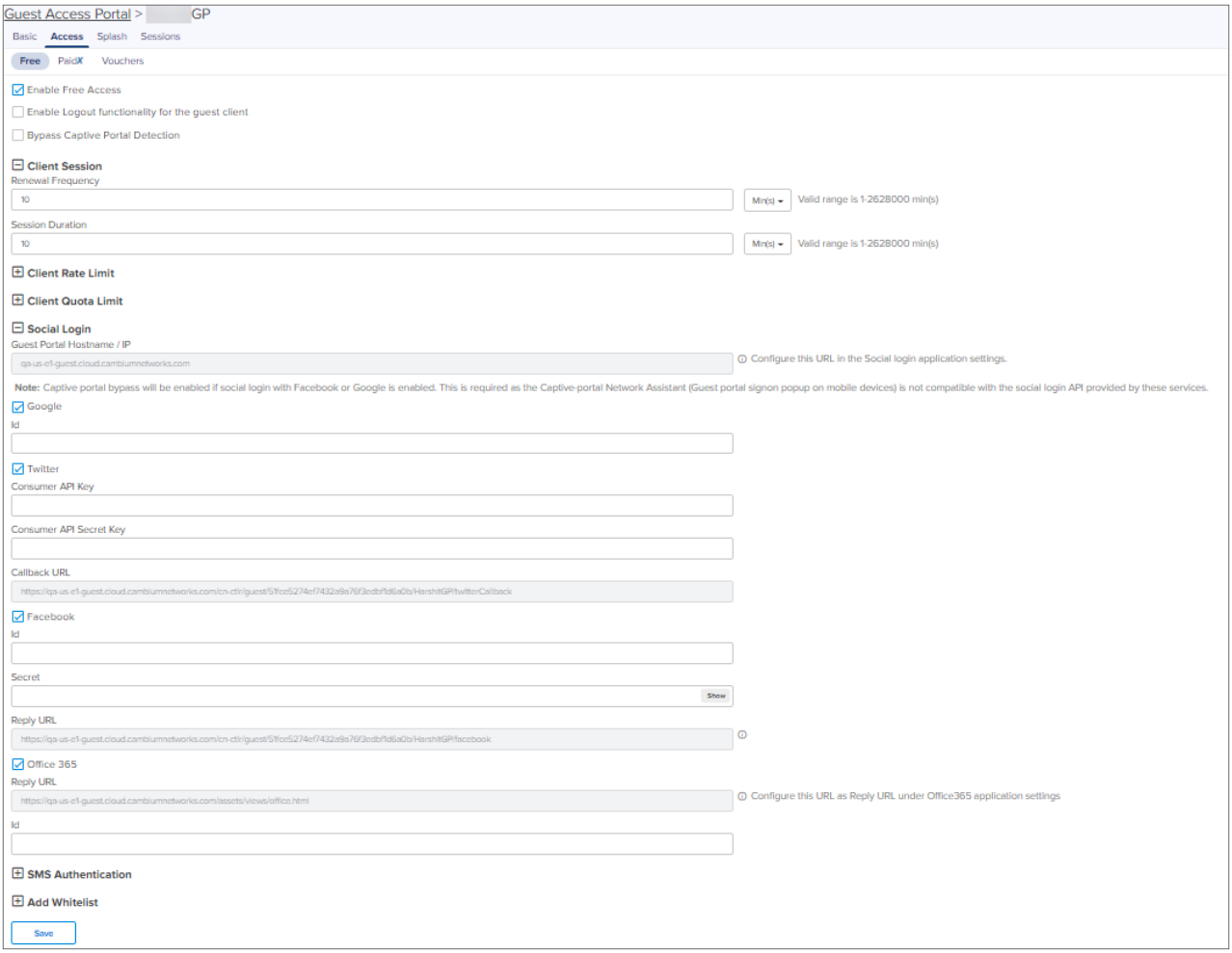
4. Click **Edit Guest Portal Details.**



5. Navigate to the **Access** > **Free** tab and expand the **Social Login** section.



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



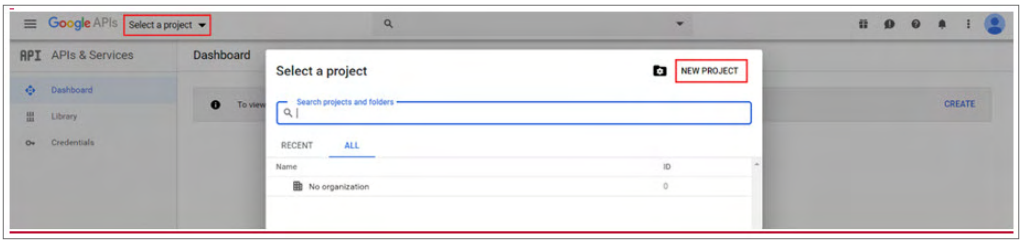
API Key Generation

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

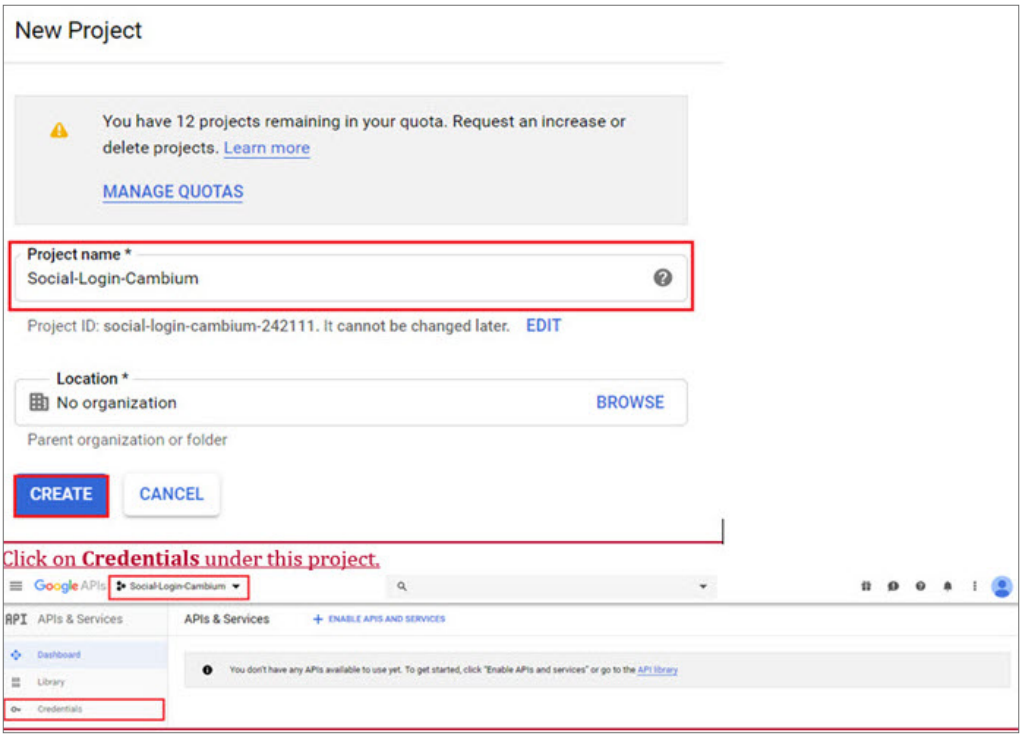
- Google
- Twitter
- Facebook
- Office 365

Google

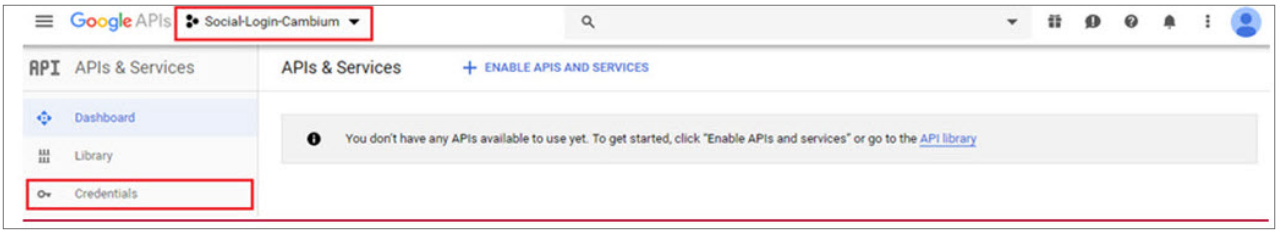
1. Login to Google Account and navigate to https://console.cloud.google.com/.
2. Click **Select a Project** and create a **New Project.**



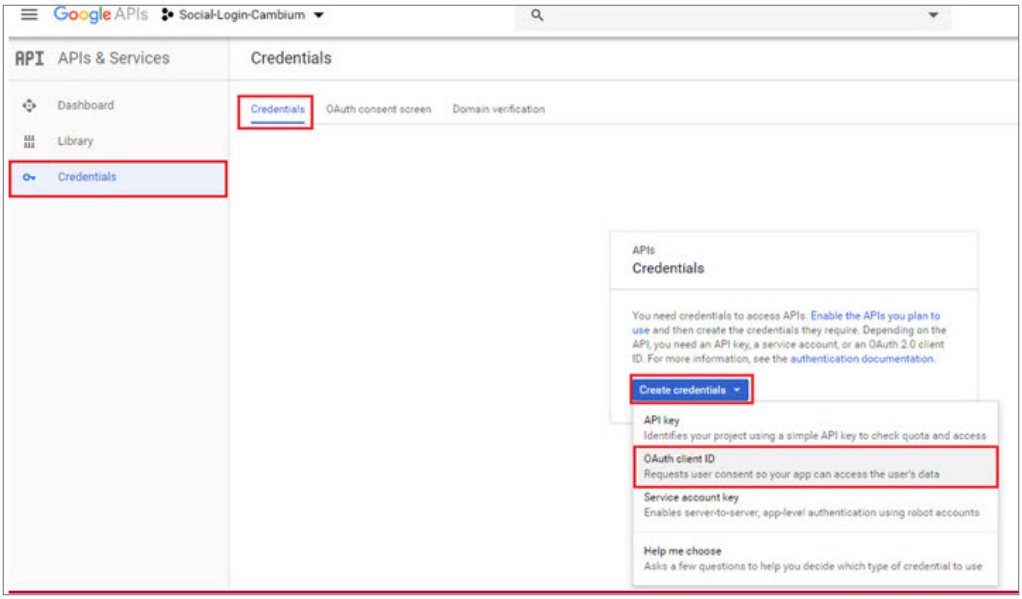
3. Give a name to the Project and click **CREATE**..



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

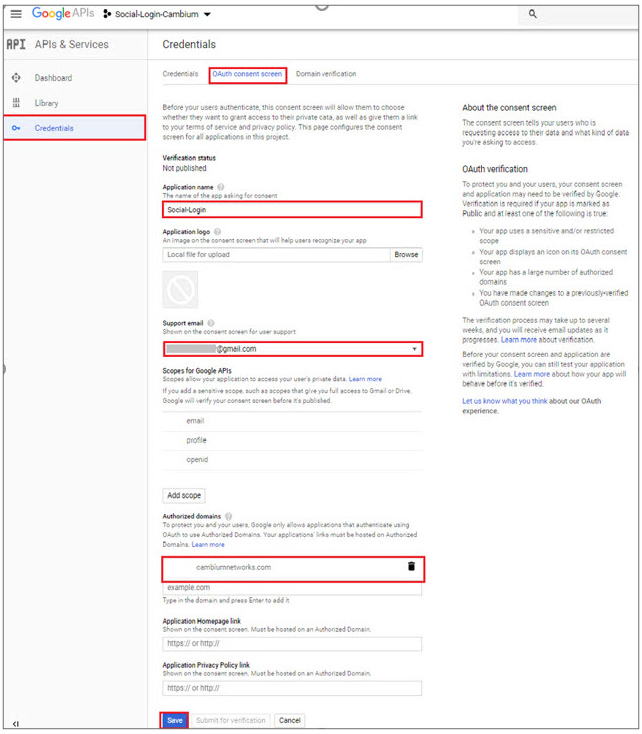


5. Under **Credentials** tab, create OAuth Client ID.

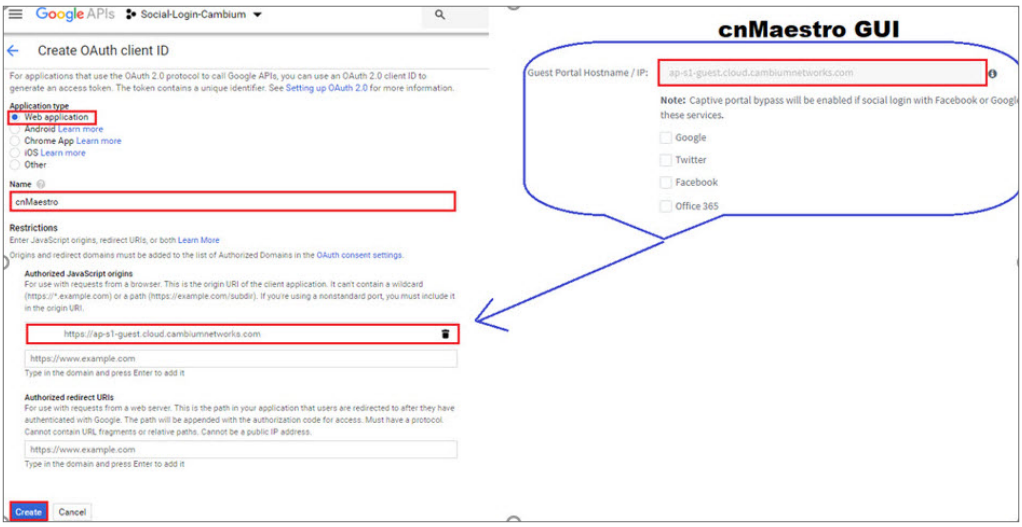


6. Click **Configure Consent Screen**

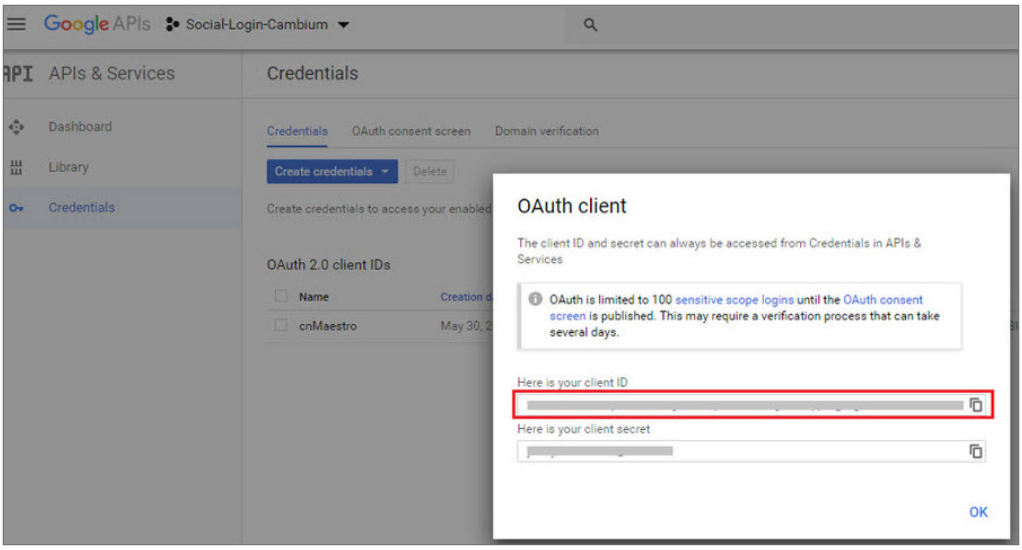
7. Assign a name to the application, map to an email address, add cambiumbnetworks.com to the authorized domain and click **Save**.



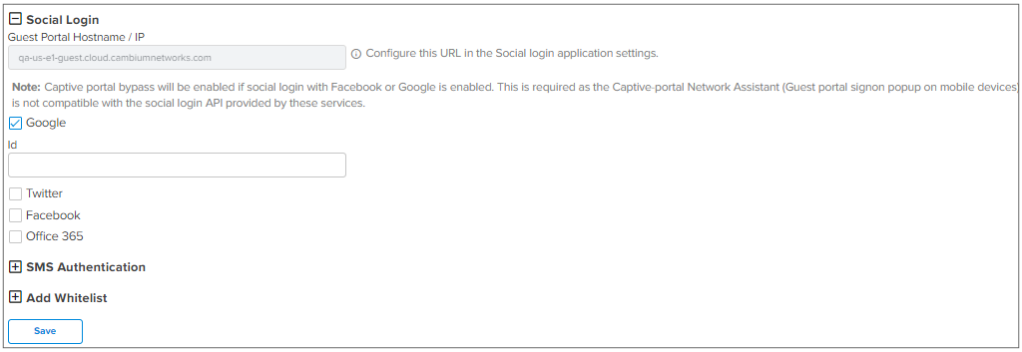
8. Once clicked **Save** for above page it redirects to creation of OAuth Client ID.
9. Select **Application type** as **Web Application**, give a Name, add Guest Portal Hostname URL/IP which you will get from cnMaestro UI and click **Create**.



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

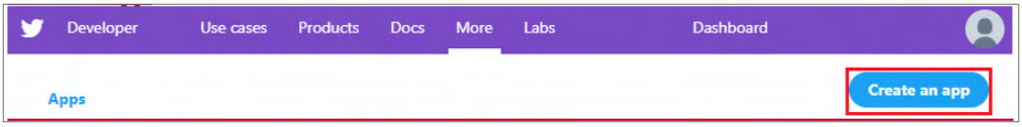


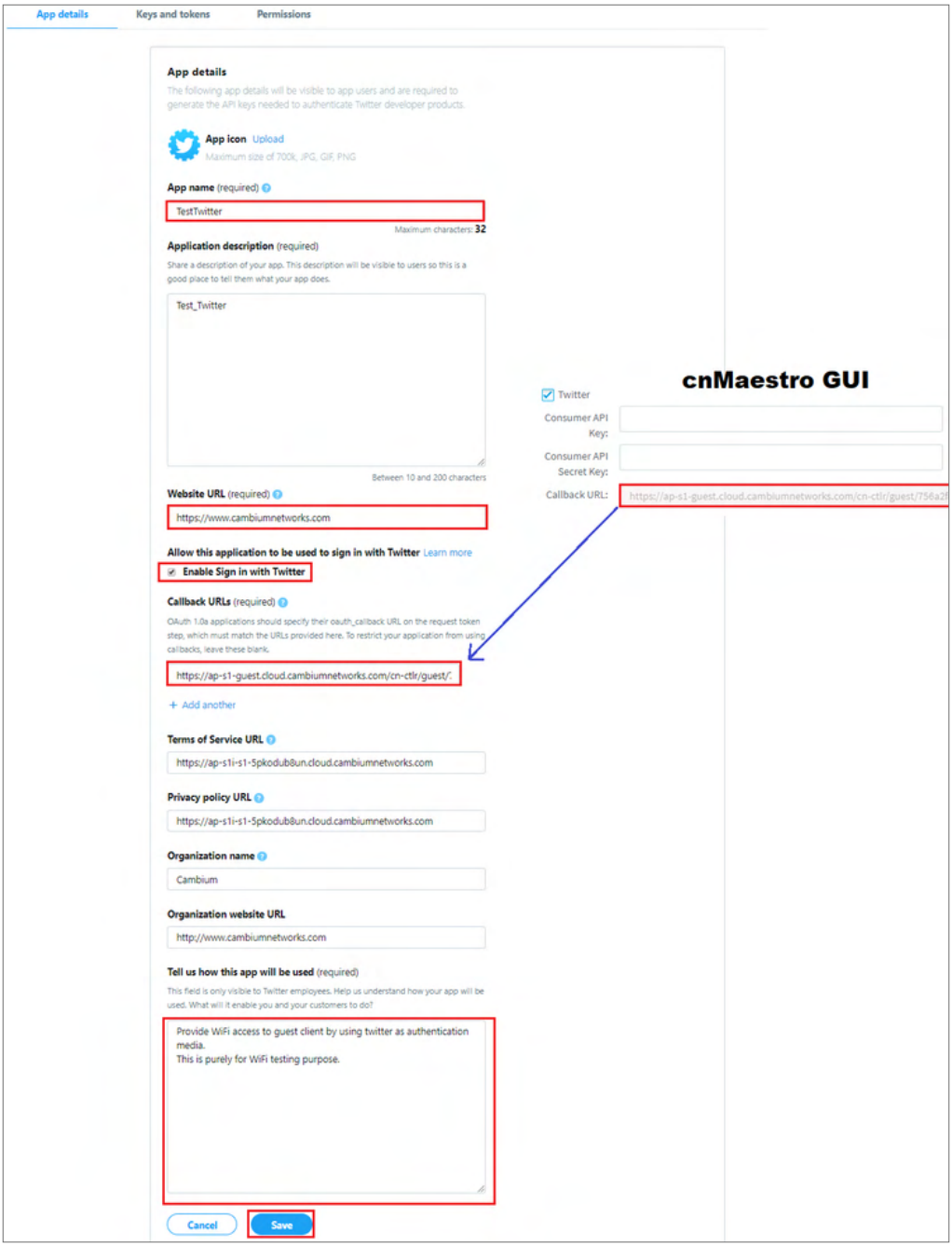
11. Copy the Client ID and paste it to the cnMaestro enabling Google under Social Logins and click **Save**.



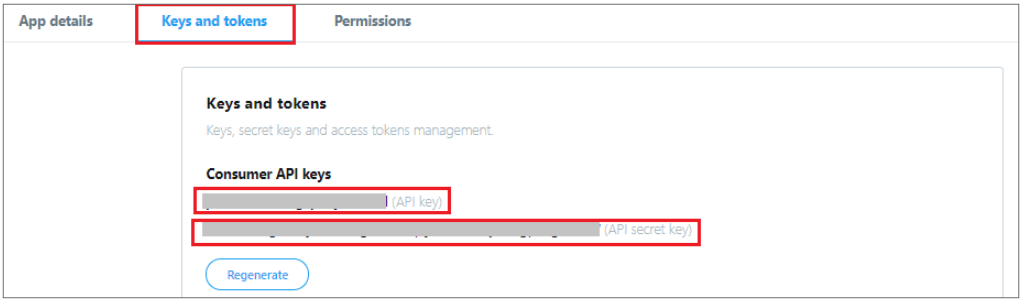
Twitter

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

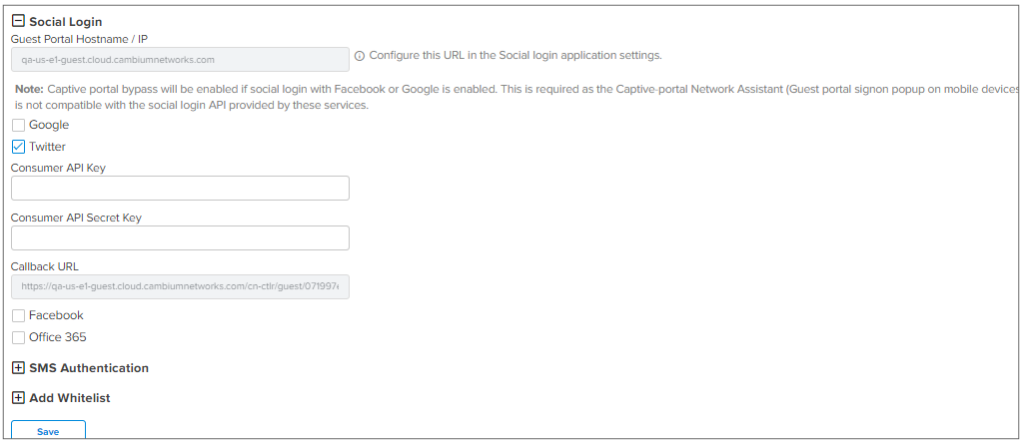




2. Click **Keys** and **Tokens** and copy **Consumer API Key** and **Consumer API Secret Key**..

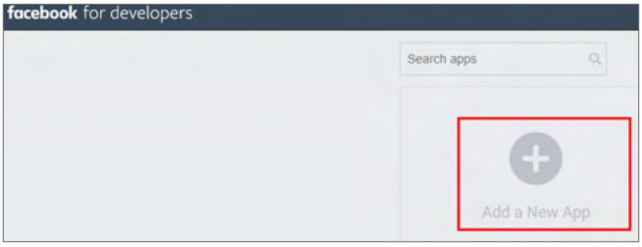


3. Paste them to cnMaestro GUI for Twitter social login.

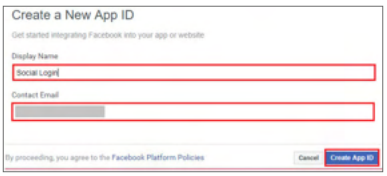


Facebook

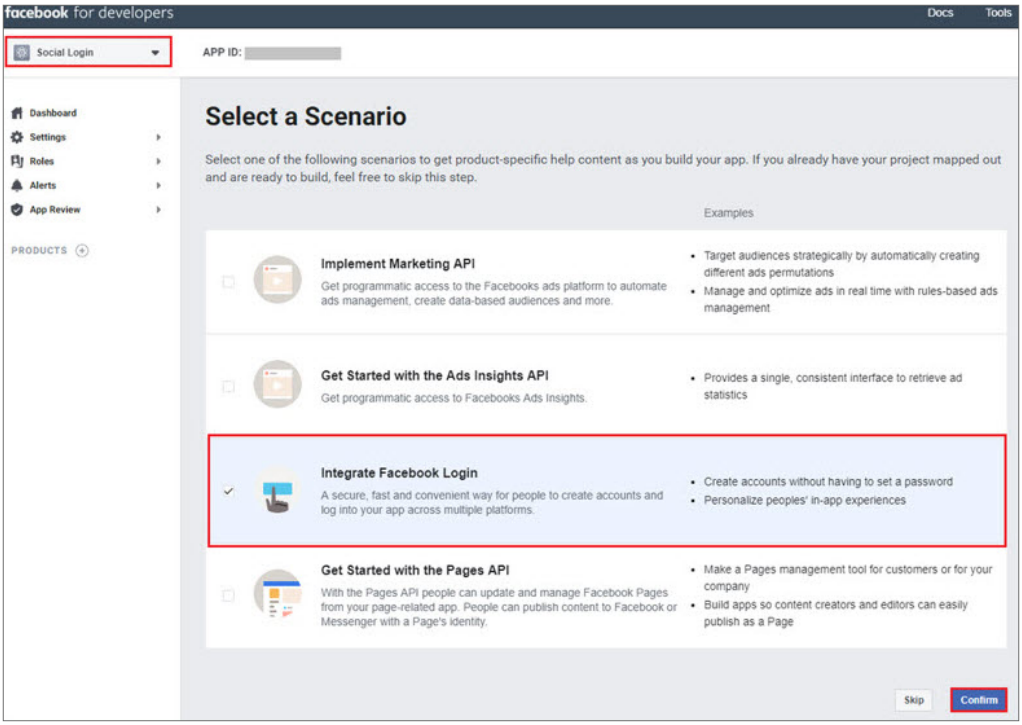
1. Login to Facebook Account and access **https://developers.facebook.com/apps/** and click **Add a New app**.



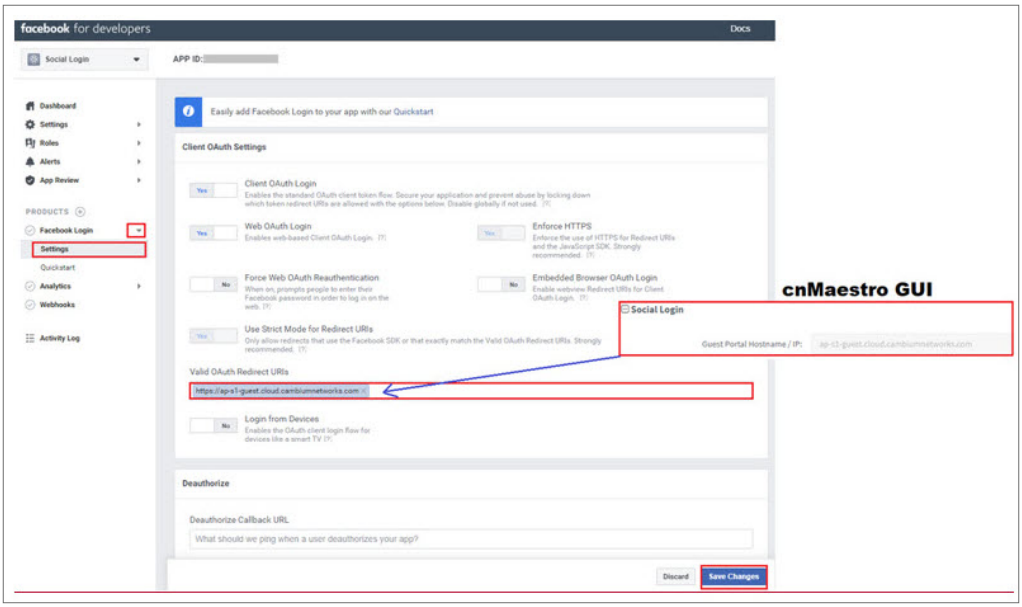
2. Enter App **Display Name**, **Contact Email**, and click on **Create App ID**.



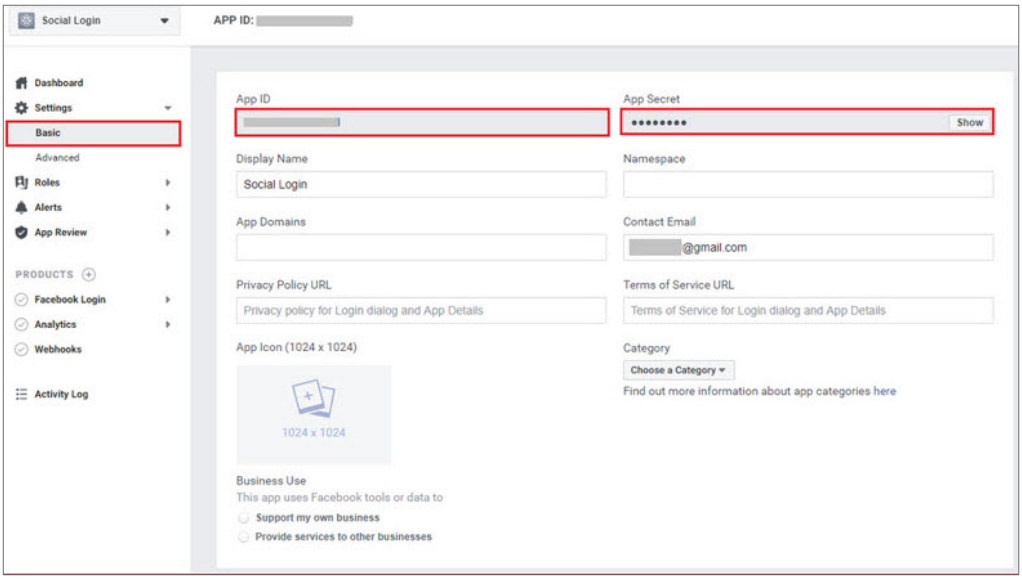
3. Select a Scenario as Integrate Facebook Login and click **Confirm.**

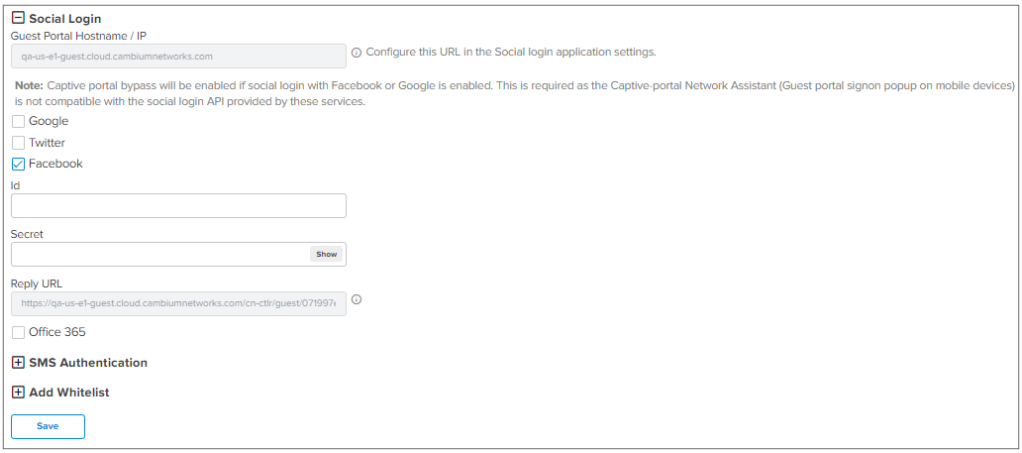


4. Navigate to **Settings** tab under Facebook Login and add Guest Portal Hostname from cnMaestro to Valid OAuth Redirect URLs section and click **Save Changes**.



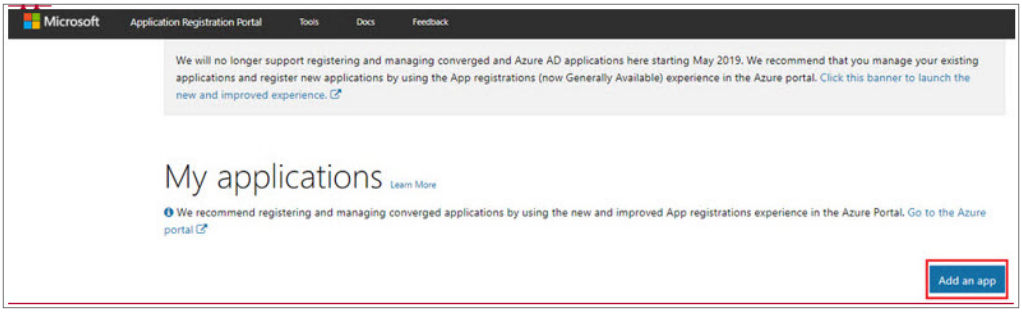
5. Navigate to **Settings** > **Basic** and copy **App ID** and **App Secret**.

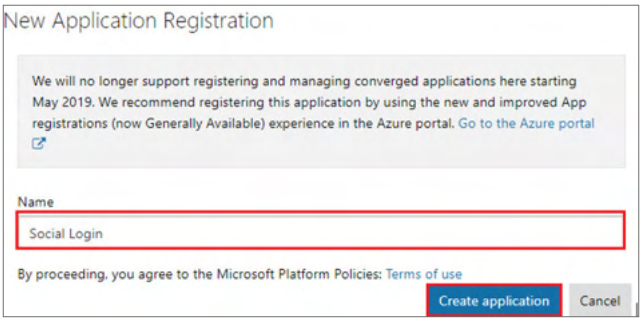




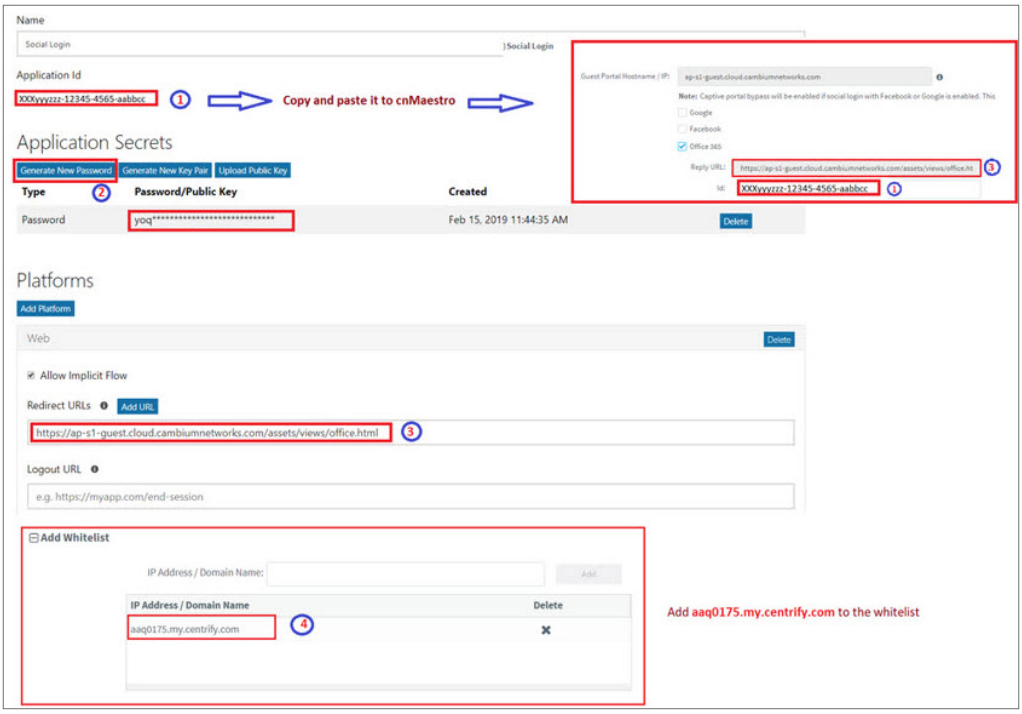
Office 365

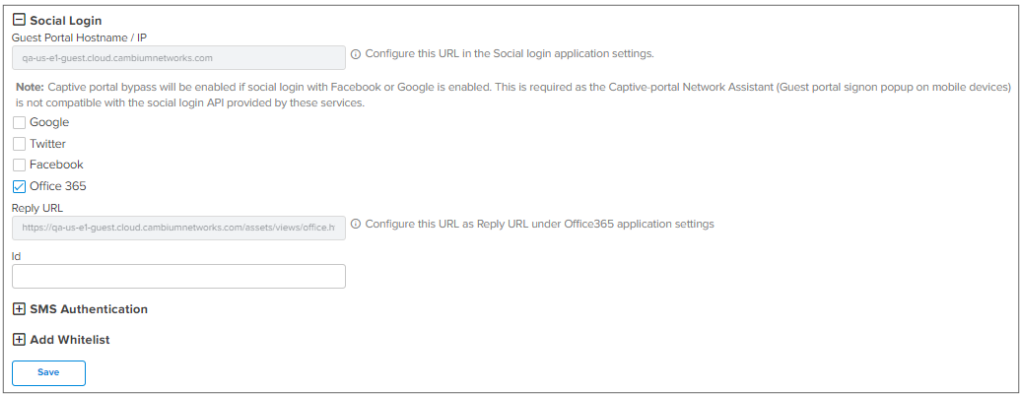
1. Login to Office 365 Account and access https://apps.dev.microsoft.com/ and click **Add an app**.





2. Upon Adding your App name and clicking Create application, it redirectes 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.

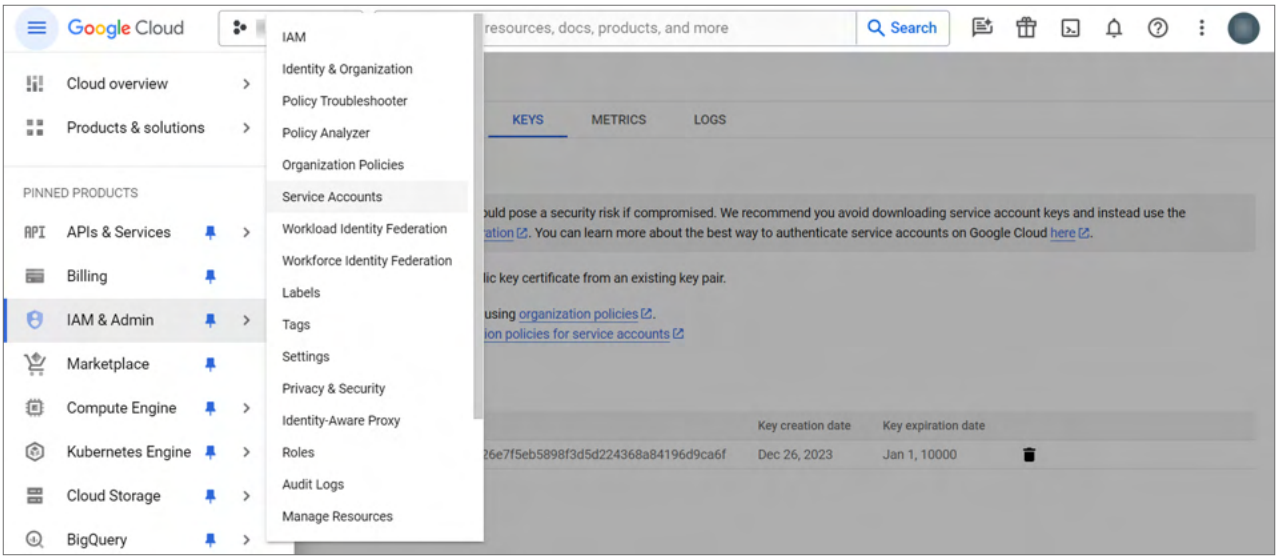




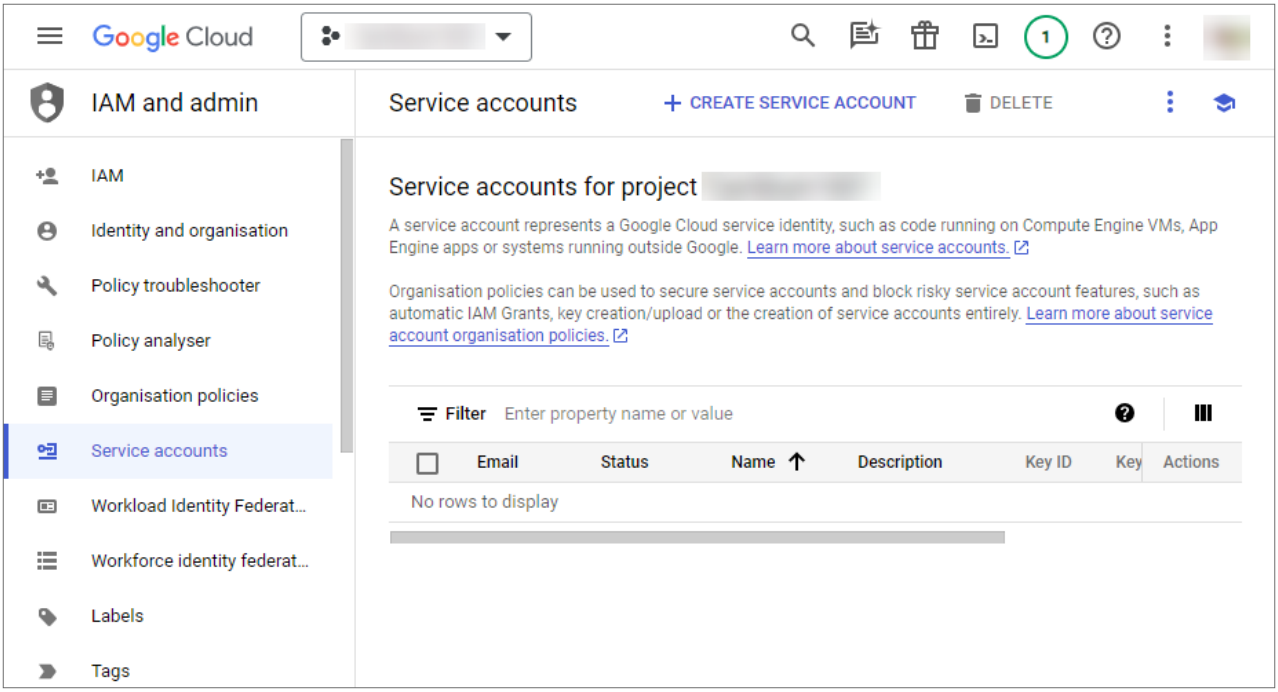
Creating Google Service Account

To create a Google Service Account for Guest Access Portal configuration and obtain the JSON file, complete the following steps:

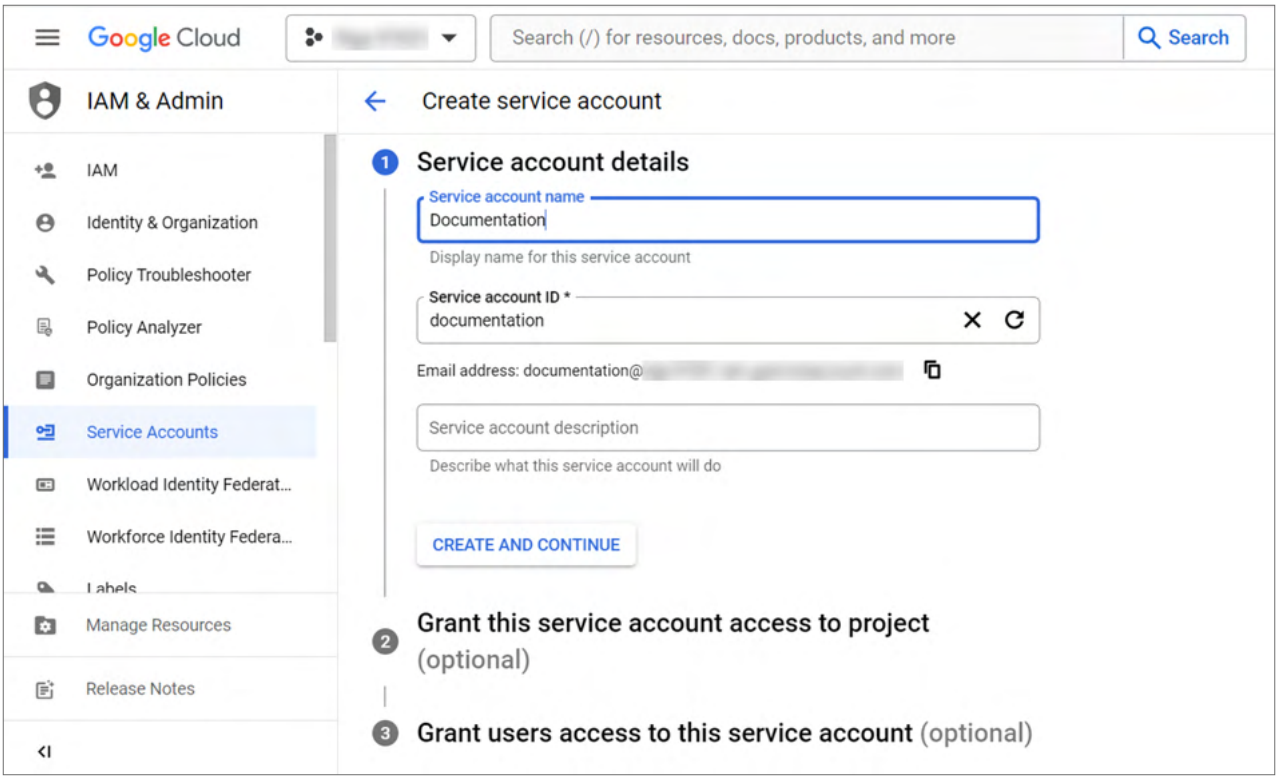
1. Login to your Google account and navigate to https://console.cloud.google.com/.
2. Navigate to **IAM & Admin** > **Service Accounts**.



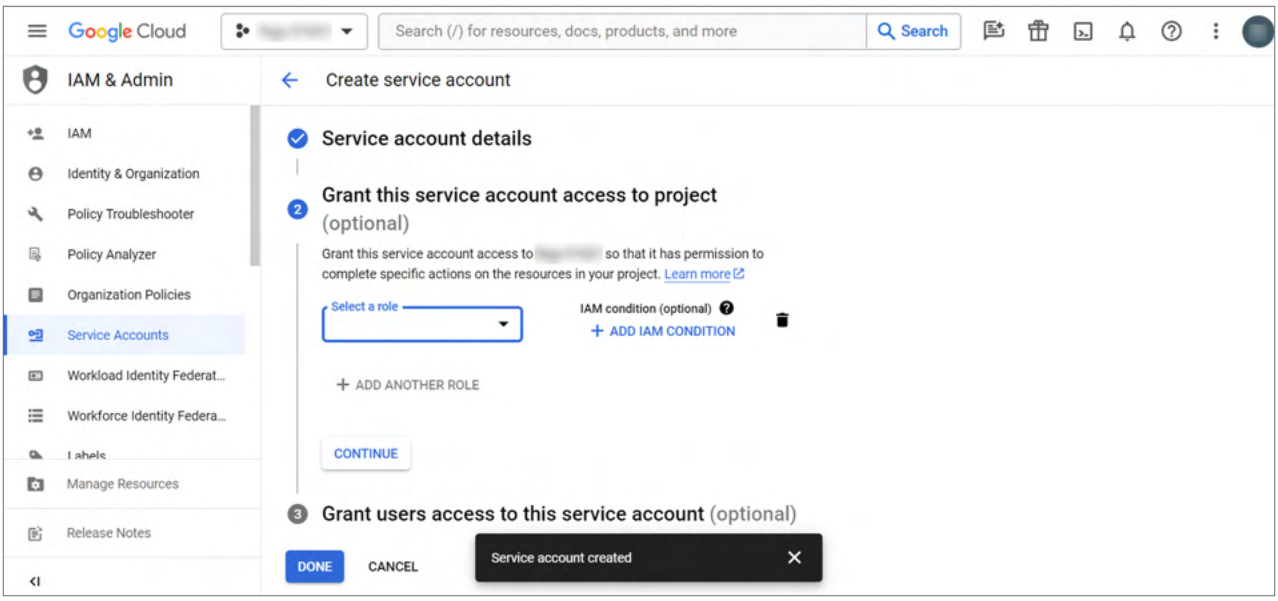
3. Click **Create Service Account**.



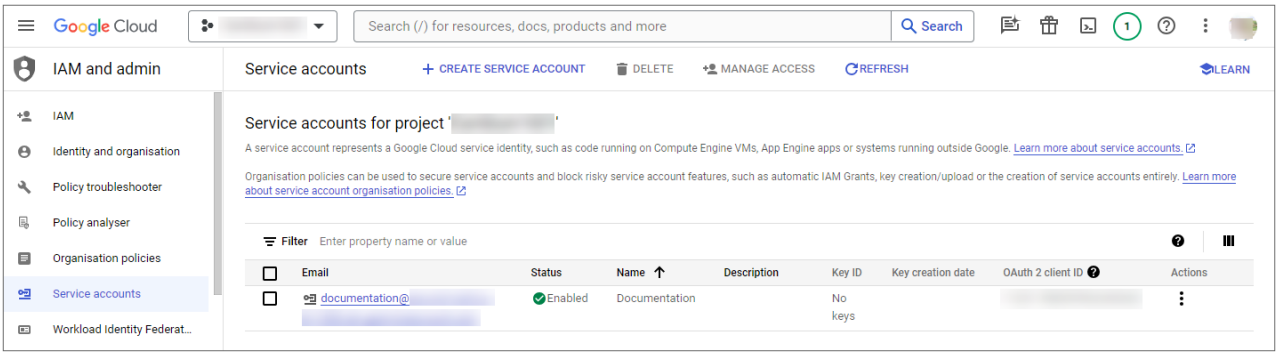
4. Provide a unique name to the service account and click **Create and Continue**.



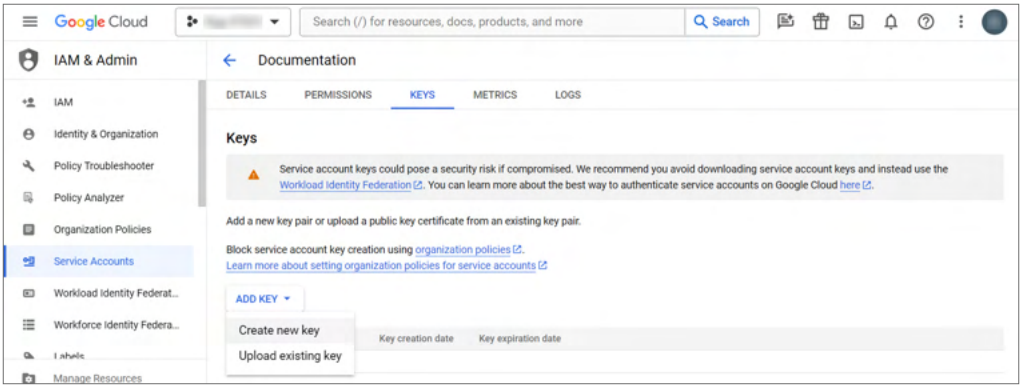
5. Click **Done**.



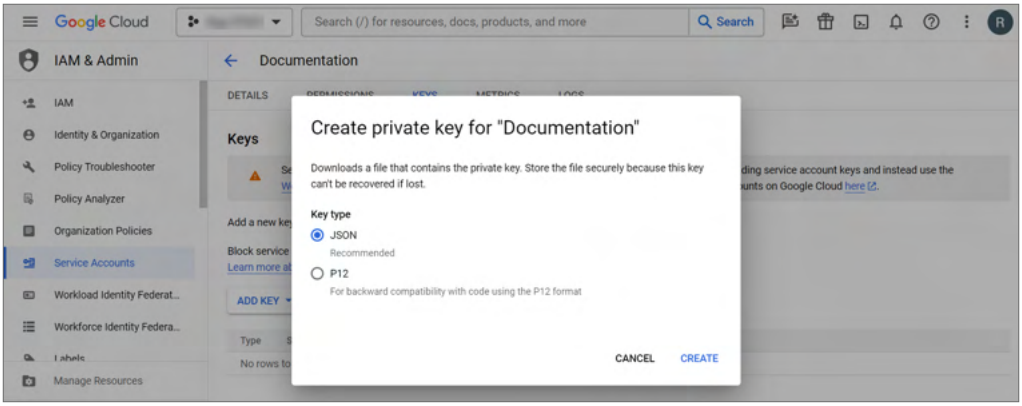
6. Click the Service Account that you created and navigate to the **Keys** tab.



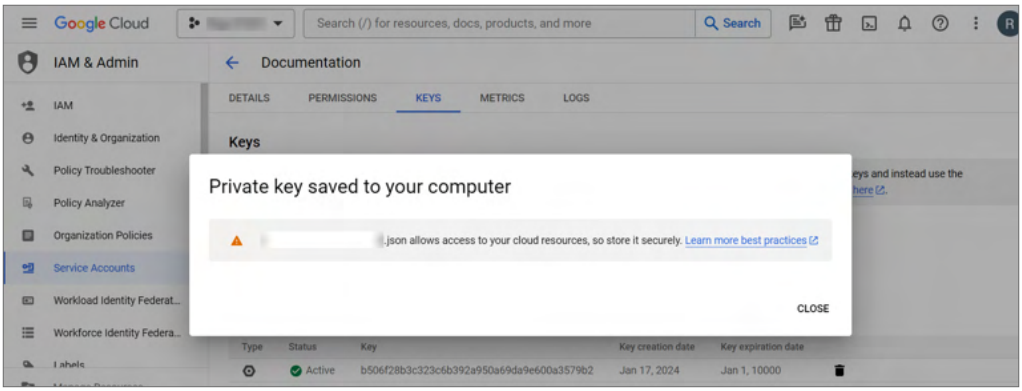
7. From the **Add Key** dropdown list, select **Create new key**.



8. Select **JSON** as the **Key type** and click **Create**.

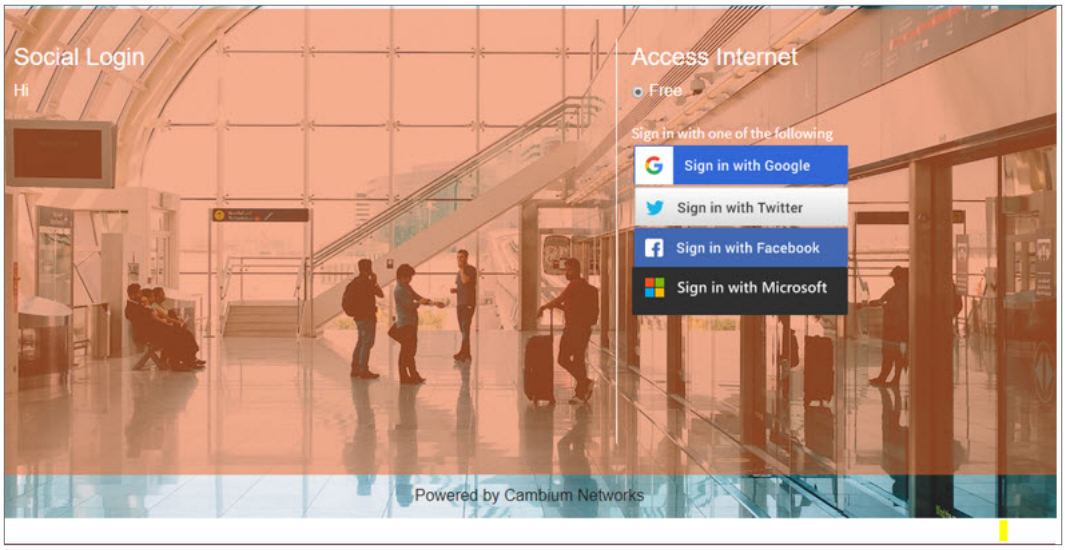


9. The private key in the JSON file format is downloaded automatically.



Sample Template

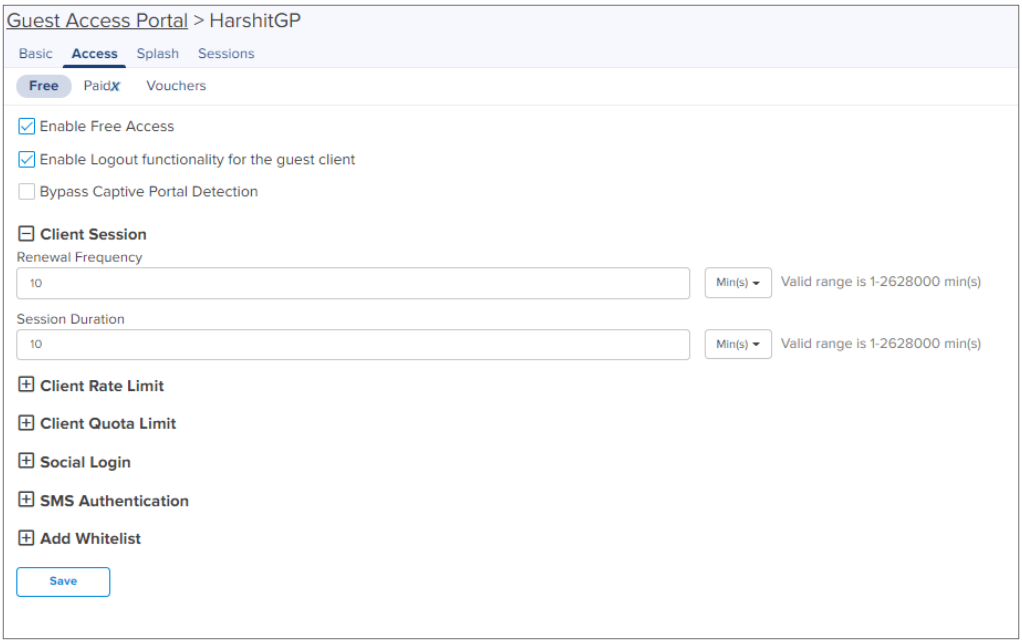
Sample of client login page is displayed below:



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**.



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 nZYIoU7QoUxfD03ct1CC2YvInqI7DmUAH6RYz01K1" \
"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 nZYIoU7QoUxfD03ct1CC2YvInqI7DmUAH6RYz01K1 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 To|mobile|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 sents 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 sents 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.

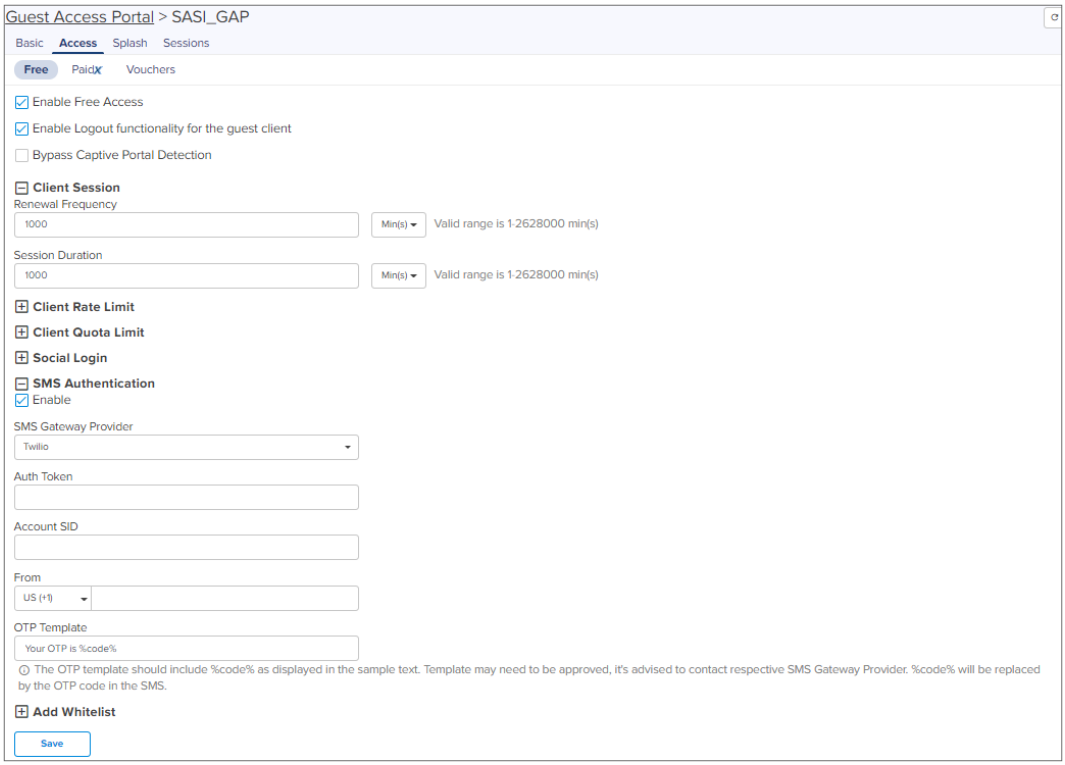
XML reply failure element value

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 460 : *Guest Access Portal*



Maintenance

This section provides the following details:

- Command Line alternatives
- SSH Access
- Data Backup
- Extending the Data Disk
- Account Recovery
- Application Account Recovery
- Configure Network Time Protocol (NTP)

Command Line alternatives

Cambium Networks highly recommends using the cnMaestro UI for all application operations; however, in case the cnMaestro system is not executing correctly, a number of command-line alternatives exist. You can access these by logging into the cnMaestro CLI (through the VM Console) and selecting the “Shell” option to launch a Unix shell.

Enabling TLS 1.0/TLS 1.1

From On-Premises 3.2.0 onwards, TLS 1.0 and TLS 1.1 are not supported. Cambium Networks does not recommend enabling the lower version of TLS. Devices that work only with TLS 1.0 fails to connect On-Premises version 3.2.0 and above. It may be re-enabled through the command line for devices that cannot support TLSv1.2. This degrades the security of the device and care must be taken to avoid exposure to the open networks in this state.

The following command disconnects and reconnects the managed devices from the On-Premises instance:

```
sudo /srv/bin/cnmaestro-degrade-tls
sudo service nginx restart
```

Note

If you are running an HA system, then execute this command on both the instances.

Export cnMaestro Data

Navigate to **Manage** > **Server** > **Operations** > **System Backup** to the UI version of this command. From the command line the data can be exported using the following:

```
sudo cnmaestro-export
```

The location of the exported data file is printed when the command completes. It can then be copied to an external directory using SCP or FTP. From there it can be imported into a different cnMaestro instance.

Import cnMaestro Data

Navigate to **Manage** > **Server** > **Operations** > **System Backup** to the UI version of this command. From the command line the data can be imported using the following:

```
sudo cnmaestro-import <data file>
```

The data file needs to be copied to the cnMaestro instance prior to executing this command. This can be done using either SCP or FTP.

Technical Support Dump

The UI version of this command is located at: **Manage** > **Server** > **Diagnostics** > **Technical Support Dump**. From the command line the technical support dump can be exported using the following:

```
sudo cnmaestro-techdump
```

The location of the file will be printed when the command completes. It can then be copied to an external directory using SCP or FTP and then sent to Cambium Networks support personnel.

Apply OVA Upgrade

This section describes a failsafe mechanism to apply an OVA Upgrade using the Command Line. First make the image accessible to the operating system either by downloading it through SCP (and storing in /srv/storage/tmp/) or mounting a shared folder. Then execute the following commands:

- Extract and stage the image into the unused partition

```
sudo /srv/bin/cnmaestro-image stage <OVA Filename>
```

- View status of the extraction (wait until it completes 100% — about 10 minutes)

```
watch -n2 sudo /srv/bin/cnmaestro-image status
```

- Boot into the new image. Use the inactive partition from the status command

```
sudo /srv/bin/cnmaestro-image upgrade <os2 or os1>
```

> **Note**
>
> Command line upgrade is only a failsafe if the UI upgrade is unavailable. It should not be used for downgrades, which are unsupported.

Apply Package Upgrade

Manage > **Server** > **Operations** > **Apply cnMaestro Package** is the UI version of this command. From the command line, package upgrade can be applied using the following:

`sudo /srv/bin/cnmaestro-image patch <package-file>`

The upgrade file needs to be copied to the cnMaestro instance prior to executing this command. This can be done using either SCP or FTP. The update file itself is downloaded from Cambium Networks.

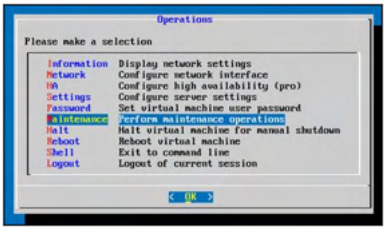
SSH Access

cnMaestro supports SSH access using the cambium user account and password. Enabling this feature is not recommended, due to the password security, but it is available if needed.

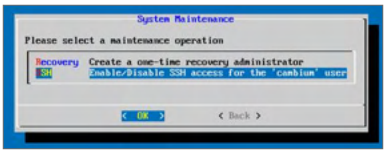
Enabling SSH Access

Follow the below steps to enable SSH access:

1. From the **Operations** page, select **Maintenance**.

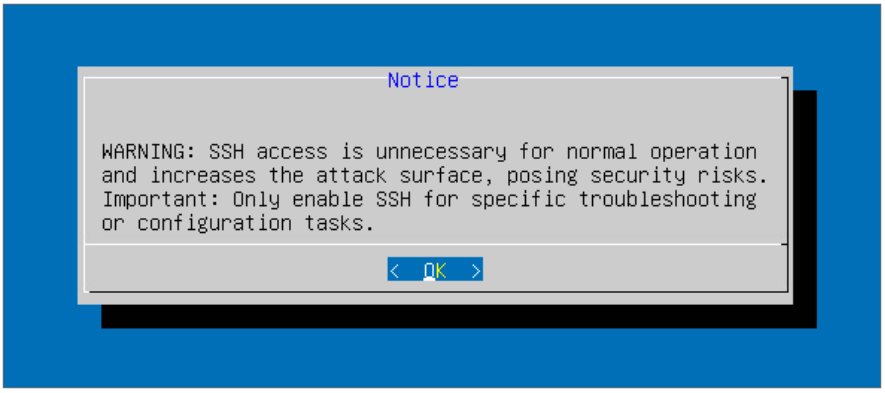


2. Select **SSH** for the SSH Server page.

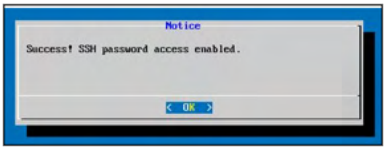


3. Select **Enable SSH** option.

4. Click **OK**.



A screen pops up if SSH is enabled successfully.



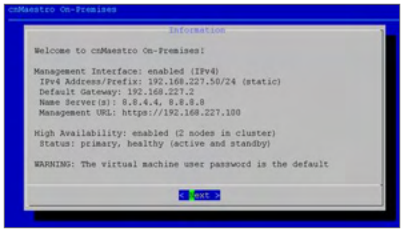
You can then log into the cnMaestro system using the same cambium users used to log in through the Console.

```
# ssh cambium@192.168.127.51
```

Note

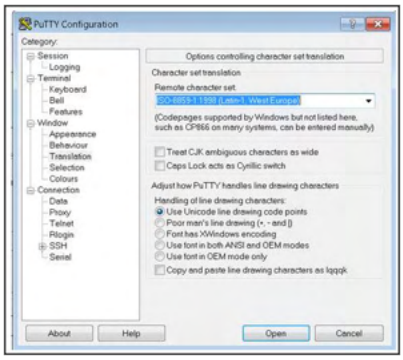
The cambium user has sudo access, so if using SSH, be sure to change the default password of this user before enabling the feature.

The Windows application putty, by default, will not print the dialog correctly, and the customer needs to set the Translation accordingly.

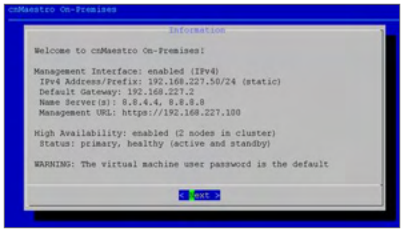


Note

When accessing the CLI from putty on Windows devices, you may need to change the Remote Character Set (**Window** > **Translation** in the putty **Configuration** dialog) to “ISO-8859-1 1998 (Latin-1, West Europe)” to correctly display the menu.



After setting the configuration properly, the window appears as below:



Data Backup

Overview

> **Note**
>
> cnMaestro backups taken from version 3.0.0 and later will include only the statistics for the last month (in addition to configuration). To backup all statistics in a cnMaestro X account (up to 2 years), you must periodically copy the data disk outside of cnMaestro.

cnMaestro On-Premises stores its configuration and statistics on a virtual **data** disk. This disk could be tens of gigabytes in size. Backing up the disk requires snapshotting and copying it using the virtualization infrastructure.

cnMaestro configuration backups should normally be made using the standard cnMaestro backup mechanism available through the UI. When full historical data is required, a snapshot-based disk backup mechanism should be used.

cnMaestro backups

Standard cnMaestro backups are done through the cnMaestro UI. They are fast: ideal for pre-change checkpointing or upgrades. They can be executed on-demand or on a schedule, and they are quick to restore cnMaestro configuration. Standard backups also restore the last week of device statistics, but they do not save any Wi-Fi Client statistics.

> **Note**
>
> Standard cnMaestro backups are performed using the cnMaestro UI.

Full Backups

Full backups copy all cnMaestro data, including configuration and long-term statistics. They can be taken from a running system, but they can only be restored when the system is shut down, because they require swapping the

data disk.

The method of creating snapshot backups varies per virtualization technology, but the basics are the same: a point in time snapshot of the data disk is created, and the snapshot is used as the source for the backup.

If snapshot backups are taken of a running instance, the backup will be "crash consistent". This means the instance will be restored to a similar state as a power shutdown. While small amounts of uncommitted data may be lost, this is generally safe, because the cnMaestro data is stored transactionally. If you prefer to have a fully consistent backup, power down the instance before taking the snapshot. In the case of an HA cluster, always take data backup of the Primary Server.

Note

- It is recommended to use snapshot backup methods only, as data is constantly being written. Otherwise, backups are likely to be inconsistent or unusable.
- Following is the recommended procedure for restoring HA data:
  1. Power OFF the existing Secondary Server, so that the Primary Server will be in Peer-Down state.
  2. Replicate or attach the disk of the backed-up Primary Server to the newly created server.
  3. After backup replication is done, Power OFF the existing Primary (cnMaestro Active) Server and Power ON the newly created server. The new server will become Primary (cnMaestro Active) in Peer-Down state.
  4. Power ON the Secondary Server. HA replication will occur.

Virtualization System Backup Methods

VMware

Dedicated backup software for either VMware or your datastore device is recommended. A basic disk clone backup without additional backup software can be performed through the following:

- Delete all existing snapshots
- Create a new snapshot of the disk
- Clone the disk using vmkfstools
- Delete the snapshot

Disk clone backup using additional backup software can be performed using this alternatives Veeam Backup & Replication or Vinchin Backup.

Standard snapshot-based backups work with existing VMware-supported backup tools, and are likely to work with your existing backup solution. It is not recommended attempting to backup snapshot or disk files directly from storage.

Note

The backup process will consume resources and may impact performance of all VMs, henceforth plan backup accordingly. Initial full backups are likely to take a long time depending on disk size and type.

Hyper-V

It is recommended to use dedicated backup software for Hyper-V, a basic crash-consistent disk backup can be made using either Hyper-V manager or (Export-VM). There are a number of backup solutions available, if snapshot

backup is supported it will successfully backup cnMaestro data disks. Test your backup solution before starting backup process. If you do not have an existing backup solution for your VMs, disk backup using additional software using the alternatives such as Veeam Backup & Replication or Vinchin Backup.

Citrix Hypervisor (XenServer)

To backup Citrix Hypervisor refer Back up and restore hosts and VMs. There are a number of backup solutions available, if snapshot backup is supported it will successfully backup cnMaestro data disks. Test your backup solution before starting backup process. If you do not have an existing backup solution for your VMs, disk backup using additional software using the alternative such as Vinchin Backup.

Extending the Data Disk

cnMaestro has two virtual disks, one for the operating system, and the second for data. If the data disk becomes overloaded, it can be extended. This is done by increasing the disk size through the virtual machine, and then following the command line instructions in this guide.

The process will have two phases:

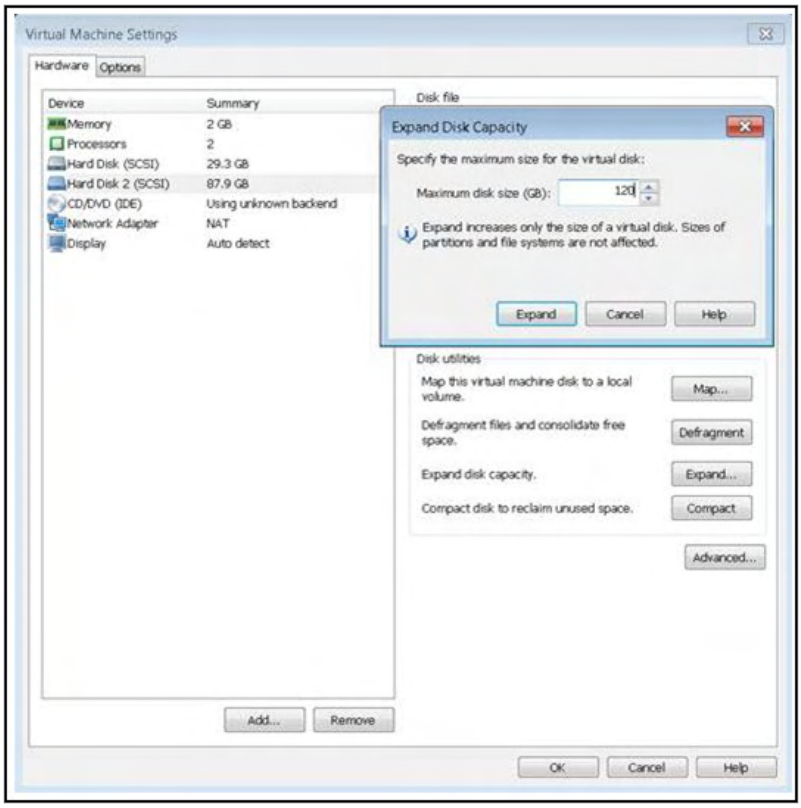
- Phase 1: Expand the virtual disk (using the virtual machine infrastructure).
- Phase 2: Extend the cnMaestro partition and file system (using the command line instructions listed below).

Note

Please take a backup copy of your virtual machine before performing any operations below.

VMware Workstation Disk Expansion

To expand the virtual disk in VMware Workstation, make sure the virtual machine has no VMware snapshots and is currently turned off. You can then select Hard Disk 2 and click **Expand** to select a new disk size. Only expansion is allowed (the data disk can grow but not shrink). An Expand Disk Capacity window launches to update the size. Once a new disk size is chosen, restart cnMaestro. A similar mechanism is used for ESXi.



VirtualBox Disk Expansion

VirtualBox requires command line expansion of the virtual disk. One also needs to convert the disk format from VMDK to VDI before the transformation, and then back again when finished. The commands below are for the Windows installation of VirtualBox. The steps are to convert to VDI; then resize the VDI disk; then convert back to VMDK.

Once the resized.vmdk is created, replace the current Disk 2 in the VirtualBox UI with the resized vmdk and restart the virtual machine.

```
> "C:\Program Files\Oracle\VirtualBox\VBoxManage" clonehd source.vmdk clone.vdi --format vdi
> "C:\Program Files\Oracle\VirtualBox\VBoxManage" modifyhd clone.vdi --resize 120000
> "C:\Program Files\Oracle\VirtualBox\VBoxManage" clonehd clone.vdi resized.vmdk --format vmdk
```

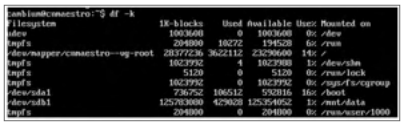
Once the resized.vmdk is created, replace the current Disk 2 in the VirtualBox UI with the resized vmdk and restart the virtual machine.

Partition and File System Updates

cnMaestro will not recognize the additional disk space until the partition is extended. So after the reboot, launch the cnMaestro CLI and select **Shell** to exit to the command line. There type the following commands to grow the partition and file system disk; then convert back to VMDK.

```
$ sudo growpart /dev/sdb 1
$ sudo resize2fs /dev/sdb1
```

You can validate the command completed successfully by typing `df -k` and reviewing the size of `/dev/sdb1 (/mnt/data)`.



Account Recovery

cnMaestro has two types of accounts:

- Virtual Machine (Console) account
- cnMaestro Application account

Both of these can be recovered if the administrator password is lost.

Virtual Machine (Console) Account Recovery

cnMaestro is installed on Ubuntu Server and can leverage the Ubuntu Recovery Mode process to reset the **Cambium Networks** console login password. The steps are the following:

1. When booting up cnMaestro in the VM Console after a full shutdown, quickly press and hold the Shift key after the BIOS has finished loading. This will launch the GNU GRUB menu.

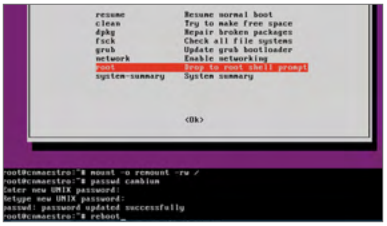
2. Select **Advanced Options** and then **Ubuntu Recovery Mode**.

3. In the **Recovery Menu**, select the **root** option to enter a root shell.

4. The shell will display a command parser along the bottom of the screen. Type the following (without the '#') to reset the password of the **cambium** user.

```
# mount -o remount -rw /
```

```
# password cambium
# reboot
```



5. You should now be able to login to the console using the new password.

cnMaestro Application Account Recovery

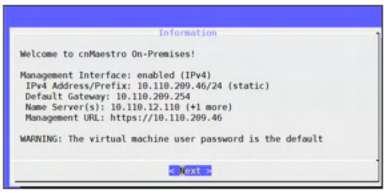
Application Account recovery is useful if you are unable to log in to the cnMaestro UI. It allows you to create a one-time password through the command line, so you can access the UI as a Super Administrator and update current authentication settings.

Application Account Recovery

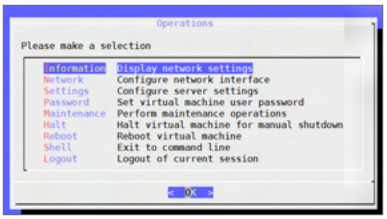
Console administrators can create a one-time password providing Super Administrator access to the cnMaestro UI for a single session (the password will expire in one hour or after a single use). This is a fail safe mechanism that allows cnMaestro access to update current authentication settings.

To create a one-time password:

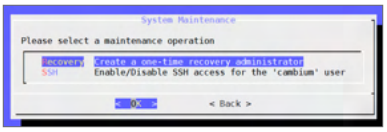
1. Log into the cnMaestro Console and following window pops up:



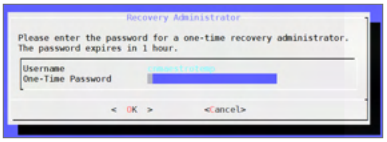
2. Click **Next**.
3. Select **Information** and click **OK**.



4. Select **Recovery** tab and click **OK**.



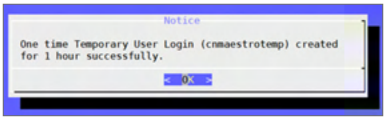
5. Enter the password in the **OneTime Password** text box.



> **Note**
>
> The username for temporary user login is **cnmaestrotemp**. It cannot be changed.

6. Click **OK**.

   The following window is displayed:



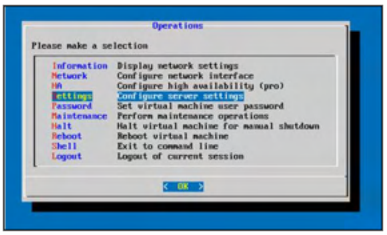
Configure Network Time Protocol (NTP)

cnMaestro uses NTP for time synchronization. This is particularly important for HA environments. By default, NTP is configured to use Google NTP services. NTP can be disabled, if one wants to leverage the NTP feature of VMware, or changed to enable a customized group of NTP servers.

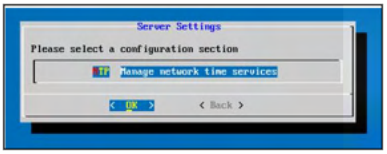
Disabling NTP Support

Follow the below steps to disable NTP Support:

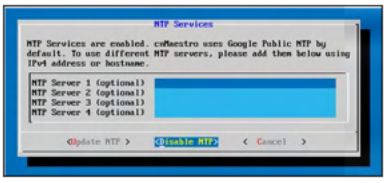
1. From the **Operations** page, select **Settings**.



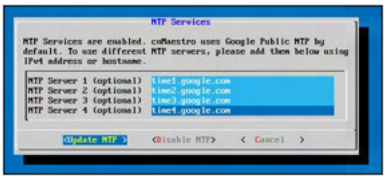
2. Select **NTP** to **Manage Network Time Services.**



3. To disable **NTP**, select the **Disable NTP** Option.



4. Set custom **NTP** servers and **Update NTP**.



Anchor Account and Benefits

This section provides the following details:

- Creating a Cloud Anchor Account
- Benefits of a Cloud Anchor Account
- Data Security and Privacy
- Information that is synced with the Cloud Anchor account
  - On-Premises instance information
  - Registration information
  - Onboarded device information
- Upgrade of On-Premises from 3.1.x to 3.2.0

cnMaestro was launched as both a cloud-based service and as a service hosted on a virtual machine in a customer's data center. The two versions provided essentially the same features. Starting with Cloud version 3.0.0, cnMaestro X was introduced to provide advanced features for Fixed Wireless Broadband and Enterprise customers.

cnMaestro 3.0.0 introduced the cloud-based Anchor Account, and with the release of 3.2.0, all On-Premises instances were required to be connected to a Cloud Anchor account. This appendix describes the benefits of the Cloud Anchor account and discusses its important security features.

With a Cloud Anchor account, network management functionality continues to be performed through the On-Premises instance, while device inventory-related functions are managed through the Cloud Anchor account. A single Cloud Anchor account can support multiple independent On-Premises instances.

Note

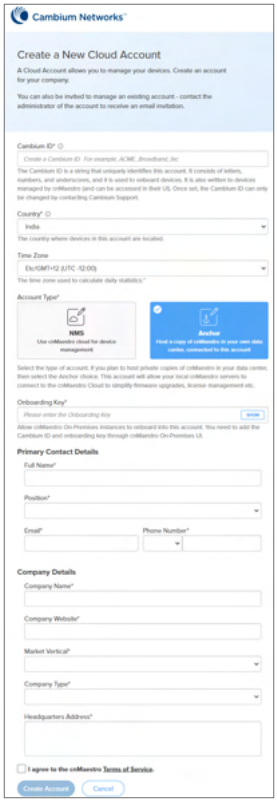
The Cloud Anchor account does not communicate with devices directly nor are devices exposed to the Internet.

Creating a Cloud Anchor Account

Cloud Anchor accounts are created on https://cloud.cambiumnetworks.com, When creating a Cloud account there are two options:

- NMS Account
- Anchor Account

Figure 461 *Account Type*



After an On-Premises instance is onboarded to an Cloud Anchor account, the following information is reported by the On-Premises instance to its Cloud Anchor account:

- System-level details of each On-Premises instance, such as disk, processor, RAM, uptime, and VM vendor (e.g., VMware).
- Total managed devices, device type distribution and count including ESN/MSN and model, On-Premises software version (OVA and package), login user role distribution and count, Account View (Backhaul, Enterprise, and Industrial Internet), and Country.
- Enabled On-Premises features such as Auto Provisioning, CBRS, and MSP.

Always-on connection is recommended; however, regular synchronization is acceptable. Synchronization is required every time devices are removed or onboarded.

The connection to the Cloud Anchor account is outbound and cnMaestro On-Premises instances are never exposed to the internet.

Benefits of a Cloud Anchor Account

A Cloud Anchor account provides one-click upgrade of device firmware and cnMaestro software as well as a single place to view device inventory, subscriptions, and billing across Cloud and multiple On-Premises instances.

Following is a detailed list of benefits:

- The Cloud Anchor account will automatically push announcements of new device firmware and cnMaestro software images to connected On-Premises instances. This makes software upgrades easier and faster.
- Prevent lost or stolen devices from being claimed in other Cloud accounts and other On-Premises instances connected to the Cloud.
- Single place to view device inventory, subscriptions and billing.
- Faster resolution of RMA issues.
- Receive proactive notifications on vulnerability disclosures and security patches (including automated updates).
- Better customer service, feature velocity, and improved quality due to more efficient operations and improved decision-making.

Data Security and Privacy

To ensure data security and privacy the following actions have been implemented:

- All PII and sensitive data is stored securely on the local cnMaestro On-Premises instance.
- Network, Client, and Subscriber configuration data is never sent to the Cloud Anchor account.
- Only device inventory and feature usage reports are sent to the Cloud Anchor account.
- Connection to the Cloud Anchor account is outbound and cnMaestro On-Premises server is never exposed to the internet. An outbound HTTP proxy can also be enabled.
- Data in cnMaestro Cloud is stored using industry-standard best practices.
- A Cloud Anchor account can securely configure devices to trust the cnMaestro On-Premises instance.
- Stolen devices cannot be claimed in other cnMaestro Cloud accounts.

Information that is synced with the Cloud Anchor account

The On-Premises instance synchronizes certain information with the Cloud Anchor account, such as device inventory, VM hardware and software versions, and feature usage statistics.

Note

The On-Premises instance never shares the following information with the Cloud Anchor account:

- Network configuration
- Client data
- Subscriber configuration

The following sections provide details about information that the On-Premises instance syncs with the Cloud Anchor account:

- On-Premises instance information
- Registration information
- Onboarded device information

On-Premises instance information

The following table lists the information about the On-Premises instance that is synced with the Cloud Anchor account.

Field	Description
System / VM hardware-related information	
`uptime`	Duration for which the VM has been running.
`mem_size + mem_size_unit`	Total memory allocated to the VM.
`disks[]`	Disk information (info, size, unit) of each of the disks.
`proc_info`	Processor-related information of the VM CPU (For example, 4 Core(s), Intel).
`prod_family`	Product family that the VM hardware belongs to.
`target`	Deployment type of the VM—AMI / OVA.
cnMaestro application-related information	
`image.activeOvaVersion`	Active OVA version.
`image.activePatchVersion`	Active package version.
`image.inactiveOvaVersion`	Inactive OVA version.
`image.inactivePatchVersion`	Inactive package version.
cnMaestro Account-related information	
`account.view`	Account view mode (Backhaul / Enterprise)
`account.zeroTouchOnboarding`	Indicates whether zero-touch device onboarding is enabled.
`account.pTokenOnboarding`	Indicates whether device onboarding using parent device token is enabled.
`account.isMSP`	Indicates whether the MSP feature is enabled or not.
`account.country`	The country associated with the account.
`account.userCount`	Total number of users.
`account.userCountDist`	Total number of users, grouped by role type.
Managed device inventory summary	
`mgd_devices_summary[eType].count`	Total number of managed devices, grouped by device type.
`mgd_devices_summary [eType].versions[]`	Total number of managed devices, grouped by their active software version.

Registration information

The following table lists the information that is synced after the On-Premises instance is registered with the Cloud Anchor account.

Field	Description
`serialNo`	Serial number of the On-Premises instance.
`type`	On-Premises instance type.
`configVersion`	Cloud synchronization data version.
`activeSwVersion`	Active software version.

Field	Description
`hostname`	Hostname of the On-Premises instance.
`ipAddress`	IPv4 address of the On-Premises instance.

Onboarded device information

The following table lists the information about the approved devices that the On-Premises instance syncs with the Cloud Anchor account.

Field	Description
`mac`	MAC address of the device.
`sn`	Serial number of the device.
`mode`	Operating mode of the device.
`model`	Model name of the device.
`type`	Type of device.
`onboarding`	Details of device onboarding to cnMaestro On-Premises, such as tier, state, flags, device sub-object.
`mcid`	ID of the Managed Account to which the device is onboarded.
`sys.prodName`	The device's product name.
`cfg.*`	The configured name, location, and country of the device.
`mgmt.*`	Device-related information, such as software, hardware, and device agent versions.

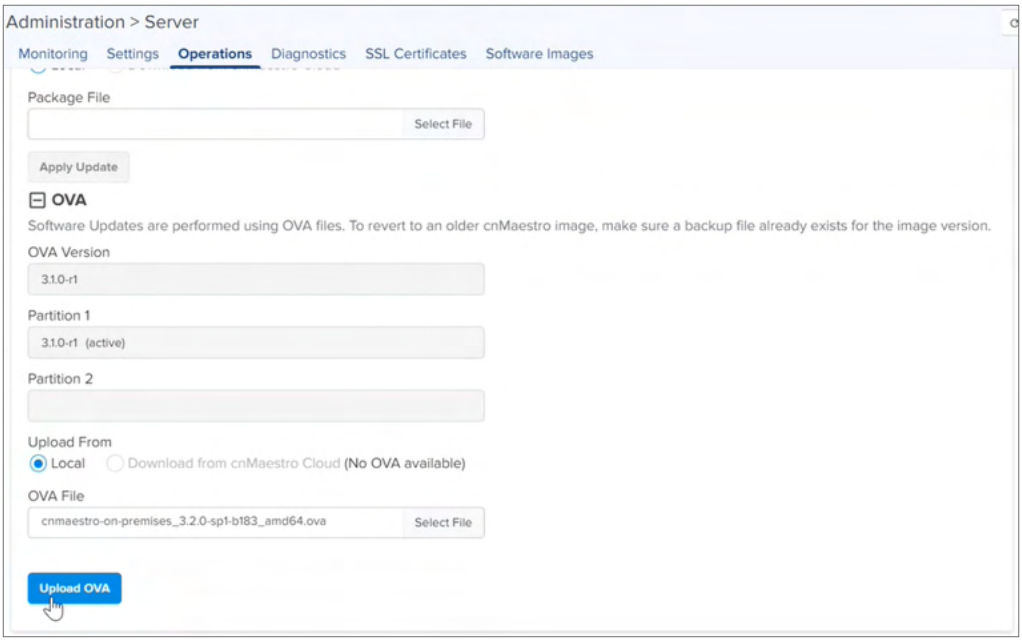
Upgrade of On-Premises from 3.1.x to 3.2.0

To upgrade the On-Premises from 3.1.x to 3.2.0 existing users must ensure the following:

- Connect the On-Premises Instance to a Cloud Anchor account before upgrading.
- On successful upgrade, the Cloud Anchor and On-Premises account will be activated with **cnMaestro X**^{Trial} for 90-days.

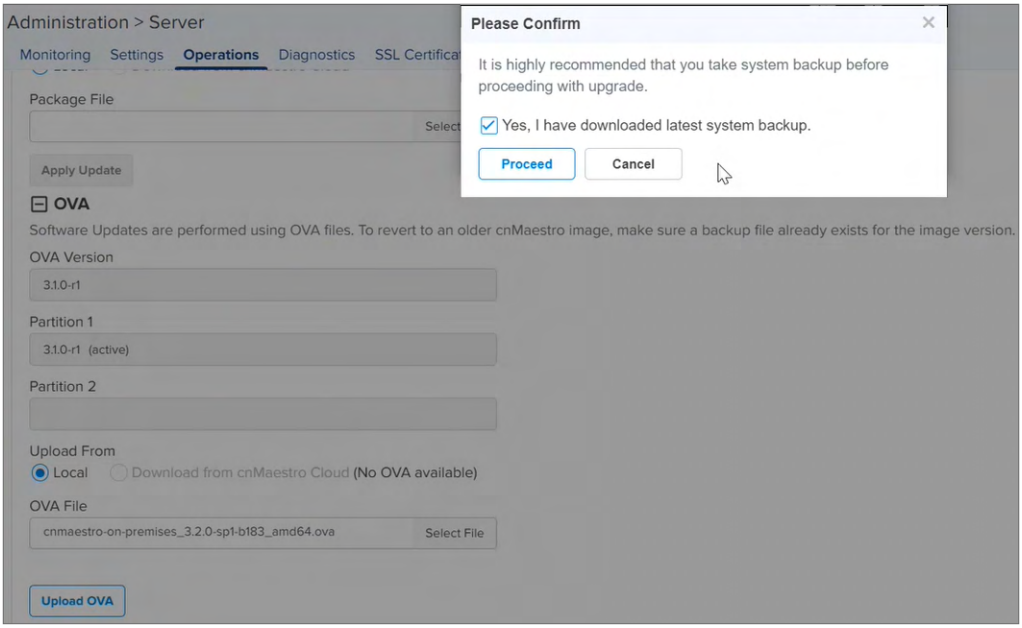
To upgrade to 3.2.0, perform the following steps:

1. Navigate to **Administration** > **Server** > **OVA**.
2. In **Upload From** select **Local**.
3. Select the downloaded **OVA File** of 3.2.0.



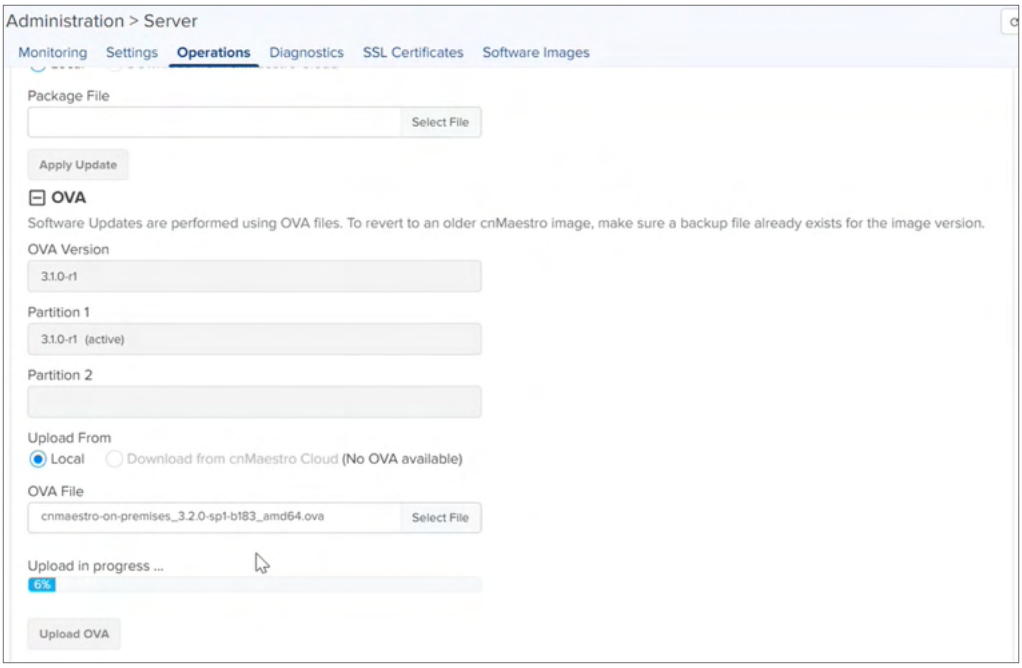
4. Click **Upload OVA.**

   A confirmation window pops up.

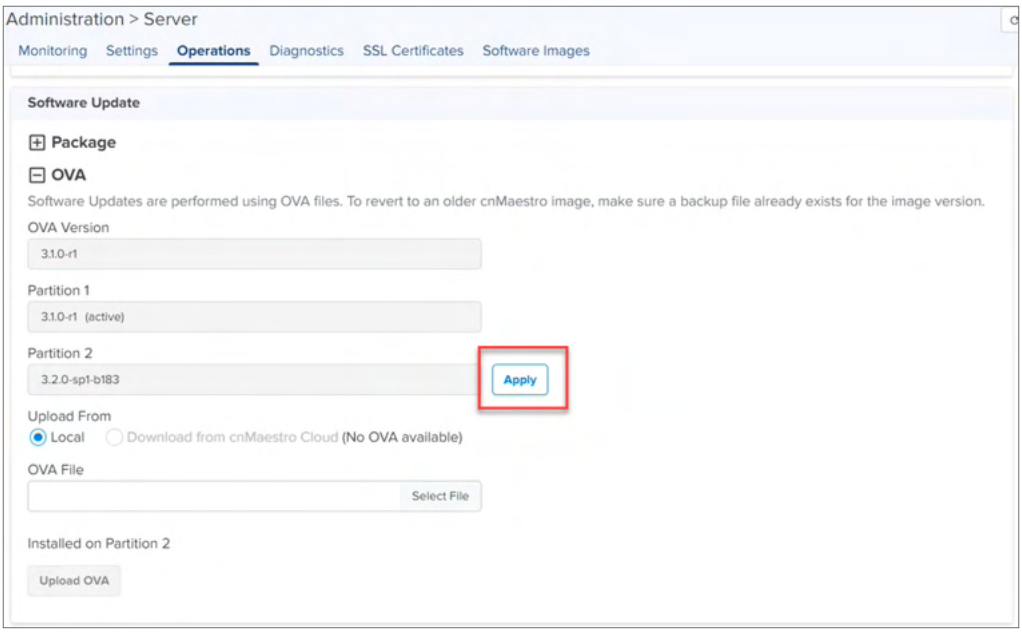


5. Enable **Yes, I have downloaded latest system backup**.
6. Click **Proceed.**

   File upload will be in progress to On-Premises instance.



7. If the upload is successful, the **Apply** button appears.

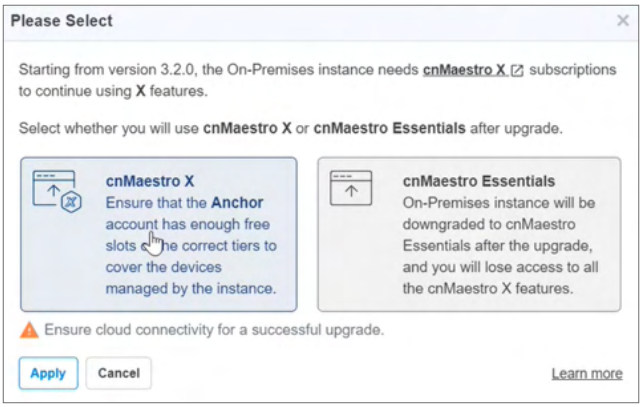


Note

The selected OVA file will be uploaded to On-Premises instances.

8. Click **Apply.**

   Please Select window pops up.

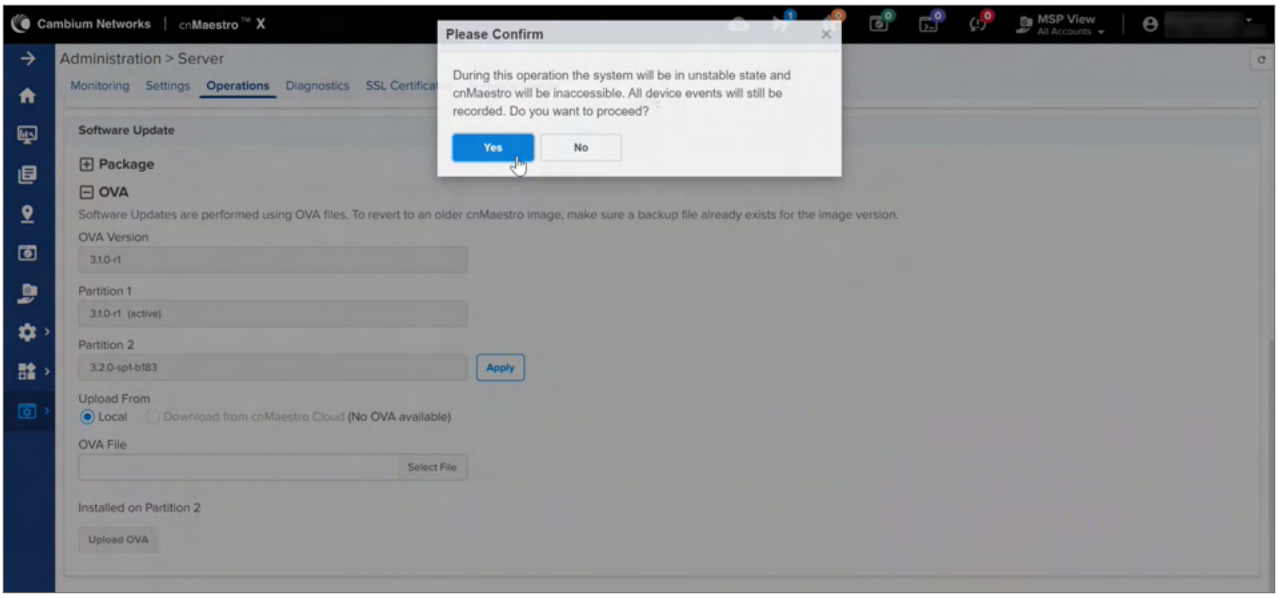


Note

If you select **cnMaestro Essentials**, the account will be in data retention mode.

9. Select **cnMaestro X**.

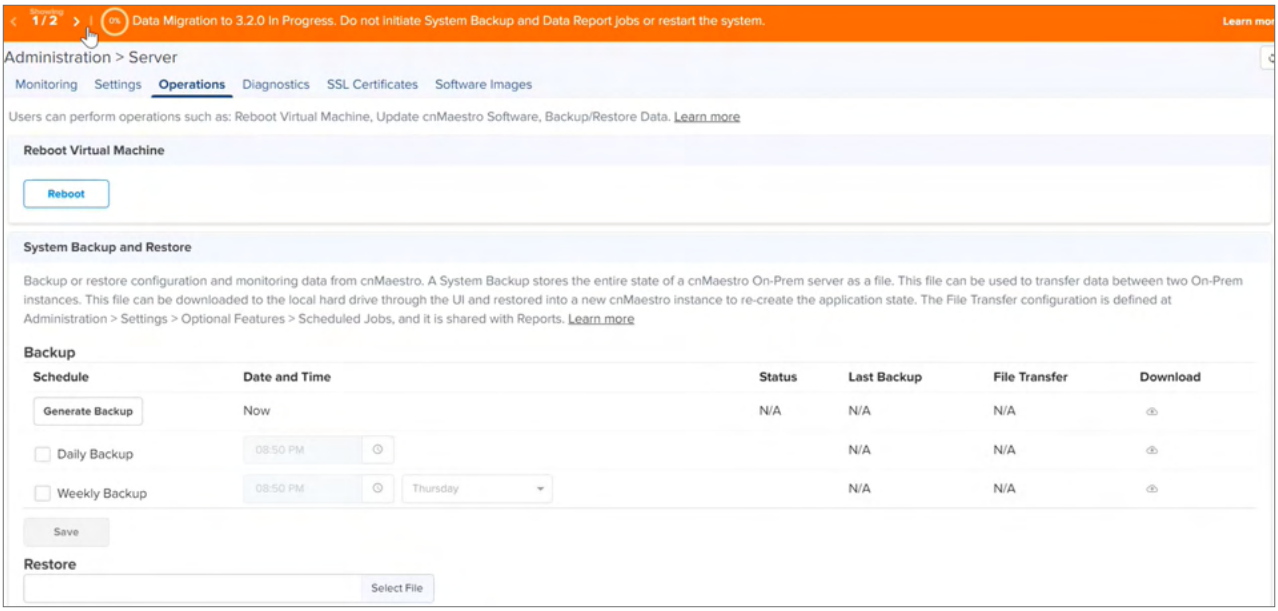
   Please Confirm window pops up.



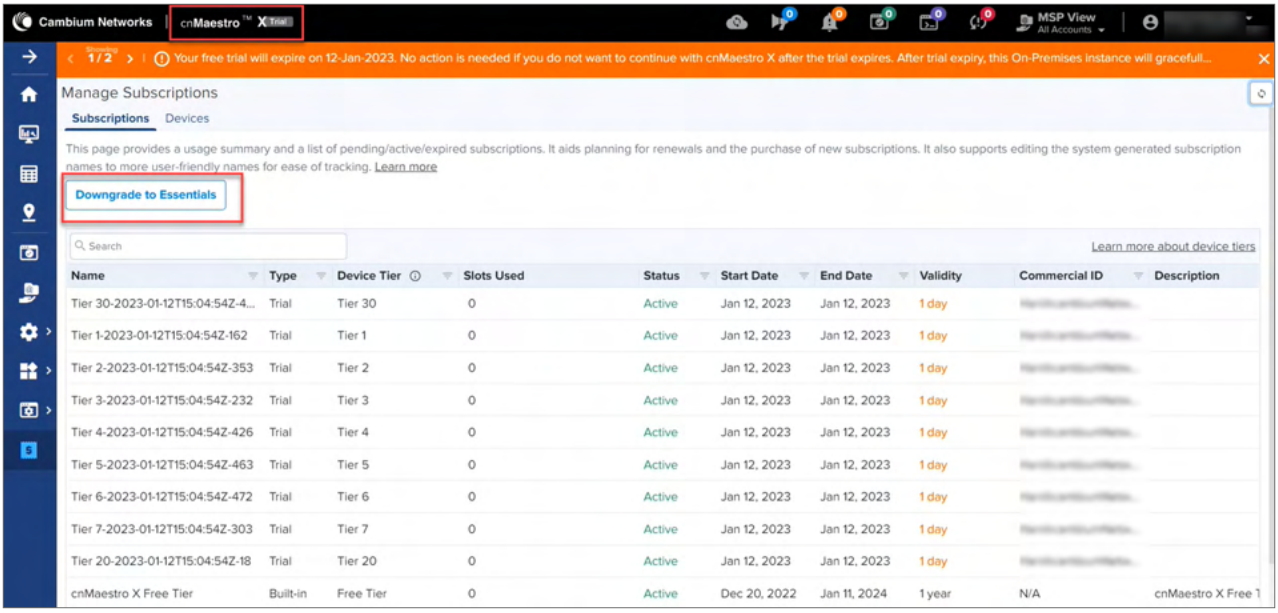
10. Click **Yes**.

    On-Premises instances restart automatically.

11. Data migration displays in the **In Progress** banner as shown below.



On successful upgrade, **cnMaestro X**^{Trail} is displayed in On-Premises instances.



All instances will be listed as onboarding in the anchor account on **Subscriptions** > **Instances** page.

Deployments

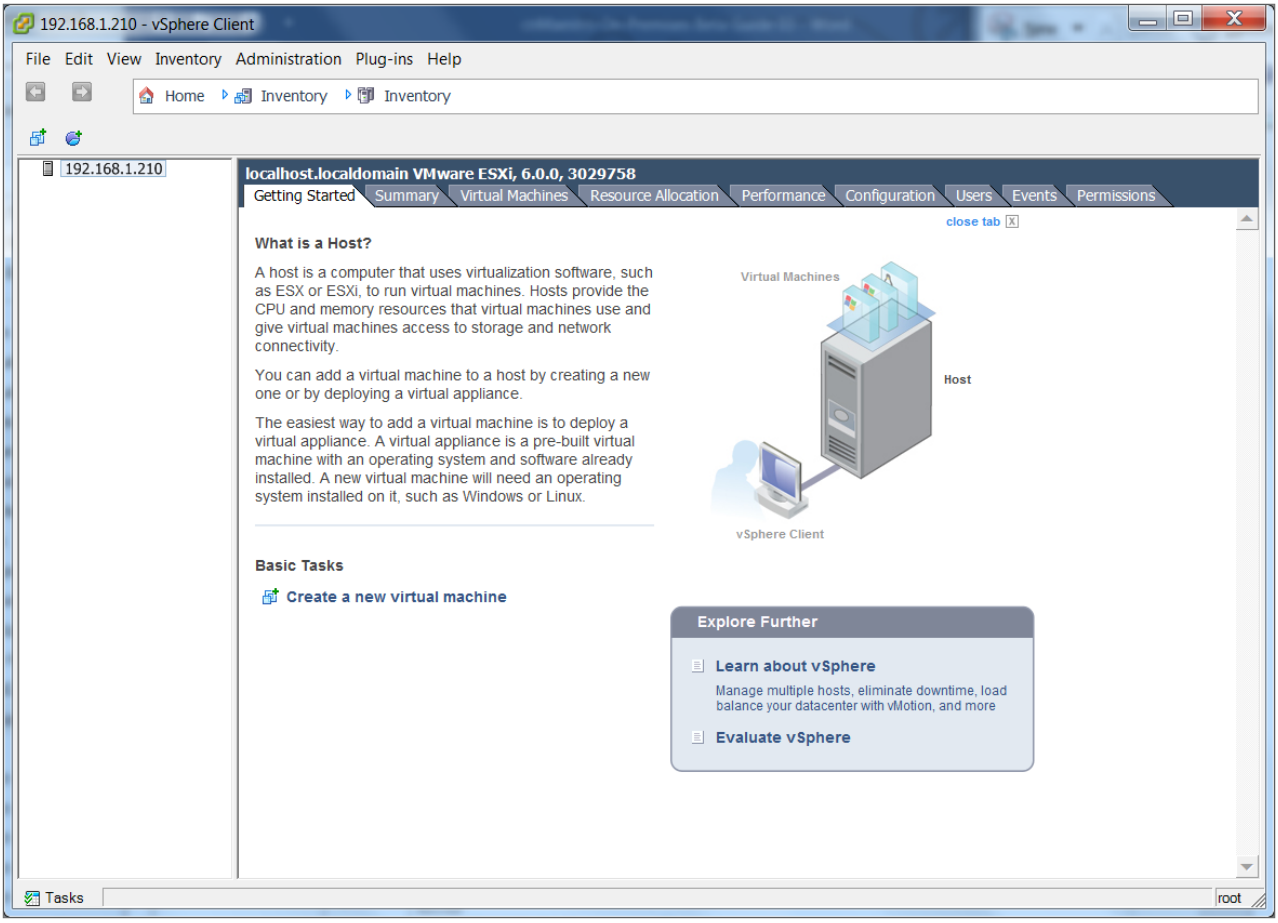
VMware ESXi Installation

Note

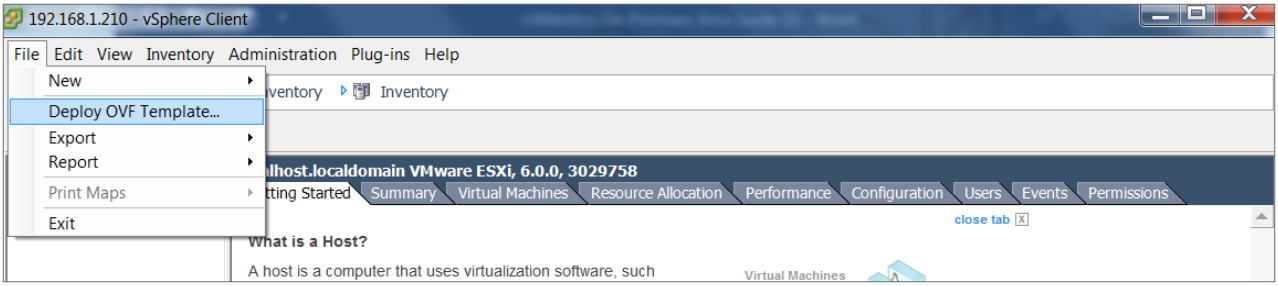
Deploying ESXi is an involved process. The steps below assume you have VMware ESXi version 6.0.0 Update 3 (Build 7967664) or higher already installed on hardware. If you do not have an ESXi hypervisor available, you can download it from the VMware website. VMware provides directions for installing the ESXi ISO on a server.

cnMaestro VM Deployment

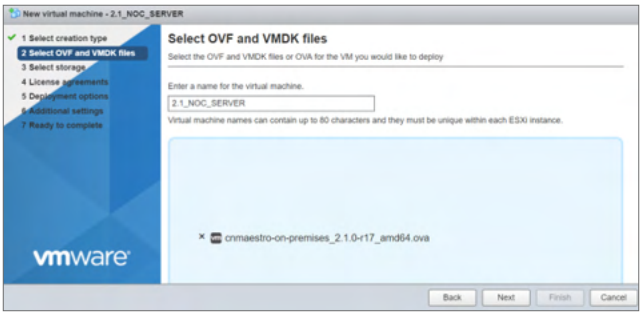
1. Login to ESXi host.
2. Click **Virtual Machines**.



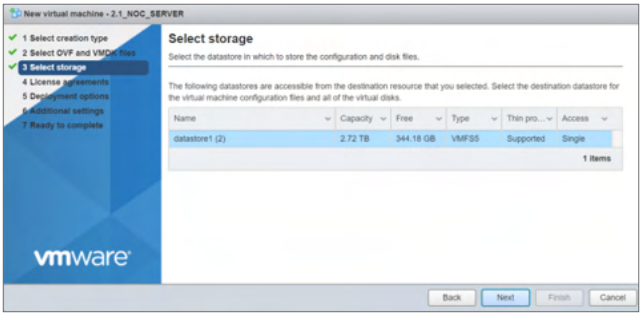
3. Click **Create/Register VM.**



4. Click **Next**.

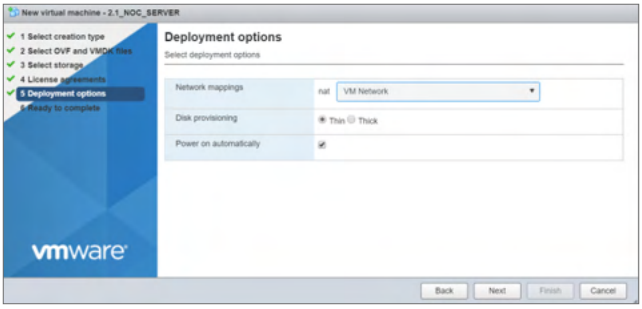


5. Select datastore which has more space.

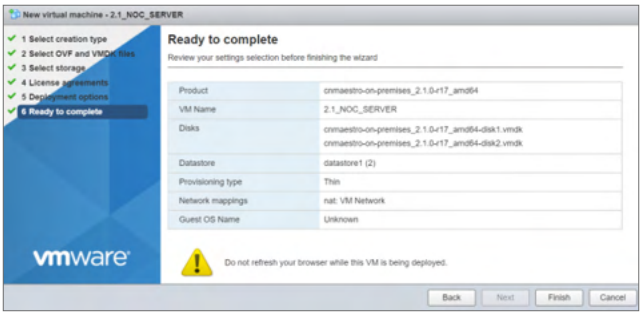


6. Click **Next**.

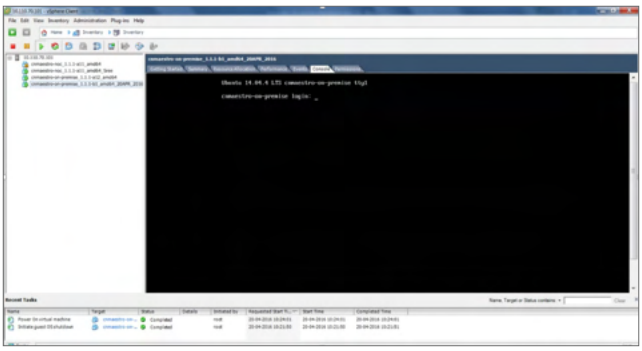
7. Click **I Agree** the license agreements and click **Next**.



8. Select the network and click **Next.**



9. Verify the details and click **Finish** to complete deployment**.**
10. When the loading is complete, a virtual machine with the name chosen will appear. Choose the VM and click **power on** button.



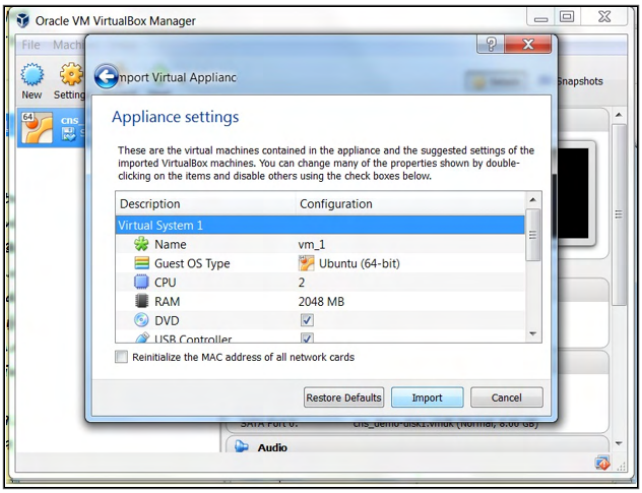
11. Enter the default credentials (cambium/cnmaestro) in the console tab.

Oracle VirtualBox 5 Installation

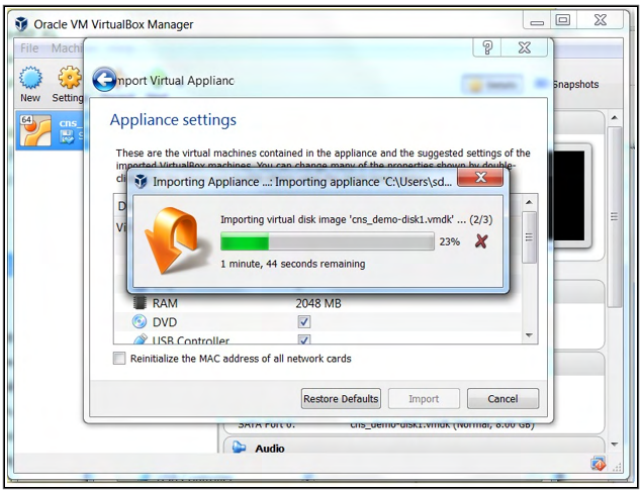
Deployment

The steps to import Cambium cnMaestro On-Premises into Oracle VirtualBox are below. VirtualBox is not recommended for a production environment.

1. Open Oracle VirtualBox Manager, and select **File** > **Import Appliance**.
2. Browse and select Cambium cnMaestro On-Premises release OVA file and click **Next** to continue.
3. Configure the resources required for the VM.

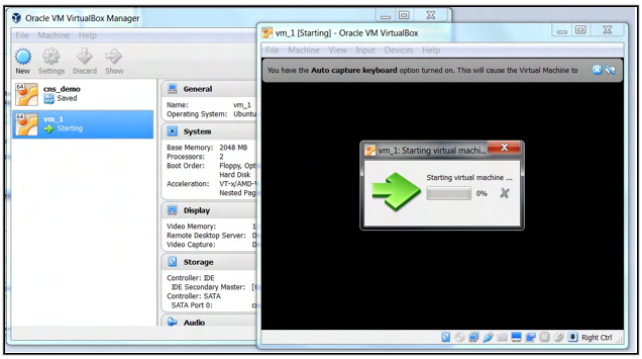


4. Click **Import**.



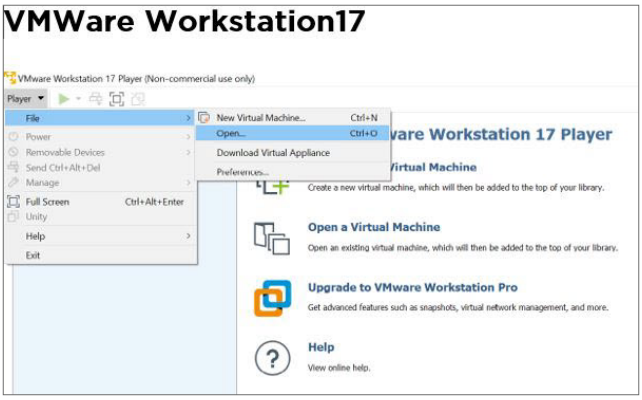
5. The new VM will appear on the left panel. Select the VM and click **start VM** and navigates to the configuration screen.

   The new virtual machine appears in the left panel. After the VM is started, customer gets the login screen, and continue to configure cnMaestro and access the UI.

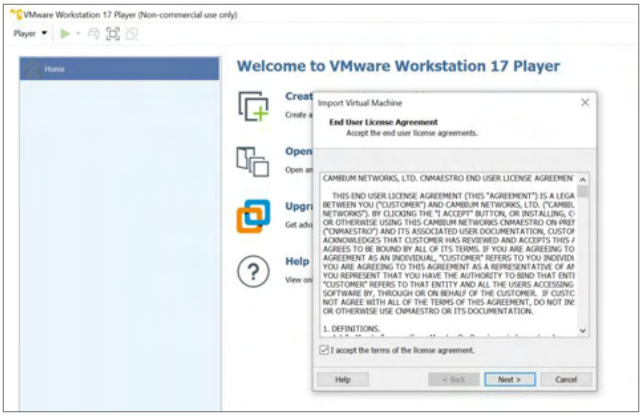


VMWare Workstation

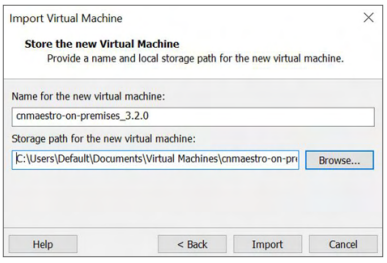
1. Open VMware workstation player. Navigate to **Player** > **File** > **Open Menu** and select Cambium cnMaestro On-Premises release OVA file.



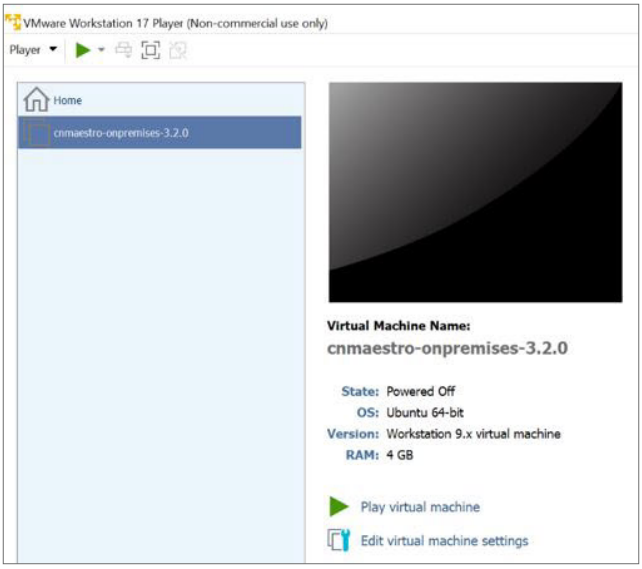
2. Accept the cnMaestro EULA, once the EULA is accepted, cnMaestro will be imported into the VM environment and it could take a couple minutes.



3. Click **Import** to start the deployment.



4. Once the file is loaded, click **Play** and wait for the configuration screen.



KVM Installation

Note

KVM is not officially recommended for cnMaestro deployment. The directions below are for customers who want to evaluate the system in a KVM 0.9.5 or later environment.

Deployment

After installing KVM on the hardware, follow the steps b.....elow to import Cambium cnMaestro On-Premises into KVM:

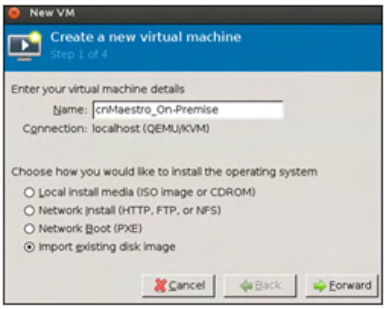
1. Extract cnMaestro On-Premise OVA

```
$ tar xvf cnmaestro-on-premises_1.2.1-b19_amd64.ova
cnmaestro-on-premises_1.2.1-b19_amd64.ovf
cnmaestro-on-premises_1.2.1-b19_amd64.mf
cnmaestro-on-premises_1.2.1-b19_amd64-disk1.vmd
```

2. Convert vmdk image to qcow2

```
$ qemu-img convert -O qcow2 cnmaestro-on-premises_1.2.1-b19_amd64-disk1.vmdk cnmaestro-on-premises_1.2.1-b19_amd64.qcow
```

3. Create New VM
   a. Launch Virtual Machine manager.
   b. Create new VM.
   c. Choose **Import existing disk image**.
   d. Click **Forward.**

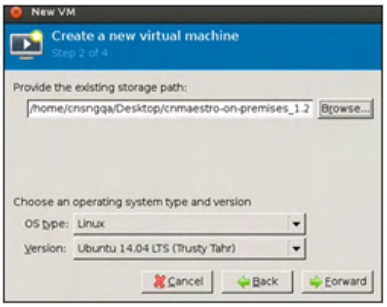


4. Select disk image file

   a. Choose **qcow2** image that is created in earlier steps.

   b. Select OS type as **Linux.**

   c. Click **Forward.**



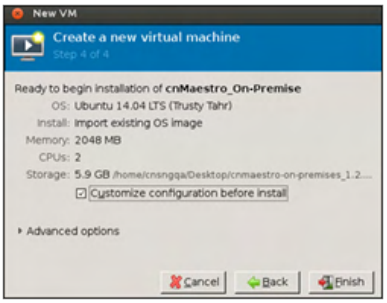
5. Configure Memory and CPU

   Configure Memory and CPU settings as per the requirements.

6. Customize other VM Configuration

   a. Select **Customize Configuration before install** checkbox.

   b. Click **Finish**.



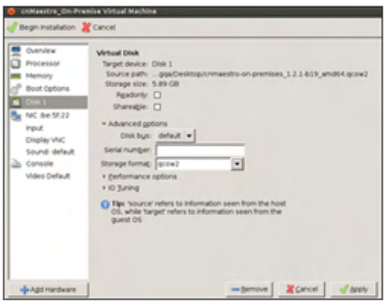
7. Set Disk format to qcow2

a. Select **Disk** from the options on the left side**.**

b. Expand **Advance options** section.

c. Choose Storage format: as “qcow2”.

d. Click **Apply**.

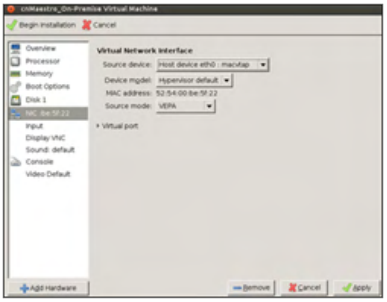


8. Configure Network Adapter

a. Select NIC from the left pane.

b. Select the appropriate source device. Default: NAT.

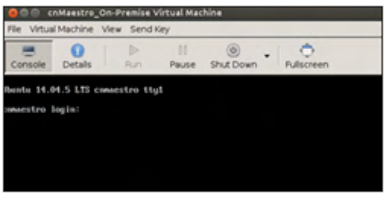
c. Click **Apply**.



9. Begin Installation

a. Click **Begin Installation** on the top left. It would take few minutes to complete.

b. During installation process console may blank for an extended time. Wait for 10-15 minutes. Restart VM if **cnmaestro login** prompt is not shown.



Windows DHCP

This section details how to configure a Microsoft Windows-based DHCP server to send DHCP Options to Cambium Networks devices such as ePMP, ePMP 1000 Hotspot, and cnPilot Enterprises and Home devices.

Following settings must be configured:

- Option 43 and Option 60
- Option 15

- Vendor Class Identifiers (VCI)
- DHCP Policies

DHCP servers are a popular way to configure clients with basic networking information such as an IP address, default gateway, network mask, and DNS server. Most DHCP servers have the ability to also send a variety of optional information, including the Vendor-Specific Option Code Option 43. When a Cambium device requests Option 43 Vendor Specific Information, the DHCP server responds with values configured by the DHCP administrator.

Configuring Option 60

This section describes how to configure the Vendor Class Identifier Code (option 60) on a Microsoft Windows-based DHCP server. As mentioned in the overview section, option 60 identifies and associates a DHCP client with a particular vendor. Since option 60 is not a predefined option on a Windows DHCP server, you must add it to the option list.

Windows DHCP Server Configuration

1. On the DHCP server, open the DHCP server administration tool by clicking **Start** > **Administrative Tools** > **DHCP**.
2. Find your server and right-click on the scope to be configured under the server name. Select **Set Predefined Options**.
3. In the Predefined Options and Values dialog box, click **Add**.
4. In the Option Type dialog box, enter the following information and click **OK** to Save.

Field	Information
Name	CambiumOption60
Code	60
Data Type	String (select the Array checkbox also)
Description	Cambium AP vendor class identifier

5. In the Predefined Options and Values dialog box, make sure **060 CambiumOption60** is selected from the Option Name dropdown list.
6. In the Value field, enter the following information: String: Cambium, Cambium-WiFi-AP, Cambium-cnPilot r200P, Cambium-cnPilot R201P.
7. Click **OK** to save this information.
8. Under the server, select the scope you want to configure and expand it. Select **Scope Options**, then select **Configure Options**.
9. In the Scope Options dialog box, scroll down and select **060 CambiumOption60**. Confirm the value is set as mentioned in point 7 above and click **OK**.

Note

The Data type must be string. If only one device type is to be onboarded to the cnMaestro server, then there is no need to select the Array option. If multiple device types need to be onboarded, then please select the Array option, so the value can contain multiple option 60 entries.

Configuring Option 43

Option 43 returns the cnMaestro URL to the Cambium Devices.

Windows DHCP Server Configuration

1. On the DHCP server, open the server administration tool by clicking **Start** > **Administration Tools** > **DHCP**.
2. Find your server and right-click on the scope to be configured under the server name. Select Set Predefined options.
3. In the Predefined Options and Values dialog box, click **Add**.
4. In the Option Type dialog box, enter the following information:

Field	Information
Code	43
Data Type	String
Description	Cambium AP Option 43
Name	CambiumOption43

5. Click **OK** to save this information.
6. In the Predefined Options and Values dialog box, make sure **043 CambiumOption43** is selected from the option name dropdown list.
7. In the Value field, enter the following information: String: https://<NOC Server Hostname/IP>
8. Click **OK** to save this information.

Note

If Option 43 is already in predefined options with the data type as Binary, then it cannot be changed to string. If this is the case, while defining the policies, specify the values in the ASCII column in the Actions tab of the policy after selecting Option 43. This will be detailed in the Policies section later in the document.

Configuring Option 15

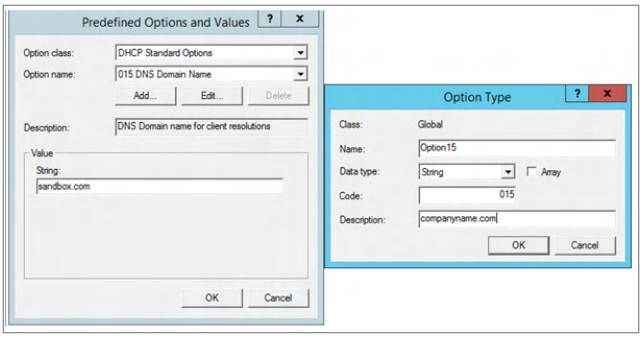
Option 15 returns the domain name to the Cambium Devices.

Windows DHCP Server Configuration

1. On the DHCP server, open the server administration tool by clicking **Start** > **Administration Tools** > **DHCP**.
2. Find your server and right-click on the scope to be configured under the server name. Click on Set Predefined Options.
3. In the Predefined Options and Values dialog box, click **Add**.
4. In the Option Type dialog box, enter the following information:

Field	Information
Code	15
Data Type	String
Description	Cambium AP Option 15
Name	CambiumOption15

5. Click **OK** to save this information.
6. In the Predefined Options and Values dialog box, make sure **015 CambiumOption15** is selected from the Option Name dropdown list.
7. In the Value field, enter the following information: String: <companyname.com>.
8. Click **OK** to save this information.

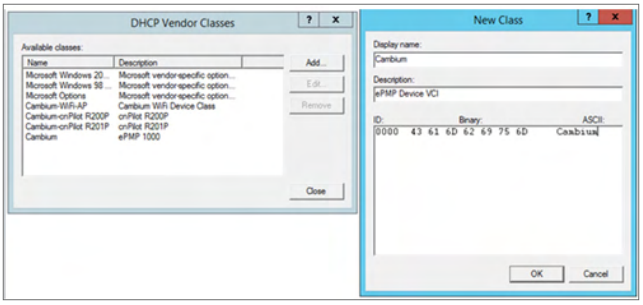


Note

In the DNS Server, the user needs to map the cnMaestro hostname to the IP address of the cnMaestro On-Premises server.

Configuring Vendor Class Identifiers

1. On the DHCP server, open the server administration tool by clicking **Start** > **Administration Tools** > **DHCP**.
2. Find your server and right-click on the scope to be configured under the server name. Click on the **Define Vendor Classes** and click the **Add** button in the dialog box that appears.
3. Provide the Display name, Description and then click in the ASCII column and enter the value as Cambium as shown in the below figure, and then click **OK**.



The above example is for an ePMP device. In order to create the VCI for other device types, please follow the same steps, and in the ASCII column provide the following values:

Product	VCI (DHCP Option 60)
cnMatrix	Cambium-cnMatrix-EX2K
cnPilot r190	Cambium-cnPilot r190
cnPilot r195	Cambium-cnPilot r195
cnPilot r200P	Cambium-cnPilot r200P
cnPilot r201P	Cambium-cnPilot r201P
cnPilot e400/e410/e430W cnPilot e425H/e505 cnPilot e500/e501S/e502S/e510 cnPilot e700/e600 XE3-4, XE3-4TN, XE5-8 XV2-2, XV2-2T0, XV2-2T1, XV2-22H, XV2-21X, XV2-23T, XV3-8	Cambium-WiFi-AP
ePMP	Cambium
ePMP 1000 Hotspot	Cambium-WiFi-AP
PMP 430 SM	Cambium PMP 430 SM
PMP 450 AP	Cambium PMP 450 AP
PTP 450 BHM	Cambium PTP 450 BHM
PMP 450 BHS	Cambium PTP 450 BHS
PMP 450 SM	Cambium PMP 450 SM
PMP 450b SM	Cambium PMP 450b SM
PMP 450i AP	Cambium PMP 450i AP
PMP 450i BHM	Cambium PTP 450i BHM
PTP 450i BHS	Cambium PTP 450i BHS
PMP 450i SM	Cambium PMP 450i SM
PMP 450m APs	Cambium PMP 450m AP

Typically, Option 43 is the preferred mechanism to configure the cnMaestro URL. Example configuration for the ISC DHCP Server is presented below (from the /etc/dhcp/dhcpd.conf file).

```
option option-43 code 43 = string;

# ePMP/PMP Devices
class "Cambium" {
    match if option vendor-class-identifier = "Cambium";
    # DHCP server MUST return the device's Vendor Class back, in the offer.
    option vendor-class-identifier "Cambium";
    # cnMaestro On-Premises IP is 192.168.0.100
    option option-43 "https://192.168.0.100";
}

# WiFi Devices
class "Cambium-WiFi-AP" {
    match if option vendor-class-identifier = "Cambium-WiFi-AP";
    option vendor-class-identifier "Cambium-WiFi-AP";
    option option-43 "https://192.168.0.100";
}

# cnPilot R200P Devices
class "Cambium-cnPilot R200P" {
    match if option vendor-class-identifier = "Cambium-cnPilot R200P";
    option vendor-class-identifier "Cambium-cnPilot R200P";
    option option-43 "https://192.168.0.100";
}

# cnPilot R201P Devices
class "Cambium-cnPilot R201P" {
    match if option vendor-class-identifier = "Cambium-cnPilot R201P";
    option vendor-class-identifier "Cambium-cnPilot R201P";
    option option-43 "https://192.168.0.100";
}
```

Using DHCP Option 15

DHCP Option 15 allows the device to derive the cnMaestro URL from the domain name. For example, if the domain name in DHCP Option 15 is **mycompany.com**, the device will try to access the cnMaestro server at **cnmaestro.mycompany.com** (essentially the string **cnmaestro** is prepended to the domain). The domain itself, and the IP address of cnMaestro, must be configured in the DNS server for this to work correctly.

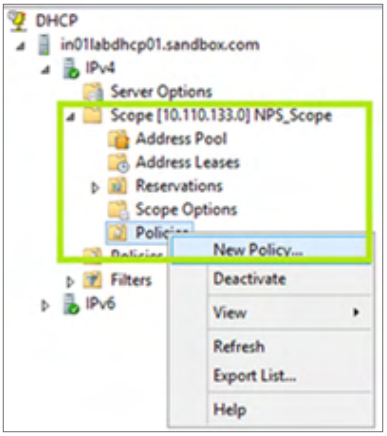
Sample configuration for the ISC DHCP Server is presented below (from the /etc/dhcp/dhcpd.conf file).

```
option domain-name "mycompany.com";
```

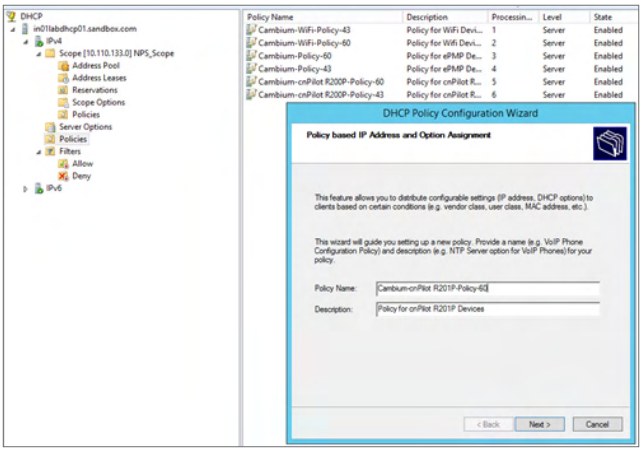
Configuring the Policies at the SCOPE Level

Once Options 43, 60, 15, and Vendor Classes are created, one needs to create policies at scope level. This allows the DHCP server to send the Option 43 and 60 to the Cambium Devices -- based on their VCI for that device. The policy will make sure these options are only sent if the VCI matches that provided by the device.

1. Select the scope in which you want to create the policy, and then right click on the Policies option. Select New Policy.



2. In the pop up, enter the Policy Name and Description and click **Next** button.

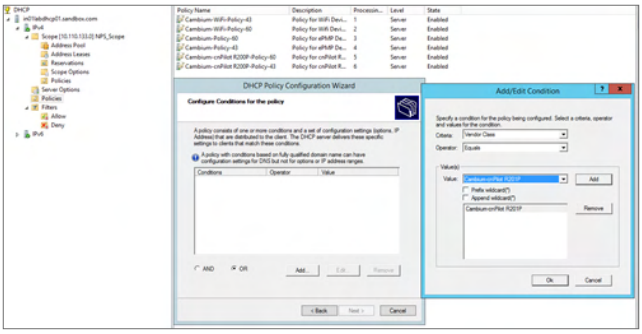


3. The Policy consists of Matching conditions based on Vendor Class, user class, MAC Address, Client Identifiers, FQDN and Relay Agent Information. For Cambium Devices we need Vendor Class based match conditions only.

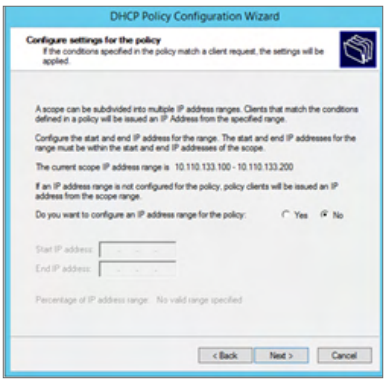
a. In the dialog, click on the **Add** button and in the pops-up select the Criteria as **Vendor Class**, the Operator as **Equals**, and the Value as the VCI created for the Cambium Device type.

b. For example, for cnPilot R201P device the Vendor Class selection is “Cambium-cnPilot R201P”.

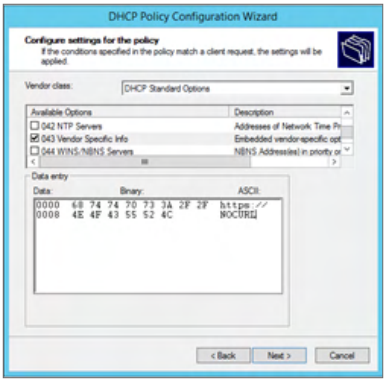
c. Click **Add** and then **OK** in the pop-up. Click **Next** in the Policy Configuration Wizard.



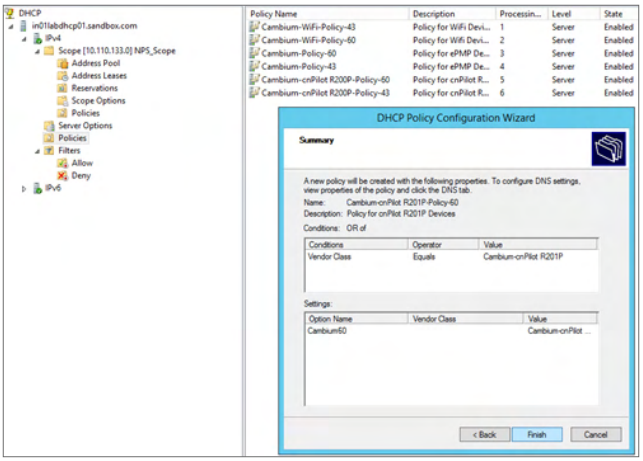
4. In the policy configuration settings wizard, select the option **No** and click **Next**.



Then select the vendor class as DHCP standard options and Select the options 43 and 60 from the available options and specify the values that need to be sent to the device. Click **Next** once the options are selected and values are specified.



5. Click Finish in the final settings page. The policy is displayed in the RHS pane.



The above Policy is a generic one. For all the device types, the policies should be created with the match conditions and action. The policies can be created at the Scope level or Server level. If separate scope is defined for Cambium devices, it is better to define scope level policies; otherwise the policies can be defined at the Server level in the similar way.

Device Type	Match Condition	Actions
cnPilot E-Series	Vendor Class for E400/E410/E425H/E500/E501S/E502S/E505/E600	Cambium option 43 and 60 selected and values specified
cnPilot Home	Vendor Class for cnPilot R190/R195/R200/R201	Cambium option 43 and 60 selected and values specified
ePMP	Vendor Class for ePMP	Cambium option 43 and 60 selected and values specified
ePMP 1000 Hotspot	Vendor Class for Hotspot	Cambium option 43 and 60 selected and values specified
Xirrus Series	Vendor Class for Xirrus	Cambium option 43 and 15 selected and values specified

Citrix Hypervisor Installation

cnMaestro can be installed on Citrix Hypervisor (formerly known as XenServer). The OVA image can be downloaded from the Cambium Support Center https://support.cambiumnetworks.com/.

Resources

The following resources are required for deployment.

Note

- If NBI APIs or Performance Data Reports are extensively used, you must increase the vCPUs and RAM capacity by 50%.
- Solid State Drive (SSD) disks are recommended to improve performance.

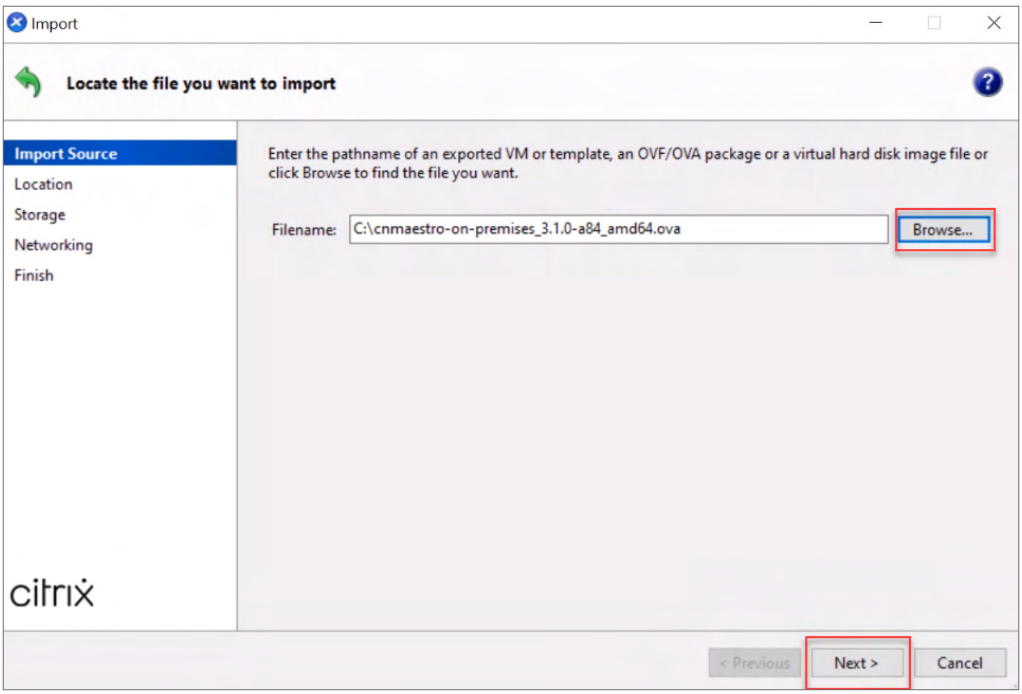
Table 160 *Supported devices*

Number of Devices	Wireless Clients	Number of vCPUs	RAM Size (GB)	Hard Disk (GB)
1 - 100	Up to 1500	2	4	88
101 – 1,000	Up to 15,000	4	4	100
1,001 - 4,000	Up to 60,000	4	8	150
4,001 - 10,000	Up to 150,000	8	16	250
10,001 - 20,000	Up to 300,000	16	32	500
20,001 - 25,000	Up to 375,000	20	40	650

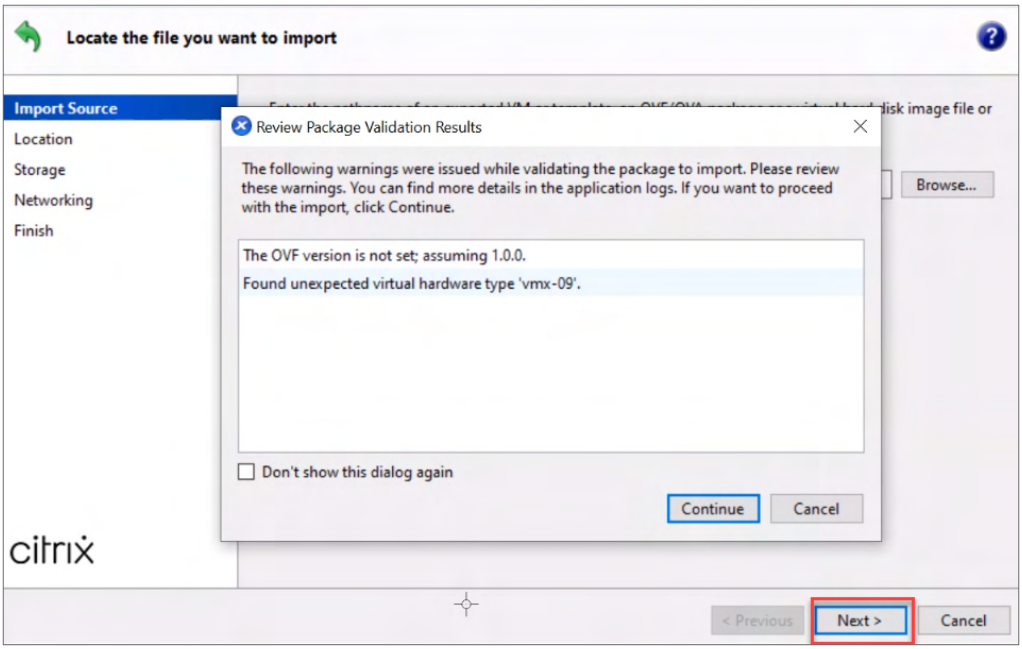
Import using Citrix Hypervisor

Perform the following steps to install the Citrix Hypervisor:

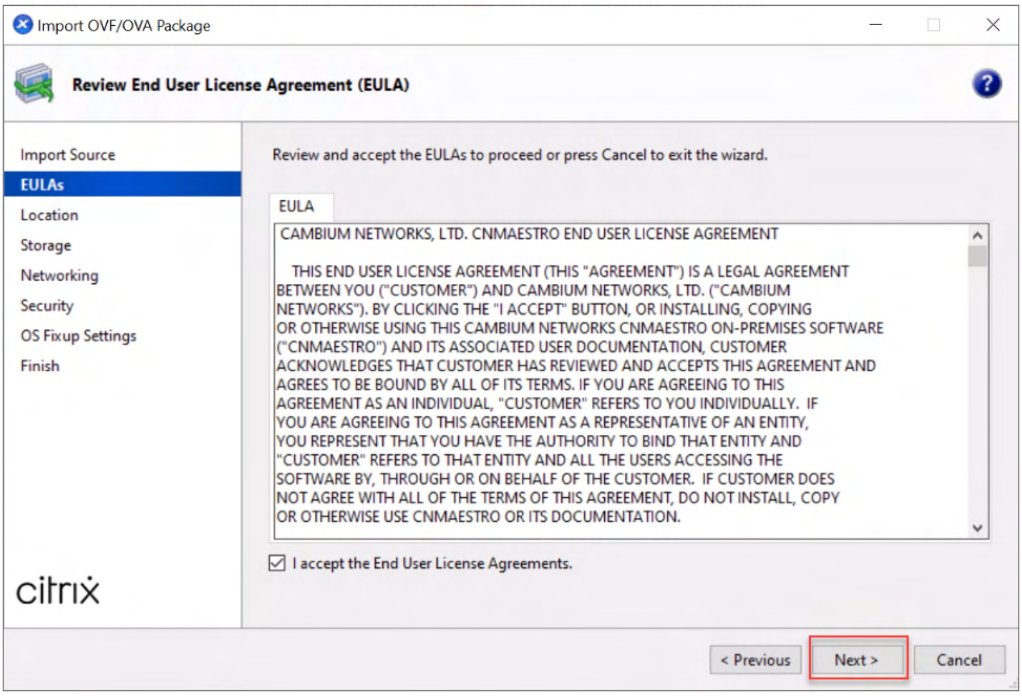
1. Navigate to **XenCenter** and right-click **citrix hypervisor.**
2. Click **Import**.
3. Click **Next** on the import wizard, browse to the downloaded OVA and click **Next.**



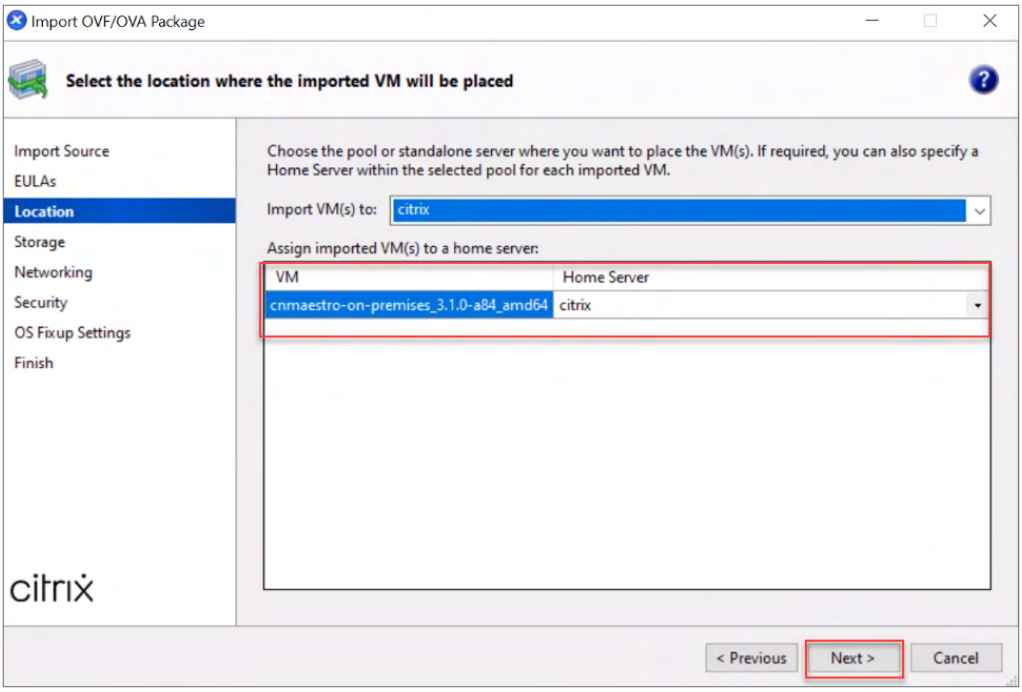
4. Review the Package Validation results and click **Next**.



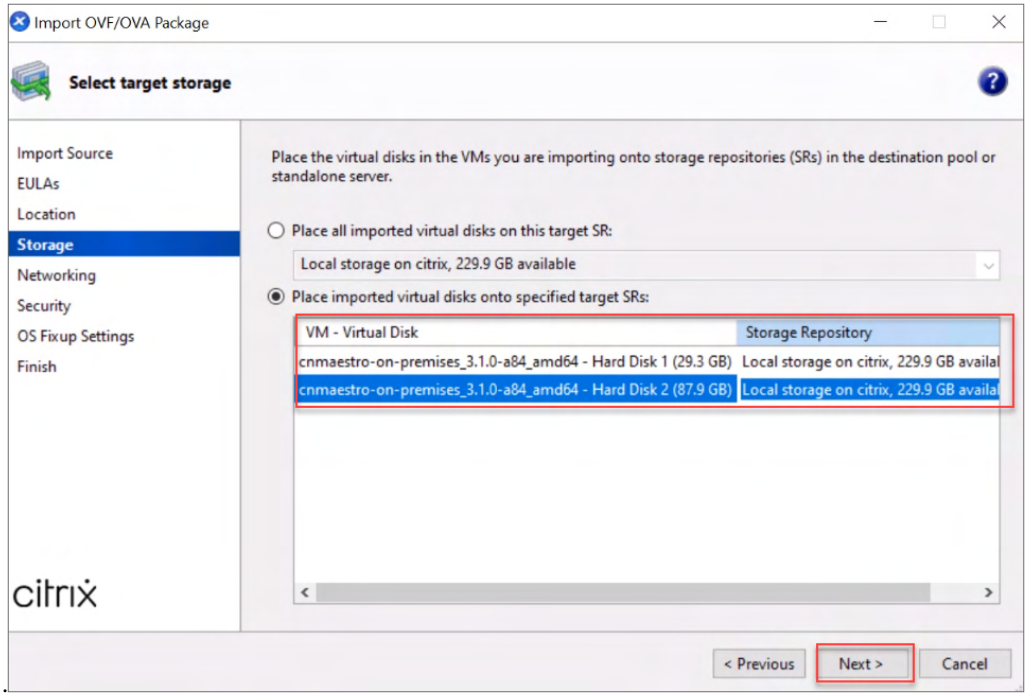
5. Accept the EULA.



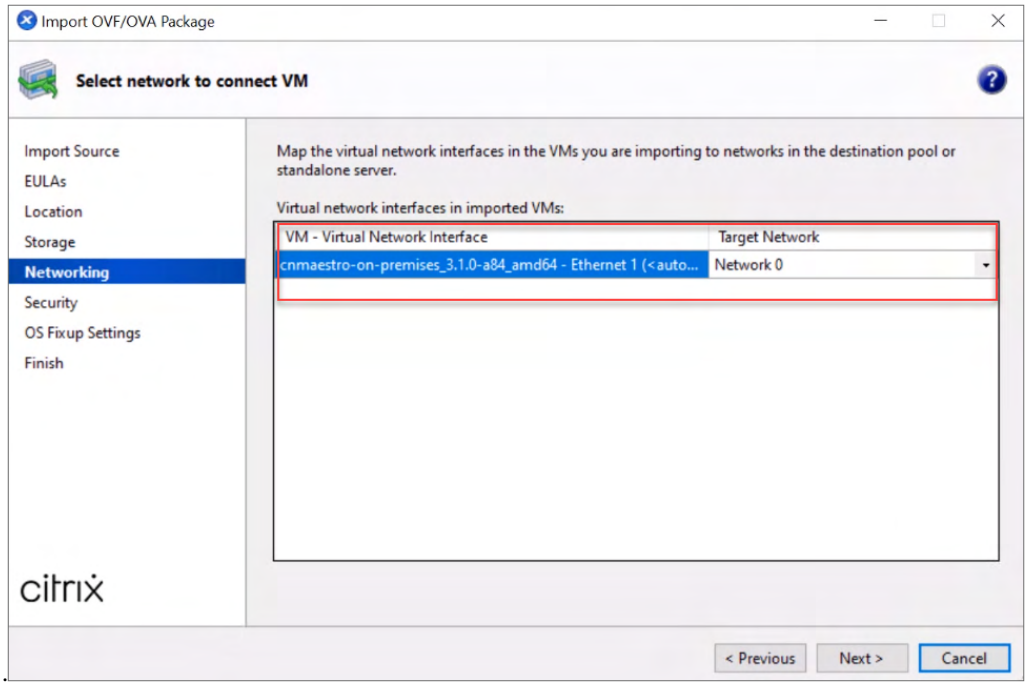
6. Select the location where the imported VM will be placed.



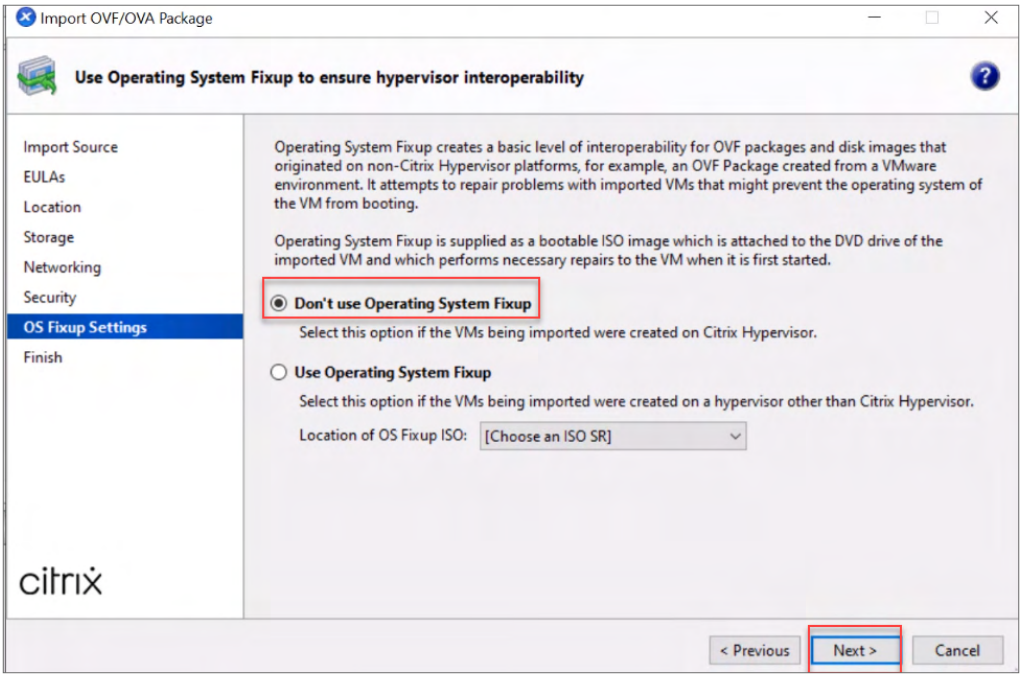
7. Select a storage repository for the second/data disk.



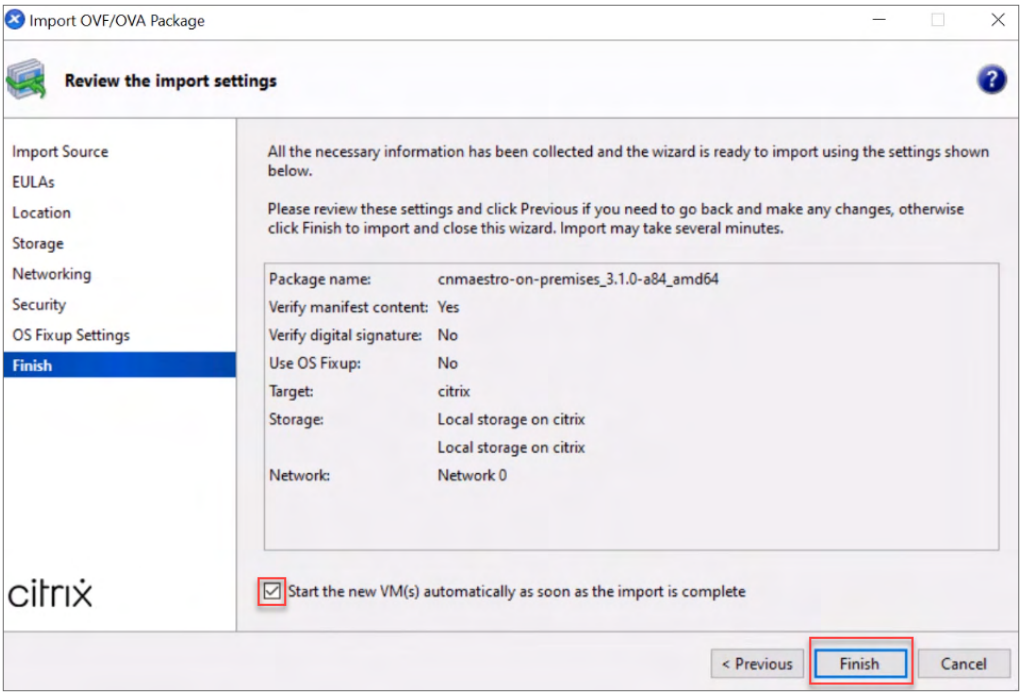
8. Select a network.



9. Verify the included manifest to ensure the OVA is not damaged. Select **Don't use Operating System Fixup**.

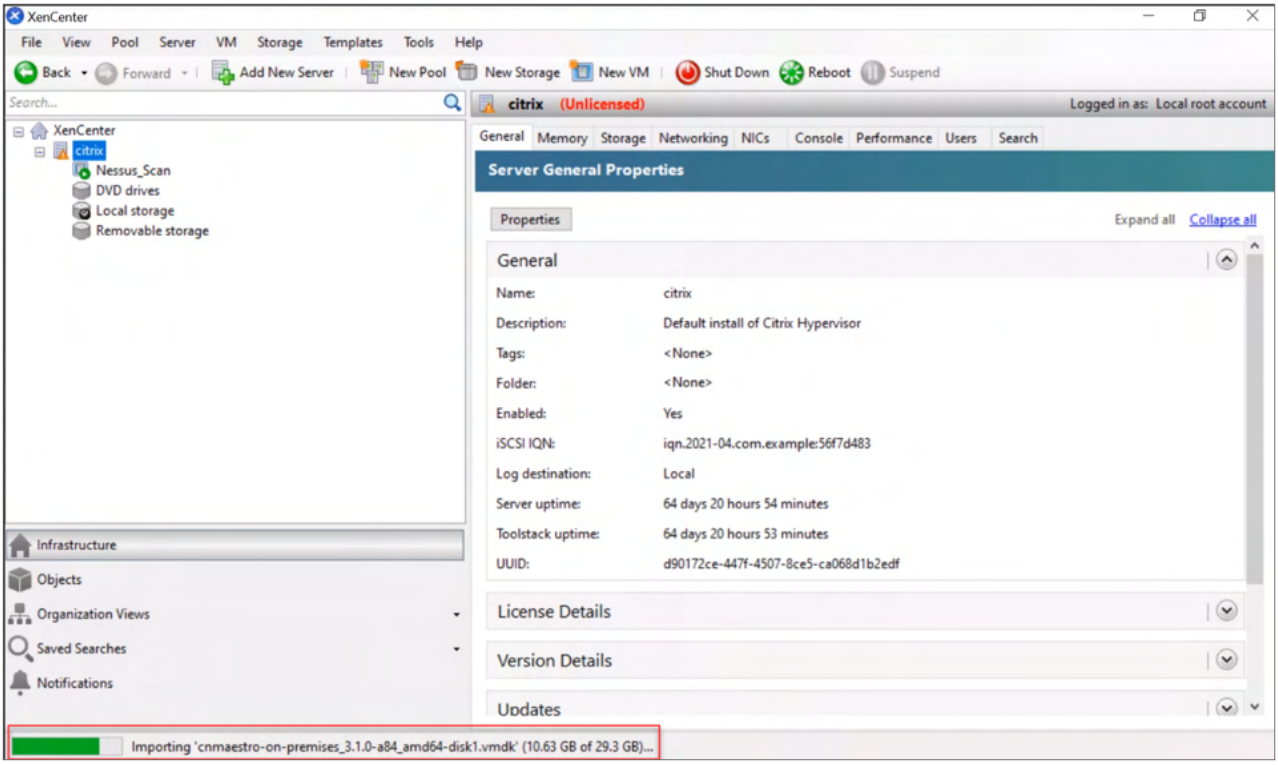


10. Enable the checkbox to start a new VM when the import completes.

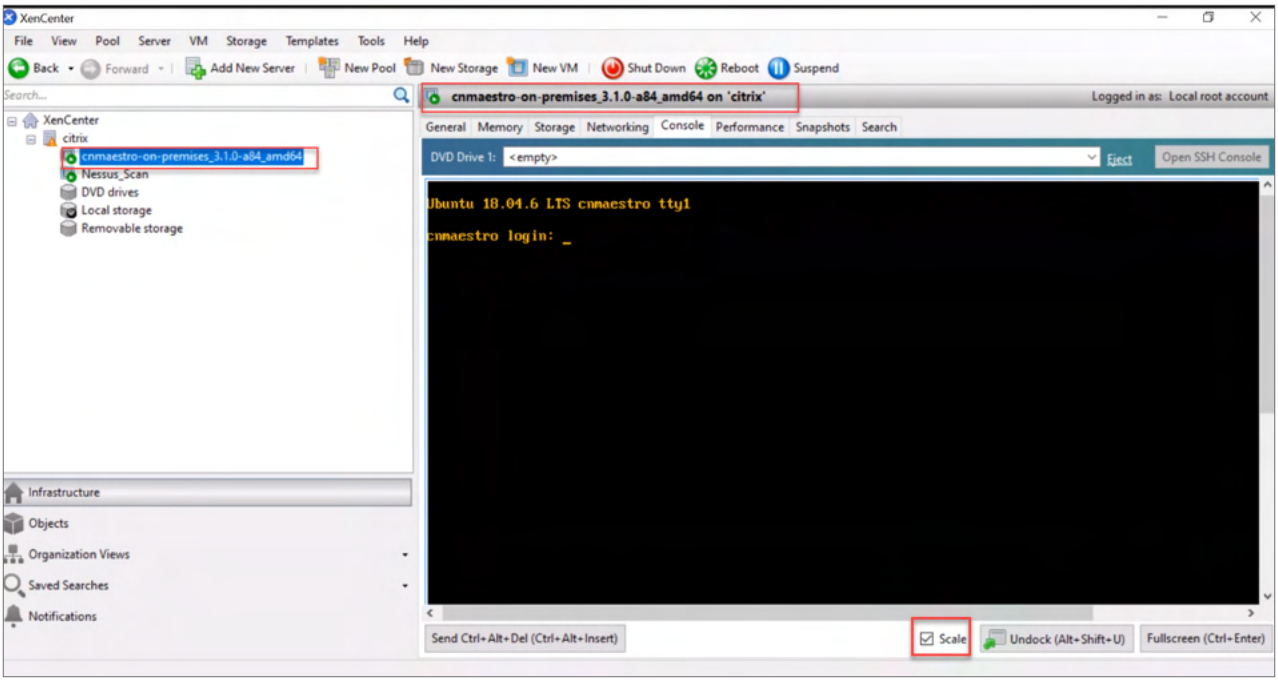


11. Click **Finish**.

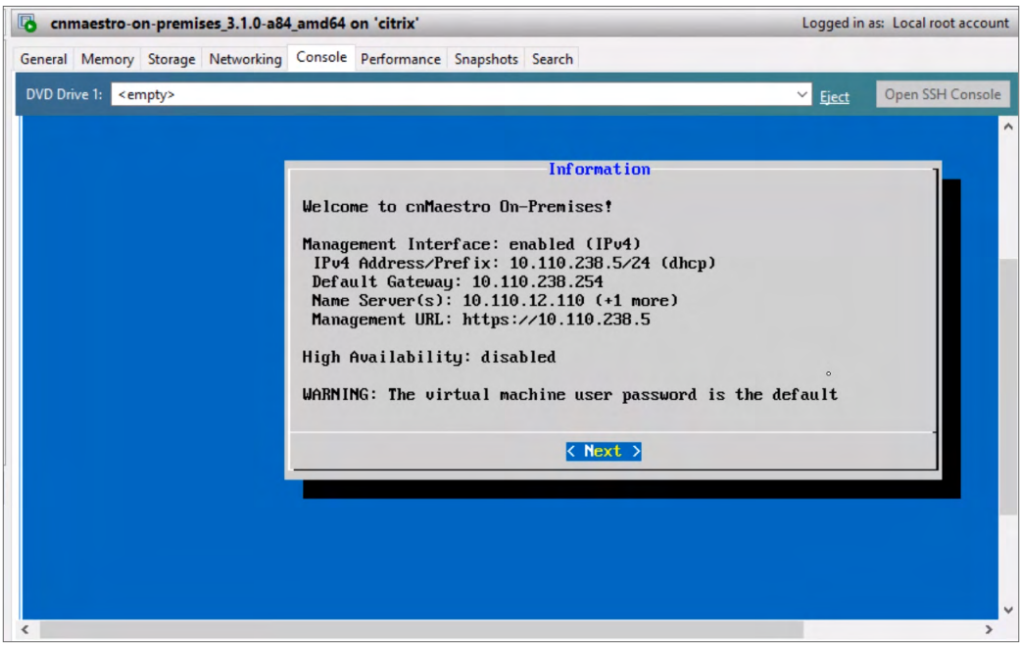
    The Import might take few minutes depending on the network, number of hard disks, and the Storage Repository speed. Once the Import completes, start the VM. The Import status can be viewed in the status bar as shown in the figure below.



12. The new VM will appear on the left panel. Select the VM and click **Start VM** and navigate to the configuration screen.



13. Open the **Console** tab and login with user name **cambium** and default password **cnmaestro**.
14. If needed, the **Scale** option may make the console easier to view.
15. The console provides status as well as a basic settings interface for the appliance.



Access cnMaestro

SSH Access

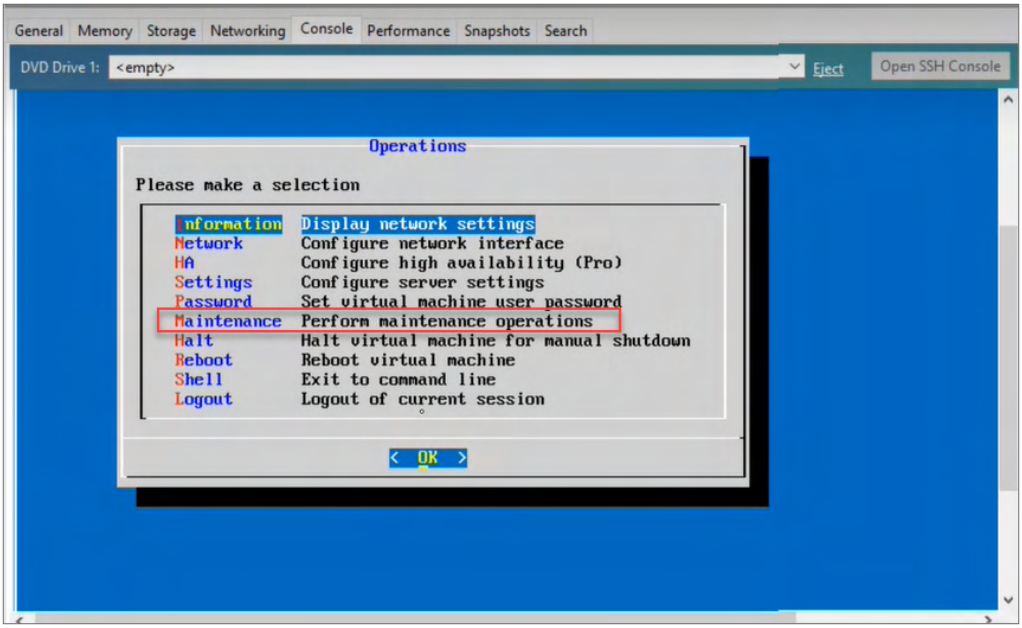
Note

- The TUI warns if you have not changed the default password.
- Clear the **Scale** option to view console.

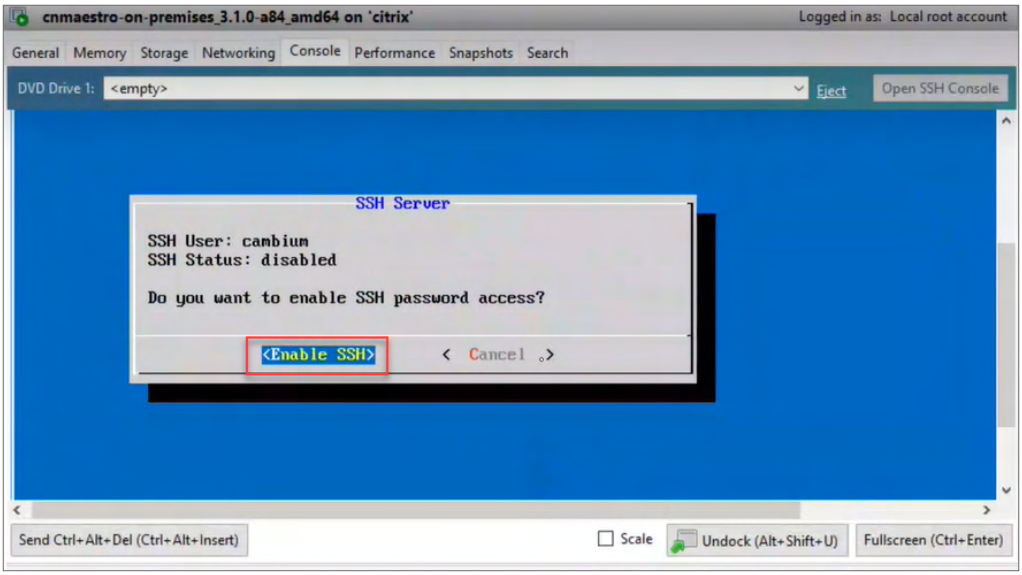
SSH access is disabled by default.

To enable SSH:

1. Navigate to **Maintenance** > **SSH** in the menu.



2. Select **Enable SSH**.



Once enabled, you can access cnMaestro over SSH. You must change the default password before enabling SSH.

HTTPS Access

You can launch the web UI over HTTPS by entering the cnMaestro IP address in the browser. The default SSL certificate is self-signed and will generate a self-signed certificate error. After logging in, you can upload a custom certificate by navigating to **Administration** > **Server** > **SSL Certificates** in the web UI.

Advanced Options

Expand the Data Disk

Warning:

Always take a snapshot of the data volume before expanding it.

The data volume can be expanded at any time as the number of devices in the account increases. The process consists of two parts:

- Expand the volume through Citrix Hypervisor
- Expand the file system within cnMaestro

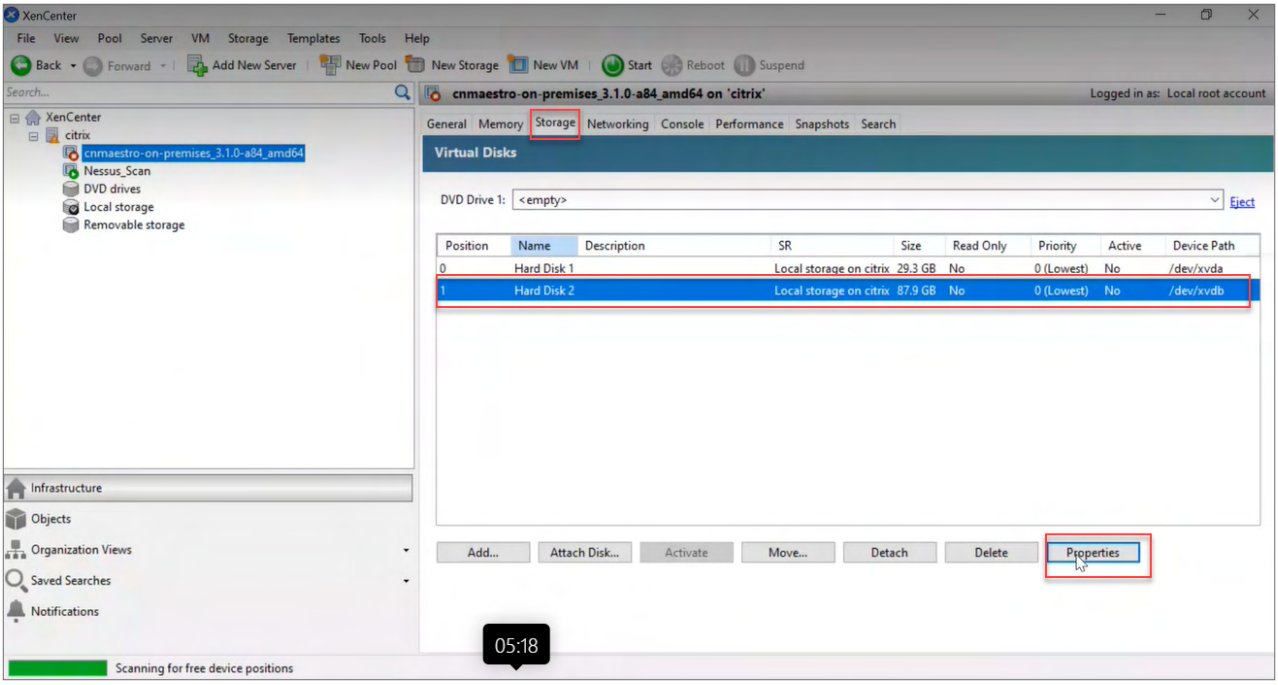
Expand the volume through Citrix Hypervisor

Expand the volume using the Citrix Hypervisor:

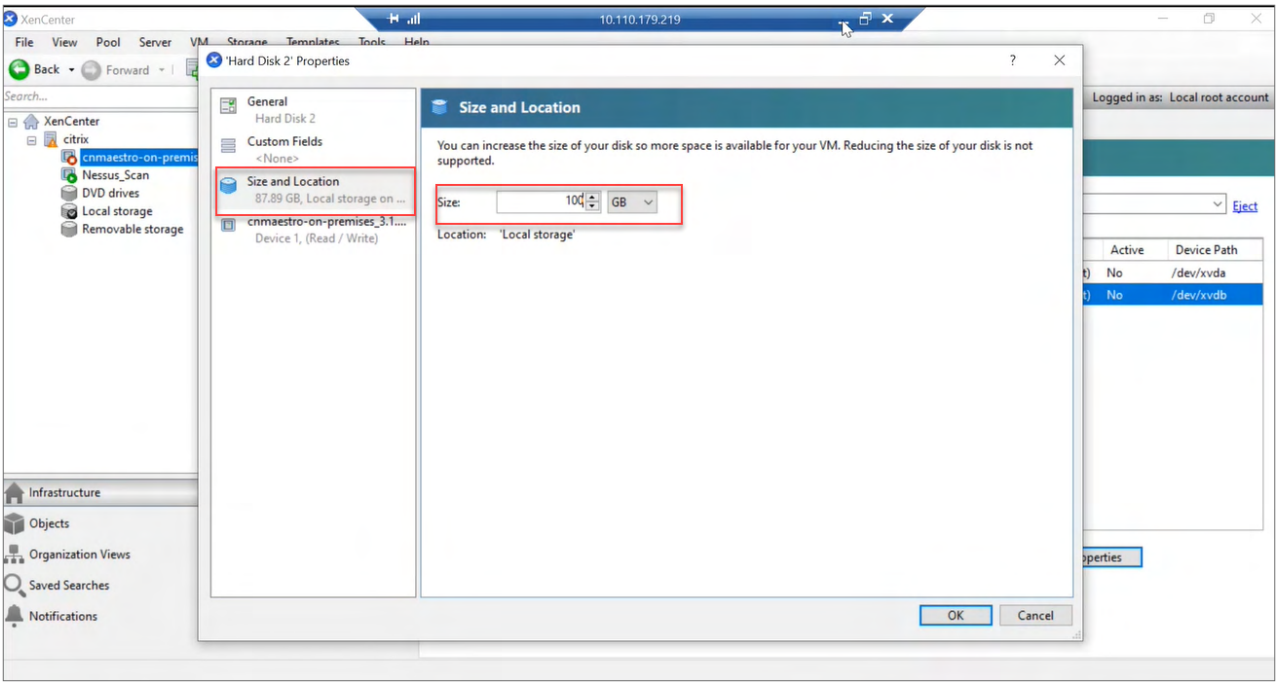
Note

Shutdown the VM before increasing the hard disk size.

1. Open the VM **Storage** tab.



2. Right-click on the data disk (by default **Hard Disk 2** is selected).
3. Click **Properties**.
4. In the **Size and Location** tab, increase size of hard disk selected and click **OK**.



5. Restart the VM.

Expand the file system within cnMaestro

If the file system is not automatically expanded, you may need to do this manually. You can do this by using the cnMaestro Console or SSH.

1. Login to cnMaestro through SSH and exit to the command line.
2. Run `lsblk` command to determine the disk that maps to the data store.
   - The name might be different, depending on the type of image originally selected for the instance.
3. Grow the partition to use the full disk.

   For example, expand partition 1 of the /dev/xvdb device:

   ```
   sudo growpart /dev/xvdb 1
   ```

4. Grow the file system mapping to /mnt/data. For the above example, execute the below command:

```
sudo resize2fs /dev/xvdb1
```

```
tmpfs                   391M  4.5M  386M   2% /run
/dev/mapper/system-os1  7.3G  4.8G  2.2G  69% /
tmpfs                   2.0G   48K  2.0G   1% /dev/shm
tmpfs                   5.0M     0  5.0M   0% /run/lock
tmpfs                   2.0G     0  2.0G   0% /sys/fs/cgroup
/dev/mapper/system-tmp  1.8G  5.7M  1.7G   1% /tmp
/dev/mapper/system-os2  7.3G   34M  6.9G   1% /mnt/os2
/dev/mapper/system-log  5.5G   77M  5.1G   2% /var/log
/dev/xvda1              464M   83M  354M  19% /boot
/dev/xvdb1               87G  733M   81G   1% /mnt/data
tmpfs                   391M     0  391M   0% /run/user/1000
cambium@cnmaestro:~$ sudo growpart /dev/xvdb 1
CHANGED: partition=1 start=2048 old: size=184317952 end=184320000 new: size=209713119,end=209715167
cambium@cnmaestro:~$ sudo resize2fs /dev/xvdb1
resize2fs 1.44.1 (24-Mar-2018)
Filesystem at /dev/xvdb1 is mounted on /mnt/data; on-line resizing required
old_desc_blocks = 11, new_desc_blocks = 13
The filesystem on /dev/xvdb1 is now 26214139 (4k) blocks long.

cambium@cnmaestro:~$ df -kh
Filesystem              Size  Used Avail Use% Mounted on
udev                    1.9G     0  1.9G   0% /dev
tmpfs                   391M  4.5M  386M   2% /run
/dev/mapper/system-os1  7.3G  4.8G  2.2G  69% /
tmpfs                   2.0G   48K  2.0G   1% /dev/shm
tmpfs                   5.0M     0  5.0M   0% /run/lock
tmpfs                   2.0G     0  2.0G   0% /sys/fs/cgroup
/dev/mapper/system-tmp  1.8G  5.7M  1.7G   1% /tmp
/dev/mapper/system-os2  7.3G   34M  6.9G   1% /mnt/os2
/dev/mapper/system-log  5.5G   77M  5.1G   2% /var/log
/dev/xvda1              464M   83M  354M  19% /boot
/dev/xvdb1               98G  742M   93G   1% /mnt/data
tmpfs                   391M     0  391M   0% /run/user/1000
cambium@cnmaestro:~$
```

Network Port Requirements

Inbound Ports

The following table provides information about network port requirements for inbound:

Table 161 *Inbound Port Details*

Port Number	Port Type	Purpose
443	TCP	HTTPs Web Access and device communication
18301	TCP/UDP	Wi-Fi Performance Test
161	UDP	SNMP Communication
22	TCP	Data Replication (High Availability)
8300	TCP	Distribution Synchronization (High Availability)
8301	TCP/UDP	Distribution Synchronization (High Availability)
3799	UDP	RADIUS CoA for RADIUS Proxy feature

Outbound Ports

The following table provides information about network port requirements for outbound:

Table 162 *Outbound Port Details*

Port Number	Port Type	Purpose
18301	TCP/UDP	Wi-Fi Performance Test
162	UDP	SNMP Trap Receiver
465 and 587	TCP	SMTP Server communication
20 and 21	TCP	FTP and SFTP communication
49	TCP/UDP	TACACS+ Server communication
1812	UDP	Free RADIUS Server Authentication communication
1813	UDP	RADIUS Server Accounting communication
389 and 636	TCP/UDP	LDAP or Active Directory (AD) server communication
514	UDP	Syslog server

Custom Network Scripts

If your network requirements are more complex than cnMaestro configuration, you can script custom networking commands, so they are executed after cnMaestro initializes networking. The commands are added to the file **/srv/files/etc/cnmaestro-network.override**, which also contains directions and a sample static route.

Xirrus Migration using Tool

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:

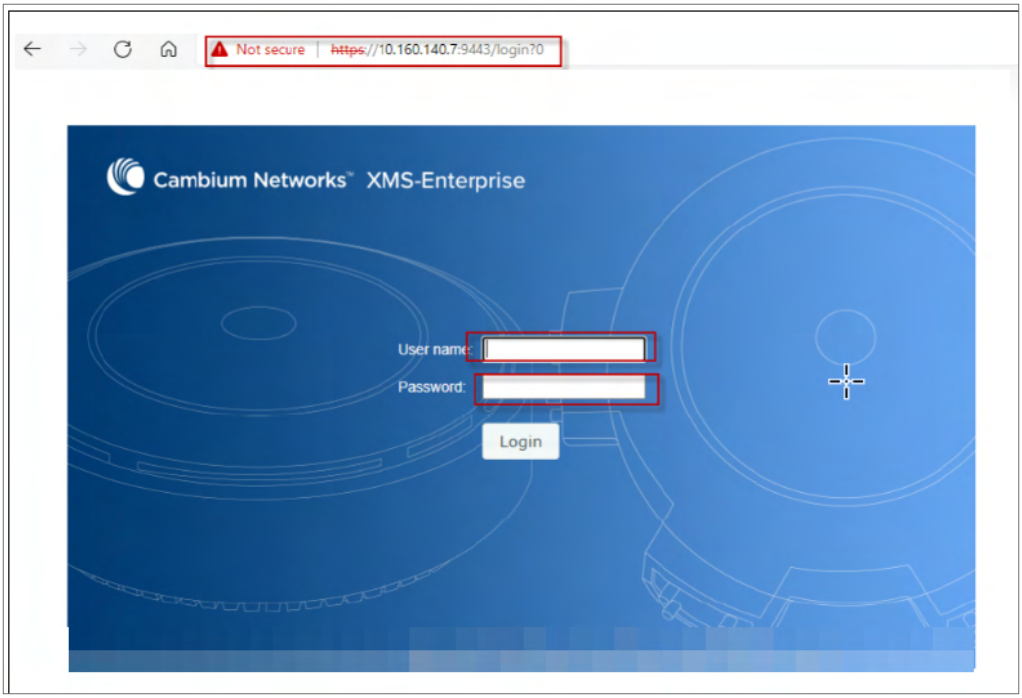
1. In XMS-E:
   - Export Golden Configuration
   - Migrate to cnMaestro X
2. In cnMaestro X:
   - Create Wi-Fi AP Group
   - Claiming the Wi-Fi Devices
   - Import and Apply AP configuration

XMS-E system

To login to XMS-E, complete the following steps:

1. Type the IP address in the URL.
2. Enter the username and password.

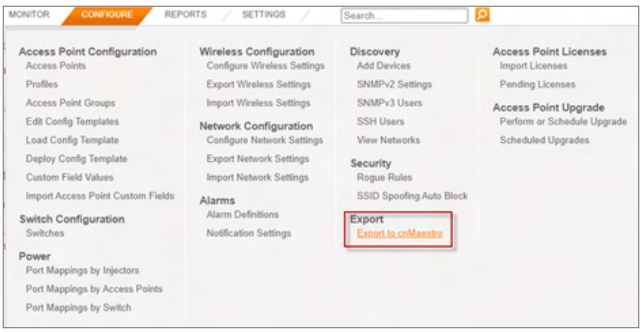
3. Click **Login**.



Export Golden Configuration

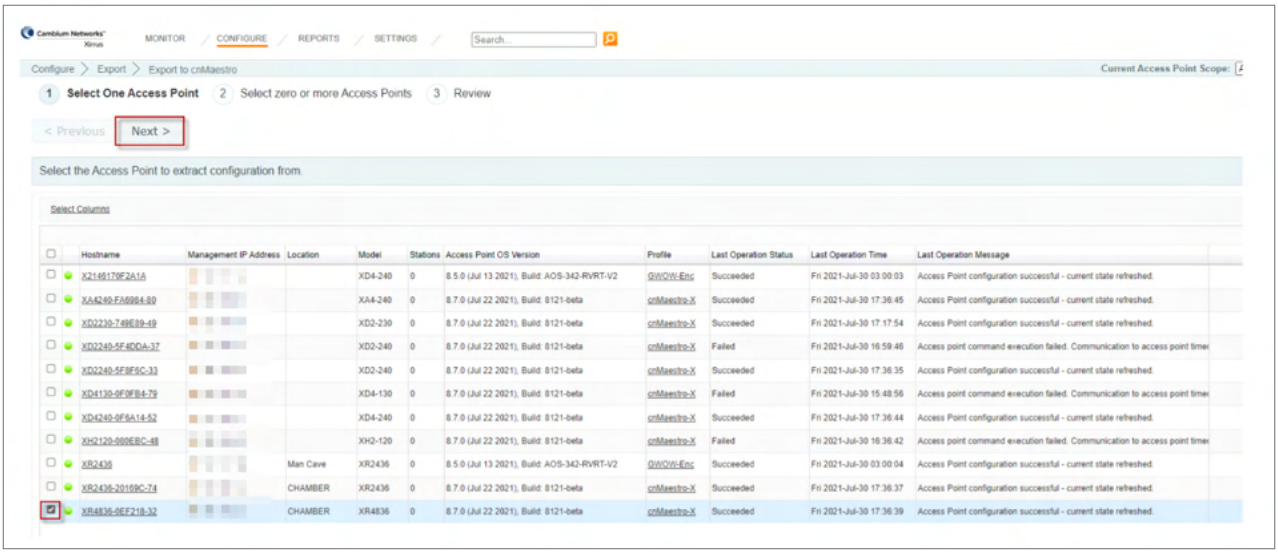
To start export golden configuration in XMS-E, navigate to **Configure** tab > **Export**.

1. Select **Export to cnMaestro**.

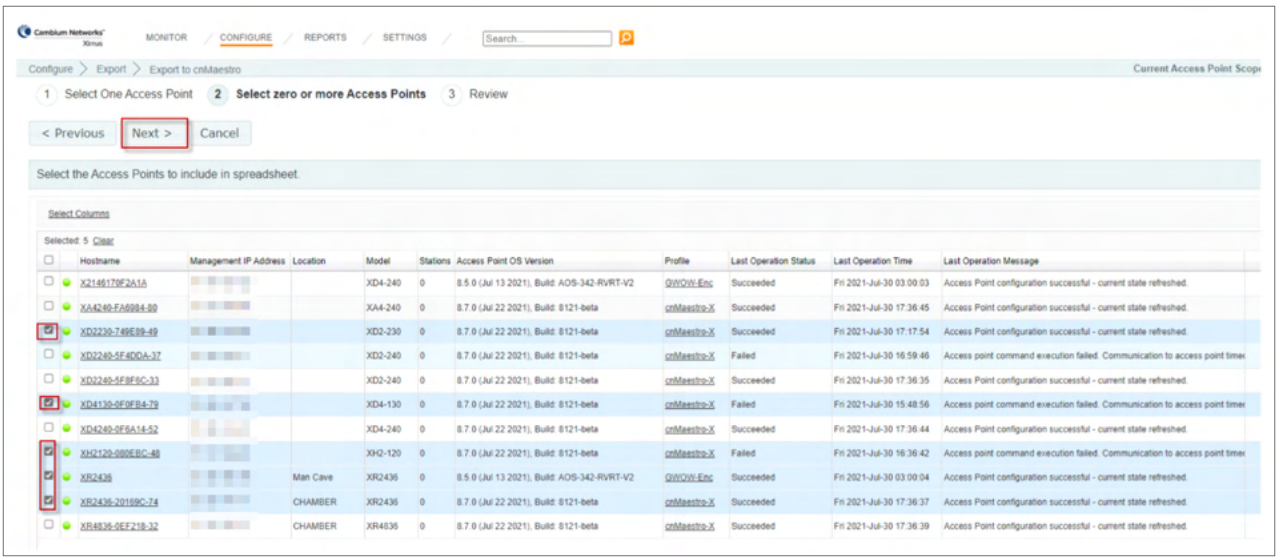


2. Select the AP to create the golden configuration for a group of APs and click **Next**.

> **Note**
>
> Select the AP with the maximum radios and the highest capability.



3. Select group of APs to be added to the spreadsheet that requires overrides and click **Next**.

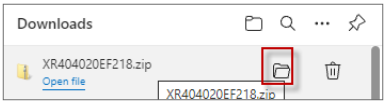


4. Click **Export**.

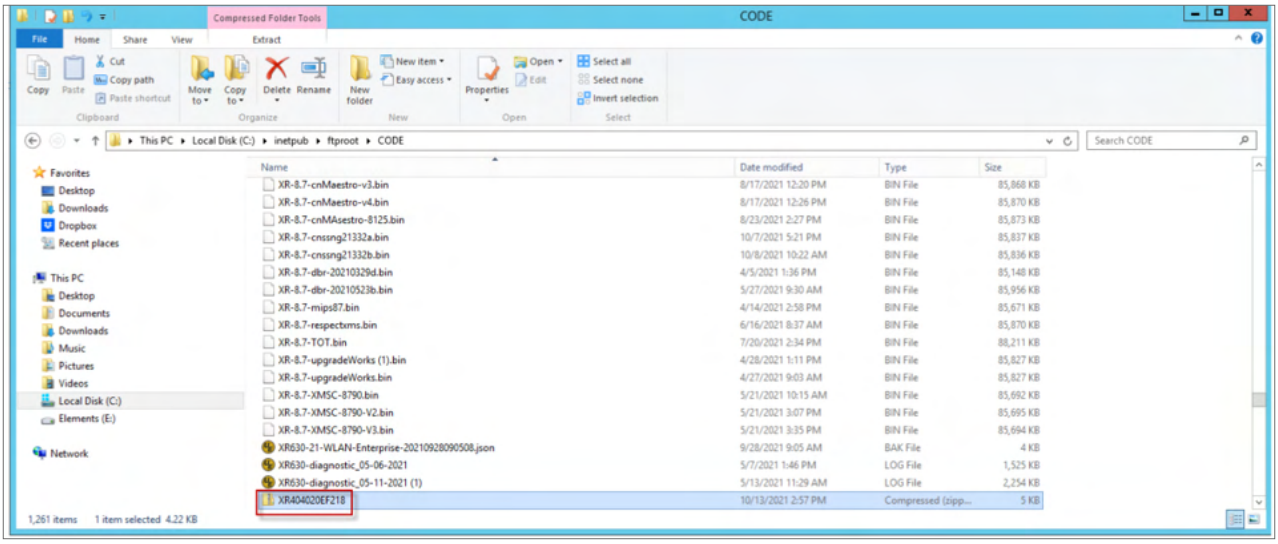
   It creates a zip file, which consists of two files—conf and csv. The conf file contains the full configuration of the AP with dollar variables, and the CSV file contains the override values.

5. Unzip the directory and move the files to local directory.

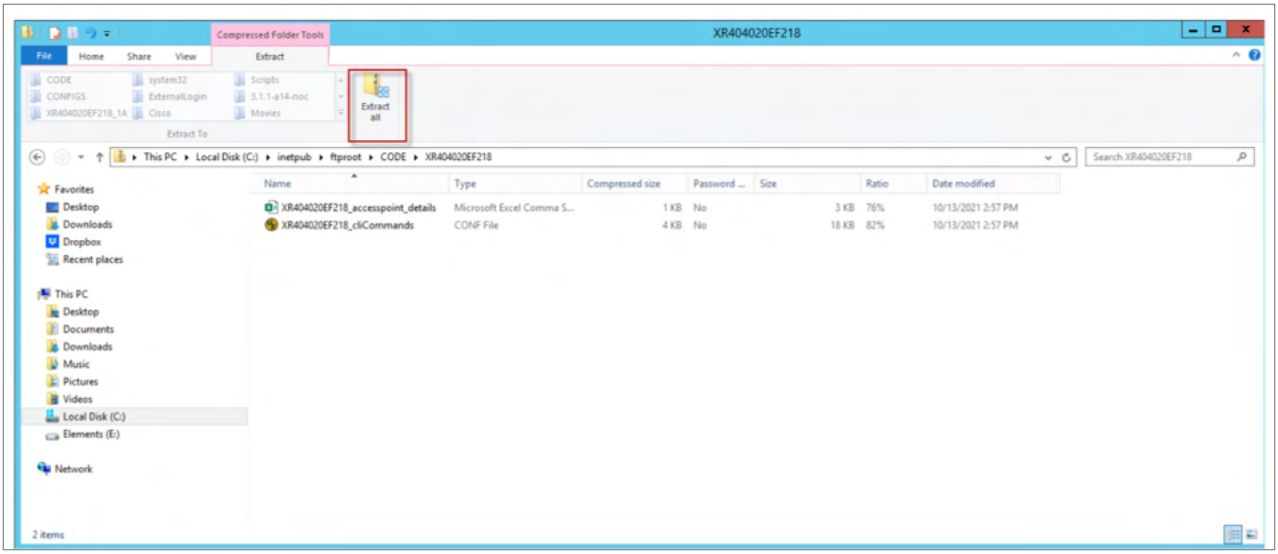
6. Go to the folder where the zipped files are saved and extract the contents to a folder.



7. Open the directory path where the file is stored and double-click on the zipped file.



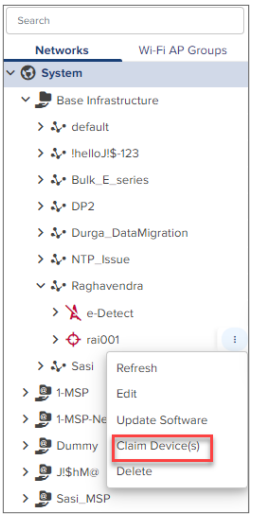
8. Click **Extract all**.



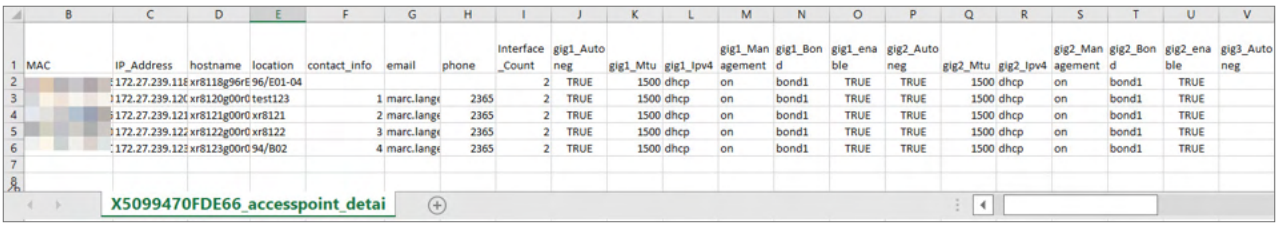
Claiming the Wi-Fi Devices

To claim multiple APs from the Site dashboard, perform the following steps:

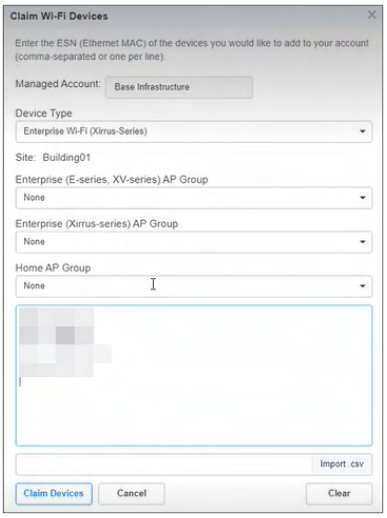
1. Navigate to **Manage** > **Networks** tree view and select the dropdown menu for the Site.
2. Click **Claim Devices** from the dropdown.



3. Select the AP Group that should be applied for Xirrus devices. The devices claimed under the Site will have the configuration settings from the selected AP Group.



MAC	IP_Address	hostname	location	contact_info	email	phone	Interface_Count	gig1_Autoneg	gig1_Mtu	gig1_Ipv4	gig1_Management	gig1_Bond	gig1_enable	gig2_Autoneg	gig2_Mtu	gig2_Ipv4	gig2_Management	gig2_Bond	gig2_enable	gig3_Autoneg
	172.27.239.118	xr8118g96r	96/E01-04				2	TRUE	1500	dhcp	on	bond1	TRUE	TRUE	1500	dhcp	on	bond1	TRUE	
	172.27.239.12	xr8120g00r0	test123	1	marc.lange	2365	2	TRUE	1500	dhcp	on	bond1	TRUE	TRUE	1500	dhcp	on	bond1	TRUE	
	172.27.239.121	xr8121g00r0	xr8121	2	marc.lange	2365	2	TRUE	1500	dhcp	on	bond1	TRUE	TRUE	1500	dhcp	on	bond1	TRUE	
	172.27.239.122	xr8122g00r0	xr8122	3	marc.lange	2365	2	TRUE	1500	dhcp	on	bond1	TRUE	TRUE	1500	dhcp	on	bond1	TRUE	
	172.27.239.123	xr8123g00r0	94/B02	4	marc.lange	2365	2	TRUE	1500	dhcp	on	bond1	TRUE	TRUE	1500	dhcp	on	bond1	TRUE	

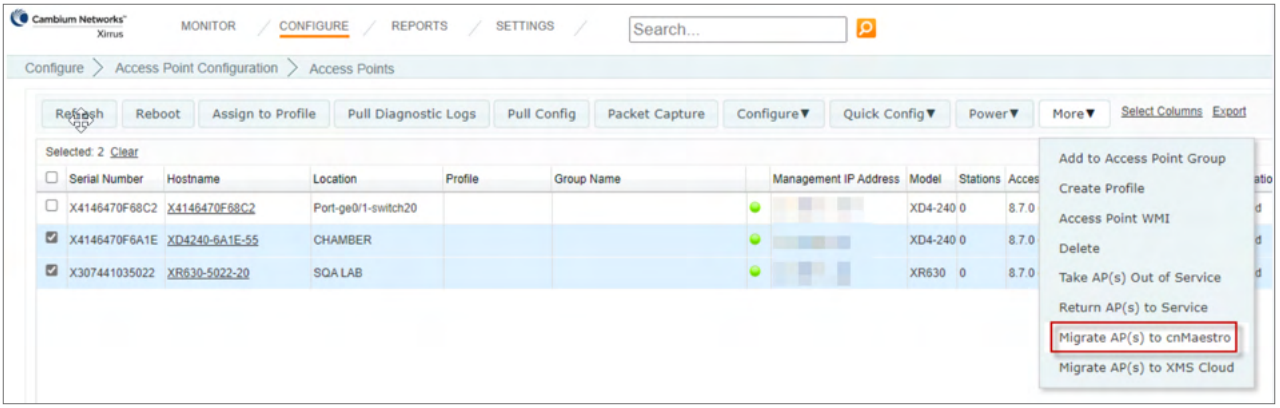


4. Specify the MAC Address of the devices line-by-line or comma-separated, (MAC address are copied from csv files) or use the **Import .csv** option to import the MAC of the devices from a file.

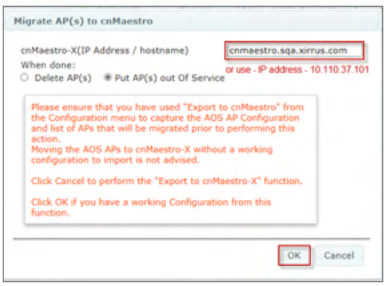
Migrate to cnMaestro X

Perform the following steps to migrate to cnMaestro X.

1. Select APs to migrate.



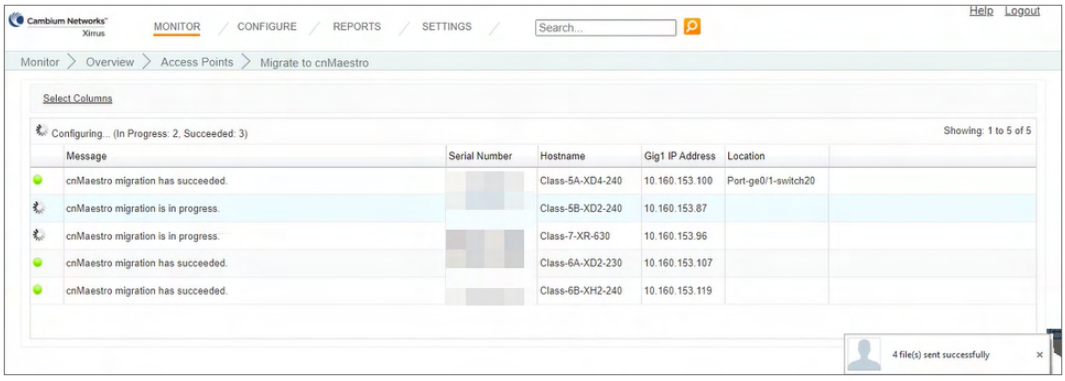
2. Enter the IP address or Hostname mapped in DNS for cnMaestro X.
3. Select **Delete AP** or **Put AP(s) out of Service** and click **OK.**



Note

- **Out of service APs** are not removed from XMS-E, so if there is an issue, you can **Return APs** to Service and they will be available on XMS-E.
- You have to reset using the AP CLI command `snmp trap host 1 Xirrus-XMS` on the AP for the Return to Service to work.
- If you select **Delete APs**, they will be removed and you have to rediscover them on the network to add them back to XMS-E.
- You should also remove the Device Network from the Device discovery section to clean up XMS-E.

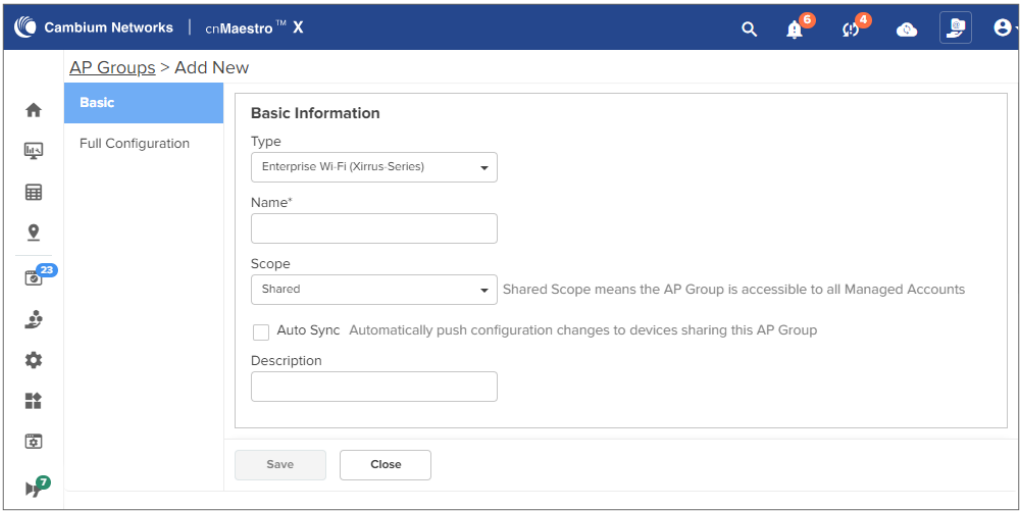
A success message from XMS-E for each of the APs migrated to cnMaestro X is displayed.



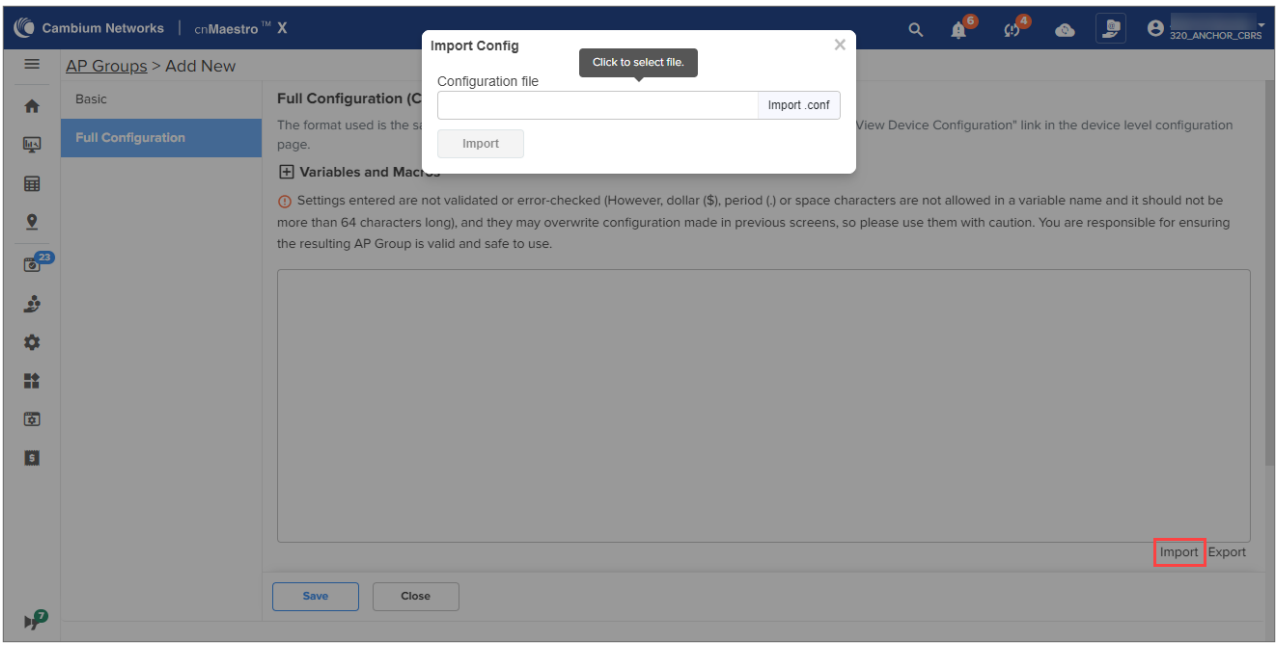
Create Wi-Fi AP Group

Create Wi-Fi AP Group and import CLI command file from exported directory.

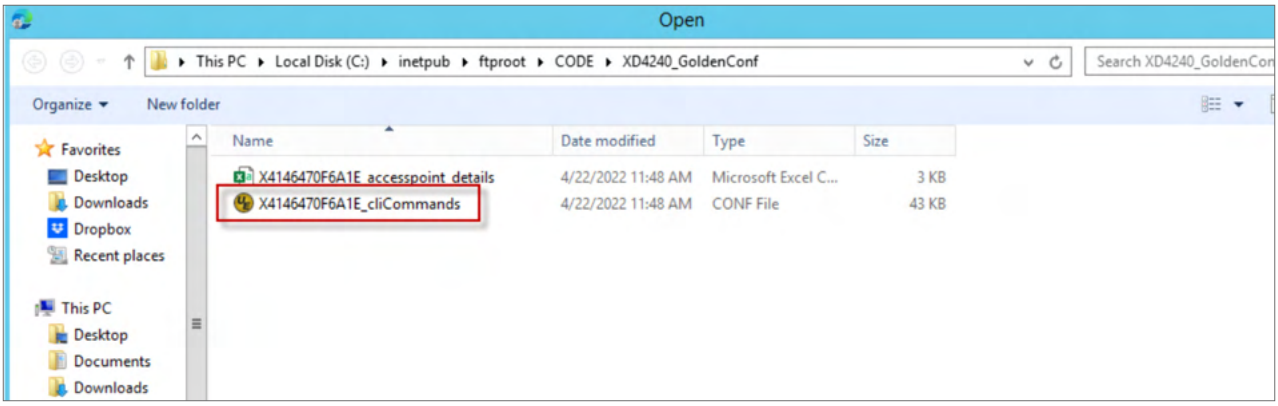
1. Navigate to **Shared Settings** > **AP Groups and WLANs.**
2. Enter the required parameter details.
3. Click **Save.**



4. In the **Full Configuration** page, import the golden configuration conf file as the full configuration of the Wi-Fi AP Group.

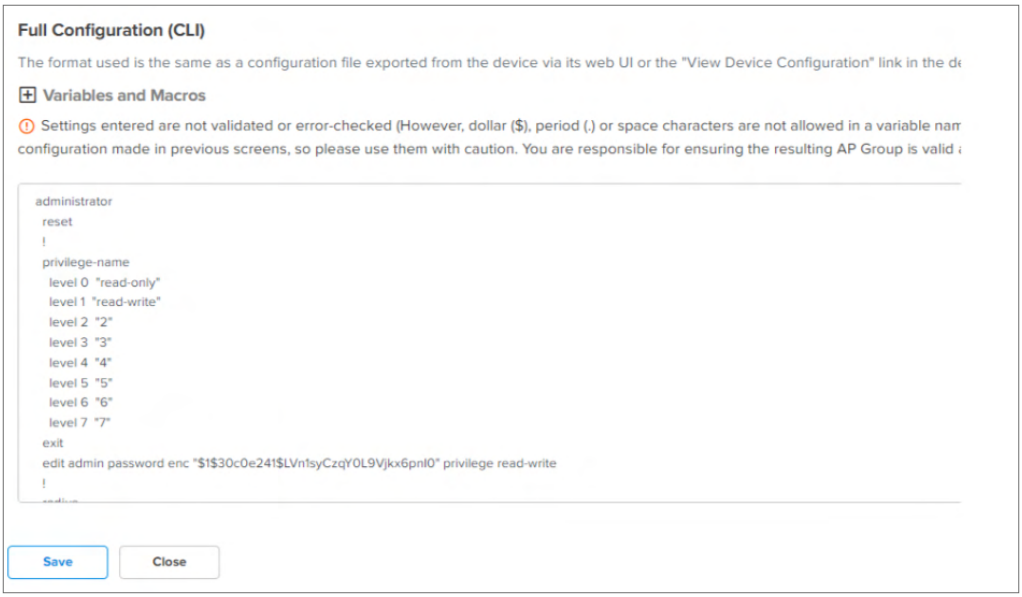


5. Select the CLI command file from the unzipped directory.



6. Click **Import**.

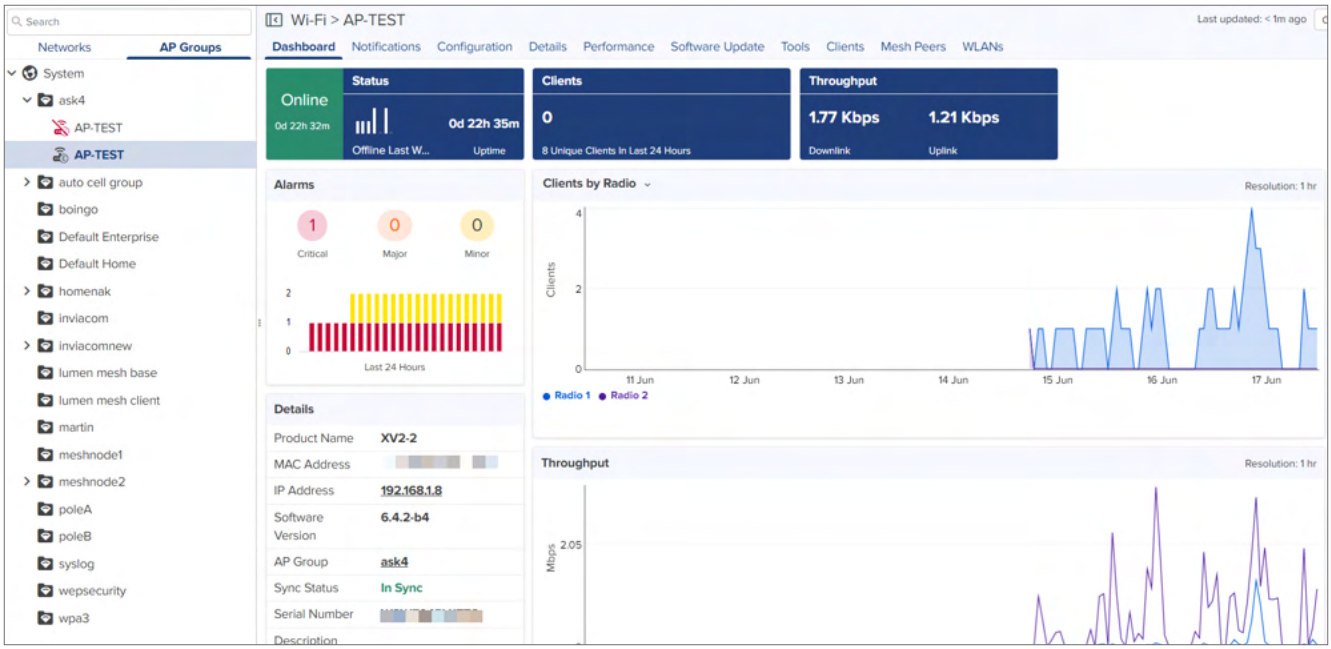
The configuration file is displayed.



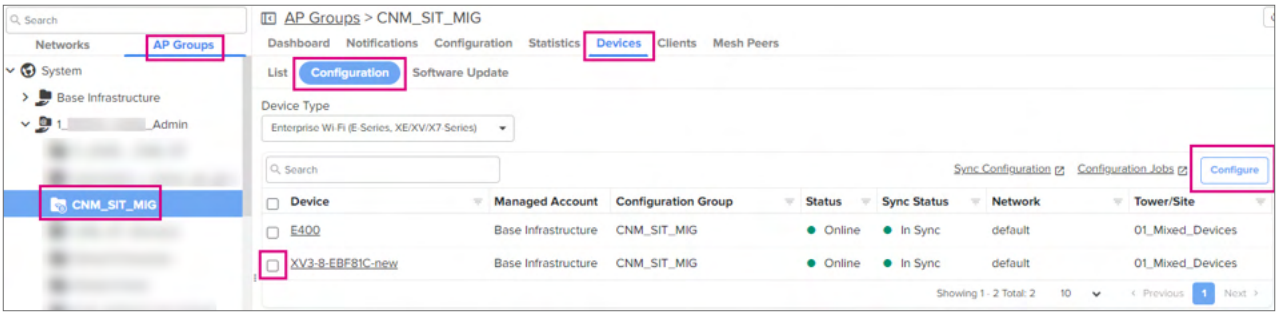
7. Click **Save**.

Import and Apply AP configuration

APs imported are ready for basic configuration. Import AP configuration using .csv file from exported directory.

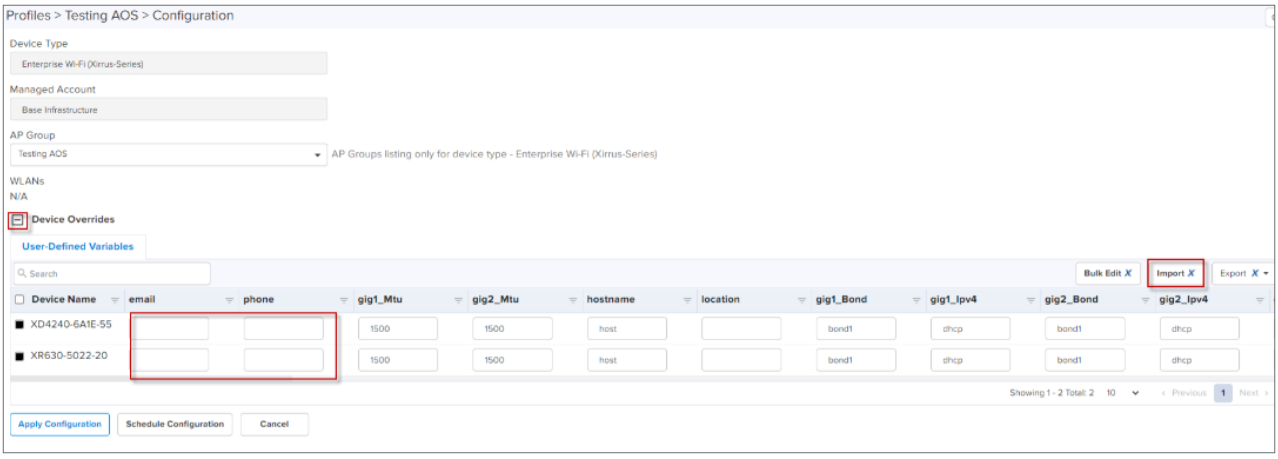


1. Navigate to **AP Groups** > select AP Group > **Devices** tab > **Configuration**.
2. Select all APs to configure, click **Configure.**

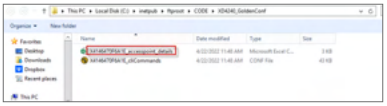


3. In the Device Override table, verify AP details and click **Import.**

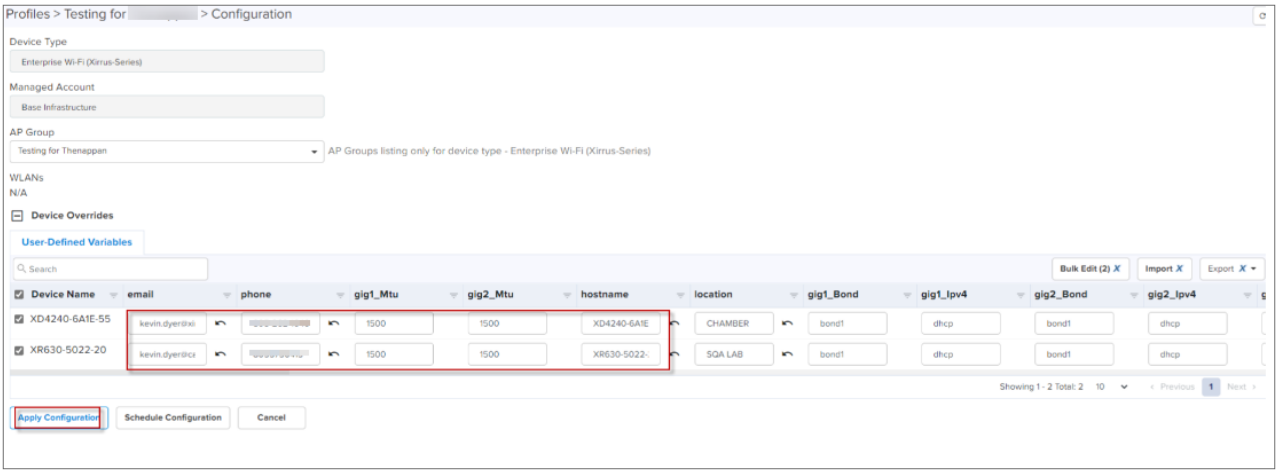
> **Note**
>
> Any unique device level overrides are auto populated from the .csv file.



4. Select the .csv import file from the unzipped directory folder and click **Apply**.

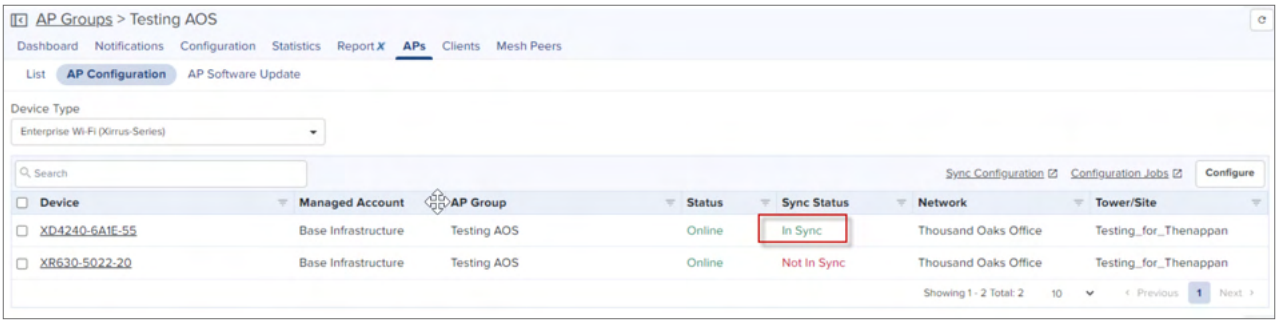


All the configuration values from the .csv file are populated for each AP. The data is auto populated to the **User Defined Variables** tab. The APs receive complete configurations including their IAP settings.



5. Click **Apply Configuration.**

When the APs are configured, **Sync Status** is displayed as **In Sync**. You have to refresh the page to view the updated **Sync Status.**



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™ www.cambiumnetworks.com

Cambium Networks and the stylized circular logo are trademarks of Cambium Networks, Ltd. All other trademarks are the property of their respective owners.

Copyright © 2026 Cambium Networks, Ltd. All rights reserved.