



Cambium Networks™











USER GUIDE

cnMaestro Cloud

Release 6.2.0

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 ***30***

Supported Devices and Features **30**

Devices and minimum software versions 30

Supported browsers 33

Network connectivity 34

cnMaestro features 34

Quick Start **41**

Create and manage accounts **41**

Create a Cambium Support Center login 41

Create a cnMaestro account 43

Log on to cnMaestro 45

Claim and onboard devices **47**

Claim devices by serial number 47

Claim devices by Cambium ID 49

Cambium ID configuration 49

Onboarding Key configuration 50

Onboard device using Onboarding Key 52

Creating a Cloud Account **54**

Overview 54

Creating a Support Center User ID 54

Creating a Cloud NMS Account 55

Creating an Anchor Account 57

Multiple Cloud Accounts 59

Account selection 60

Concurrent access 60

Managing users 60

Organization 61

cnMaestro X **62**

NSE subscription 62

cnMaestro X Trial self-activation 63

cnMaestro X activation **64**

Slot Deficit 67

Subscription Management **70**
Manage Subscriptions 71
Usage Summary 72
Device Tiers 72
Devices 73
Swap Subscription 74
Change Subscription 75
Delete on Expiry 76
Expiry Notification 77
Expired Device 78
Retention of Data After Expiry and Reinstatement of Service 79
Creating Scopes for Subscriptions 80
Enabling and adding scopes 80
Editing, deleting, and disabling scopes 82
Overdraft Subscription 82
Download a Bill of Material (BoM) 83
cnMaestro X features behavior state **85**
Navigating the cnMaestro UI **92**
Account View 93
Access and Backhaul view 94
Enterprise view 94
User consent to allow device diagnostic access to Cambium Support 94
Home page 94
Page structure 95
Searching for cnMaestro resources using the Search bar 97
Page navigation 97
Access and Backhaul View 98
Overview 98
Enterprise Account view 105
Overview 105
System 105
Devices 105
AP Groups 106
WLANs 107
Switch Groups 107
NSE Groups 108
Sites 108

Side menu 108
Section tabs 109
System status 109
Data Tables and Chart UI Controls 110
Logout 110
Device Onboarding 111
Onboarding Overview 111
Claiming Devices 111
Claiming Devices with Serial Number 112
Claiming Devices with Cambium ID 114
Onboarding Queue 116
Serial Number flow 116
Cambium ID flow 116
Onboarding fields 117
Onboarding Configuration 118
Onboarding Actions 119
60 GHz E2E Controller Onboarding 119
Header Notification 120
Zero Touch Configuration 120
Claiming Your First Wi-Fi AP (Cloud) 120
Claiming a single Wi-Fi AP from the Home page 121
Claiming a single Wi-Fi AP using the AP Group menu 122
Claiming multiple Wi-Fi APs from the AP Group 123
Claiming multiple Enterprise devices from the Enterprise Site dashboard 124
Claiming multiple Enterprise devices using CSV import 125
Points to consider when importing enterprise devices using CSV import option 128
Miscellaneous Onboarding Issues 128
Configuring Devices after Onboarding 128
Deleting Devices 128
Transferring Device Ownership 128
Onboarding Examples 128
Onboarding Existing Networks 129
Onboarding New Devices 129
Claiming Devices using Cambium ID and Device UI 129
Claiming Devices Using Cambium ID and SNMP 130
Device-Specific Onboarding Instructions 130
Onboarding cnMatrix 130

Onboarding cnMatrix through UI 131
Onboarding cnRanger 131
Setting static URL for cnMaestro on Sierra 800 131
Setting static URL for cnMaestro on Tyndall 101 132
Onboarding cnReach 132
Onboarding through UI 132
Onboarding cnPilot R-Series 133
Onboarding through UI 133
Onboarding through SNMP 134
Onboarding cnVision 134
Onboarding cnVision Client 134
Onboarding cnVision Hub 135
Onboarding Enterprise AP 135
Onboarding through UI 135
Onboarding ePMP 1000 136
Onboarding through UI 136
Onboarding through SNMP 137
Onboarding PMP 138
Onboarding through UI 138
Onboarding through SNMP 139
Onboarding PTP 650/670/700 139
Onboarding Xirrus device 139
Onboarding a cnWave 5G Fixed BTS device 140
Claiming a cnWave 5G Fixed BTS device 140
Claiming a cnWave 5G Fixed BTS device with the Serial Number 143
Onboard Edge Controller 145
Onboard PTP 820/850 devices 145
Onboarding the NSE 3000 Devices 146
Onboarding Home Mesh Routers 147
Onboarding PON devices 147
Onboarding 60 GHz cnWave devices 148
Onboarding a 60 GHz device with external E2E Controller 149
Onboarding a 60 GHz device with Onboard E2E Controller 151
Deleting Devices in Bulk 154
Device-specific restrictions 154
Deleting devices in bulk 155
Viewing the status of device deletion and retrying 156

Export All as CSV **158**
Exporting and downloading all data in the CSV format 159
Replacing Devices **160**
Points to remember and prerequesites for replacing a cnMatrix switch or AP 160
Replacing devices 161
Monitoring ***162***
Network Monitoring **162**
Assists X 162
Exporting assists information 165
Assists filter 165
Assists Status 166
Device filter 168
Enable Assist 169
Assists X fix now 169
Dashboard 171
KPI (Key Performance Indicators) 171
Application History X and Applications X 172
Device Health 173
Connection Health 174
Charts and Graphs 174
Site dashboard 175
Enterprise Site dashboard 176
Devices widget (Total, Offline, Out of Sync) 177
Throughput 178
Client Connection Health X 179
Wi-Fi Client Analytics X 179
Assists X 179
Alarms 179
Top Active Alarms 180
AP Types 180
Stacked Clients by Band 180
Channel Distribution by Band 181
Clients Performance by Band (Enterprise Wi-Fi) 181
Clients SNR by Band (Enterprise Wi-Fi) 181
Connected 6 GHz Client Capability 181
Application History X (Category History X) 182

Client Capability History 182
Radio Distribution by Band 183
WLAN Distribution by Band 183
Throughput Graph 183
Top Wi-Fi APs by Throughput or Clients 184
Top Clients by Session 184
Top Clients by Usage 184
RV22 Home Site Dashboard 184
60 GHz cnWave Site Dashboard 185
PON Site Dashboard 186
Notifications 187
Event/Alarm Source 188
Aggregation 189
Storage 189
Events 189
Event Severity 189
Event Export 189
Alarms 263
Alarm History 266
Wi-Fi Events 268
Configuration 269
Statistics and Details 270
Statistics page 270
Details page 281
PON (OLT) 307
PTP 650/670/700 308
PTP 820/850 Details 309
Home Mesh Routers 313
Performance **313**
Map **328**
Map Navigation 330
Mode 330
Embedded Maps 331
Sector Visualization 331
Tools **335**
60 GHz cnWave Tools 336
cnMatrix Tools 336

Cable Diagnostic 337
Port Enable or Port Disable 338
PoE Toggle 339
PoE Enable or PoE Disable 340
Remote CLI 342
cnPilot Home Tools 344
cnRanger Tools 346
cnRanger BBU 347
cnRanger SM 347
cnReach Tools 347
cnVision Tools 348
Edge Controller Tools 349
Enterprise Wi-Fi Tools 349
Packet Capture 351
ePMP Tools 355
PMP Tools 357
cnWave 5G Fixed Tools 359
Status 359
Link Test 359
Ping Test 361
RV22 Home Mesh Tools 362
Status 362
Debug 363
Network Connectivity 363
Wi-Fi Analyzer 364
Speed Test 365
Packet Capture 366
Wireless Intrusion Detection System (WIDS) 367
Neighboring APs 368
Rogue APs 370
Honeypot APs 371
Wired Devices 371
Ad Hoc Networks 372
Allowlist APs 373
Configuring WIDS 374
Configuring Wired Neighbor Discovery 375
Wireless Flood Detection 375

Wireless Intrusion Prevention System (WIPS) 376
Off Channel Scan (OCS) 377
Network Service Edge (NSE) **378**
Dashboard 378
Notifications 379
Configuration 380
Advanced Settings 380
Factory Reset 383
User-Defined Overrides 384
Configuration Lock 385
Security 385
Threats 385
DNS Filtering 387
Vulnerabilities 388
Network 394
LAN 394
Routes 395
WAN 396
VPN Sites 397
Tailnet 398
Starlink 399
Cellular WAN 401
Firewall Counters 404
Debug Tools 407
Clients 409
Device-level information 410
Network- and Site-level information 412
Client-level information 415
Certificate 418
PMP Dashboard **418**
Multiple Component Carrier (CC) Support in PMP 450v 419
PMP 450v 4×4 AP/BHM dashboard 419
PMP 450v 4×4 SM/BHS and PMP 450v 2×2 SM/BHS dashboard 420
PMP 450v 4×4 AP/BHM Map View 421
Wireless LAN Dashboards **422**
Wi-Fi Monitoring 422
Dashboard 422

Clients 423
Details 430
Mesh Peers 434
Site Dashboard 435
Client Connection Health X 437
Wi-Fi Client Analytics X 437
Assists X 437
Alarms 437
Top Active Alarms 438
AP Types 438
Stacked Clients by Band 438
Channel Distribution by Band 438
Clients Performance by Band (Enterprise Wi-Fi) 439
Clients SNR by Band (Enterprise Wi-Fi) 439
Connected 6 GHz Client Capability 439
Application History X (Category History X) 440
Client Capability History 440
Radio Distribution by Band 441
WLAN Distribution by Band 441
Throughput 441
Throughput Graph 442
Top Wi-Fi APs by Throughput or Clients 442
Wi-Fi devices widget (Total, Offline, Out of Sync) 442
Top Clients by Session 442
Top Clients by Usage 443
Floor Plan 443
Statistics 448
Wireless Clients 449
WLANs Dashboard 450
Fiber OLT and ONU 454
Dashboard 455
Alarms 456
Port Status 456
ONU by Signal Level 456
ONU by Signal Level per Port 457
ONUs 457
PON Downlink Utilization 457

PON Downlink Throughput 458
PON Uplink Throughput 458
Ethernet Downlink Throughput 458
Ethernet Uplink Throughput 459
Notifications 459
Configuration 460
Details 461
Performance 462
ONUs 462
Viewing and updating ONU profile 463
Export ONUs 465
Rename ONUs 465
Ports 466
Software Update 469
OLT Software Update 469
ONU Software Update 470
Tools 471
ONU Dashboard 471
Inventory 475
Inventory Export 475
Bulk Delete 475
Bulk Reboot 476
Schedule Reboot 477
Import Device Configuration 477
Sample Configuration File 478
Sample Configuration File (60 GHz cnWave) 478
Uploading a Configuration File 479
Reports 481
Data Reports 482
Devices Report 483
Audit Logs Report 492
Performance Report 493
Active Alarms Report 500
Alarm History Report 501
Events Report 502
Wireless Clients Report 503
Wi-Fi Events Report 504

Guest Access Login Events 505
Reports jobs 506
Graphical Reports **507**
Create Graphical Report Templates 509
Generate Reports Based on Templates 513
Provisioning ***515***
Software Update **515**
Software Update Overview 515
Create Software Update Job 516
Device Selection 516
Device Type 516
Software Update Dashboard 516
Software Update 521
Device Table 522
Retry Software Update 523
Options 523
Upgrade steps 524
Software Update Jobs and Parameters 525
Abort Software Job 525
Viewing Running Jobs in header 526
Fixed Wireless Configuration **526**
Overview **527**
Configuration Templates 527
Sample ePMP Template 527
Configuration Variables 528
Variable Usage 528
Macros 528
Variable Caching 528
Device Type-Specific Configurations 529
Device Mode restrictions 529
Variable validation 529
Sample Templates 529
Template file creation 529
Template **529**
BTS and CPE Configuration 531
Configuration Template for PTP 820/850 532

NTP Configuration 534
Time Services 534
SNMP 535
Security 535
Configuration Update 536
Device Selection 536
Device Type 536
Device Table 536
Options 537
Configuration Update Steps 537
Configuration Jobs 538
Configuration Update at Onboarding 539
Wi-Fi Configuration 539
Enterprise Wi-Fi AP 540
Configuring Enterprise Wi-Fi APs using Wi-Fi Profiles 540
Create an AP Group 541
Configuring 802.1X port-based authentication 560
IPv6 Support 561
Map WLANs to AP Groups 563
Lock device Configuration 564
Retrying configuration 564
Apply AP Group to Device 565
AP Group and WLAN Import/Export 566
Creating a WLAN 568
Creating an ePSK WLAN 585
Configuring Wi-Fi offloading and Passpoint 591
Access Control 595
Services 598
Pre-Defined Overrides 599
Advanced Settings 599
User-Defined Overrides 600
User-Defined Variables 601
Bulk Overrides 602
Location 605
Management VLAN 607
Radios 607
WLANs 608

Ethernet VLAN 609
User-Defined Variables 610
Synchronize (Sync) Configuration 611
Manual synchronization 611
Configuration Job Status 613
Factory Reset 613
Association ACL 615
Overview 616
Configuring Association ACL 616
Access Control Policies 617
Configuring Access Control Policies for AP Groups and WLANs 618
Custom Applications 619
cnMatrix Switch Profiles 621
Switch Groups 621
Basic 623
Management 625
Network 627
Security 631
Port Overrides 632
User-Defined Overrides 639
Switch Group Operations 639
Retry Configure 640
Create a Configuration Job 641
Synchronize (Sync) Configuration 641
Policy Based Automation (PBA) 644
Devices 646
Ports Stack 647
Port Templates 648
Port Templates Operations 651
Configuration 652
Device Configuration 653
Advanced Settings 654
Factory Reset 657
Device Details 658
Details Overview 659
Topology 659
Port Statistics 660

Clients 661
60 GHz cnWave Network Configuration **662**
Managing E2E Network 662
Dashboard 662
Notifications 668
Configuration 668
E2E Controller 674
High Availability X 675
Links 678
Statistics 688
Software Update 689
Reports 693
Map 693
Troubleshooting 703
Changing channel or Golay for specific 60 GHz cnWave links 714
Setting the Last Resort Metric (LRM) for a cnWave 60 GHz link 717
Tools 719
Site Configuration 731
Site Dashboard 734
Node Configuration 734
PoP Node configuration 736
DN/CN Node configuration 737
PoP Node 740
Dashboard 740
Configuration 741
Links 754
Details 759
Tools 760
DN/CN Node 763
Dashboard 763
Configuration 764
JSON 767
Links 769
Tools 771
NSE Configuration **773**
Claiming an NSE device associated with a site **774**
High availability support for NSE **775**

Licensing 775
Constraints on NSE devices 776
Creating an HA pair in cnMaestro 776
Onboarding an NSE device as an HA spare 776
Claiming an NSE device as an HA spare 779
Moving the HA pair (in the tree) 780
Deleting an NSE device from the HA pair 780
Deprecation of device overrides 780
Upgrading the firmware 781
Viewing aggregated data of HA pair 781
Creating Wireguard clients for NSE HA pair 782
Configuring NSE using cnMaestro Cloud 782
Basic 783
Management 785
Network 787
Groups 801
WAN 803
Adding a virtual WAN interface 819
Configuring rule precedence 824
Firewall 825
Automatically assigning system-generated names to existing DNAT rules 836
DNS 836
Threat Protection 840
VPN 843
Site-to-Site VPN configuration 843
Client VPN configuration 847
User configuration for Client VPN protocols 850
Tailscale configuration 852
RADIUS Client configuration 853
VPN Server interface configuration 854
User-Defined Overrides 854
Configuring WAN in the device UI 855
Configuring Auto VPN 858
Hub and Spoke mode 859
Mesh mode 859
Creating Auto VPN groups 859
Adding hubs and spokes for sites 862

Disabling or Enabling the Security Plus License Mode for NSE **869**
Disabling the Security Plus mode 871
Enabling the Security Plus mode 874
Configuring Advanced Features **877**
Lock Device Configuration 877
Strict Device Password Policy 877
Auto-Provisioning **878**
Creating Auto-Provisioning Rule 878
Managing Home Mesh Router **879**
Configuring Home Mesh Router **882**
Configuring WLAN Profiles (SSIDs) for Home Mesh Routers **882**
Configuring AP Groups for Home Mesh Routers **886**
Onboarding the Home Mesh Router to cnMaestro **898**
cnMaestro Subscriber application branding **899**
Adding a Home Site **901**
Managing subscribers (end-customer) **902**
Adding a Subscriber Service Profile 902
Adding a subscriber 904
Modifying the owner details for the Subscriber App 908
Claiming the Home Mesh Router 909
Setting up the Home Mesh Router **911**
Setting up the Home Mesh Router—Standalone mode **911**
Setting up the Home Mesh Router—Wireless Mesh Mode **912**
Wireless mesh: 1-1 deployment 912
Wireless mesh: 1-1-1 deployment 913
Wireless mesh: 1-2 deployment 915
Wireless and wired mixed mesh 1-2 deployment 916
Setting up the Home Mesh Router—Wired Mesh Mode **917**
Wired mesh: 1-1 deployment 918
Wired mesh: 1-1-1 deployment 918
Wired mesh: 1-2 deployment 919
Viewing router system information and network traffic status **920**
Viewing, editing, and blocking connected clients **922**
Viewing connected clients 922
Editing a client's host name 923
Blocking clients 923
Monitoring and troubleshooting the Home Mesh Router **923**

Monitoring the Home Mesh Router **924**
Home Site Dashboard 924
Notifications 925
Alarms 925
Alarms History 925
Events 926
Wi-Fi Events 927
Software Update 927
Performance 928
Troubleshooting the Home Mesh Router **930**
Status 930
Downloading tech support file 931
Debug 931
Network Connectivity 931
Wi-Fi Analyzer 932
Speed Test 933
Packet Capture 935
Upgrading the Home Mesh Router firmware **936**
Assurance X ***938***
Analyzing Connection Failures of Wi-Fi Clients and Poor Performance of Wi-Fi Networks **938**
Overview **939**
Use cases **942**
Resolve connectivity issues 942
Address poor performance of applications 942
Identify OS, SSID, and AP-specific issues 943
Accessing the Assurance X page **943**
Accessing Site-level consolidated details at the System- and MSP-levels **946**
Setting filters to view the connection data **947**
Suppressed clients 949
Classifying clients as suppressed 949
Viewing suppressed clients and events 950
Removing a manually suppressed client from the Suppressed Clients list 952
Viewing the connection events **952**
Dashboard page 953
Assurance X page 954
Connection tab 954

Disconnection tab 960
Viewing hourly data and corresponding events 964
Viewing a client or host-specific connection or disconnection event 966
Viewing an event-based connection or disconnection event 972
Viewing AP-specific information 974
System-level Assurance **976**
Managed Services ***977***
Managed Accounts **977**
Overview **977**
Managed Accounts 977
Accounts 978
Access Points 978
Managed Account Service 978
Account UI 979
Account Service Users (Administrators) 980
Account Service Users (Administrators) Roles 980
Configuring Managed Account Services **981**
Enable Managed Accounts 981
Additions in the cnMaestro UI when Managed Accounts is Enabled 982
Creating Managed Account Services 983
Creating Account 985
Validating Account Users 986
Check Email for Invite 987
Create Account in Account Service 988
Login to the Accounts UI 988
Managed Account Administration **989**
Overview 989
Important Points to Remember 989
System View 990
Account View 990
Account Administrator (User) View 991
Users View 991
System Dashboard 992
Account Administration 992
Device Management 993
System Onboarding 993

Device Onboarding ... 993
Moving a Device Between Accounts ... 993
Account Deletion ... 994
Disabling the Managed Accounts feature ... 995
Managing subscribers (end-customer) ... **995**
Adding a Subscriber Service Profile ... 995
Adding a subscriber ... 997
Modifying the owner details for the Subscriber App ... 1001
Claiming the Home Mesh Router ... 1002
Network Services ... ***1004***
API Client ... **1005**
Overview ... **1005**
API Clients ... **1005**
RESTful API Specification ... **1007**
Authentication ... 1007
Establish a Session ... 1007
API Access ... 1008
Session Expiration ... 1008
Rate Limiter ... 1008
Swagger API ... **1011**
Introduction ... 1011
API Session ... **1012**
Introduction ... 1012
Retrieve Access Token ... 1012
Access Resources ... 1014
API Details ... **1014**
HTTP Protocol ... 1014
HTTP Response codes ... 1014
HTTP Response codes ... 1014
REST Protocol ... 1015
Resource URLs ... 1015
Responses ... 1016
Parameters ... 1017
Field selection ... 1017
Filtering ... 1018
Time Filtering ... 1019

Sorting 1019
Pagination 1020
Internal Response limits 1020
Access API **1021**
Token (basic request) 1021
Request 1021
Response 1022
Example 1022
Token (alternate request) 1022
Request 1022
Response 1023
Example 1023
Validate Token 1023
Request 1023
Response 1023
Example 1024
API Changes **1024**
Sunsetted APIs/Fields 1024
Deprecated APIs/Fields 1024
Devices, Statistics, and Performance APIs **1025**
Overview 1025
cnMaestro v2 API 1025
Devices API Response (v2 Format) 1026
Supported values for onboarding state 1028
Supported values for device type 1029
Device onboarding failure error codes 1029
Statistics API Response (v2 Format) 1030
60 GHz cnWave 1030
cnMatrix 1031
cnReach 1032
Fixed Wireless (cnVision, ePMP and PMP) 1033
PTP 650/670/700 1036
PTP 820/850 1037
Wi-Fi 1038
cnWave 5G Fixed 1040
Performance API Response (v2 Format) **1043**
60 GHz cnWave 1044

cnMatrix 1044
cnReach 1045
Fixed Wireless (cnVision, ePMP and PMP) 1046
PTP 650/670/700 1047
PTP 820/850 1049
Wi-Fi 1050
cnWave 5G Fixed 1050
Client API Response (v2 Format) 1051
External Guest Access Login API 1052
60 GHz cnWave RESTful API 1054
E2E Network 1054
Device (Node) Configuration 1056
E2E Controller 1057
EasyPass 1058
Guest/Public Access 1059
Employee/Student Access 1060
Combined 1060
Implementation of EasyPass portals for various types of users 1061
EasyPass configuration 1062
Creating a portal 1063
Configuring common parameters 1067
The Basic screen parameters 1067
The Limits screen parameters 1068
The Design screen parameters 1070
The Voucher screen parameters 1076
The One Click screen parameters 1077
The Plans screen parameters 1079
Accessing the common tabs 1084
Sessions 1084
Guests 1085
Vouchers 1086
Paid Transactions X 1087
Users X 1088
Creating One Click portal 1088
Creating Self Registration X portal 1088
SMS Gateway Providers 1090
Creating Sponsored Guest X portal 1097

Creating Voucher portal 1098
Creating Paid X portal 1099
Creating WiFi4EU portal 1099
Creating Microsoft Entra ID X portal 1100
Creating Google Login X portal 1102
Creating Onboarding X portal 1103
Adding a new user 1107
Importing user data using a CSV file 1108
Creating One Click + Voucher portal 1110
Creating One Click + Paid X portal 1110
Creating Voucher + Paid X portal 1111
Creating a Third-Party Integration portal 1111
Creating a portal and secret key 1112
Revoking and generating the secret key 1113
Using the Secret Key in API Requests 1113
Creating a Hospitality PMS Beta portal 1113
MarketApps X 1115
Overview 1116
Target audience 1116
Benefits 1117
Prerequisites 1117
Key features 1117
Adding a new MarketApps App 1118
MDU Managed Wi-Fi app 1119
Basic tab 1119
Settings tab 1119
Wi-Fi Management 1120
Site Monitoring 1123
Users & Other Settings 1124
Design tab 1124
MDU Self-Service Personal Wi-Fi app 1126
Basic tab 1126
Personal Wi-Fi configuration 1126
Outdoor Hospitality Managed Wi-Fi app 1127
Basic tab 1128
Settings tab 1128
Design tab 1129

Units tab 1129
Senior Living Managed Wi-Fi app 1130
Basic tab 1130
Settings tab 1130
Design tab 1131
Units tab 1132
Configuring units by property managers / front desk staff / Wi-Fi support staff 1132
Managing units in the MDU Managed Wi-Fi app 1133
Managing units in the Self-Service Personal Wi-Fi App 1133
Adding units in cnMaestro Cloud 1136
Replacing all units in cnMaestro Cloud 1140
Managing units in the Wi-Fi Manager / Wi-Fi Support / Wi-Fi Front Desk Apps 1141
Signing in to the Wi-Fi Manager / Wi-Fi Support / Wi-Fi Front Desk Apps 1142
Assigning units in the Wi-Fi Manager App 1148
Assigning residents in bulk 1153
Settings 1154
Theme settings 1155
Help 1155
AP Health 1155
MarketApps app selector 1157
View options in the Property Manager App 1157
View options in the Resident App 1159
Monitoring Sites in the Wi-Fi Manager / Wi-Fi Support / Wi-Fi Front Desk Apps 1167
Installer app 1168
Basic tab 1169
Settings tab 1169
Enterprise Installer 1169
60 GHz cnWave Installer 1171
Design tab 1172
Nodes tab 1174
Accessing the Installer App interface 1175
Additional options on the summary page 1179
Viewing installed devices and switching between apps 1180
Locating installed devices in cnMaestro 1180
Replacing devices in the Installer app 1180
Searching, updating, and replacing existing device in the Installer App 1183
Exporting Installation Summary information 1186

Citizens Broadband Radio Service (CBRS) **1186**
Enabling CBRS in Cloud 1186
Management Tool **1192**
Export 1192
Relinquish Grant 1192
Creating a Management Tool Sector 1193
Domain Proxy View **1211**
Searching a Domain Proxy Sector 1212
Domain Proxy Sector view 1212
Searching a Domain Proxy in Non Sector View 1212
Actions for Existing CBRS On-Premises Users **1215**
Link an Anchor Account to this Account 1216
Convert this Account to Anchor Account 1217
Organizations for CBRS **1218**
Create an Organization **1219**
Primary Account 1219
Secondary Account 1221
Additional service requests from the Secondary Account 1222
Removing Accounts **1223**
Remove through Primary Account 1223
Remove Organization from Secondary Account 1225
Disable Secondary Account services **1226**
With no active services 1226
With active shared SAS ID services 1227
With active Unified Payments 1229
Edit Services **1230**
Enable services in the Primary Account 1230
Request services from Secondary Account 1231
Review service request in Primary Account 1232
Share CBRS Configuration with the On-Premises Instance **1234**
Organization History **1235**
LTE **1235**
Adding SIM Cards **1236**
Delete SIM Cards 1236
Update SIM Details 1236
Viewing BBU SIM Status 1237
Managing Edge Controller **1238**

Topology Sync 1238
Edit 1238
Delete 1239
Dashboard **1240**
Configuration **1240**
Rules 1241
Import 1242
Export 1243
Delete 1243
Edit 1243
Blacklist 1244
Advanced Settings 1244
Tools **1245**
Diagnostics 1245
Technical Support Dump 1245
Logging Severity 1246
Service Logs 1247
Operations 1248
Services 1248
Monitoring 1249
Installation Summary **1249**
Configuration **1252**
Photos and Location **1252**
Link Test Result **1252**
AP Scan Result **1252**
Spectrum Analyzer X **1253**
Administration ***1259***
Users **1259**
Managing Users **1259**
Role-Based Access 1260
Role-Mappings 1260
Creating Users and Configuring User Roles 1265
Whitelisting specific domains 1266
Assigning roles for IdP-based domain users **1267**
Advantages 1268
Prerequisite tasks 1268

Assigning roles for IdP-based domain users ... 1268
Session Management ... **1269**
Sessions ... 1269
Cloud Anchor Account ... **1269**
Manage Instances ... **1270**
Onboarding ... 1270
On-Premises Instances ... 1272
Notifications ... 1272
Inventory ... **1273**
Administration ... **1273**
Users ... 1274
Role-Based Access ... 1274
Creating Users and Configuring User Roles ... 1274
Session Management ... 1275
Network Services ... **1275**
CBRS ... 1275
Organization ... 1275
Manage Subscriptions ... **1275**
Subscriptions ... 1276
Devices ... 1277
Webhooks X ... **1277**
Configuring Webhooks template ... **1278**
Supported variables ... 1280
Error and retransmission ... 1282
Notifications ... **1282**
Adding a notification ... 1283
HTML email example ... 1286
JSON email example ... 1287
Supported source types ... 1287
Audit Logs ... **1288**
Updating Company Information ... **1290**
Updating information through the Company Information page ... 1293
Appendix ... ***1295***
Guest Access ... **1295**
Configuration ... **1296**
Creating the Guest Access Portal in cnMaestro ... 1296

Basic Details 1296
Access Portal 1296
Design Page 1312
Guests 1317
Mapping the device to Guest Access Portal in cnMaestro 1318
Configuration at device level 1318
Configuration at cnMaestro side 1319
Access Types 1320
Guest Access using Social Login 1321
Configuration 1321
API Key Generation 1323
Sample Template 1331
Guest Access Portal Logout 1332
SMS Authentication 1333
Generic SMS Gateway configuration 1333
Sample configuration in the cnMaestro 1340
Network Port Requirements 1340
Network Port Requirements for Outbound Access 1340
XMS-Enterprise to cnMaestro X 1341
XMS-E System 1341
Export Golden Configuration 1342
Migrate to cnMaestro X 1345
Create Wi-Fi AP Group 1346
Approve APs into Wi-Fi AP Group 1348
Import and Apply AP configuration 1349
Converting Tier 2 Unused Slots 1351
Cambium Networks 1354

Introduction

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

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

This section covers the following topics:

- Supported Devices and Features
- Quick Start
- Creating a Cloud Account
- cnMaestro X
- cnMaestro X features behavior state
- UI Navigation
- Device Onboarding
- Deleting Devices in Bulk
- Export All as CSV

Supported Devices and Features

Devices and minimum software versions

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

Table 1 *Supported devices and minimum software versions*

Device	Minimum Software Version
60 GHz cnWave V1000	1.1
60 GHz cnWave V2000	1.2.2
60 GHz cnWave V2000i	1.8
60 GHz cnWave V3000	1.1
60 GHz cnWave V5000	1.1
60 GHz cnWave V5000i	1.8
cnMatrix (All series except the below two switches)	5.0.2-r4
cnMatrix EX3030RM-P	6.2

Table 1 *Supported devices and minimum software versions*

Device	Minimum Software Version
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
ePMP 1000	4.5.0
ePMP 2000	4.5.0
ePMP 3000	4.5.0
ePMP 3000L	4.5.0
ePMP 4600	5.4.0
ePMP 4600L	5.4.0
ePMP Elevate	3.2
ePMP Elevate SXGLIT5/LHG5	4.5.0
ePMP Elevate XM/XW	4.5.0
ePMP Force 130 2.4 GHz	4.5.0
ePMP Force 130 5 GHz	4.5.0
ePMP Force 180/200	4.5.0
ePMP Force 190	4.5.0
ePMP Force 200L	4.7.0
ePMP Force 300	4.5.0
ePMP Force 300-13	4.5.0
ePMP Force 300-13L	4.5.0
ePMP Force 300-13LC	4.5.0

Table 1 *Supported devices and minimum software versions*

Device	Minimum Software Version
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
NSE3000	1.0
NSE4000	2.0
PMP 450i	22.1.2
PMP 450 MicroPoP Omni	22.1.2
PMP 450 MicroPoP Sector	22.1.2
PMP 450b Retro	22.1.2
PMP 450v	23.0
PON (OLT and ONU)	1.1.0
PTP 650	01-50
PTP 670 (650 Emulation)	01-50, 03-12
PTP 670, PTP 700	03-11
PTP 820, PTP 850	11.9
XV3-8	6.6.0.3
XV2-2	6.6.0.3
XV2-2T0	6.6.0.3
XV2-2T1	6.6.0.3
XV2-22H	6.6.0.3
XV2-21X	6.6.0.3
XV2-23T	6.6.0.3
XE3-4	6.6.0.3
XE3-4TN	6.6.0.3
XE5-8	6.6.0.3
X7-35X	7.0
X7-53X	7.1.1

Table 1 *Supported devices and minimum software versions*

Device	Minimum Software Version
X7-55X	7.1.1
X7-56X	7.1.2
RV22 Home Mesh Router	1.0.0

Table 2 *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
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 3 *Supported browsers*

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

Network connectivity

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

cnMaestro features

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



Note

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

Table 4 *Features supported by cnMaestro*

Feature	Description	Cloud	On-Premises
Account Recovery	Ability to resolve password and account recovery issues locally.		✔
Advanced Troubleshooting	Display tower-to-edge status in a single graphic, which is used to: • View Wi-Fi client details and health. • Troubleshoot client connectivity directly on the AP.	✔	✔
Access Control Policies	Configure policies that define who can connect to the network, and when they are allowed to connect and access a specific device.	✔	✔
Automated Frequency Coordination (AFC) X	Manage and allocate radio frequencies efficiently for a specific region or country.	✔	
Assurance X	View the health of Wi-Fi client connections, including root cause analysis of failures and possible remediations.	✔	
AP Group Configuration	Support configuration of Enterprise Wi-Fi and cnPilot Home devices.	✔	✔
AP Group Dashboard	Display aggregate Wi-Fi AP statistics for the configured AP Group.	✔	✔
API Client X	Create API clients and access tokens to programmatically manage deployments using customer's own client applications.	✔	✔
Applications X	View details of applications accessed by users in a particular site.	✔	✔
Auto-Provisioning X	New devices, such as cnPilot Home (R-Series), cnVision, Enterprise Wi-Fi, Enterprise Wi-Fi (Xirrus-Series), ePMP, and PMP,	✔	✔

Table 4 *Features supported by cnMaestro*

Feature	Description	Cloud	On-Premises
	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 the 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)	✓	✓

Table 4 *Features supported by cnMaestro*

Feature	Description	Cloud	On-Premises
	• 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 • WiFi4EU—Available only in the European Union • Third-Party Integration	✔	✔
EasyPass—Microsoft Azure, Google Login	Create captive portal to allow clients to access the network through the following portals: • Microsoft Azure X	✔	

Table 4 *Features supported by cnMaestro*

Feature	Description	Cloud	On-Premises
	• Google Login X • Onboarding X		
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.	✔	✔
Home Mesh Routers	Onboard and manage Home Mesh Routers (RV22).	✔	
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.	✔	✔

Table 4 *Features supported by cnMaestro*

Feature	Description	Cloud	On-Premises
	• Wi-Fi APs, IIoT, and cnMatrix up to 1 year.		
LTE	Manage cnRanger LTE devices.	✓	✓
Managed Services X	Allow cnMaestro account owners to split their installation into separate Managed Accounts. Each Managed Account contains independent administration and configuration.	✓	✓
Maps and Map Modes—Street View	Leverage maps to position devices and visualize their health and connectivity. Change the map mode to display various wireless key performance indicators.	✓	✓
Maps and Map Modes—Satellite and Terrain X		✓	✓
MarketApps X	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 • Enterprise Wi-Fi (Xirrus-Series) • ePMP • NSE • PMP • PON	✓	✓

Table 4 *Features supported by cnMaestro*

Feature	Description	Cloud	On-Premises
	• PTP 650/670/700 • PTP 820/850 • RV22 Home Mesh **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 • Enterprise Wi-Fi (Xirrus-Series) • NSE		
Multi-Floor Plans	Multiple floor plans for Sites.	✔	✔
Notifications	Communicate immediate status with stateful alarms and events. Notifications help troubleshoot customer issues.	✔	✔
Node Throughput Test X	Test the throughput between a node and PoP. Using this option, you can conduct a throughput test for each hop seamlessly. Applicable only to 60 GHz cnWave devices.	✔	✔
NSE	Onboard and Manage Network Service Edge (NSE) devices.	✔	
Onboarding	In the Cloud version, devices onboard using either the device Manufacturer Serial Number (MSN) or through the Cambium ID or Onboarding Key (entered on the device). In the cnMaestro On-Premises version, all the cloud modes of onboarding or devices contacting cnMaestro are added to the Onboarding Queue, where they are approved and managed.	✔	✔
On-Premises Console	Configure networking parameters and update the system password using the CLI available through the virtual machine console.		✔
Organization X	Allow users to manage multiple accounts through a single CBRS payment subscription.	✔	✔
PON (OLT/ONU)	Onboard and manage Passive Optical Network (PON) devices, including Optical Line Terminal (OLT) and Optical Network Unit (ONU).	✔	✔
RADIUS Proxy	Proxy RADIUS packets are sent through cnMaestro (On-Premises) instead of directly to the RADIUS server from the AP.		✔
Reports X (Data, Graphical, and Graphical Report Template)	• Export Active Alarms, Alarm History, Audit Logs, Devices, Events, Guest Access Login Events, Performance, Wi-Fi Events, and Wireless Clients data in CSV format. • Generate various data in graphical format and export the details in a PDF file.	✔	✔
RESTful API X	Support HTTPS RESTful API for inventory, monitoring, performance, notification, and basic provisioning.	✔	✔

Table 4 *Features supported by cnMaestro*

Feature	Description	Cloud	On-Premises
Role-Based Access	Assign the following roles to users: • Super Administrator • Administrator • Operator • Monitor • CPI	✔	✔
Scheduled Configuration Update	Specify a time to configure devices.	✔	✔
Scheduled Software Update	Specify a time to install device software.		✔
cnMaestro Software Upgrade	Enable three types of software upgrade: • **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	Track current cnMaestro users and support forced logoff.	✔	✔

Table 4 *Features supported by cnMaestro*

Feature	Description	Cloud	On-Premises
Management X			
Webhooks X	Send alarm notifications to the external servers.	✓	✓
Wi-Fi Speed Test	Test the speed between the Wi-Fi APs and cnMaestro.		✓
WLANs Dashboard X	View details of all WLANs that are applied on devices at a given site. Also view the details of APs connected to these WLANs.	✓	✓
Zero Touch Onboarding	Allow cnVision Client, PMP SMs, and ePMP SMs to automatically appear in the onboarding queue if the parent AP is already onboarded.	✓	✓

Quick Start

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

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

- **For account management:**
  1. Create a Cambium Support Center login (if you do not have one already).
  2. Create a cnMaestro account.
  3. Login to cnMaestro.
- **For claiming devices:**
  1. Claim devices using a Manufacturer Serial Number (MSN).
  2. Claim devices using a Cambium ID.

Create and manage accounts

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

Create a Cambium Support Center login

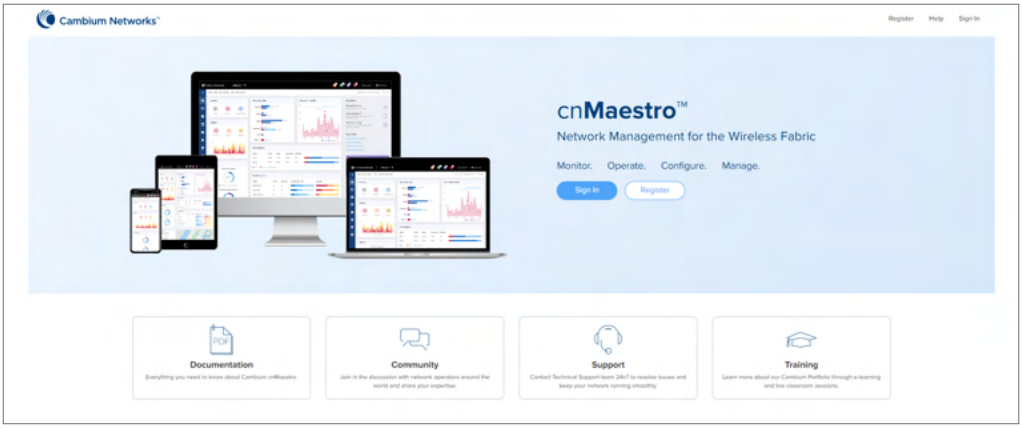
cnMaestro uses an existing Cambium Support Center account. If you do not have an account, you must create one.

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

1. Open a web browser and enter https://cloud.cambiumnetworks.com into the address bar.

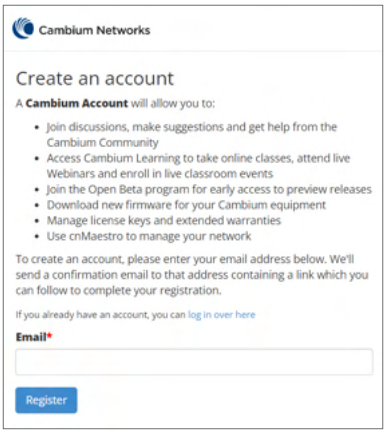
   The cnMaestro Main login page appears, as shown in Figure 1.
2. Click **Register**.

Figure 1 *The main login page*



A registration form appears, as shown in Figure 2.

Figure 2 *Initial registration form*

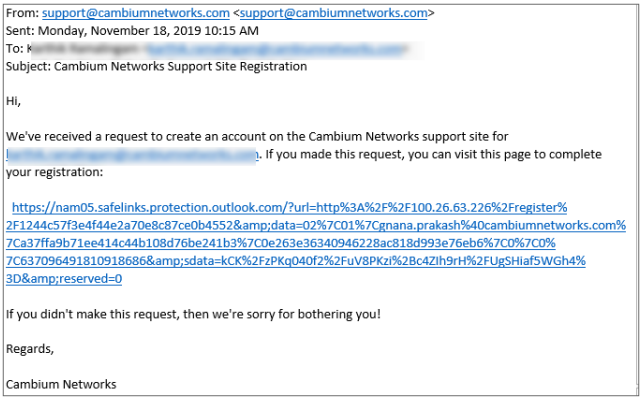


3. Enter your email address and click the **Register** button.

   An email from Cambium Support Center is sent with a link for validation.

4. Check email and click the validation link, as shown in Figure 3.

Figure 3 *Email from Cambium Support to validate account*



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

Hi,

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

https://nam05.safelinks.protection.outlook.com/?url=http%3A%2F%2F100.26.63.226%2Fregister%2F1244c57f3e4f44e2a70e8c87ce0b4552&data=02%7C01%7Cgnana.prakash%40cambiumnetworks.com%7Ca37ffa9b71ee414c44b108d76be241b3%7C0e263e36340946228ac818d993e76eb6%7C0%7C0%7C637096491810918686&sdata=kCK%2FzPKq040f2%2FuV8PKzi%2Bc4ZIh9rH%2FUgSHiaf5WGh4%3D&reserved=0

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

Regards,

Cambium Networks

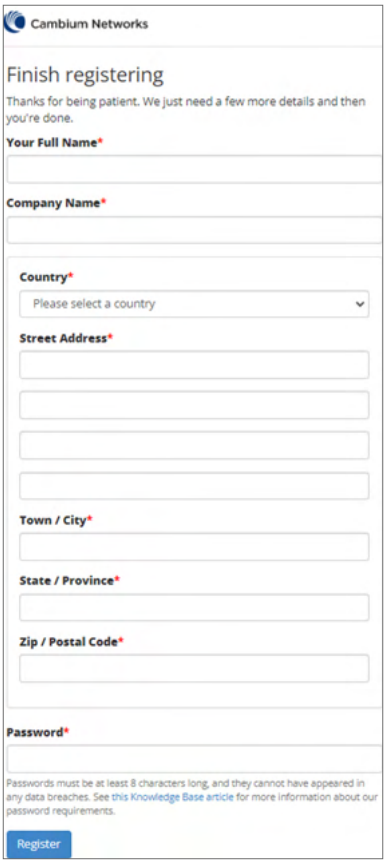


Note

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

The **Finish registering** form appears, as shown in Figure 4.

Figure 4 *Finish registering form*



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

Create a cnMaestro account

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

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

   The **Create a New Cloud Account** window appears, as shown in Figure 5.

Figure 5 *Creating a new Cloud account*

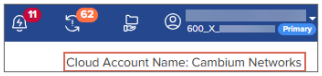


3. Enter the required details as described below:

Table 5 *NMS Cloud management fields*

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

Table 5 *NMS Cloud management fields*

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

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

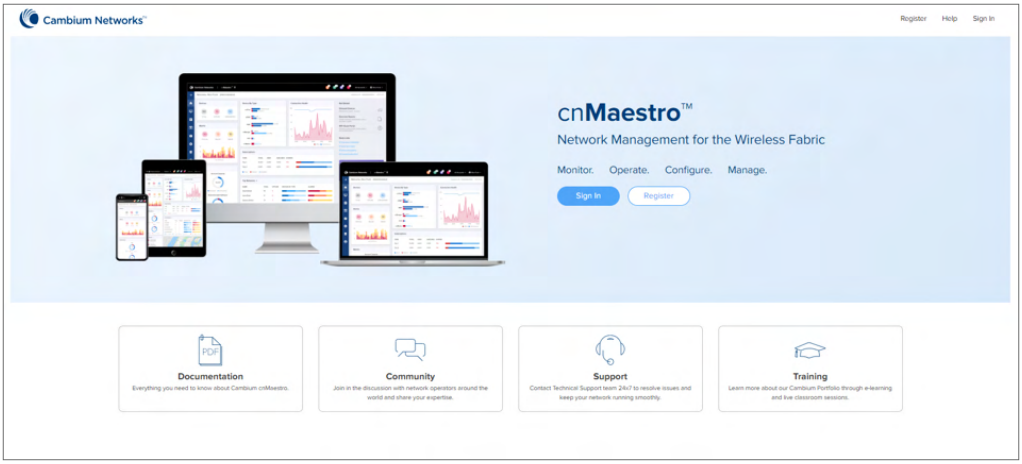
Log on to cnMaestro

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

1. Open a web browser and enter https://cloud.cambiumnetworks.com into the address bar.

   The cnMaestro Main login page appears, as shown in Figure 6.

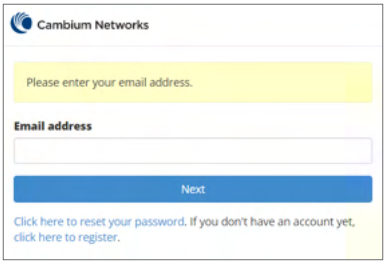
   Figure 6 *Main login page*

2. Click **Sign In**.

   Please enter your email address page appears as shown in Figure 7.

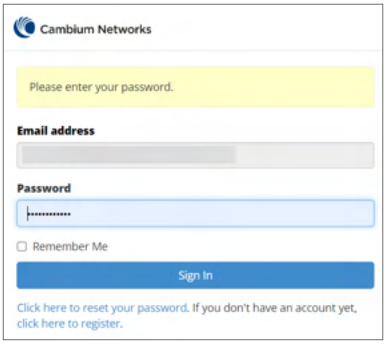
Figure 7 *Email address page*



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

   Please enter your password page appears as shown in Figure 8.

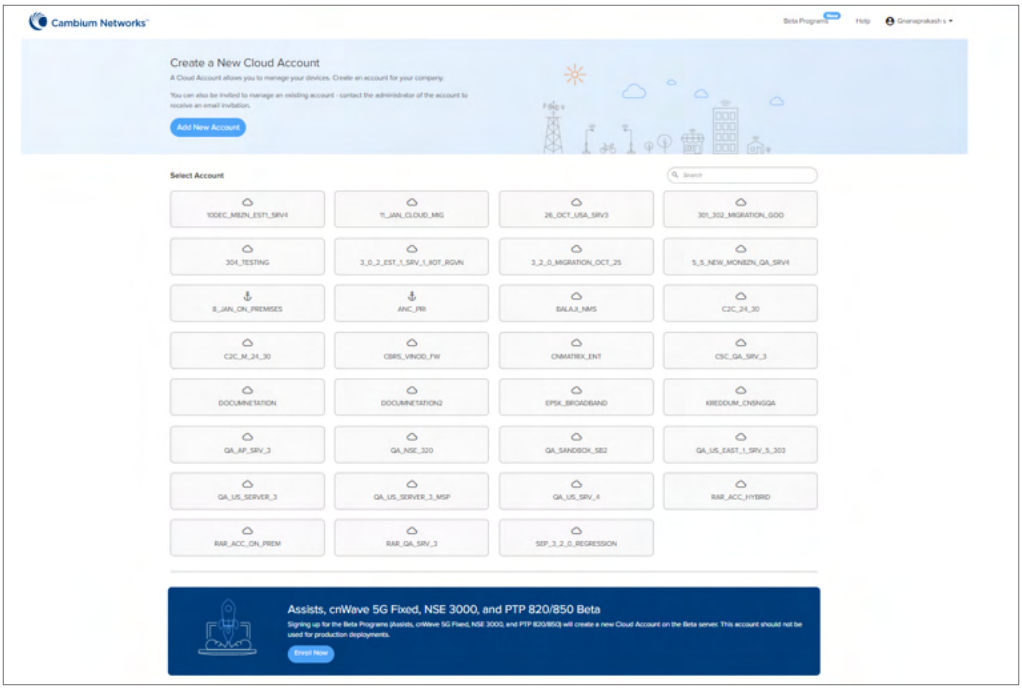
Figure 8 *Password page*



5. Click **Sign in**.

   Select Account page appears as shown in Figure 9.

Figure 9 *Select account page*

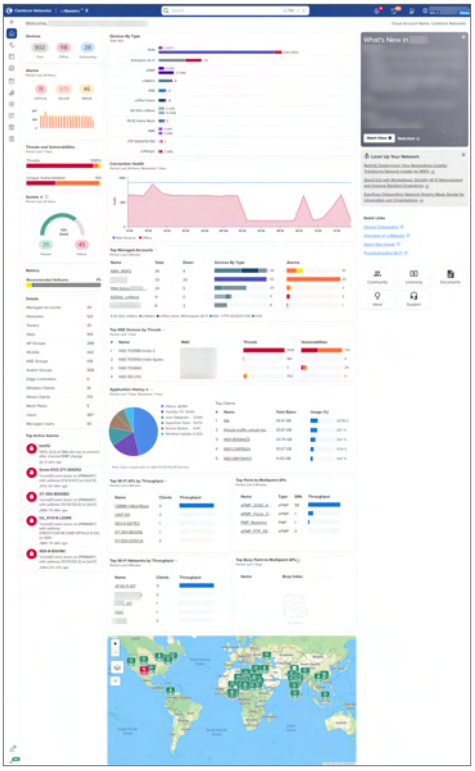


In **Select Account** page you can use search option to search the account.

6. Click the selected account.

   The cnMaestro **Home** page appears, as shown in Figure 10.

   Figure 10 *cnMaestro Home page*



Claim and onboard devices

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

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

Claim devices by serial number

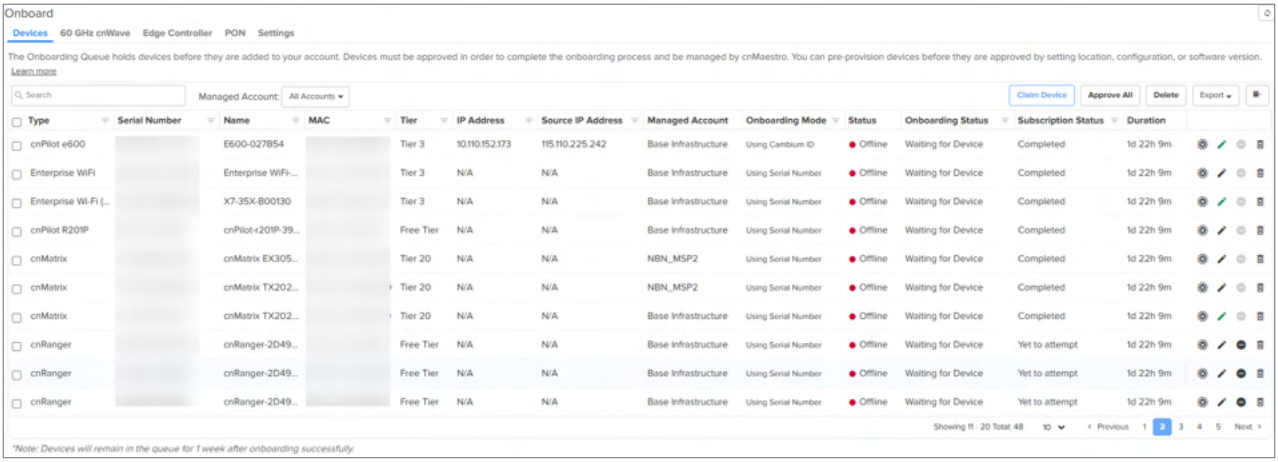
You can claim a device by using the Manufacturer Serial Number (MSN). The system prompts the user to validate the devices before applying them. After being claimed, devices are placed into the Onboarding Queue, where they can be pre-provisioned to update software or configuration before onboarding.

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

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

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

Figure 11 *Onboard page*



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

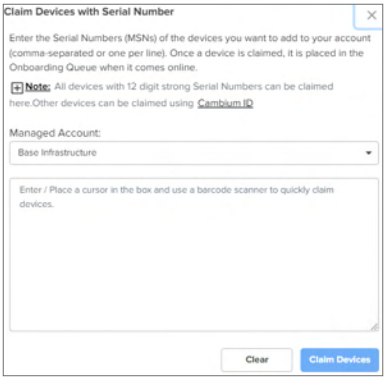
   The **Claim Devices with Serial Number** page appears, as shown in Figure 12.

3. Enter the Serial Number(s) of the device(s) in the text box, as shown in Figure 12.

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

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

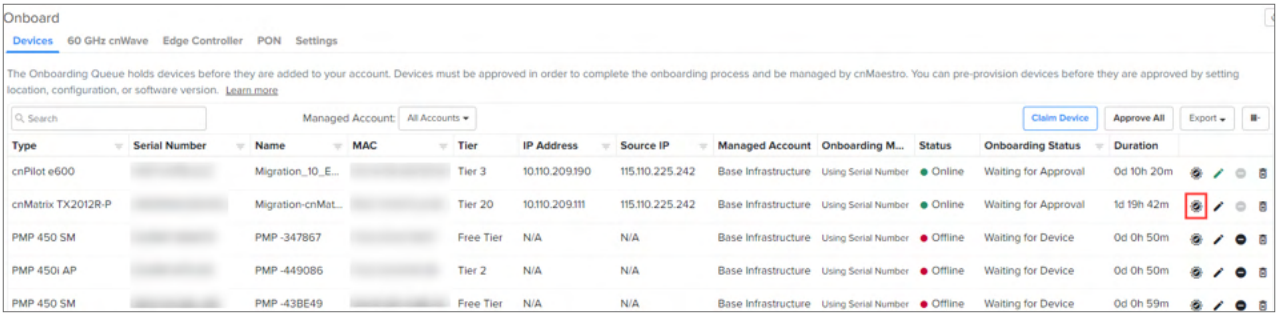
Figure 12 *Claim Devices with Serial Number page*



4. Click **Claim Devices.**

5. To onboard the device when it contacts cnMaestro, click the **Approve Device** ( ) icon or **Approve All** at the right side of the Onboard page, as shown in Figure 13.

Figure 13 *Onboarding Queue*



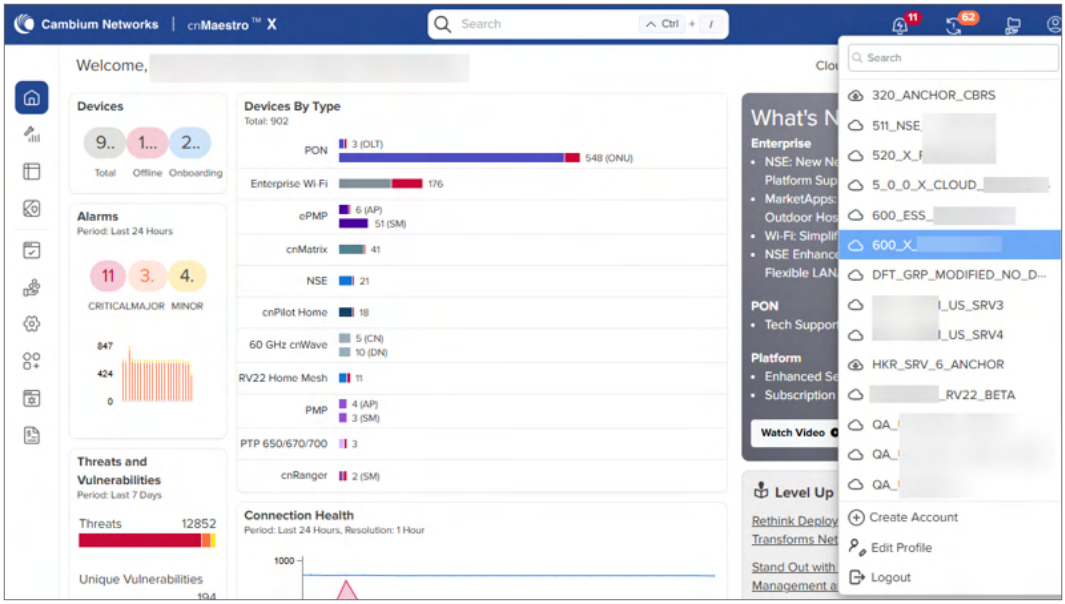
Note

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

Claim devices by Cambium ID

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

Figure 14 *Cambium ID*



A Cambium ID with an Onboarding Key is:

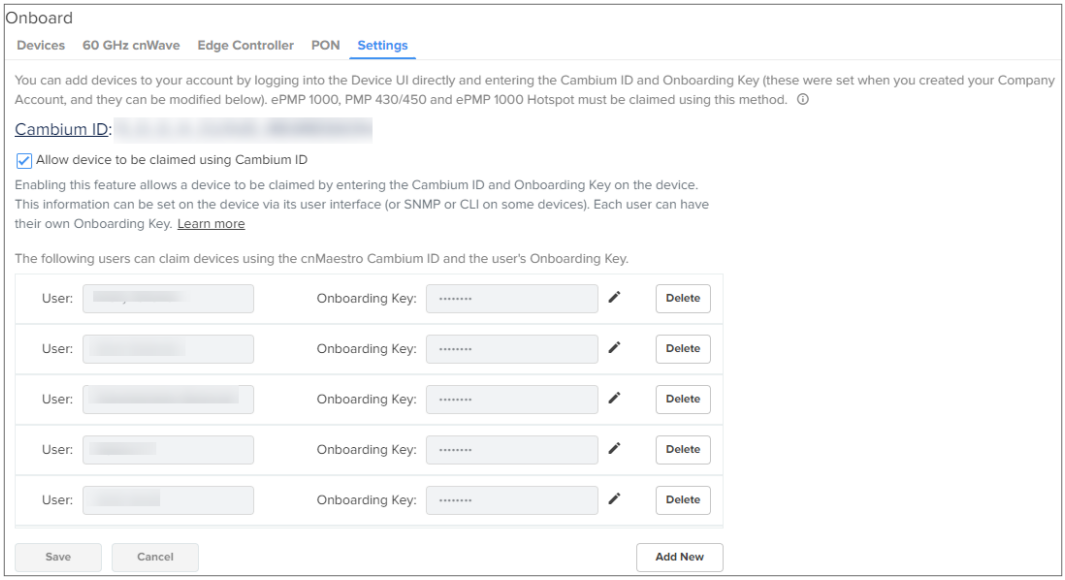
- Required to claim legacy devices that do not have a 12-character serial number (these devices are usually 5+ years old).
- Optional for devices that have 12-character serial numbers (though generally not used).

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

Cambium ID configuration

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

Figure 15 *Cambium ID configuration*



Onboarding Key configuration

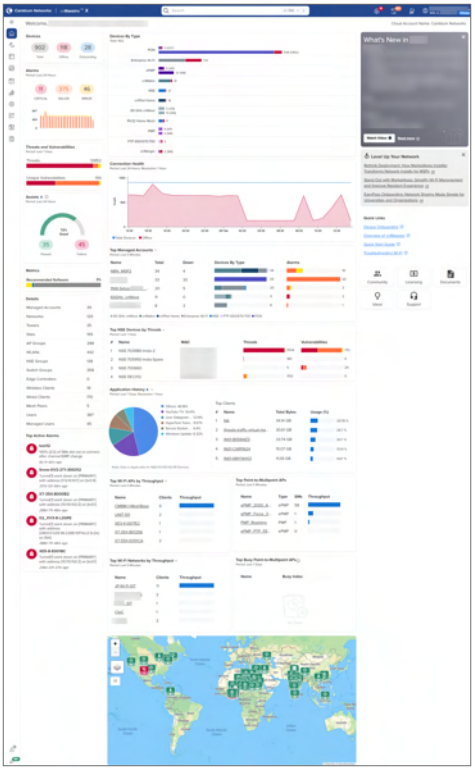
Each Onboarding Key is mapped to an individual User account. This mapping allows Cambium Cloud to know who is onboarding a device, and the key can be revoked if needed.

To configure the Onboarding Key, perform the following steps:

1. Log on to your cnMaestro account.

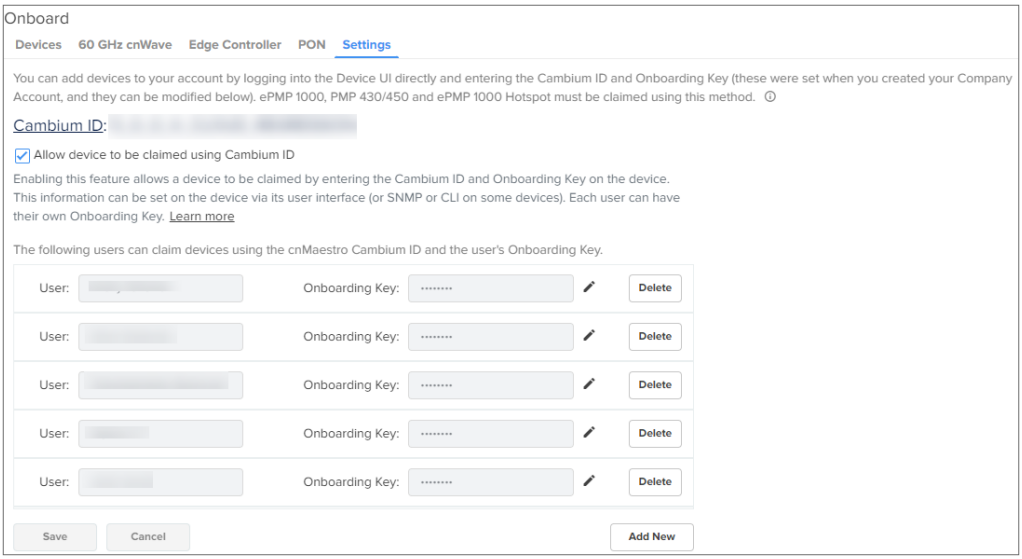
   The Home page appears, as shown in Figure 16.

Figure 16 *Home page*



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

Figure 17 *Onboard settings page*



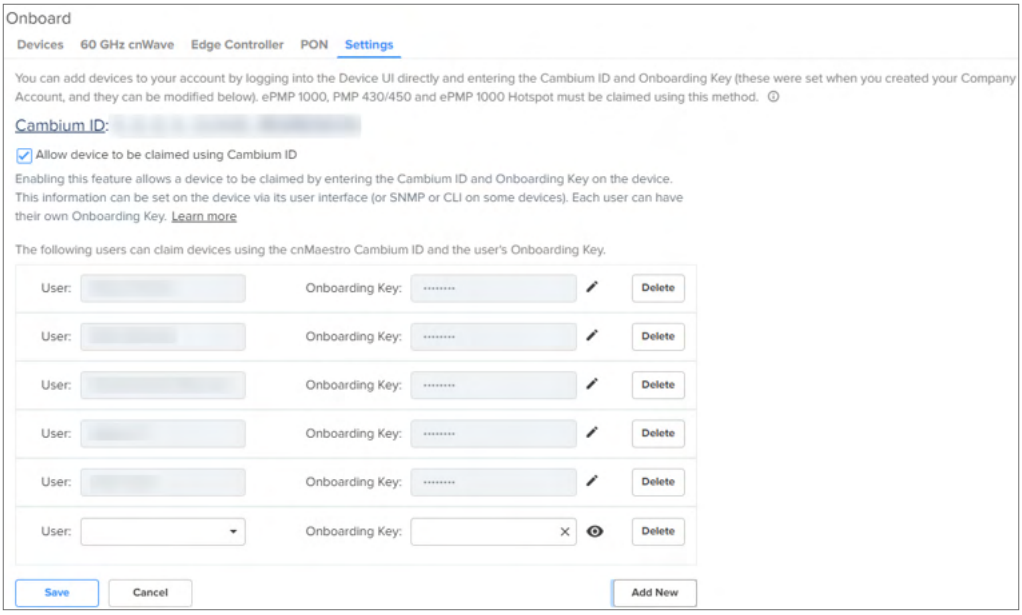
3. Select the **Allow device to be claimed using Cambium ID** checkbox**.**

   Enabling this feature allows one to add Onboarding Keys mapped to individual Users.

4. Click **Add New** to add a User and Onboarding Key.

   A new row appears as shown in Figure 18.

Figure 18 *New onboarding key*



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

Onboard device using Onboarding Key

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

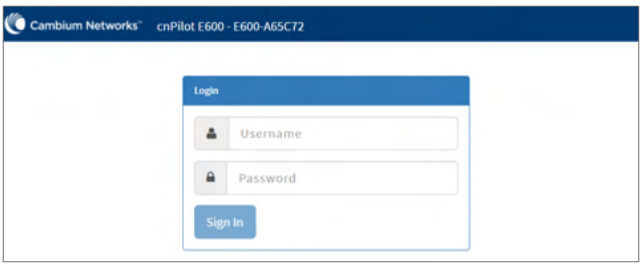
Device UI

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

1. Log on to the Device UI.

   The **Sign In** page appears, as shown in Figure 19.

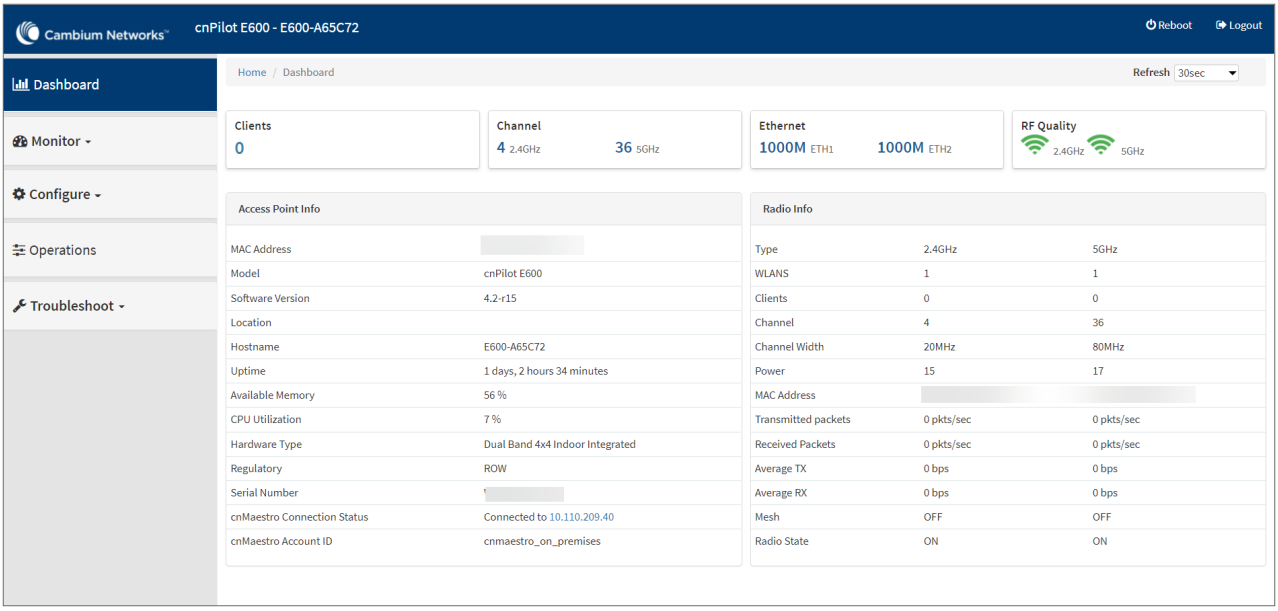
   Figure 19 *Login page*



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

   The device home page appears, as shown in Figure 20.

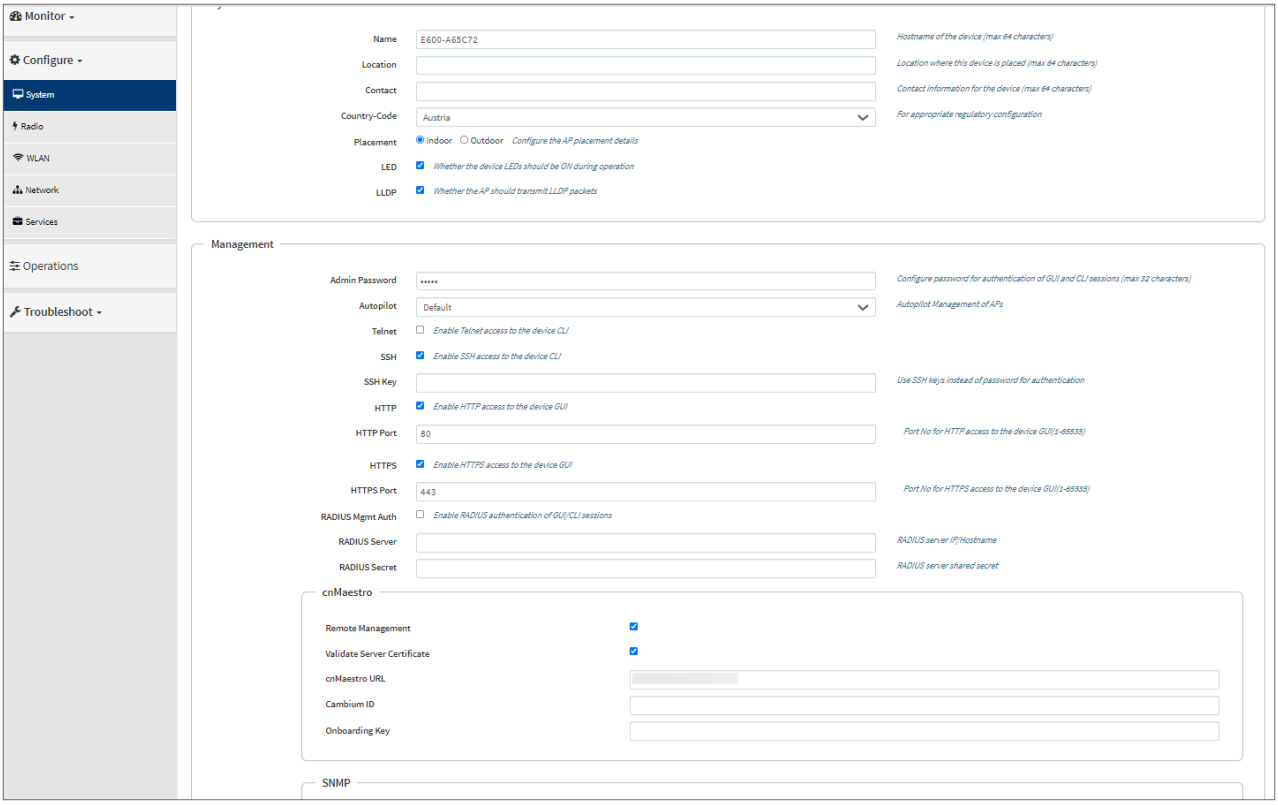
Figure 20 *Device home page*



4. From the Home page, navigate to **Configure > System > Management.**

   System configuration page appears, as shown in Figure 21.

Figure 21 *cnMaestro configuration*

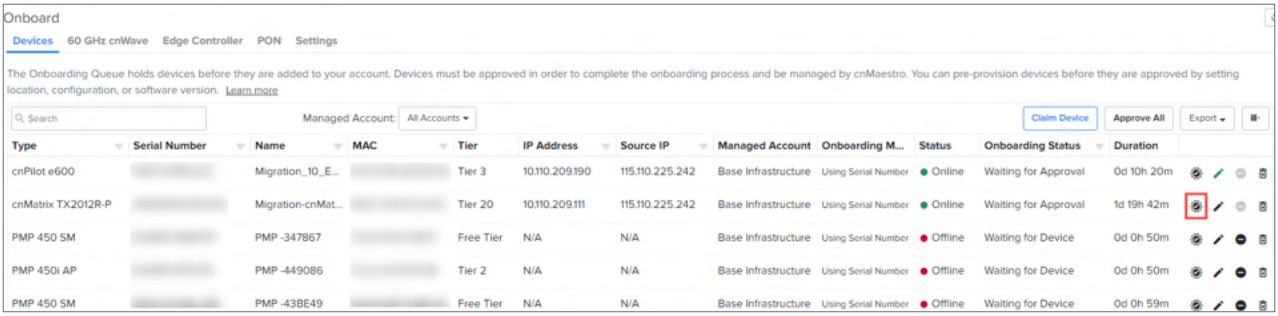


5. Enter URL in **cnMaestro URL** to connect the server (by default it will be cloud.cambiumnetworks.com), as shown in Figure 21.
6. Enter the **Cambium ID**.

7. Enter the **Onboarding Key.**
8. Click **Save.**

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

Figure 22 *Device approval*



Creating a Cloud Account

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

- Overview
- Creating a Support Center User ID
- Creating a Cloud NMS Account
- Creating an Anchor Account
- Multiple Cloud Accounts

Overview

There are two types of accounts for cnMaestro cloud management.

Table 6 *Account types*

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

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

Creating a Support Center User ID

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

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

Creating a Cloud NMS Account

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

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

Figure 23 *Create Cloud NMS account*



The required fields are defined below:

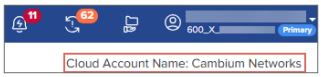
Table 7 *NMS Cloud management fields*

Parameter	Description
Cambium ID	The **Cambium ID** identifies this account externally. Supported characters—alphabets, integers, and underscore only. Once created, it can only be changed by contacting Cambium Support.
Country	Determines where the devices in this account are located.

Table 7 *NMS Cloud management fields*

Parameter	Description
	Cambium has data centers in North America, Europe, and Asia. If your devices are located in more than one region, you must create a separate account for a country in each region.
Time Zone	Specifies the time zone used to calculate device statistics. Daily statistics are collected at 12 AM in the configured time zone.
Account Type	Specifies the type of cnMaestro account you want to use to manage devices. Following options are supported: • **NMS**—Manage devices through cnMaestro Cloud • **Anchor**—Manage devices locally on your own data center through cnMaestro On-Premises
Account View	Specifies the cnMaestro account view based on the devices you intend to manage. • **Access and Backhaul**— ◦ 60 GHz cnWave ◦ cnMatrix ◦ cnPilot Home (cnPilot R-Series) ◦ RV22 Home Mesh ◦ cnRanger ◦ cnReach ◦ cnVision ◦ cnWave 5G Fixed ◦ Enterprise Wi-Fi (E-Series and XE/XV/X7-Series) and cnPilot Enterprise (ePMP 1000 Hotspot) ◦ Enterprise Wi-Fi (Xirrus-Series) ◦ ePMP ◦ NSE ◦ PMP ◦ PON ◦ PTP 650/670/700 ◦ PTP 820/850 • **Enterprise**— ◦ cnMatrix ◦ Enterprise Wi-Fi (E-Series and XE/XV/X7-Series) and cnPilot Enterprise (ePMP 1000 Hotspot) ◦ Enterprise Wi-Fi (Xirrus-Series) ◦ NSE You can change this view later by navigating to the **Administration** > **Settings > General**

Table 7 *NMS Cloud management fields*

Parameter	Description
	page.
Primary Contact Details	
Full Name	User's full name to appear in the cnMaestro account.
Position	Designation of the user in the company. Select from the dropdown list.
Email	Email ID of the user.
Phone Number	Phone number of the user. Select the country code from the dropdown list and provide a valid phone number.
Company Details	
Company Name	Name of the company. This name will appear as the **Cloud Account Name** in the cnMaestro home page. 
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.

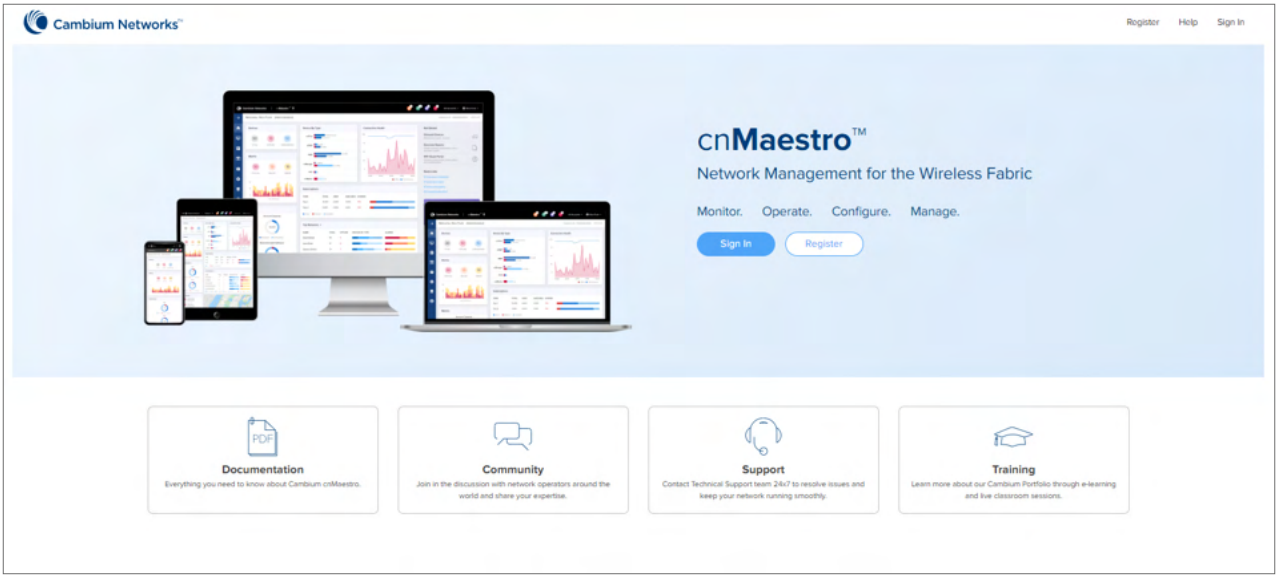
6. Click the dropdown next to the username or search option to view the created Cloud account.

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

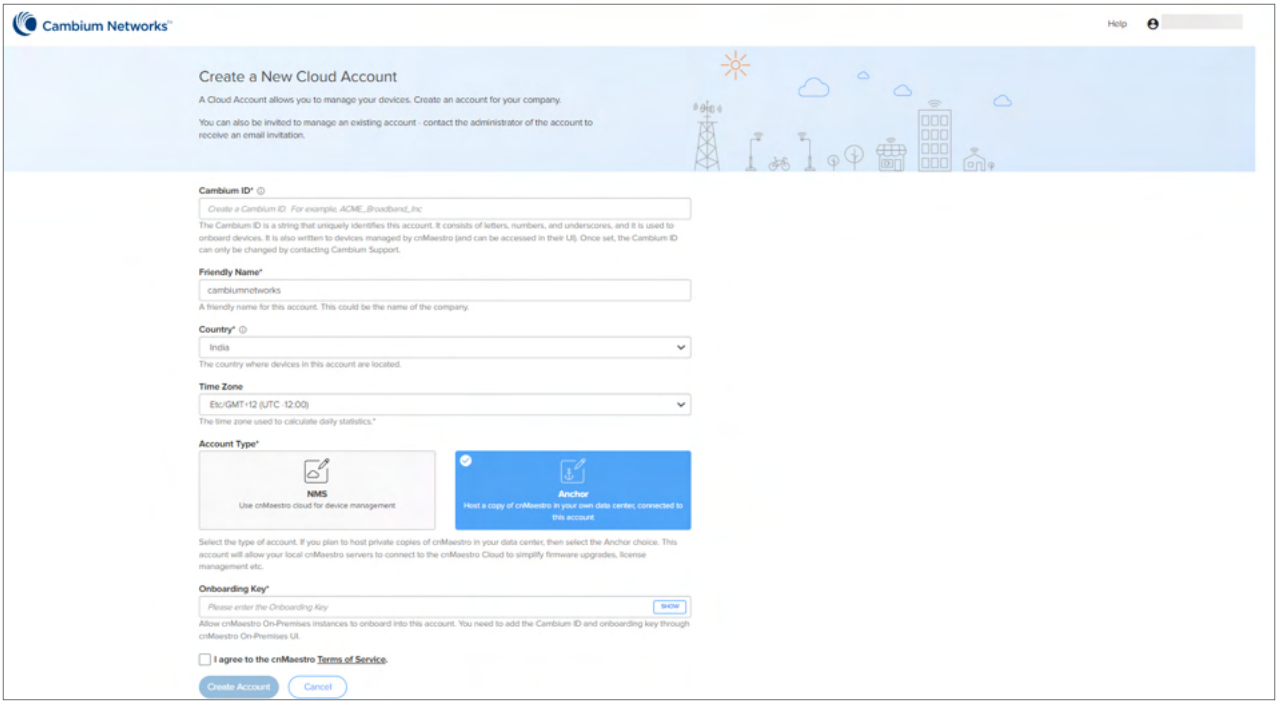
Creating an Anchor Account

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

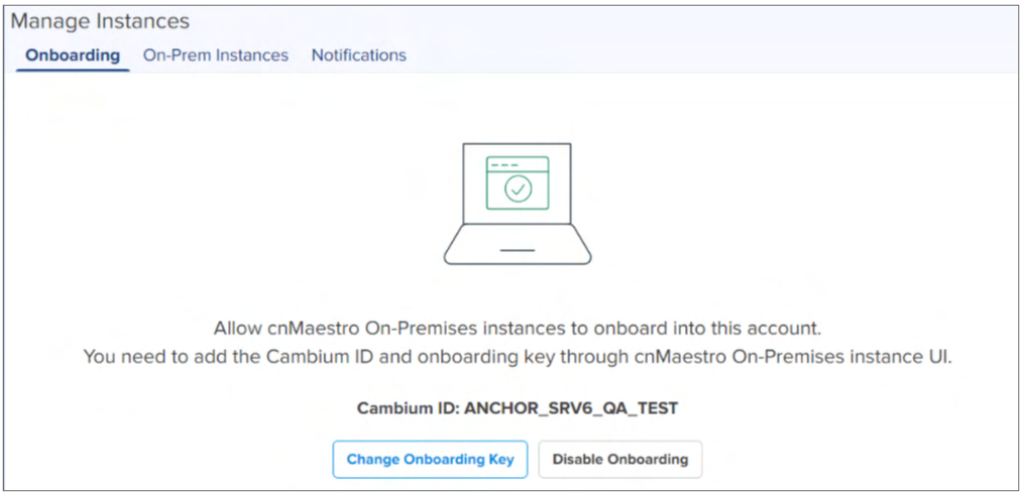
1. Log in to the cnMaestro UI https://cloud.cambiumnetworks.com.



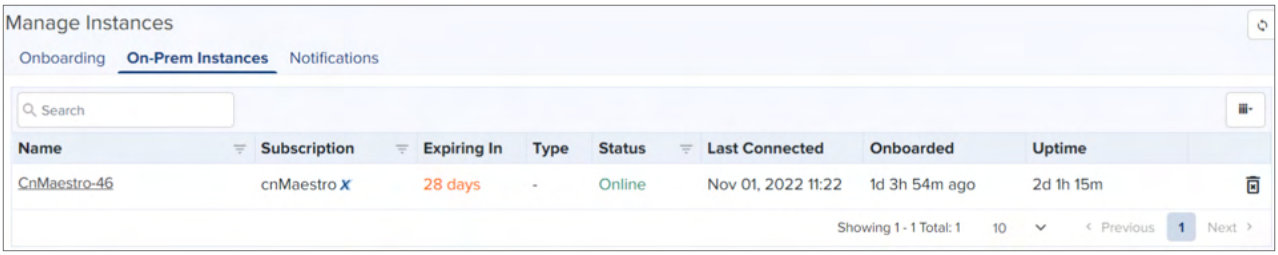
2. In **Account Type**, select **Anchor**.



3. Once the Anchor Account is created, an Onboarding Key must be set to allow On-Premises instances to connect.
4. Navigate to the **Manage Instances** page as shown below and edit the **Onboarding Key**. This key needs to be entered in the cnMaestro On-Premises UI to connect to the Anchor Account.



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

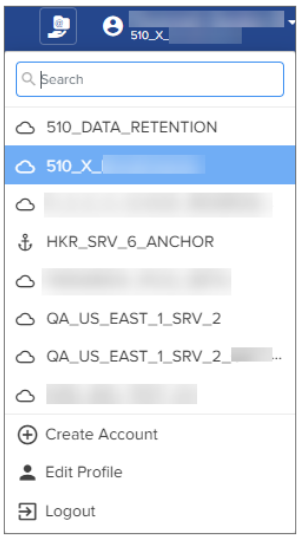


Clicking the instance host name displays the server information collected.

Multiple Cloud Accounts

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

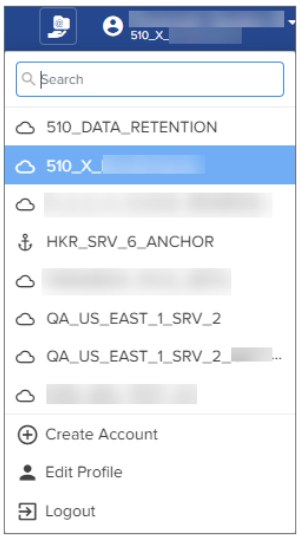
Figure 24 *Multiple Cloud Management Accounts*



Account selection

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

Figure 25 *Account selection*



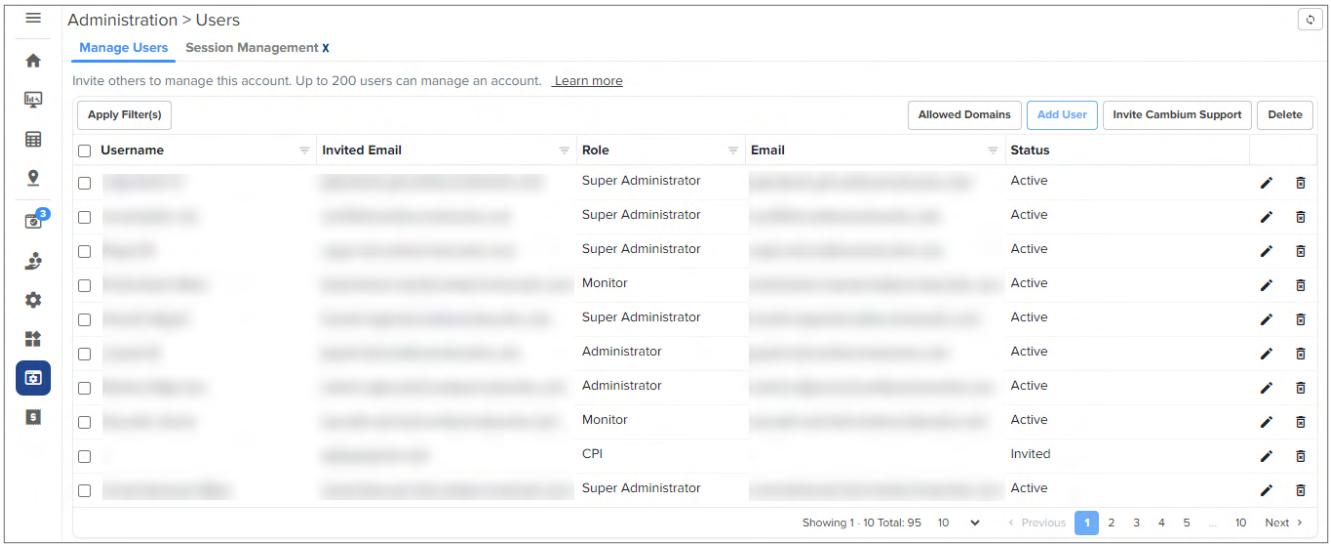
Concurrent access

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

Managing users

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

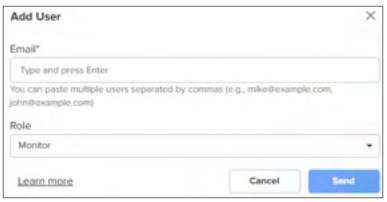
Figure 26 *Managing users*



Creating Users and Configuring User Roles

To add a user:

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



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

   For more details on user Roles, refer to Role-Based Access .
5. Click **Send**.
6. Cambium Cloud sends an email with directions on how to access the Cloud management account.

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

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

Organization

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

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

Organizations are currently only used with CBRS. Refer CBRS on how they can simplify CBRS management across multiple accounts.

General details of Organizations include:

1. One Organization can include accounts created in different countries and regions.
2. The maximum number of accounts managed by an Organization is 5.
3. There is one required Primary Account in an Organization and optionally multiple Secondary Accounts.

4. Removing the Primary Account will dissolve the Organization.
5. Both NMS and Anchor Accounts can be included in an Organization, and either can be Primary.

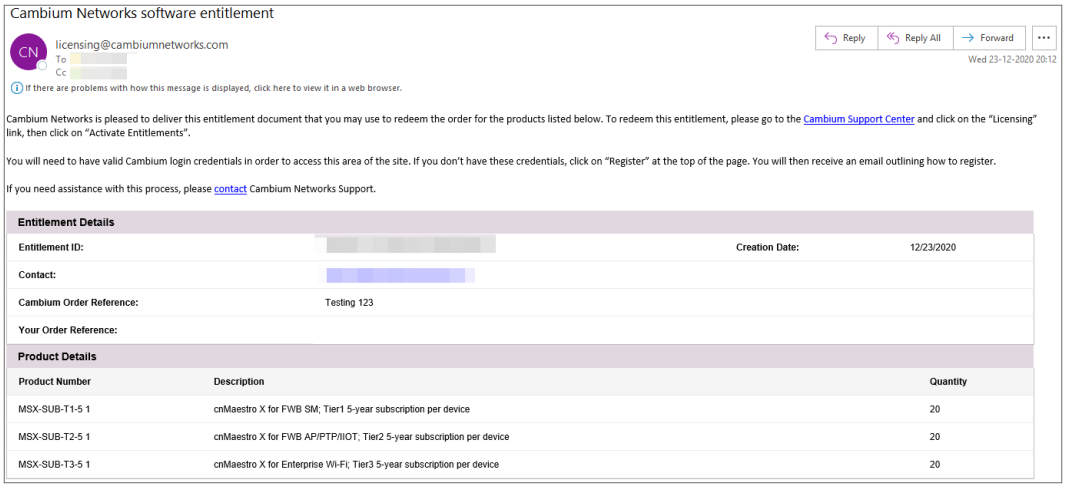
cnMaestro X

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

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

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

Figure 27 *Example of Entitlement ID*



Cambium Networks software entitlement

CN licensing@cambiumnetworks.com
To
Cc

Reply | Reply All | Forward
Wed 23-12-2020 20:12

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

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

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

If you need assistance with this process, please contact Cambium Networks Support.

Entitlement Details

Entitlement ID:		**Creation Date:**	12/23/2020
Contact:			
Cambium Order Reference:	Testing 123		
Your Order Reference:			

Product Details

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

Note

- If you are creating new accounts after cnMaestro 3.0.0, then you can request a 90-day free trial either through the link available on the cnMaestro home page or https://www.cambiumnetworks.com/cnmaestro-x/.

  For more information about cnMaestro X trial, see cnMaestro X Trial self-activation.
- The 90 days free trial gets activated automatically for the accounts created before cnMaestro 3.0.0.

NSE subscription

- The NSE device subscription is supported in cnMaestro Essentials as well as cnMaestro X in the cnMaestro Cloud deployment.
- You can avail the Entitlement ID for NSE with the required device slots according to the Device Tiers by contacting the reseller or distributor.

- When you move other devices from cnMaestro Essentials to cnMaestro X, you can continue to use the same NSE subscription.
- When you have only Free Tier devices and a subscription for NSE, you can manually upgrade to cnMaestro X and downgrade to Essentials on your own.

cnMaestro X Trial self-activation

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

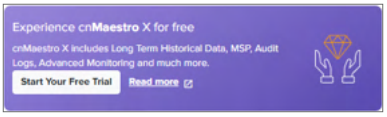
- There must no subscriptions in the Essentials account.
- Users must not have used cnMaestro X earlier.

  If the users have already used cnMaestro X earlier, then downgraded to Essentials, and now want to try cnMaestro X trial, then they must contact the Cambium Support team by filling the form at https://www.cambiumnetworks.com/cnmaestro-x/.
- Users must not have activated cnMaestro X Trial earlier.

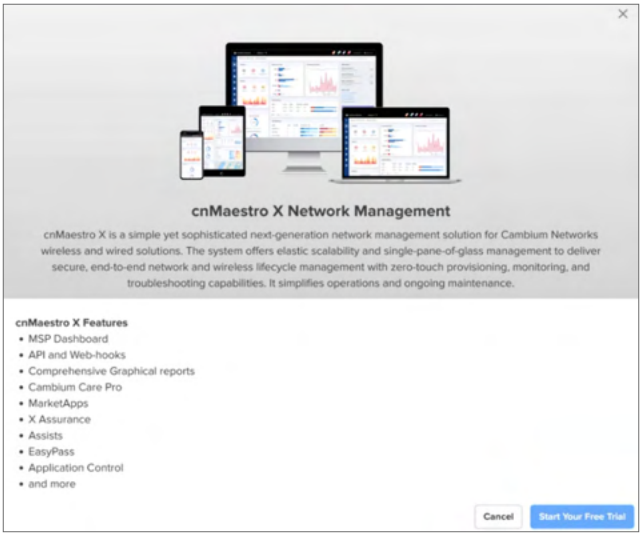
  If the trial was activated earlier and users want to try cnMeastro X Trial again, users must contact the Cambium Support team by filling the form at https://www.cambiumnetworks.com/cnmaestro-x/.

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

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

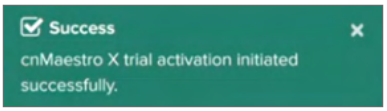
   

   The cnMaestro X Network Management pop-up is displayed.

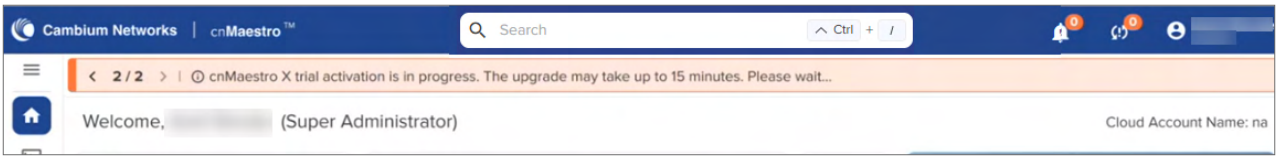
   

3. Click **Start Your Free Trial**.

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



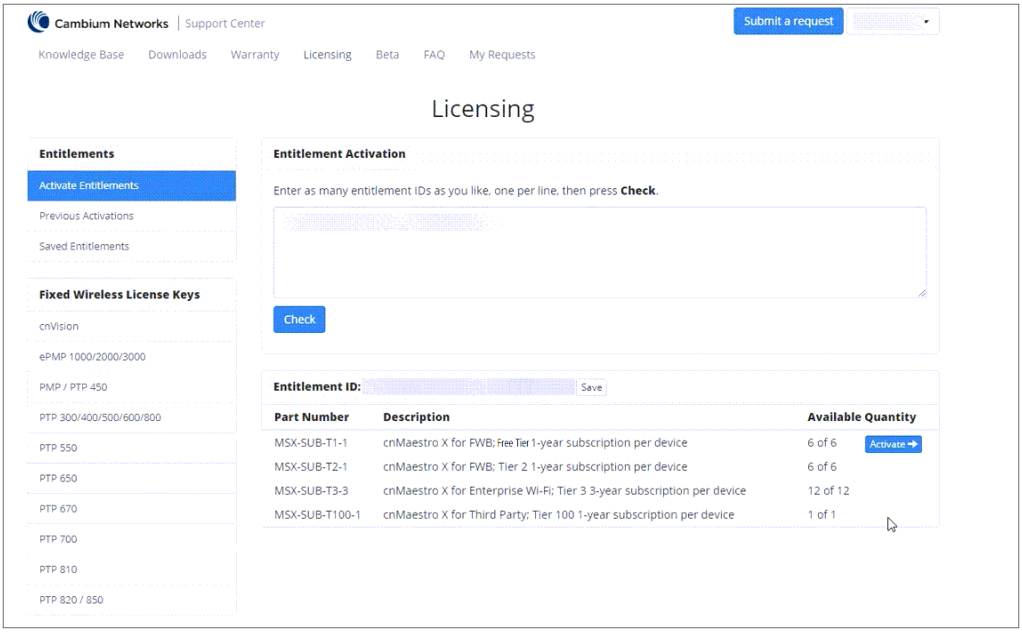
A banner also appears mentioning that the trail activation has started.



cnMaestro X activation

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

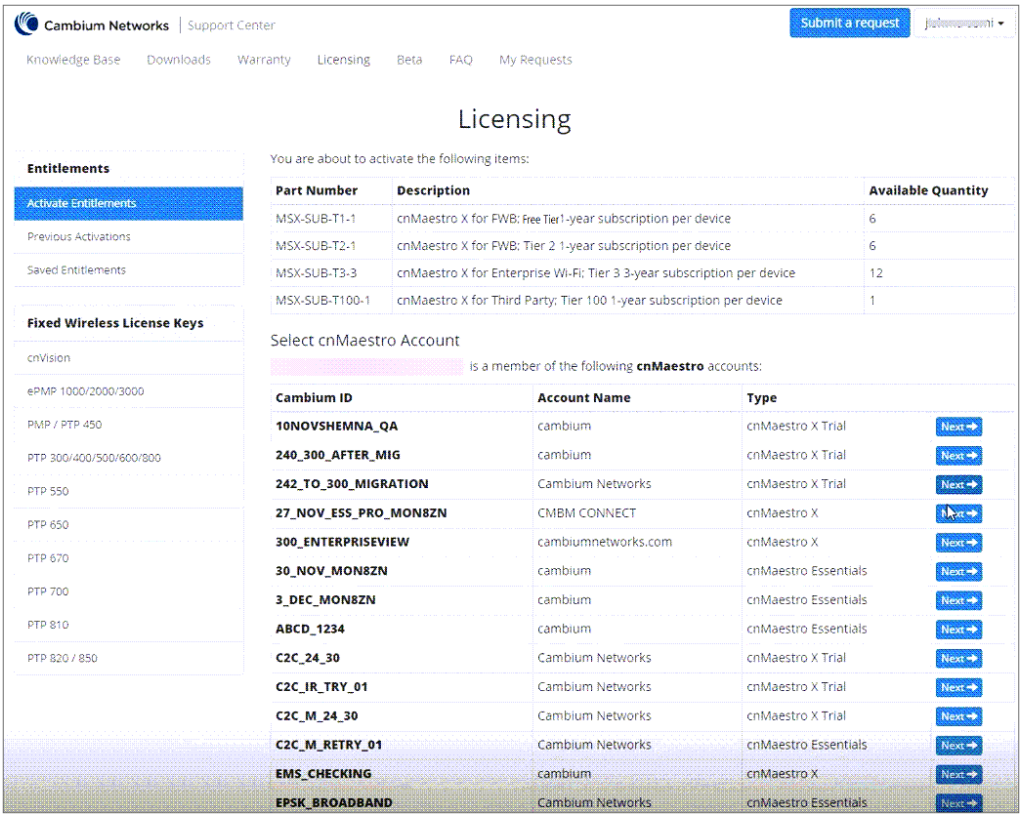
1. Navigate to https://support.cambiumnetworks.com/entitlements, or from the cnMaestro home page click the **Licensing** tile.
2. In the Licensing page under **Entitlements** select **Activate Entitlements**.
3. Enter the **Entitlement ID** received from licensing@cambiumnetworks.com.
4. Click **Check.**



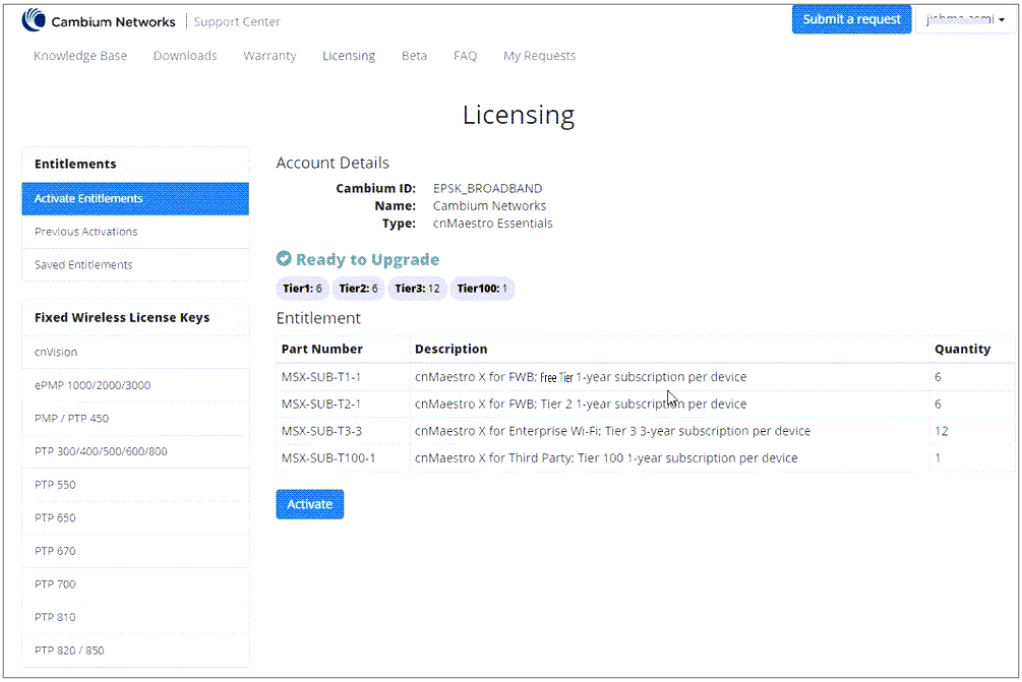
5. Once the **Entitlement ID** is validated, the **Activate** button is enabled.

> **Note**
>
> All subscribed part numbers must be activated under each **Entitlement ID**.
>
> The part numbers subscribed with **MSX** must be activated together.

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



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



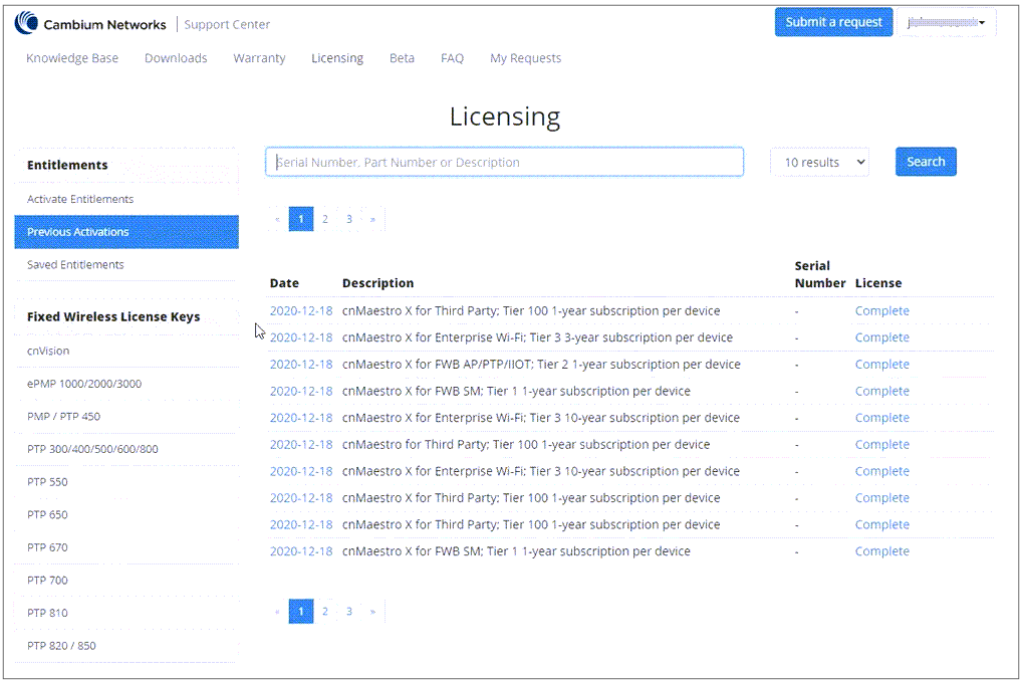
9. 1. Click **Activate**.



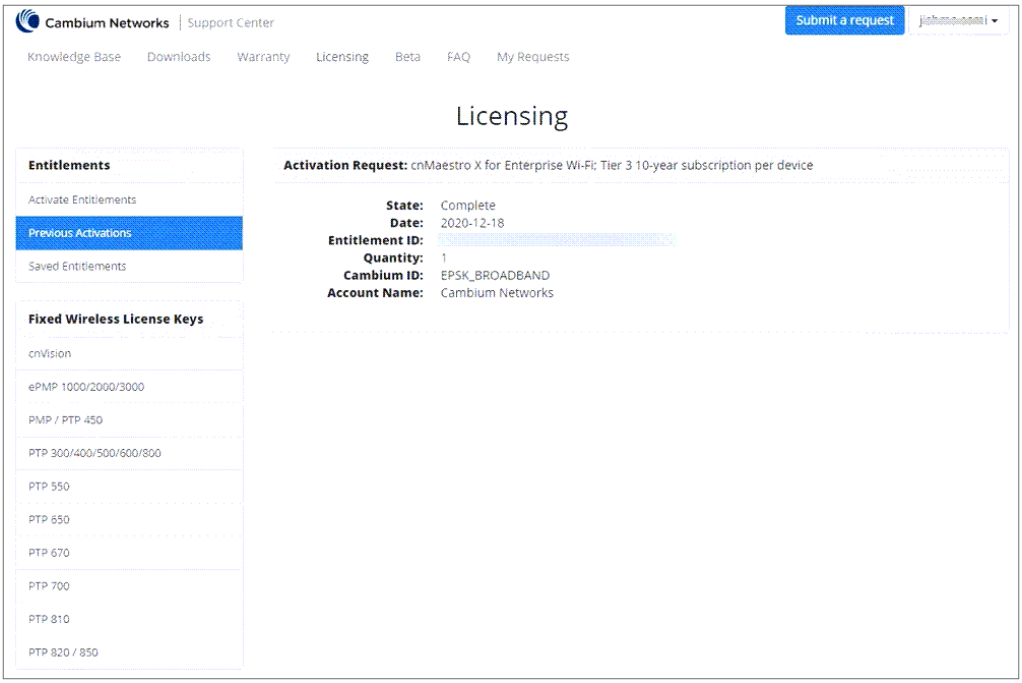
Note

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

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

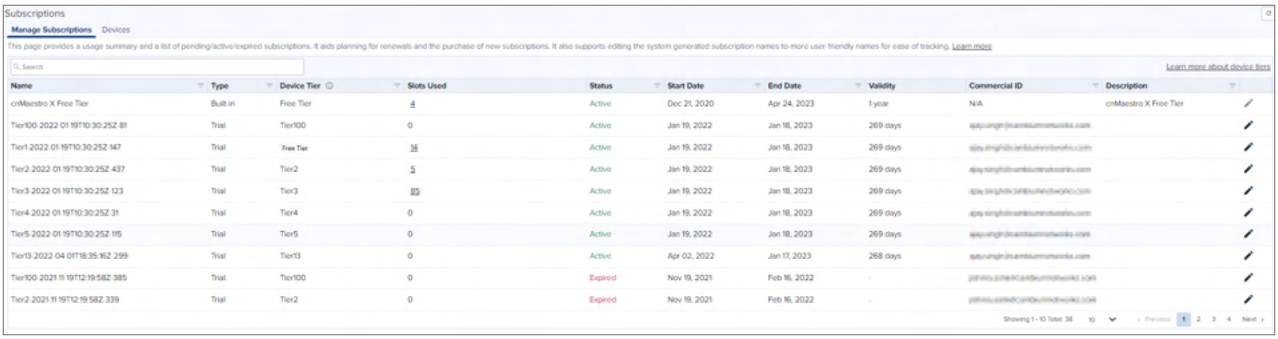


11. Click any licensed description which is marked **Complete**.

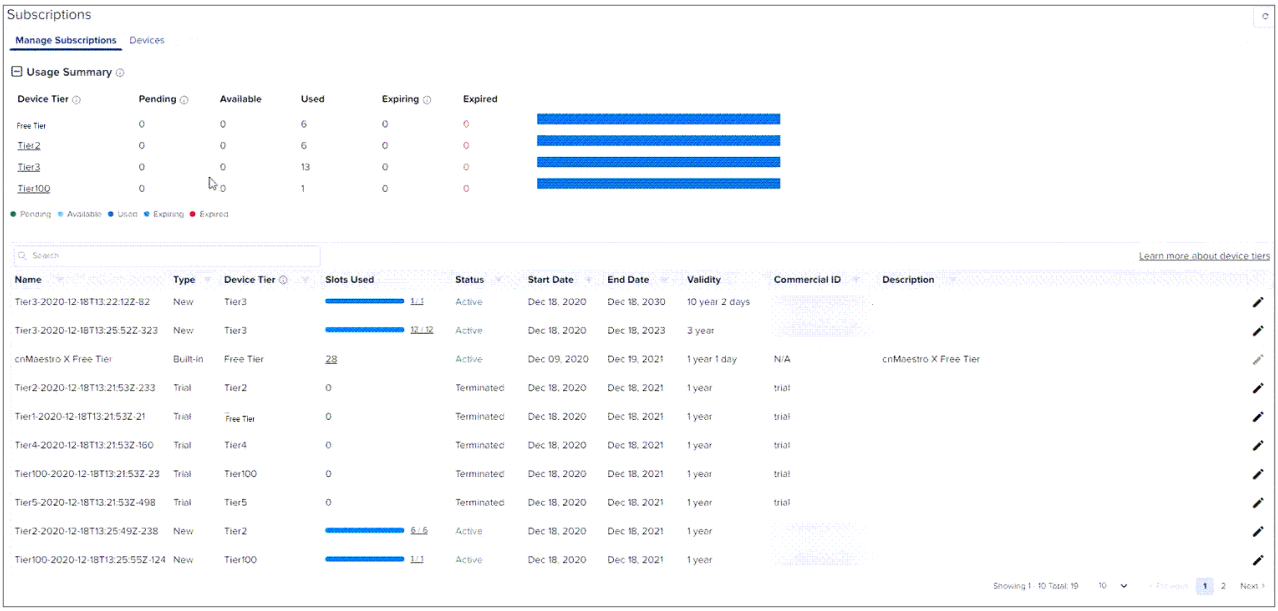


The Subscription is activated with the number of requested slots.

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



The user account upgrades to a cnMaestro X account.

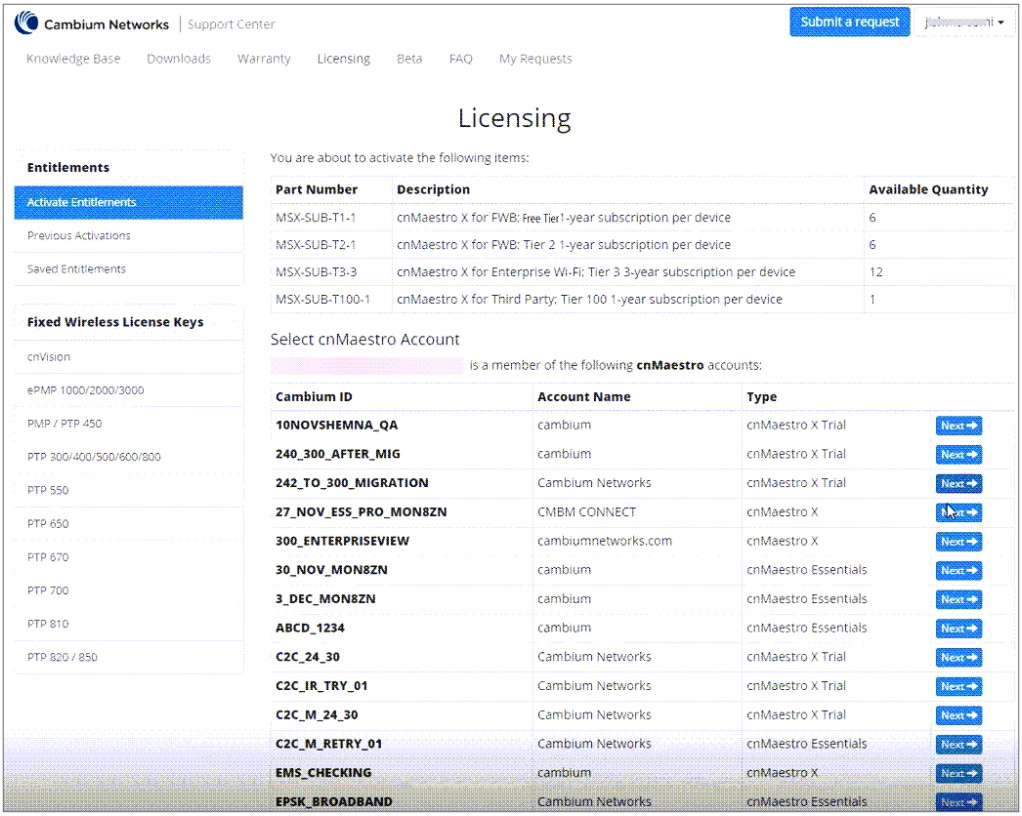


Slot Deficit

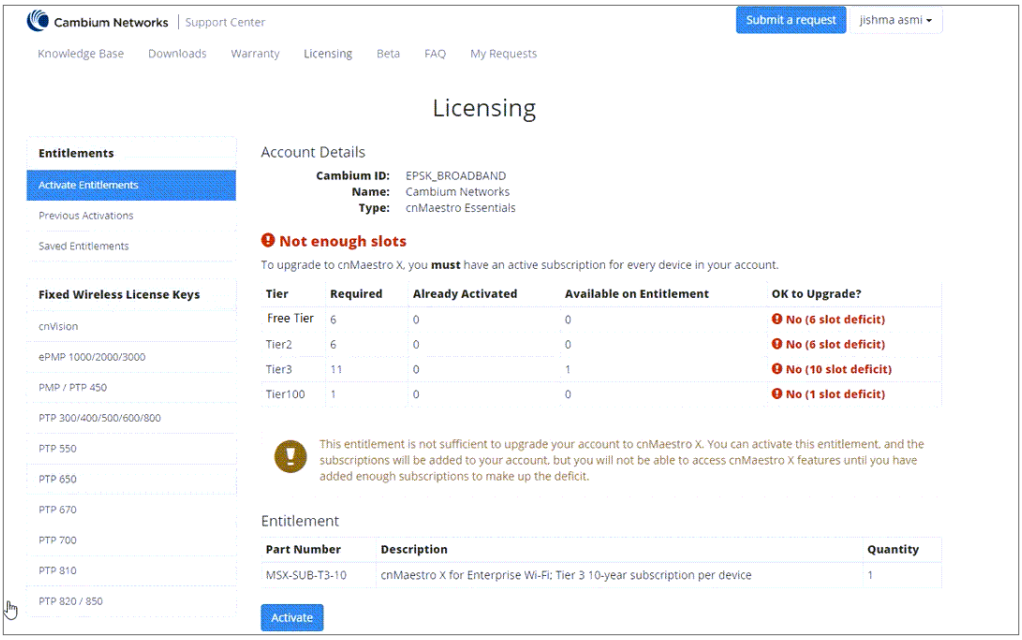
A Slot Deficit occurs when the number of slots (one for each device) activated from the entitlement is less than the slots required. This can occur if there are more devices in the account than slots.

Upgrading to cnMaestro X will be pending until either devices are removed to match the available slots or more slots are added to cover the deficit.

1. Select the **Cambium ID** from the list and click **Next**.

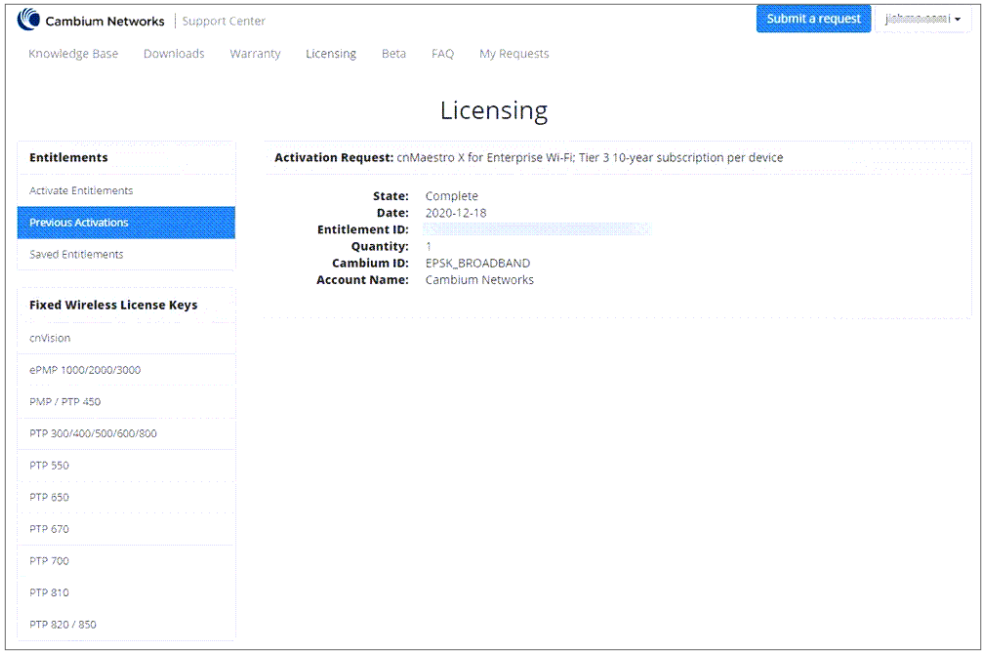


2. The **Active Entitlement** page displays **Not enough slots** when there is a slot deficit.

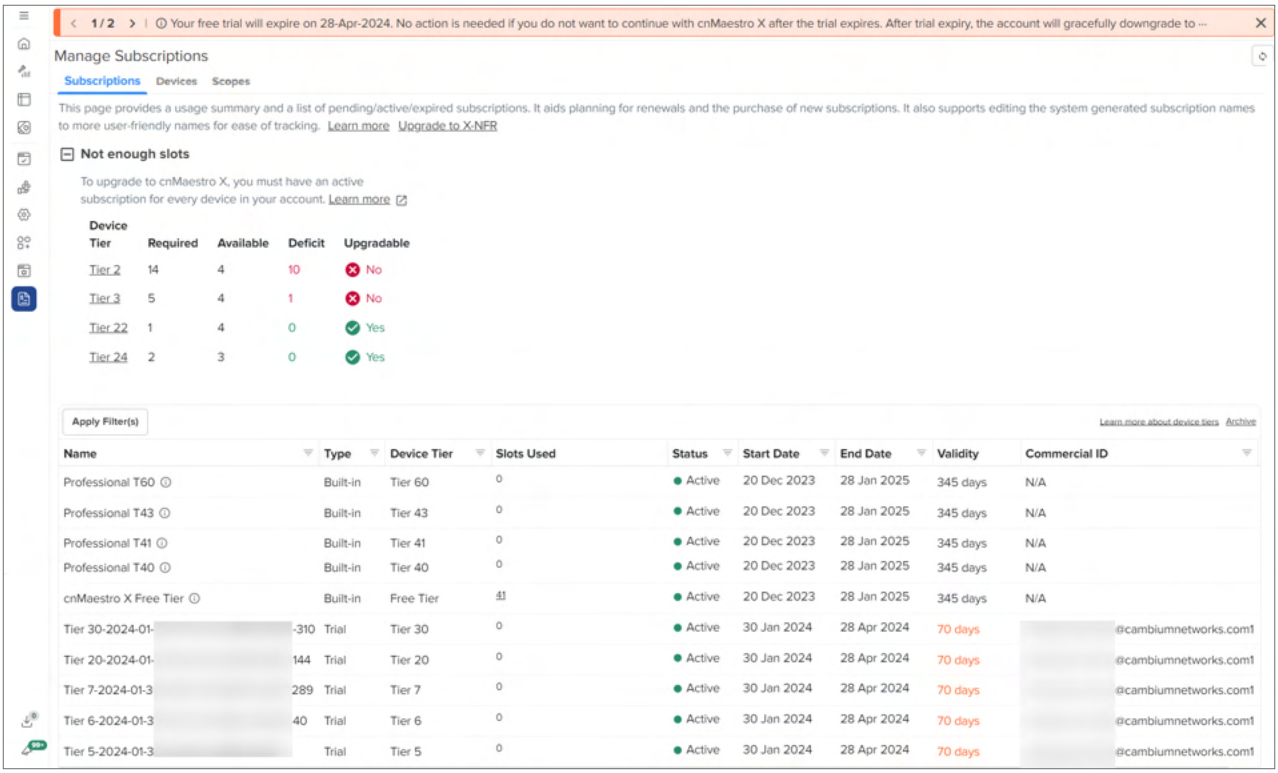


3. If the user activates even with the slot deficit warning.

- Activation process completes.



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



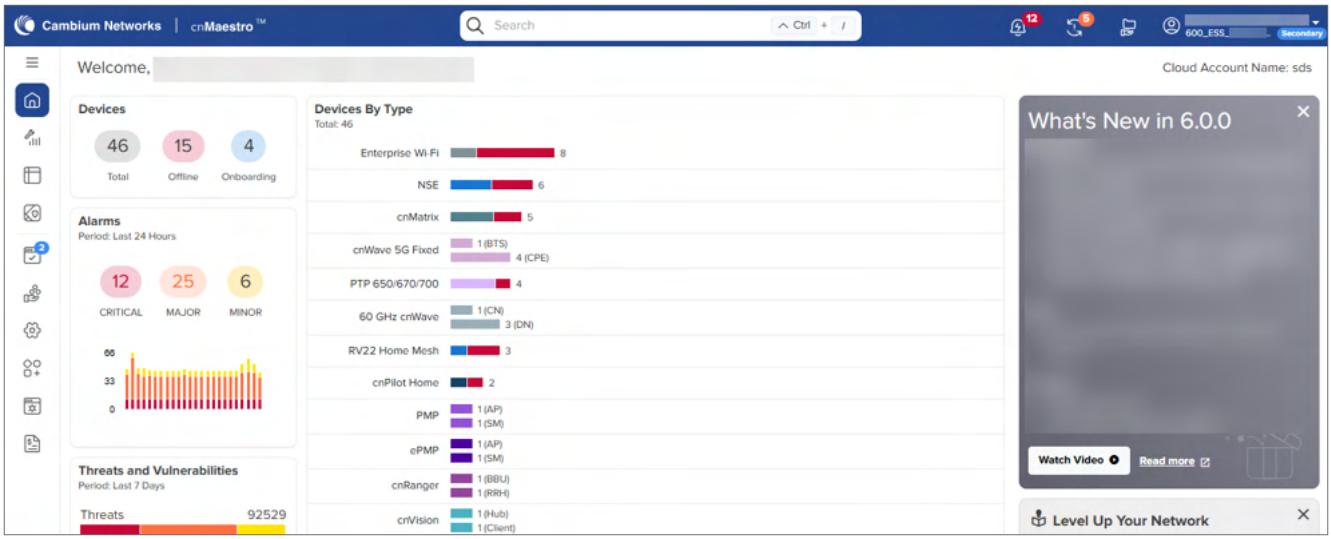
4. Once the user removes the deficit, the account automatically upgrades to cnMaestro X.

Subscription Management

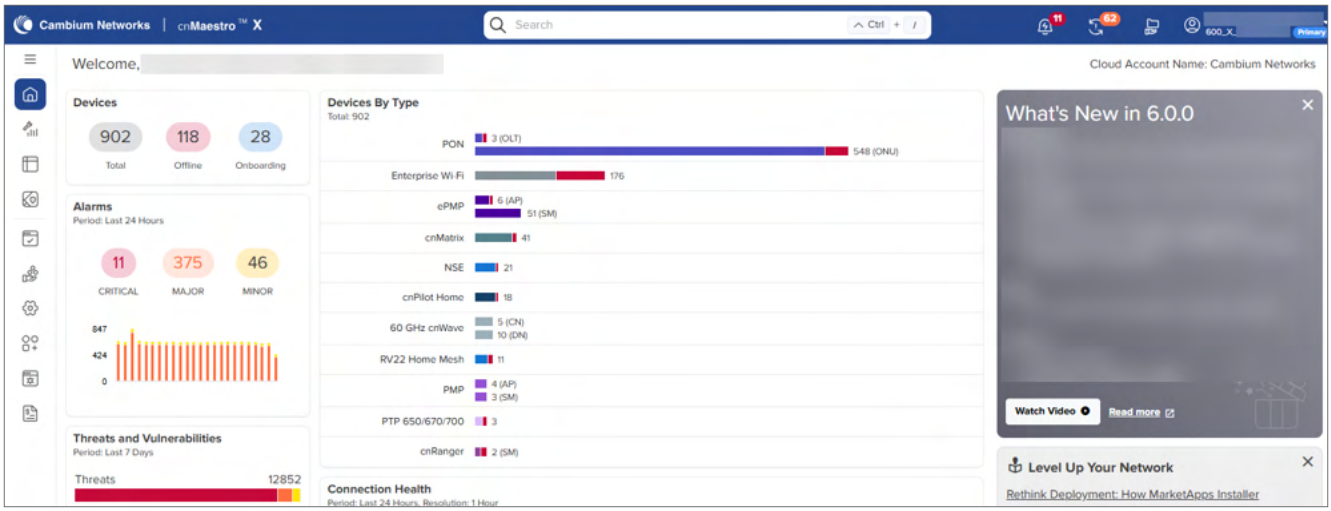
cnMaestro supports the following modes:

- Essentials—Unpaid Subscription
- cnMaestro X—Paid Subscription

A cnMaestro Essentials account can be identified as shown below.



If a subscription is active, the cnMaestro X banner is displayed, as shown in the following figure.



This topic contains the following sections:

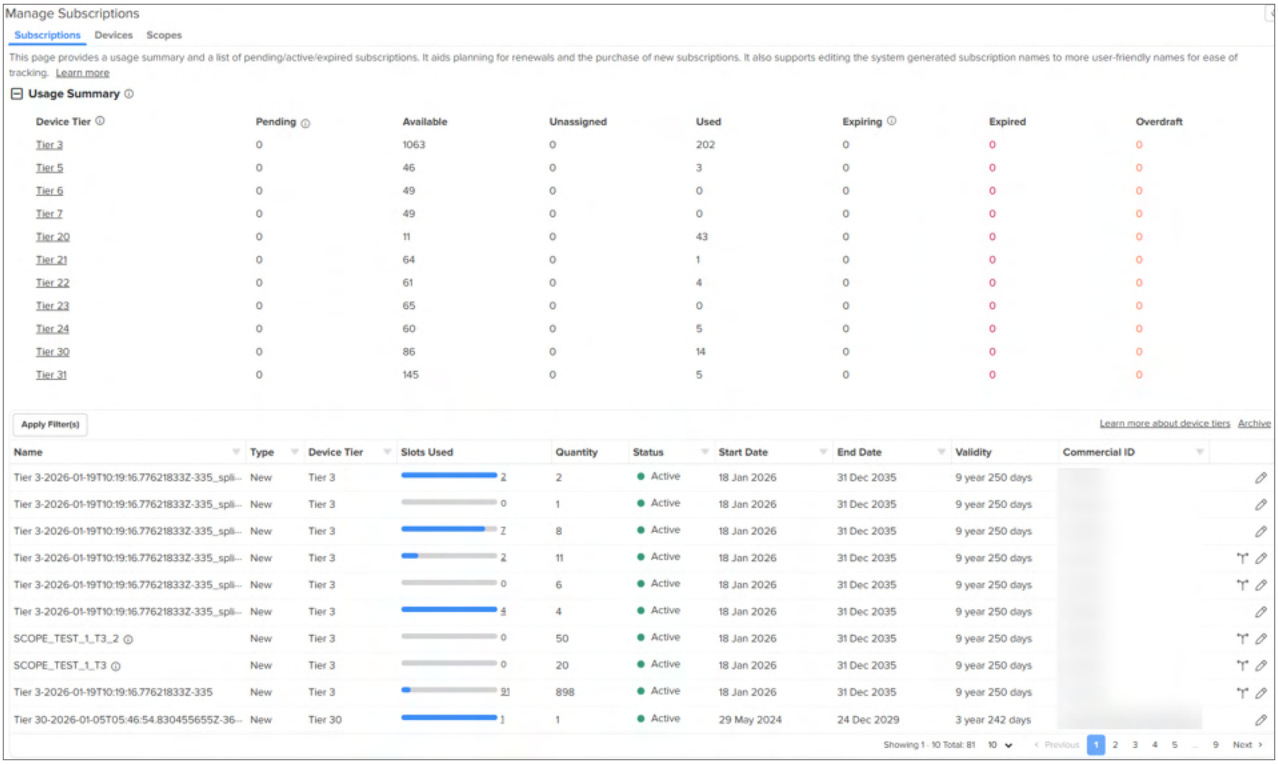
- Manage Subscriptions
- Usage Summary
- Device Tiers
- Devices
- Expiry Notification
- Retention of Data After Expiry and Reinstatement of Service

- Creating Scopes for Subscriptions
- Overdraft Subscription
- Download a Bill of Material (BoM)

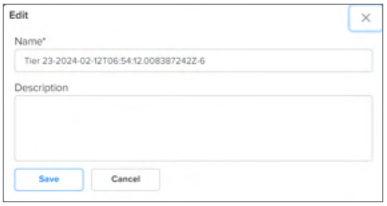
Manage Subscriptions

Users can view, edit, check the validity and status of subscriptions. You can also view details of the subscriptions that are expired or terminated.

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



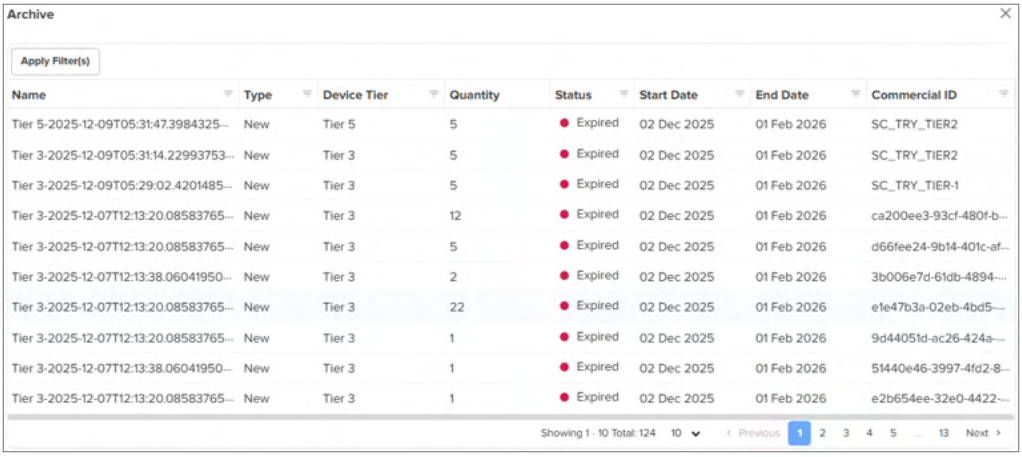
2. Click the **Edit** icon to edit the subscription **Name** and **Description** and click **Save.**



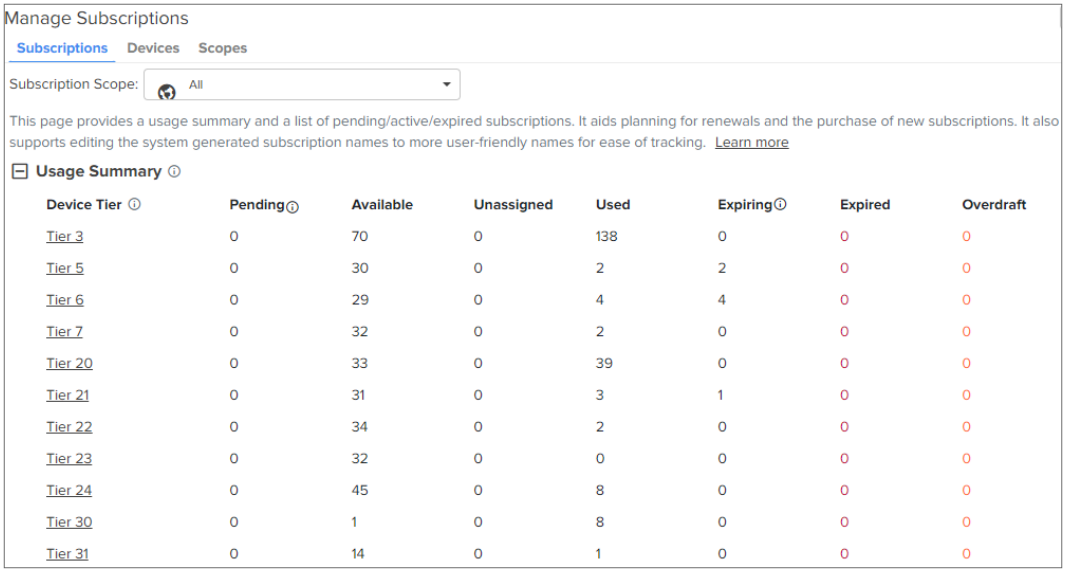
   - Onboard devices according to the allotted slots.
   - New devices are added to the subscription with the earliest expiration.

3. To view the expired or terminated subscription details, click **Archive**.

The Archive table is displayed.



Usage Summary



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

Device Tiers

Device Tiers display the classifications allotted for each device.



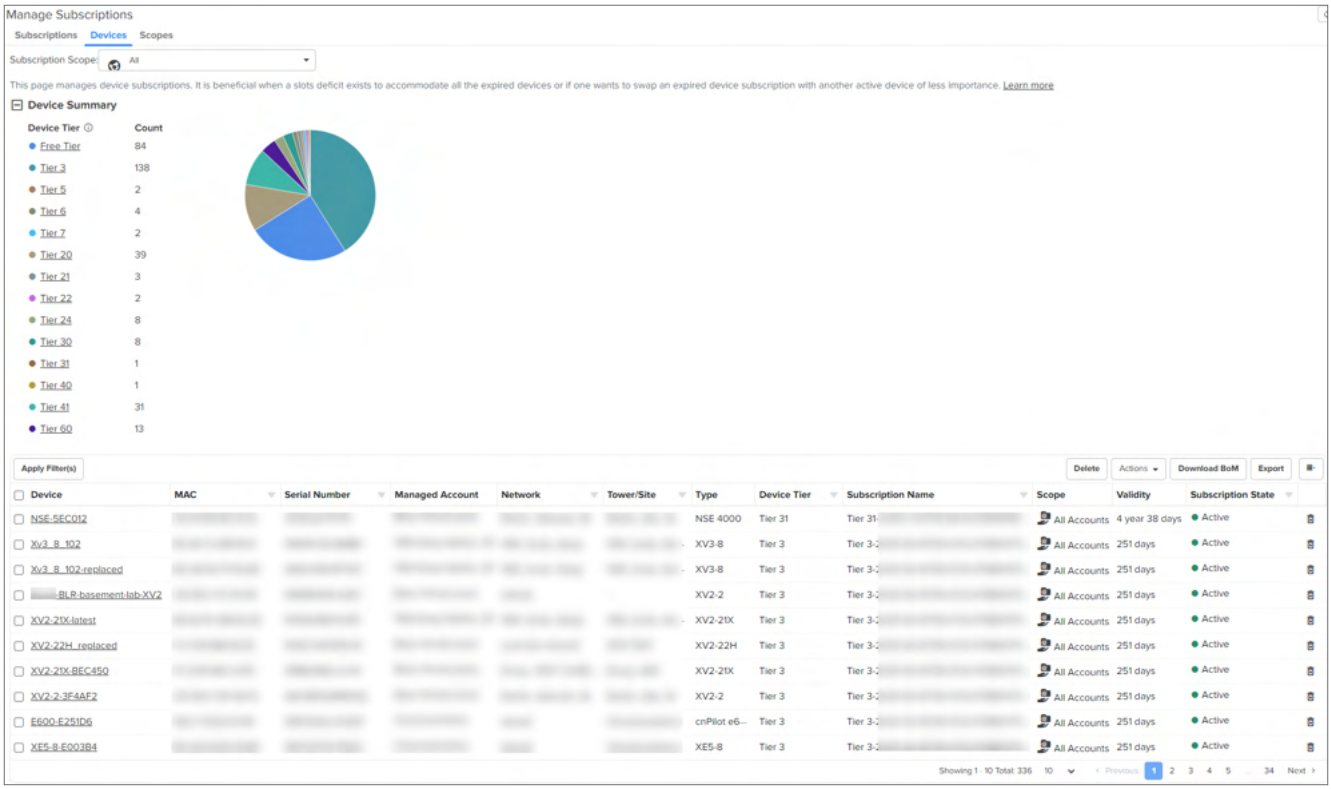
Unlisted devices do not require paid subscription. They are part of the Free Tier (Tier 0). All Tier 0 through Tier 7 devices can be used with an Essentials account. Tier 20 and Tier 30 licenses require paid subscription even in Essentials mode.

Note

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

Devices

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



Swap Subscription

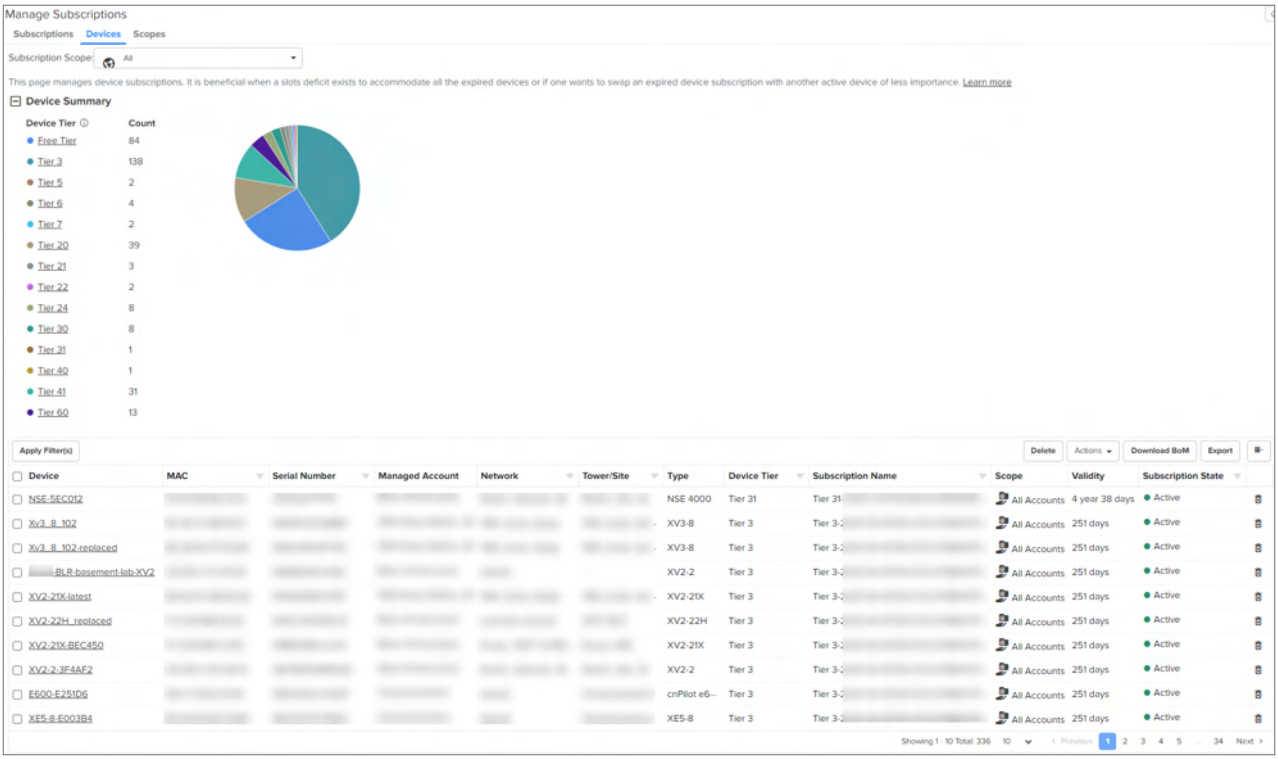
Swap Subscription allows the user to swap one device subscription with another device of the same tier. It can be performed at any time.

Note

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

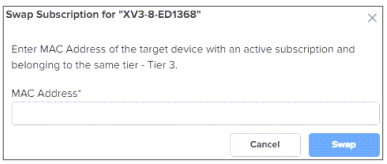
To swap subscriptions:

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



2. Select the device to be swapped to another subscription.
3. From the **Actions** dropdown list, click **Swap Subscription.**

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



   A success notification is displayed on successful subscription swapping.

Change Subscription

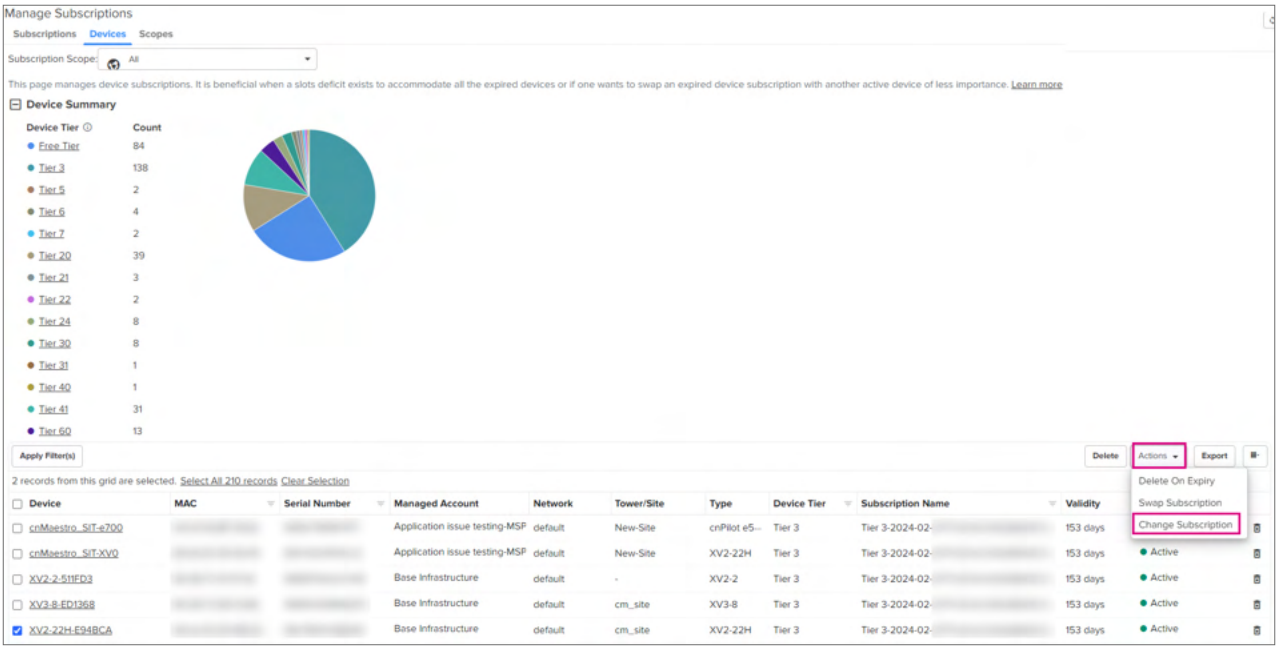
Change Subscription changes the device from one subscription to another of the same tier when slots are available.

Note

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

To change subscription:

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



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



4. Click **Change**.

   A success notification is displayed on successful subscription change.

Delete on Expiry

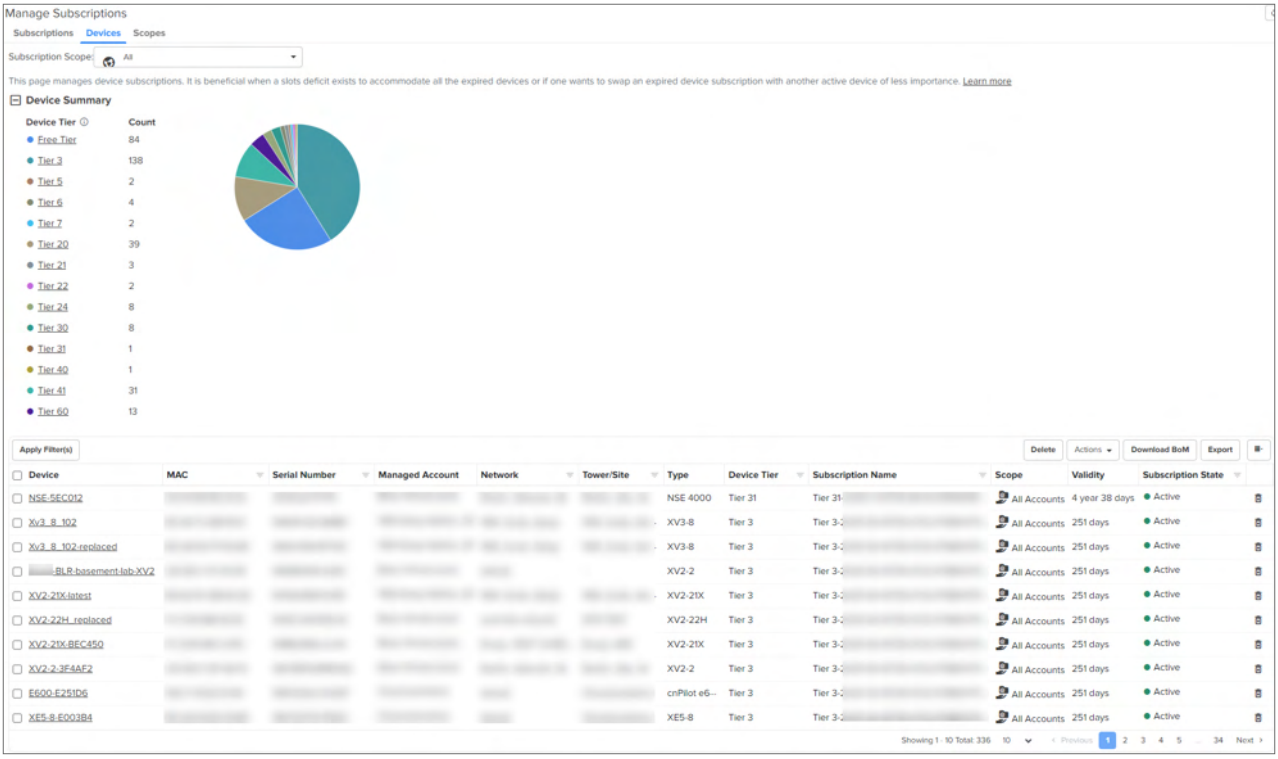
Note

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

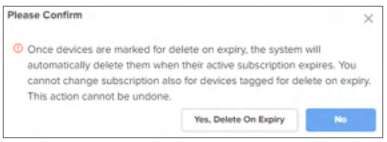
User can select the device and set the subscription state to **Delete on Expiry**, once the device is expired, it automatically is deleted from the device list.

To set the delete on expiry option:

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



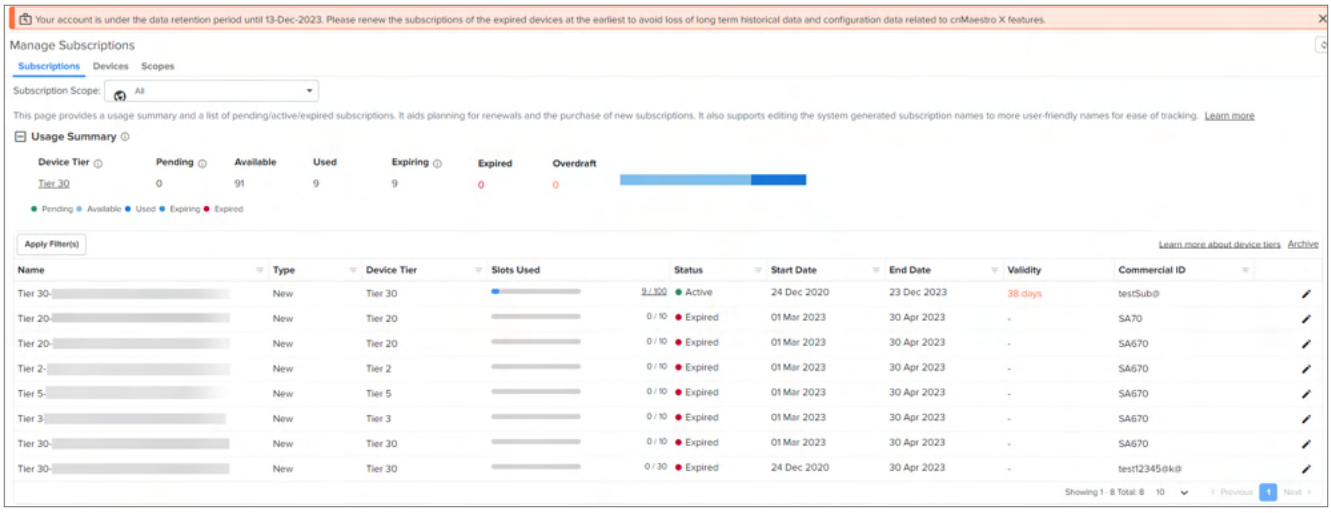
2. From the **Actions** dropdown list, click **Delete on Expiry.**
3. Click **Yes, Delete On Expiry** in the confirmation window.



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

Expiry Notification

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



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

Expired Device

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

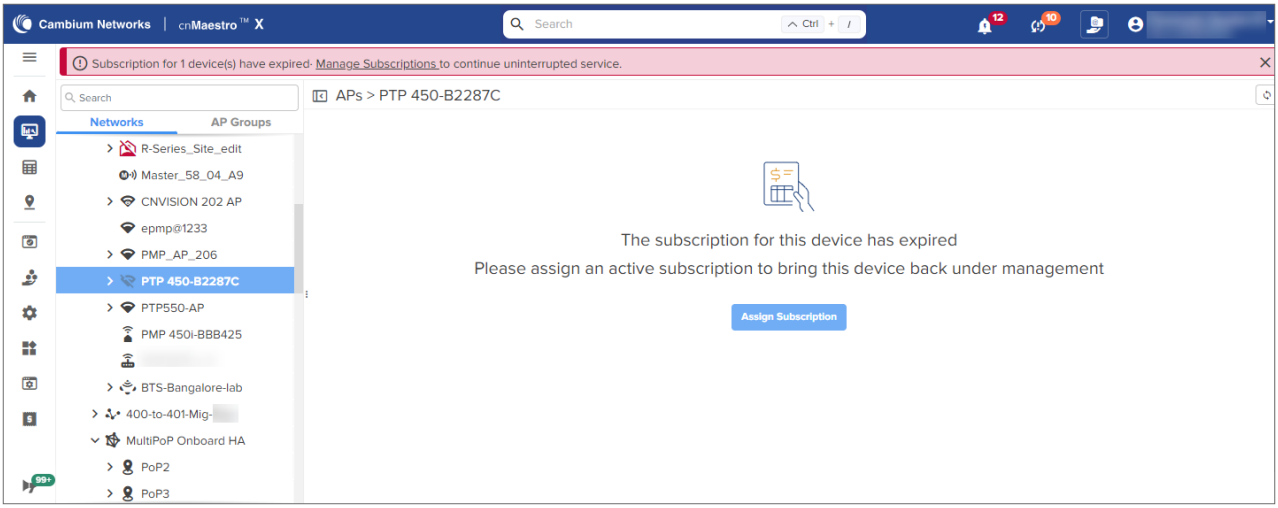
Note

In the expired device dashboard:

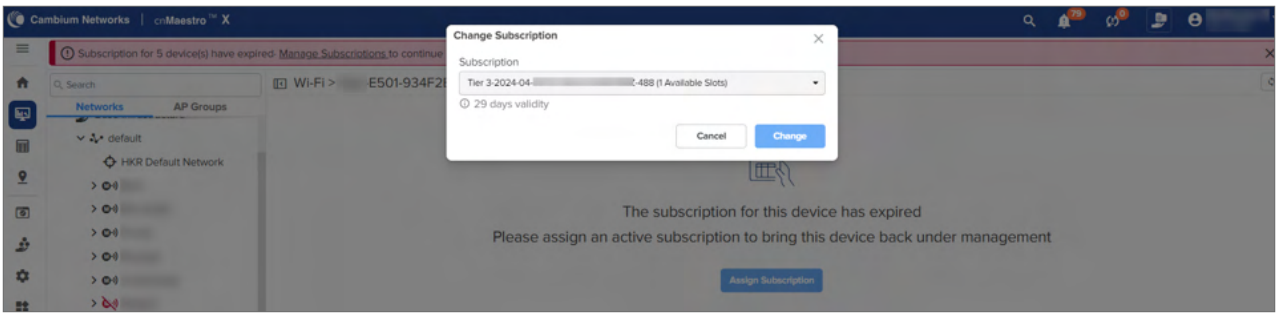
- If any free slots are available Change Subscription will be enabled.
- If free slots are not available Swap Subscription will be enabled with the specific device MAC address.
- If you have an X account with expired devices, you can downgrade to Essentials and manage all devices without X features. The activated subscriptions will be moved to pending state.

Change Subscription at device level

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

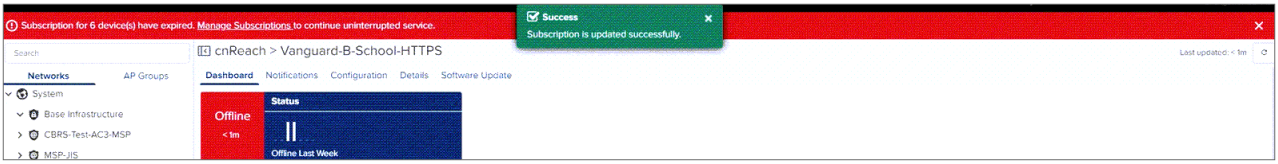


2. Click **Assign Subscription** and select the **Subscription** from the list.



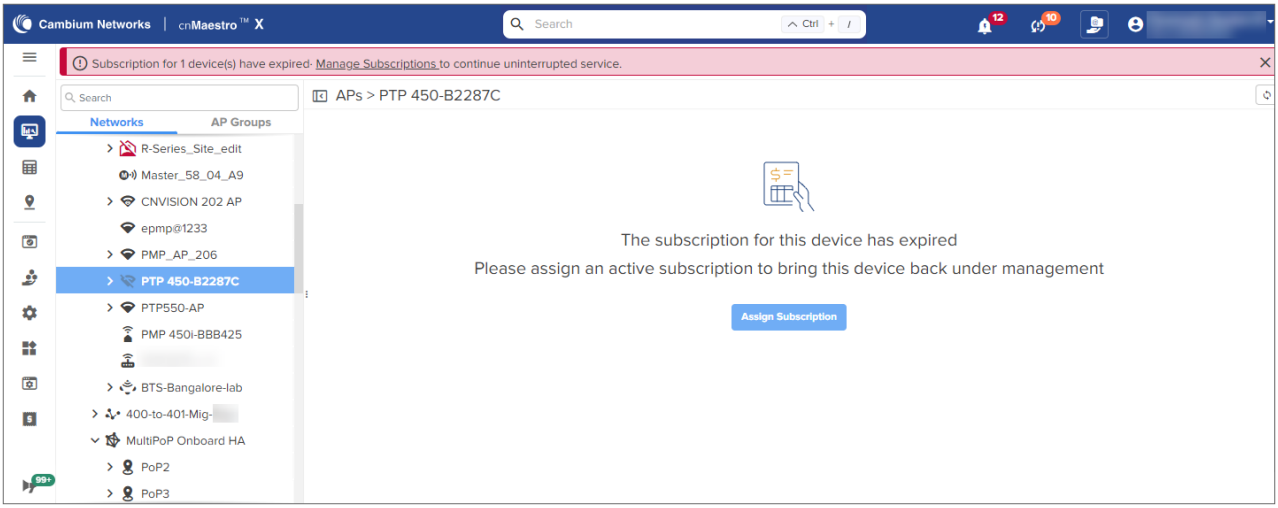
3. Click **Save**.

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

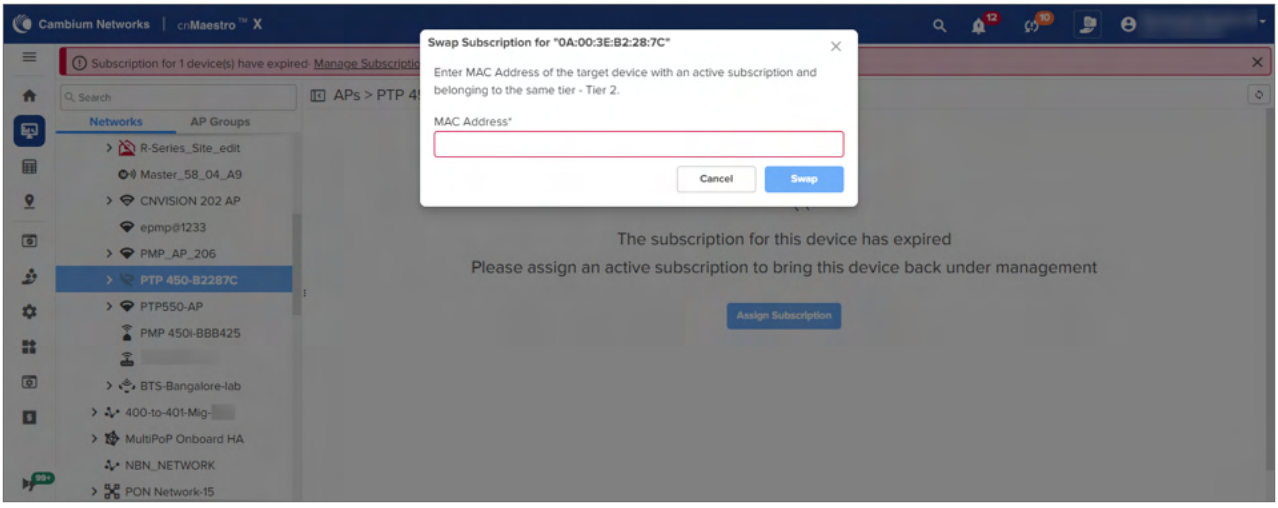


Swap Subscription at device level

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



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



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

Retention of Data After Expiry and Reinstatement of Service

If subscriptions are not renewed in time, devices under those subscriptions will expire and are no longer managed by cnMaestro. Once all subscriptions are expired, the account transitions to cnMaestro Essentials with a data retention period for historical data of 90 days. All historical data beyond one week, and cnMaestro X specific

configuration, will be retained until the data retention period of 90 days, after which it will be deleted. This is done to ensure no data loss if subscriptions are renewed before the data retention period ends.

Creating Scopes for Subscriptions

Subscription scopes introduces hierarchical control over subscription allocation, replacing the previous flat structure. It ensures that subscriptions are utilized only within defined scopes, preventing cross-hierarchy usage, and providing better control of subscriptions.

Initially all subscriptions will be part of the shared pool. After scoping is enabled, subscriptions can be assigned to specific hierarchy levels. Scopes can be created at the Managed Account-, Network-, and Site-levels. Devices that are onboarded within a scope can only use the subscriptions allocated to that scope. When a scope is enabled at a particular level, for example, Network, then no other scopes can be enabled for the sites that are present under this network or the Managed Account it is part of.

When subscriptions are shared across scopes, subscriptions are automatically split based on devices present in that scope. However, new subscriptions remain unassigned until they are linked to a scope.

On the Manage Subscriptions page, a new scope filter is available to view the subscriptions assigned to that scope and the devices that are onboarded to those scopes.

- Enabling and adding scopes
- Editing, deleting, and disabling scopes

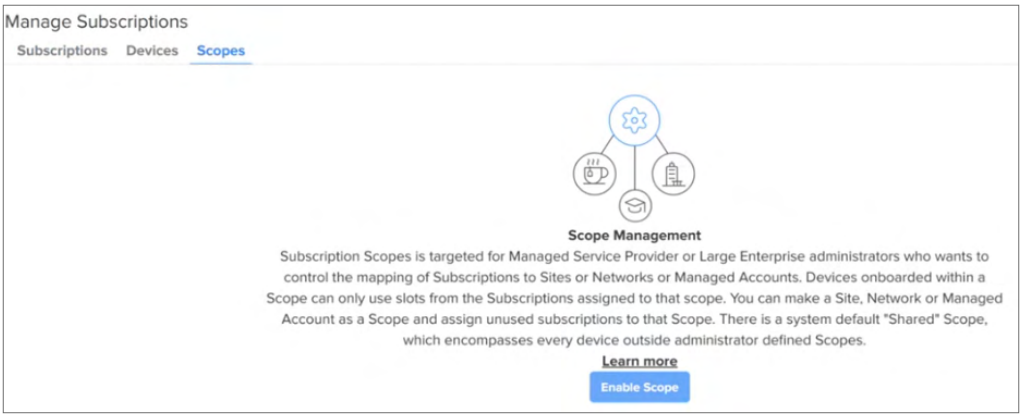
Enabling and adding scopes

To enable and add scopes for subscriptions, complete the following steps:

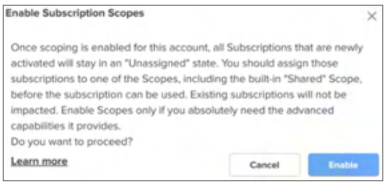
1. Navigate to the **Manage Subscriptions** > **Scopes** tab.

   The Scopes page is displayed

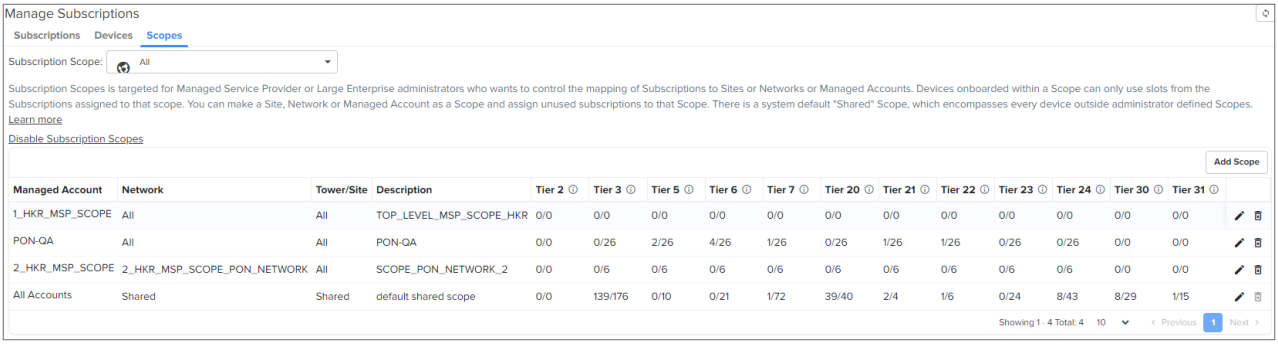
2. If scoping is not enabled, click **Enable Scope**.



3. Click **Enable** in the confirmation window that appears.



4. To add a new scope, click **Add Scope**.



The **Add Scope** window is displayed.

5. Select the required managed account, network, or site where you want to assign the scope.



6. The following options appear:

   a. If no subscriptions are shared by devices in other scopes, then the following information is displayed.

      Click **Add Scope**.



   b. If subscriptions are shared across devices in other scopes, then a conflict arises.

      This conflict must be resolved by splitting the subscriptions between the scopes.

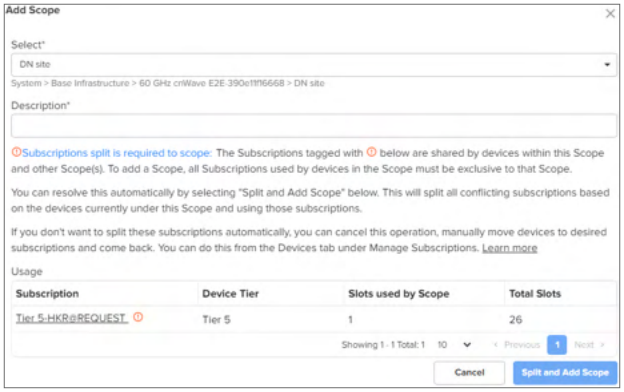
      You can resolve this conflict in one of the following ways:

      - Automatically, by selecting **Split and Add Scope**.

        This will split the subscriptions based on the number of devices present in the scope.

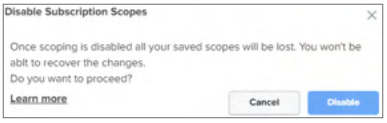
      - Manually, by individually moving the devices to the required subscriptions and repeating the steps

mentioned in this section.



Editing, deleting, and disabling scopes

1. To edit a scope, click the edit (✎) icon corresponding to the scope you want to edit.
2. To delete a scope, click the delete (🗑) icon corresponding to the scope you want to delete.
3. To disable subscription scoping, click **Disable Subscription Scopes** and click **Disable** in the confirmation window that is displayed.



Overdraft Subscription

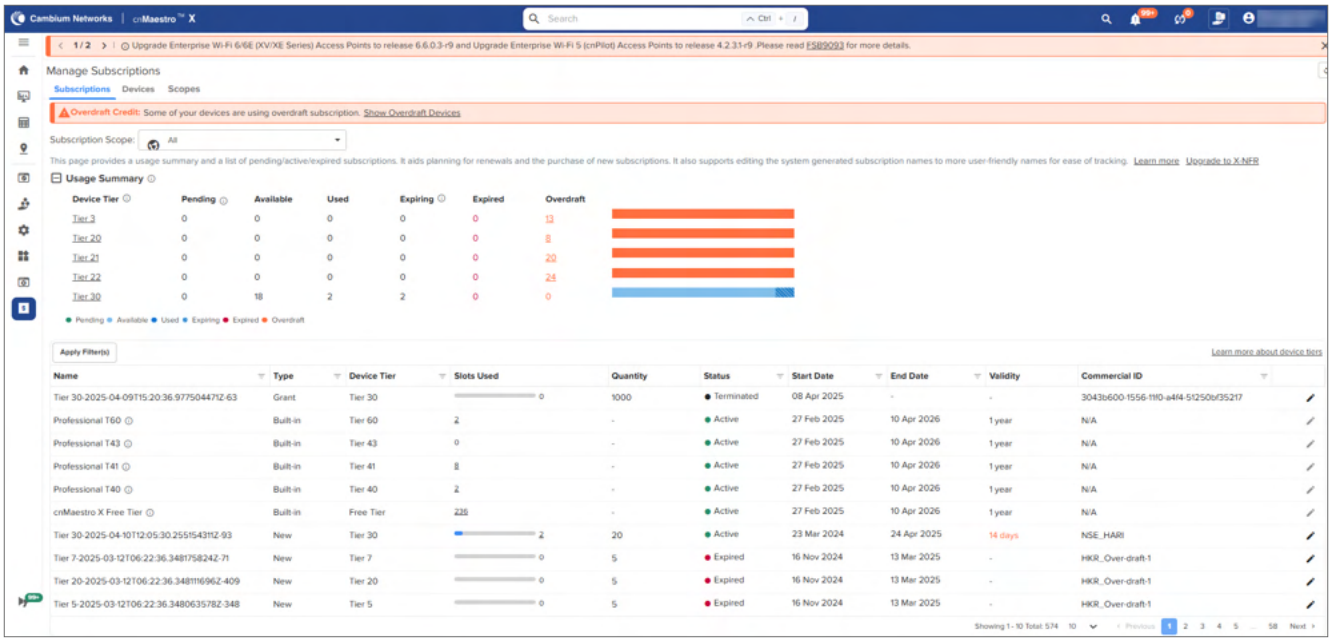
Note

- Overdraft support is available only in cnMaestro X and is applicable for NSE devices in an ESS account. A minimum of one active subscription is required to enable this feature.
- Overdraft subscription is available only once per account. From the next time onwards, the devices will display a Slot could not acquire error on the onboarding page.
- Devices in the overdraft list will be assigned subscriptions (as and when the subscriptions are added) on a first-in-first-out basis, that is, the device that first entered the overdraft list will be the first to be assigned a subscription.

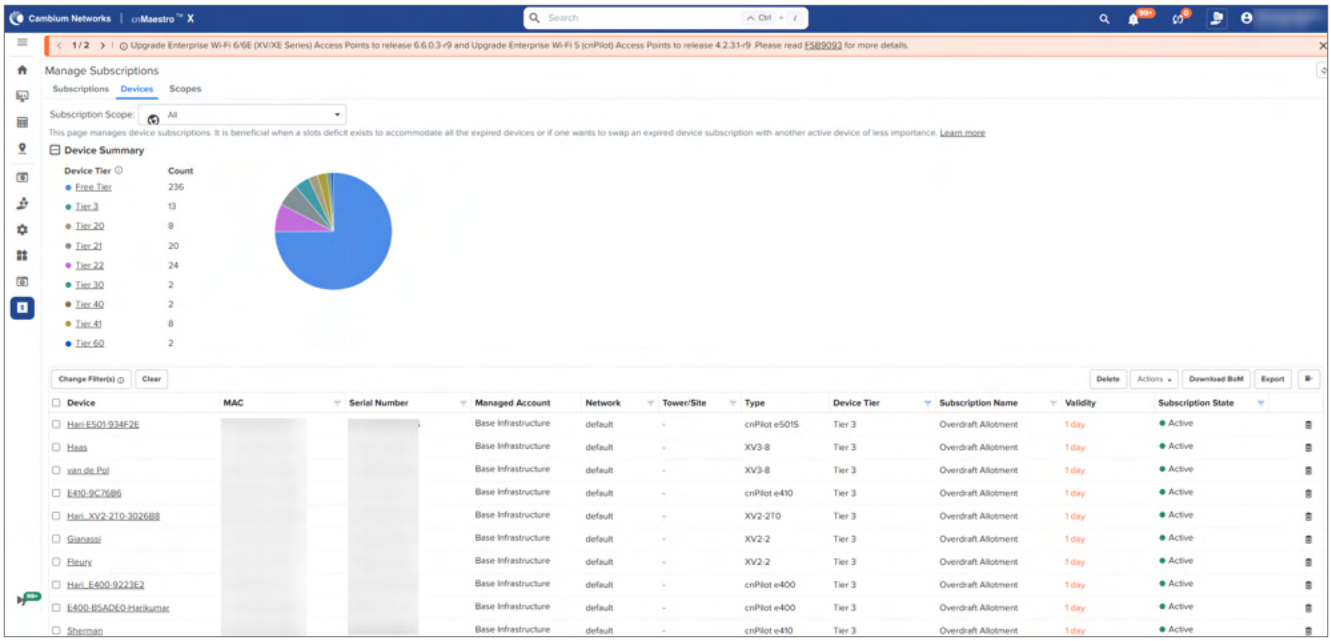
In the **Manage Subscriptions** > **Devices** page, the Overdraft Subscription feature allows newly onboarded devices to operate temporarily without an active subscription when no available slots are found. The overdraft period is assigned automatically, and access is provided for a specific duration determined by the Cambium Networks support team.

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

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

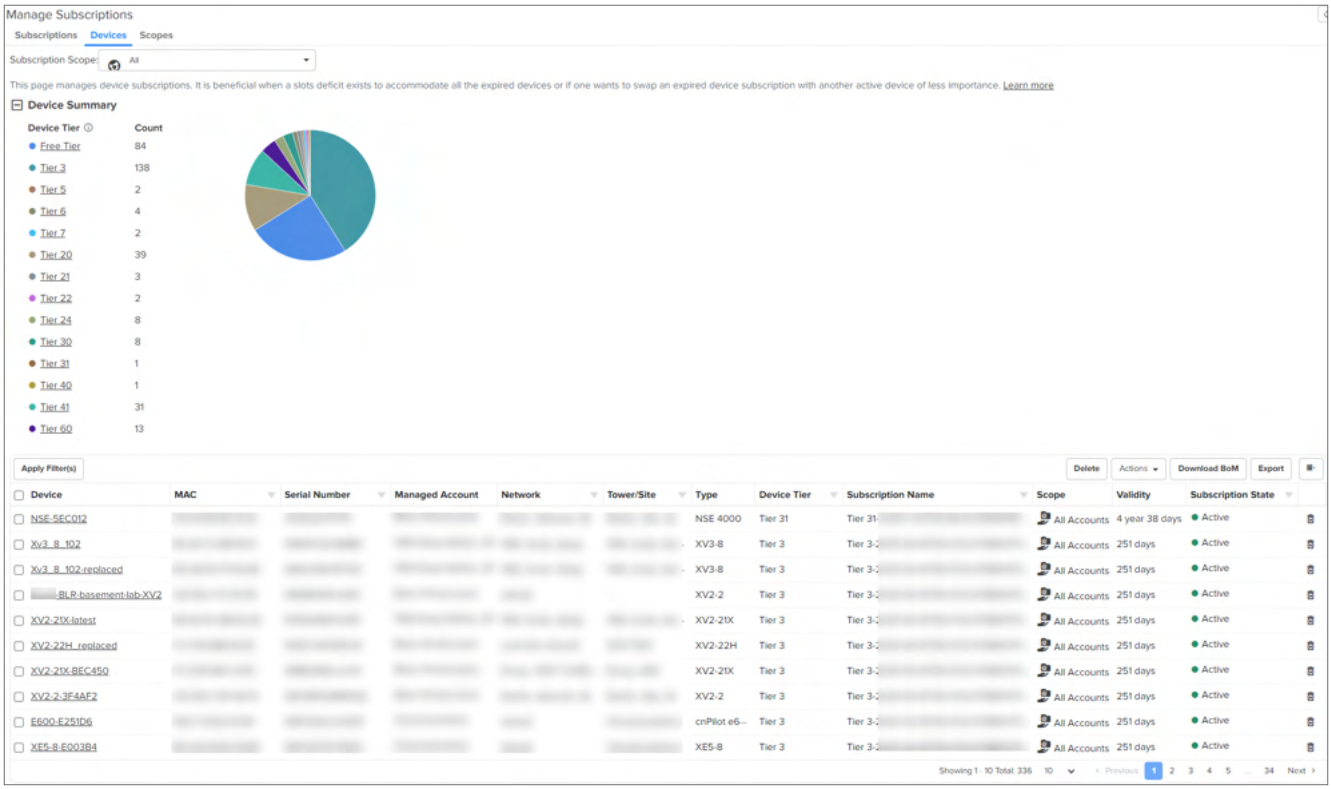


On the Devices page displays the **Overdraft Devices** as shown in the below figure.



Download a Bill of Material (BoM)

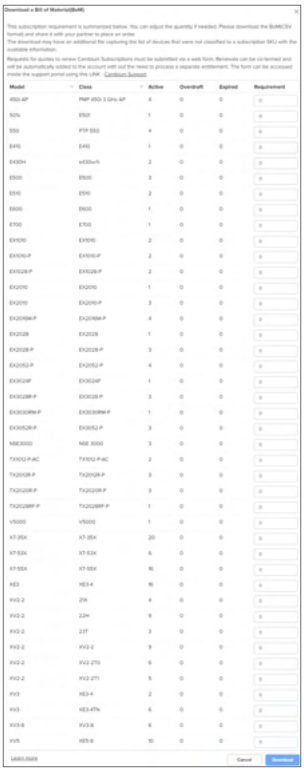
In the **Manage Subscriptions** > **Devices** page, the download BoM feature allows the users to generate a summary of the required subscriptions for an account to upgrade. The downloaded file is used to analyze and determine subscription requirements.



Perform the following steps to download the BoM:

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

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



3. The subscription requirements are generated based on the device model and class.
4. Modify the subscription count, if required.
5. Click **Download** to download the BoM files in the ZIP format.

   Success window pops up.

   The ZIP file contains the BoM files in the CSV format.

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

cnMaestro X features behavior state

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



Note

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

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

Table 8 *cnMaestro X Feature behavior state matrix*

Feature	cnMaestro X	On Downgrading cnMaestro X to Essentials and Data Retention Period	After Data Retention Period
60 GHz cnWave	**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)	**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

Feature	cnMaestro X	On Downgrading cnMaestro X to Essentials and Data Retention Period	After Data Retention Period
	• Interference Scan **High Availability** • Allows configuring a secondary (backup or passive) E2E Controller from cnMaestro		
Administrator Count	Administrator limit increased from 10 to 200.	New users cannot be added if the current count is 10 or more.	Deletes cnMaestro users with the lower privileges in **Super Administrator** > **Administrator** > **Operator** > **Monitor** to maintain 10 users.
API Clients	Create API clients and access tokens	Not accessible	Not accessible
Applications	View details of applications accessed by users in a particular site. This is available for Enterprise Wi-Fi and NSE devices.	• Enterprise Wi-Fi—Not accessible • NSE—Accessible and displays data	• Enterprise Wi-Fi—Not accessible • NSE—Accessible and displays data
Application Visibility	Enables users to control or block applications, or terminate based on consumption of applications.	Not accessible	Not accessible
Assists	Assists helps to isolate configuration issues in a deployment.	Not accessible	Not accessible
Assurance	• 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	Not accessible	Not accessible

Feature	cnMaestro X	On Downgrading cnMaestro X to Essentials and Data Retention Period	After Data Retention Period
	• **Client** dashboard > **Client History** graph displays lifecycle events • **Client** dashboard displays **Connection Success Rate** widget		
Audit Logs	Audit Logs record user activity.	Audit log generation continues through the data retention period, but users cannot access the logs.	Not accessible
Auto-Provisioning	Allows configuring and approving of devices automatically based on IP address.	Not accessible	Not accessible
Base WLAN for Personal Wi-Fi SSID (Part of **WLANs** > **ePSK** configuration)	Allows user to configure personal SSID, password, and VLAN. This disables the local ePSK and the WLAN SSID.	Not accessible	Not accessible
Bulk Edit	• 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. • Application statistics are only available for NSE, XV, XD, XE, and XR series devices.	Not accessible	Not accessible
Configuration Lock	Prevents changes to Wi-Fi AP, cnMatrix, and NSE device configuration, even if the device is updated directly.	The lock is no longer enforced.	Not accessible
Custom Applications	Configure applications with a specific IP address or a domain name, and apply filter rules.	Not accessible	Not accessible
EasyPass	Create captive portal to allow	Configuration will be retained,	cnMaestro X portal types will

Feature	cnMaestro X	On Downgrading cnMaestro X to Essentials and Data Retention Period	After Data Retention Period
	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	but the cnMaestro X portal types will no longer be available.	no longer be available.
Email Notifications	Maximum of 10 email recipients can be added per Managed Account (All Accounts, Base Infra and per MSP)	• All the configured email recipients are retained • None of the email recipients are deleted. • Only the 2 earliest added subscribers per Managed Account would receive email notifications.	Only the 2 earliest added recipients are retained. The remaining email recipients are deleted automatically.
ePSK Limit	ePSK limit increased from 300 to 2000.	New ePSK entries cannot be added if the current count is 300 or more.	Only 300 entries are retained, and the remaining entries will be deleted.
Guest Portal—Access	Connect a wireless service through following access methods: • Paid access • Enterprise: ◦ Microsoft Azure ◦ Sponsored Guests ◦ Self Registration ◦ Google	Configuration will be retained, but the feature will no longer be available.	Not accessible

Feature	cnMaestro X	On Downgrading cnMaestro X to Essentials and Data Retention Period	After Data Retention Period
	• Guests page— Allows to view details of self registered guests connecting to the wireless network.		
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. • Only portal delete option is available to the user. • All existing client sessions will continue without any disruption.	Only 4 portals will be retained and rest will be deleted.
Graphical Reports Template	• **Assurance** (Only at the Site-level)—Top Access Points Reporting Client Disconnections, Top Client Connection Failures, Top Affected Client OS by Failure Count, Top Affected Client Types by Failure Count • **Access Points**—Top Access Points by Traffic Usage • **Clients**—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	Not accessible.	Not accessible.

Feature	cnMaestro X	On Downgrading cnMaestro X to Essentials and Data Retention Period	After Data Retention Period
	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	Installation summary of PMP and ePMP SMs, cnMatrix, and Enterprise Wi-Fi APs installed using the Installer mobile application.	Not accessible	Not accessible
Layer 7 (Application Filtering) (Part of **Wi-Fi Profiles** > **Access Control Policies** > **IP and Application Filtering Rules**)	Filter individual applications or applications belonging to a category.	Not accessible	Not accessible
Long term Historical Data	Displays the devices performance graph: • Performance graphs for Wi-Fi APs and cnMatrix 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.

Feature	cnMaestro X	On Downgrading cnMaestro X to Essentials and Data Retention Period	After Data Retention Period
	• 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.		
Managed Services	Provides separate Managed Accounts – each 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 Plan	Allows to create 50 floor plan per site.	• All floor plans are viewable as read-only. Cannot create additional floor plans or edit any existing floor plans if more than one configured in a Site. • Edit is available only when all additional floor plans are deleted.	• Additional floor plans is deleted and devices on those floors is unmapped. • Only the latest floor is available.
Reports	Schedule Devices, Performance, Active Alarms, Alarm History, Events, Clients, Mesh Peers, and Guest Access Login Events Reports.	Reports tab will not be accessible, and all previously scheduled reports will be skipped.	All jobs will be terminated and Reports are not accessible.

Feature	cnMaestro X	On Downgrading cnMaestro X to Essentials and Data Retention Period	After Data Retention Period
Satellite View	It allows to view maps in Satellite view.	Not accessible	Not accessible
Session Management	Tracks the current cnMaestro user sessions and optionally allows to logout cnMaestro user sessions.	Not accessible	Not accessible
Spectrum Analyzer	Analyzes and monitors the wireless spectrum for 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
Terrain View	It allows to view maps in Terrain view.	Not accessible	Not accessible
Wireless Intrusion Detection System (WIPS)	Protect wireless networks from unauthorized access and potential security threats. • WIDS data is processed • APIs are supported	Statistics is not available through API	Not accessible
Wireless Intrusion Prevention System (WIPS)	Enhances security of wireless networks by deauthenticating rogue APs and clients. • 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:

- Navigating the cnMaestro UI
- Account View
- Home page
- Page structure
- Page navigation
- Access and Backhaul View
- Enterprise Account view
- Side menu
- Section tabs
- System status
- Data Tables and Chart UI Controls
- Logout

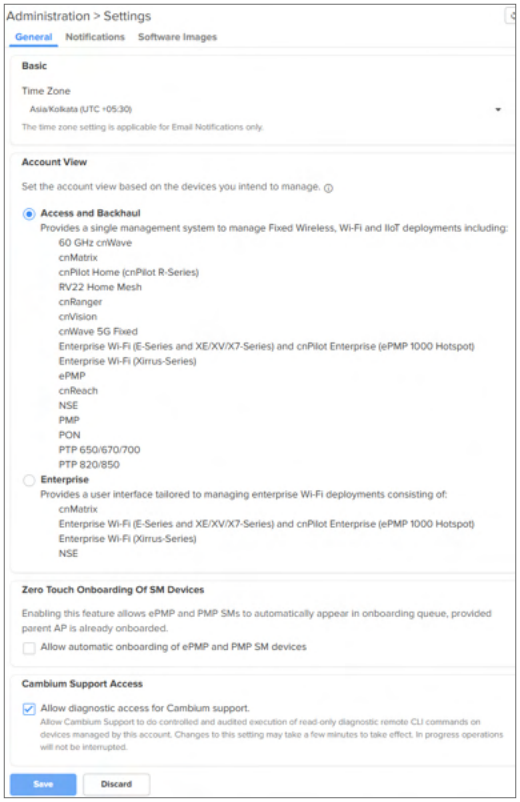
Account View

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

- Access and Backhaul view
- Enterprise view

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

Figure 28 *Account View*



Access and Backhaul view

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

Enterprise view

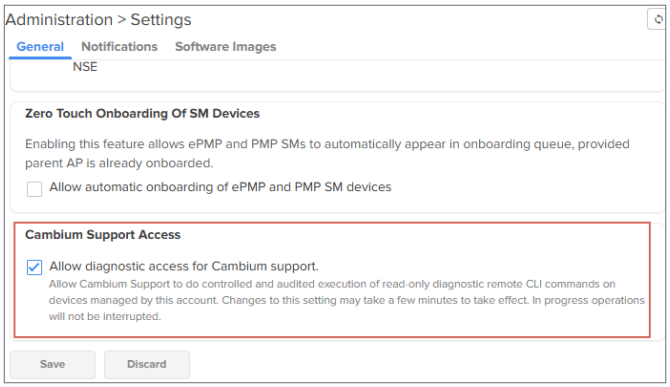
The Enterprise View supports the Enterprise Wi-Fi portfolio, which includes the cnPilot Enterprise APs, cnMatrix, and Enterprise Wi-Fi APs (E-Series, and XE/XV/X7-Series), and Enterprise Wi-Fi (Xirrus-Series), and NSE. It provides a simplified UI for Wi-Fi components (hiding fixed wireless features such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

User consent to allow device diagnostic access to Cambium Support

Once enabled, this option allows Cambium Support Team to access the device and execute diagnostic CLI commands. Audit logs are generated whenever the Customer Support executes a CLI command.

To enable this option, navigate to the **Administration** > **Settings** > **General** page and select the **Allow diagnostic access for Cambium support** checkbox.

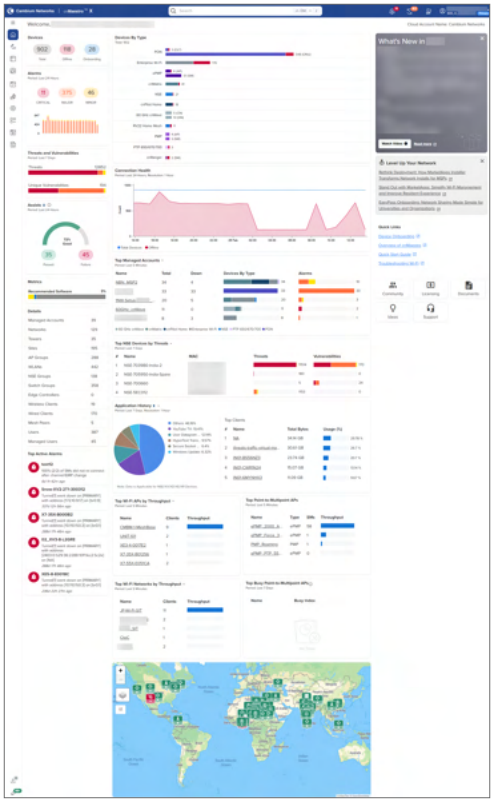
By default, this option is disabled for all accounts.



Home page

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

Figure 29 *cnMaestro Home page*



Page structure

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

Figure 30 *cnMaestro page structure*

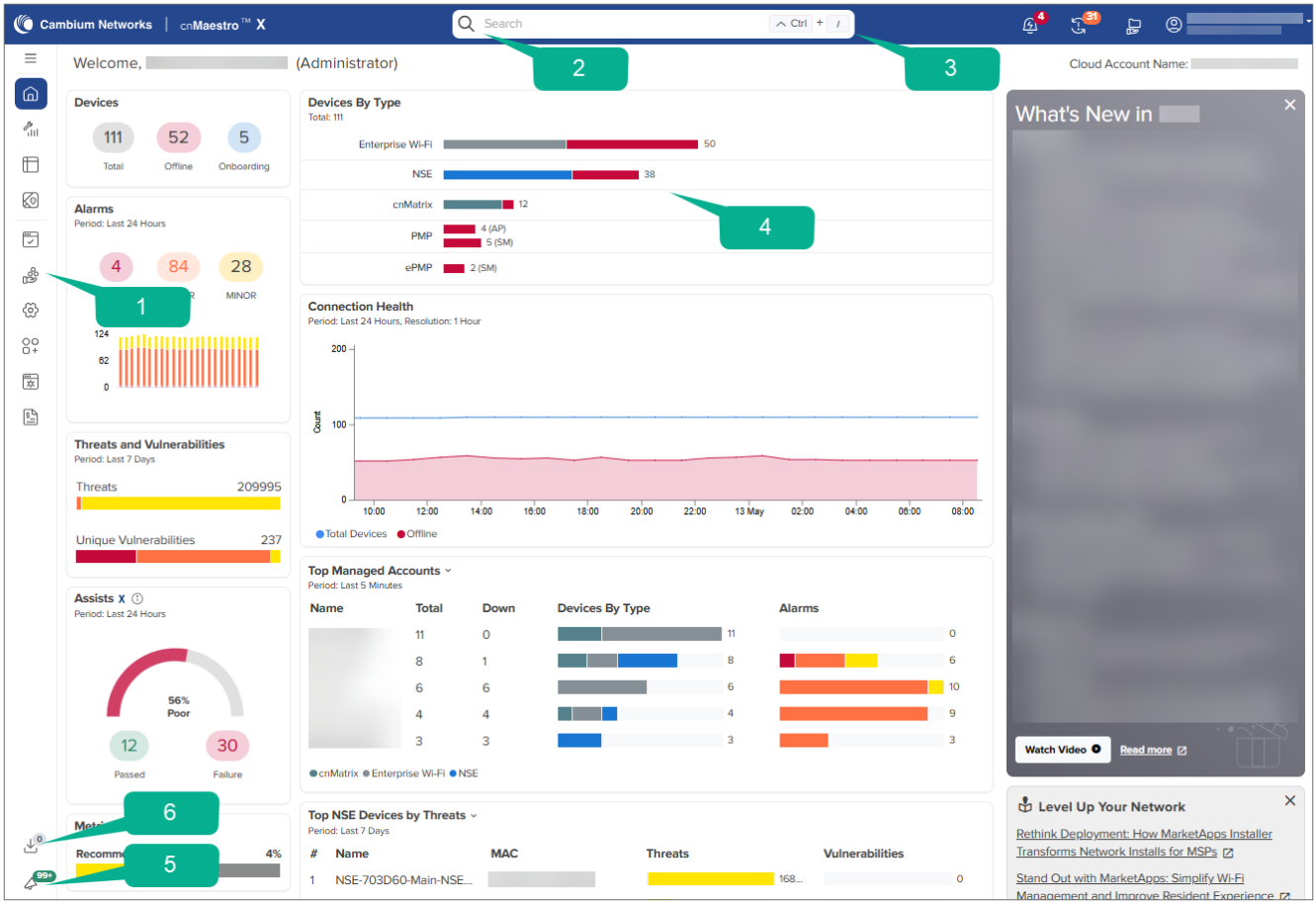
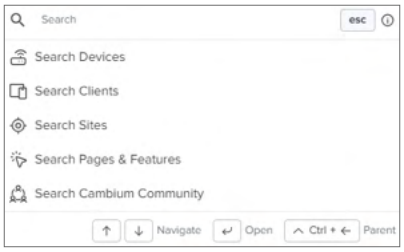


Table 9 *UI description*

Number	Elements	Description
1	Left menu	Shows the functional areas of the UI. This menu can be expanded or collapsed to view the submenu by clicking the top arrow.
2	Header	Shows the basic counters for **Major Alarms**, **Devices Awaiting for Approval**, **Software Updates Jobs**, and **Out of Sync Devices**, 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

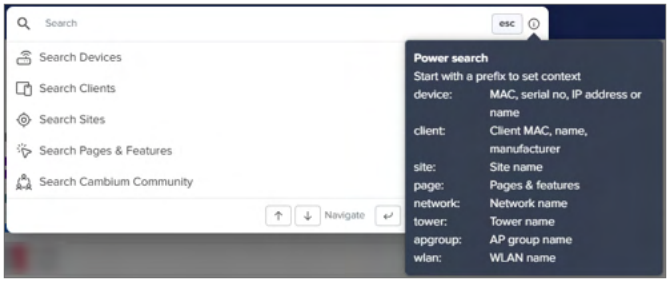
The Search bar at the top of the cnMaestro homepage allows users to easily search for and access cnMaestro resources, such as, onboarded devices, unmanaged devices, clients, sites, pages or features, and community posts. You can also search for towers, networks, WLANs, and AP groups.



- **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.

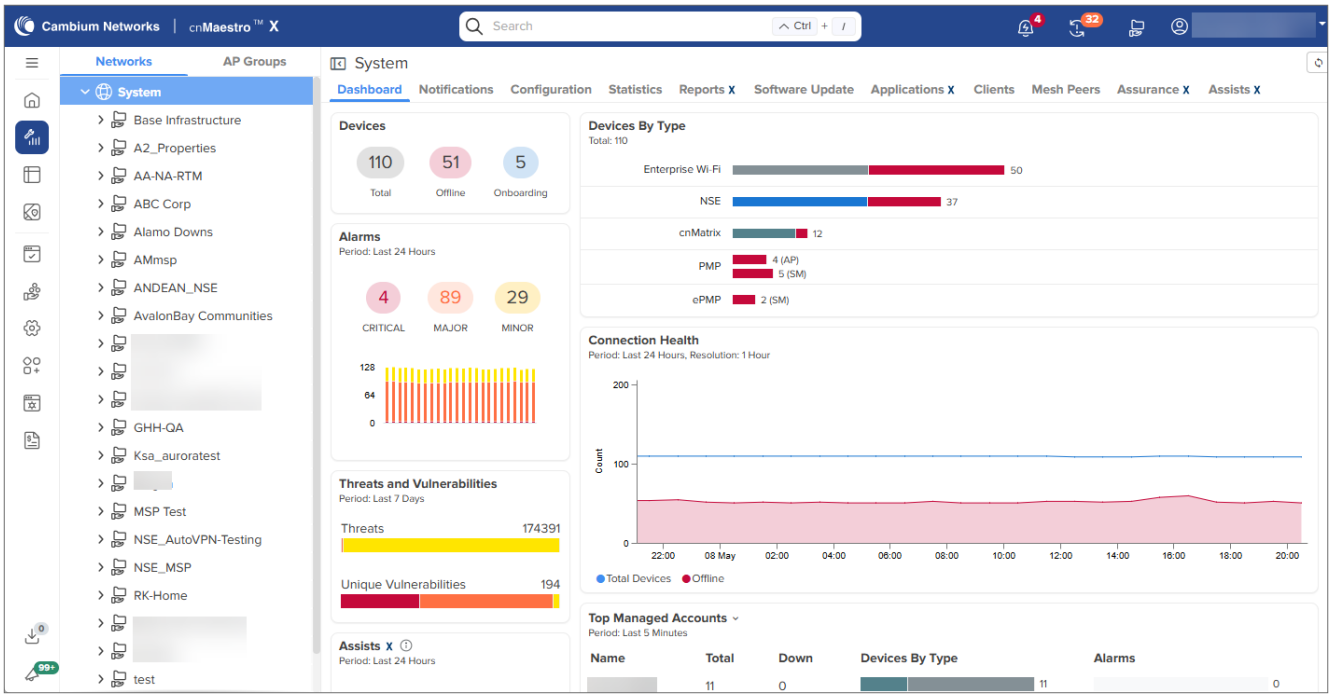
Users can also perform a power search by using certain predefined prefixes so, so as to set the context of the search, as shown below:

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 12.



Access and Backhaul View

Overview

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

Networks tab

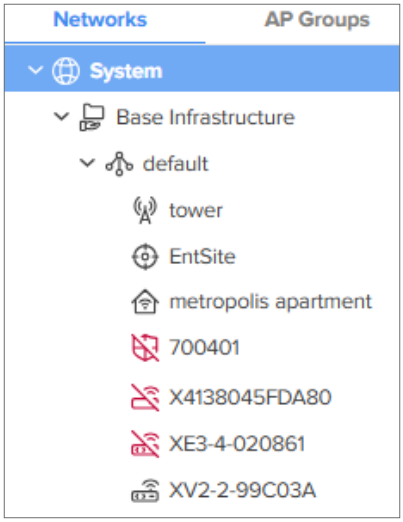
The **Network** tab displays a hierarchical view of the devices. It consists of Systems, Networks, Towers, Sites, and Devices. There is a strict ordering for how nodes can fit in the hierarchy, and as one navigates through and selects nodes, the pages display the node chosen.

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

Note

- Towers are only visible in the Fixed Wireless view and 60 GHz cnWave devices are only visible in the 60 GHz cnWave E2E Network. cnMatrix devices are visible only in 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 31 *Networks*



The structured hierarchy has the following nodes:

Table 10 *Structured hierarchy nodes*

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

Table 10 *Structured hierarchy nodes*

Icon	Name	Description
	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	cnPilot Home (R-series) devices are generally matched to a local SM and inherit its Network. They can also be mapped standalone to a Network or a Site.
	cnVision Client	cnVision Client Subscriber Modules are located in a Network (if they are standalone, which is only used for bootstrapping) or they are associated with an AP. The SM will inherit the Network and Tower of the AP to which it is associated.
	cnVision Hub	cnVision Hub are located in a Network and are optionally mapped to a Tower.
	cnWave 5G Fixed BTS	cnWave 5G Fixed BTS devices are located within a Network.
	cnWave 5G Fixed CPE	cnWave 5G Fixed CPE devices connected through cnWave 5G Fixed BTS device in a Network.
	Enterprise Wi-Fi	Enterprise Wi-Fi devices are generally matched to a local SM and inherits its Network. They can also be mapped standalone to a Network or to a Site.
	ePMP AP	ePMP Access Points are located in a Network and are optionally mapped to a Tower.
	ePMP SM	ePMP Subscriber Modules are located in a Network (if they are standalone, which is only used for bootstrapping) or they are associated with an AP. The SM inherits the Network and Tower of the AP to which it is associated.
	Home Site	Home sites are located within networks and contain cnPilot Home Router (r-series) APs and Home Mesh routers.
	Managed Account	Managed Accounts group cnMaestro devices and configuration objects (such as AP Groups, WLANs, and Sites) into independent administration domains within a single cnMaestro.
	Network	All devices are placed within Networks. Networks represenst the geographical regions or collections of devices with a shared responsibility. Accounts can have one network or many networks. Networks allow one to provide structure to accounts with many devices and also provides aggregation buckets for cnMaestro statistics (essentially the system pre-calculates statistics, so they are displayed quickly).
	NSE (3000 and 4000)	NSE device located in the Network.
	OLT	Optical Line Terminal (OLT) device located in the PON network
	ONU	Optical Network Unit (ONU) device located in the PON network.

Table 10 *Structured hierarchy nodes*

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

Default network

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

Tree menu

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

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

Table 11 *Tree menu*

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

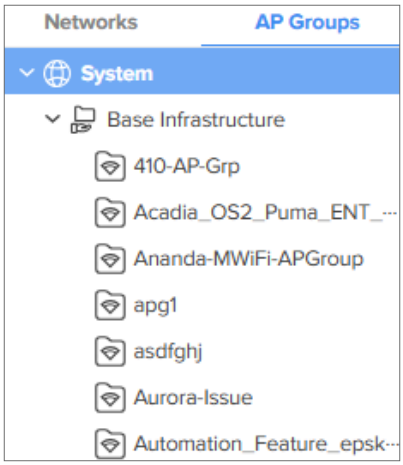
Table 11 *Tree menu*

Action	Node	Description
Actions specific to PON Network		
Sync Topology	Network	To sync the topology of PON devices (OLT/ONU).
Actions specific to Enterprise Wi-Fi AP and cnMatrix devices		
Replace Device	Network, Site, Tower	Replace offline or faulty Enterprise Wi-Fi APs or cnMatrix switches. • The new device will inherit the configuration of the old device. • You can either keep or delete the old device by selecting the checkbox in the **Replace Device** window. For more information, refer Replacing Devices.

Wi-Fi AP Groups tab

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

Figure 32 *Wi-Fi AP Group tab*



Map navigation

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

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, PTP, and RV22 Home Mesh at the site- and device-levels.

Figure 33 *Map navigation*

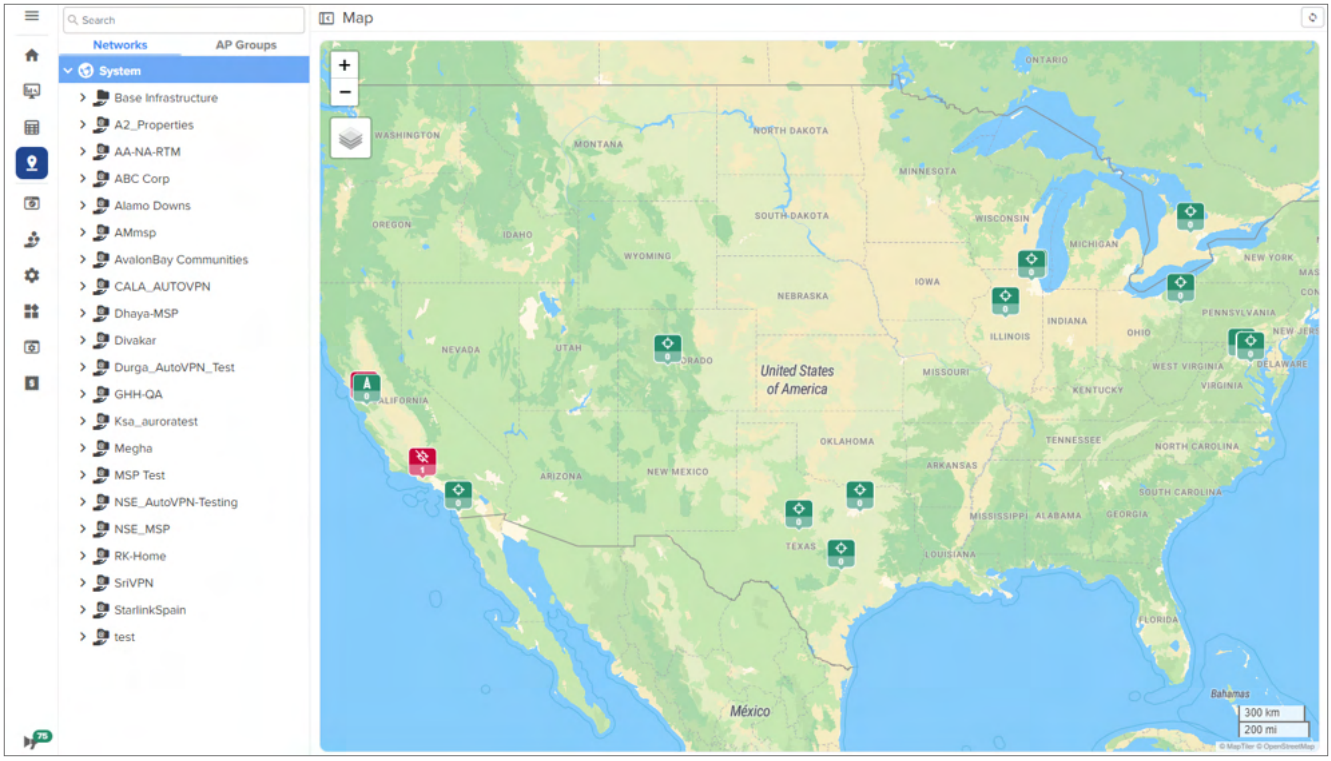


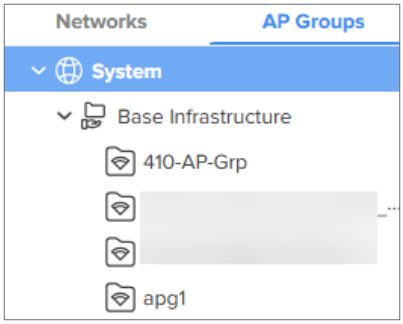
Table navigation

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

Node search

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

Figure 34 *Node search*



Enterprise Account view

Overview

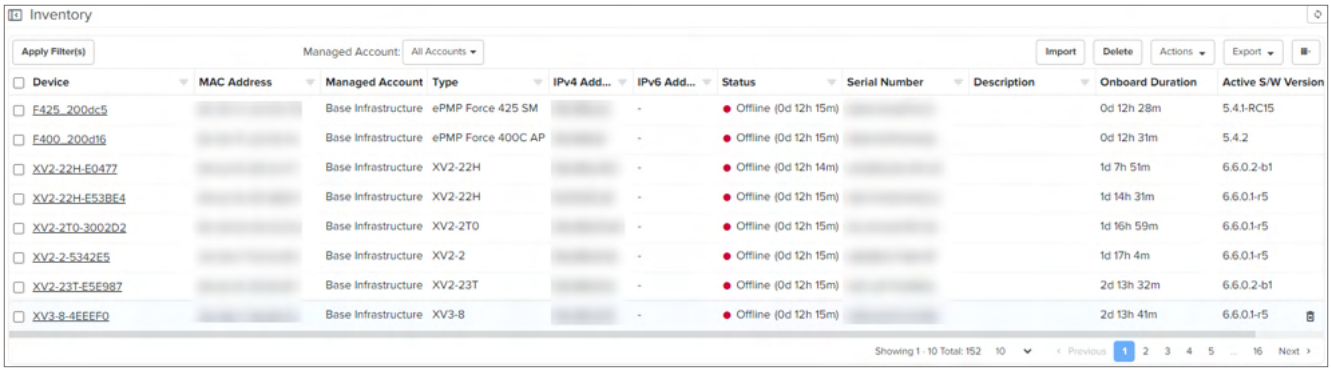
The Enterprise account differs from Access and Backhaul in that it is largely table-driven. It does not have the Quick Buttons or the Device Tree, instead, it has direct navigation for Devices, AP Groups, WLANs, Switch Groups, and Sites. Each of these is presented in tabular form.

System

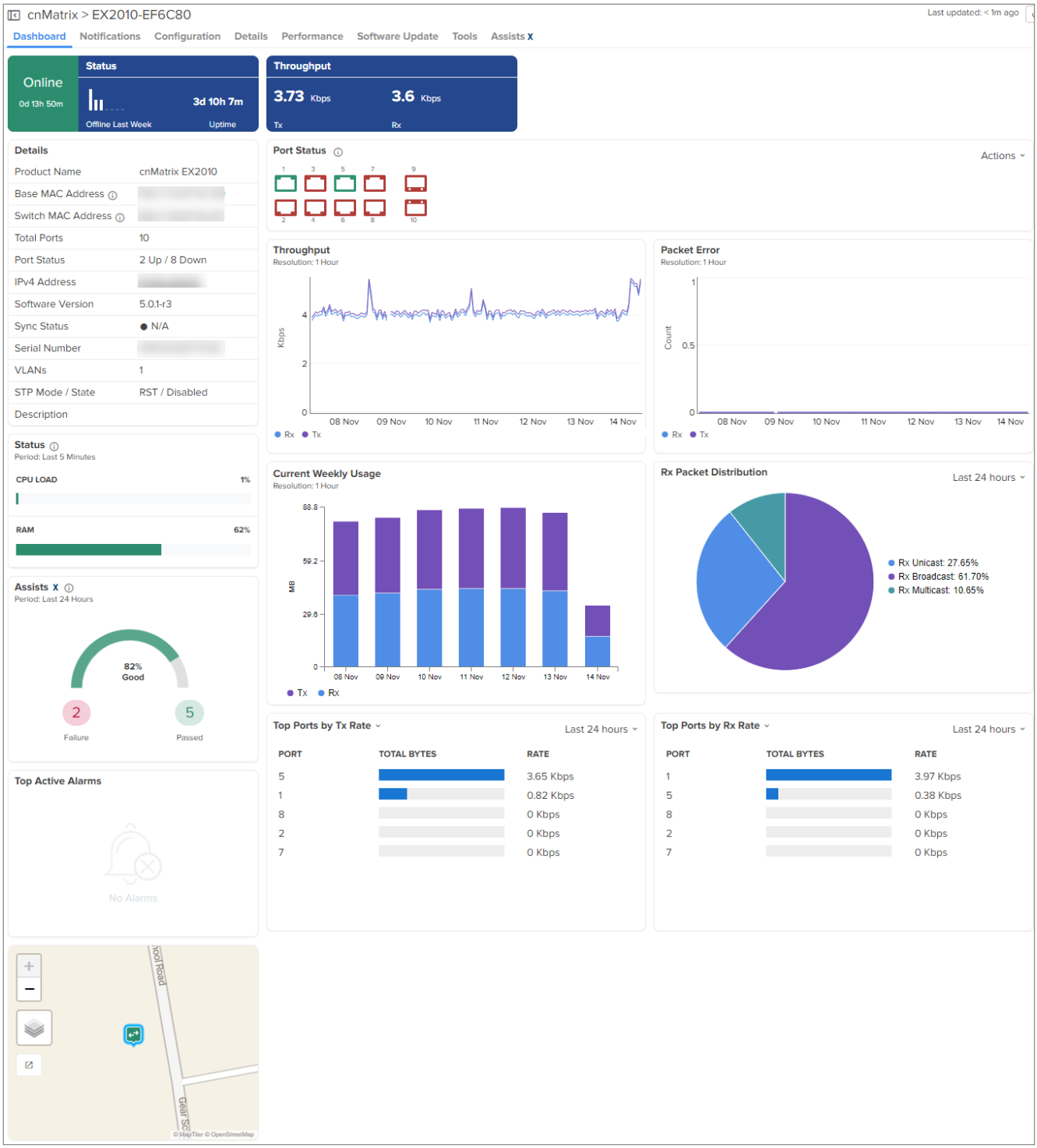
Global functionality is presented in the System menu. It aggregates data across the entire installation.

Devices

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



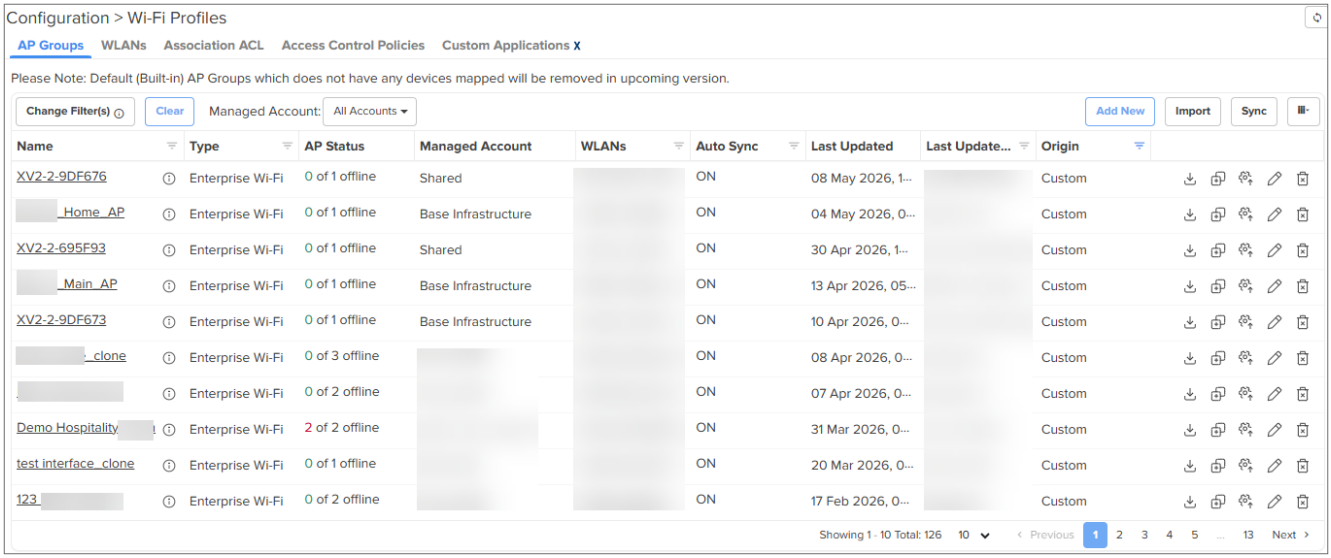
Selecting a device launches its management page.



AP Groups

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

Figure 35 *AP Groups*



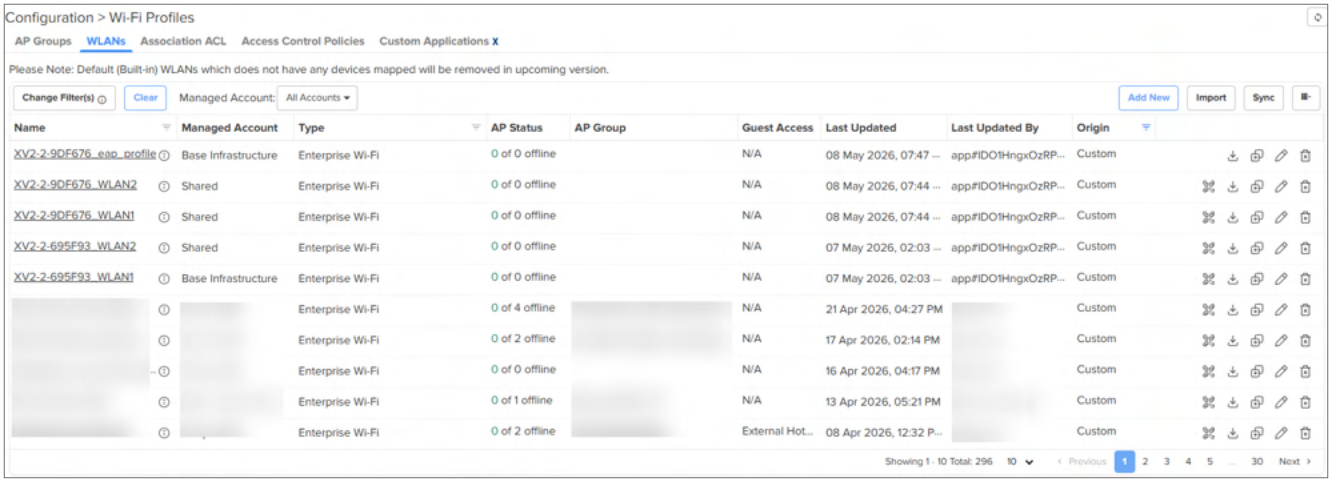
WLANs

WLANs manage shared configuration across APs.

Note

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

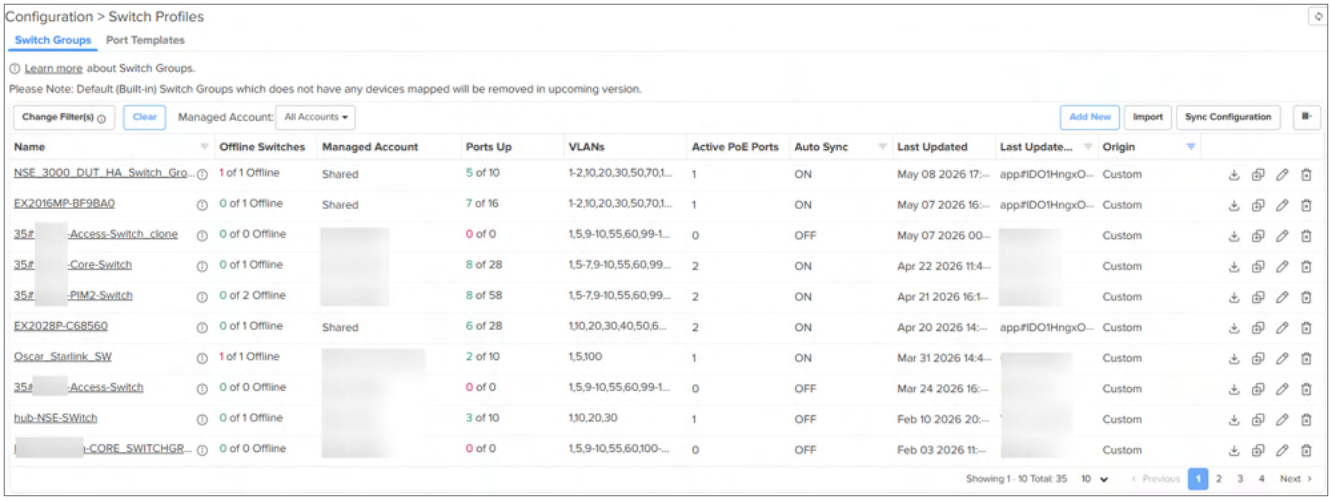
Figure 36 *WLANs*



Switch Groups

Switch Groups provide shared configuration for cnMatrix devices, and a subset of parameters that can be overridden for each device. Administrators can simultaneously edit ports (individually or in bulk) across all physical switches mapped to a switch group.

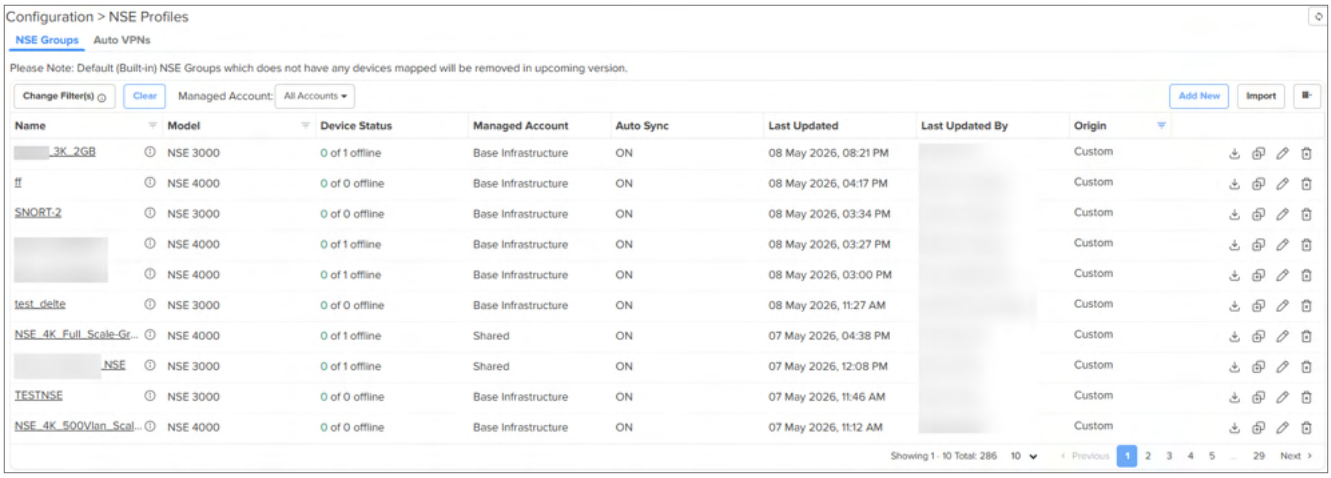
Figure 37 *Switch Groups*



NSE Groups

NSE devices are configured by creating configuration profiles called NSE Groups.

Figure 38 *NSE Groups*



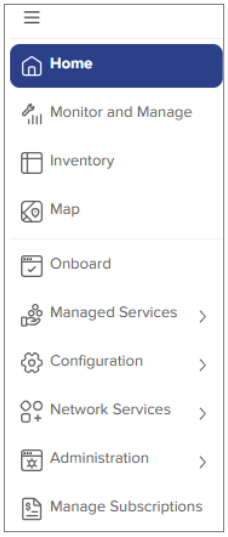
Sites

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

Side menu

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

Figure 39 *Side menu*



Section tabs

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

Table 12 *Section tabs*

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

System status

The UI header has the following System status icons.

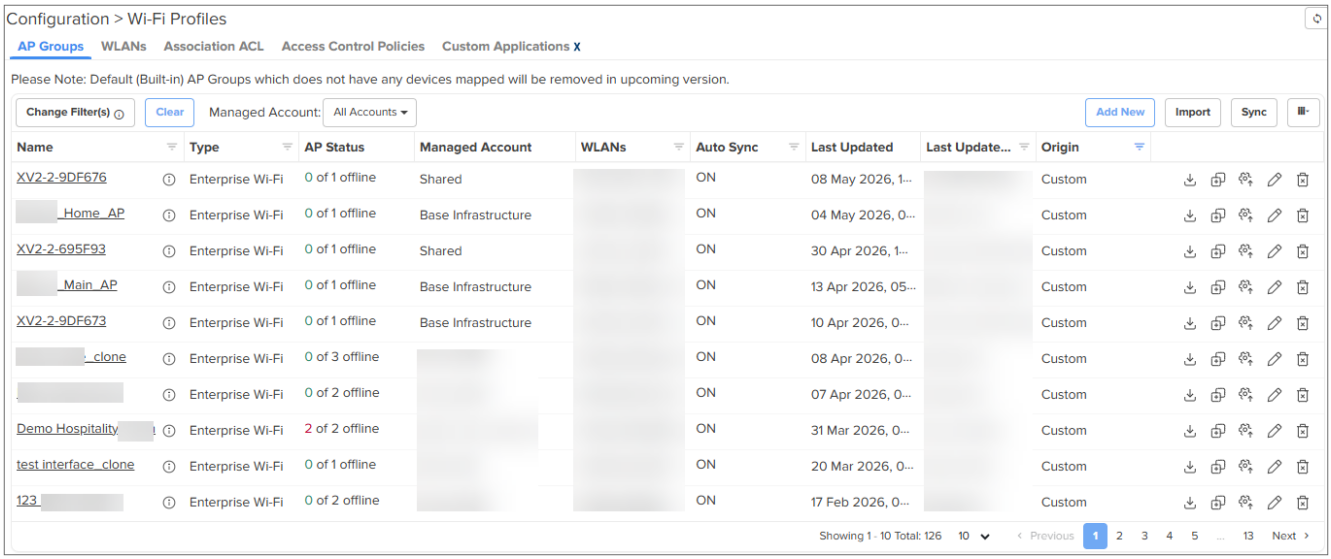
Table 13 *System status icons*

Icon	Name	Description
	Announcements	Notifies the latest Device Software images, Package, or OVA to upload from Cloud.
	Major Alarms	The count of critical and major alarms raised in the system.
	Out-of-Sync Devices	The number of Wi-Fi, NSE, 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**.



Device Onboarding

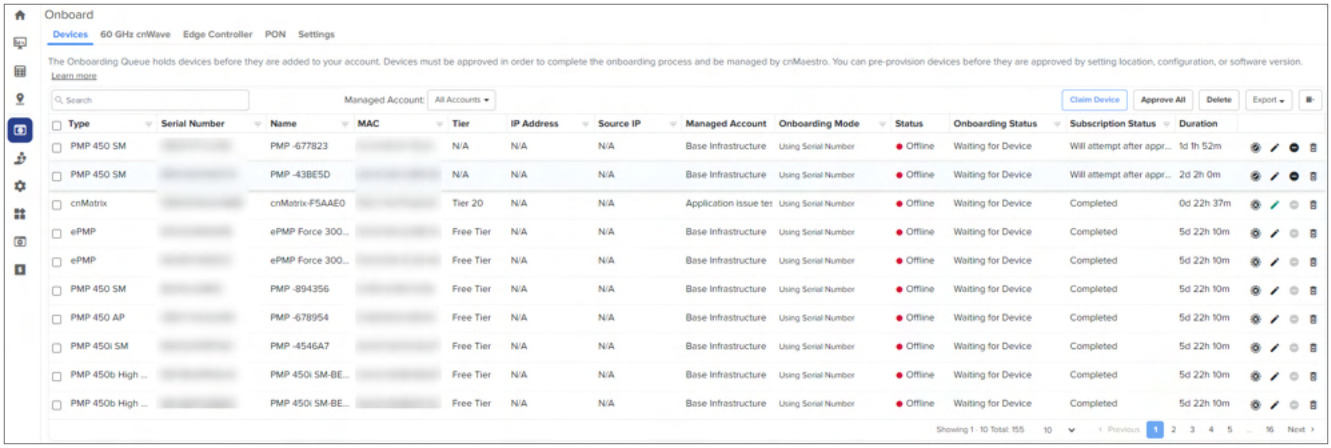
Onboarding is the process of adding a device into cnMaestro Cloud management.

This section includes the following:

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

Onboarding Overview

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



Claiming Devices

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

Note

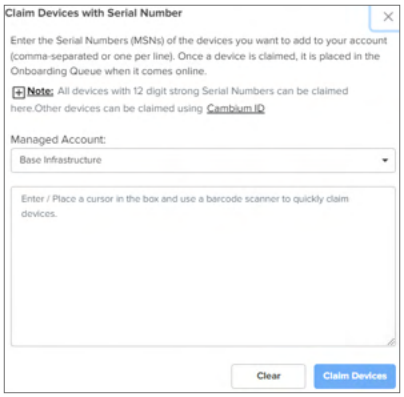
- Only serial numbers with a length of 12 characters can be claimed through the Cloud management UI.
- Devices with serial numbers less than 12 characters for example, 10 or 11 characters, need to be claimed on the device UI using the Cambium ID.

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

Claiming Devices with Serial Number

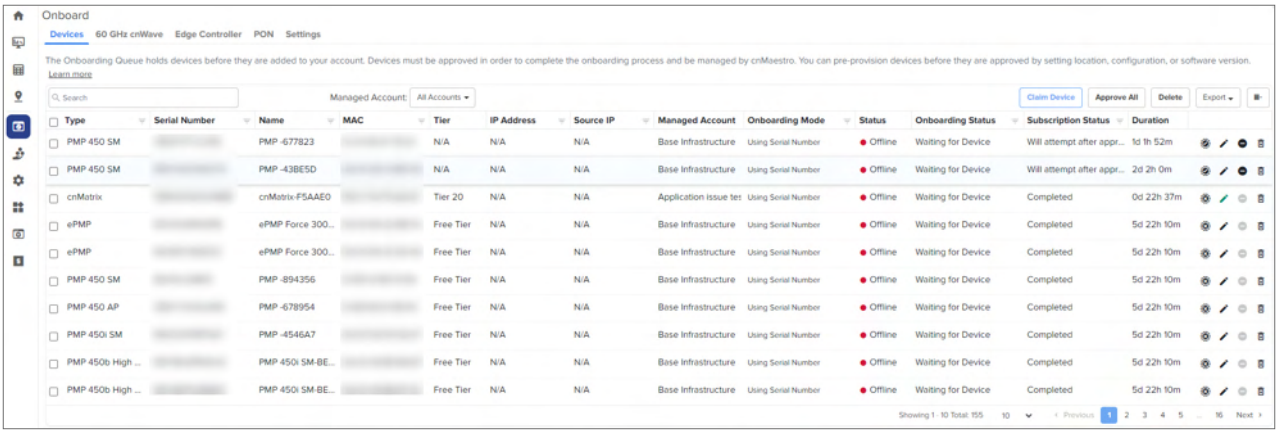
Claiming with Serial Number means entering the serial numbers of devices, one per line, and clicking the **Claim Devices** button. The system prompts the user to validate the devices before applying them. When complete, they will be placed into the onboarding queue, where they can be pre-provisioned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

Figure 40 *Claiming Devices with Serial Number*



To claim a device using the Serial Number:

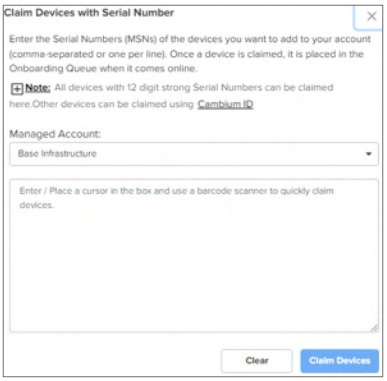
1. Navigate to **Onboard** page > click **Claim Device**.



Claim Devices with Serial Number window appears.

Note

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



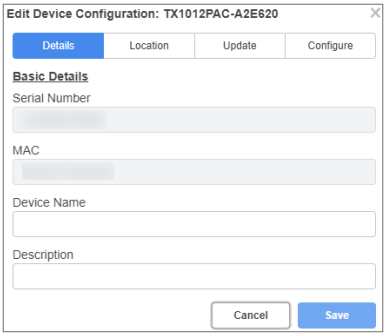
2. Enter the serial number of the device.
3. Click **Claim Devices.**

> **Note**
>
> Slot availability is available only for cnMaestro X account users.

4. The device appears on the onboarding page.

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

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



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

     You can edit only the device name and description parameters.

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

     You can edit all parameters in this tab.

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

5. Click **Approve**.

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

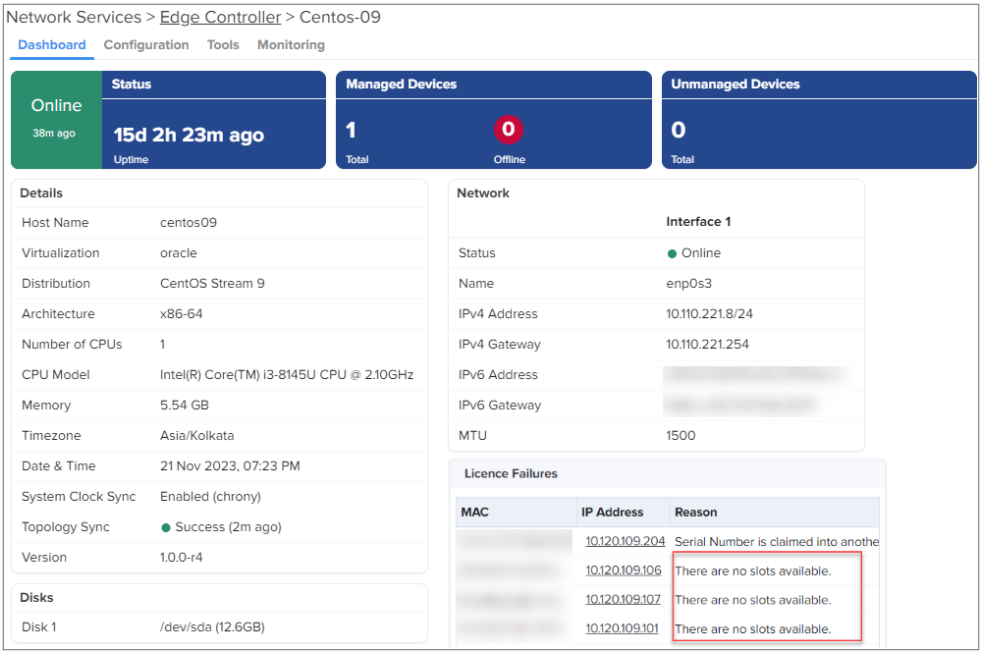
   New devices periodically query cnMaestro Cloud to see if they have been claimed (it generally takes between 1 to 15 minutes to show up in an account, depending upon when the device was last rebooted). Once a device has been added to a Cloud management account, it will be visible in the Onboarding Queue.

Note

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

- **Not Enough Slots available in PTP 820/850 devices**

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



Approving Devices

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

Note

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

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

Claiming Devices with Cambium ID

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

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

Table 14 *Types of Claiming Devices with Cambium ID*

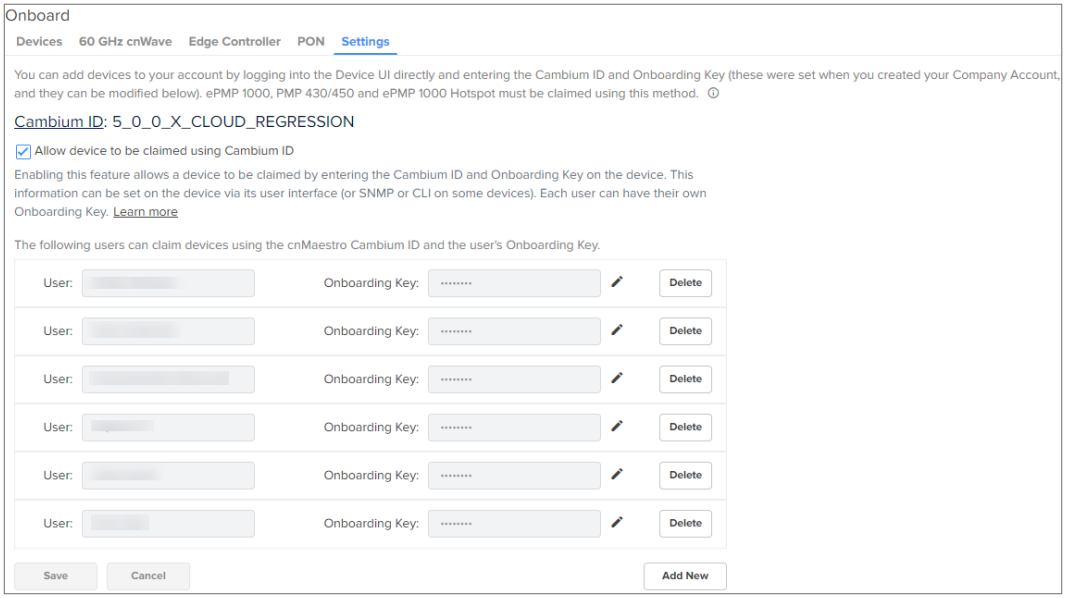
Type	Description
Device UI	Enter the Cambium ID/Onboarding Key directly into the device UI. This prompts the device to access Cambium Cloud and be placed in the onboarding queue.
Device SNMP	The Cambium ID/Onboarding Key can also be entered into the device over SNMP. This allows one to quickly onboard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

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

Cambium ID Configuration

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

Figure 42 *Cambium ID Configuration*



Cambium ID Onboarding Key

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

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

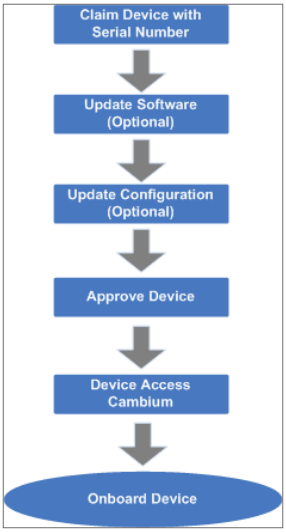
Onboarding Queue

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

Serial Number flow

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

Figure 43 *Serial Number flow*



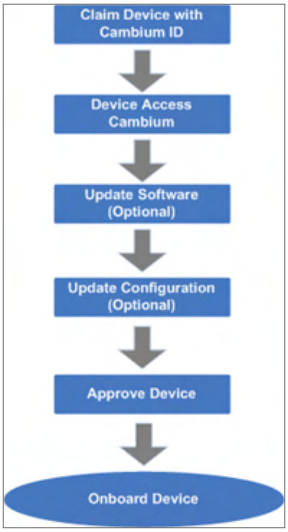
Note

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

Cambium ID flow

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

Figure 44 *Claiming Devices Using Cambium ID*



Onboarding fields

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

Table 15 *Onboarding fields*

Parameter	Description
Actions	Before a device is onboarded, it must be approved. There are two buttons available: • **Approve**: Click **Approve** to enable the device for onboarding. If the device is connected, it will be onboarded immediately. • **Delete**: If the device has been added in error, you can delete it from the Onboarding Queue. This also disconnects the device and allows it to be added to another account. The Delete button is only enabled before the device has started the onboarding process.
Added By	The user who added this device for onboarding. **Note**: If the Device is claimed by a tenant user, the user information is not shown on the Onboarding page.
Configure	This highlights configuration that is applied to the device before onboarding. It is presented as a set of icons that represent: software update, configuration update, and map placement. The icons have the following colors: • Gray: Indicates that nothing is applied. • Green: Indicates that the parameter is set and applied when onboarded.
Device	The name of the device. This is set manually, or, if unset, it will be read from the device.
Duration	Displays when the status last changed for the device.
IP Address	The IP address of the device. This is only available after the device contacts cnMaestro.
MAC Address	The MAC address of the device (if known).
Serial No	The Serial Number of the device.
Status	The current status of onboarding:

Table 15 *Onboarding fields*

Parameter	Description
	• **Waiting for Approval:** The device has contacted cnMaestro, but it has not been approved, so it is in a waiting state. • **Waiting for Devices:** The user has claimed the device, but the device has not connected. • **Onboarded:** The device has completed onboarding and must now be managed through normal Configuration and Software Update processes.
Type	The type of the device (if known or manually configured).

Onboarding Configuration

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

The color icon indicates the following:

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



Note

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

Basic Details

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

Configure Device

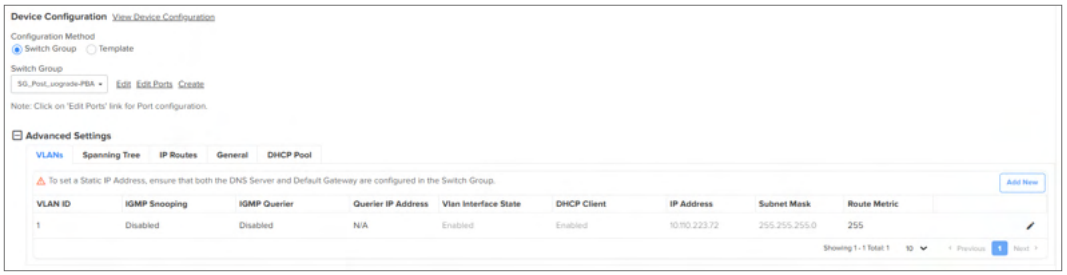
Configure Device follows the standard template system (see the section on Template Configuration for full details). The administrator can select an existing configuration template and set any required variables.

cnMatrix Configure Device

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

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

- General
- IP Routes
- Spanning Tree
- VLANs



Software Update

Software Update pushes a software image to the device. The administrators can select an image version and push to all ePMP (AP or SM) device selected in a job.

Device Location

The Device location configuration includes Network, Tower, Latitude, and Longitude on a map.

Onboarding Actions

Approve Device

An administrator needs to approve devices before onboarding can begin. This is done by selecting Approve. As soon as a device is approved, it is eligible to start the onboarding process. This occurs immediately with connected devices. Any changes to the Onboarding Configuration need to be completed before Onboarding begins; the Approval check must also be disabled.

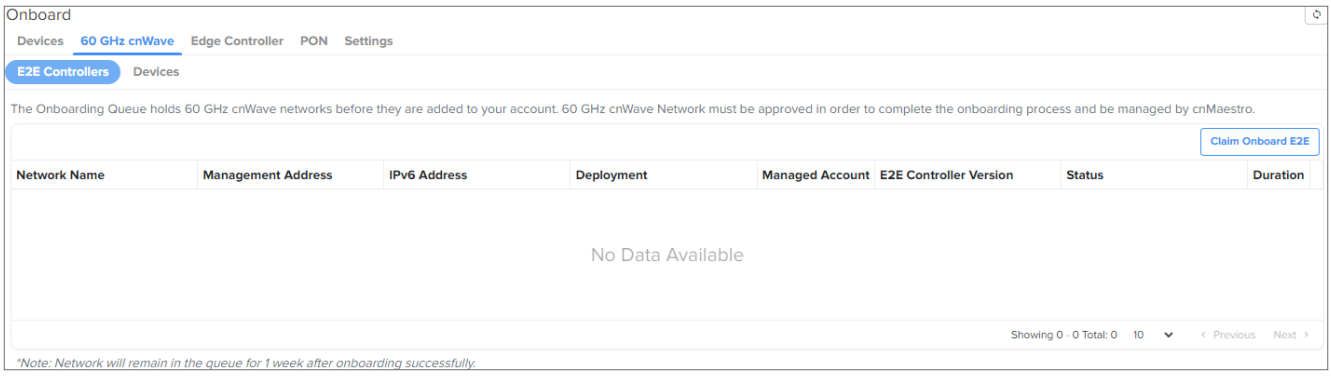
Delete Device

Devices deleted from the Onboarding Queue are removed from Cloud management. They can then be added to other accounts. See below for how to delete devices that have already onboarded.

60 GHz E2E Controller Onboarding

The 60 GHz cnWave networks are listed in the onboarding queue under on the Onboard > 60 GHz cnWave > E2E Controllers page. These networks must be approved before you can manage the networks and the corresponding the 60 GHz cnWave devices using cnMestro.

This approval can be done either through the Onboarding Queue or the Hierarchical Tree (where the E2E Network is placed).



Note

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

For information about onboarding E2E devices, refer to Onboarding 60 GHz cnWave devices.

For information about onboarding Edge Controller and PTP 820/850 devices, refer to Onboard Edge Controller and Onboard PTP 820/850 devices.

Header Notification

The header bar in cnMaestro displays the following UI controls:



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

Zero Touch Configuration

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



Claiming Your First Wi-Fi AP (Cloud)

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

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

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

Figure 45 *The Claim Your First Wi-Fi AP option*

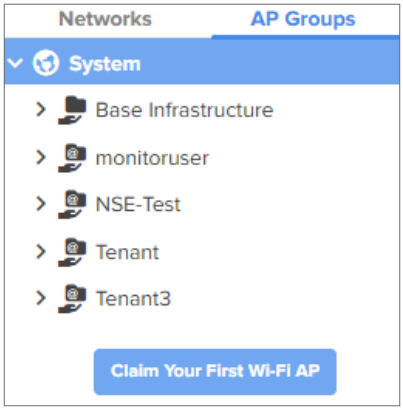
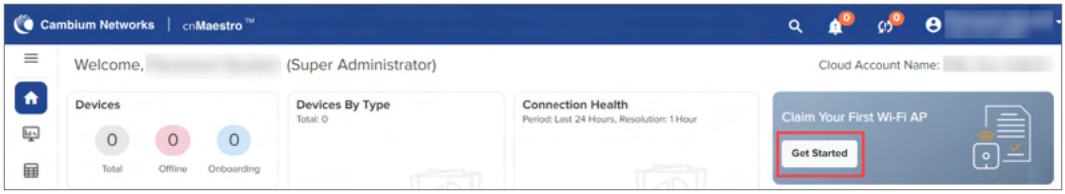


Figure 46 *The Claim Your First Wi-Fi AP widget on the Home page*



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

Claiming a single Wi-Fi AP from the Home page

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

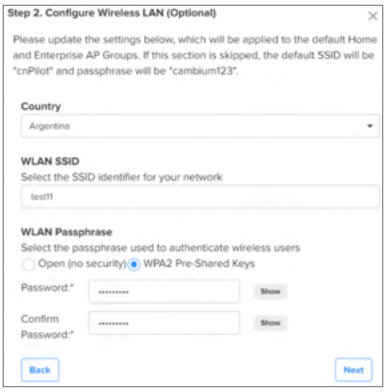
1. On the main **Home** page, locate the **Claim Your First Wi-Fi AP** widget on the right side of the page and click **Get Started** (as shown in Figure 46).

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

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

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



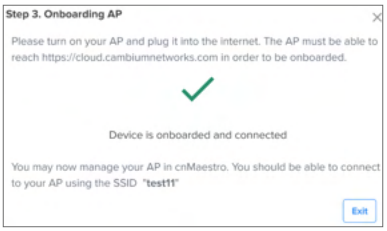
You can update the following settings based on your requirements.

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

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

3. Click **Next**.

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



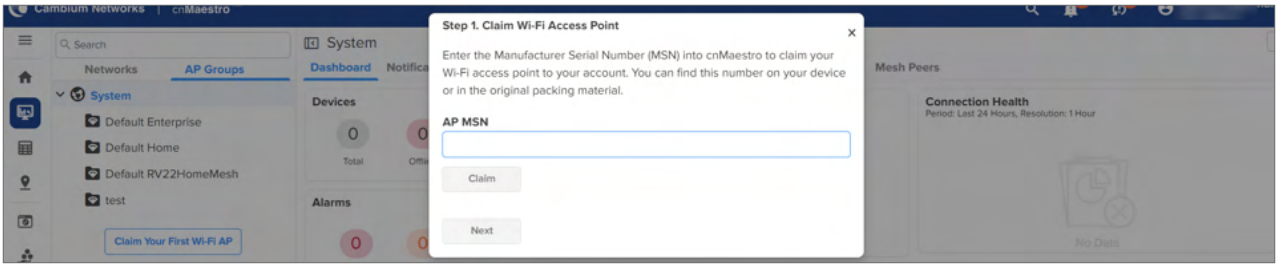
   If the onboarding fails, the **Onboarding AP** screen displays a message indicating the failure status.

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

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

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

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



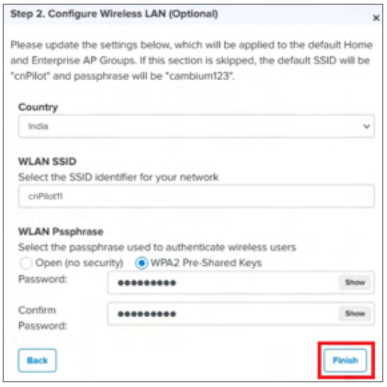
2. Enter a valid value in the **AP MSN** text box and click **Claim**.

The device is successfully claimed.

3. Click **Next**.

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

4. Enter the configuration details.



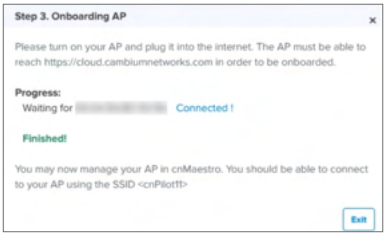
   You can configure the following settings based on your requirements:

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

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

5. Click **Finish**.

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



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

Claiming multiple Wi-Fi APs from the AP Group

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

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



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

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

Note

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

Figure 47 *Example CSV file to include the device name*

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

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

Note

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

Claiming multiple Enterprise devices from the Enterprise Site dashboard

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

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

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

Figure 48 ***Claim Enterprise Devices*** *window*



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

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

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

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

   For more information on claiming Enterprise devices using CSV files, see Claiming multiple Enterprise devices 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 49 *Example CSV file to include the device name*

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

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

Claiming multiple Enterprise devices using CSV import

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

Note

- The CSV import option is available only for cnMatrix and Enterprise Wi-Fi APs.

  CSV import option is not applicable to NSE devices.

- Also, by default, only one NSE device can be imported by adding the serial number in the box provided. To import multiple devices, High Availability (HA) must be enabled in the NSE devices.

Importing multiple NSE devices is allowed only by adding serial numbers in the box provided.

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

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

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

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

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

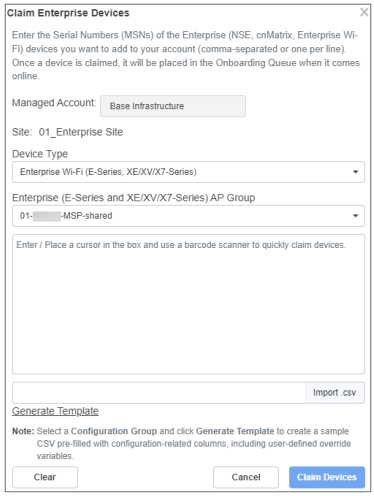
To import multiple Enterprise devices using the CSV import option, complete the following steps:

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

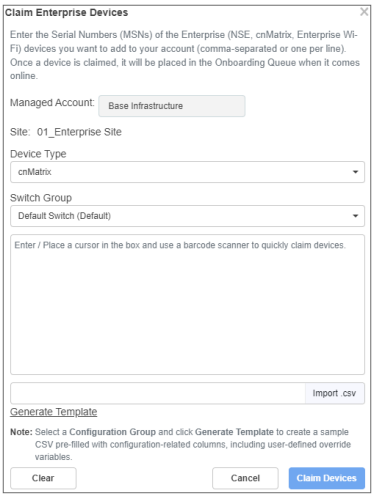
   The **Claim Enterprise Devices** window is displayed as shown in the following images.

   - At the enterprise site-level:

     Wi-FI APs



     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 **Serial Number** and **Device Name** columns, which are the default columns.

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

Points to consider when importing enterprise devices using CSV import option

- Only one AP group per CSV file is allowed. The same AP group is applied to all devices listed in the CSV file.

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

  The value of the variables must not be empty.

Miscellaneous Onboarding Issues

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

Configuring Devices after Onboarding

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

Deleting Devices

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

Transferring Device Ownership

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



Note

For examples of onboarding and device-specific onboarding procedures, check Onboarding Examples and Device-Specific Onboarding Instructions, respectively.

Onboarding Examples

This section covers the following topics:

- Onboarding Existing Networks
- Onboarding New Devices

Onboarding Existing Networks

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

Onboarding New Devices

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

Claiming Devices using Cambium ID and Device UI

- Configure cnMaestro to support Cambium ID

  First, make sure Cambium ID support is enabled, and a password field is set.

  1. Navigate to **Home > Onboard Devices** and click **Claim from Device**.
  2. Select **Allow device to be claimed using Cambium ID.**
  3. Click **Add New.**
  4. Choose the name of the user from the **Name** dropdown list.
  5. Enter the key for the user in the **Onboarding Key** textbox. The minimum length of characters for the key is 8.
  6. Click **Save**.

- Set Cambium ID on the device UI

  Launch the device UI and enter the Cambium ID and password. The example below defines how to set for ePMP.

  - Login to the device UI and navigate to **Configuration > System > cnMaestro tab**.
  - Enable the radio button for enabling **Remote Management.**
  - Enter the cnMaestro cloud URL in the **cnMaestro URL** textbox.
  - Enter Cambium ID in the **Cambium ID** textbox.
  - Enter the Onboarding key in the **Onboarding Key** textbox.
  - Click **Save** the device.

- Approve the device for onboarding:

  1. Navigate to **Home > Onboard Devices** and click the **Onboard** tab.
  2. Find the device and onboard using the Cambium ID.
  3. You can able to see who onboarded the device.
  4. The Status field should display **Waiting for Approval**.

5. Make any additional onboarding configuration changes you want.
6. Approve the device by clicking the **Approve** button under **Actions**.
7. The device status will change to **Onboarded** after onboarding finishes under the **Status**.

Claiming Devices Using Cambium ID and SNMP

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

Device-Specific Onboarding Instructions

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

- Onboarding cnMatrix
- Onboarding cnRanger
- Onboarding cnReach
- Onboarding cnPilot R-Series
- Onboarding cnVision
- Onboarding Enterprise AP
- Onboarding ePMP 1000
- Onboarding PMP
- Onboarding PTP 650/670/700
- Onboarding Xirrus device
- Onboarding a cnWave 5G Fixed BTS device
- Onboard Edge Controller
- Onboard PTP 820/850 devices
- Onboarding the NSE 3000 Devices
- Onboarding Home Mesh Routers
- Onboarding PON devices
- Onboarding 60 GHz cnWave devices

Onboarding cnMatrix

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

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

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

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

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

```
login as: admin
admin@10.110.221.83's password:

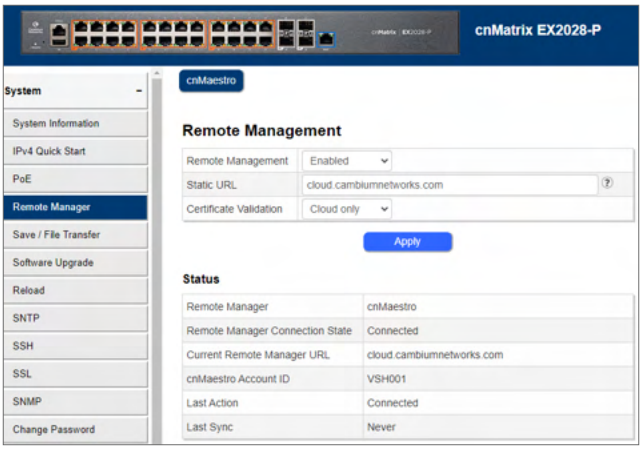
                Cambium Networks cnMatrix EX2028-P Ethernet Switch

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

Onboarding cnMatrix through UI

In the cnMatrix device UI, complete the following steps:

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



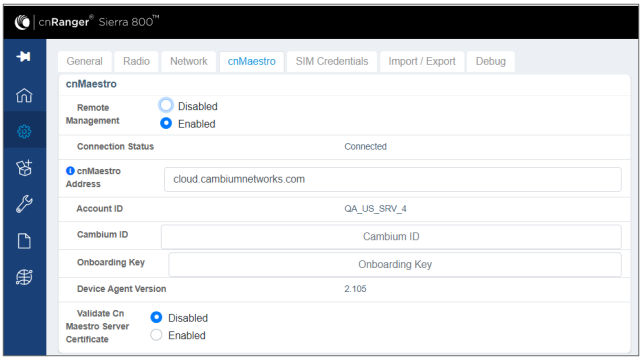
Onboarding cnRanger

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

Setting static URL for cnMaestro on Sierra 800

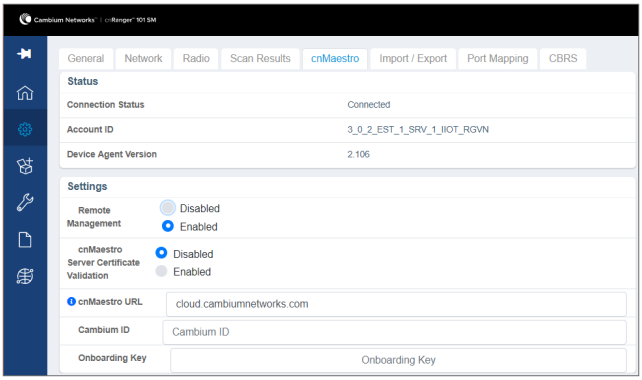
1. Navigate to **Configuration > cnMaestro**.
2. Under cnMaestro section, enter the URL in the cnMaestro Address.

3. Click **Save**.



Setting static URL for cnMaestro on Tyndall 101

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



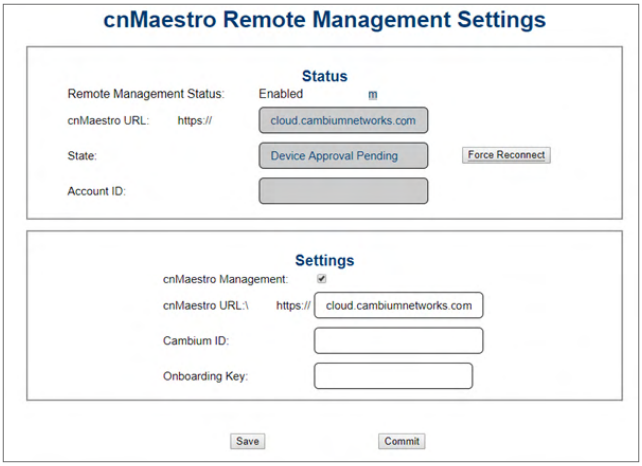
Onboarding cnReach

Onboarding through UI

In the cnReach device UI, complete the following steps:

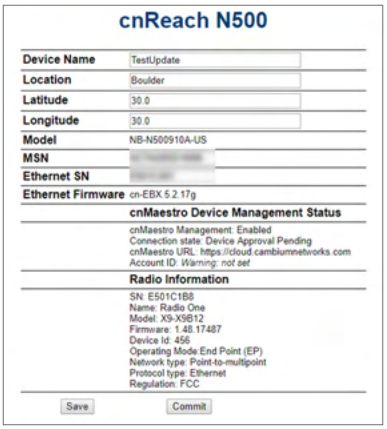
1. Navigate to **cnMaestro** > **Management Settings**.
2. Enable **cnMaestro Management** in Settings section.
3. Enter your **Cambium ID** and **Onboarding Key**.
4. Click **Save**.
5. Navigate to home page to view the status of the cnReach device connection to cnMaestro.

Figure 50 *Onboarding cnReach through UI*



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

Figure 51 *Viewing the cnReach connection to cnMaestro*



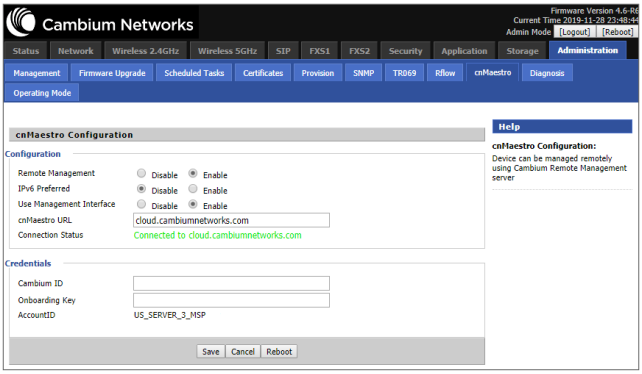
Onboarding cnPilot R-Series

Onboarding through UI

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

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

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



Onboarding through SNMP

The following OIDs can be configured:

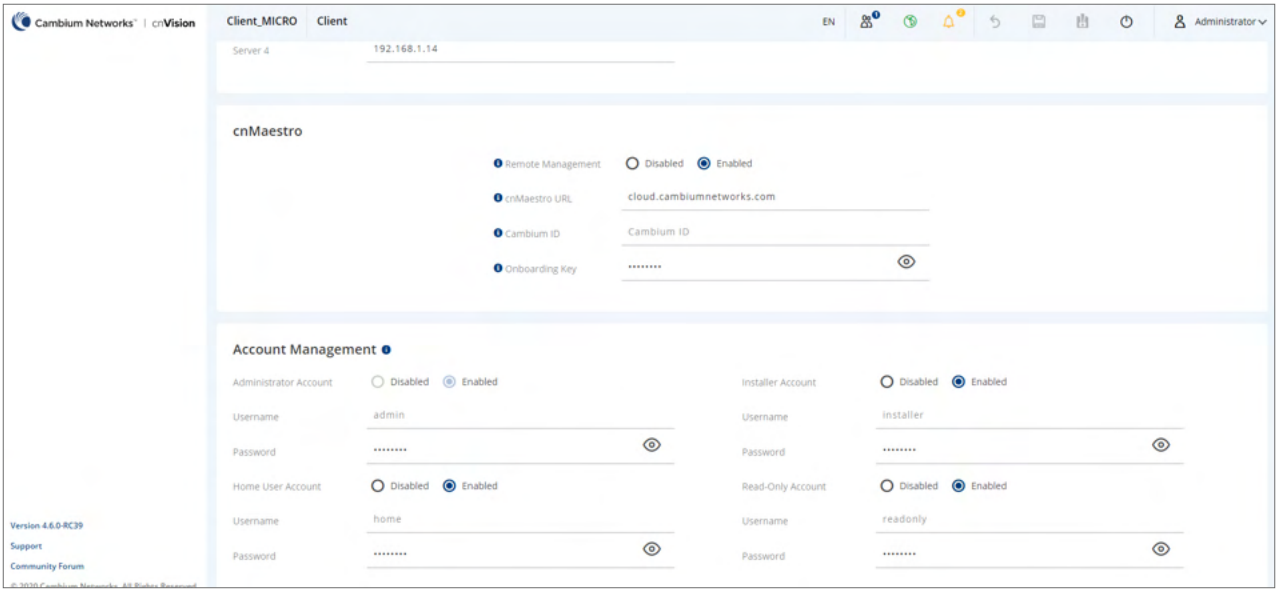
- cambium_id
- cambium_token
- cns_staic_url

Onboarding cnVision

Onboarding cnVision Client

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

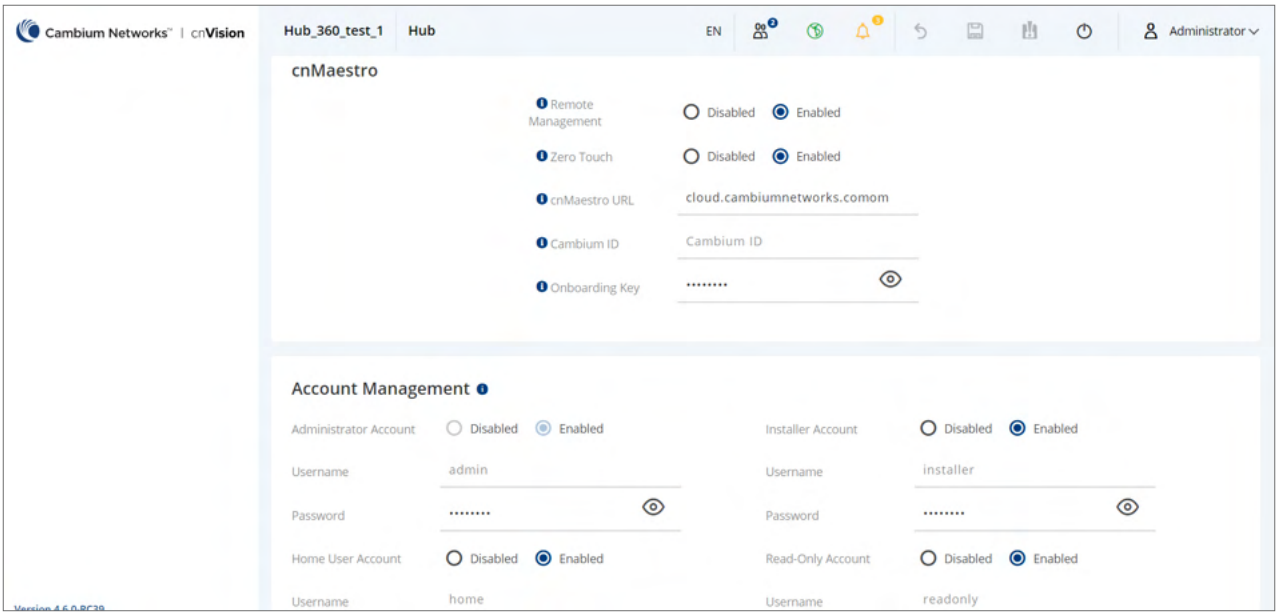
1. Navigate to **Configuration > System.**
2. Under cnMaestro section, enter cnMaestro URL.
3. Click **Save**.



Onboarding cnVision Hub

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

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



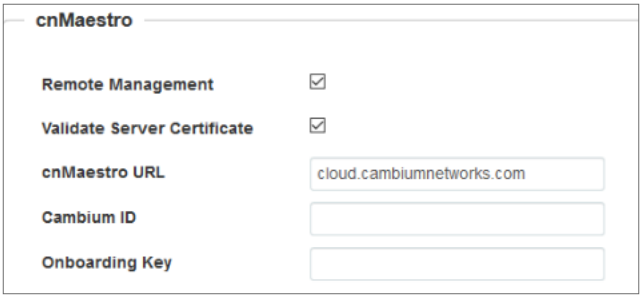
Onboarding Enterprise AP

Onboarding through UI

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

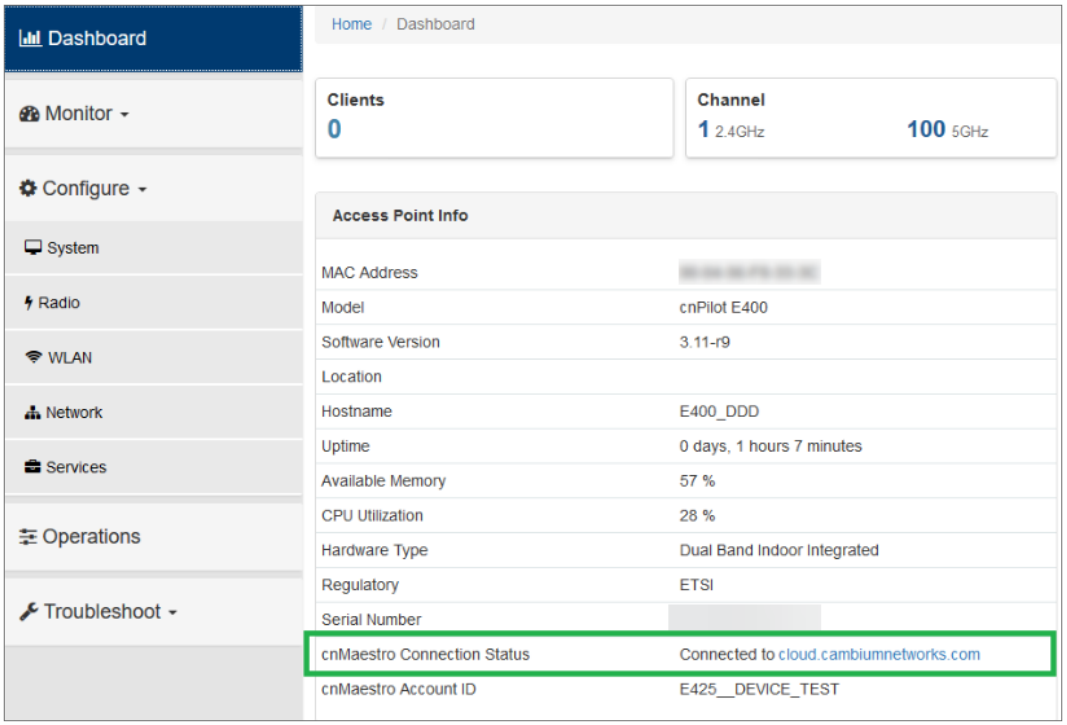
1. Navigate to **Configure > System**.
2. Scroll to **Management** > **cnMaestro**.
3. Enable **Remote Management**.
4. Enable **Validate Server Certificate** if required.
5. Enter **cnMaestro URL**.
6. Enter **Cambium ID** and **Onboarding Key.**
7. Navigate to **Dashboard** to view the status of the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

Figure 53 *Onboarding Enterprise AP through device UI*



To view the status of the device connection to cnMaestro:

Figure 54 *Viewing the Enterprise AP connection to cnMaestro*



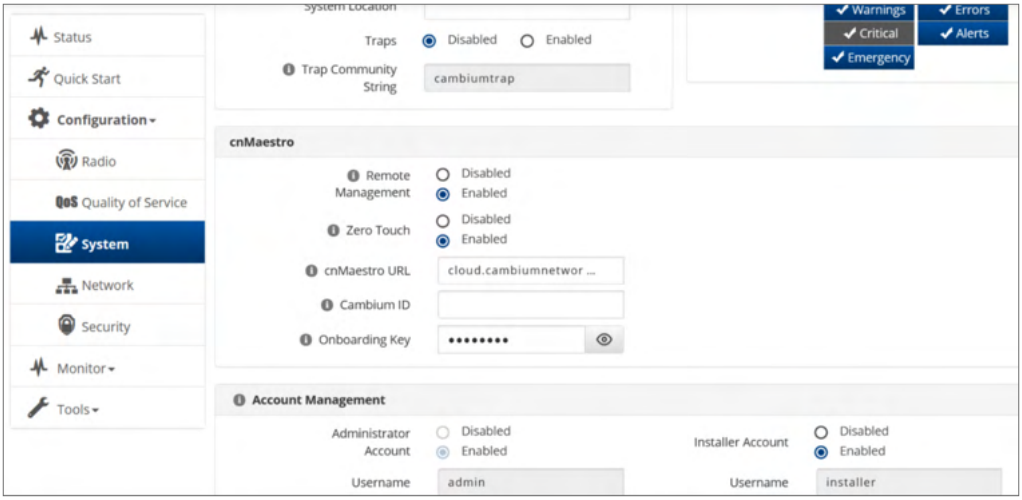
Onboarding ePMP 1000

Onboarding through UI

In the ePMP device UI, complete the following steps:

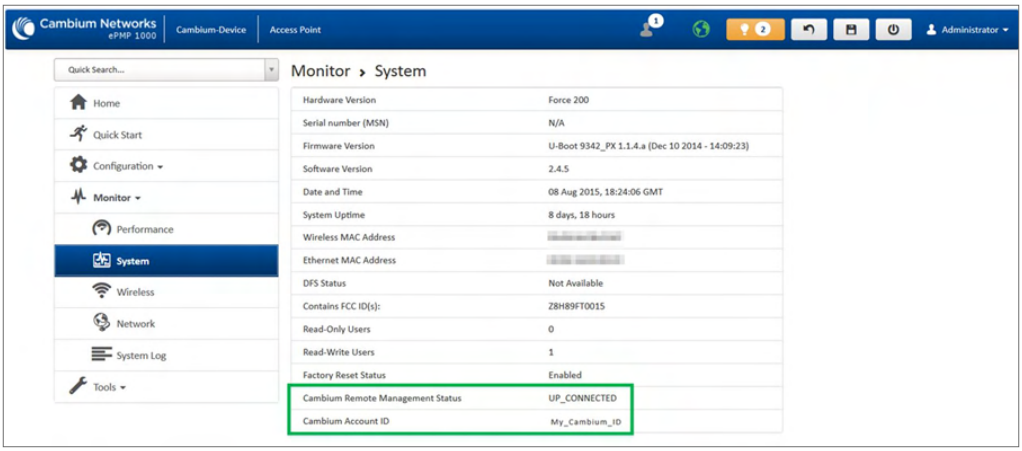
1. Navigate to **Configuration** > **System**.
2. Scroll to **cnMaestro**.
3. Select **Enable** and enter your Cambium ID and the user's Onboarding Password.
4. Navigate to **Monitor** > **System** to view the status of the ePMP device connection to cnMaestro.

Figure 55 *Onboarding ePMP 1000 through UI*



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

Figure 56 *Viewing the ePMP device connection to cnMaestro*



Onboarding through SNMP

The following OIDs can be configured:

- `cambiumDeviceAgentEnable`
- `cambiumDeviceAgentCNSURL`
- `cambiumCNSDeviceAgentID`
- `cambiumCNSDeviceAgentPassword`

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

- `cambiumCnsServConsStat`

Onboarding PMP

Onboarding through UI

To onboard PMP device connection to cnMaestro:

In the PMP device UI, complete the following steps:

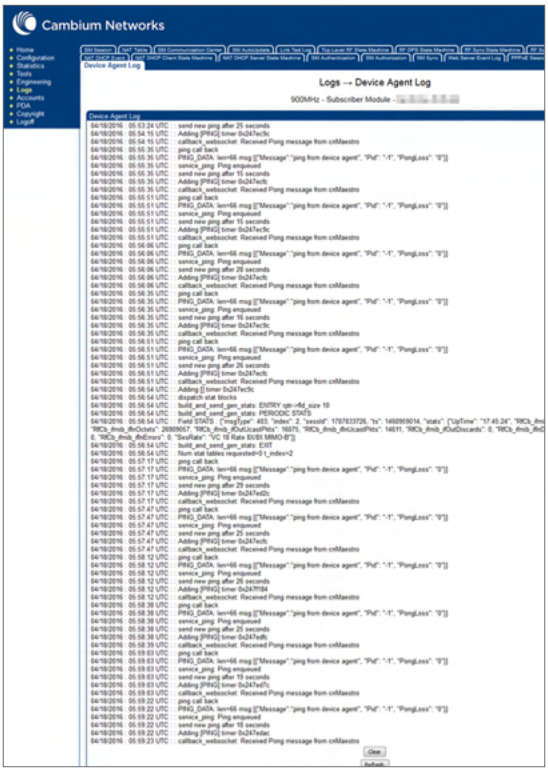
1. Navigate to **Configuration** > **cnMaestro**.
2. Under **Configuration**, provide the following details:
   a. Select **Enable** under **Remote Management**.
   b. Enter the URL to connect to cnMaestro in the **cnMaestro URL** textbox.
3. Under **Credentials**, enter the **Cambium ID and the Onboarding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

Figure 57 *Onboarding PMP through UI*



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

Figure 58 *Viewing Logs*



Onboarding through SNMP

The following OIDs can be configured:

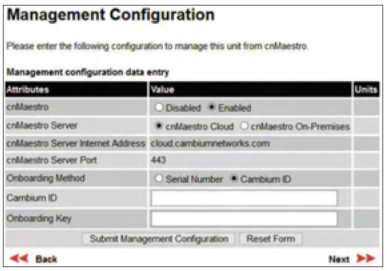
- cnMaestro Enable
- cnMaestro Url
- cambium ID
- cam Onboard Key

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

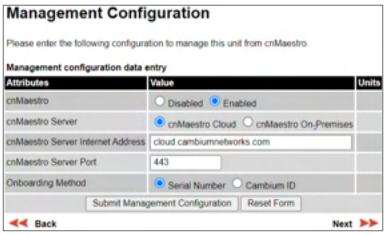
- cam AccID
- cnMaestro Status

Onboarding PTP 650/670/700

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



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



Onboarding Xirrus device

Perform the following steps to onboard Xirrus device through CLI.

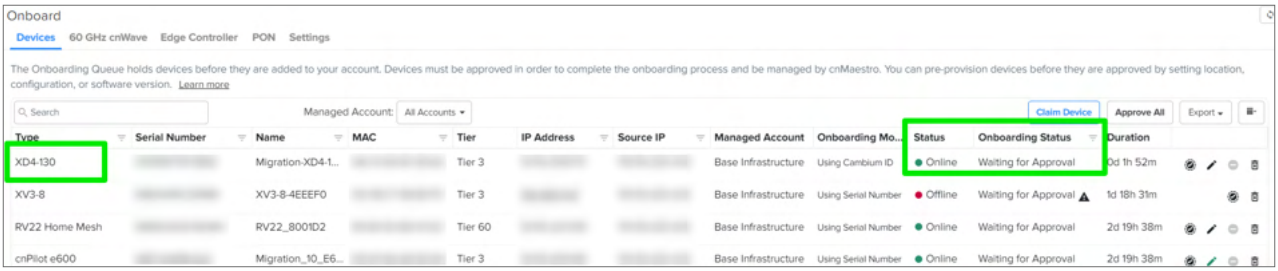
1. Connect to the device using any SSH tool.
2. Login as admin, the default password is admin.
3. Execute the following command in ssh console:

```
#ssh admin <device IP address>
#password <admin>
#configure
```

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

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

Figure 59 *Xirrus Device Waiting for Approval*



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

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

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

For details to migrate Xirrus devices from XMS to cnMaestro X using a tool, see XMS-Enterprise to cnMaestro X.

Note

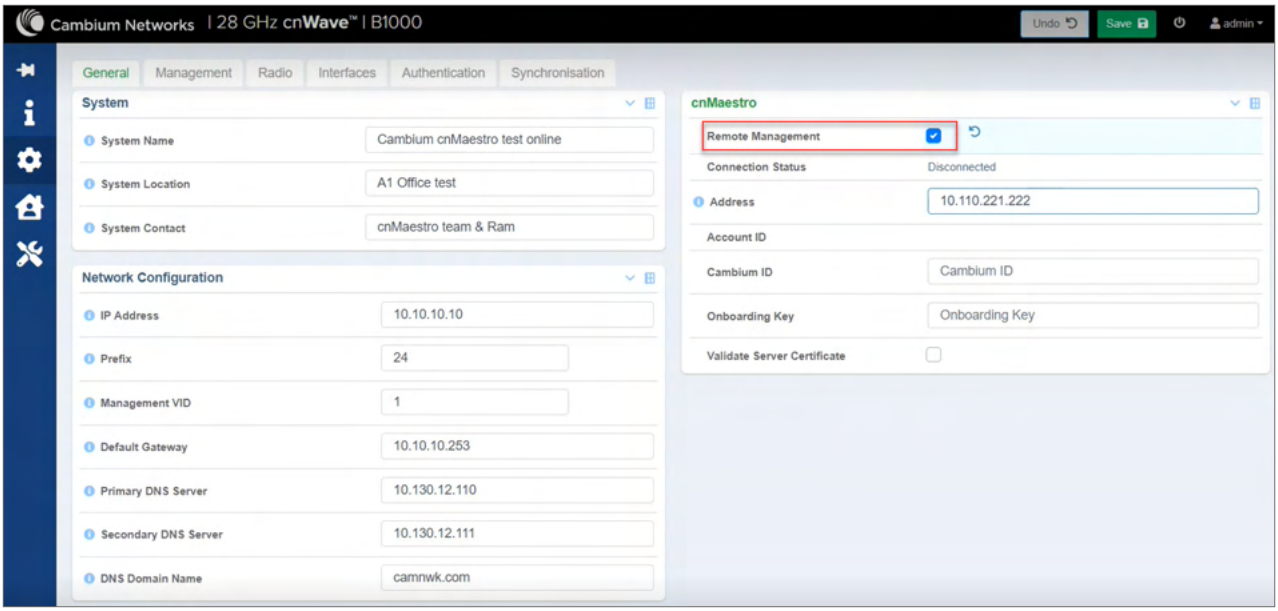
- Xirrus APs are onboarded only to cnMaestro X accounts not to cnMaestro Essentials.
- Tier 3 subscription is applicable to Xirrus APs.
- Xirrus devices can only be onboarded using Cambium Id and Onboarding Key for Cloud account.

Onboarding a cnWave 5G Fixed BTS device

Claiming a cnWave 5G Fixed BTS device

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

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



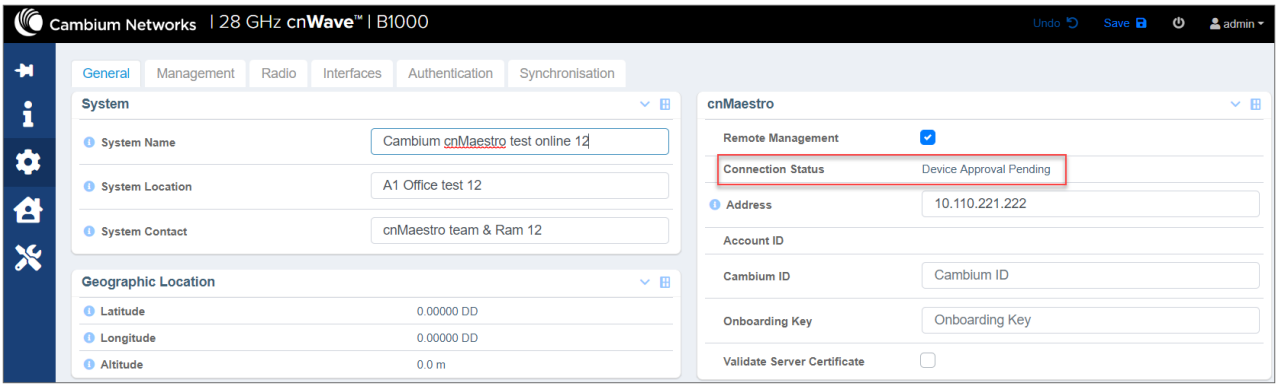
3. In the **Address** field, enter the cnMaestro URL or IP Address.
4. Enter your **Cambium ID** and **Onboarding Key**. **Validate Server Certificate** is an optional field.

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

5. Click **Save**.

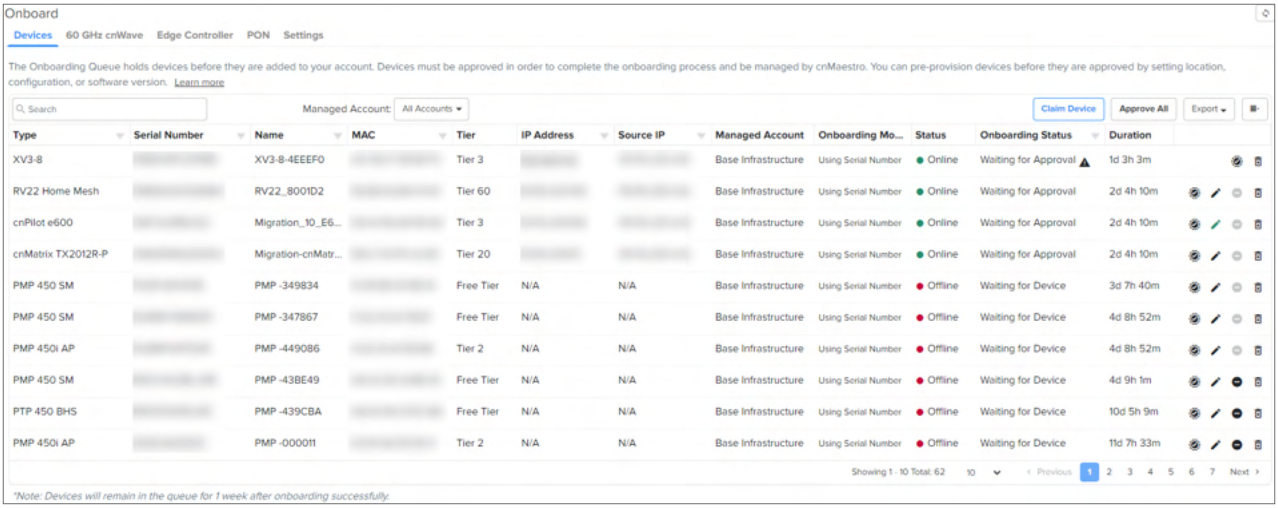
   When the cnWave 5G Fixed BTS device is onboarded to the cnMaestro for the first time, the **Connection Status** field in the cnWave 5G Fixed BTS device UI displays **Device Approval Pending** as shown in Figure 60.

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



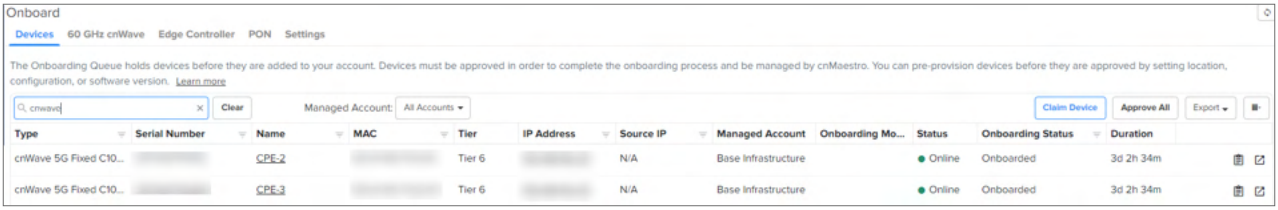
6. In the cnMaestro UI, navigate to **Onboard** > **Devices** and click **Approve**, as shown in Figure 61.

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



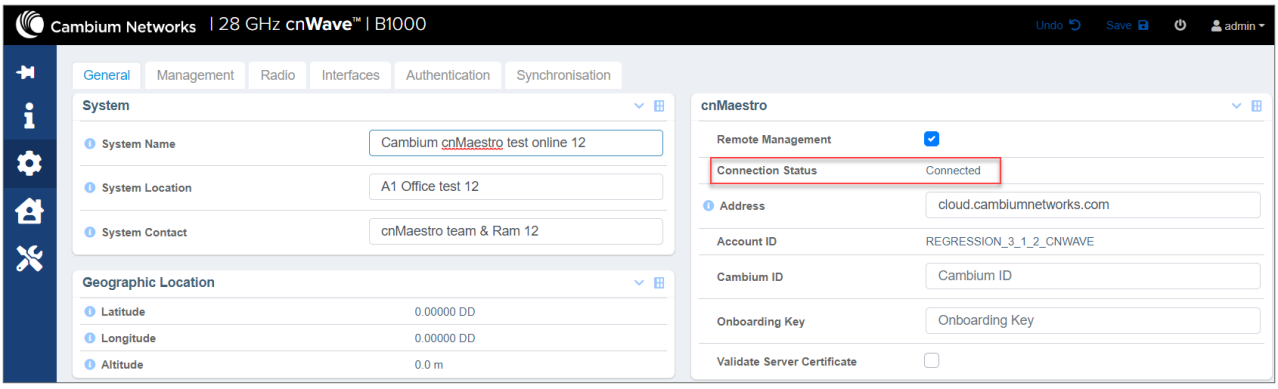
The cnWave 5G Fixed BTS device is onboarded to cnMaestro.

Figure 62 *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 63.

Figure 63 *cnWave 5G Fixed BTS device Connected*

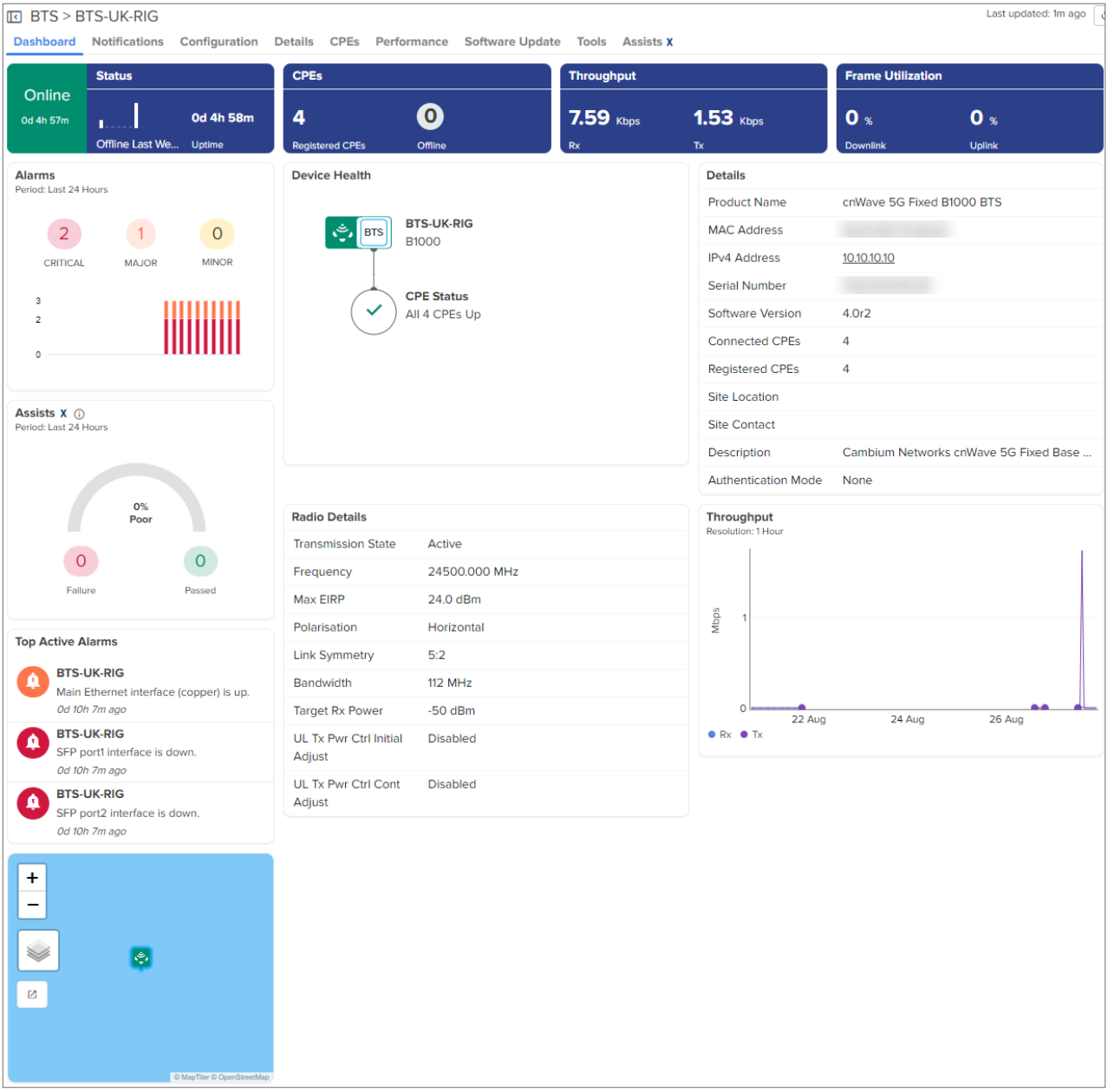


To view the cnWave 5G Fixed BTS device in cnMaestro, complete the following steps:

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

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

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



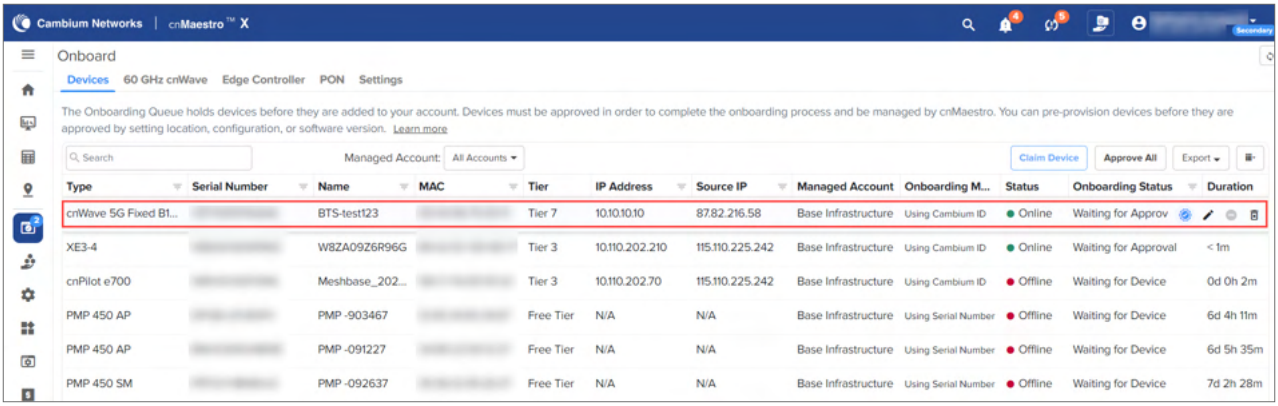
Claiming a cnWave 5G Fixed BTS device with the Serial Number

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

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

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

Figure 65 *Onboard page*



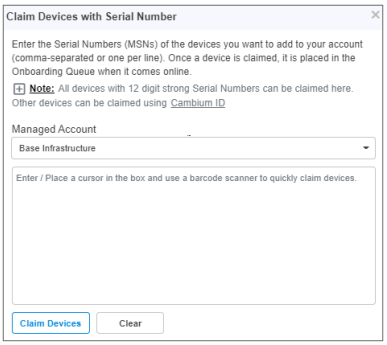
2. Click **Claim Device** located at the right side of the **Onboard** page, as shown in Figure 65.

   The **Claim Devices with Serial Number** page appears, as shown in Figure 66.

3. Enter the serial number of the cnWave 5G Fixed BTS device in the text box, as shown in Figure 66.

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

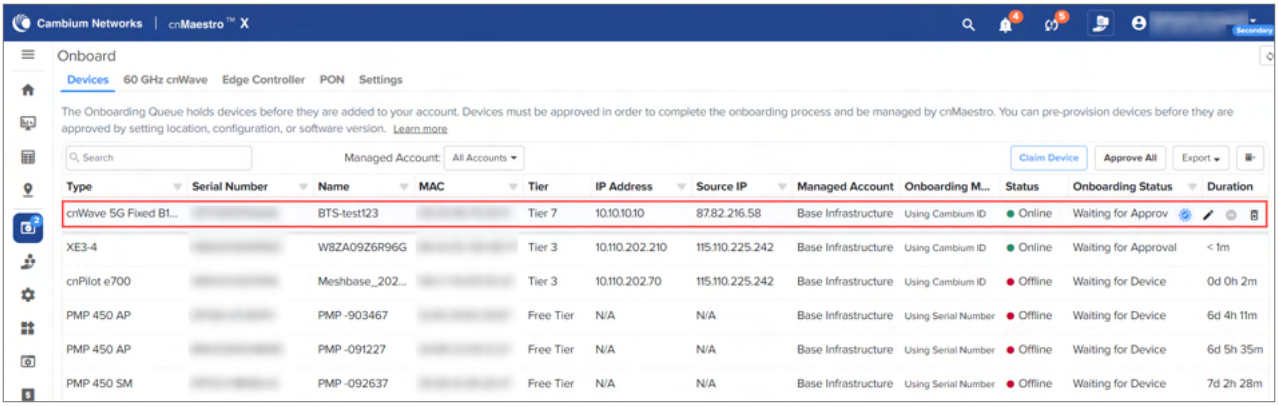
Figure 66 *Claim Devices with Serial Number page*



4. Click **Claim Devices.**

5. To onboard the cnWave 5G Fixed BTS device, click **Approve** located at the right side of the **Onboard** page, as shown in Figure 67.

Figure 67 *Onboarding Queue*



Note

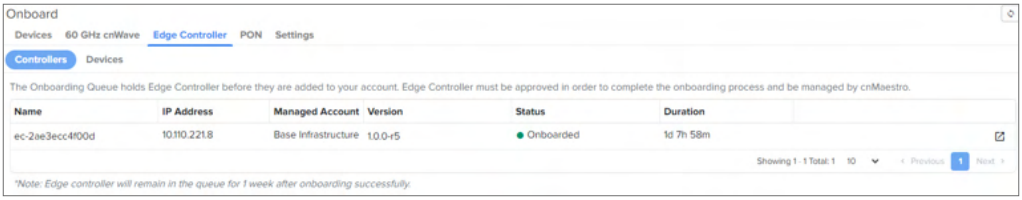
If you do not click **Approve**, the device remains in the Onboarding Queue.

Onboard Edge Controller

To onboard Edge Controller, complete the following steps:

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

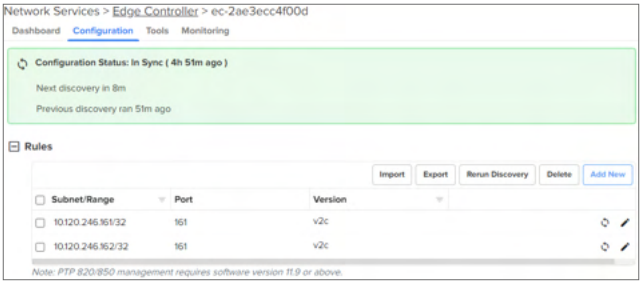
Figure 68 *Edge Controller*



Onboard PTP 820/850 devices

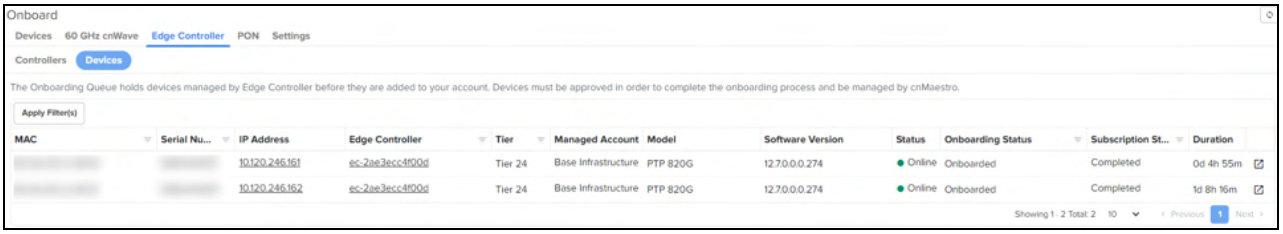
To onboard PTP 820/850 devices, complete the following steps:

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



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

Figure 69 *PTP 820/850 devices*



Onboarding the NSE 3000 Devices

Note

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

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

Figure 70 *: MSN of device*



To onboard the device, complete the following steps:

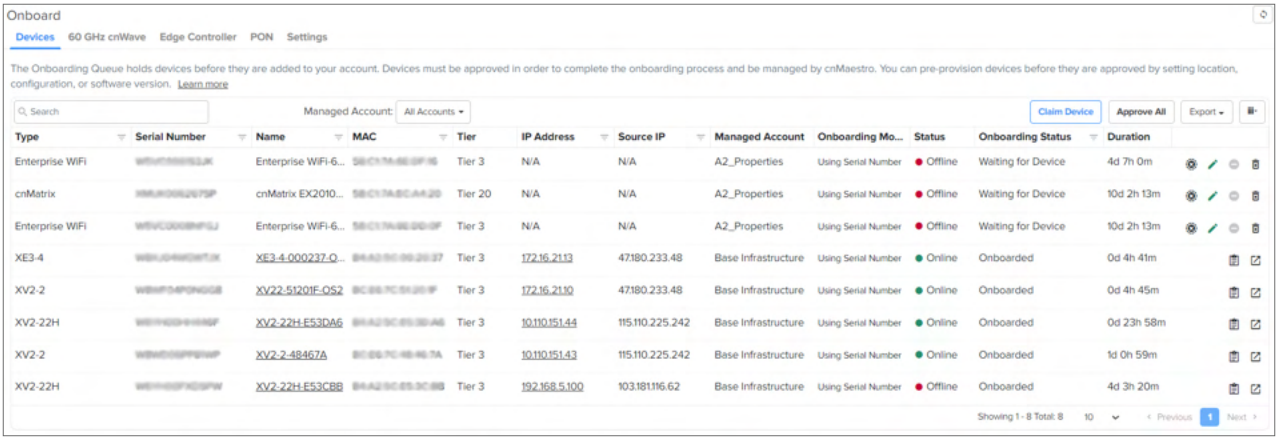
1. Open a web browser and type the URL https://cloud.cambiumnetworks.com.

   The sign in page appears.

2. Create a new cnMaestro X account or select an existing cnMaestro X account. A tier 30 subscription is required.

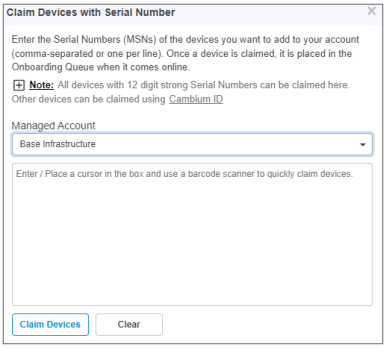
3. Navigate to cnMaestro **Home** > **Onboard** > click **Claim Device.**

   Figure 71 *Onboard page*



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

Figure 72 *Claim devices with Serial Number*



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

   The device will be listed in the Onboarding Queue.

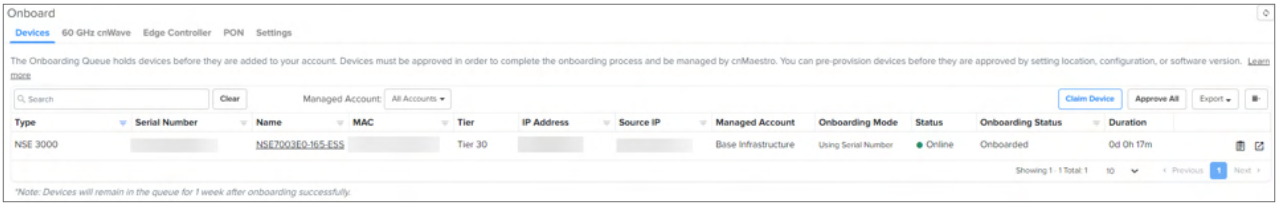
8. Click the **Approve Device** ( ) icon or **Approve All** at the right side of the Onboard page, as shown in

Figure 73 *Approve*



When device is approved appears on the Onboard page as shown below in Figure 74.

Figure 74 *NSE 3000 Device Onboard*



Onboarding Home Mesh Routers

To onboard the Home Mesh Router to cnMaestro, see Onboarding the Home Mesh Router to cnMaestro.

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

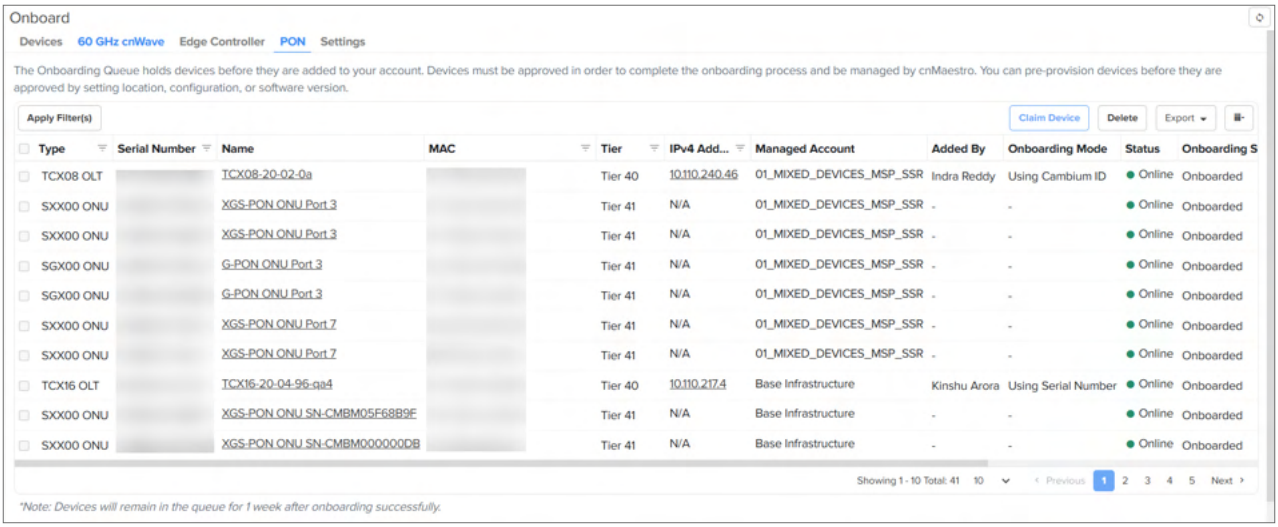
Onboarding PON devices

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

To onboard the router, complete the following steps:

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

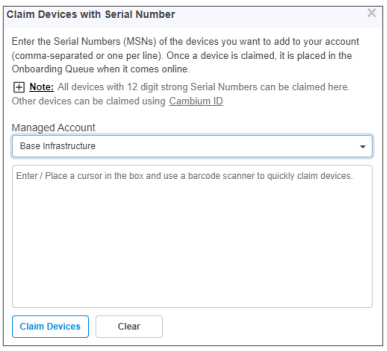
   Figure 75 *Onboard page for PON devices*



2. Click **Claim Device**.

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

   Figure 76 *Claim devices with Serial Number*



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

   The device will be listed in the Onboarding Queue.

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

Onboarding 60 GHz cnWave devices

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

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

60 GHz cnWave devices support the following E2E Controllers types:

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

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

Note

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

- Ensure that the required E2E Controller type is hosted on the 60 GHz device. For detailed information on deploying the E2E Controller for the 60 GHz device, refer to the 60 GHz cnWave E2E Controller User Guide.
- Enable the E2E Controller (after hosting) using the device UI. For detailed information on enabling the E2E Controller for the 60 GHz device, refer to the latest 60 GHz cnWave User Guide.
- Ensure that the IP address of the E2E Controller is set. The E2E Controller and cnMaestro are two separate entities and they can be hosted on separate computers or the same computer. The E2E Controller uses IPv4 to communicate with the cnMaestro and uses IPv6 to communicate with the cnWave radios.

This topic covers the following sections:

- Onboarding a 60 GHz device with external E2E Controller
- Onboarding a 60 GHz device with Onboard E2E Controller
- Onboarding the Onboard E2E Controller using Serial Number

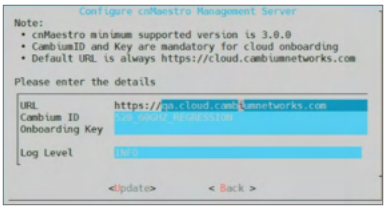
Onboarding a 60 GHz device with external E2E Controller

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

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

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

   The Configure cnMaestro Management Server window opens.



5. Set appropriate values for the following parameters:

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

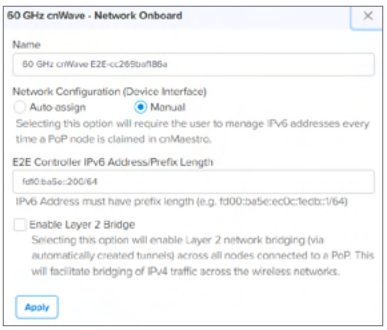
  A Cambium ID is a string that uniquely identifies an account (which you create). It consists of letters, numbers, and underscores. Example: 60GHz_xxx_xxxxxxxxxx. It is used to onboard devices and is assigned to the devices managed by cnMaestro.
- **Onboarding Key**: Enter an appropriate onboarding key (if configured) that is mapped to an individual user account. You can set the onboarding keys for the required user accounts using the **Onboard** > **Settings** page in the cnMaestro UI. For more details, check Onboarding Key configuration.

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



8. Click **Approve**.

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



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

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

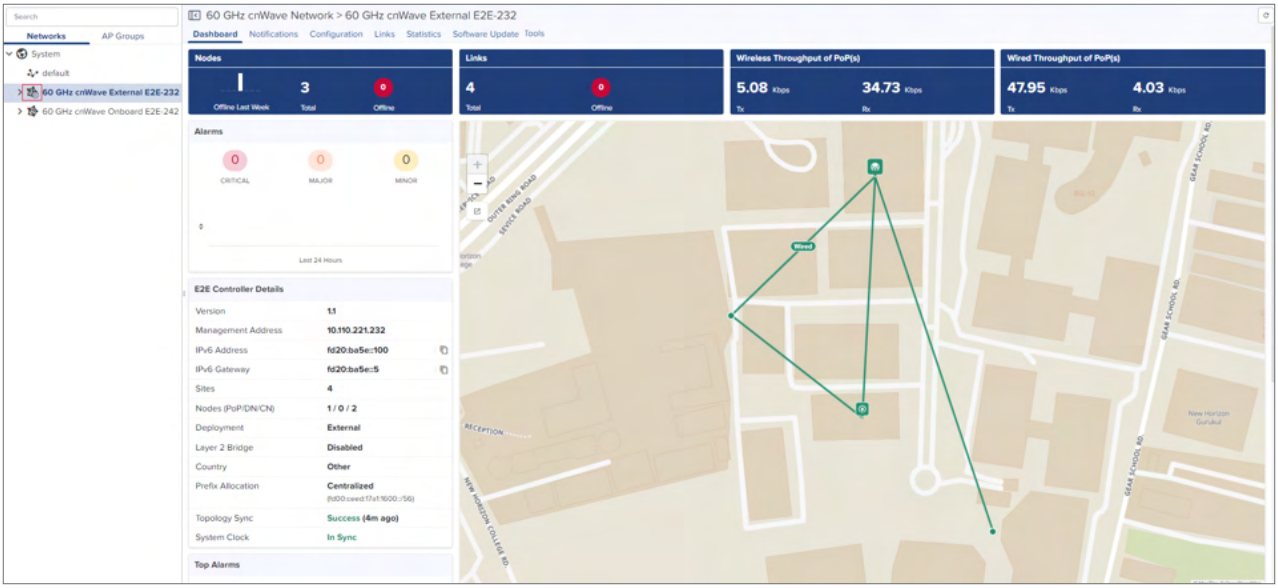


Note

The **Onboard** page in cnMaestro UI supports a separate tab for 60 GHz cnWave. Using this **60 GHz cnWave** tab, you can check the onboarding queue for E2E Controllers and cnWave devices. Users must approve the60 GHz E2E Controller before it is added to cnMaestro as an E2E Network. The users can approve either through the Onboarding Queue or the Hierarchical Tree (where the E2E Network is placed on the Monitor and Manage page).

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

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



Onboarding a 60 GHz device with Onboard E2E Controller

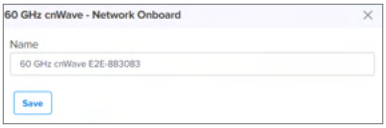
To onboard a 60 GHz device with the internal Onboard E2E Controller (which is running on the 60 GHz cnWave device), complete the following steps:

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



4. Click **Approve**.

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

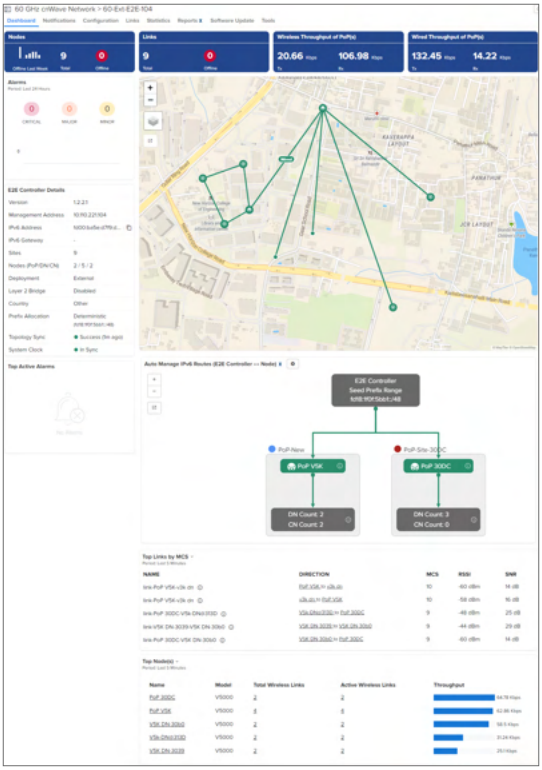


5. Edit the network name and click **Save**.

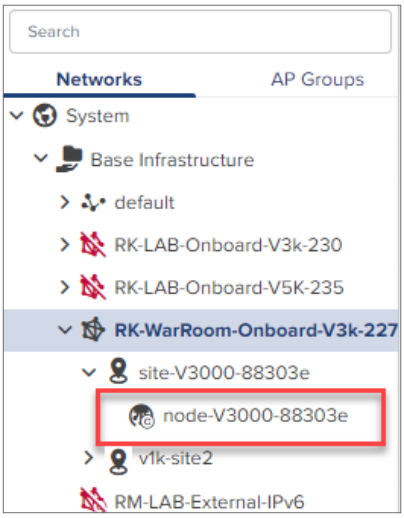
   You must wait until the network onboard successful message is displayed.



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



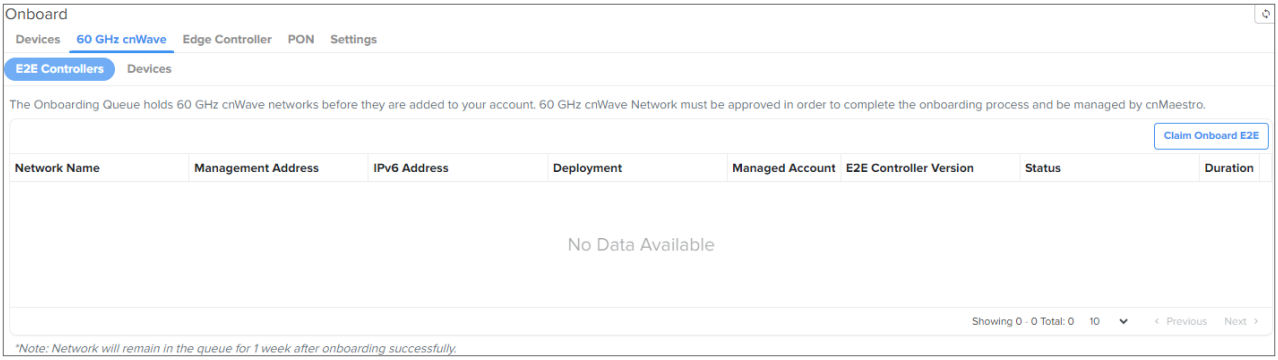
If a PoP node is running the Onboard E2E Controller, then the icon indicates the PoP as shown in the figure below.



Onboarding the Onboard E2E Controller using Serial Number

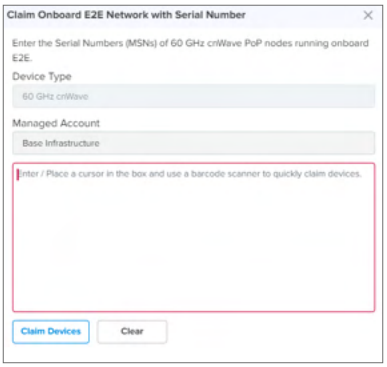
To onboard the internal running 60 GHz Onboard E2E Controller using its serial number, complete the following steps:

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



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

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



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

Deleting Devices in Bulk

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

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

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

The following topics are described:

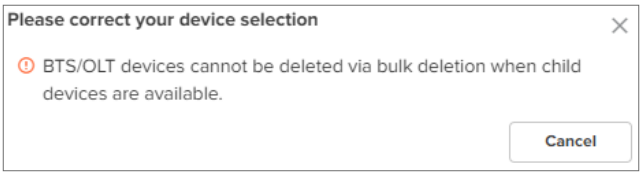
- Device-specific restrictions
- Deleting devices in bulk
- Viewing the status of device deletion and retrying

Device-specific restrictions

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

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

  Figure 77 *Deleting BTS/OLT devices in bulk*

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

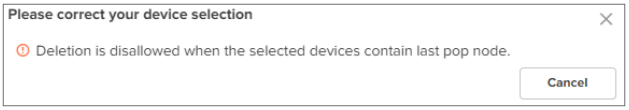
  Figure 78 *Deleting single BTS/OLT device*

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

    The following message appears:

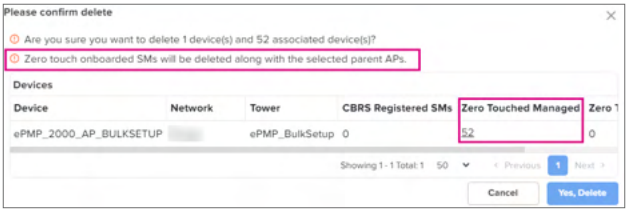
Figure 79 *Deleting Onboard E2E Controllers with last pop node*



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

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

    Figure 80 *Deleting APs with SMs onboarded using zero touch method*

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

    Figure 81 *Deleting APs with SMs onboarded without zero touch method*

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

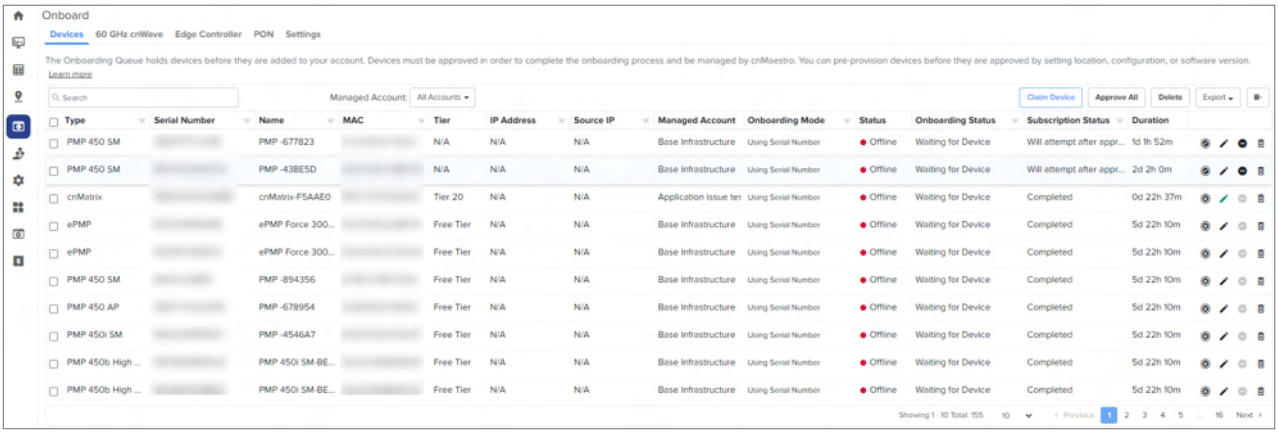
  This occurs even when CBRS-claimed SMs are not selected for bulk deletion.

Deleting devices in bulk

To delete devices in bulk, complete the following steps:

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

   Figure 82 *Onboard > Devices page*

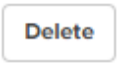
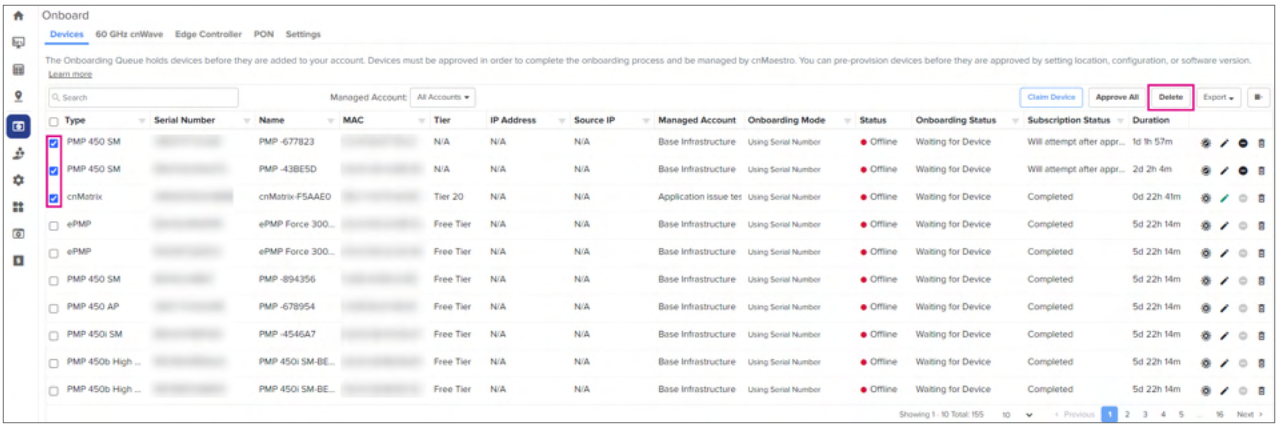
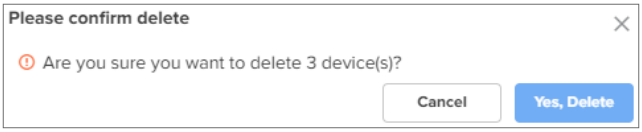
2. Select the checkboxes corresponding to the devices that you want to delete and click the **Delete** () button.

Figure 83 *Select devices*



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

Figure 84 *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 85 *Deletion job banner*



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

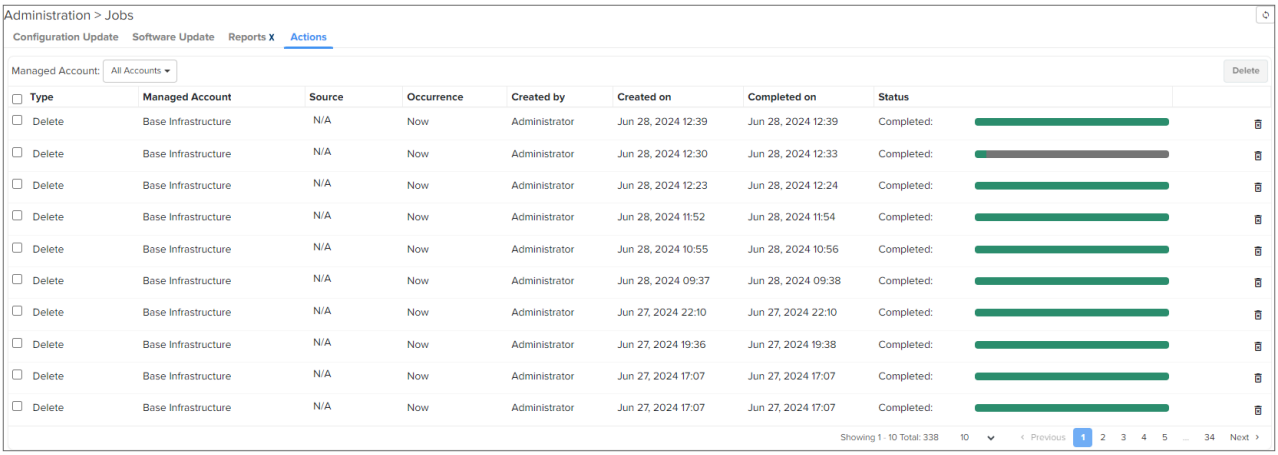
Viewing the status of device deletion and retrying

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 86 ***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 87 *Delete Status window*

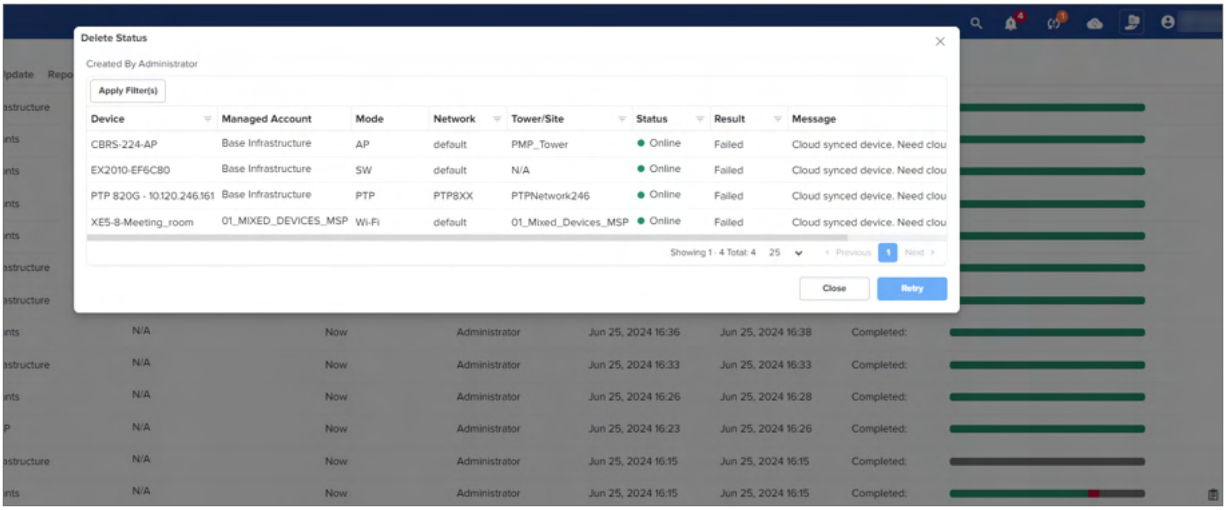


   The following colors display the various statuses of the bulk delete activity:

   - 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 88 *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	50000	20000

Parameter		cnMaestro X	cnMaestro Essentials
	limit. Following are some of the pages where this limit is not applicable: • **Statistics** • **Clients** • **Inventory** • **Device Overrides**		
Number of concurrent exports per account		5	3

Note

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

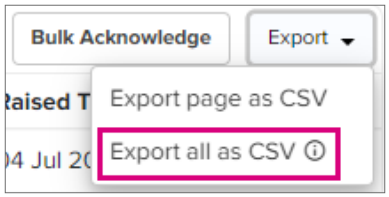
Exporting and downloading all data in the CSV format

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**.

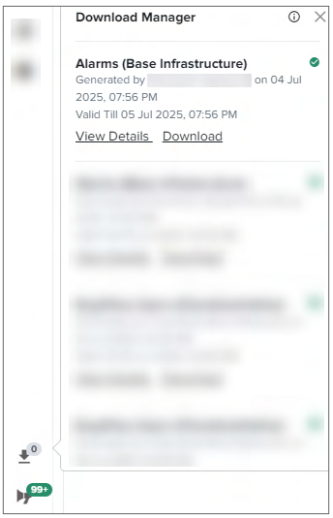
   You can either download the complete data or download a specific set of filtered data.

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



   A message is displayed informing the data is being populated.

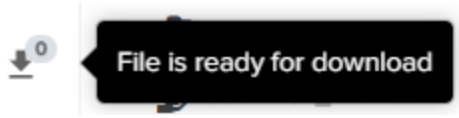
3. Click the download manager ( ) icon on the bottom left of the page.



   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**.

Replacing Devices

cnMaestro allows replacing Enterprise WI-Fi APs and cnMatrix switches from the MSP, site, tower, or device levels.

Points to remember and prerequesites for replacing a cnMatrix switch or AP

The following points must be considered before replacing the cnMatrix switches and APs in cnMaestro UI:

- You can replace switches of the same model only.
- Users must have access to the site or tower where the devices must be replaced.

  Users will not be allowed to replace devices from sites they do not have access to.
- If the existing device has a custom device name, then after replacing, the new device takes the same device name as the old one that was replaced.

  Also, the `-replaced` suffix is added to the old device name.

  For example, if the old AP has a custom device name `XE5-8-152`, and the new device's name is `XYZ-XE5-8-123`, then after replacement, the device name of the new AP will be `XE5-8-152`.

  And the device name of the old AP is renamed as `XE5-8-152-replaced`.
- If the existing device has the default device name (for example, EX2028-EFD000), then after replacing this device, the new device will take its own default name for example, EX2028-F1D8A0).
- If the existing device was mapped to a cnMatrix switch or AP group, then the same cnMatrix switch or AP group and the corresponding configuration is applied on the new device respectively, along with ports details and overrides for switches.
- If the new device already exists in the MSP, site, or tower, then appropriate error message is displayed.
- Sufficient subscription slots must be available while replacing the new device.

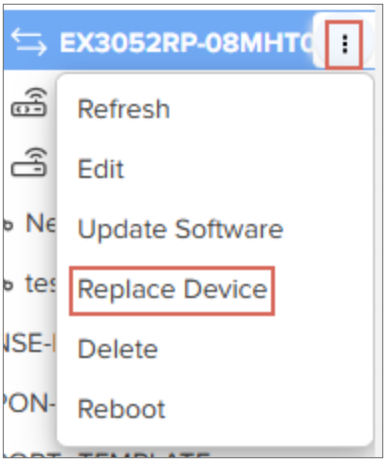
In case no subscription slots are available and a new device is onboarded for the first time, the new device will be added in the Overdraft list.

Else, it will remain in the onboarding list with a subscription error.

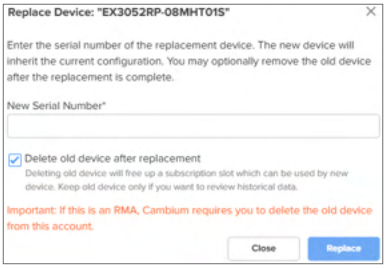
Replacing devices

To replace a device, complete the following steps:

1. Navigate to the device which you want to replace.
2. Click the actions (⋮) icon and select **Replace Device**.



3. The Replace Device window is displayed.



4. Enter the serial number of the new device in the **New Serial Number** parameter.
5. If you want to delete the old device after replacement, then select the Delete old device after replacement checkbox.

Monitoring

This section includes the following topics:

- Network Monitoring
- Network Service Edge
- Wireless LAN Dashboard
- Fiber OLT and ONU
- Inventory
- Reports



Note

Following are the retention period for various data in cnMaestro:

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

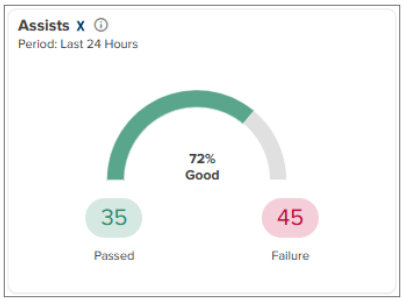
Network Monitoring

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

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

Assists X

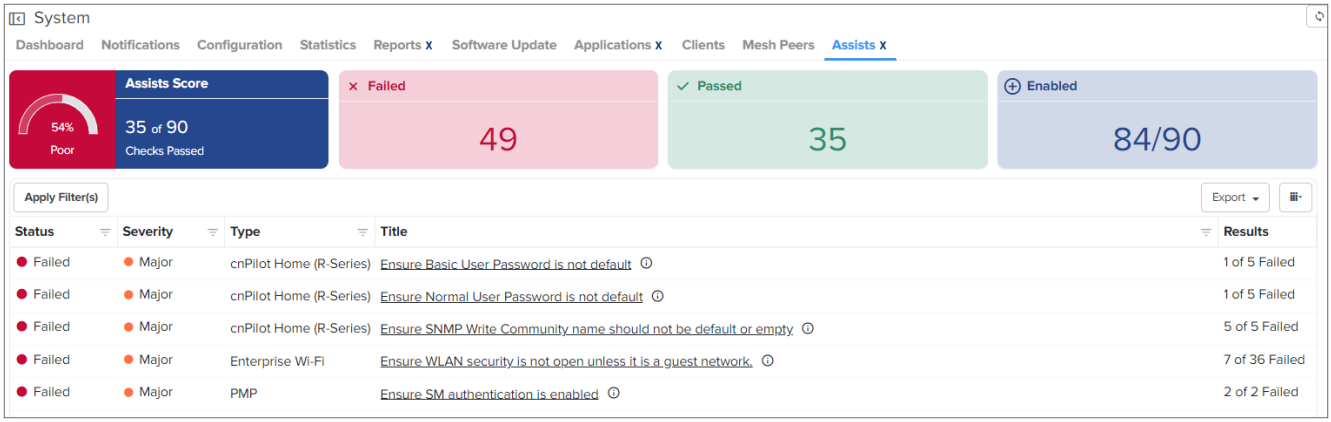
Assists X displays scanned configuration scores and results for last 24 hours.



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

This enables prioritization of management traffic.

Figure 89 *Assists X home page*



Note

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

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

Table 16 *Assist Scores*

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

Table 17 *Assists X parameters*

Fields	Description
Status	Status of the assists are shown as follows: • 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 90.

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

Figure 90 *Assists X Results*

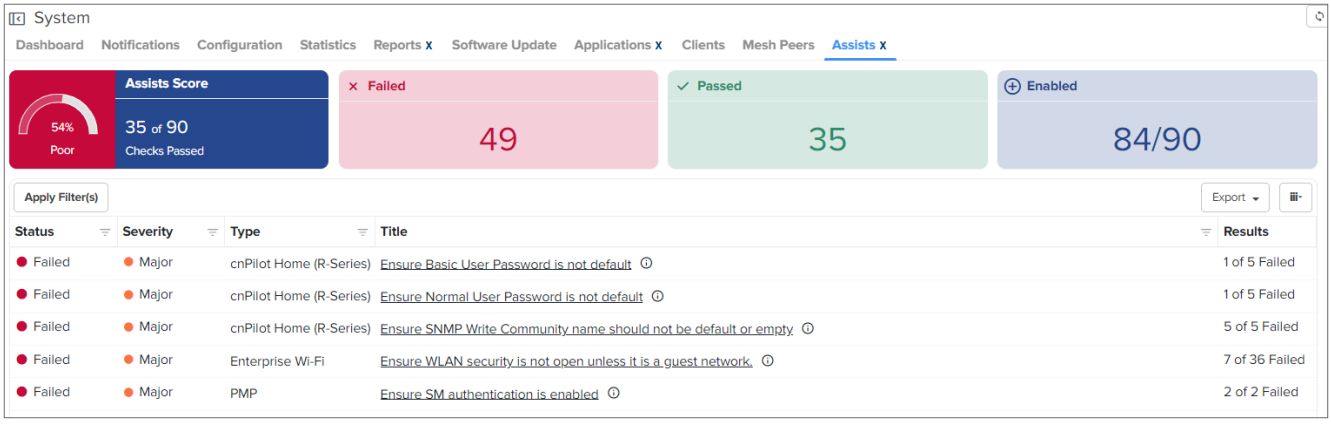


Table 18 *Assist Result Status*

Assist Result	Description
Passed	Assists recommendations are met.

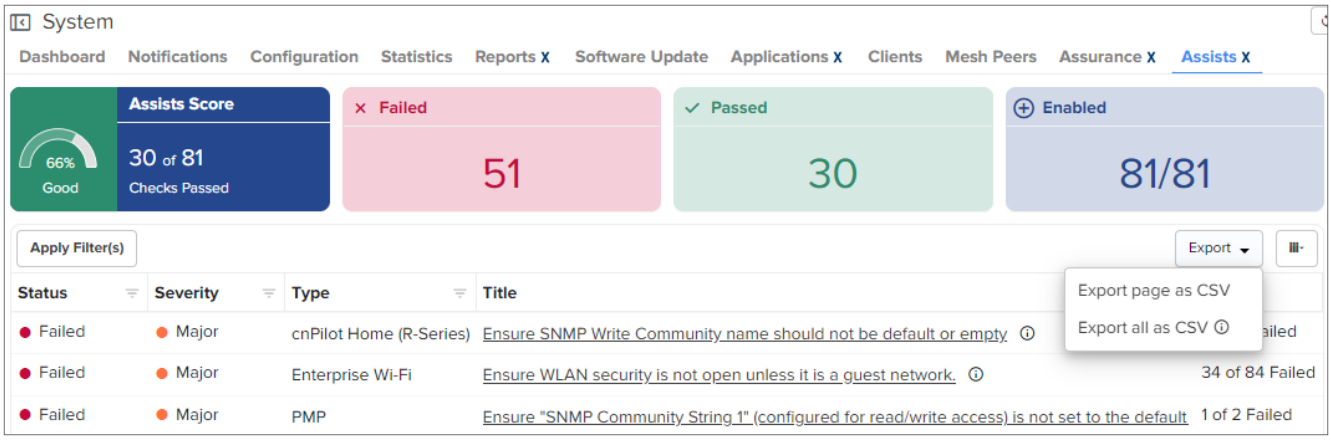
Table 18 *Assist Result Status*

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

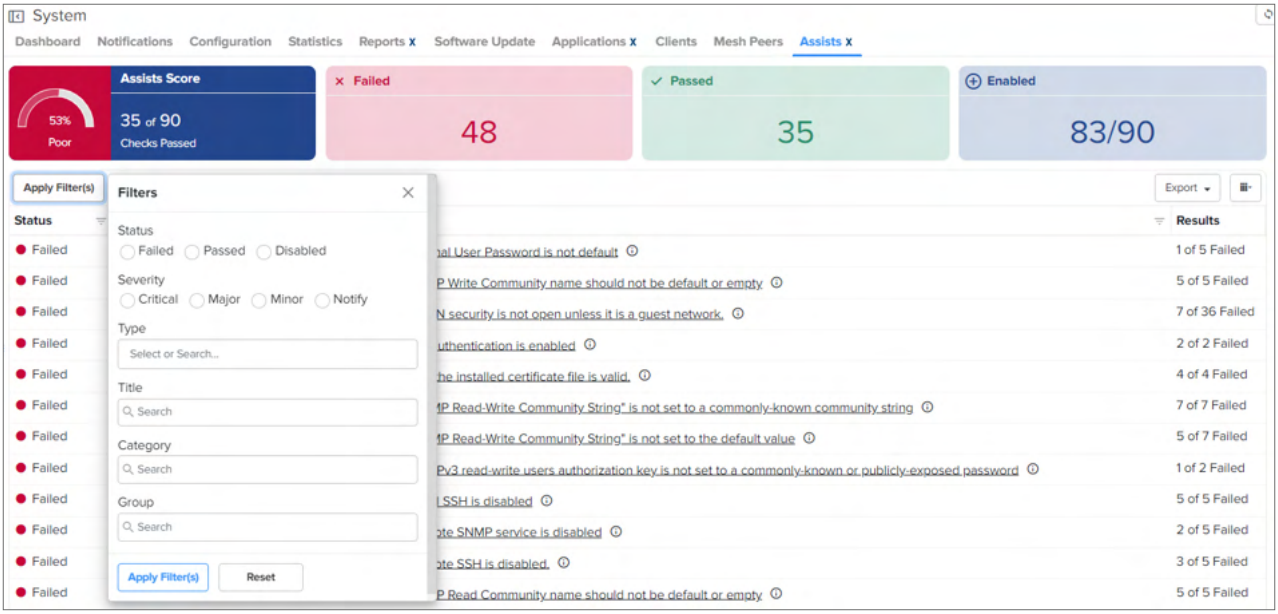


Assists filter

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 91 *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.

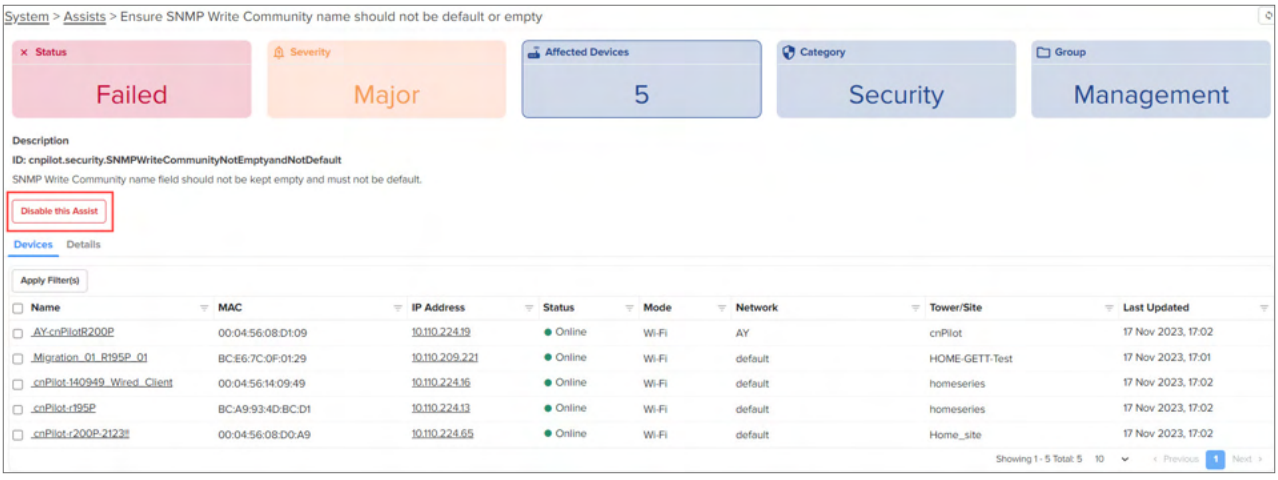
Assists Status

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 92.

To disable Assists, perform the following steps:

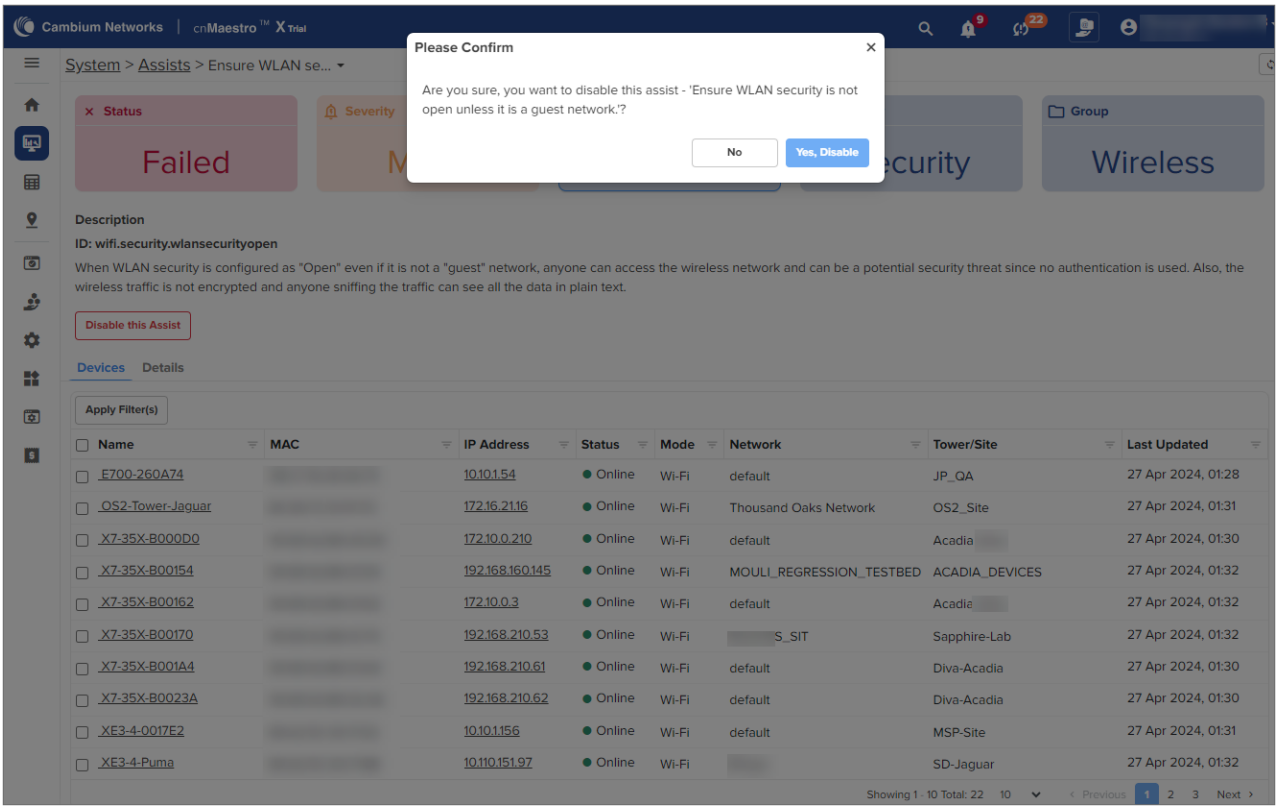
1. In the **Assist Status** page, click **Disable this Assist.**

   Figure 92 *Assist Status page*



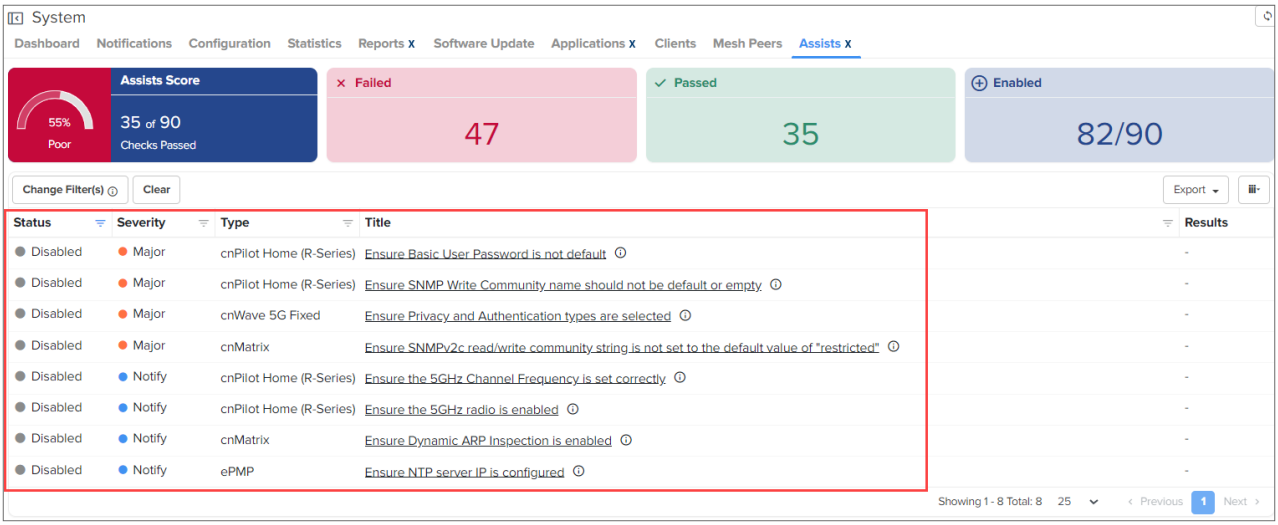
A confirmation message appears for the assist to disable.

2. Click **Yes, Disable**.

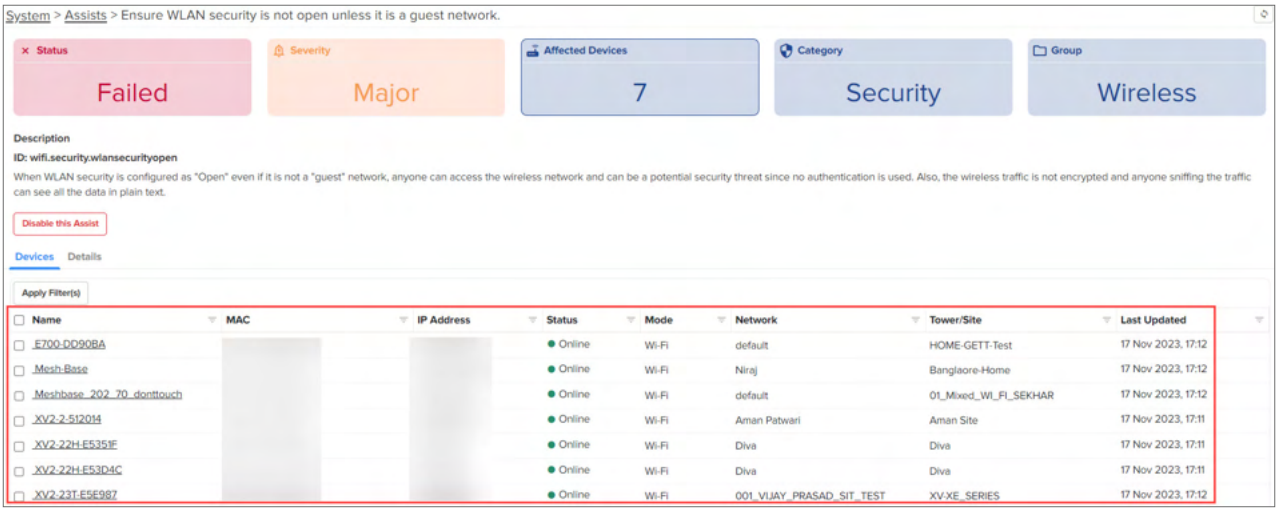


Disabled Assists are listed at the bottom of the Assists X home page. The **Results** column do not indicate the progress bar for the Assists Disabled as shown in Figure 93. The total number of enabled Assists in the home page is reduced when Assists is disabled.

Figure 93 *Assists Disabled*



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

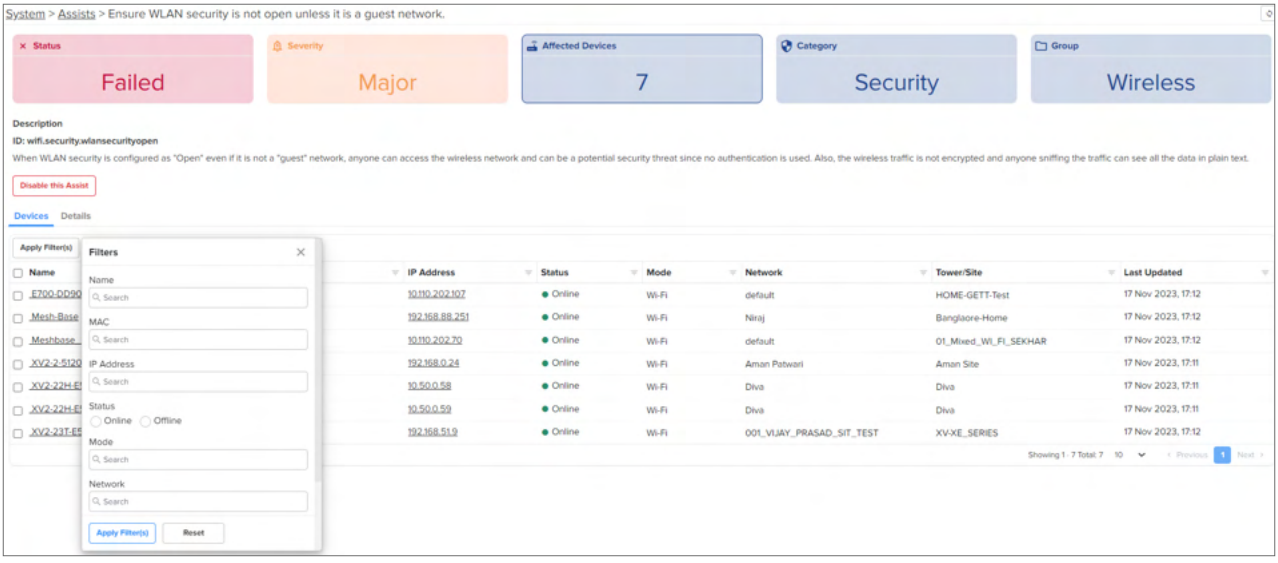


Device filter

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

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

Figure 94 *Assists device filter*



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

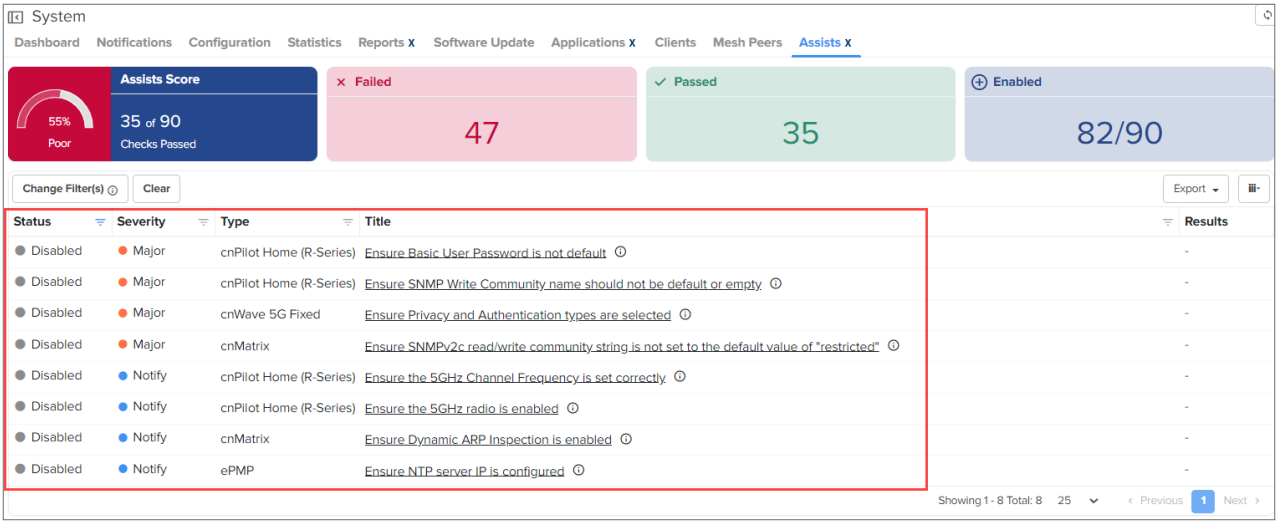
6. Click **Reset** to reset the filter option in the device table.
7. Click **Clear Filters** to clear all the filter options.

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

Enable Assist

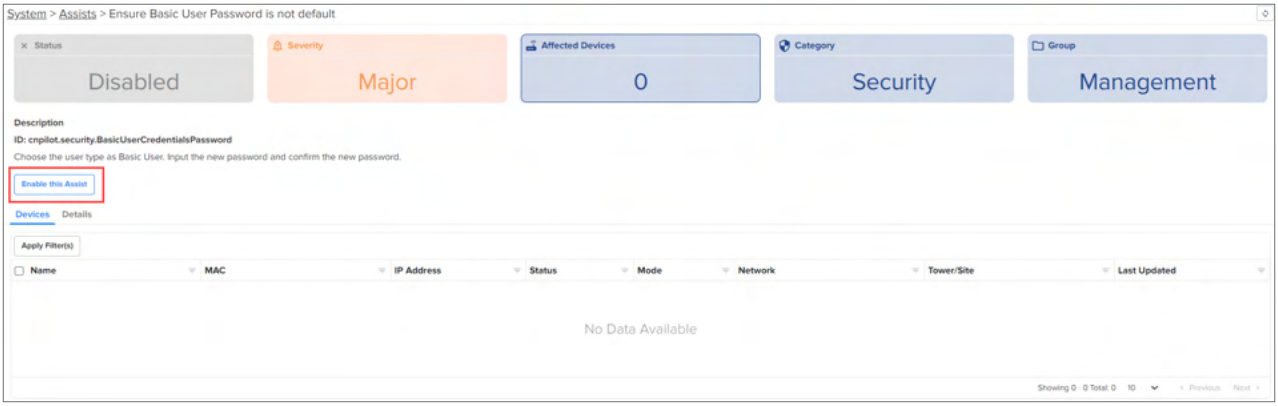
To enable assist, perform the following steps:

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



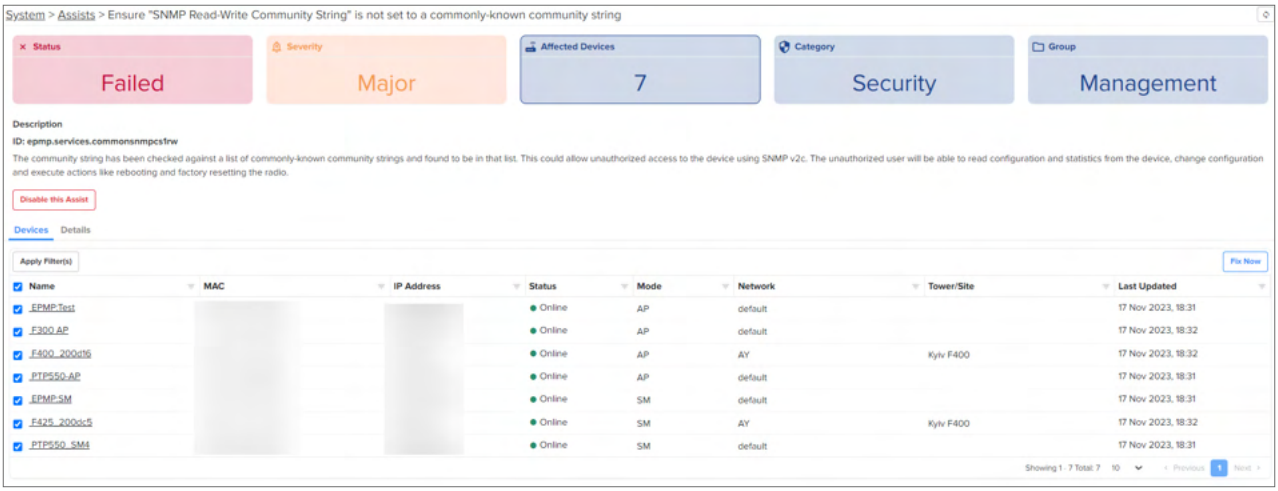
Note

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.



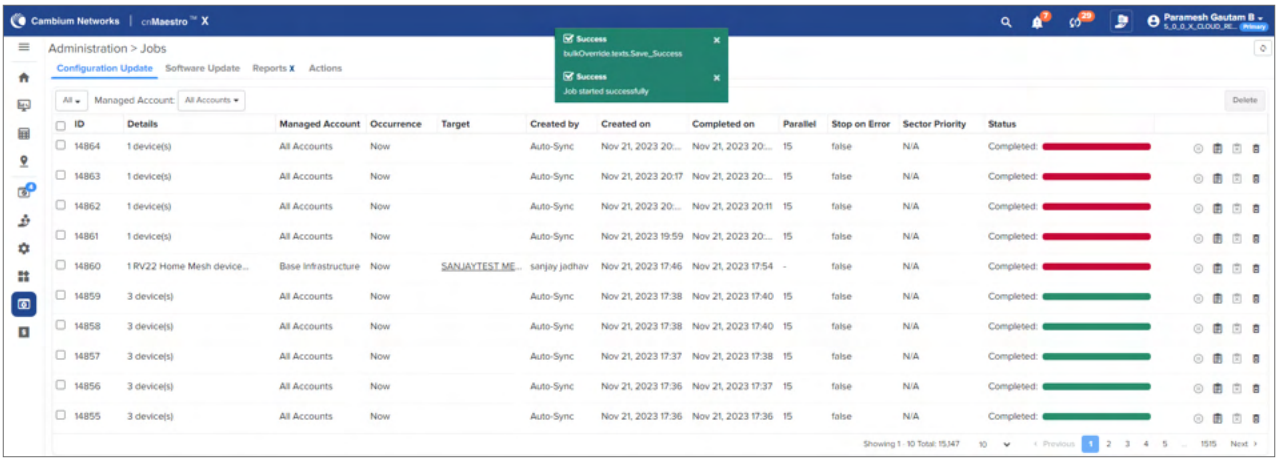
3. Click **Fix now**.

   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 95.

Figure 95 *Passed Assists*



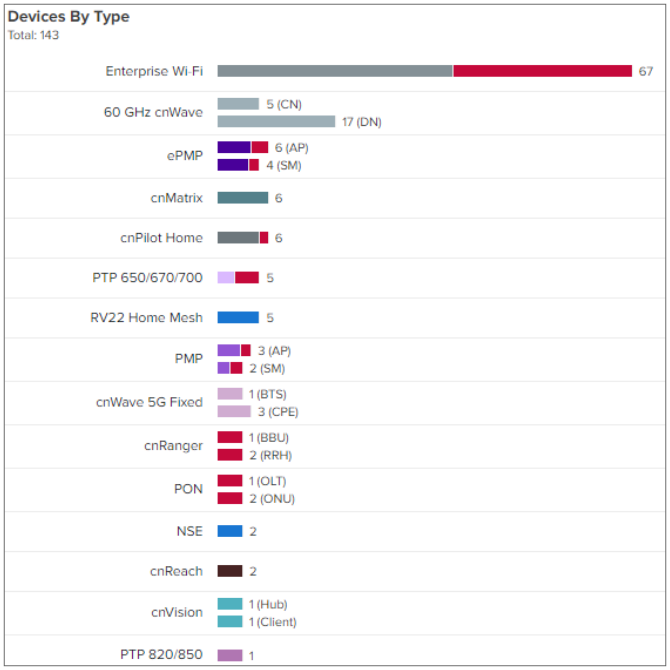
Dashboard

The **Dashboard** page in cnMaestro is customized for each device type and aggregation level (such as System, Network, Tower, and Site). Pages representing devices provide information on location, significant configuration parameters, and performance. System, Network, Tower, and Site nodes aggregate dashboard data for devices they contain.

KPI (Key Performance Indicators)

Each page has a set of KPIs tailored to the node type. These display a current value and often historical trend data over the last 24 hours.

Figure 96 *Device by Type*



Note

KPI widgets at network and Tower-level show minimum four widgets when no data is available in KPI's. Shows wireless clients KPI when at least one Wi-Fi device is available. Wireless clients KPI is moved beside Wi-Fi KPI. Machfu KPI is not supported any more.

Application History X 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 97 *Application History X*

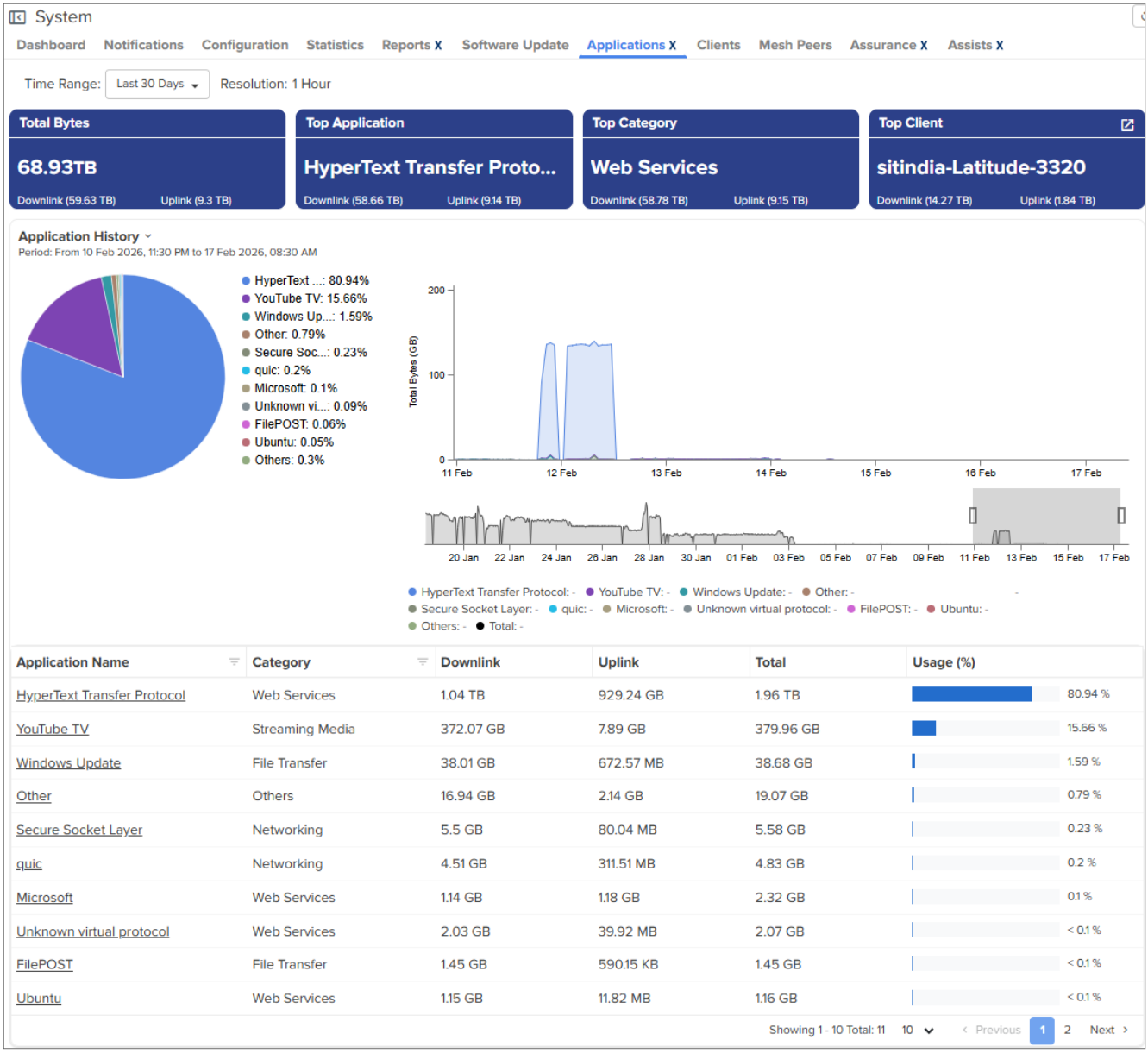


Figure 98 *Category History X*



The **System > Applications X** page displays detailed system-level application usage for a duration of 24 hours, 7 days, and 30 days. It displays usage details of the applications.

Figure 99 *System > Applications X*



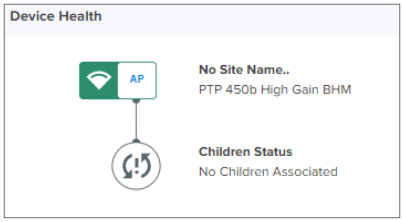
Note

- By default, the application statistics for last 24 hours is displayed.
- Application data is available for a maximum of 30 days.
- Application data is available for NSE and Enterprise Wi-Fi (XD, XE, XR, and XV) devices only.
- Application data is available only for the clients connected to NSE in Essentials accounts.

Device Health

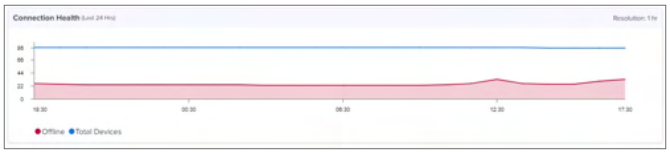
Device Health displays the health of the network from the Tower to the edge Device.

Figure 100 *Device Health*



Connection Health

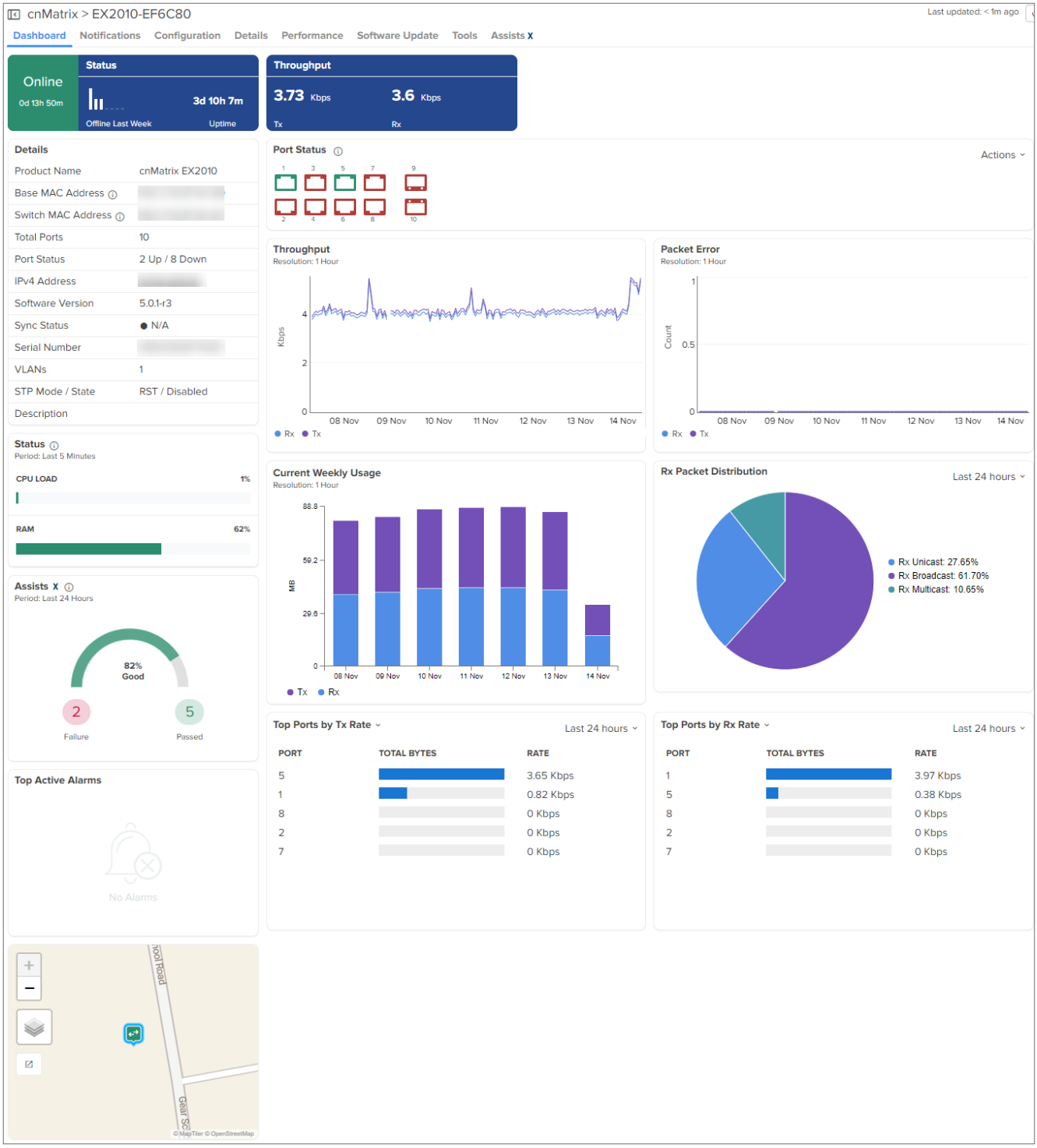
Connection Health displays the health of the devices connected to the network.



Charts and Graphs

Contextual charts and graphs provide details on important dashboard metrics.

Figure 101 *Charts and Graphs*



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, NSE devices, and cnMatrix switches)
- Home site (for RV22 Home Mesh Routers and R-series APs)

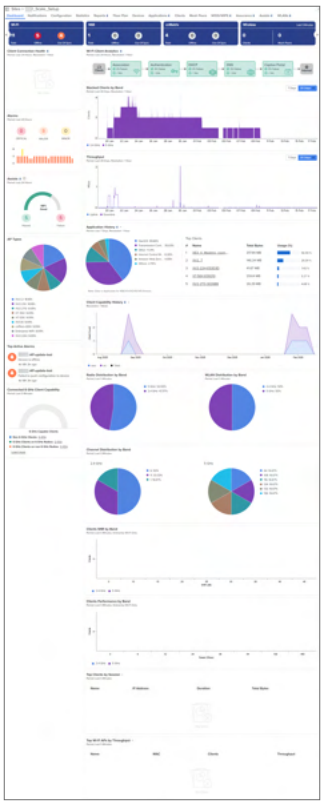
- 60 GHz cnWave site (for 60 GHz cnWave devices)
- PON site (for PON devices—OLTs, ONUs)

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

- Enterprise Site dashboard
- RV22 Home 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, NSE devices, and cnMatrix switches.



The Enterprise Site Dashboard displays the following graphics:

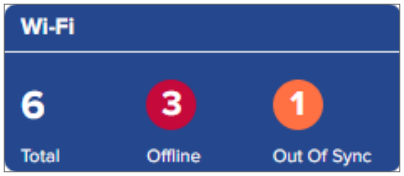
- Devices widget (Total, Offline, Out of Sync)
- Throughput
- Client Connection Health X
- Wi-Fi Client Analytics X
- Assists X
- Alarms
- Top Active Alarms
- AP Types

- Stacked Clients by Band
- 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

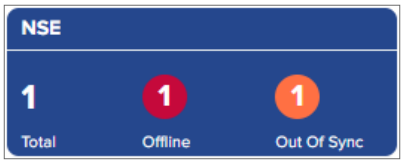
Devices widget (Total, Offline, Out of Sync)

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

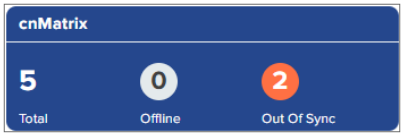
Wi-Fi APs widget (Total, Offline, Out of Sync)



NSE devices 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, NSE devices, and cnMatrix switches.

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

Figure 102 *Devices > Configuration page for Enterprise Wi-Fi APs*

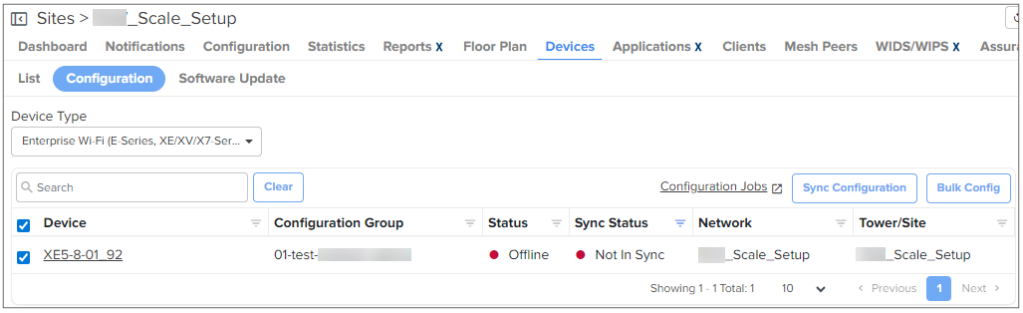


Figure 103 *Devices > Configuration page for cnMatrix switches*

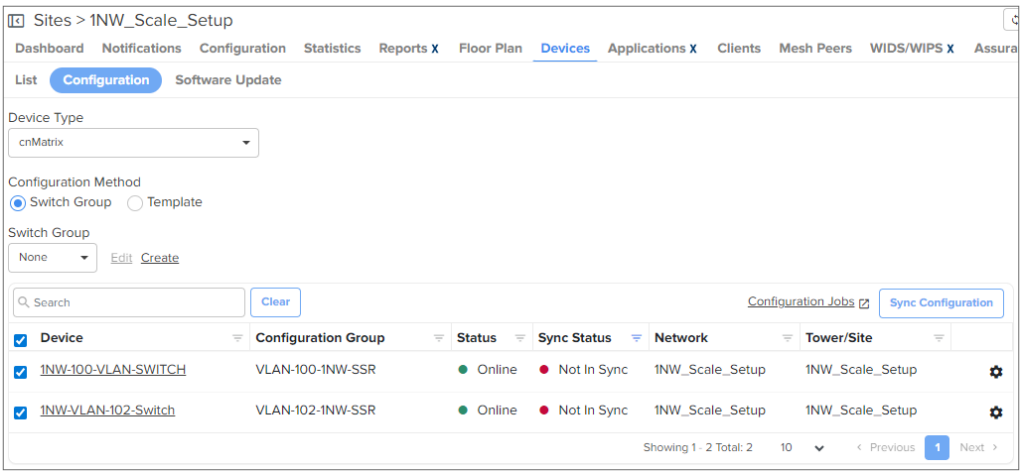
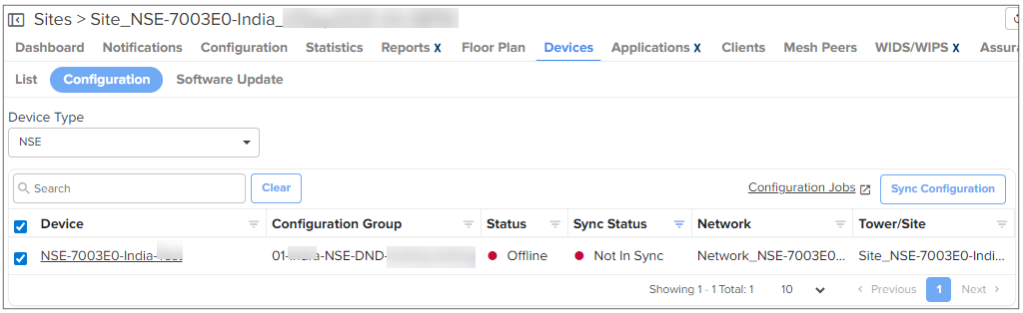


Figure 104 *Devices > Configuration page for NSE devices*



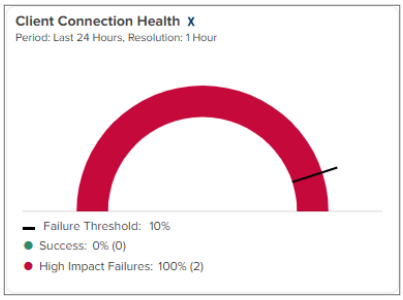
Throughput

Displays aggregated throughput for all the clients.



Client Connection Health X

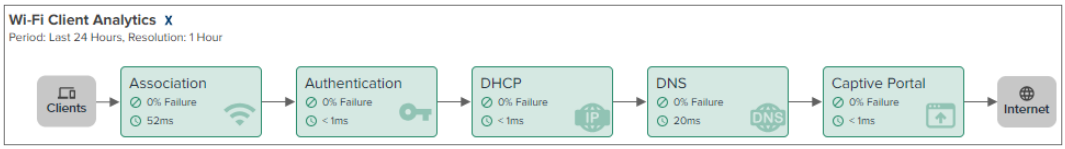
Displays the percentage of success and failed client connections in that site.



Wi-Fi Client Analytics X

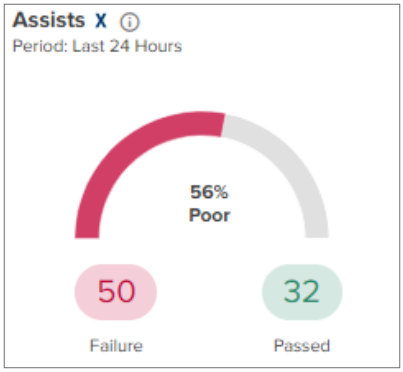
Displays the failure percentage in each stage of the client connection to the AP and subsequent network access.

For more information, refer to Assurance X.



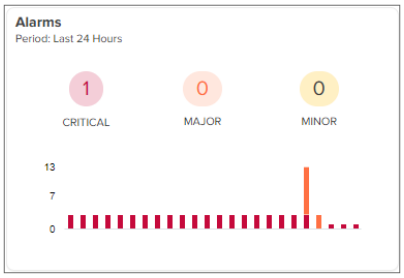
Assists X

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.



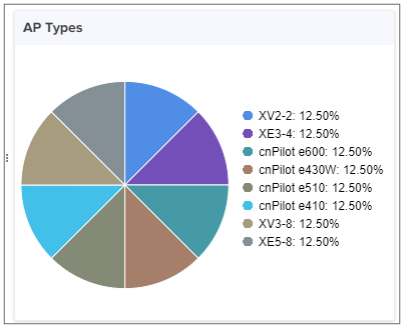
Top Active Alarms

Displays the topmost active alarms raised in that Site.



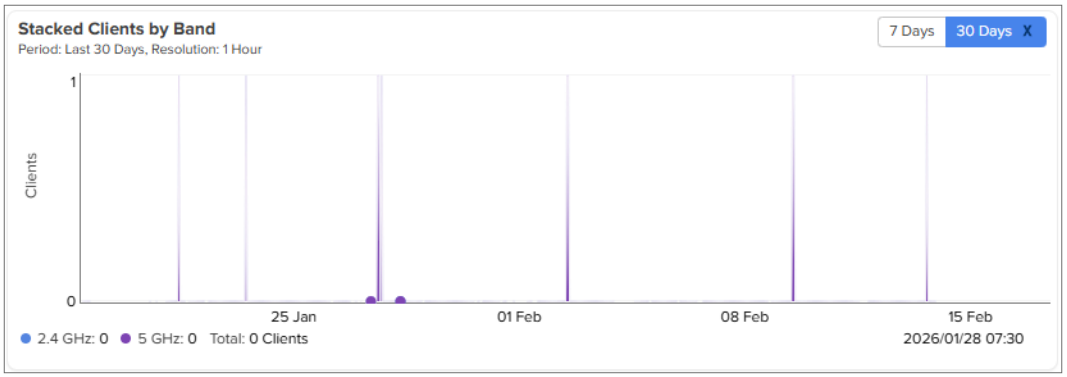
AP Types

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



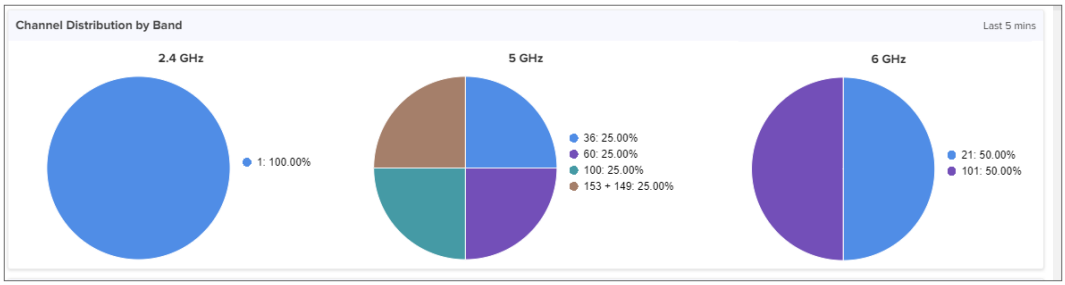
Stacked Clients by Band

Displays the number of clients connected to the APs per radio band that is supported. The data is displayed for a duration of 7 days or 30 days (**X**).



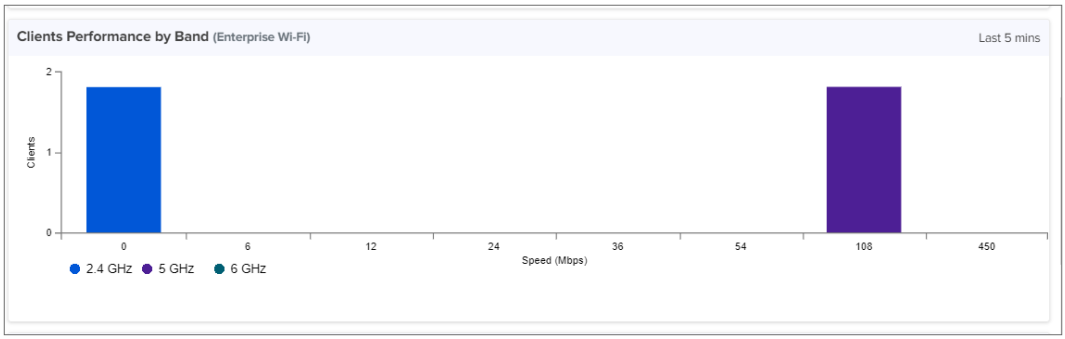
Channel Distribution by Band

Channel distribution displays usage of channels in 2.4 GHz, 5 GHz and 6 GHz. This helps in planning and implementing WLANs within a high-density environment. It displays the usage details for last 5 minutes.

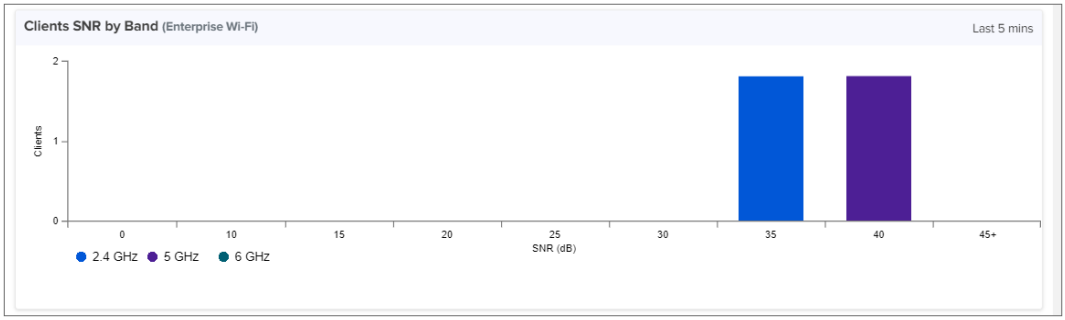


Clients Performance by Band (Enterprise Wi-Fi)

Clients performance details is displayed for last 5 minutes.



Clients SNR by Band (Enterprise Wi-Fi)



Connected 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:

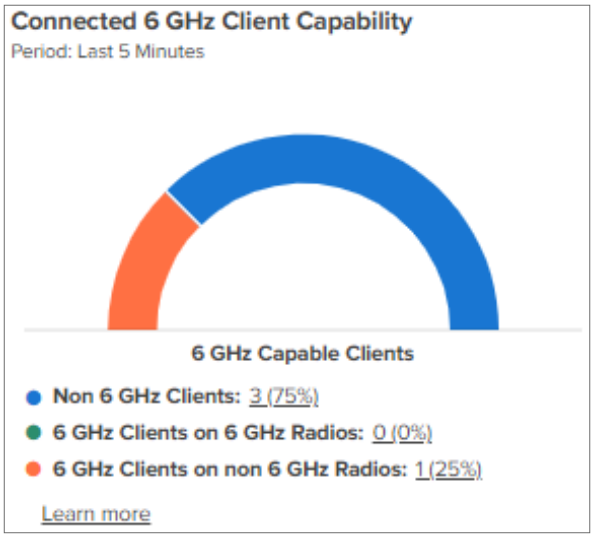
- Non 6 GHz Clients: represents non 6 GHz clients connected across the devices at the Site level.
- 6 GHz Clients on 6 GHz Radios: represents 6 GHz clients connected across the devices at the Site level.

- 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 105 *Connected 6 GHz Client Capability*



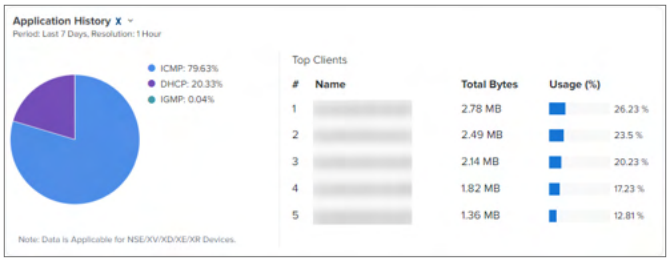
Clicking next to clients number navigates to **Wireless Clients** page.

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 (NSE/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.

Clicking on the clients in the **Top Clients** section displays the Site-specific **Client Dashboard** page. For more details, refer to Viewing a client or host-specific connection or disconnection event.



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 106 *Clients History in line chart*

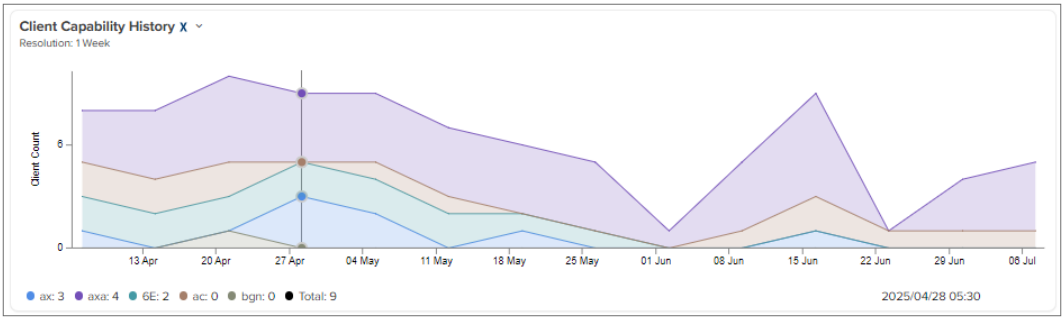
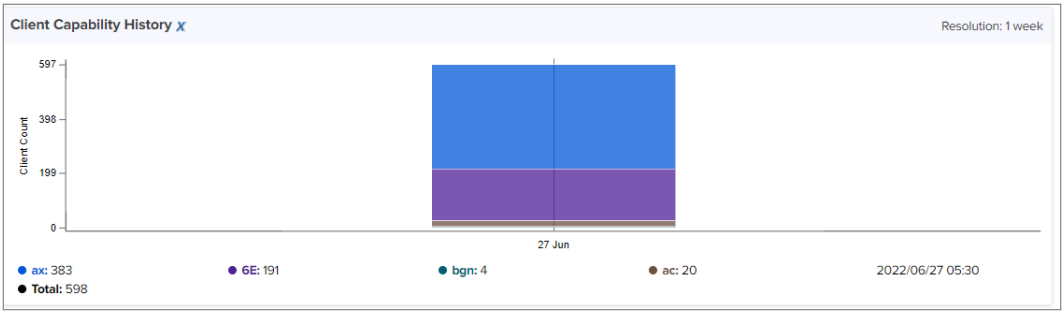
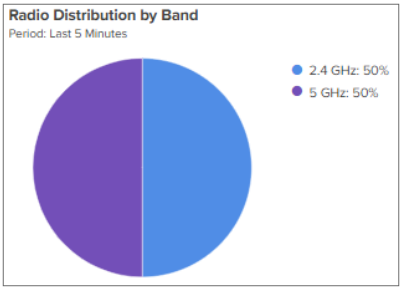


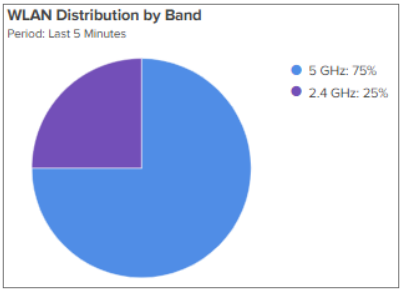
Figure 107 *Clients History in bar chart*



Radio Distribution by Band

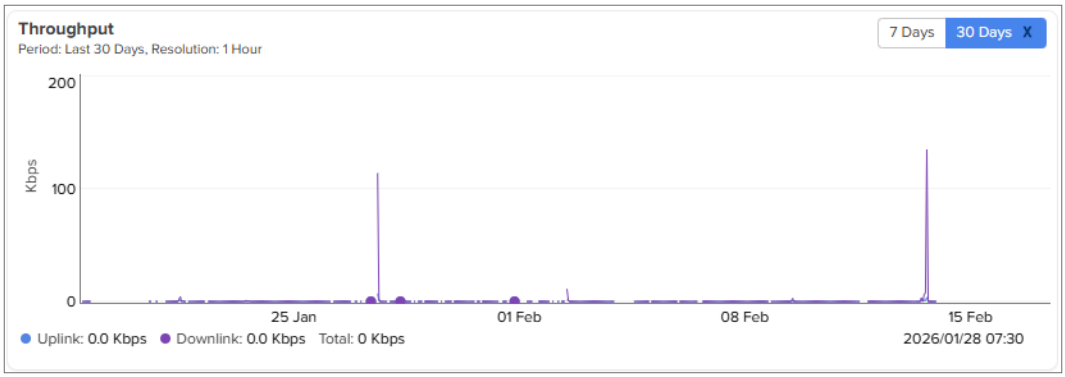


WLAN Distribution by Band



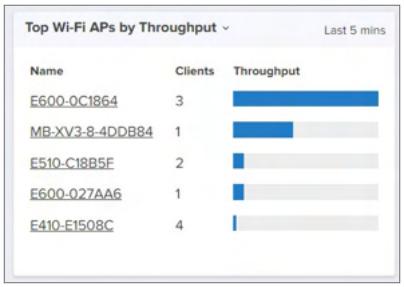
Throughput Graph

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



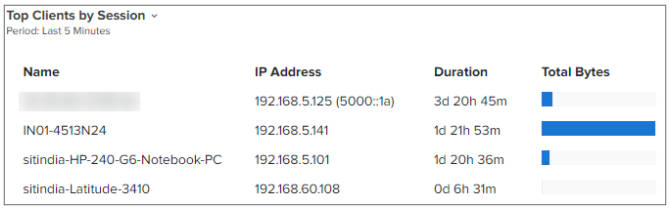
Top Wi-Fi APs by Throughput or Clients

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



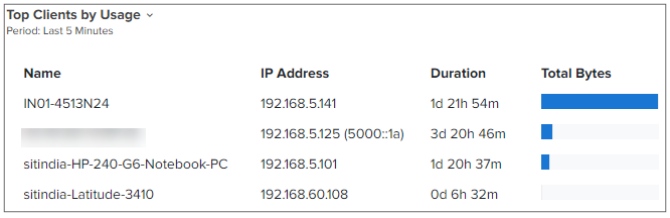
Top Clients by Session

Displays the top clients by session and the respective details.



Top Clients by Usage

Displays the top clients by usage and the respective details.



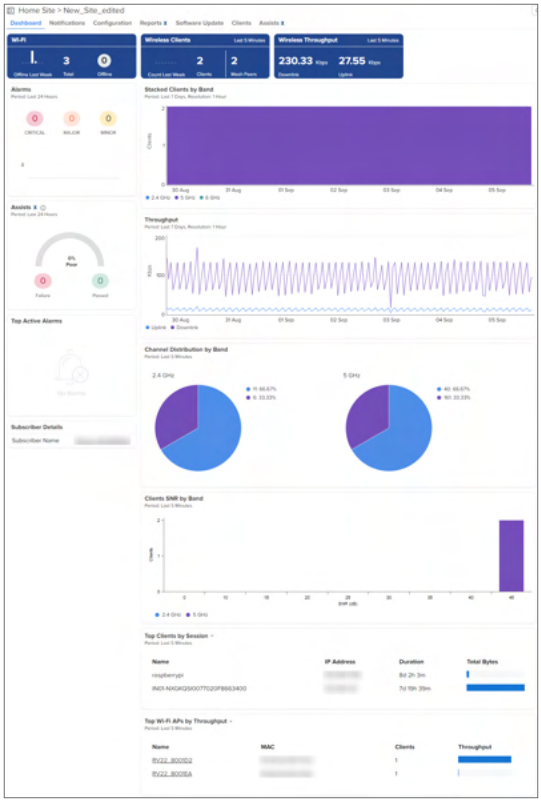
RV22 Home Site Dashboard

To view the RV22 Home Site dashboard, access the **Dashboard** page under **Monitor and Manage >** <Home-site-name> **> Dashboard**.

The dashboard displays the following widgets and graphs:

- Wi-Fi, Wireless Clients and Wireless Throughput widgets
- Alarms
- Assists X
- Top Active Alarms
- Subscriber Details
- Stacked Clients by Band graph
- Throughput graph
- Channel Distribution by Band graph
- Clients SNR by Band graph
- Top Clients by Session (or Usage)
- Top Wi-Fi APs by Throughput (or Clients

Figure 108 *RV22 Home Site Dashboard*



60 GHz cnWave Site Dashboard

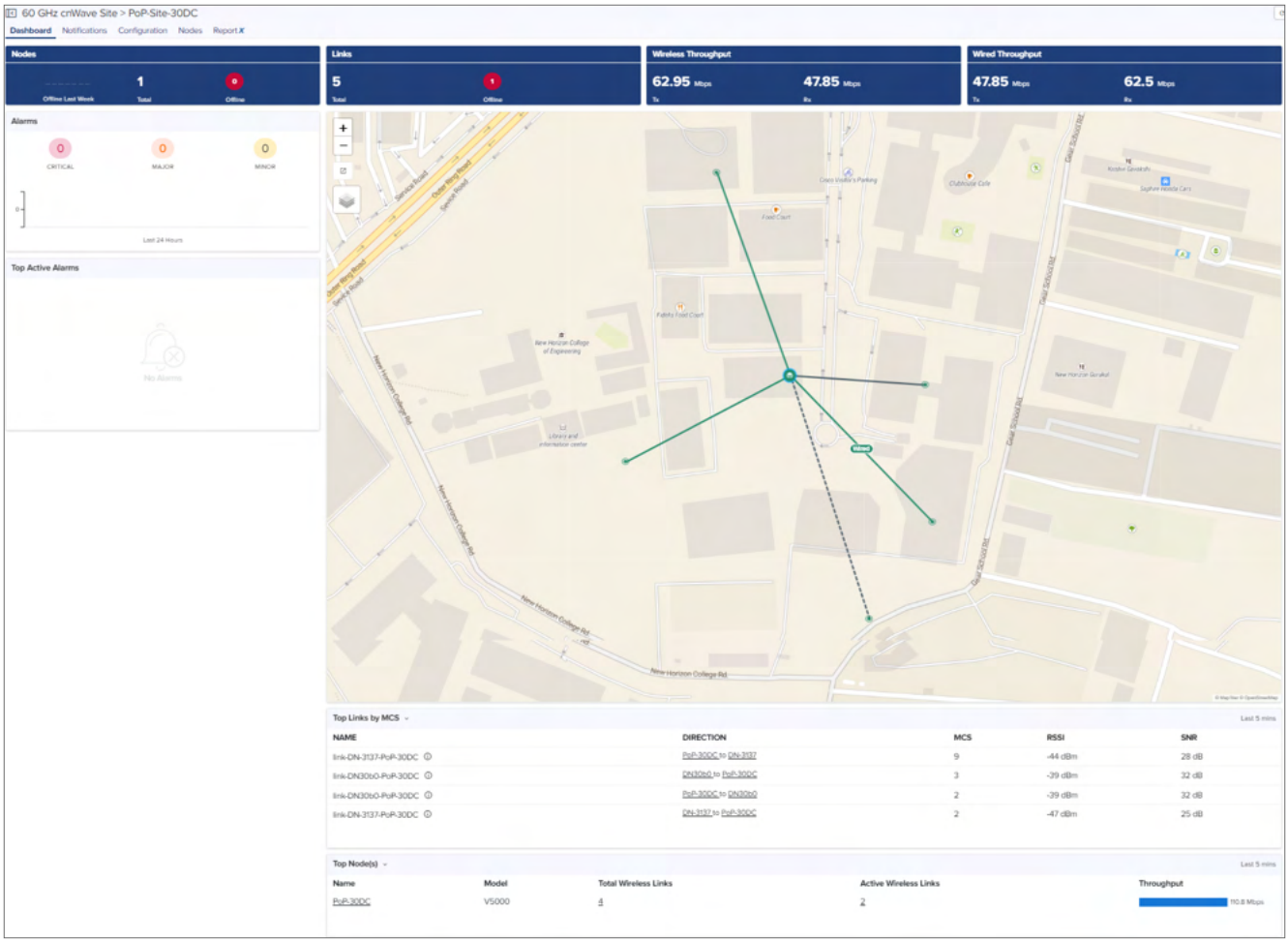
Dashboard pages are customized for each device type and aggregation level.

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 109 *60 GHz cnWave Site Dashboard*



PON Site Dashboard

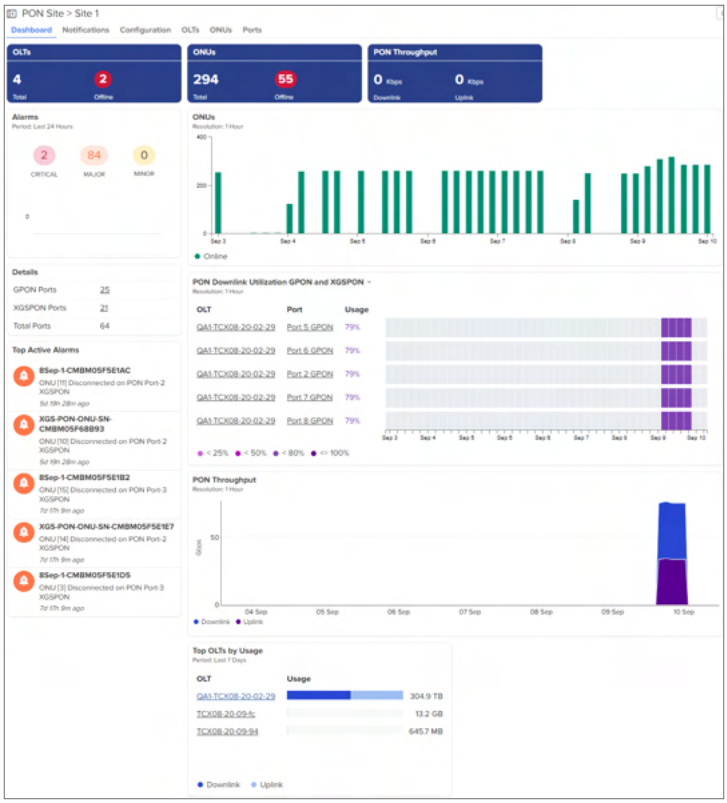
Dashboard pages are customized for each device type and aggregation level.

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 110 *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 19 *Notification overview*

Type	Description
Alarms	Alarms indicate state and persist as long as the problematic activity continues; they reflect the current health of the devices in the network.
Alarms History	Expired Alarms are added to the Alarm History. The Alarm History page displays historical active alarm counts. **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 111 and Figure 112:

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

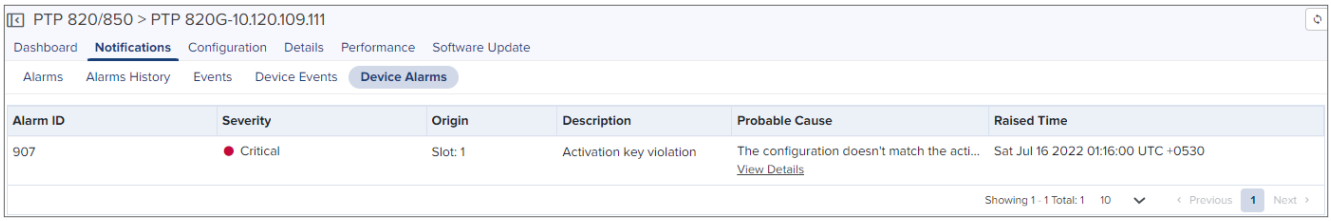
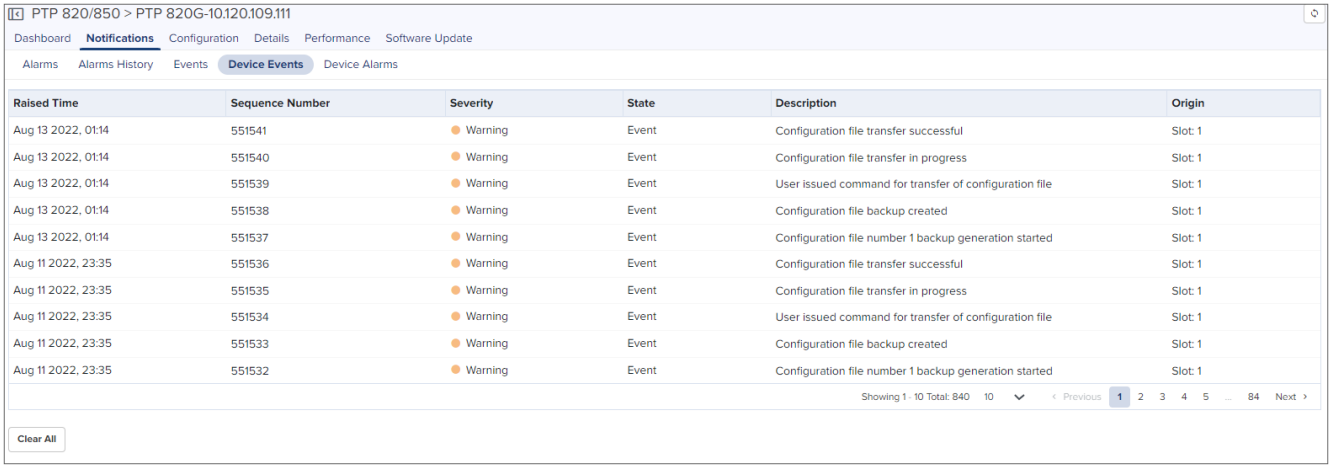


Figure 112 *PTP 820/850 Device Events*



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 20 *Event Severity*

	Severity	Definition
	Critical	Catastrophic problem that makes the product/feature unusable.
	Major	Issue that greatly degrades the product/feature, but it is still usable.
	Minor	Limited issue that alters product functionality in a targeted way.
	Notify	Message used primarily for information.

Event Export

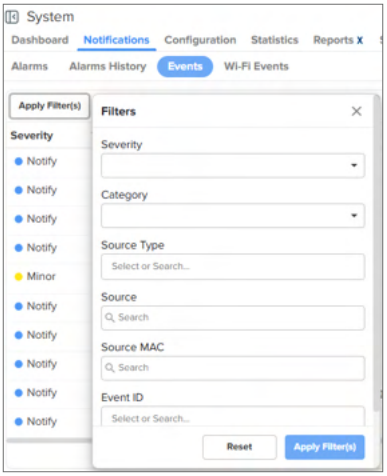
The data in the Event table is exported in a CSV file format. The following export options are available:

- Export page as CSV
- Export all as CSV

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 113 *Events: New Filter*

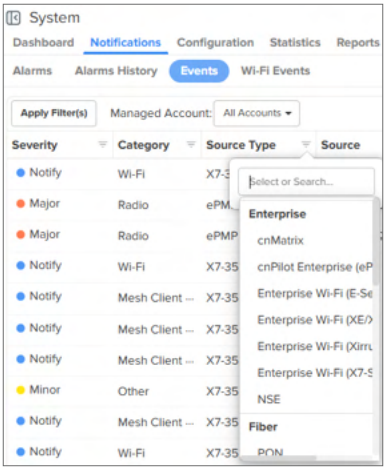


You can manually filter or search by typing parameters in the column header of the Events table.

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 114 *Events: Source Type filter*



The **Source Type** column header is grouped based on the Device or System events. The **Event ID** column header is grouped based on the category names. The category name with corresponding subcategories and codes are shown in Table 21.

Figure 115 *Events: Name filter*

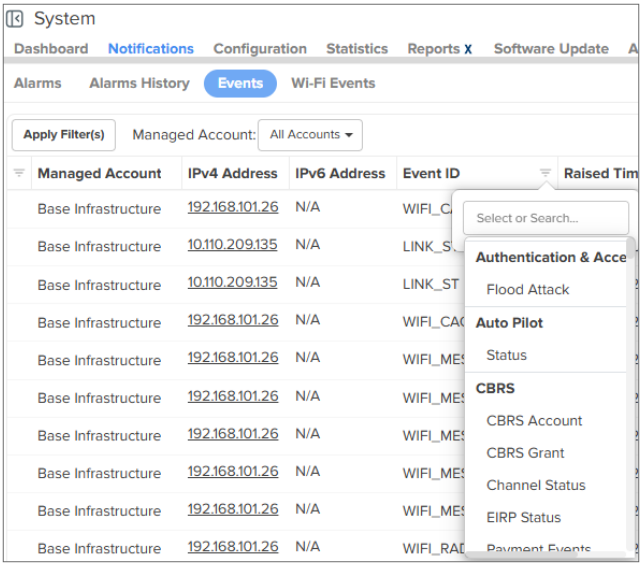


Table 21 *Category Names and Codes*

Category	Subcategory	Codes
Authentication & Access Control	Flood Attack	WIDS_AUTH_FLOOD
		WIDS_DEAUTH_FLOOD
Auto Pilot	Auto Pilot Status	AUTOPILOT_ADDED_AP
		AUTOPILOT_AP_CONNECTED
		AUTOPILOT_AP_DISCONNECTED
		AUTOPILOT_REMOVED_AP
CBRS	CBRS Account	CBRS_ACCOUNT
	CBRS Grant	CBRS_ALARM_PROXY_TIME_MISMATCH
		CBRS_GRANT_SUSPEND
		CBRS_GRANT_TERMINATE
		CBRS_OPERATIONAL_PARAM_CHANGE
		CBRS_TX_DISABLE
		CBRS_TX_ENABLE
		SM_RECONNECT_FAILURE
	Channel Status	CBRS_ATTEMPT_CHANNEL_EXPANSION
		CBRS_START_CHANNEL_HUNT
		CHANNEL_CHANGE
	EIRP Status	CBRS_EIRP_CHANGE
	Payment Events	CBRS_PAYMENT
	SAS Notfications	SAS_ID_GENERATION
Cloud Sync	Cloud Connectivity	CLOUD_SYNC
		CLOUD_SYNC_STATUS_DOWN
		CLOUD_SYNC_STATUS_UP

Category	Subcategory	Codes
Configuration	Config Sync Status	CFG_IMP
		CFG_EXP
		CONFIG_SYNC
		CFG_UPD_ST
		SYSTEM_CONFIG_APPLIED
	Warning	DISALLOWED_CONFIG_OBJECT
		UNSUPPORTED_APPS_DETECTED
		UNSUPPORTED_APPS_DETECTED_CFG_PUSH
		UNSUPPORTED_CONFIG_OBJECT

Category	Subcategory	Codes
Device	AFC	AFC_CHANNEL_NOT_AVAILABLE

Category	Subcategory	Codes
		AFC_EIRP_CHANGED

Category	Subcategory	Codes
		AFC_SERVER_NOT_REACHABLE

Category	Subcategory	Codes
		AFC_WAITING_FOR_GPS_COORDINATES

Category	Subcategory	Codes
		WIFI_AFC_AGENT_STATUS

Category	Subcategory	Codes
		WIFI_AFC_JSON_WEB_TOKEN

Category	Subcategory	Codes
		WIFI_AFC_REGULATORY_DATA_VALIDITY

Category	Subcategory	Codes
		WIFI_AFC_SERVER_RESPONSE_FAILURE

Category	Subcategory	Codes
		WIFI_AFC_SERVER_RESPONSE_SUCCESS

Category	Subcategory	Codes
	Connection Status	INTERPOP_INSUFFICIENT_MTU

Category	Subcategory	Codes
		INTERPOP_SUFFICIENT_MTU

Category	Subcategory	Codes
	CPE	SECTOR_HAS_IDENTICAL_CPE_VERSION

Category	Subcategory	Codes
		SECTOR_HAS_MIXED_CPE_VERSION

Category	Subcategory	Codes
	Default AUTH key	DEF_KEY_USED_TRAP

Category	Subcategory	Codes
	Device Notifications	CISCO_POWER_SUPPLY_STATUS

Category	Subcategory	Codes
		IET8222_MPPHSDR_INFO

Category	Subcategory	Codes
		IET8222_MPPHSDR_NOTICE

Category	Subcategory	Codes
		IET8222_MPPHSDR_WARNING

Category	Subcategory	Codes
		SPECTRUM_ANALYSIS

Category	Subcategory	Codes
	Device Up/Down	STATUS_DOWN

Category	Subcategory	Codes
		STATUS_UP

Category	Subcategory	Codes
	Interface Status	DHCP_CLIENT_UPD

Category	Subcategory	Codes
		LLDP_ADR_EVENT

Category	Subcategory	Codes
		NNI_INTERFACE_DOWN

Category	Subcategory	Codes
		NNI_INTERFACE_UP

Category	Subcategory	Codes
		PBA_AV_CLIENT_AUTH_FAIL

Category	Subcategory	Codes
		PBA_DYN_DATA

Category	Subcategory	Codes
		RENEW_INTERFACE_IP

Category	Subcategory	Codes
		WANLB_WANLB_LINK_UP

Category	Subcategory	Codes
	Link Status	ETHERNET_AT_FULL_SPEED

Category	Subcategory	Codes
		ETHERNET_NOT_AT_FULL_SPEED

Category	Subcategory	Codes
	Onboarding	ONBOARDING

Category	Subcategory	Codes
	PoE Status	SYSTEM_POWER_POLICY

Category	Subcategory	Codes
	Port Status	ETHERNET_PORT_DOWN

Category	Subcategory	Codes
		ETHERNET_PORT_UP

Category	Subcategory	Codes
		SFP_PORT1_DOWN

Category	Subcategory	Codes
		SFP_PORT1_UP
		SFP_PORT2_DOWN
		SFP_PORT2_UP
	RADIUS Events	RADIUS_CONNECTED
		RADIUS_DISCONNECTED
	Reboot	SA_MODE
		SYS_REB
		SYSTEM_SYSTEM_ADMIN_REBOOT
	S2S VPN	S2SVPN_3_CHILD_SA_UNINSTALLED
		S2SVPN_3_IKE_DOWN
		S2SVPN_3_IKE_FAILED
		S2SVPN_4_CHILD_SA_INSTALLED
		S2SVPN_4_IKE_UP
	Smart Antenna Events	BSA_ST
	Status	AP_REG
		ASSETMGMT_AEROSCOUT_SRV_DOWN
		AUTHENTICATION_FAILURE
		CAEM_VOLTAGE_NOTIFICATION
		GATEWAY_REACHABLE
		GATEWAY_UNREACHABLE
		L2GRE_TUNNEL_DOWN
		L2GRE_TUNNEL_UP
		SYS_UP
		SYSTEM_EVENT_MSG
		TOPOLOGY_UPDATE
		WANLB_WANLB_LINK_DOWN

Category	Subcategory	Codes
Device Agent	Warning	PBA_FILE_DOWN_FAIL
		PMAC_UPD
		REGULATORY_FAIL
		STA_REG_FAIL
		THRESH_CLIENT_COUNT
		THRESH_CPU_UTIL
		THRESH_DEVICE_TRAFFIC
		USER_ADDED
		USER_DELETE
		USER_LOGIN
		USER_LOGOUT
		USER_PASSWORD_UPDATED
		WIFI_RADIUS_AUTH_SERVER_UNRESPONSIVE
	Status	COLD_START
		WARM_START
DNS	Security	DNS_REQUEST_REJECTED
E2E	Upgrade	E2E_CTLR_IMG_UPD
GPS	GPS Status	GPS_FW_UPD_ST
		GPS_SYNC
		GPS_SYNC_ST
		GPS_VER
HA	Cluster Status	HA_SERVICE
		HA_STATE_CHANGE
High Availability	Operations	HA_STATE_CHANGE_EVENT
Mesh Client Status	Status	WIFI_MESH_CLIENT_CONNECTED
		WIFI_MESH_CLIENT_DISCONNECTED
		WIRED_MESH_CLIENT_CONNECTED
Misc	Others	unknown

Category	Subcategory	Codes
Monetization	Monetization State Update	OFFLINE_NOC_ACTIVATED_SUCCESSFULLY
		OFFLINE_NOC_AMENDED_SUCCESSFULLY
		ONPREM_SUBSCRIPTION_FEATURE_STATE_ CHANGE
		ONPREM_SUBSCRIPTION_FEATURE_STATE_ TRANSITION
		SUBSCRIPTION_FEATURE_STATE_CHANGE
		SUBSCRIPTION_FEATURE_STATE_TRANSITION
		SUBSCRIPTION_STATE_CHANGE
	Monetization Subscription State	ONPREM_SUBSCRIPTION_DEFICIT
		SUBSCRIPTION_DEFICIT
		SUBSCRIPTION_FEATURE_EXPIRY_NOTICE
		SUBSCRIPTION_SLOT_DEFICIT
Network	AP Connectivity	NETWORK_WWAN_BACKUP
		NETWORK_WWAN_DOWN
		NETWORK_WWAN_UP
		SYSTEM_AP_UPLINK_STATUS
	Authentication	NETWORK_PPPOE_AUTH_FAILED
	DHCP	DHCP_CLIENT_IP
		DHCP_COMPLETE_EVENT
		DHCP_SRVR_IP_ASSIGNED
		DHCPSRVR_IP_ASSIGNED
		DHCPSRVR_POOL_STARTED
		NETWORK_DHCP_MTU_IGNORED
		NETWORK_RENEW_INTERFACE_IP
	Network	MGMT_VLAN_CHANGED
		NETWORK_INTERFACE_CHANGE
		NETWORK_STATUS_DOWN
		NETWORK_STATUS_UP
	PPPoE Status	PPPOE_AUTH_FAILED
		PPPOE_CONNECTED
	Tunnel	NETWORK_TUNNEL_DOWN
		NETWORK_TUNNEL_UP
	WAN Connectivity	NETWORK_PPPOE_CONNECTED
		NETWORK_PPPOE_DISCONNECTED

Category	Subcategory	Codes
PON	Interface Status	PON_INTERFACE_DOWN
		PON_INTERFACE_UP
	ONU Notifications	ONU_ACTIVATED
		ONU_DEACTIVATED
		ONU_DGI
		ONU_DISCONNECTED
		ONU_DISCOVERED
		ONU_PROVISIONED
	Status	PON_LOS
		PON_LOS_CLEAR
	Upgrade	OLT_SW_UPGRADE_FAILED
		OLT_SW_UPGRADE_SUCCESS

Category	Subcategory	Codes
PTP	Device Notifications	INSTALL_ARM_STATE
		LBT_DETECTED
		LICENSE_REMAINING_TRIAL_PERIOD
		REGULATORY_BAND
		SNTP_SYNC
		TDD_SYNC
		WIRELESS_LINK_STATUS
	Port Status	AUX_PORT_POE_OUTPUT_STATUS
		AUX_PORT_STATUS
		DATA_BRIDGING_STATUS
		MAIN_PSU_PORT_STATUS
		SFP_PORT_STATUS
	Warning	AUX_PORT_CONFIG_MISMATCH
		CAPACITY_VARIANT_MISMATCH
		DFS_IMPULSIVE_INTERFERENCE
		INCOMPATIBLE_MASTER_SLAVE
		INCOMPATIBLE_REGULATORY_BANDS
		LINK_MODE_OPTIMIZATION_MISMATCH
		MAIN_PSU_PORT_CONFIG_MISMATCH
		NO_WIRELESS_CHANNEL_AVAILABLE
		PORT_ALLOCATION_MISMATCH
		SFP_ERROR
		SFP_PORT_CONFIG_MISMATCH
		UNIT_OUT_OF_CALIBRATION
Radio	DFS	DFS_ST
		RADAR_DETECT
	Interface Status	LINK_DOWN
		LINK_UP
	Radio Link	LINK_ST
	Warning	RF_OVER_LOAD

Category	Subcategory	Codes
Rate Limit	Client Events	CLIENT_EVENT_BLOCKED
		CLIENT_EVENT_RATELIMIT
		CLIENT_EVENT_UN_BLOCKED
	Device Events	DNS_EVENT_BLOCKED
		DNS_EVENT_UN_BLOCKED
		EVENT_BLOCKED
		EVENT_RATELIMIT
		EVENT_UN_BLOCKED
		IPS_EVENT_BLOCKED
		IPS_EVENT_UN_BLOCKED
	Metric Events	METRIC_BLOCKED
		METRIC_RATELIMIT
		METRIC_UN_BLOCKED
Security	Configuration	IPS_INVALID_CONFIG
	Operations	IPS_RULESET_UPDATE
		IPS_RULESET_UPDATE_FAILED
		IPS_START_FAILED
		UTM_ON_DEMAND_PORTSCAN
	Threat	IPS_THREAT_DETECTED
SM	SM Status	STA_DROP
		STA_REG
		STA_REJECT

Category	Subcategory	Codes
System	AP Internal	SYSTEM_RESET_ENV
	AP Operations	SYSTEM_CRITICAL_LOW_POWER
		SYSTEM_FIRMWARE_RECOVERY
	AP Reboot	SYSTEM_CFG_OVERWRITE_REBOOT
	Backup Notifications	SYSTEM_BACKUP
		SYSTEM_RESTORE
	Configuration	SYSTEM_CC_NOTSET
	Configuration	SYSTEM_CONFIG_APPLIED
		SYSTEM_CONFIG_APPLY_FAIL
		SYSTEM_CONFIG_DEFAULTED
	email	SYSTEM_EMAIL_NOTIFICATION
	Notifications	SYSTEM_CPU_UTILIZATION
		SYSTEM_DISK_UTILIZATION
		SYSTEM_MEMORY_UTILIZATION
		SYSTEM_PROCESS_STATUS
	Operations	SYSTEM_ADMIN_REBOOT
		SYSTEM_AUTO_VLAN_CONFIG_MISMATCH
		SYSTEM_CFG_FALLBACK_REBOOT
		SYSTEM_LOW_MEMORY_RESTART
		SYSTEM_RESTARTING_PROCESS
		SYSTEM_WATCHDOG_RESET
		SYSTEM_WATCHDOG_UNRESP
	Radio	SYSTEM_RADIOS_SHUTDOWN
	Security	SYSTEM_INVALID_LOGIN_ATTEMPT
	Threshold Events	THRESHOLD_CLIENT_CONNECTION_HEALTH
	Upgrade	SYSTEM_FW_UPGRADE_FAILED
		SYSTEM_FW_UPGRADE_SUCCESS
		SYSTEM_REINITIALIZED_NOR
		SYSTEM_UPGRADE
	Upload Status	SYSTEM_ADD_AP_FIRMWARE
	Warning	DISK_NOT_AVAILABLE_BACKUP
		SYSTEM_INSUFFICIENT_POWER_MITIGATING
		SYSTEM_LOGIN
		WEAK_ADMIN_PWD

Category	Subcategory	Codes
Upgrade	Site Upgrade	SITE_SW_SYNC
	Upgrade Status	FW_UPD_ST
		MIN_FW_VER
VPN	RWVPN	RWVPN_CERT_LOAD_FAILED
	Site-to-Site VPN	S2SVPN_CHILD_SA_INSTALLED
		S2SVPN_CHILD_SA_UNINSTALLED
		S2SVPN_IKE_DOWN
		S2SVPN_IKE_FAILED
		S2SVPN_IKE_UP
WAN	Status	WANLB_MONITOR_HOST_REACHABLE
	WAN Connectivity	WANLB_LINK_DOWN
		WANLB_LINK_UP
Webhook	Webhook Status	WEBHOOK_NOTIFY
WIDS	Ad-hoc	WIDS_ADHOC_NW_DETECTION
	Flood Attack	WIDS_ASSOC_FLOOD
		WIDS_DISASSOC_FLOOD
		WIDS_EAPOL_FLOOD
	Wireless	WIDS_DETECT_BSSID

Category	Subcategory	Codes
Wi-Fi	AP Connectivity	WIFI_AUTO_DETECT_BACKHAUL

Category	Subcategory	Codes
	AP Operations	WIFI_MONITOR_HOST_DOWN

Category	Subcategory	Codes
		WIFI_MONITOR_HOST_UP

Category	Subcategory	Codes
		WIFI_SA_WLAN_DISABLED

Category	Subcategory	Codes
		WIFI_SA_WLAN_ENABLED

Category	Subcategory	Codes
	AP Radios	SYSTEM_CONFIG_CAP_POWER

Category	Subcategory	Codes
		SYSTEM_CONFIG_ENFORCE_POWER

Category	Subcategory	Codes
		WIFI_AUTORF_CHANNEL_SWITCH

Category	Subcategory	Codes
		WIFI_AUTORF_TXPOWER

Category	Subcategory	Codes
		WIFI_CAC_COMPLETED

Category	Subcategory	Codes
		WIFI_CAC_STARTED

Category	Subcategory	Codes
		WIFI_CHANWIDTH_CHANGE

Category	Subcategory	Codes
		WIFI_NF_CHANNEL_SWITCH

Category	Subcategory	Codes
		WIFI_NOL_ADDED

Category	Subcategory	Codes
		WIFI_NOL_DELETED

Category	Subcategory	Codes
		WIFI_RADAR_DETECTED

Category	Subcategory	Codes
	Authentication	WIFI_CLIENT_LDAP_AUTH_REJECT

Category	Subcategory	Codes
		WIFI_CLIENT_LDAP_AUTH_SUCCESS

Category	Subcategory	Codes
		WIFI_CLIENT_LDAP_AUTH_TIMEOUT

Category	Subcategory	Codes
		WIFI_CLIENT_MAC_ACL_SUCCESS

Category	Subcategory	Codes
		WIFI_CLIENT_RADIUS_AUTH_REJECT

Category	Subcategory	Codes
		WIFI_CLIENT_RADIUS_AUTH_TIMEOUT

Category	Subcategory	Codes
	Auto-Channel	WIFI_ACS_SELECTED_CHANNEL

Category	Subcategory	Codes
		WIFI_ACS_TRIGGERED

Category	Subcategory	Codes
	Auto-RF Status	WIFI_AUTORF_TRIGGER

Category	Subcategory	Codes
	Configuration	WIFI_AUTOCELL_BYBAND_REQUIRES_OCS_ENABLE
	Network	WIFI_CLIENT_ICMP_FLOOD
	Radio	WIFI_IGNORE_CAC
	RADIUS	WIFI_CLIENT_RADIUS_ACCT_TIMEOUT
		WIFI_CLIENT_RADIUS_AUTH_SUCCESS
		WIFI_RADIUS_SERVER_CONFIG_REQUIRED
	Security	WIFI_CLIENT_ARP_FLOOD
	Security Threat	WIFI_SPOOFED_ARP_DETECTED
	Wi-Fi Associations	WIFI_CLIENT_AUTH_SUCCESS
		WIFI_CLIENT_CONNECTED
		WIFI_CLIENT_CONNECTION_FAILED
		WIFI_CLIENT_DISCONNECTED
		WIFI_CLIENT_EROAM_DISCONNECTED
		WIFI_CLIENT_ROAMED
		WIFI_CLIENT_ROAMED_WITHIN_AP_WLAN
		WIFI_CLIENT_WPA2_INVALID_PSK
		WIFI_DISALLOW_CLIENT
		WIFI_DYN_AUTH_COA_REQ
		WIFI_DYN_AUTH_DISCONNECT_REQ
	Wi-Fi Guest	WIFI_CLIENT_GUEST_LOGIN_SUCCESS
		WIFI_CLIENT_GUEST_LOGOUT_SUCCESS
		WIFI_CLIENT_GUEST_SESSION_TIMEOUT
	Wi-Fi Mesh	WIFI_MESH_BASE_REC_TRIGGERED
		WIFI_MESH_LOOP
		WIFI_MESH_XTNDED_DEV
	Wi-Fi AP Status	SECURITY
		SSID
		SYSTEM
		SYSTEM_WIRELESS_SERVICES_ENABLED
	Wi-Fi Channel	WIFI_ACS_CHANNEL_SWITCH
		WIFI_ACS_TRIGGERED_ON_RADIO
		WIFI_AUTORF_ICA_COMPLETE

Category	Subcategory	Codes
Wi-Fi Client	Wireless	DPI_APP_EVENT
		SYSTEM_RADIOS_DISABLED
		SYSTEM_RADIOS_ENABLED
		WIFI_CLIENT_QUOTA_EXHAUSTED
		WIFI_RADIO_ACS_CHANNEL_LIST
		WIFI_RADIO_DISABLED
	Client Dissociation	WIFI_CLIENT_DISCONNECT_INFO
	RADIUS Events	WIFI_6_CLIENT_RADIUS_AUTH_SUCCESS
	Wi-Fi Client Status	WIFI_CLIENT
WIPS	Security	WIPS_DEAUTH_CLIENT
Wired	Status	WIRED_CLIENT_CONNECTED

Alarms

Alarm Life Cycle

The basic alarm life cycle has the following states:

Table 22 *Alarm Life Cycle*

State	Description
Acknowledged	Active alarms can be acknowledged, which signifies they are known and being handled. Acknowledged alarms are not included in the total alarm count.
Active	The alarm remains active until the combination of inputs that generated it are cleared.
Inactive	Inactive alarms remain visible in the active Alarm Table for 10 minutes, before they are moved to Alarm History. An alarm becomes inactive when the inputs that generated it are no longer 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 23 *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

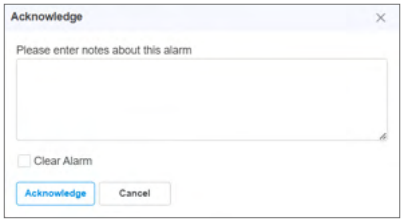
Table 24 *Alarm Types*

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 116 *Alarm Acknowledgment*

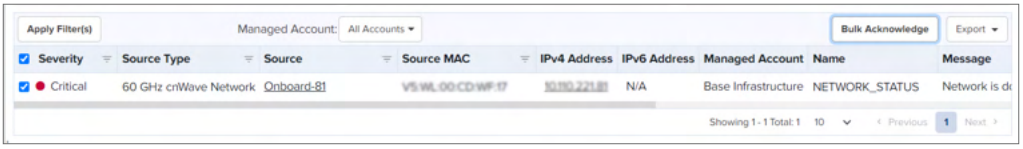


Alarm Bulk Acknowledgment

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

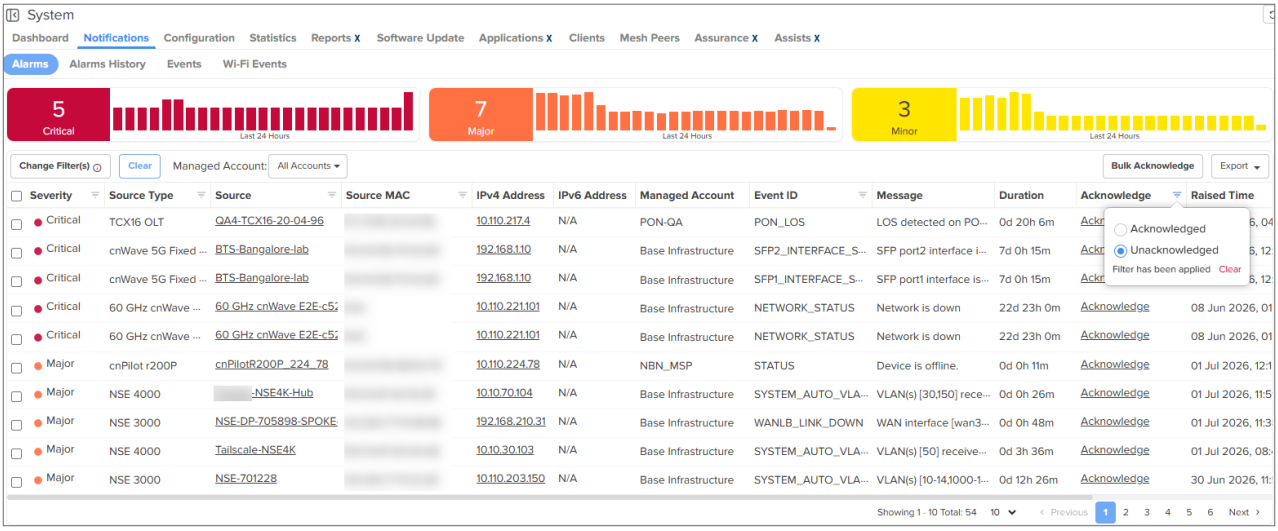
1. Navigate to the **Monitor and Manage** > **Notifications** > **Alarms** page.

   Figure 117 *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:





Note

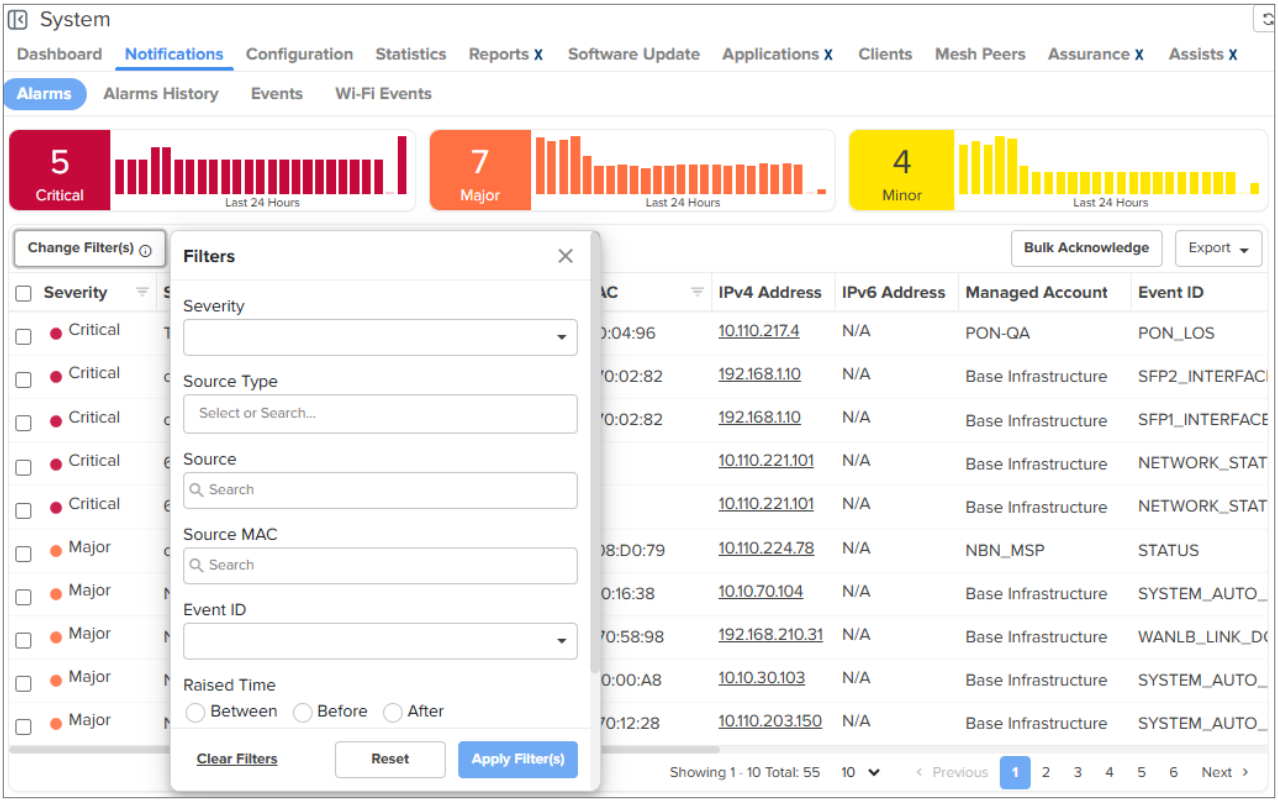
Acknowledged alarms are not shown in **Top Active Alarms**.

Alarm filters

You can create custom filters for **Alarms**. To create a custom filter, perform the following steps:

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

Figure 118 *Alarms: New Filter*



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

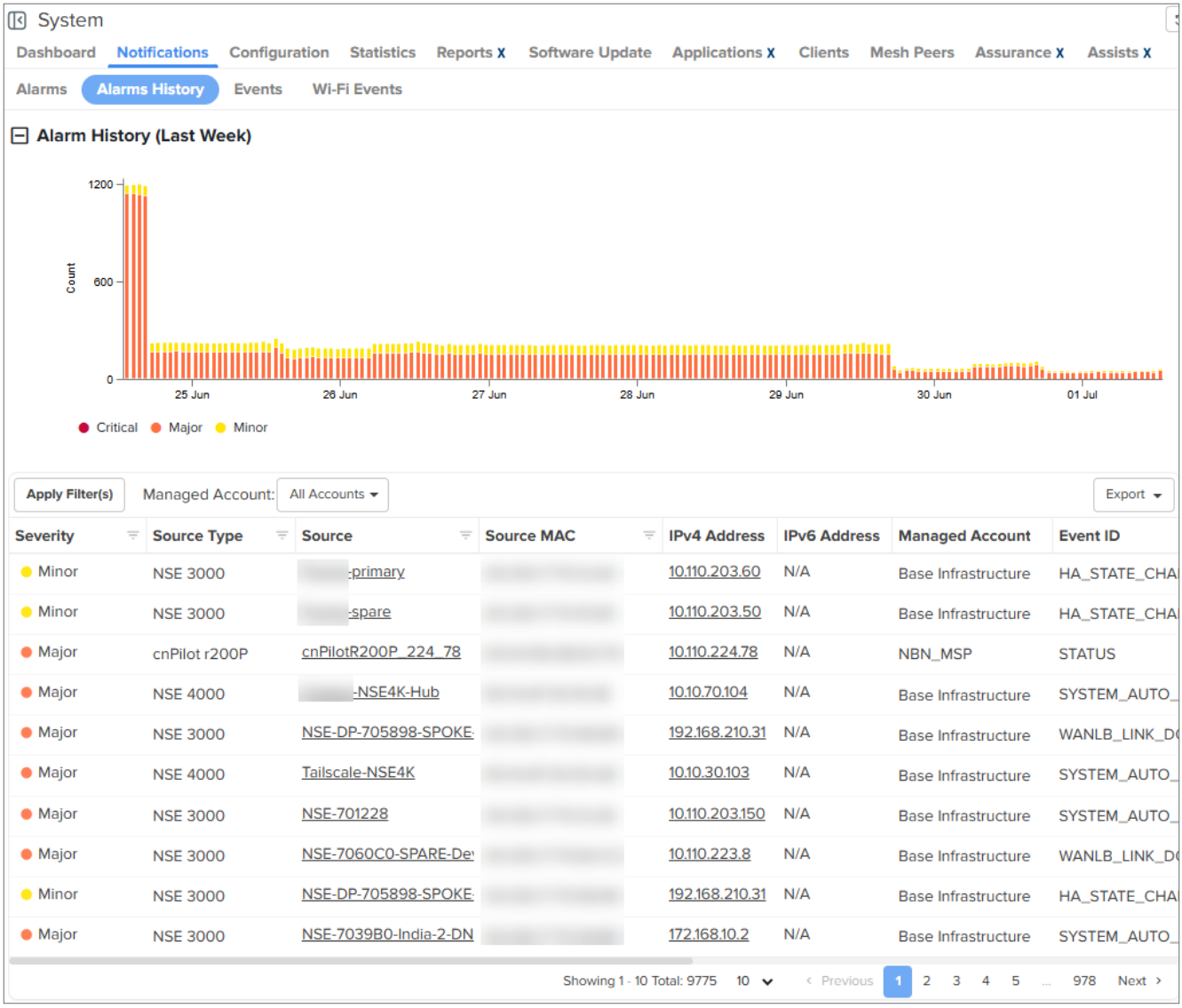
4. Click **Reset** to reset the filter option in the Alarms filter.
5. Click **Clear Filters** to clear all the filter options.

   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 119 *Alarm History*

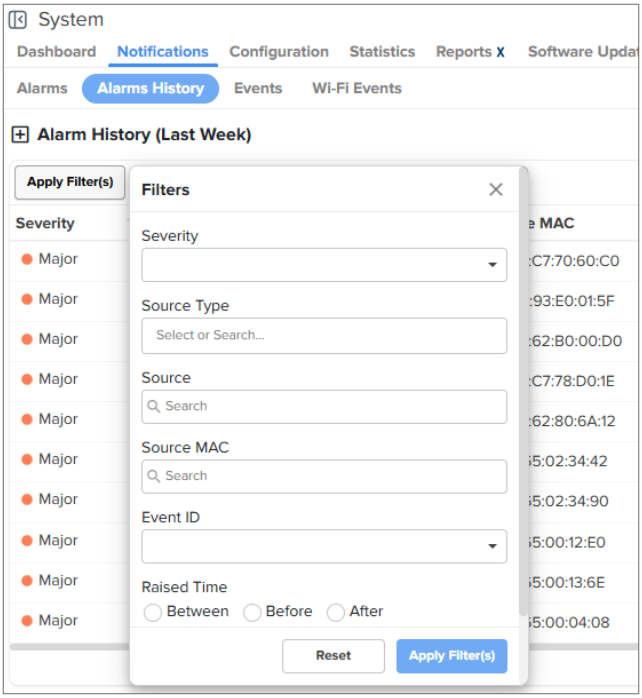


Alarm History filters

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 120 *Alarm History: New Filter*



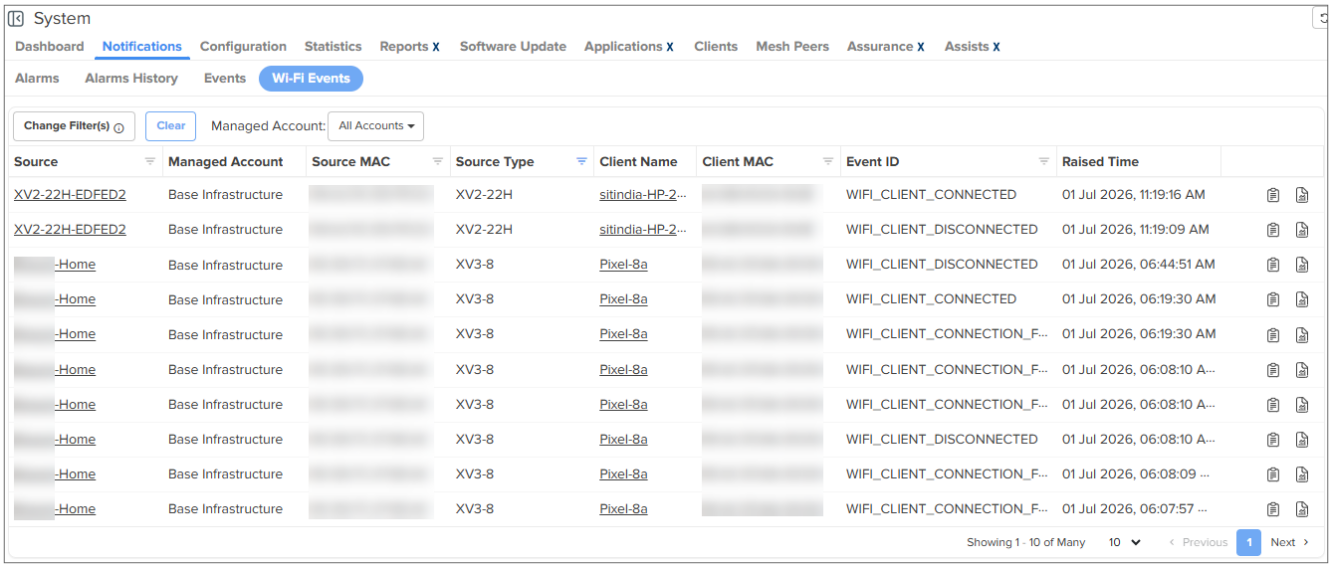
You can manually filter or search by typing parameters in the column header of the Alarm History table.

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

Figure 121 *The Configuration page - BTS*

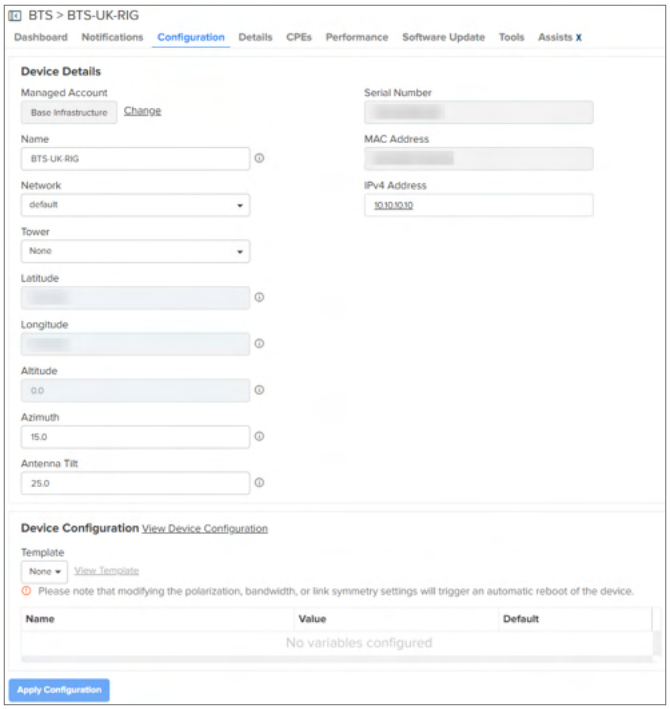


Table 25 lists and describes parameters available on the **Configuration** page for the cnWave 5G Fixed products (BTS and CPE).

Table 25 *List of parameters on the Configuration page*

Parameter	Description
Device Details	
Managed Account	Allows you to view the device user account name. For the BTS product, you can change the managed account information. When you click on **Change**, the Change Managed Account box appears providing options to modify the managed account name, network, and tower details. The Change option is not available for CPE.
Name	Name of the device (BTS or CPE). This text box allows a maximum of 64 characters.
Network	Name of the network where the BTS device is available. **Note**: This parameter is disabled for the CPE specific settings.
Tower	Name of the antenna tower where the BTS device is located. **Note**: This parameter is disabled for the CPE specific settings.
Latitude	The geographic latitude of the device (BTS or CPE) in decimal degrees (DD).

Table 25 *List of parameters on the Configuration page*

Parameter	Description
	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.	
Template	An option to select and view the configuration templates. If you modify any parameters in the template (such as polarization, bandwidth, or link symmetry), the device automatically reboots.
Apply Configuration	An option to submit or apply the new configuration changes.

Statistics and Details

The **Statistics** page provide a tabular aggregation of data, including general information on the devices monitored, as well as wireless, network, and traffic metrics. The **Details** pages, however, provide information on a single device.

This section contains information about the following topics:

- Statistics page
- Details page

Statistics page

The following table highlights information that is displayed in the **Statistics** page at the System, MSP, Network, Tower, and Site-levels:

Table 26 *Device Statistics*

Device Type	Statistics Page Information
60 GHz cnWave Nodes	**General**

Table 26 *Device Statistics*

Device Type	Statistics Page Information
	• 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 • IPv4 Address • IPv6 Address • MAC Address • Network • Product Name

Table 26 *Device Statistics*

Device Type	Statistics Page Information
	• 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 • Serial Number • Status • Tower/Site • Uptime **Wireless**

Table 26 *Device Statistics*

Device Type	Statistics Page Information
	• 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 • Product Name • Serial Number • Status • Tower/Site
cnVision Client	**General**

Table 26 *Device Statistics*

Device Type	Statistics Page Information
	• 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 • Uptime **Network** • LAN Interface • LAN Interface 2

Table 26 *Device Statistics*

Device Type	Statistics Page Information
	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 • Link Uptime • MAC • Network • Registration Count • Registration State

Table 26 *Device Statistics*

Device Type	Statistics Page Information
	• 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 • Product Name • Serial Number • Status • Tower/Site • Uptime

Table 26 *Device Statistics*

Device Type	Statistics Page Information
	Network • Uplink Port Speed **Note**: This column is displayed only for APs running version 7.1.1 and later. • ETH1 Port Speed • ETH2 Port Speed • ETH3 Port Speed **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

Table 26 *Device Statistics*

Device Type	Statistics Page Information
	• Network • 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

Table 26 *Device Statistics*

Device Type	Statistics Page Information
	• DL/UL Ratio • 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

Table 26 *Device Statistics*

Device Type	Statistics Page Information
	• Product Name • 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
RV22 Home Mesh	**General** • Device Name • IPv4 Address • IPv6 Address • MAC Address • Network • Product Name

Table 26 *Device Statistics*

Device Type	Statistics Page Information
	• Serial Number • Status • Tower/Site • Uptime **Wireless** • Radios

Details page

The **Details** page displays device-specific information, such as system info, radio parameters, and software versions.

The **Details** page is provided for the following devices:

- 60 GHz cnWave
- cnMatrix
- cnPilot Home
- cnRanger BBU
- cnRanger SM
- cnReach
- cnVision Client
- cnVision Hub
- cnWave 5G Fixed Details
  - cnWave 5G Fixed BTS
  - cnWave 5G Fixed CPE
- Enterprise Wi-Fi AP (XE-, XV-, and X7-Series)
- ePMP AP
- PMP AP
- PMP SM
- PON (OLT)
- PTP 650/670/700
- PTP 820/850 Details
- Home Mesh Routers

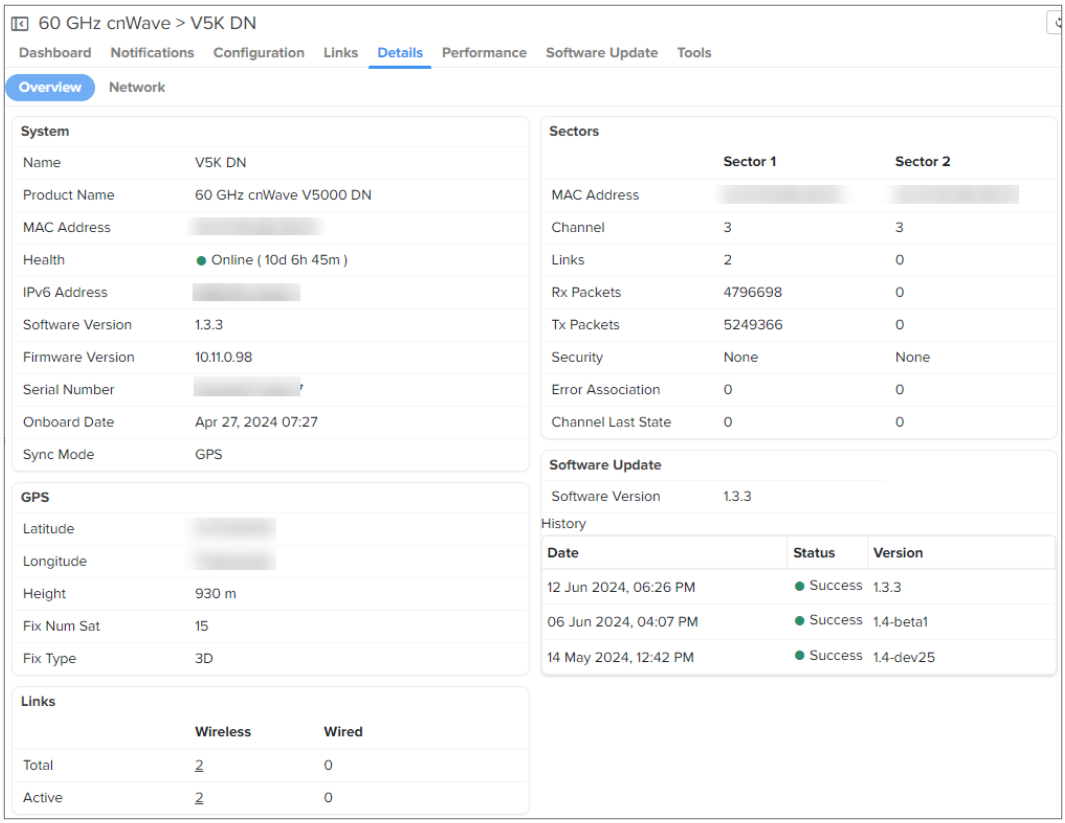
60 GHz cnWave

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

- Overview
- Network Info

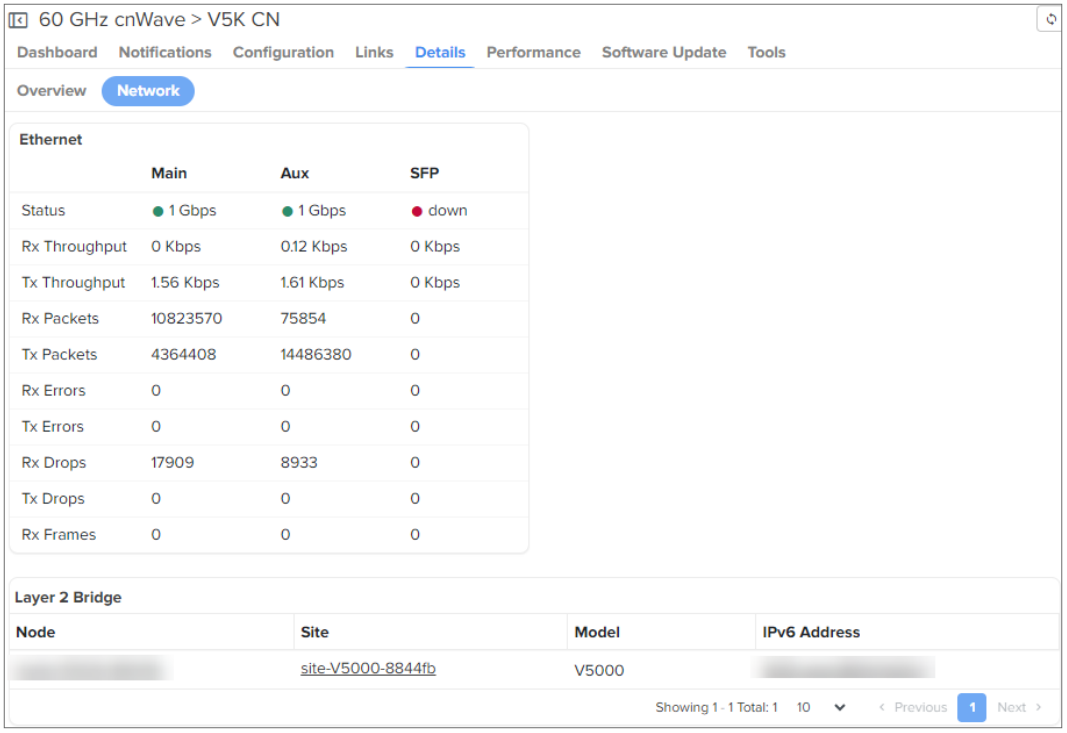
Overview

Figure 122 *60 GHz cnWave: Device > Details > Overview*



Network Info

Figure 123 *60 GHz cnWave: Device > Details > Network Info*



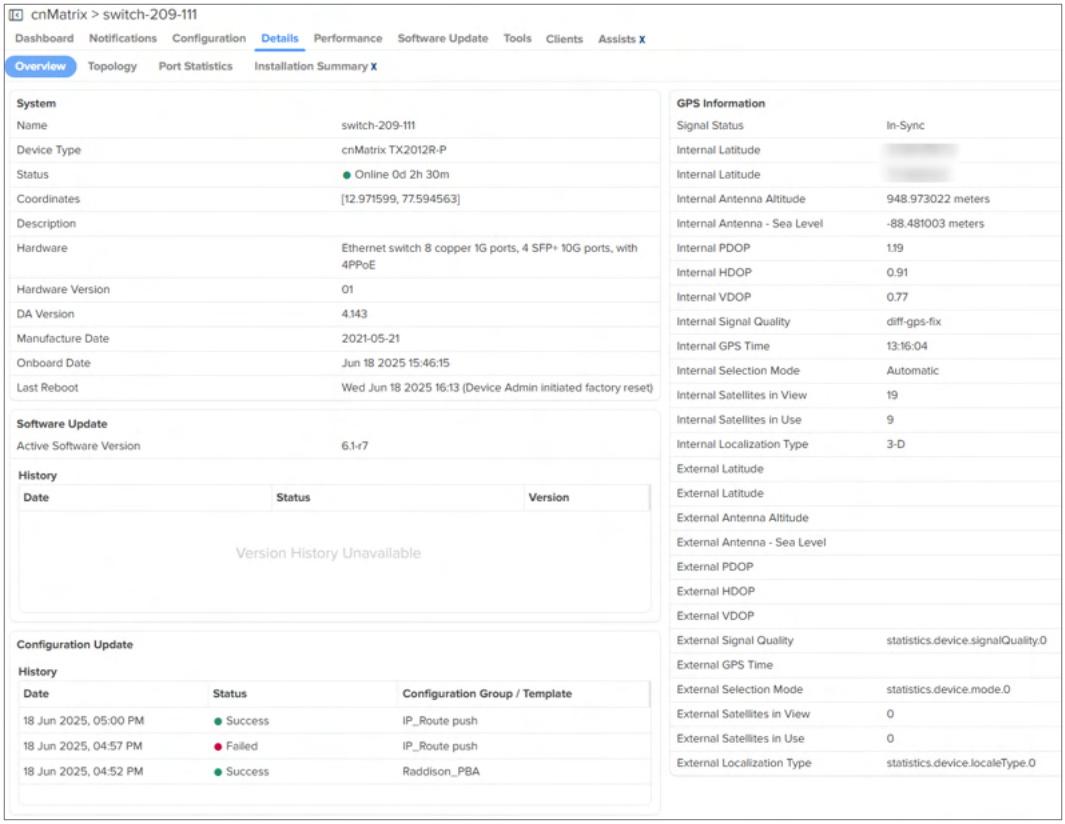
cnMatrix

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

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

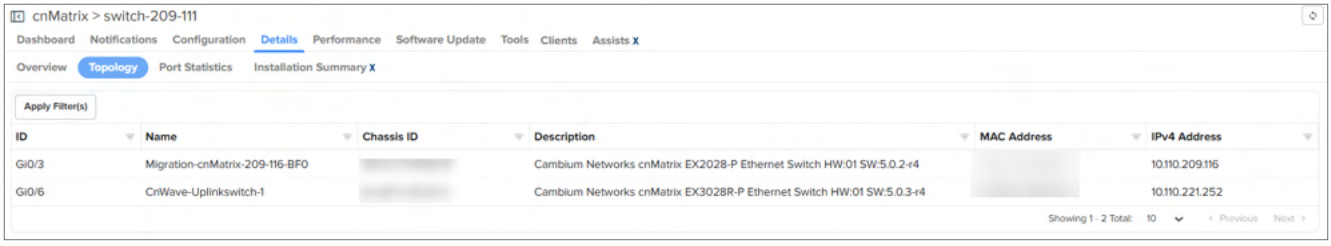
Overview

Figure 124 *cnMatrix: Device > Details > Overview*



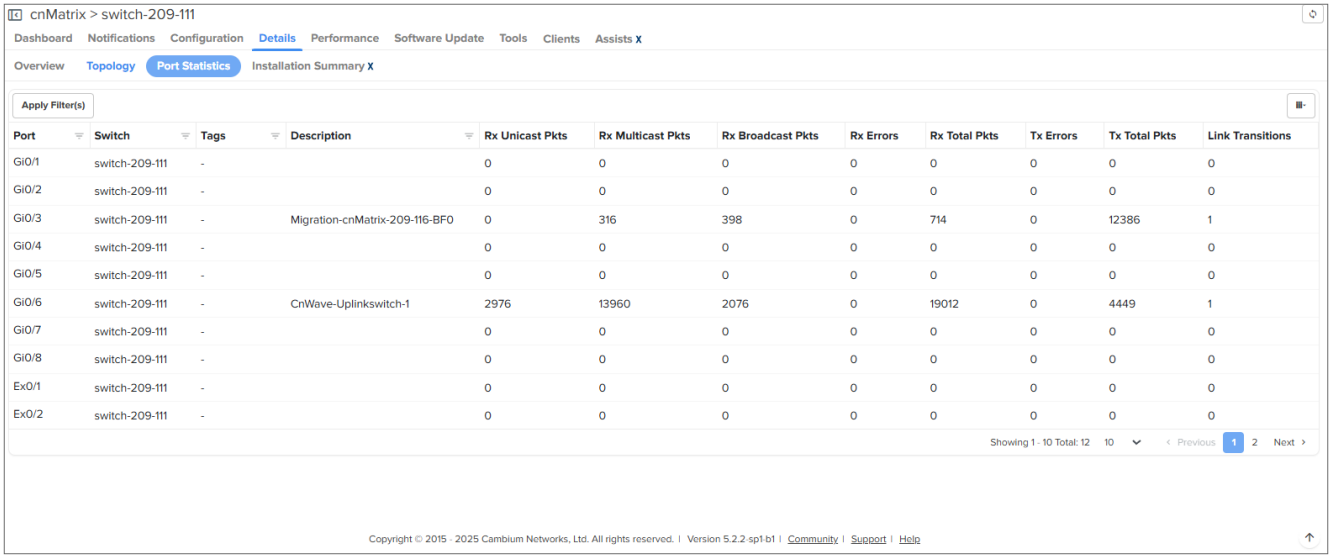
Topology

Figure 125 *cnMatrix: Device > Details > Topology*



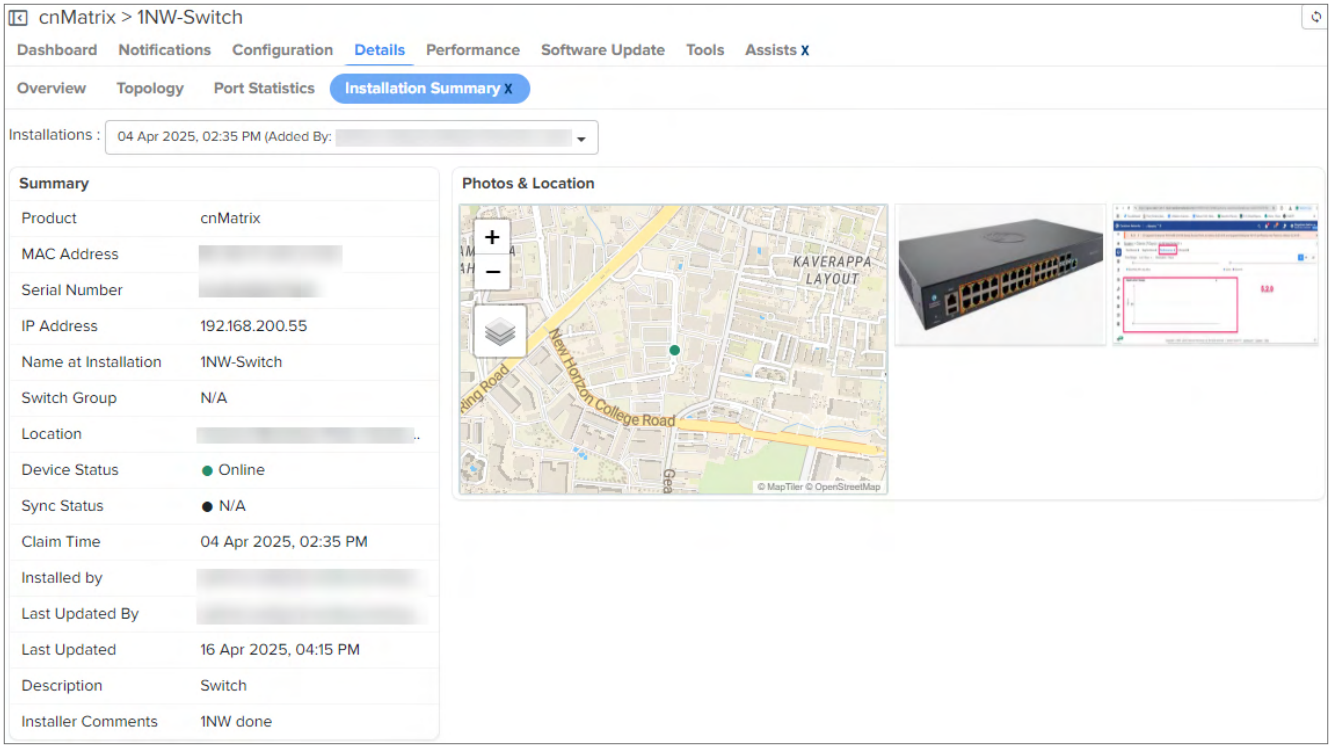
Port Statistics

Figure 126 *cnMatrix: Device > Details > Port Statistics*



Installation Summary

Figure 127 *cnMatrix: Device > Details > Installation Summary*



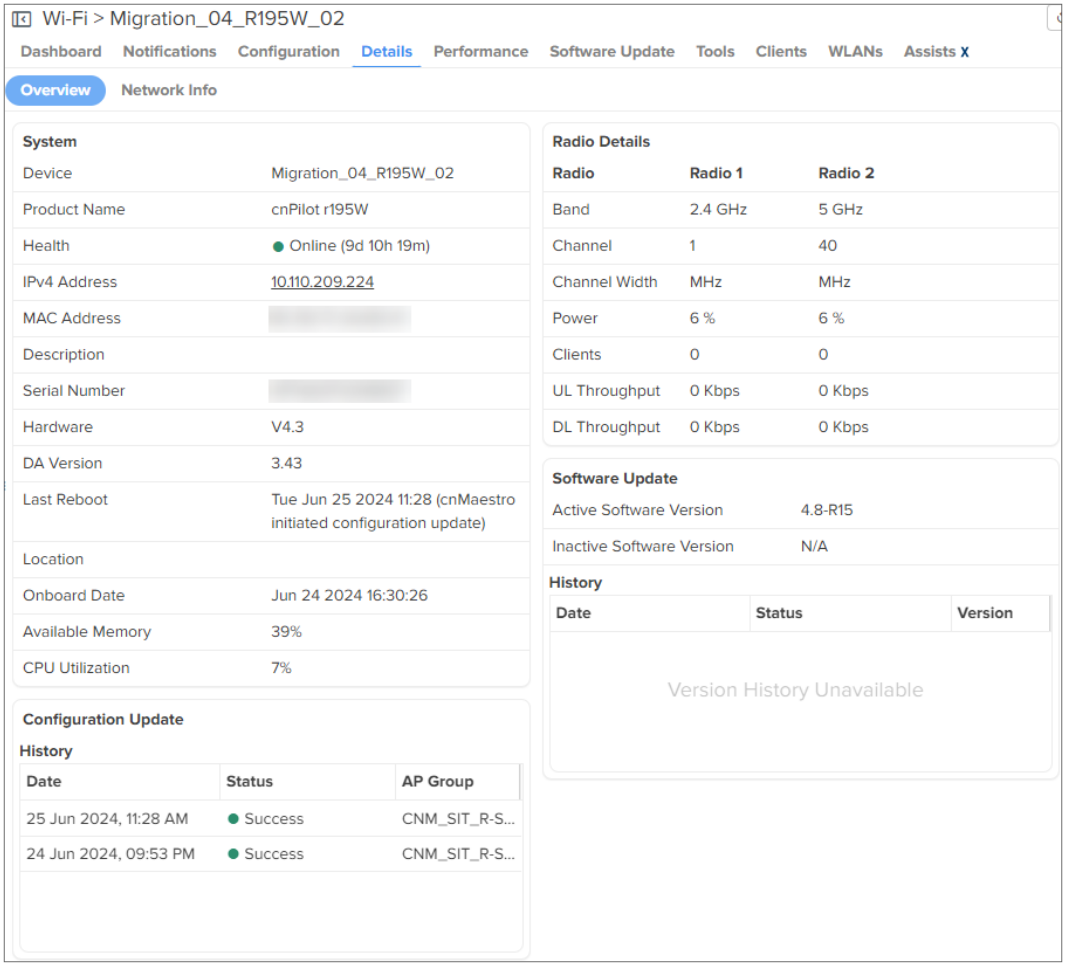
cnPilot Home

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

- Overview
- Network Info

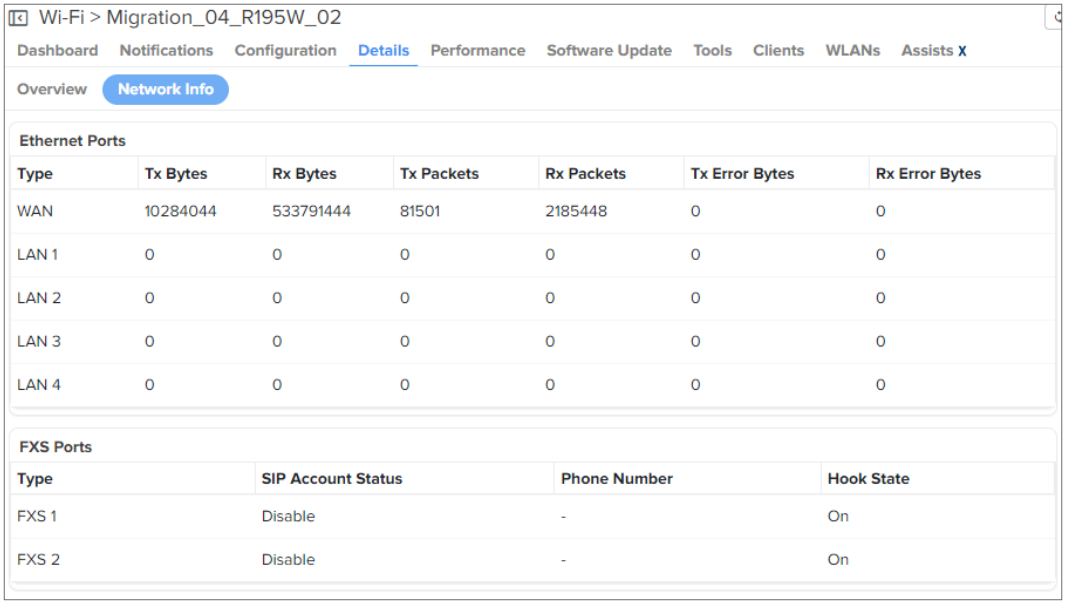
Overview

Figure 128 *cnPilot Home: Device > Details > Overview*



Network Info

Figure 129 *cnPilot Home: Device > Details > Network Info*



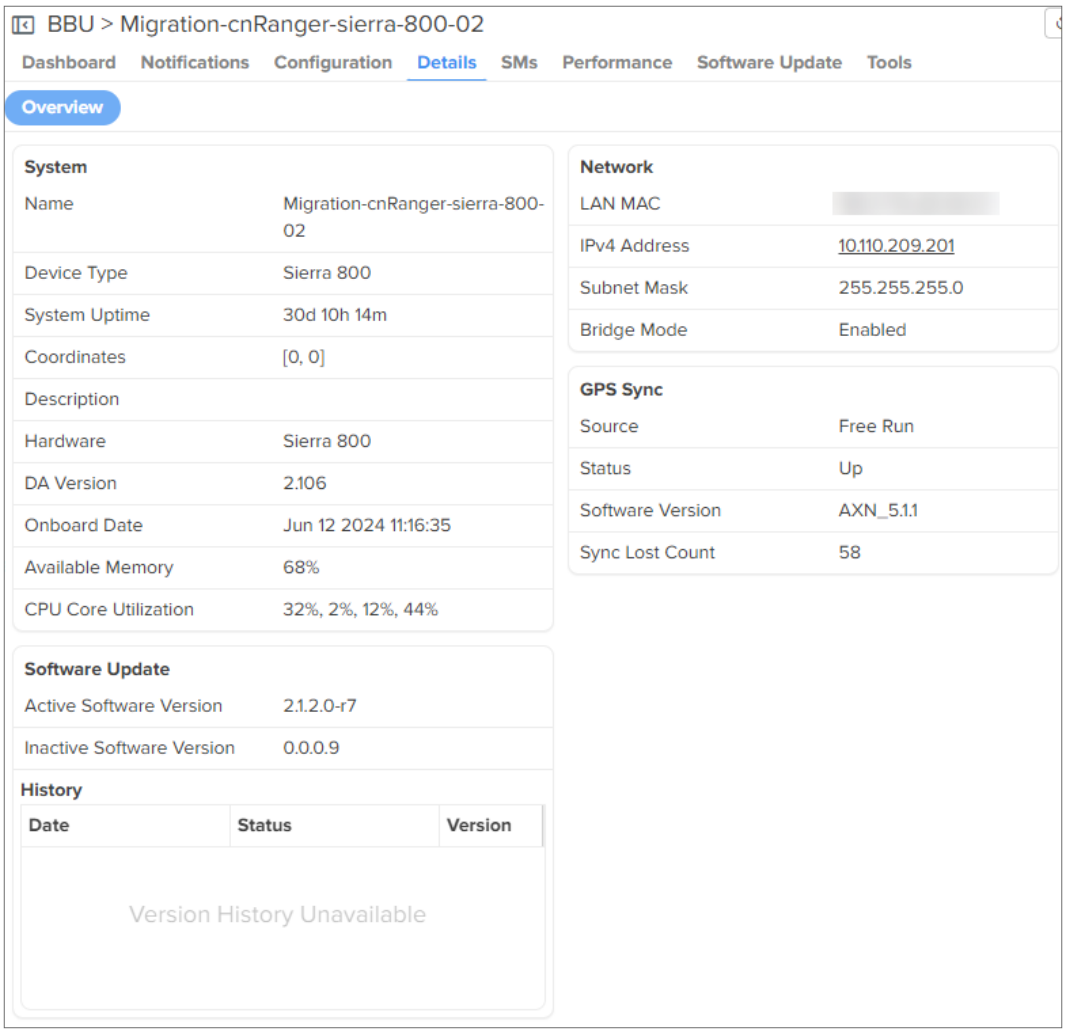
cnRanger BBU

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

- Overview

Overview

Figure 130 *cnRanger BBU: Device > Details > Overview*



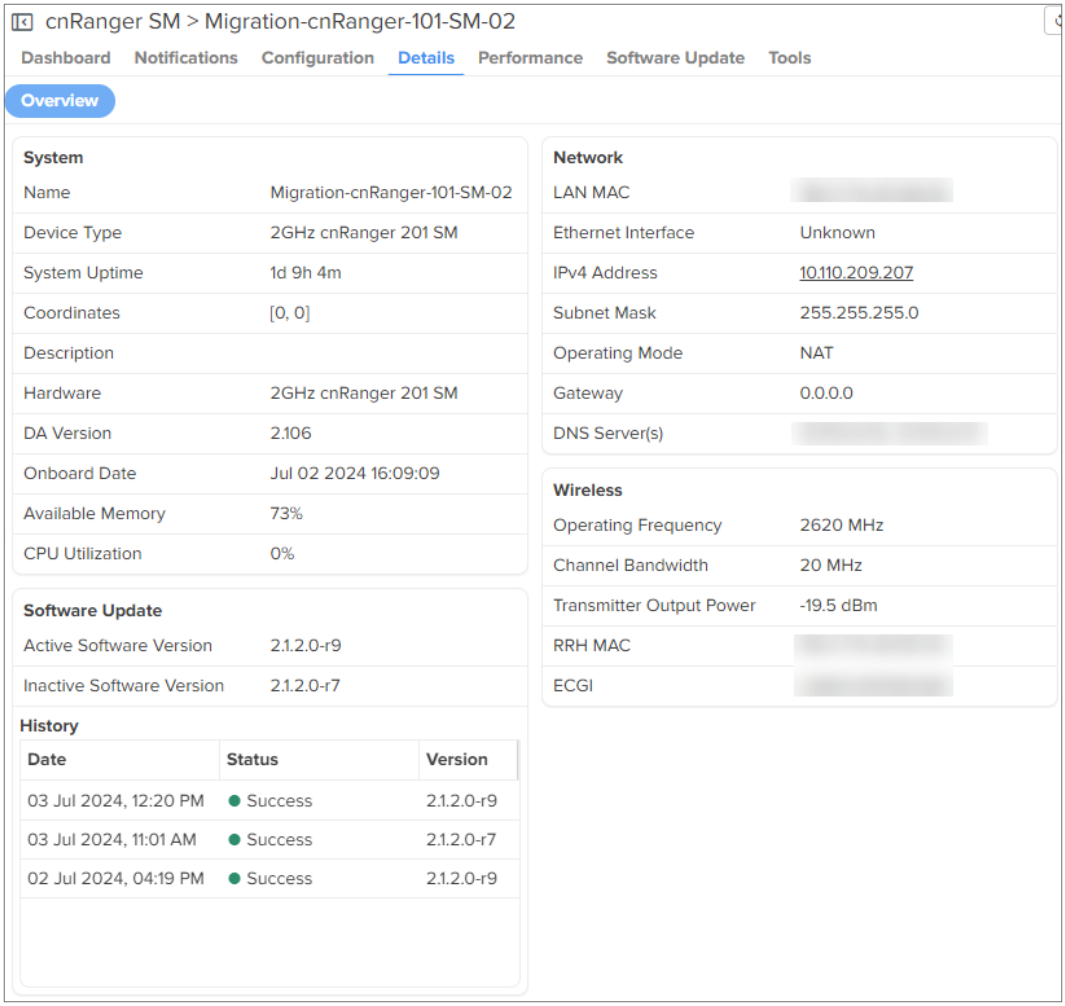
cnRanger SM

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

- Overview

Overview

Figure 131 *cnRanger SM: Device > Details > Overview*



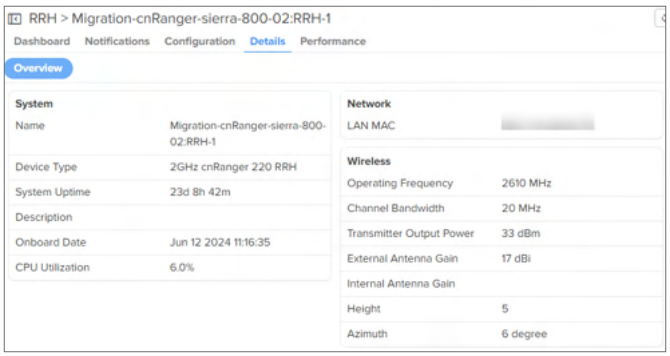
cnRanger RRH

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

- Overview

Overview

Figure 132 *cnRanger RRH: Device > Details > Overview*



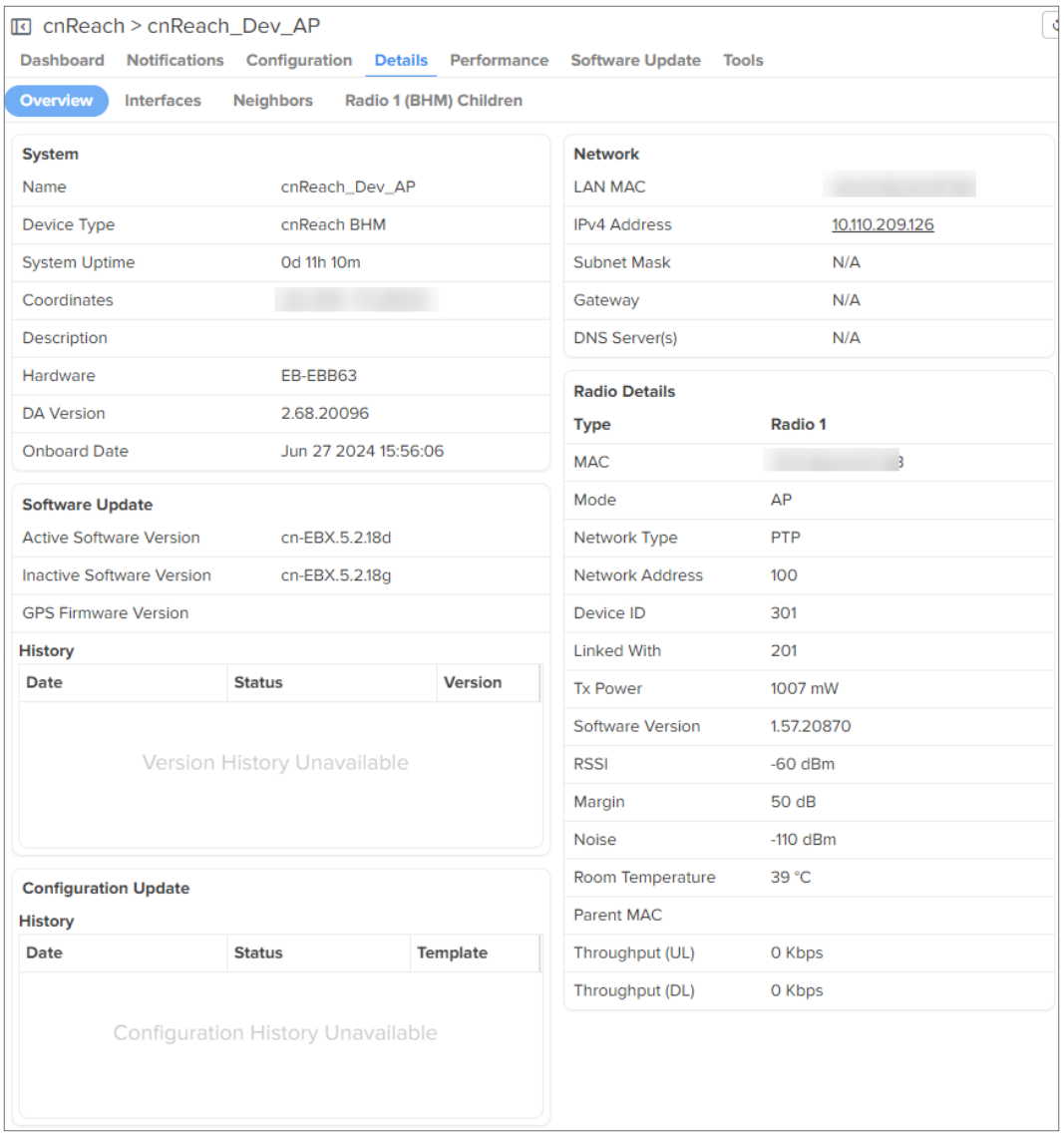
cnReach

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

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

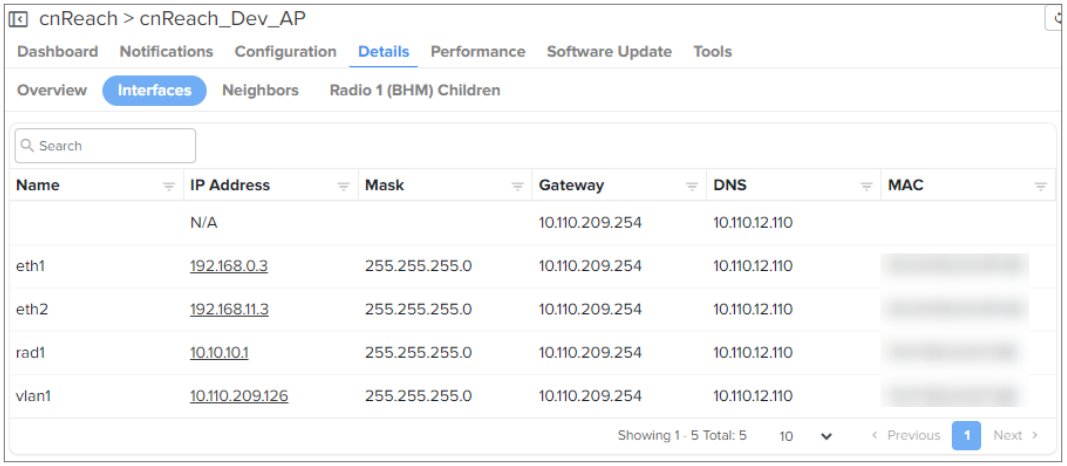
Overview

Figure 133 *cnReach: Device > Details > Overview*



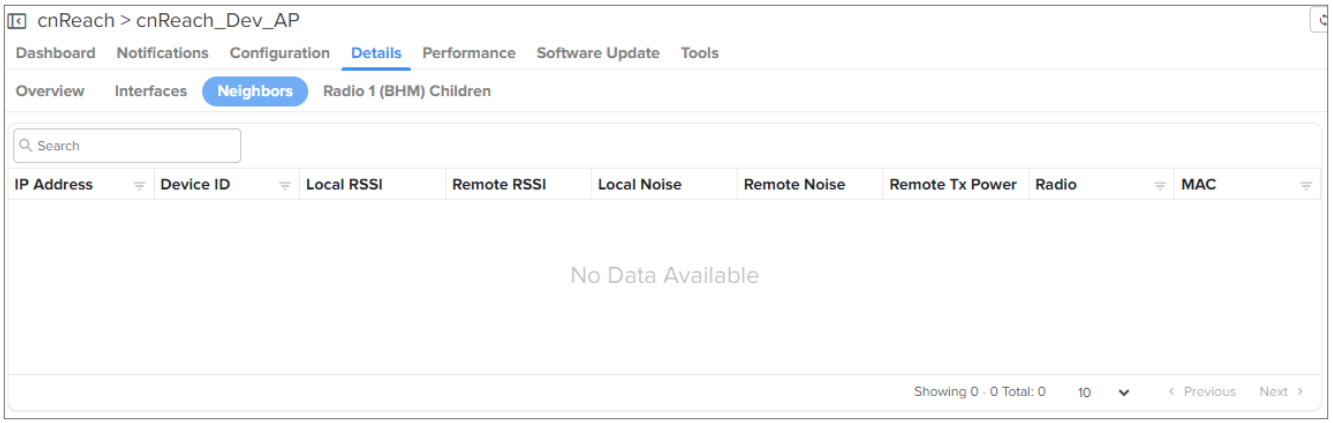
Interfaces

Figure 134 *cnReach: Device > Details > Interfaces*



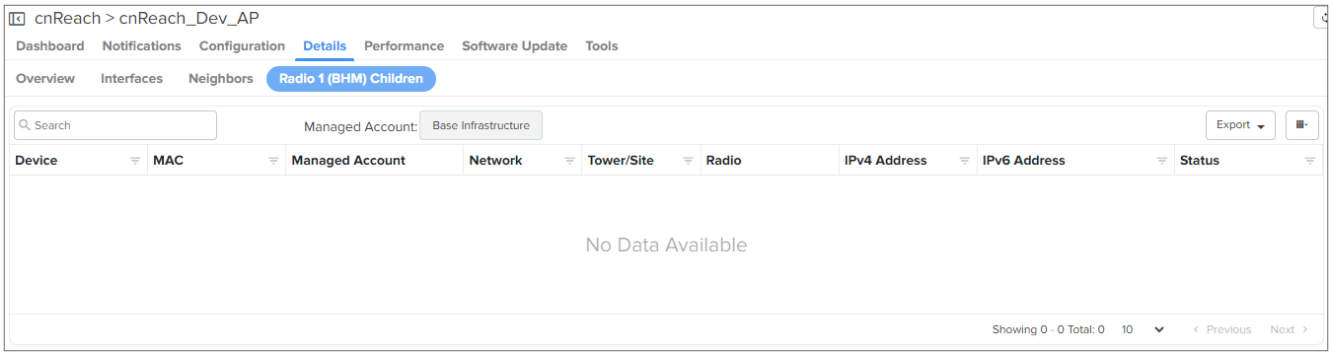
Neighbors

Figure 135 *cnReach: Device > Details > Neighbors*



Radio 1 (BHM) Children

Figure 136 *cnReach: Device > Details > Radio 1 (BHM) Children*



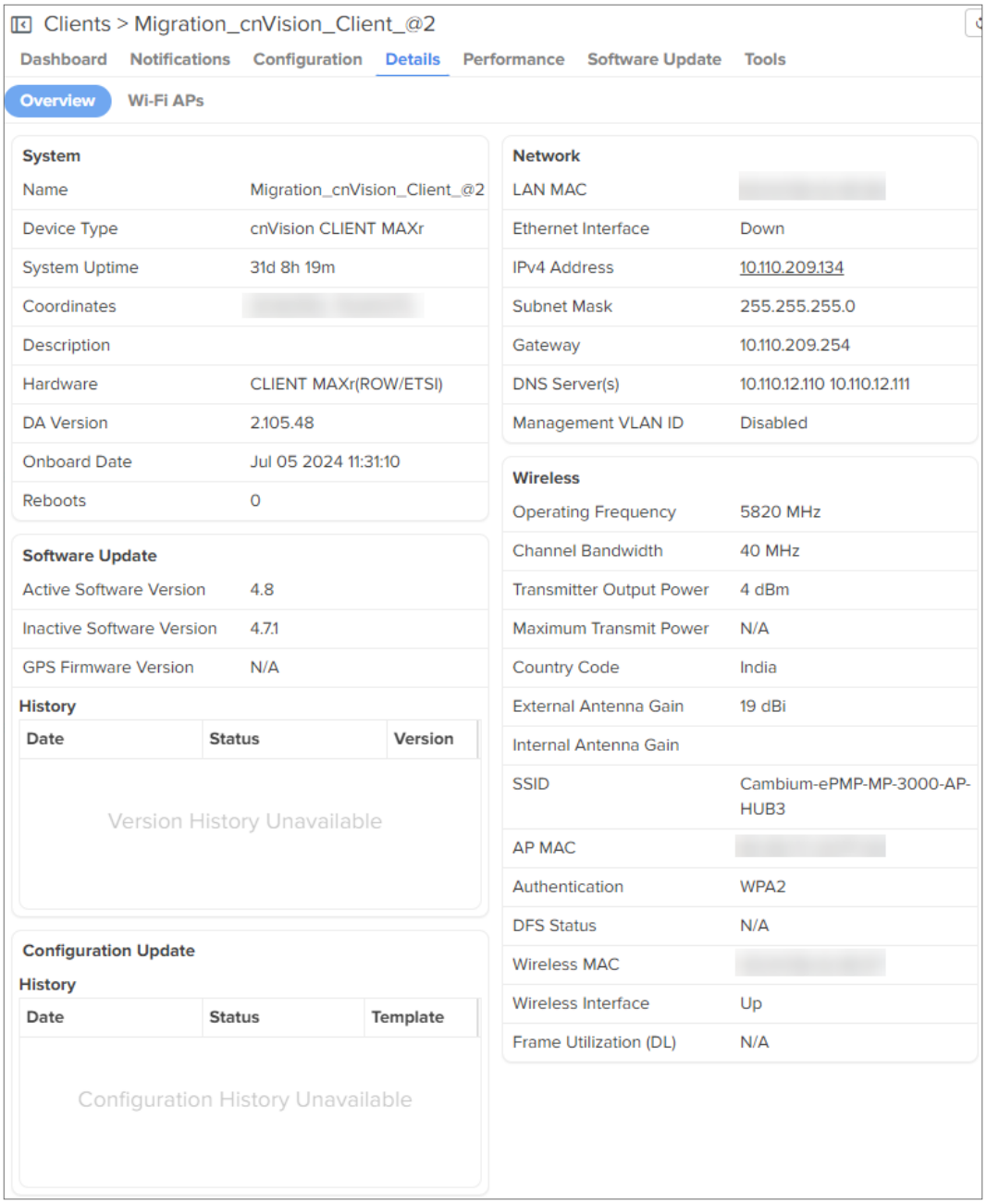
cnVision Client

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

- Overview
- Wi-Fi APs

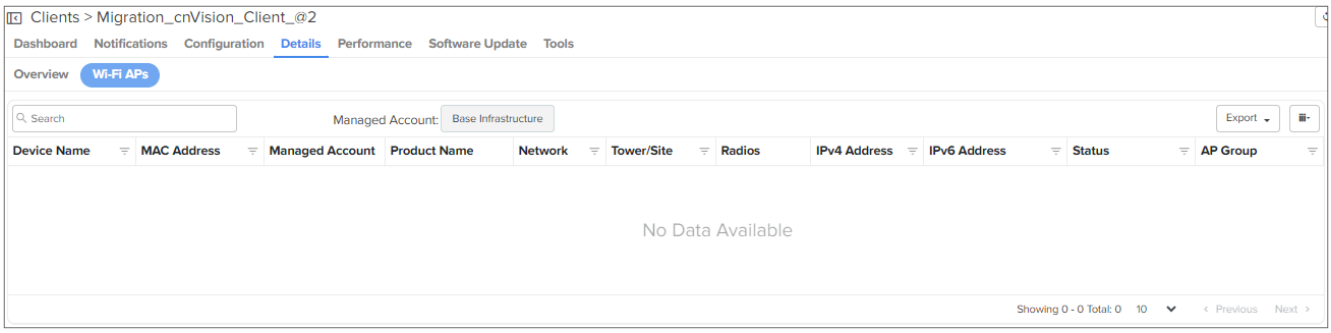
Overview

Figure 137 *cnVision Client: Device > Details > Overview*



Wi-Fi 5APs

Figure 138 *cnVision Client: Device > Details > Wi-Fi APs*



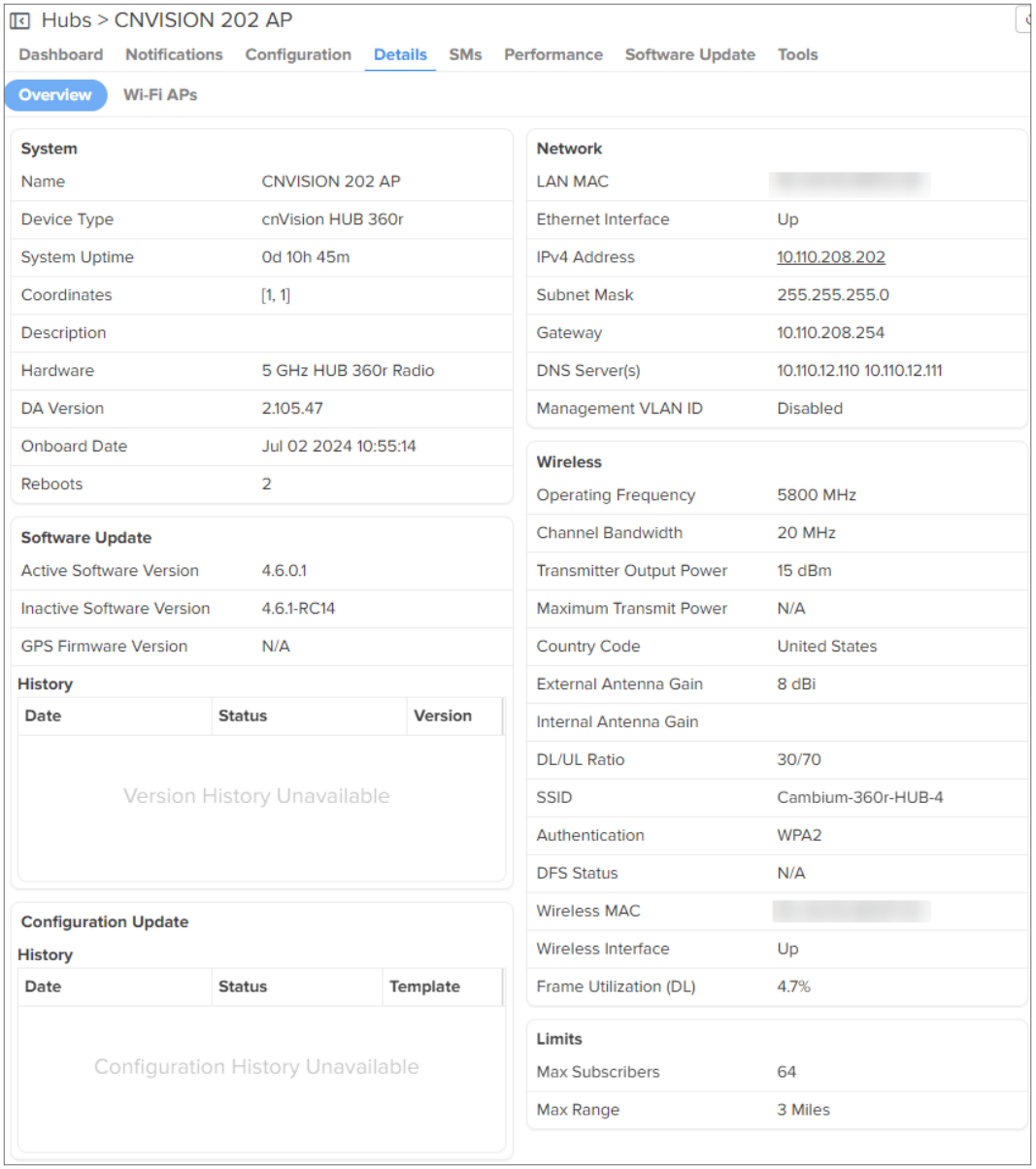
cnVision Hub

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

- Overview
- Wi-Fi APs

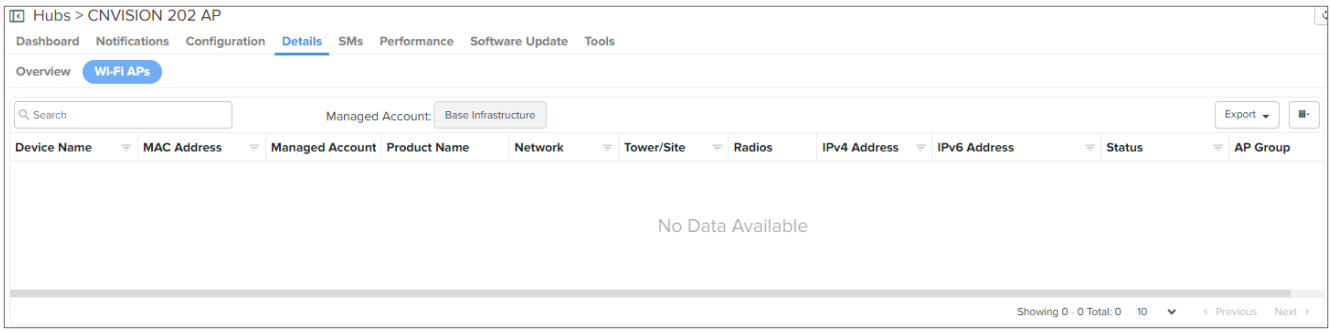
Overview

Figure 139 *cnVision Hub: Device > Details > Overview*



Wi-Fi APs

Figure 140 *cnVision Hub: Device > Details > Wi-Fi APs*



cnWave 5G Fixed Details

cnWave 5G Fixed BTS

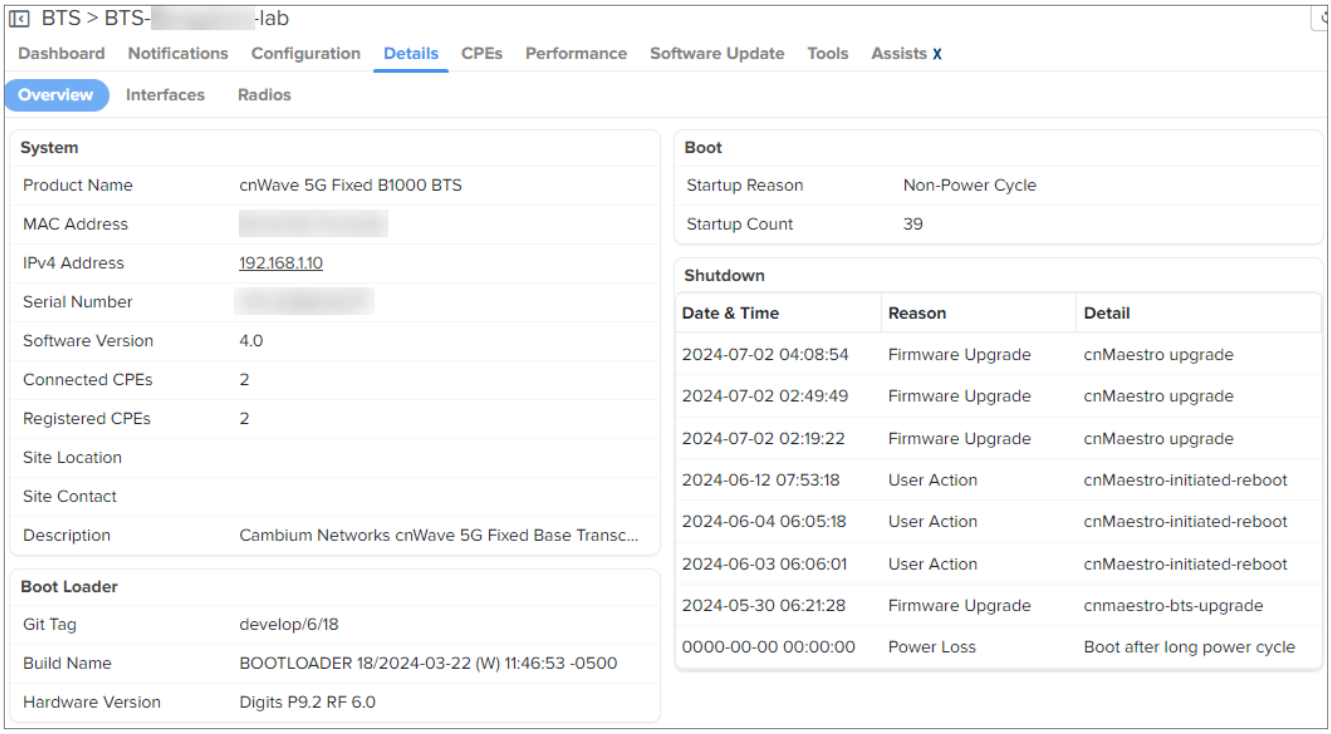
The **Details > Overview** section displays following tabs for cnWave 5G Fixed BTS device:

- Overview
- Interfaces
- Radios

Overview

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

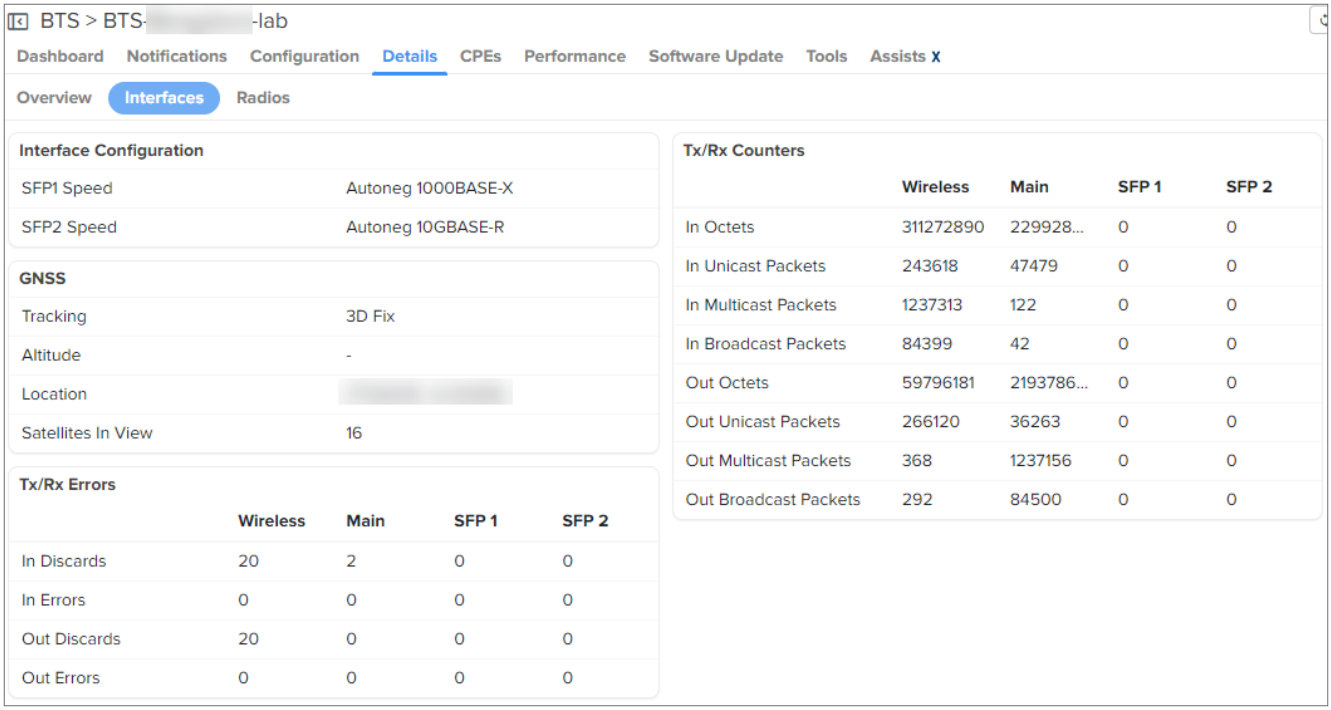
Figure 141 *cnWave 5G Fixed: Device > Details > Overview*



Interfaces

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

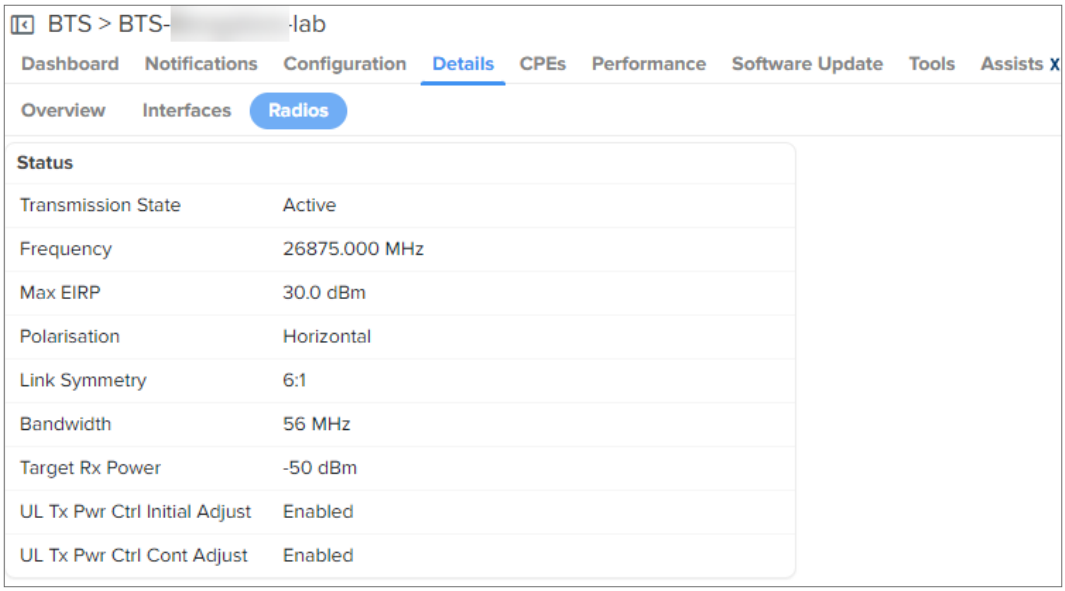
Figure 142 *cnWave 5G Fixed BTS: Device > Details > Interfaces*



Radios

Radios page provide the details of radios.

Figure 143 *cnWave 5G Fixed BTS: Device > Details > Radios*



cnWave 5G Fixed CPE

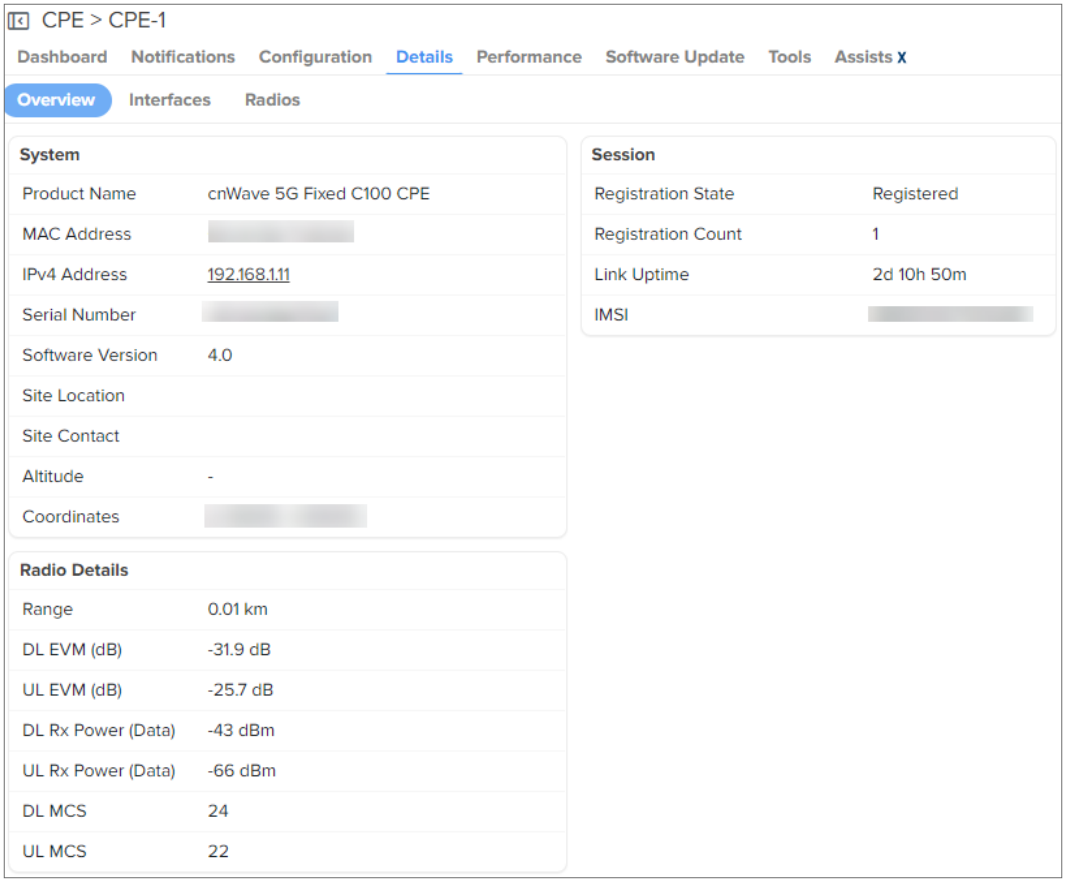
The **Details** section displays following pages for cnWave 5G Fixed CPE device:

- Overview
- Interfaces
- Radios

Overview

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

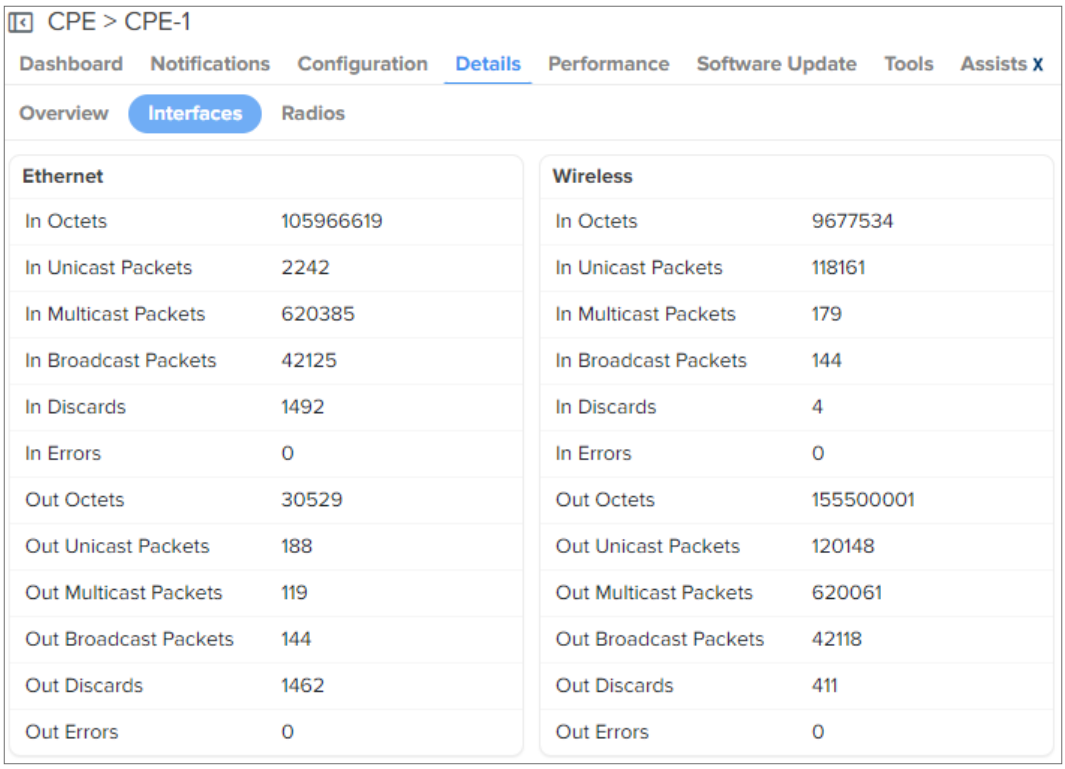
Figure 144 *cnWave 5G Fixed CPE: Device > Details > Overview*



Interfaces

Interface page provides the information such as Ethernet and Wireless.

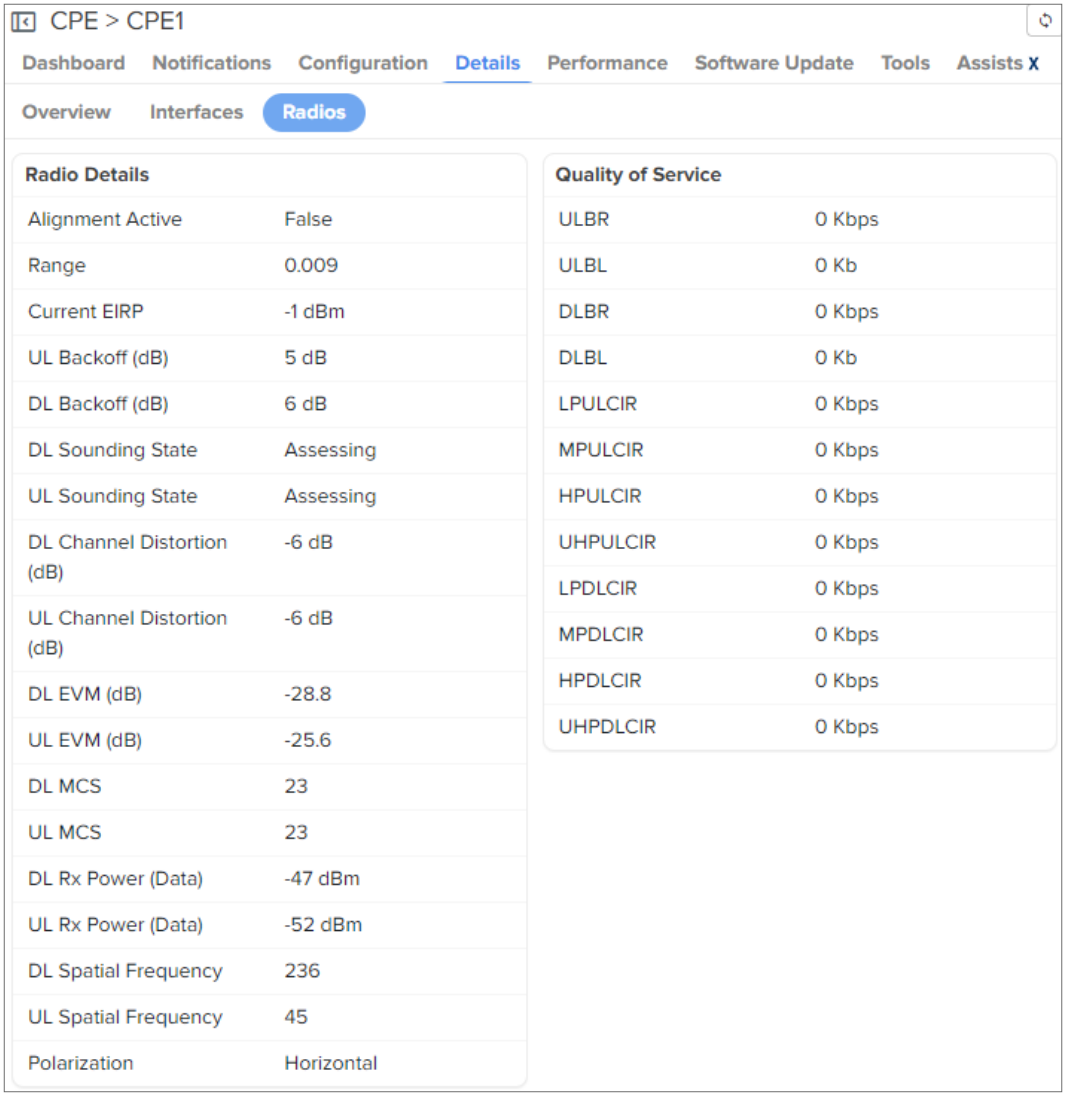
Figure 145 *cnWave 5G Fixed CPE: Device > Details > Interfaces*



Radios

Radios page provide the details of radio details.

Figure 146 *cnWave 5G Fixed CPE: Device > Details > Radios*



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

See Details.

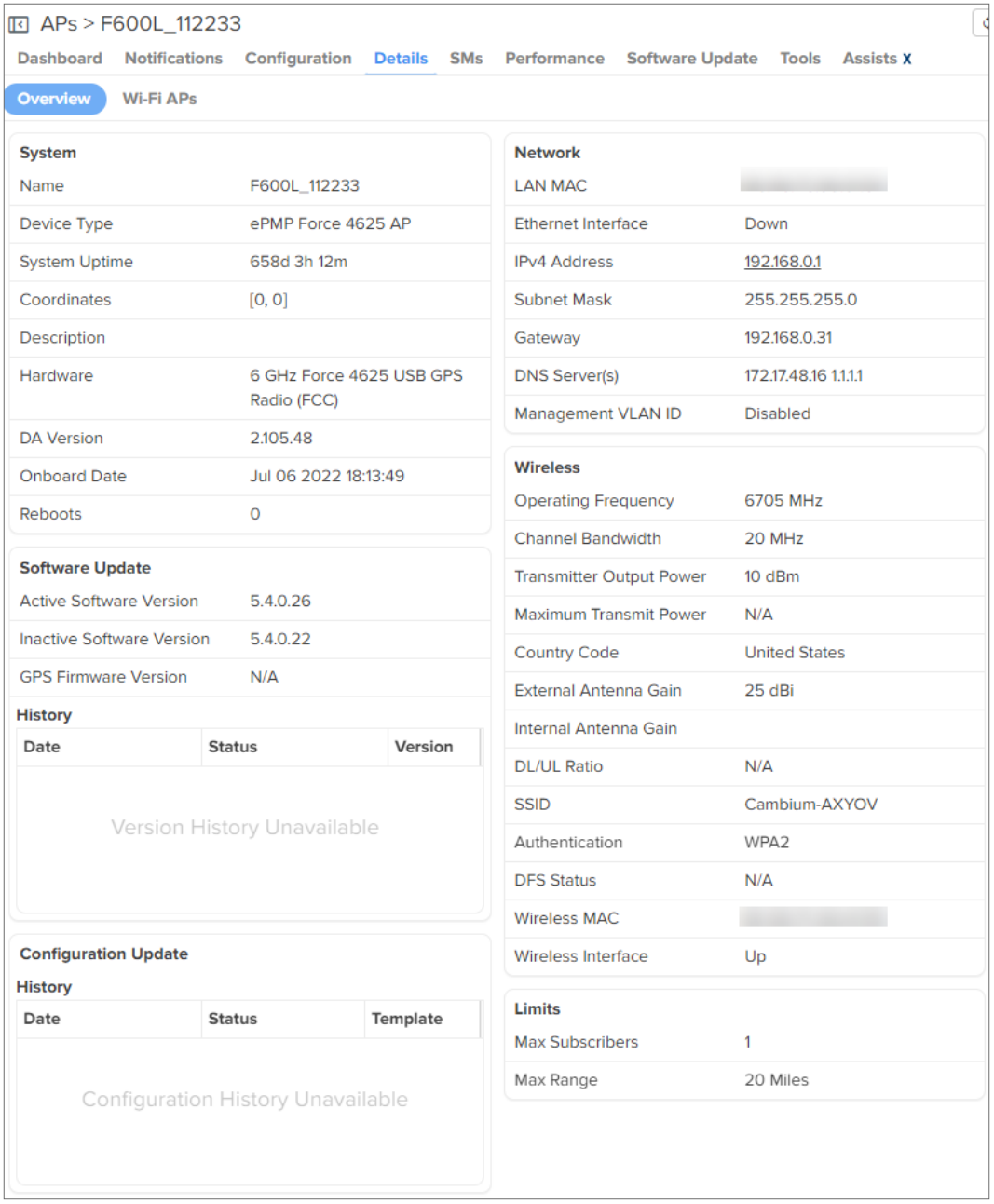
ePMP AP

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

- Overview
- Wi-Fi APs

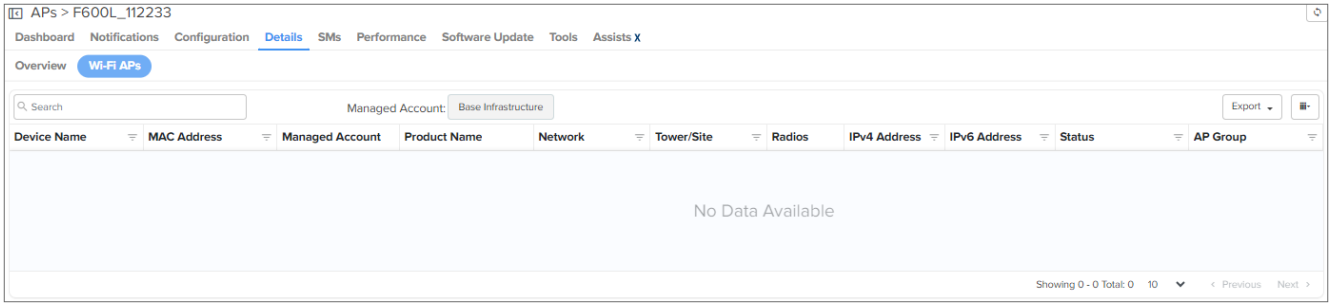
Overview

Figure 147 *ePMP AP: Device > Details > Overview*



Wi-Fi APs

Figure 148 *ePMP AP: Device > Details > Wi-Fi APs*



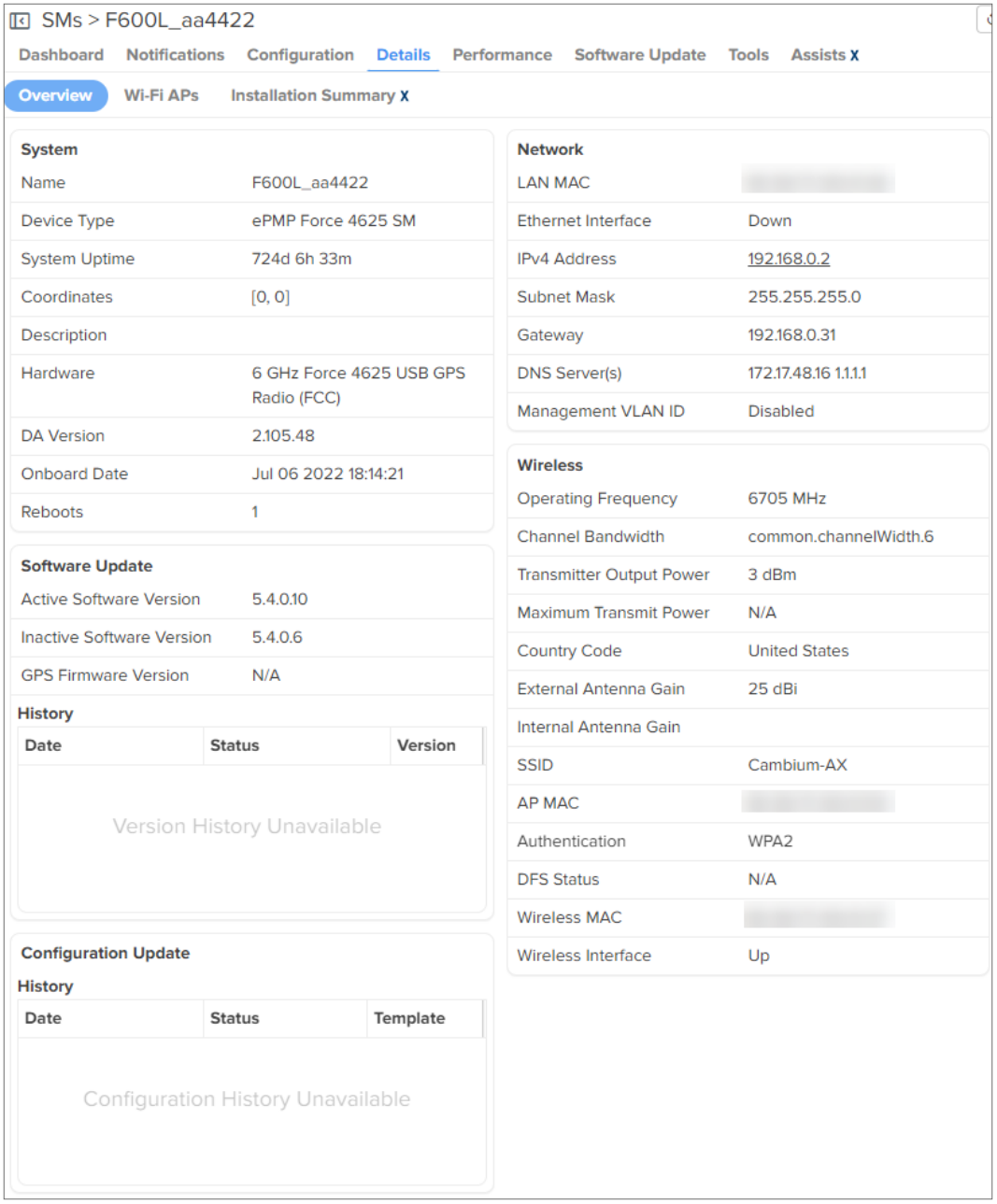
ePMP SM

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

- Overview
- Wi-Fi APs
- Installation Summary X

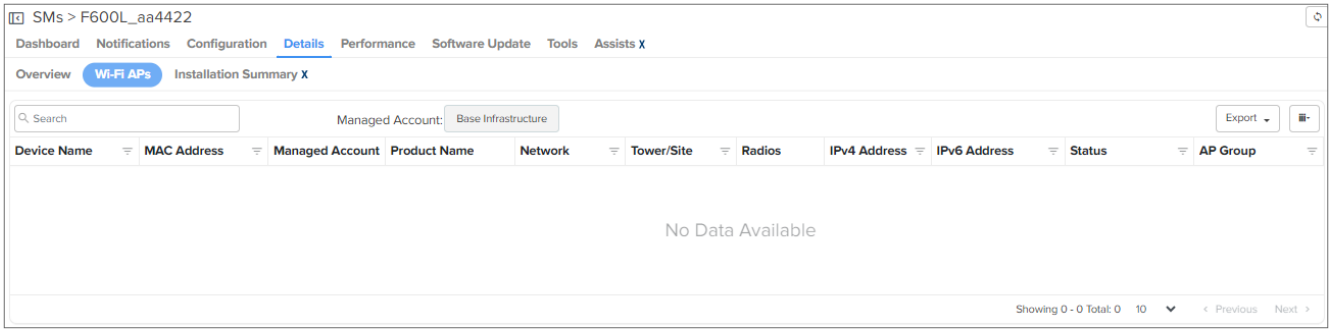
Overview

Figure 149 *ePMP SM: Device > Details > Overview*



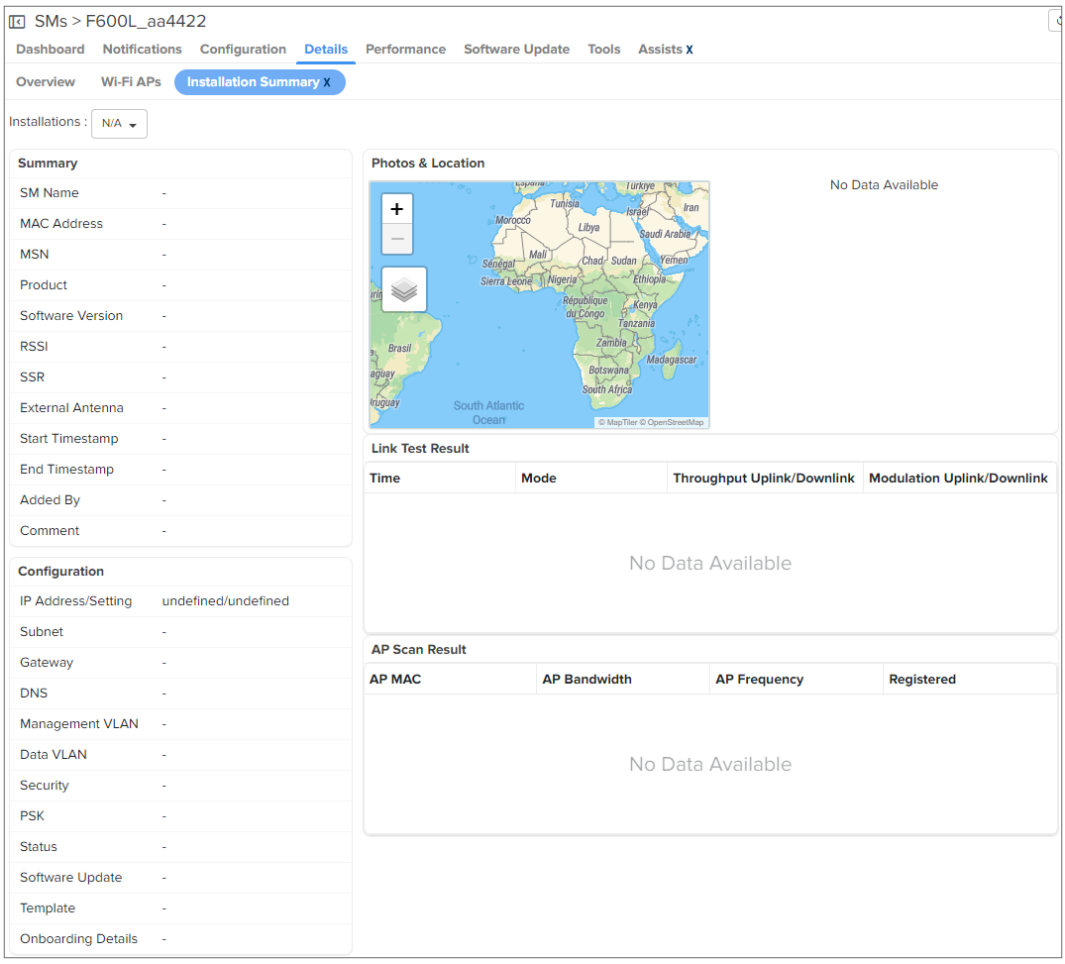
Wi-Fi APs

Figure 150 *ePMP SM: Device > Details > Wi-Fi APs*



Installation Summary X

Figure 151 *ePMP SM: Device > Details > Installation Summary* **X**



PMP AP

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

- Overview
- Wi-Fi APs

Overview

Figure 152 *PMP AP: Device > Details > Overview*

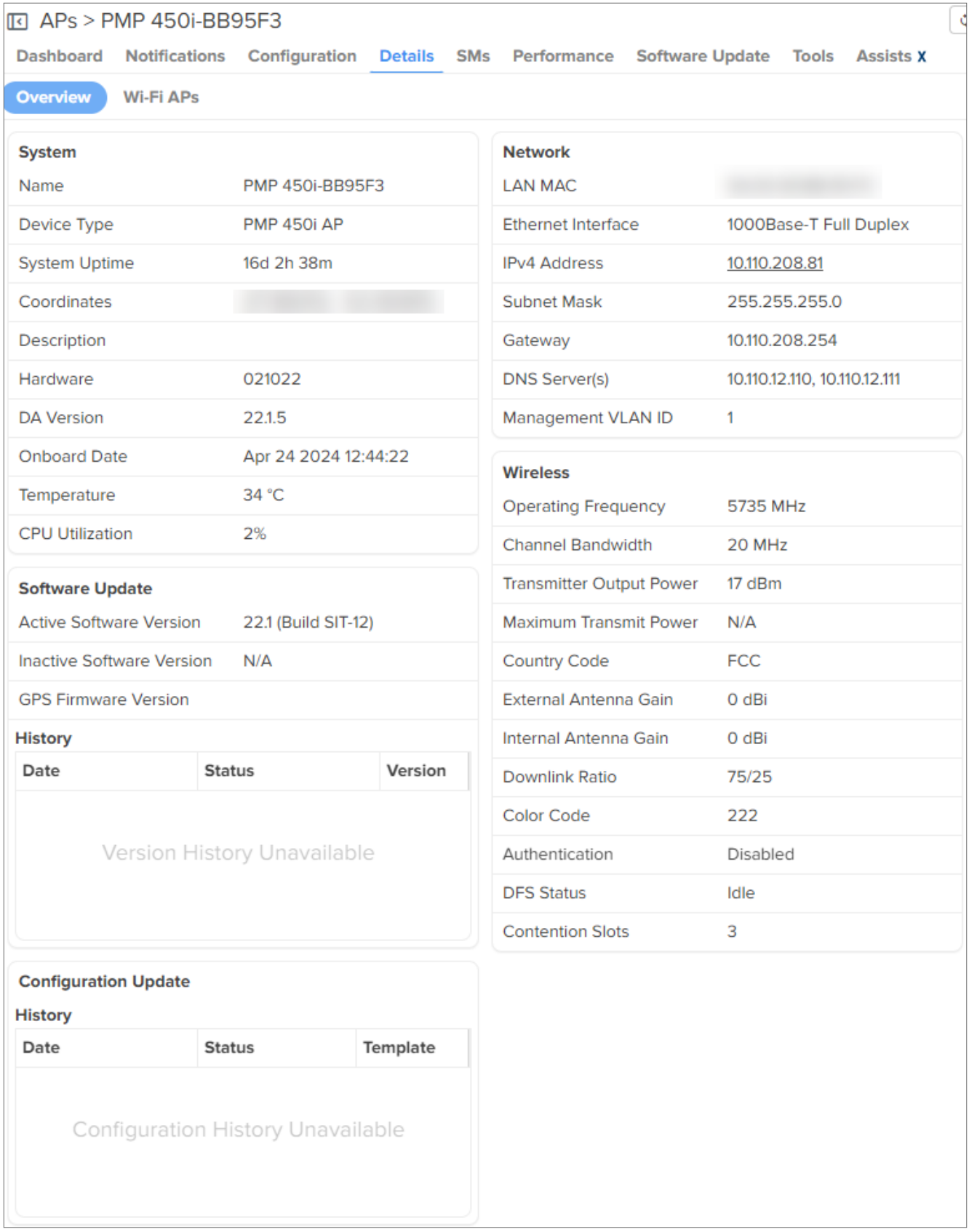
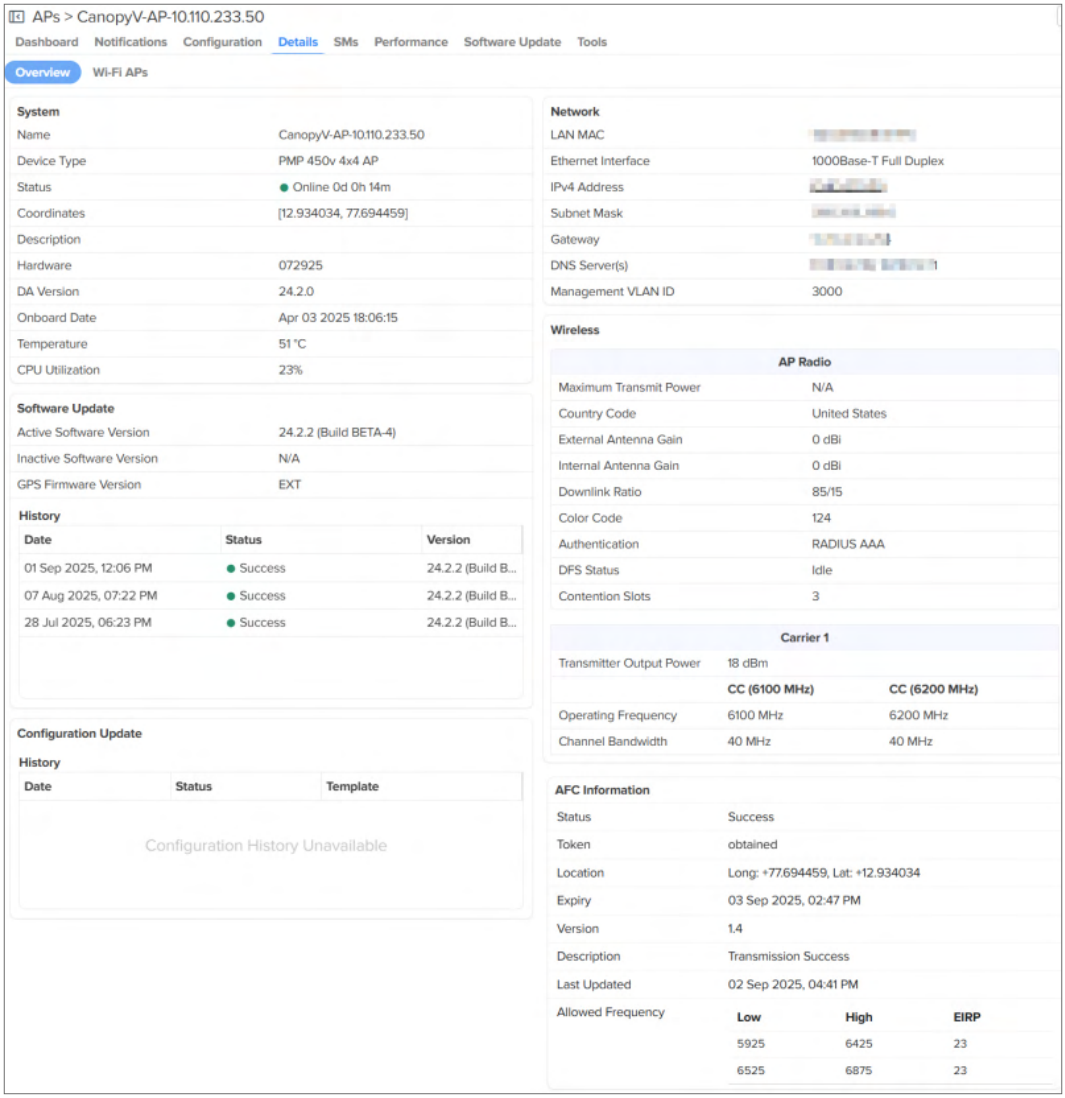
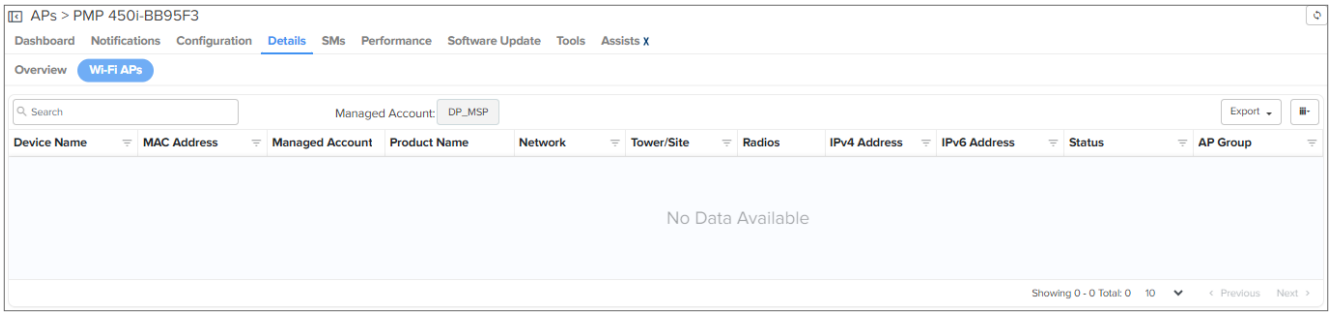


Figure 153 *PMP 450v 4 X 4 AP: Device > Details > Overview*



Wi-Fi APs

Figure 154 *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 155 *PMP SM: Device > Details > Overview*

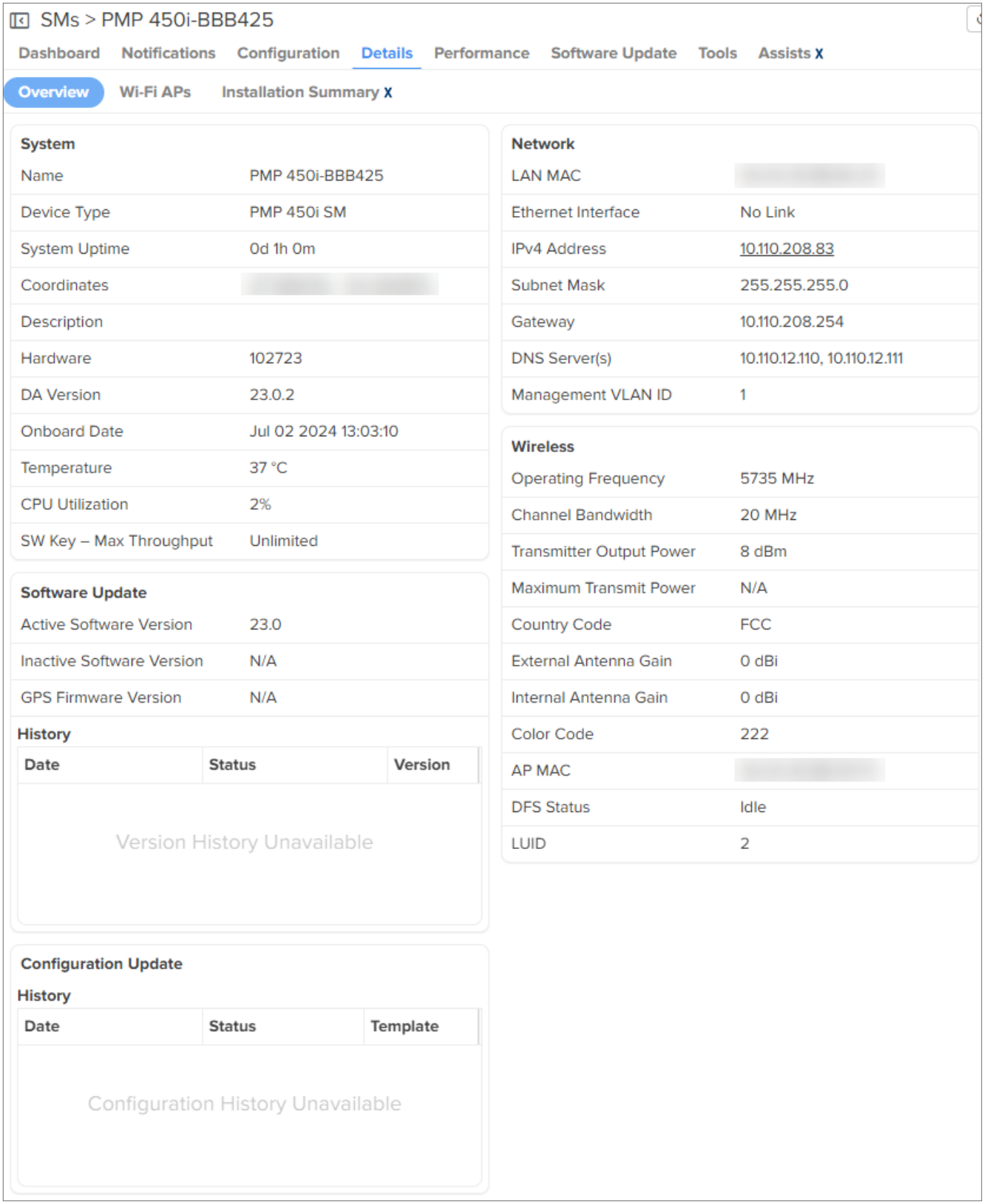
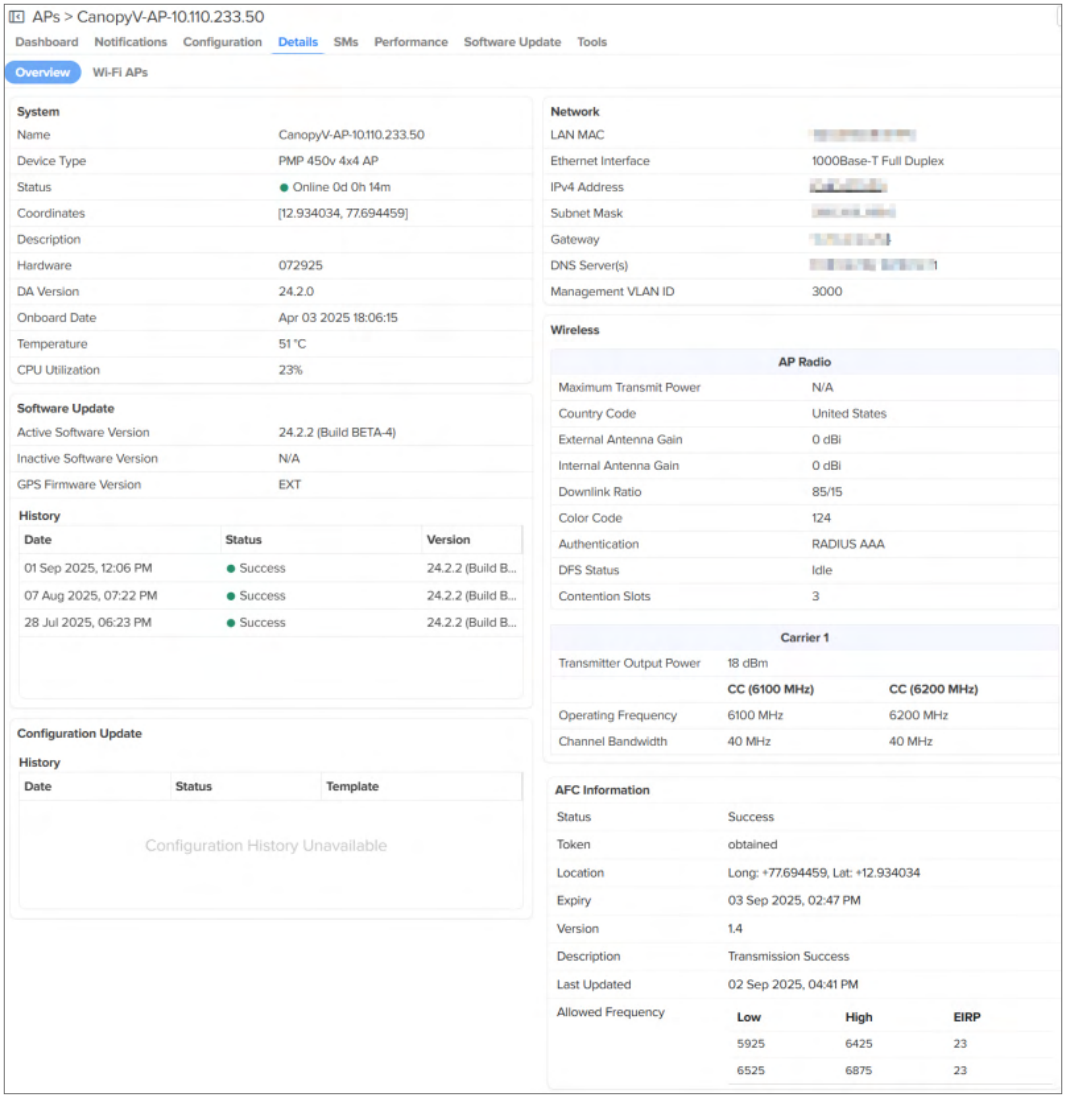
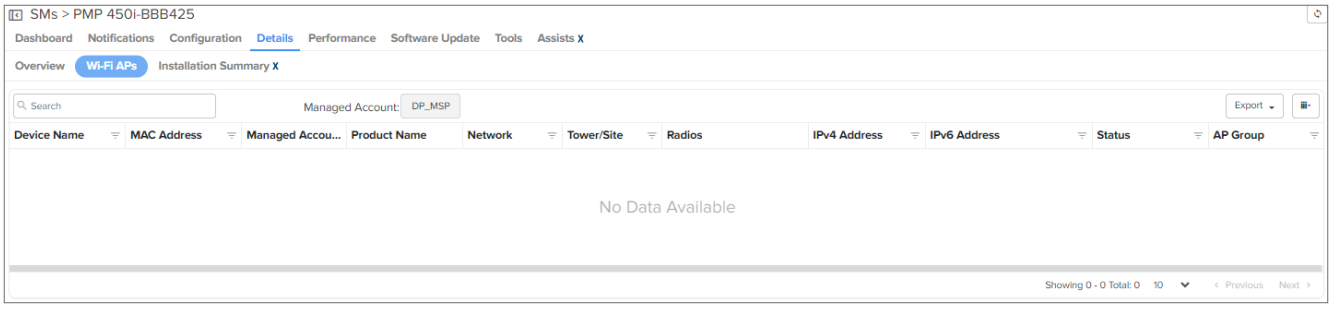


Figure 156 *PMP 450v 4 X 4 and PMP 450v 2 X 2 SMs: Device > Details > Overview*



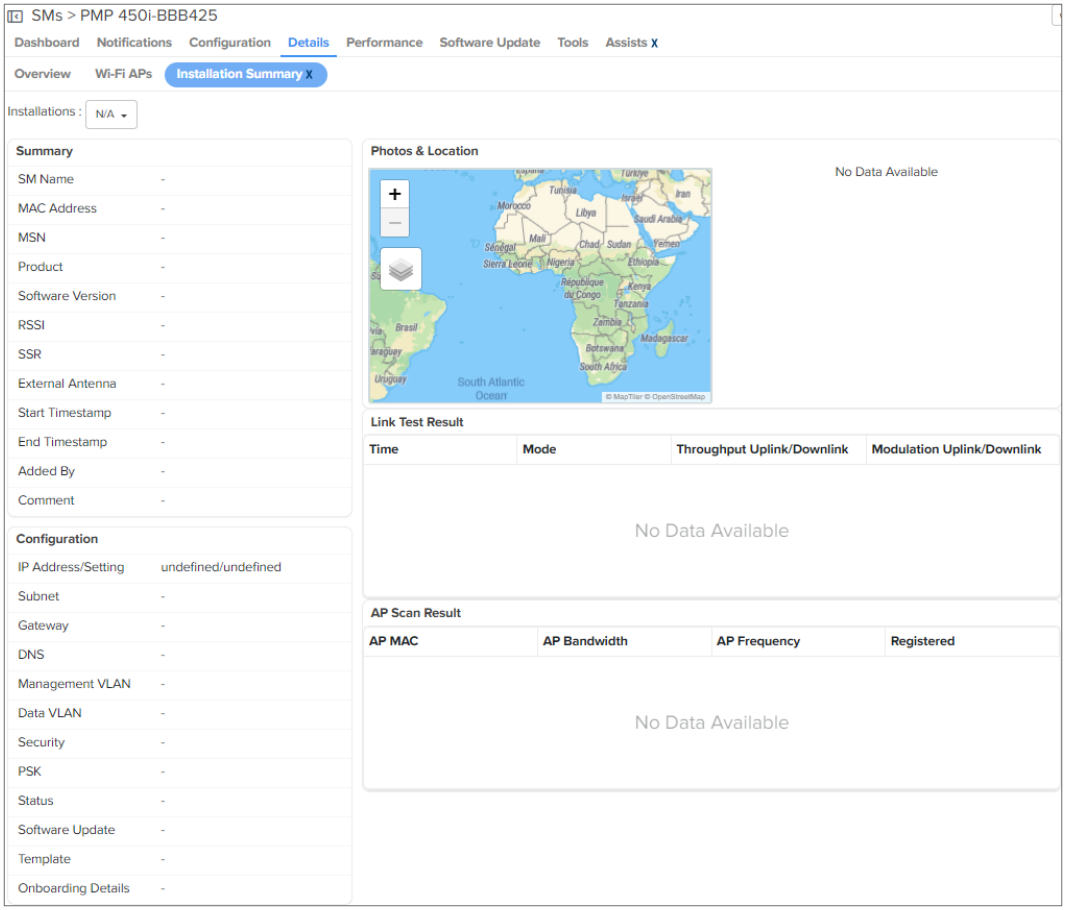
Wi-Fi APs

Figure 157 *PMP SM: Device > Details > Wi-Fi APs*



Installation Summary X

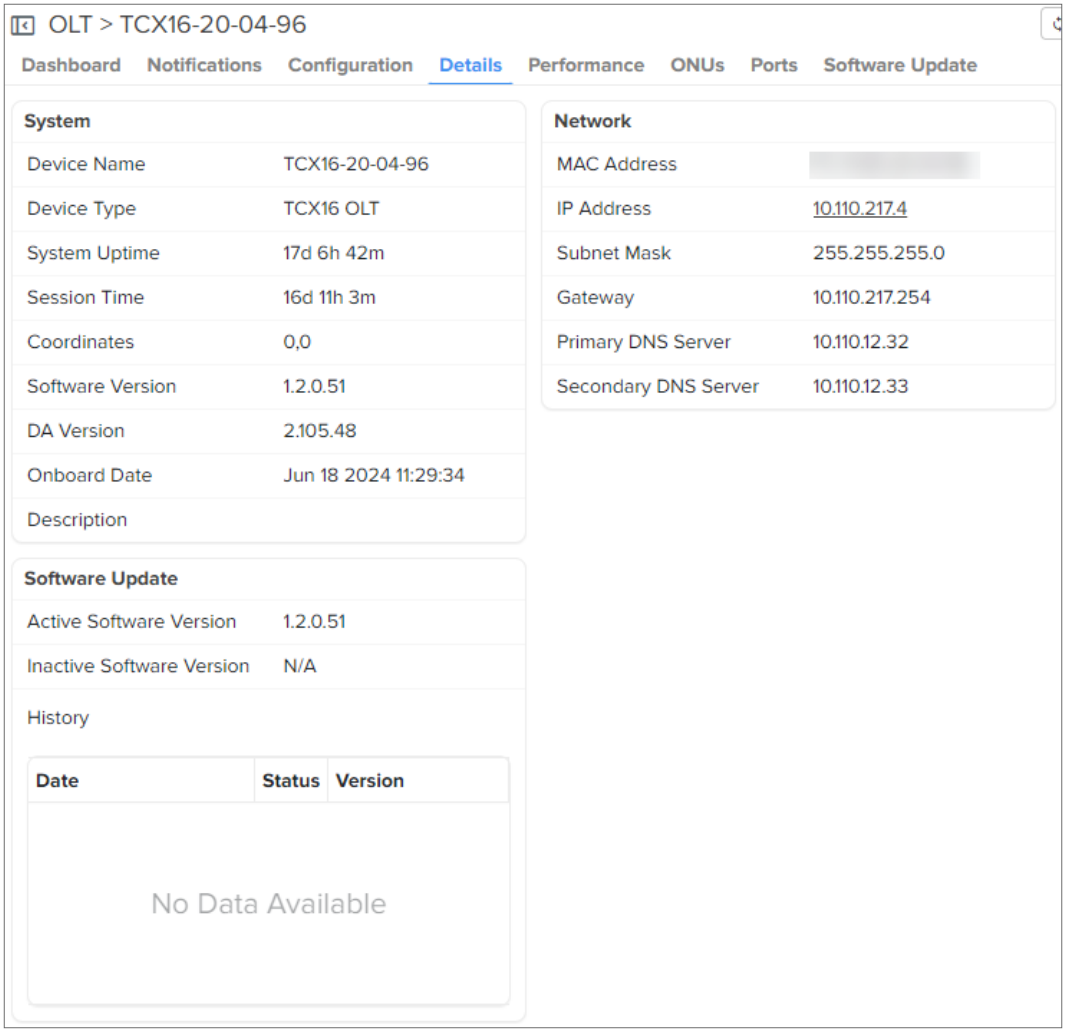
Figure 158 *PMP SM: Device > Details > Installation Summary* X



PON (OLT)

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

Figure 159 *PON (OLT): Device > Details*



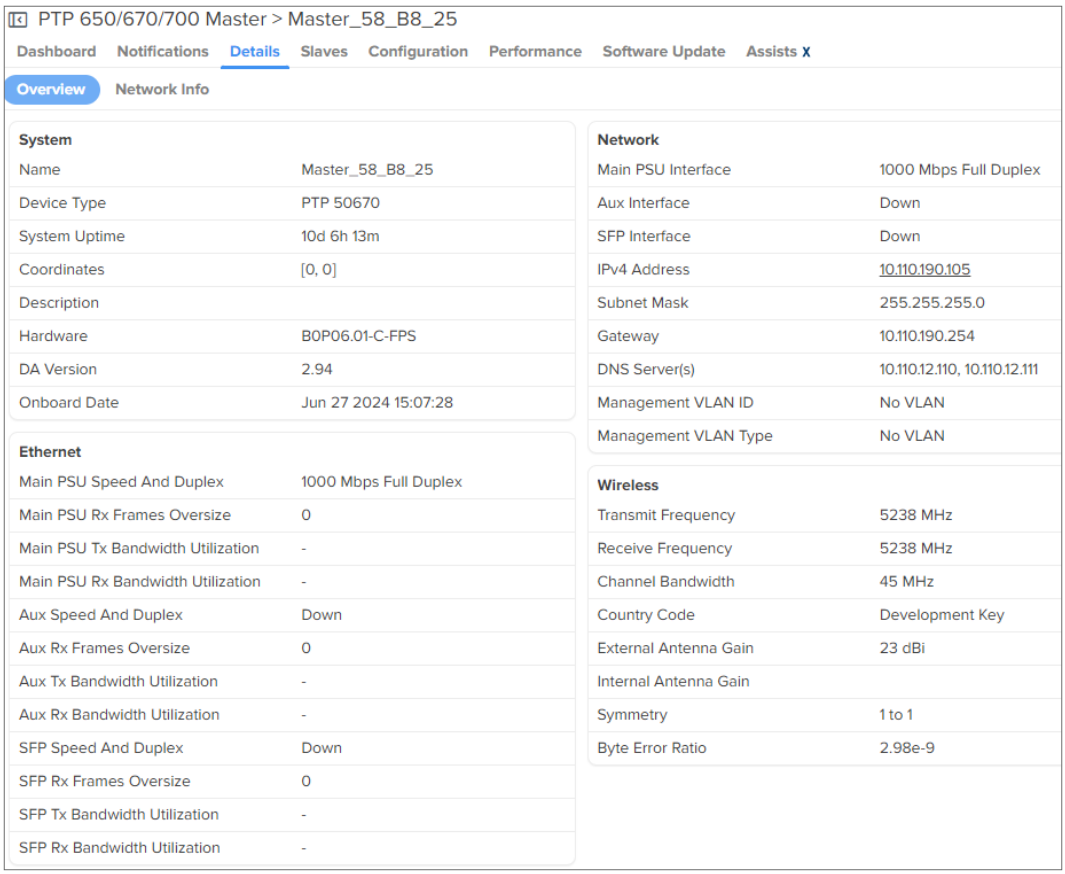
PTP 650/670/700

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

- Overview
- Network Info

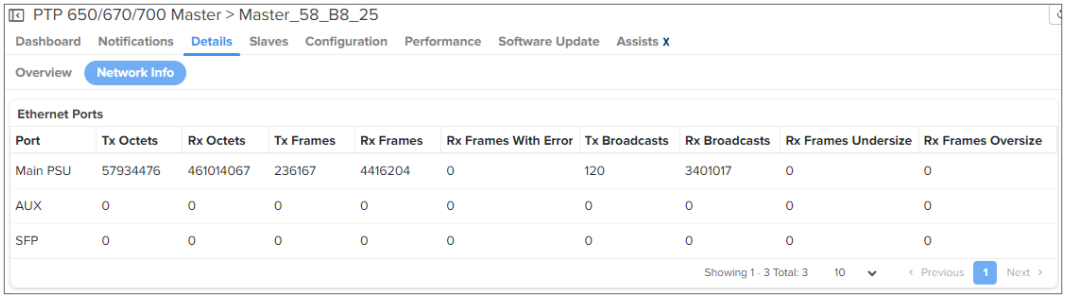
Overview

Figure 160 *PTP 650/670/700: Device > Details > Overview*



Network Info

Figure 161 *PTP 650/670/700: Device > Details > Network Info*



PTP 820/850 Details

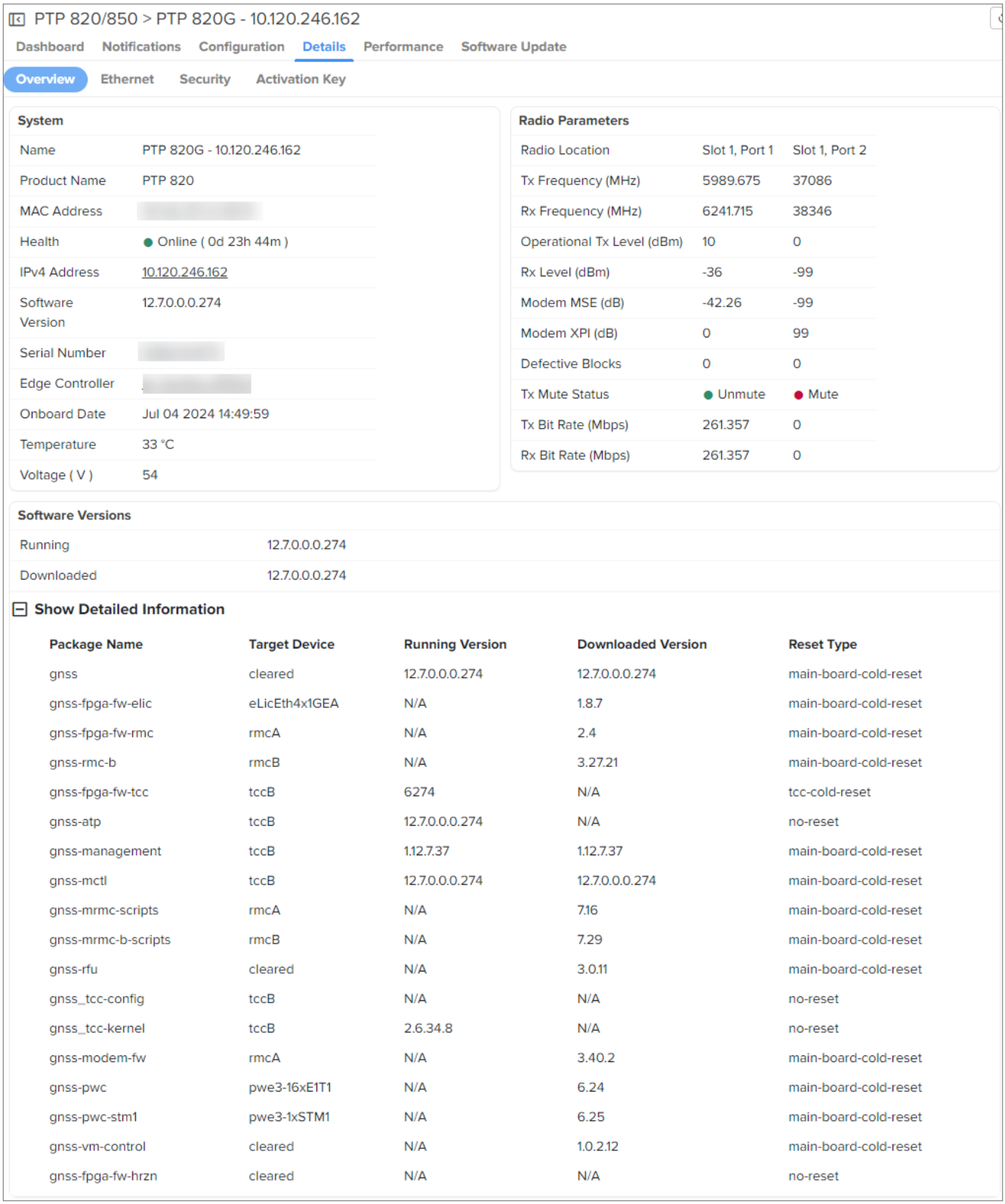
The **Details** section displays following tabs for PTP 820/850:

- Overview
- Ethernet
- Security
- Activation Key

Overview

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

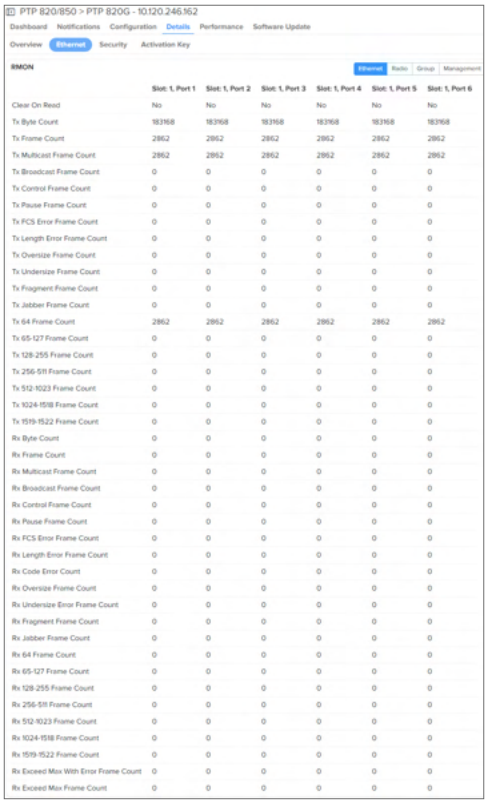
Figure 162 *PTP 820/850: Device > Details > Overview*



Ethernet

Ethernet page provides the information RMON.

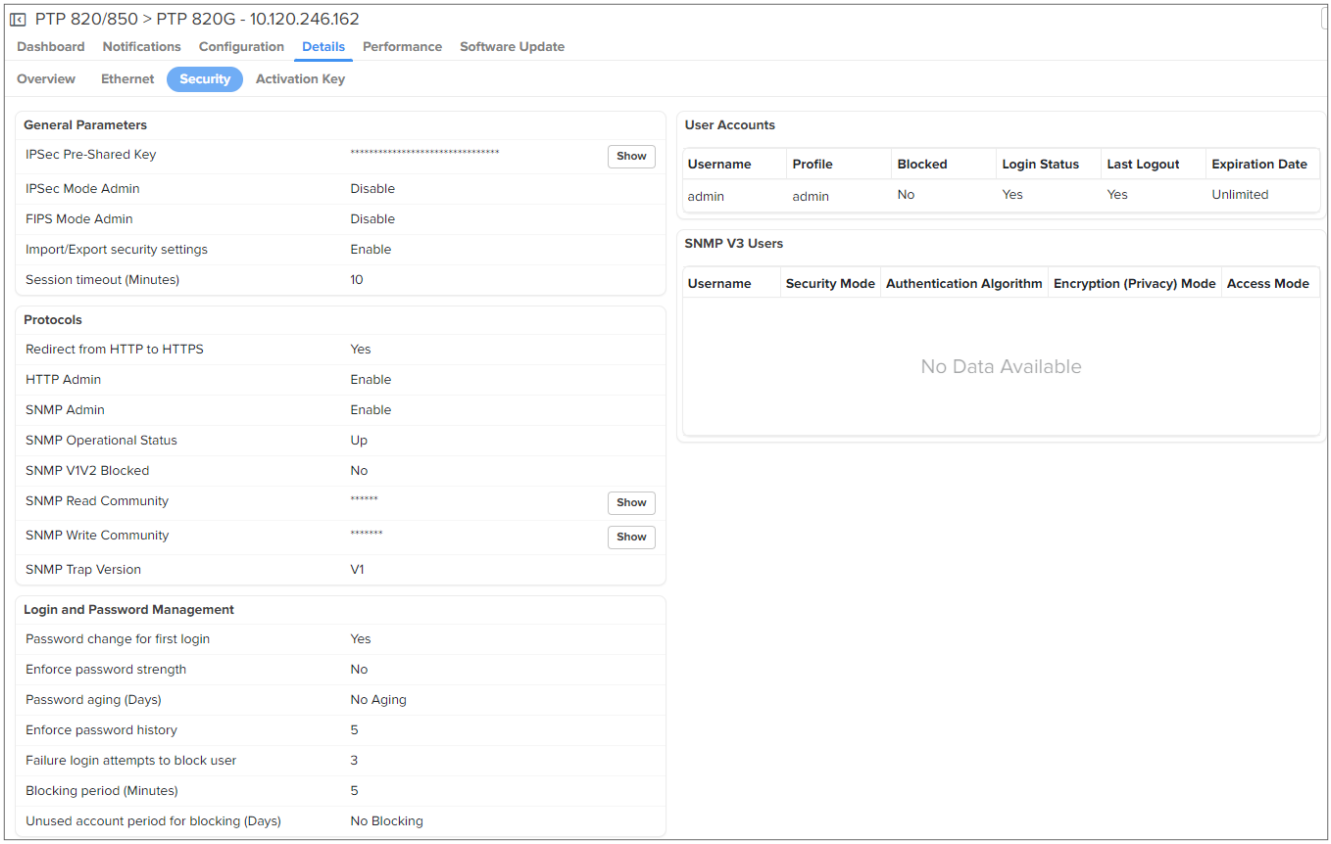
Figure 163 *PTP 820/850: Device > Details > Ethernet*



Security

Security page provides the information of General Parameters, Protocols, Login and Password Management, User Account, and SNMP V3 Users.

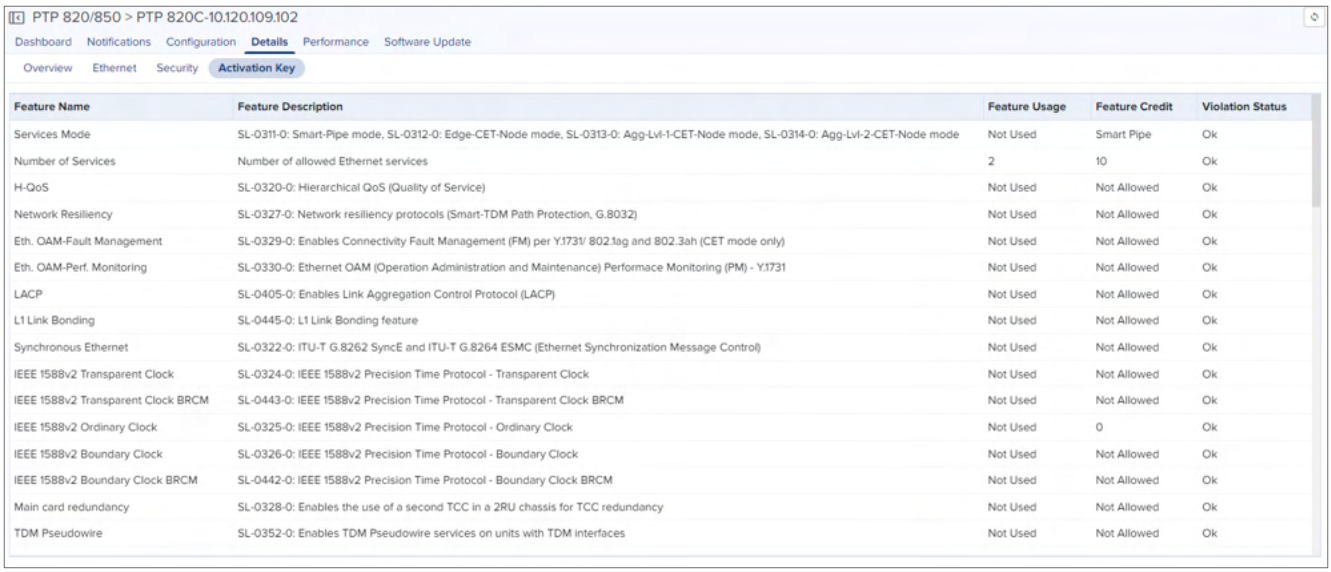
Figure 164 *PTP 820/850: Device > Details > Security*



Activation Key

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

Figure 165 *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

Home Mesh Routers

See Viewing router system information and network traffic status.

Performance

Performance pages display a synchronized view of time-series data for devices. The data can be filtered using the interval ranges in the upper left (last 1 hours to last 1 year) , or by dragging the cursor on the graph to select a specific range. The data presented varies based upon device type.



Note

cnMaestro supports 14 months of historical data for the following devices:

- cnPilot Home (R-Series)
- Enterprise devices (Enterprise Wi-Fi and cnMatrix)
- IIoT devices

cnMaestro supports 26 months of historical data for the following devices:

- Fixed Wireless

Period = 1 day is available for a Time Range of more than 24 hrs.

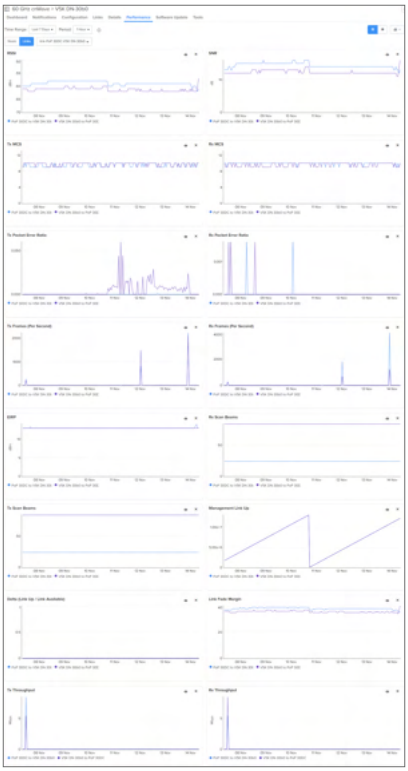
The following images represent the sample performance graphs for 60 GHz cnWave, cnMatrix, cnPilot Enterprise, cnPilot Home, cnRanger, cnReach, cnVision, cnWave 5G Fixed, ePMP AP, ePMP SM, PMP AP, PMP SM, PTP 650/670/700, and PTP 820/850.

- 60 GHz cnWave (Links)

  Displays the following graphs:

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

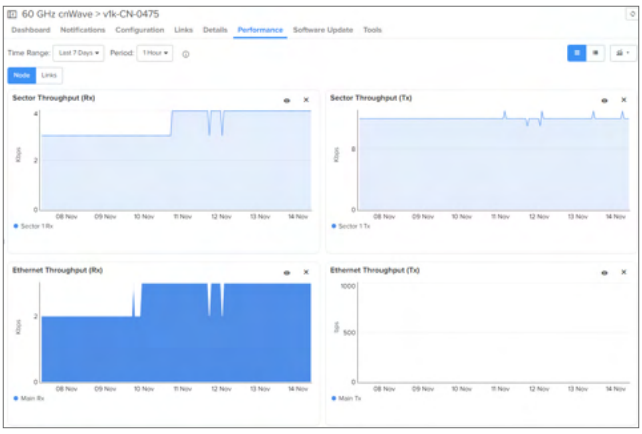
- Tx Scanbeams
- Tx Throughput



- 60 GHz cnWave (Node)

  Displays the following graphs:

  - Ethernet Throughput (Rx)
  - Ethernet Throughput (Tx)
  - Sector Throughput (Rx)
  - Sector Throughput (Tx)



- cnMatrix

  Displays the following graphs:

- CPU
- Packet Error
- Rx Packets
- Throughput
- Tx Packets



- cnPilot Home

  Displays the following graphs:

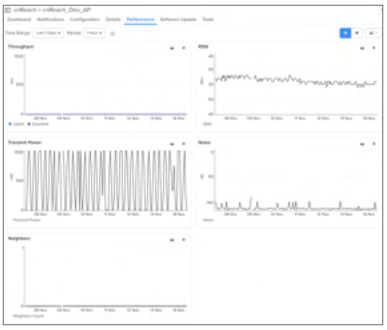
  - CPU
  - Stacked Clients by Band
  - Stacked Clients by Radio
  - Stacked Throughput by Band (Downlink)
  - Stacked Throughput by Band (Uplink)
  - Stacked Throughput by Radio (Downlink)
  - Stacked Throughput by Radio (Uplink)



- cnReach

  Displays the following graphs:

  - Neighbors
  - Noise
  - RSSI
  - Throughput
  - Transmit Power



- cnRanger BBU

  Displays the following graphs:

  - Available Memory
  - CPU
  - Interface (eth1)
  - Interface (eth2)
  - SMs Registered
  - Temperature
  - Throughput



- cnRanger RRH

  Displays the following graphs:

  - Ambient Temperature
  - CPU
  - Die Temperature
  - Frame Utilization
  - SMs Registered
  - Throughput



- cnRanger SM

  Displays the following graphs:

  - Available Memory
  - CPU
  - MCS
  - RSRP
  - RSRQ
  - RSSI
  - SINR
  - Throughput



- cnVision Client

  Displays the following graphs:

  - CPU
  - MCS
  - Retransmission
  - RSSI
  - Session Drops
  - SNR
  - Throughput



- cnVision Hub

  Displays the following graphs:

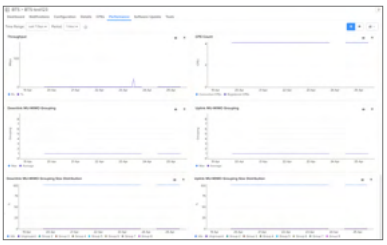
  - CPU
  - Frame Utilization
  - Retransmission
  - SMs Registered
  - Throughput



- cnWave 5G Fixed BTS

  Displays the following graphs:

  - CPE Count
  - Downlink MU-MIMO Grouping
  - Downlink MU-MIMO Grouping Size Distribution
  - Throughput
  - Uplink MU-MIMO Grouping
  - Uplink MU-MIMO Grouping Size Distribution



- cnWave 5G Fixed CPE

  Displays the following graphs:

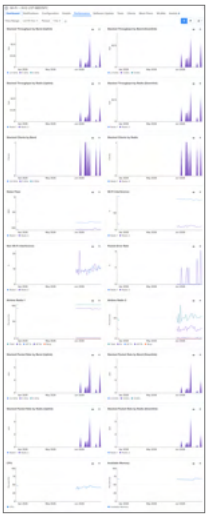
- EVM
- MCS
- Registration Count
- Rx Power
- Throughput



- Enterprise Wi-Fi

  Displays the following graphs:

  - Airtime Radio 1
  - Airtime Radio 2
  - Available Memory
  - Clients by Band
  - Clients by Radio
  - CPU
  - Noise Floor
  - Non Wi-Fi Interference
  - Packet Error Rate
  - Stacked Clients by Band
  - Stacked Clients by Radio
  - Stacked Packet Rate by Band (Downlink)
  - Stacked Packet Rate by Band (Uplink)
  - Stacked Packet Rate by Radio (Downlink)
  - Stacked Packet Rate by Radio (Uplink)
  - Stacked Throughput by Band (Downlink)
  - Stacked Throughput by Band (Uplink))
  - Stacked Throughput by Radio (Downlink)
  - Stacked Throughput by Radio (Uplink)
  - Wi-Fi Interference



- Enterprise Wi-Fi (Xirrus-Series)

  Displays the following graphs:

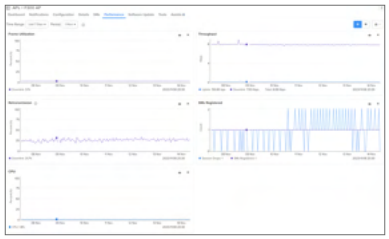
  - Available Memory
  - Clients by Band
  - Clients by Radio
  - CPU
  - Stacked Packet Rate by Band (Downlink)
  - Stacked Packet Rate by Band (Uplink)
  - Stacked Packet Rate by Radio (Downlink)
  - Stacked Packet Rate by Radio (Uplink)
  - Stacked Throughput by Band (Downlink)
  - Stacked Throughput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



- ePMP AP

Displays the following graphs:

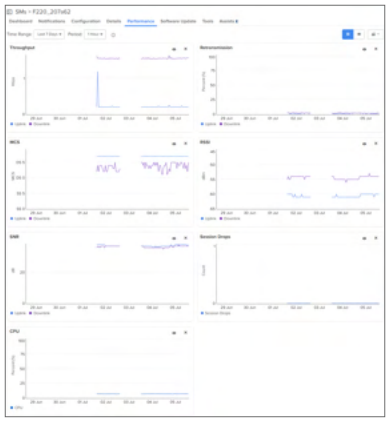
- CPU
- Frame Utilization
- Retransmission
- SMs Registered
- Throughput



- ePMP SM

  Displays the following graphs:

  - CPU
  - MCS
  - Retransmission
  - RSSI
  - Session Drops
  - SNR
  - Throughput



- NSE

  Displays the following graphs:

  - Available Memory
  - CPU



- 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

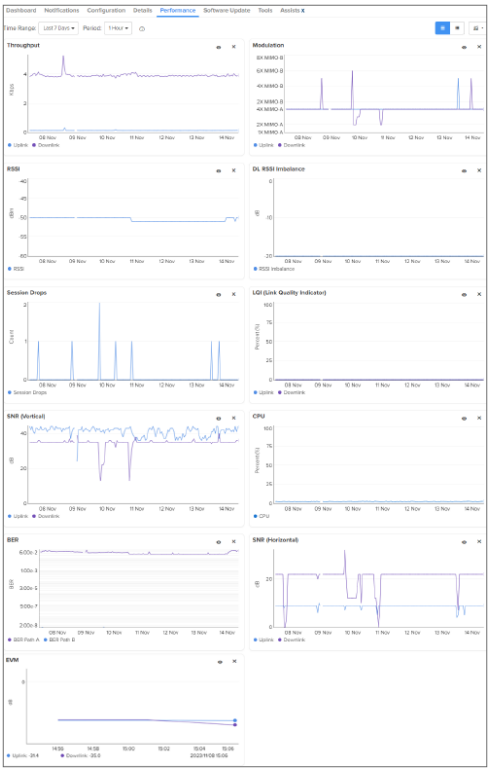


- PMP SM

  Displays the following graphs:

  - BER
  - CPU
  - DL RSSI Imbalance
  - EVM
  - LQI (Link Quality Indicator)
  - Modulation
  - RSSI
  - Session Drops

- SNR (Horizontal)
- SNR (Vertical)
- Throughput

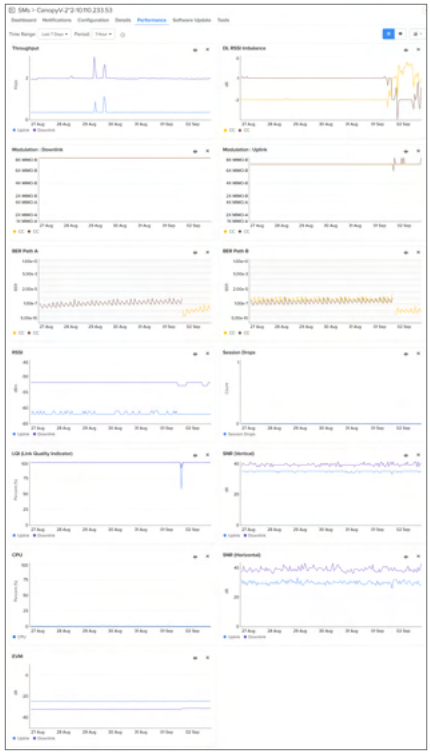


- PMP 450v 4 X 4 and PMP 450v 2 X 2 SMs

  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

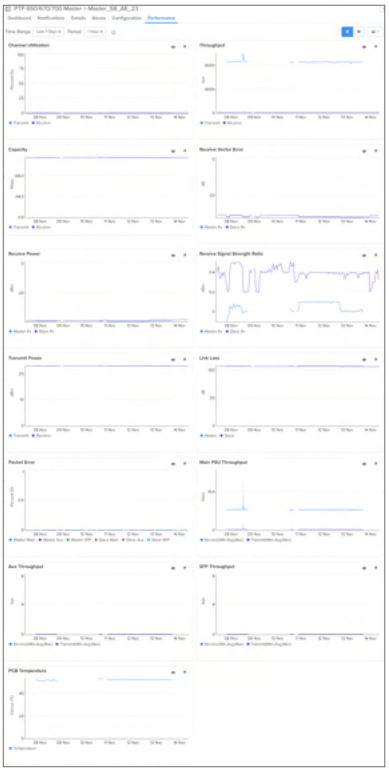


- PTP and HCMP Masters

  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

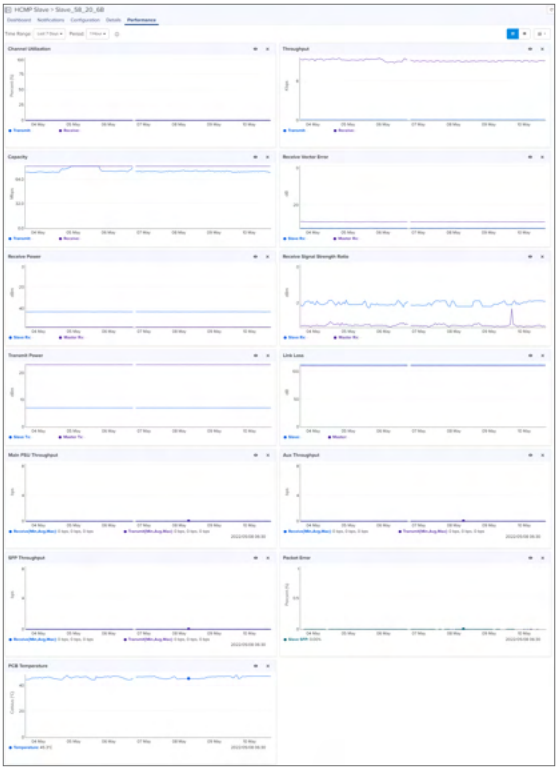


- PTP and HCMP Slaves

  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



- RV22 Home Mesh

  Displays the following graphs:

  - Airtime 2.4 GHz
  - Airtime 5 GHz
  - Available Memory
  - CPU
  - Interference
  - Noise Floor
  - Stacked Clients by Band
  - Stacked Throughput by Band (Downlink)
  - Stacked Throughput by Band (Uplink)
  - Stacked WAN Throughput



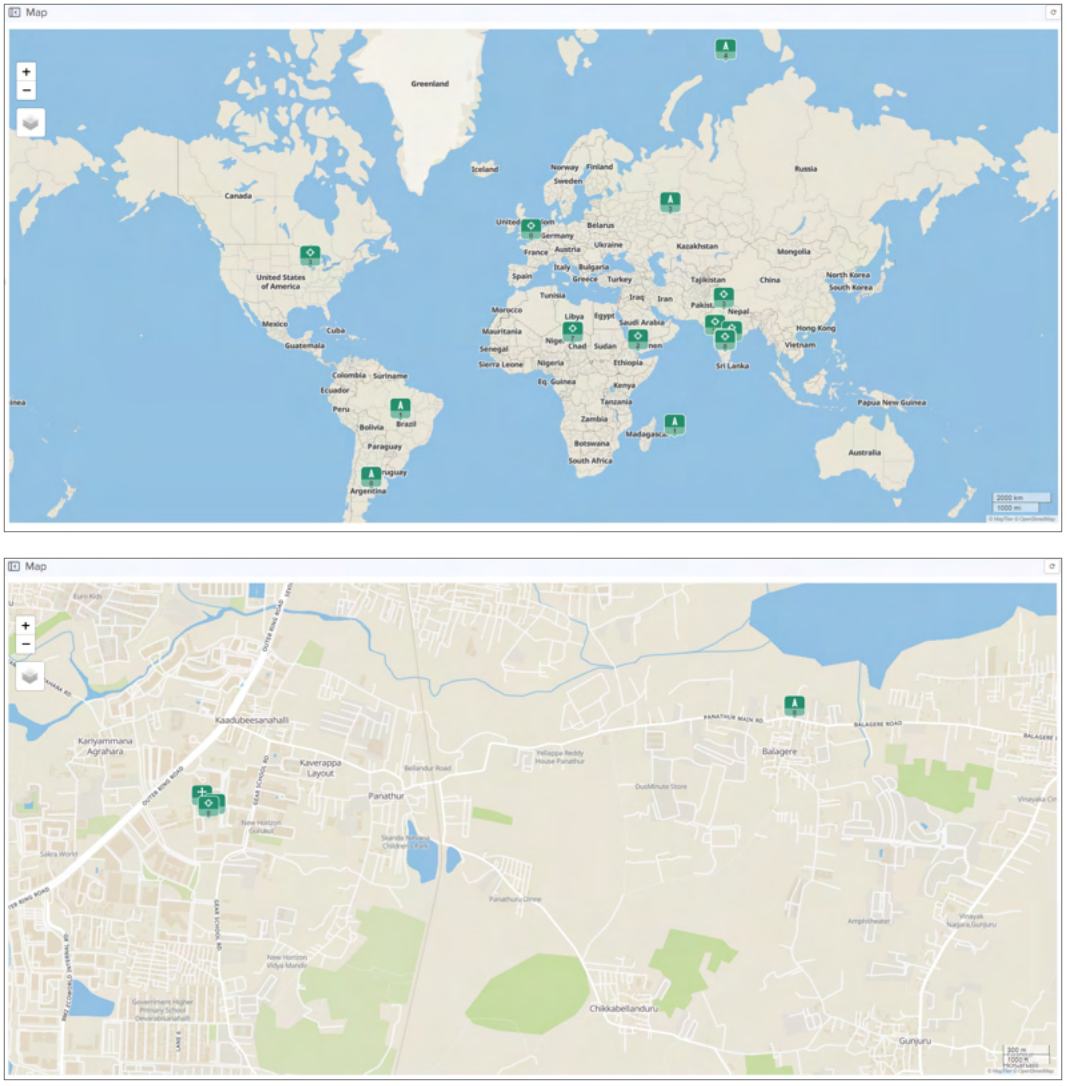
Map

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 166 *Map Street View*

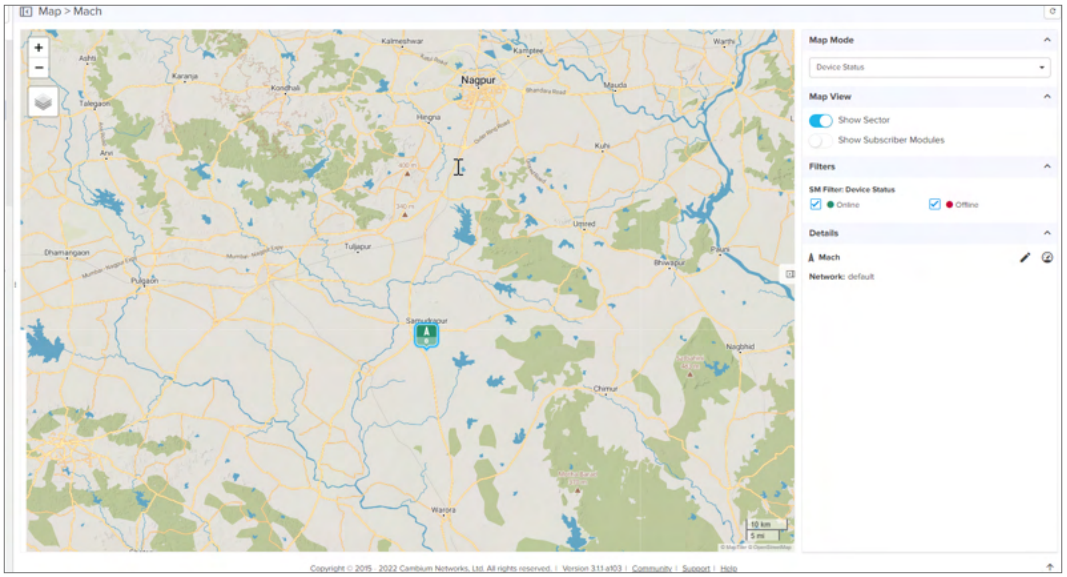


The Satellite View is supported in limited US and EU regions.

Figure 167 *Map Satellite View*



Figure 168 *Map Terrain View*



If latitude or longitudinal of Site or Tower or Device is (-90°, 90°, -180°, 180°) or (0,0) then they will not display in the map.



Note

- (0,0) is the default value for devices that do not have a location set cnMaestro does not plot devices with this location.
- (x, 180°) and (x, -180°) require the user to zoom out in order to see the markers.
- (90°, y) and (-90° ,y) also displays incorrectly.

Map Navigation

There are a various ways to navigate the map display.

Action	Description
Click	Click the following items on the Map to auto-select the same item in the Tree. • ePMP SM • 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, which define how the device status is presented.

Table 27 *Mode*

Mode	Details
Alarm Status	Highlights devices based upon alarm count (Critical, Major, Minor).
Average MCS	Displays the Uplink or Downlink average MCS per device.
Device Status	Displays whether a device is Up (Green) or Down (Red).
Frequency	Displays the device sector frequency.
Link Quality Indicator (PMP)	Displays the Uplink or Downlink status.
Packet Loss	Displays the Uplink or Downlink packet loss per device.
Reregistration Count	Displays the nodes based upon the number of re-registrations in the last 24 hours. The more re-registrations, the larger the node is display.

Table 27 *Mode*

Mode	Details
Retransmission Percentage (ePMP and cnVision)	Displays the Uplink or Downlink percentage status.

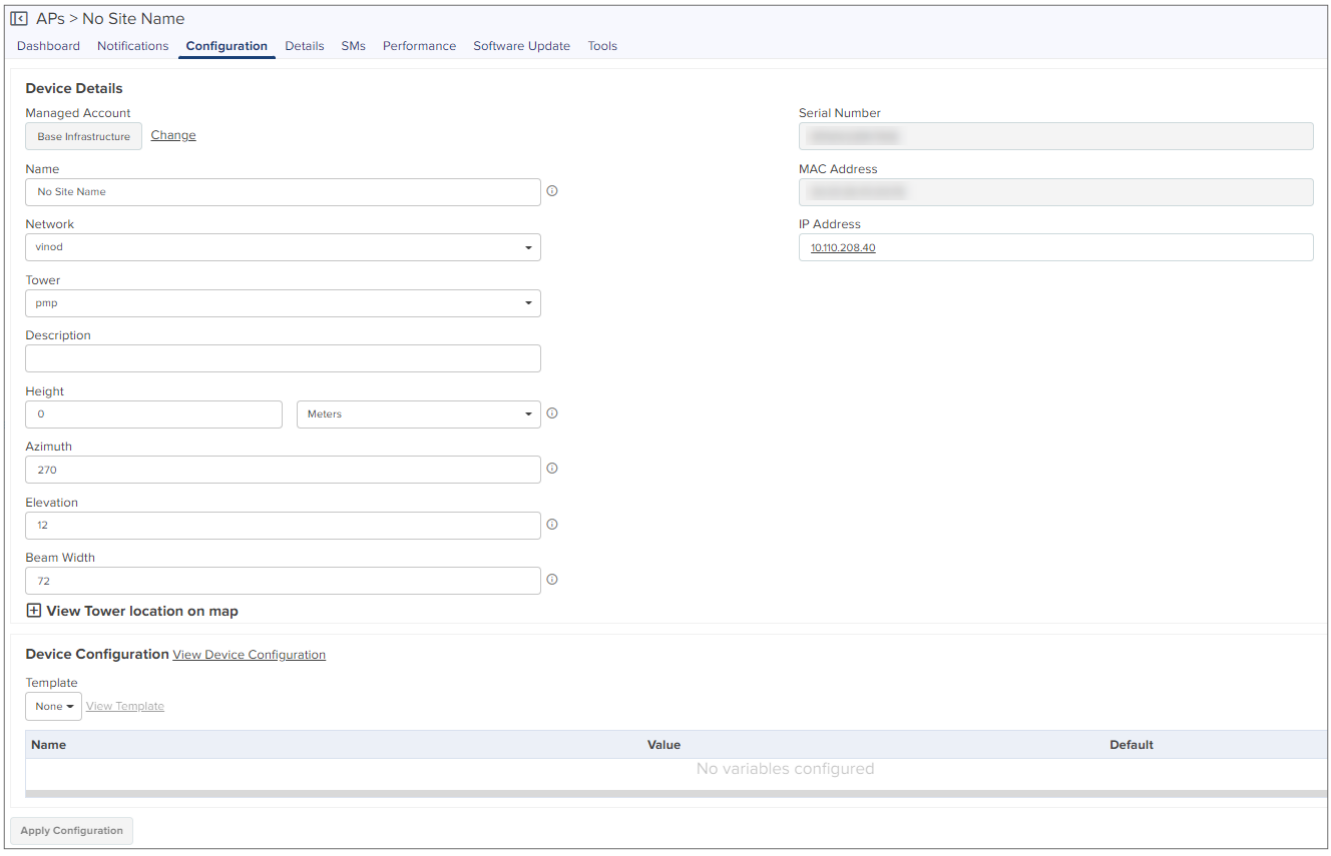
Embedded Maps

Maps are embedded into some additional UI views (most notably, the Dashboard). These embedded maps do not provide the full feature set of the map view.

Sector Visualization

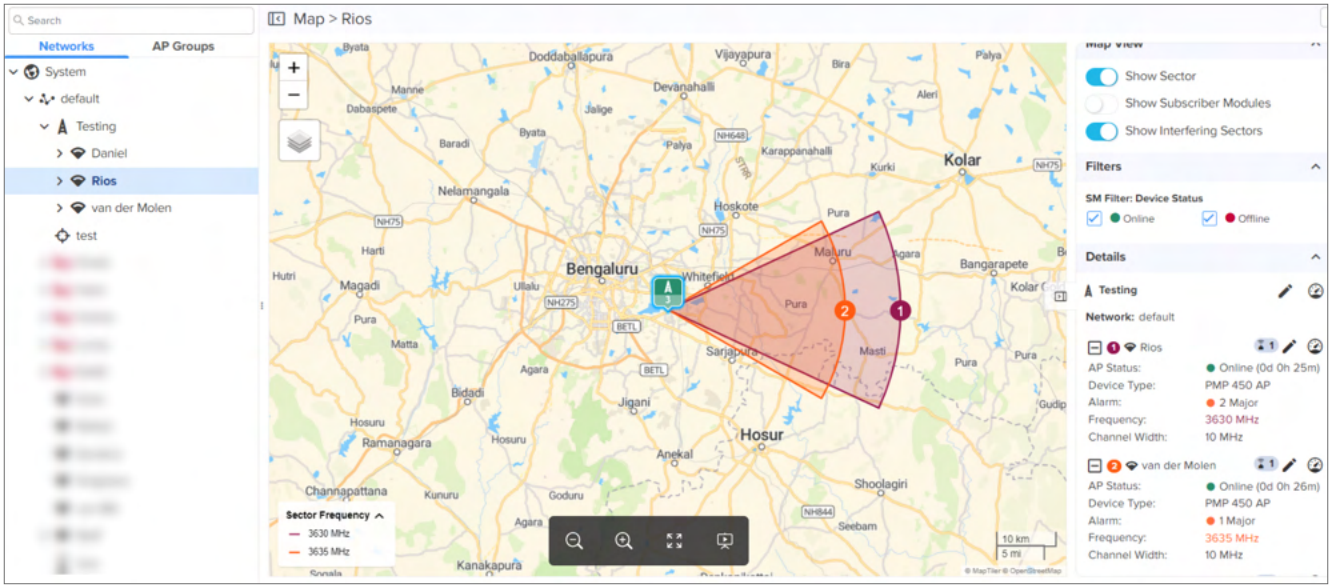
cnMaestro presents a basic sector View for ePMP and PMP fixed wireless devices. This requires configuration of Height, Azimuth, Elevation, and Beamwidth under cnRanger ePMP/PMP AP configuration. This configured data is used to generate the Sector View. The presentation is not based upon link planning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

Figure 169 *AP Configuration*



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

Figure 170 *Sector Visualization*



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

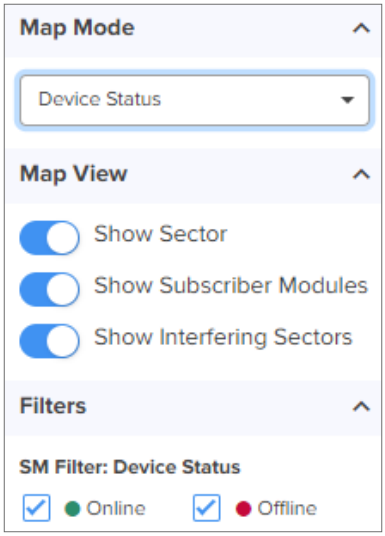
Note

- By default **Show Subscriber Modules** is disabled.
- Map view is supported for PMP, ePMP, cnRanger, cnPilot Home, PTP, 60 GHz cnWave, cnVision, cnMatrix, Enterprise Wi-Fi Series, and RV22 Home Mesh at site- and device-levels.

The **Show Interfering sector** option compares the frequency and bandwidth with all other devices in the network. The map displays the devices that have overlapping frequencies.

Note

Show Interfering Sectors is applicable only for PMP devices and is enabled only if the **Show Sector** button is **ON**.



Maps are available for the Site and Device levels. The right pane displays the device details in the map. To view the map device details, do one of the following:

- Click the (+) plus sign, next to Site or Device in the right pane of the Map page, to view the device and site details as shown in Figure 171.
- Click the Dashboard() icon next to the Site or Device name, to view the site or device dashboard details.

Figure 171 *Map: Enterprise Site level*

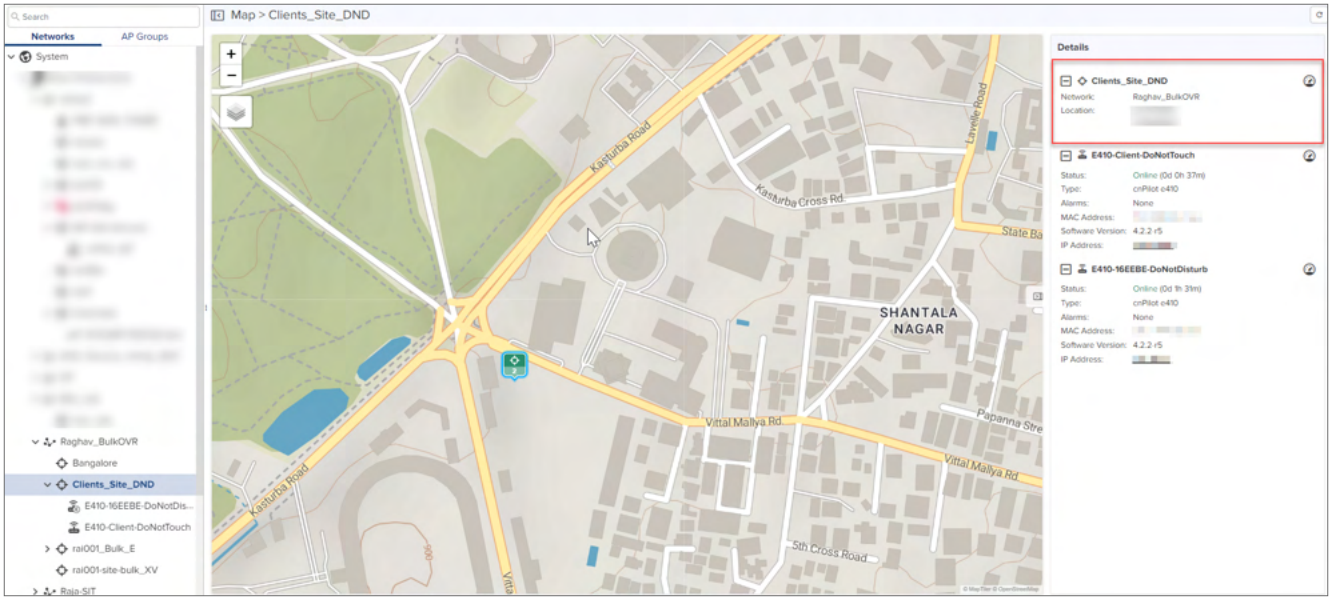


Figure 172 *Map: Home Site level*

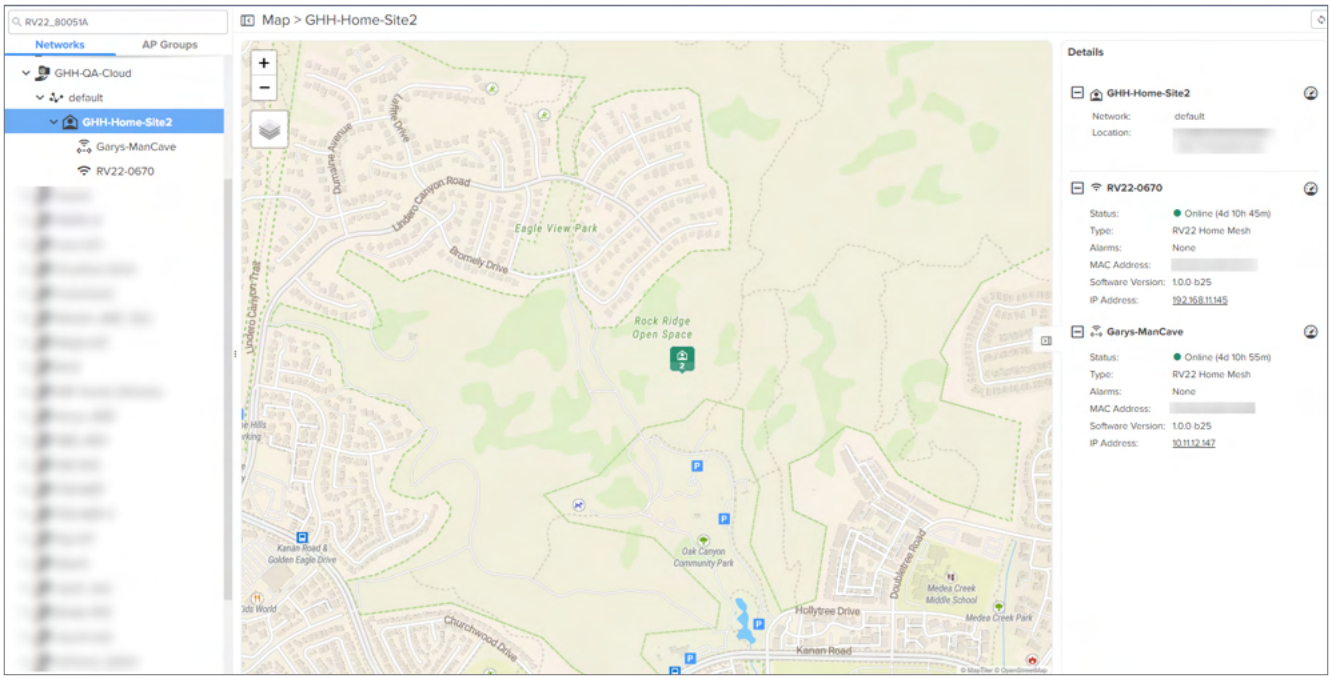


Figure 173 *Map: Device level*

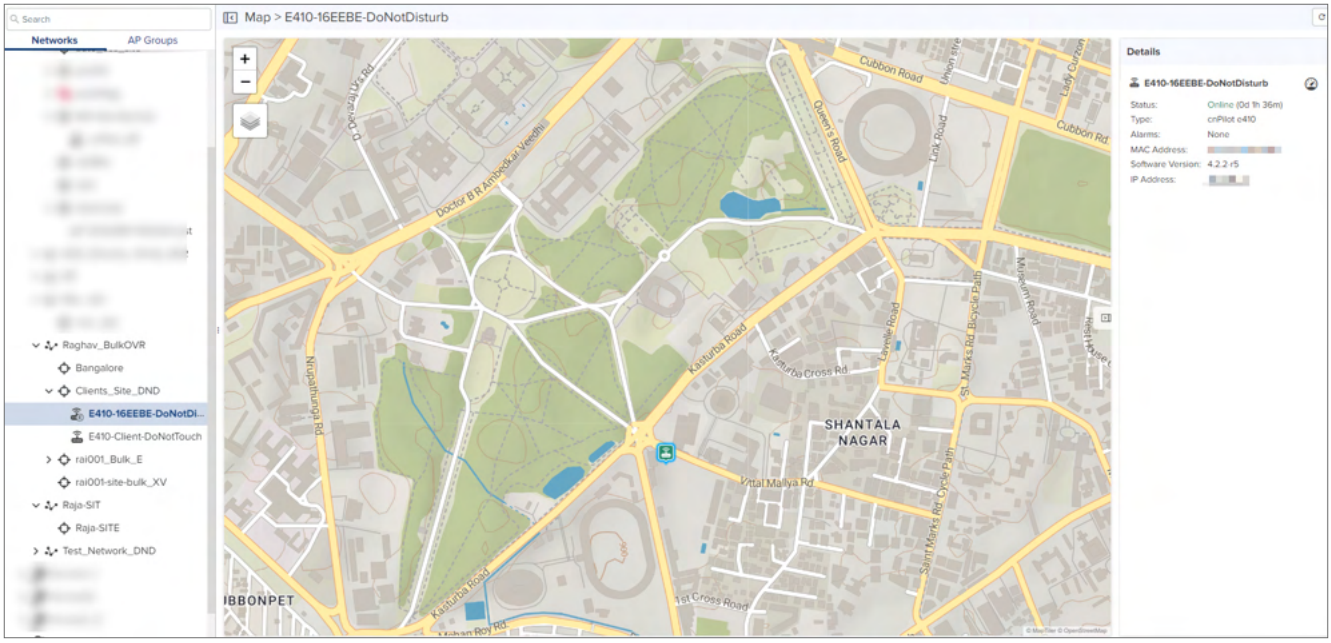


Figure 174 *Map view: cnMatrix*

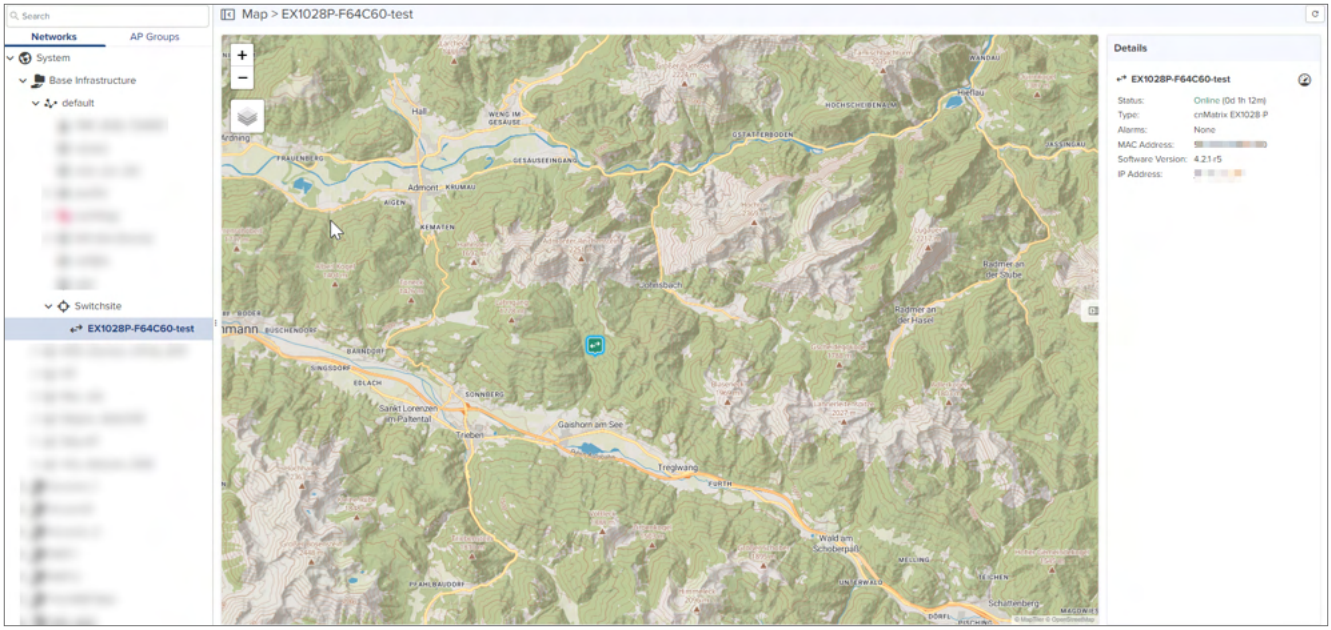


Figure 175 *Map view: Enterprise Wi-Fi (Xirrus-Series)*

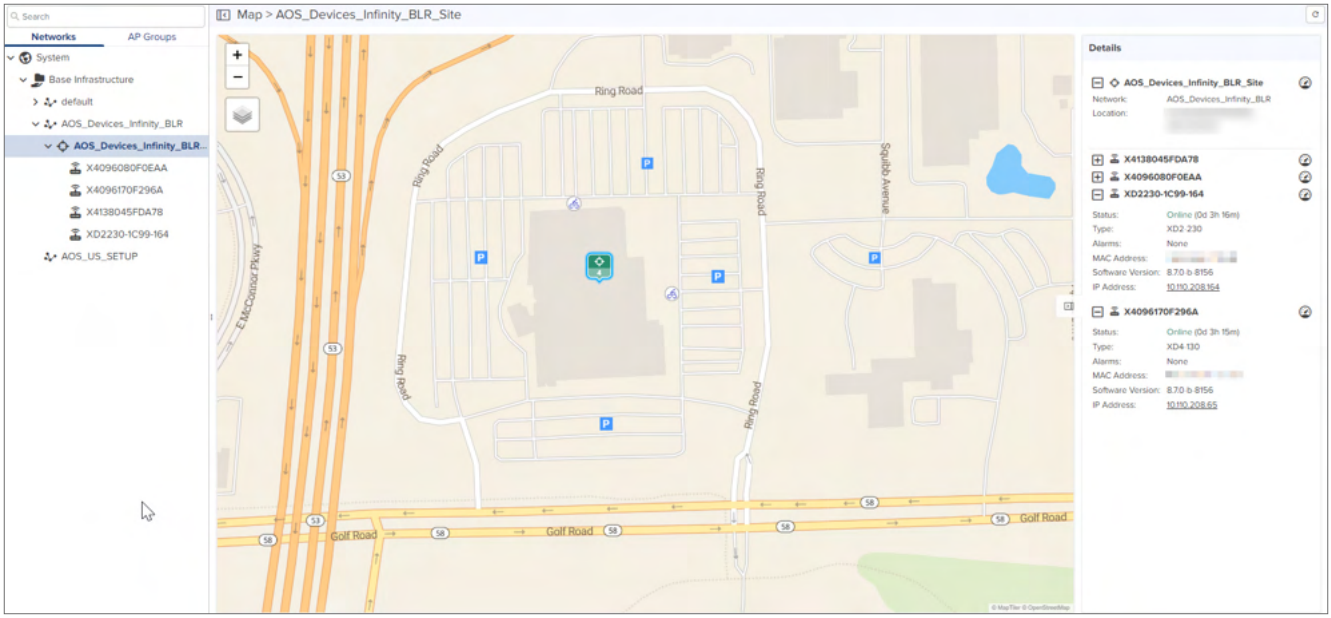
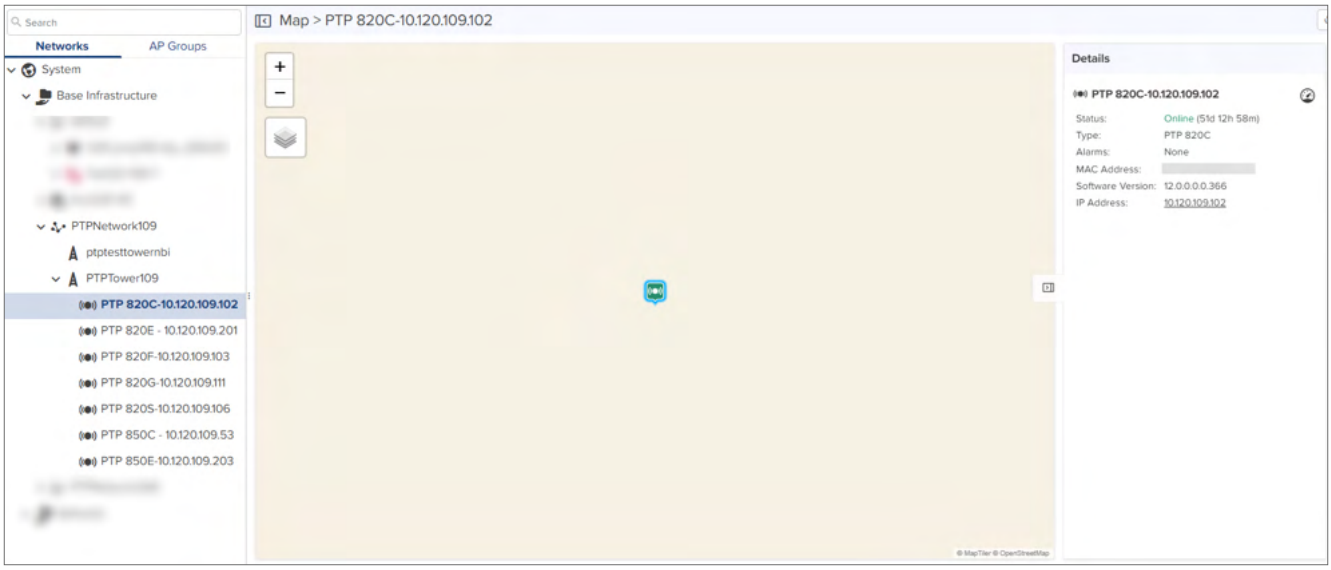


Figure 176 *Map View: PTP 820/850*



Tools

This section provides the following details:

- 60 GHz cnWave Tools
- cnMatrix Tools
- cnPilot Home Tools
- cnRanger Tools
- cnReach Tools
- cnVision Tools

- Edge Controller Tools
- Enterprise Wi-Fi Tools
- ePMP Tools
- PMP Tools
- cnWave 5G Fixed Tools
- RV22 Home Mesh Tools

60 GHz cnWave Tools

In E2E Network **Tools** tab you can view Operations, Diagnostics, Debug, Remote Command, Services, and Settings. Refer to E2E Network Tools.

In Nodes **Tools** tab you can view the Status, Debug, and Remote Command of the device. Refer to Node Tools.

cnMatrix Tools

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

Table 28 *cnMatrix Tools*

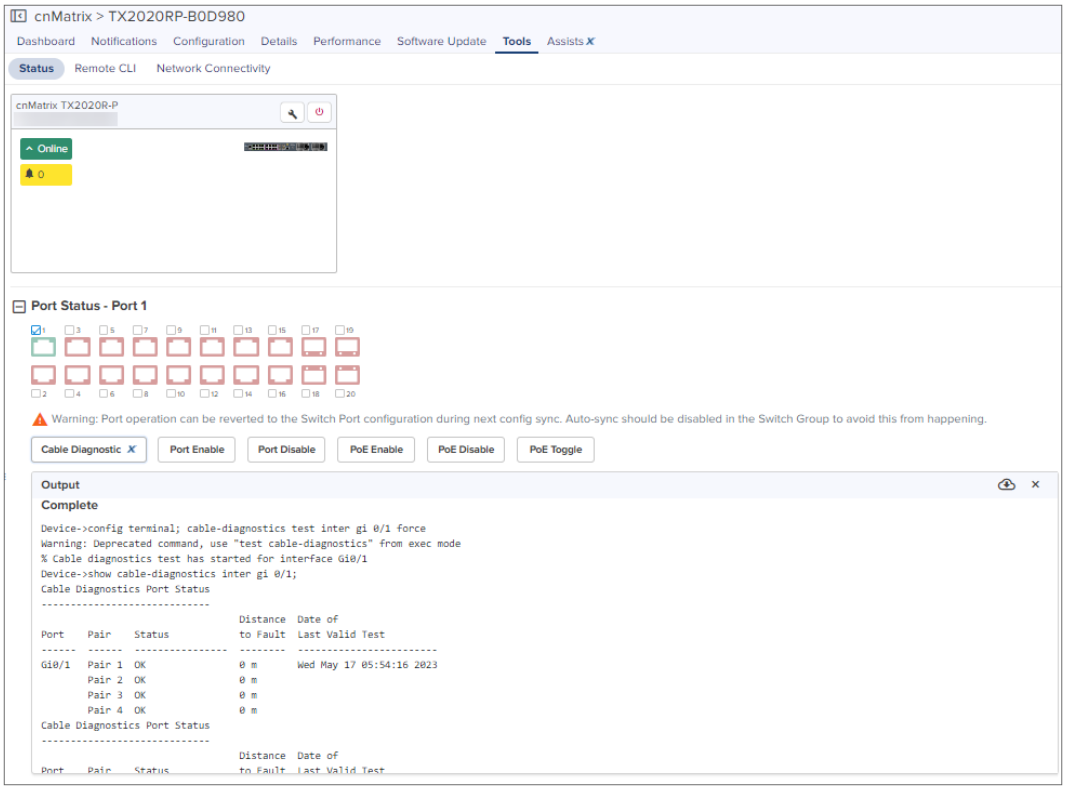
Field	Description
Network Connectivity	Executes Ping, DNS, or Traceroute tests.
Remote CLI	Enter CLI command in the command text box to execute on device. • Only Show command is allowed for Operator users. • All CLI commands are supported by Super Admin and Admin users.
Status	Displays the Status and 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.

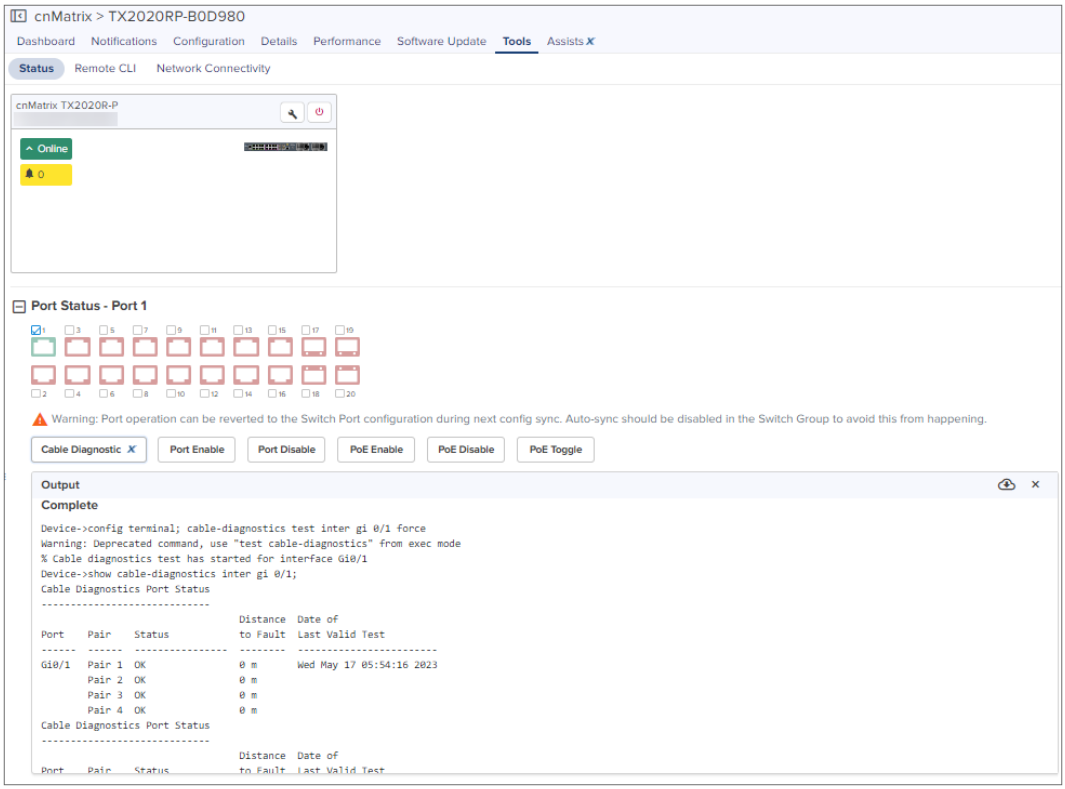


Port Status, presents the following data for the **PoE Switches**:

- 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:



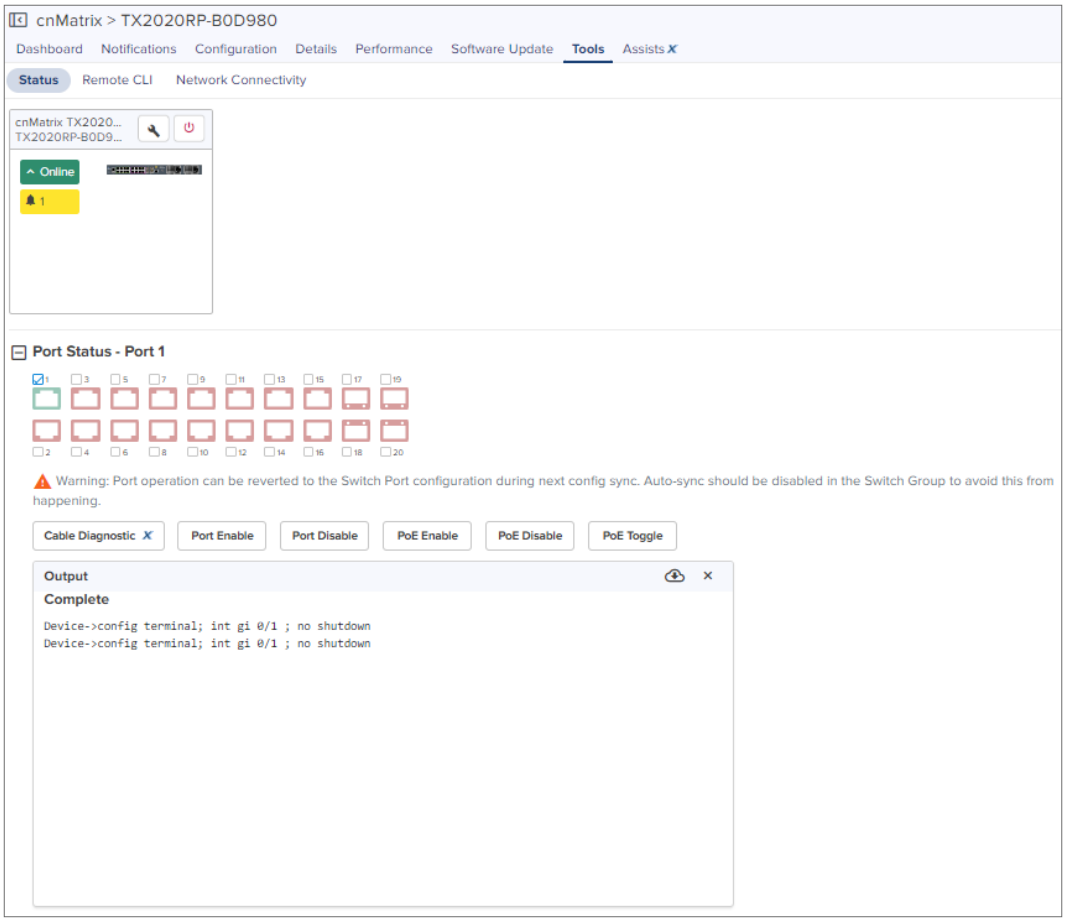
- Download the generated output by clicking the download ( ) icon.
- Clear the generated output by clicking the delete ( ) icon.

Note

Cable Diagnostic is a cnMaestro X feature.

Port Enable or Port Disable

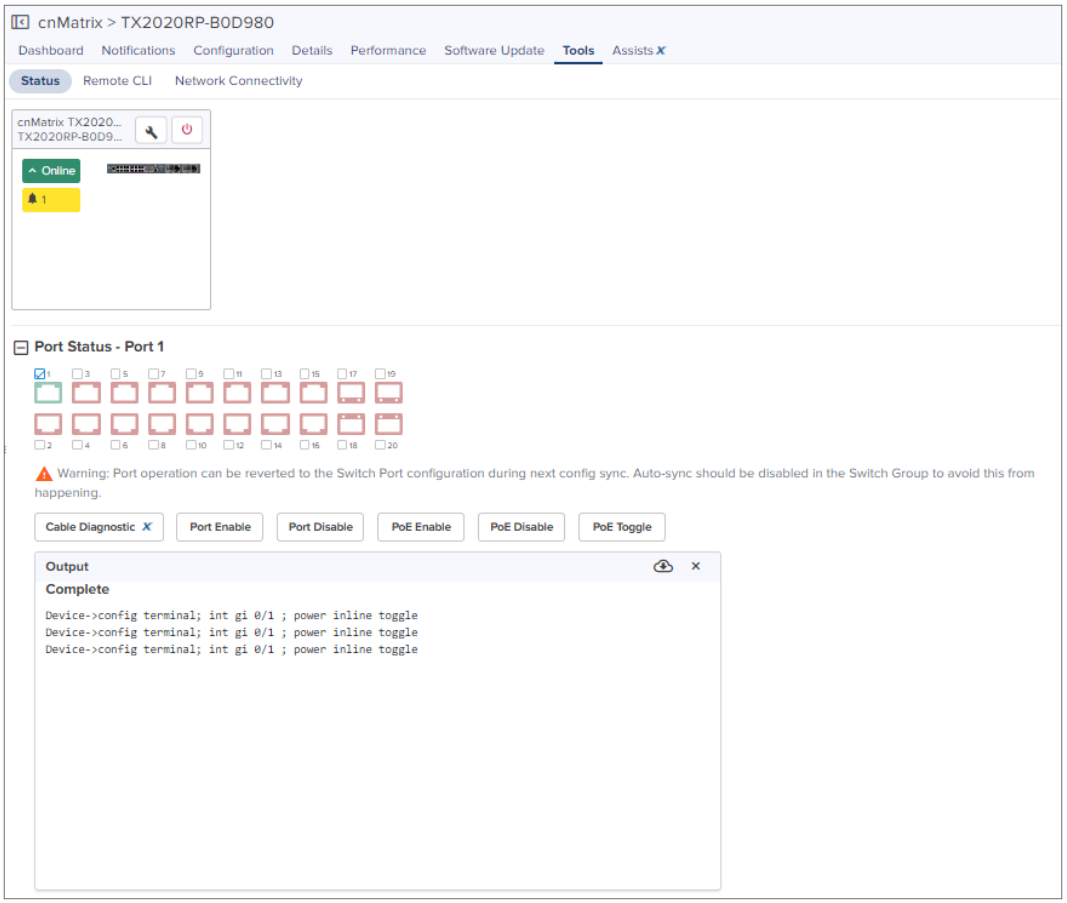
Navigate to **Tools > Status > Port Status**, select the Port and click **Port Disable** or **Port Enable**, the following output is displayed:



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

PoE Toggle

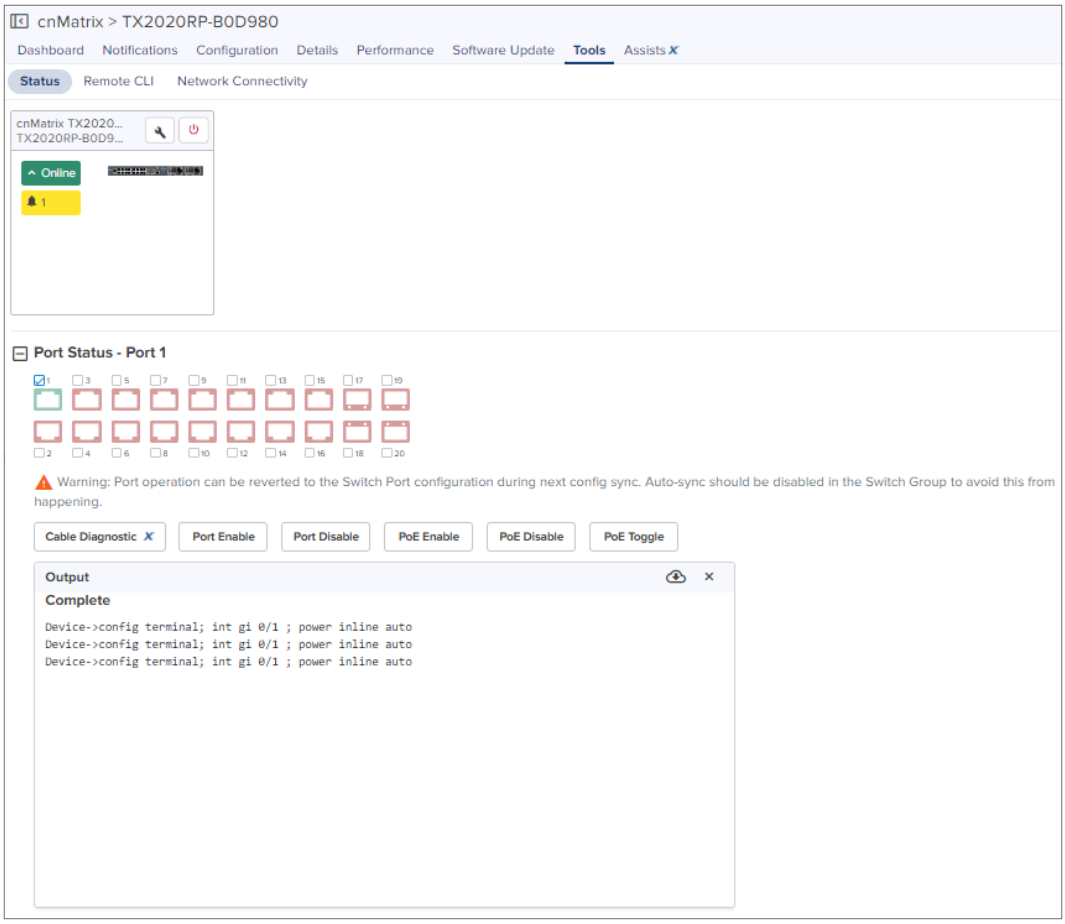
Navigate to **Tools > Status > Port Status**, select the Port and click **PoE Toggle**, the following output is displayed:



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

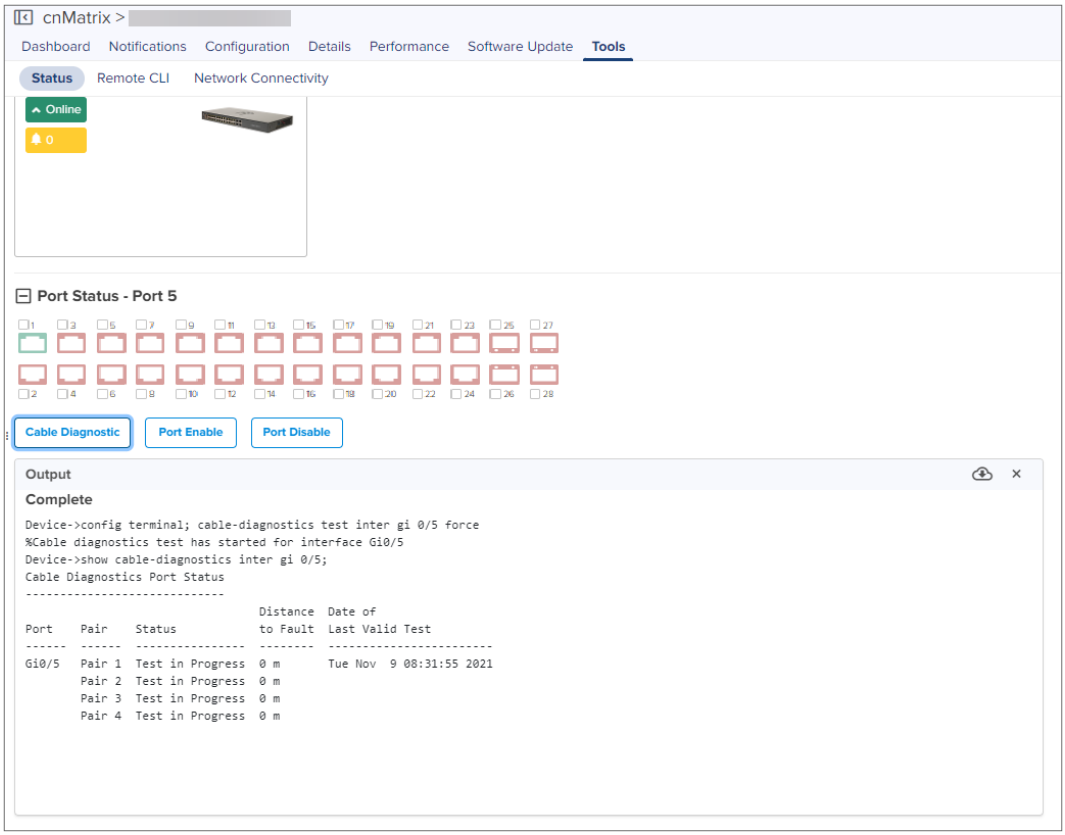
PoE Enable or PoE Disable

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



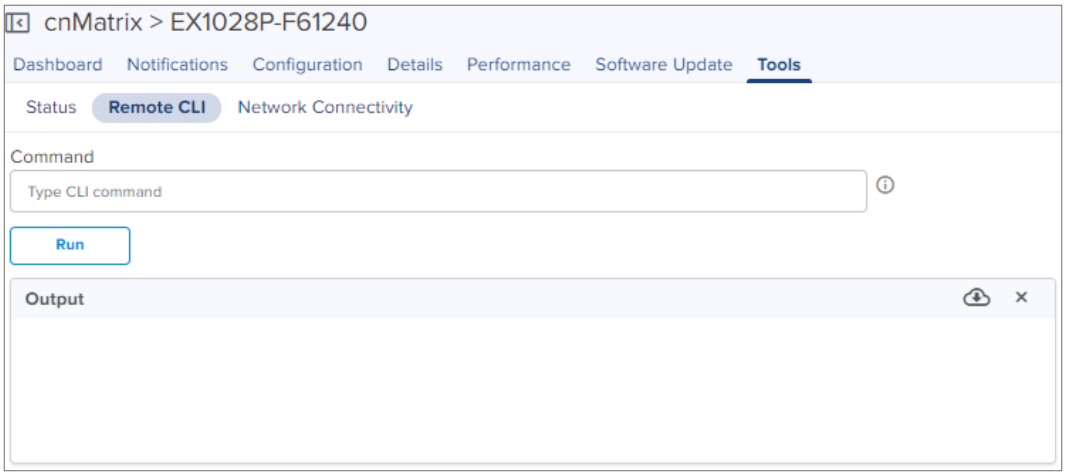
Port Status, presents the following port status for the **non-PoE Switches**:

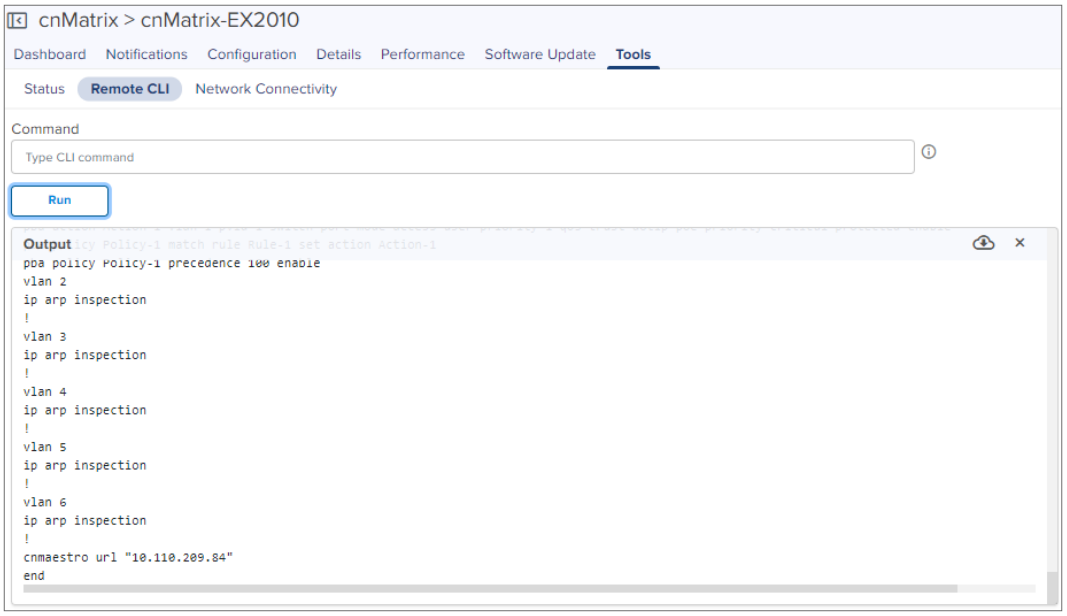
- Cable Diagnostic
- Port Enable
- Port Disable



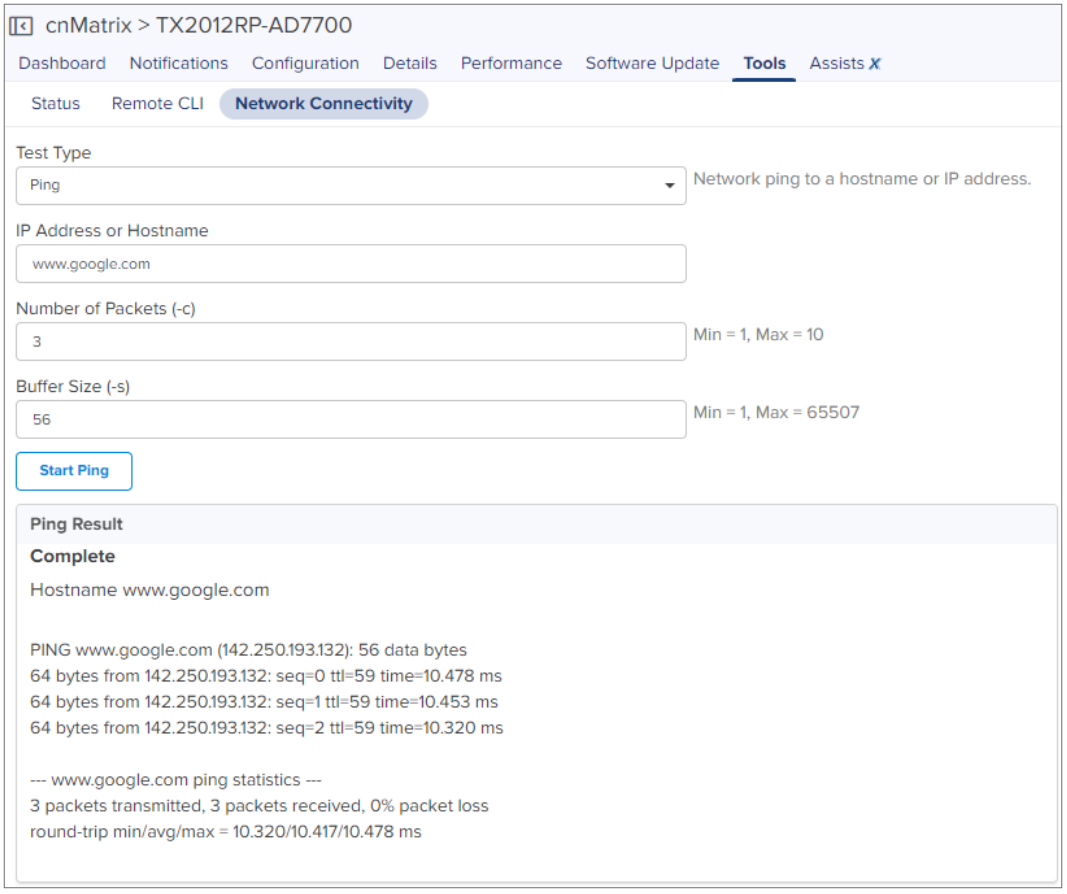
Remote CLI

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





- 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 29 *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 177 *cnPilot Tools*

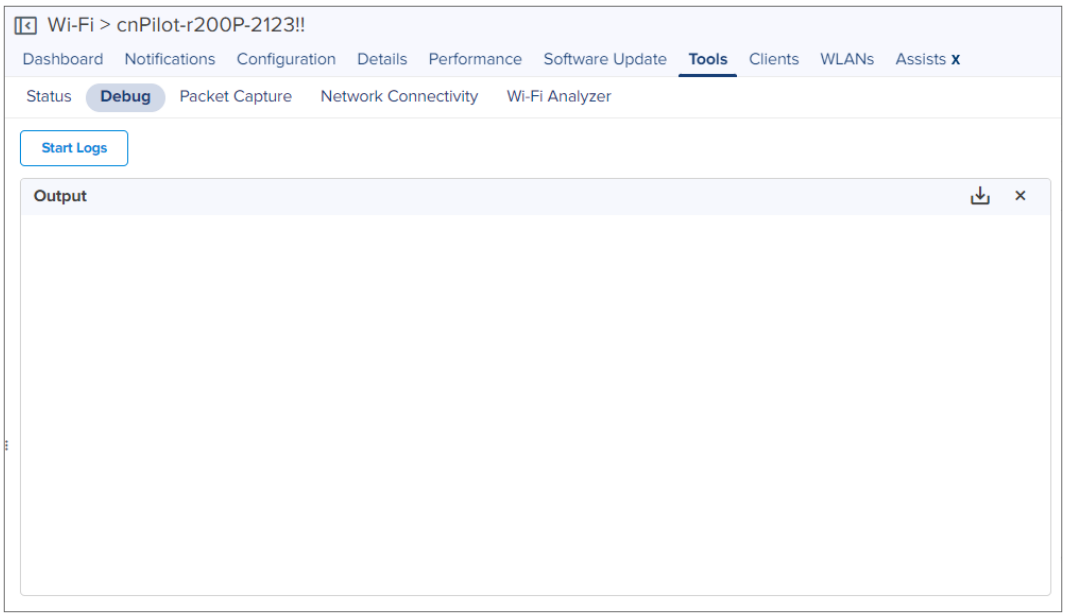


Figure 178 *cnPilot Debug Tools*

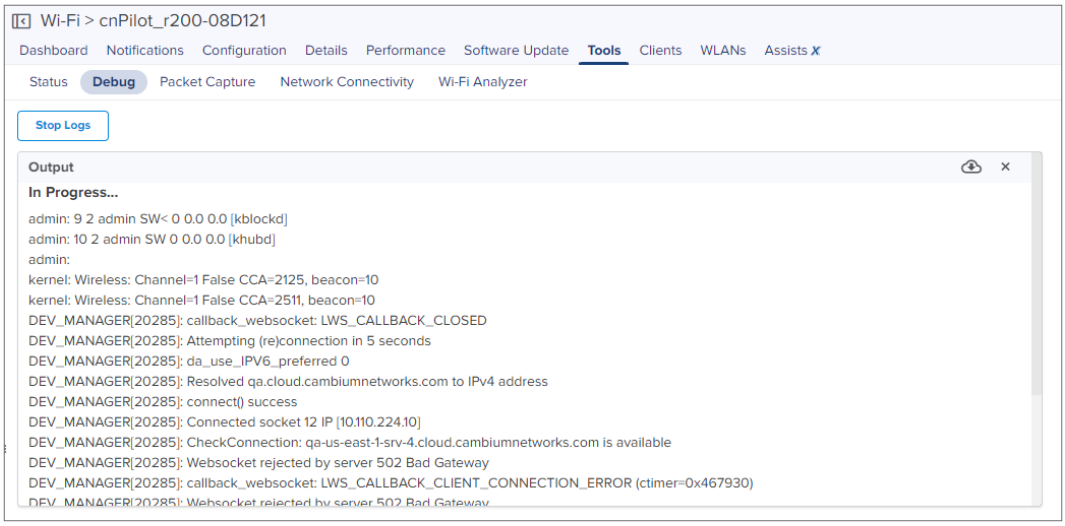


Figure 179 *cnPilot Tools Status*

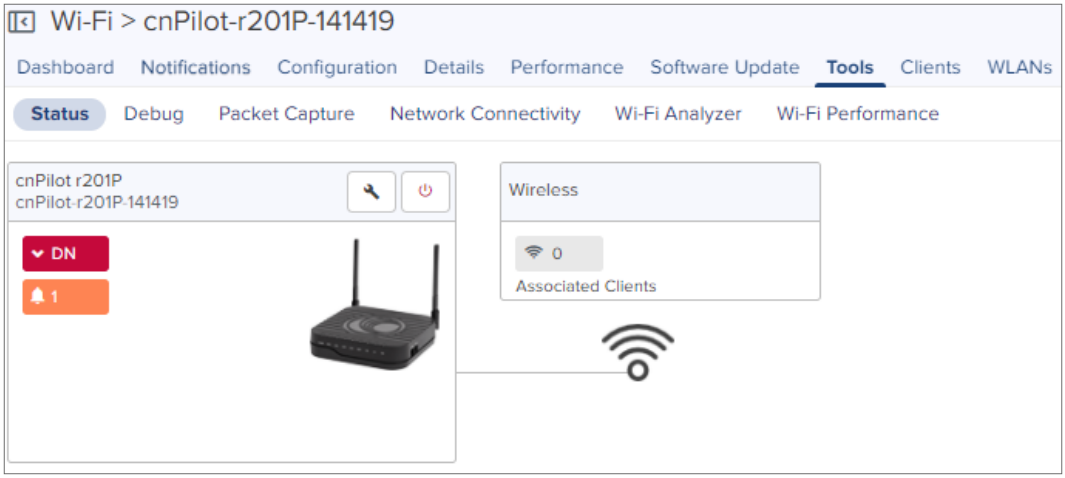


Figure 180 *cnPilot Tools > Packet Capture*

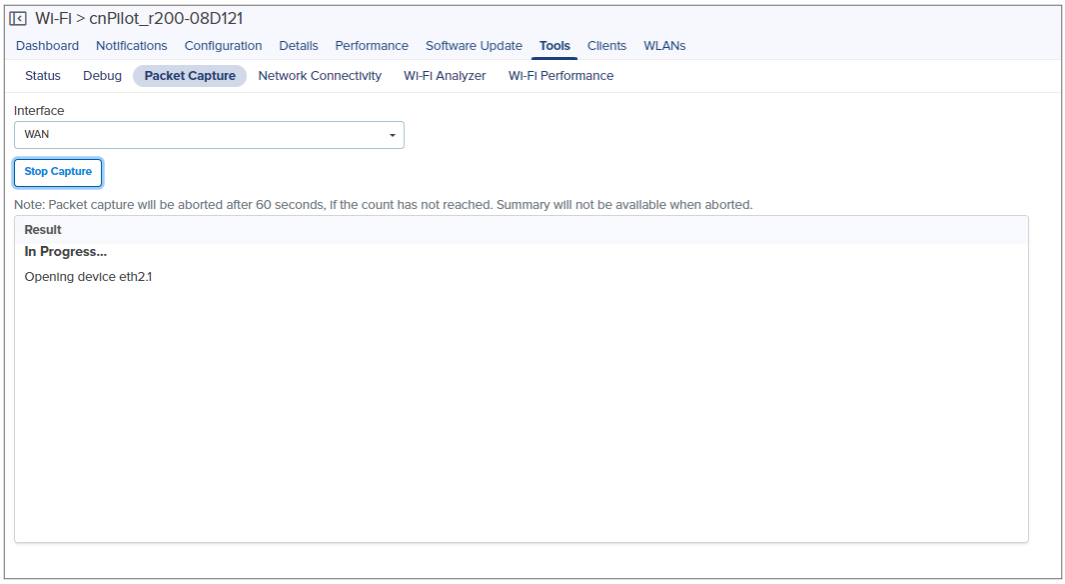


Figure 181 *cnPilot Tools > Network Connectivity*

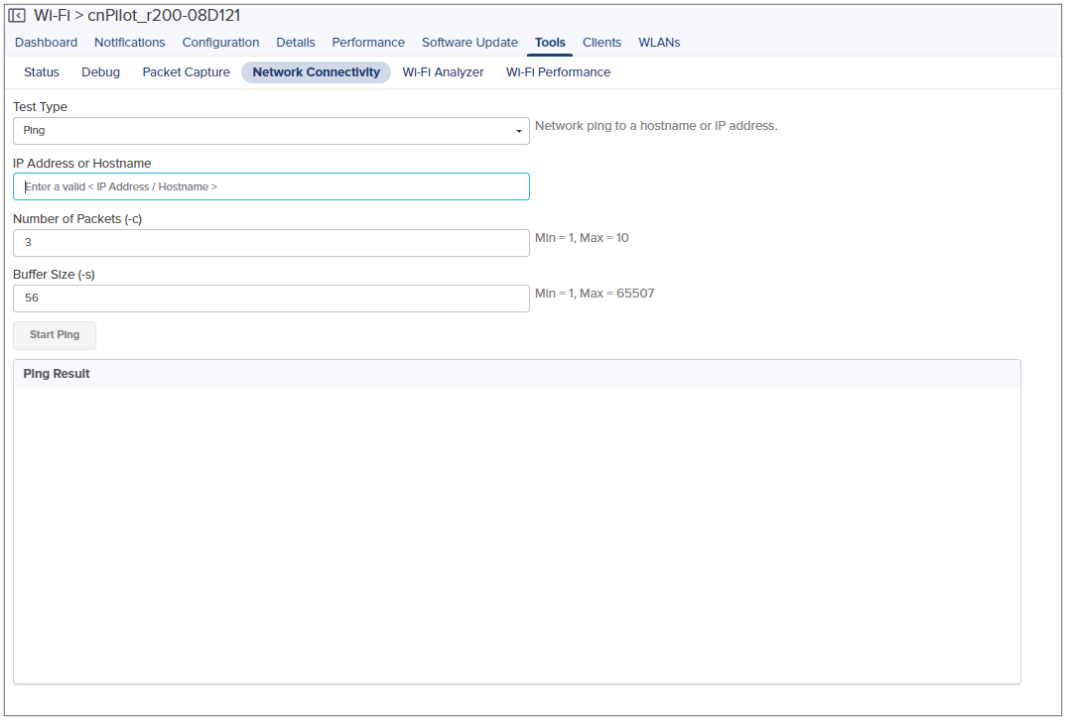
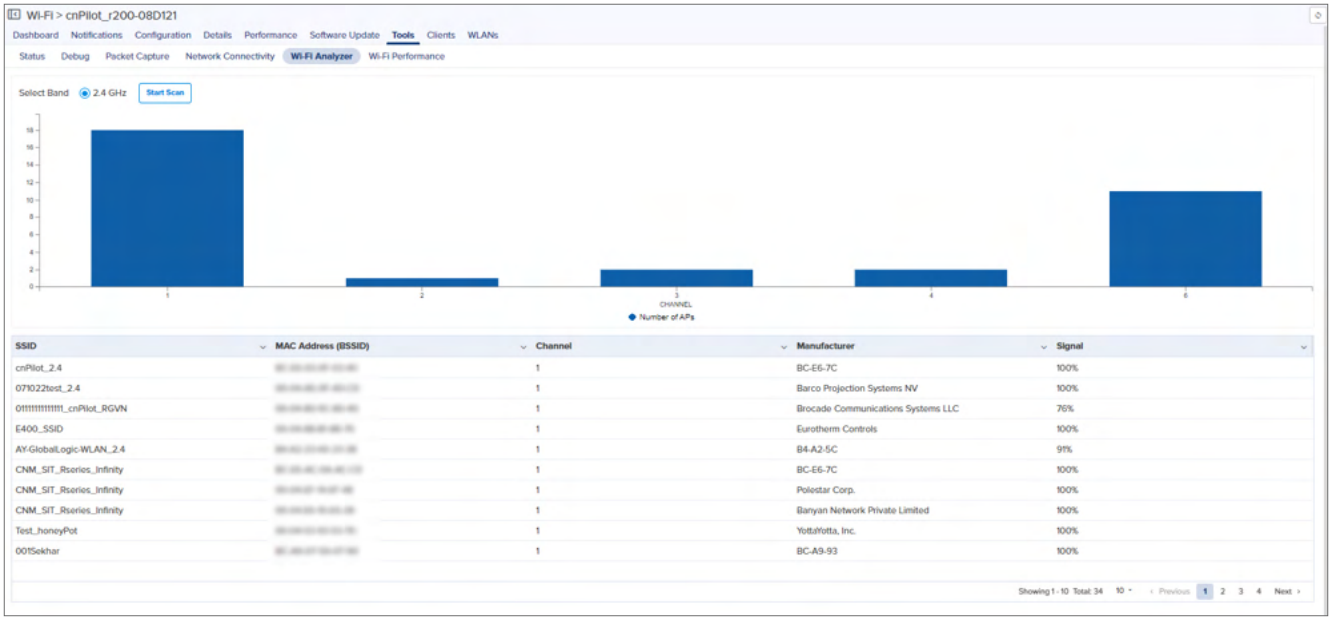


Figure 182 *cnPilot Tools > Network Connectivity*



cnRanger Tools



Note

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

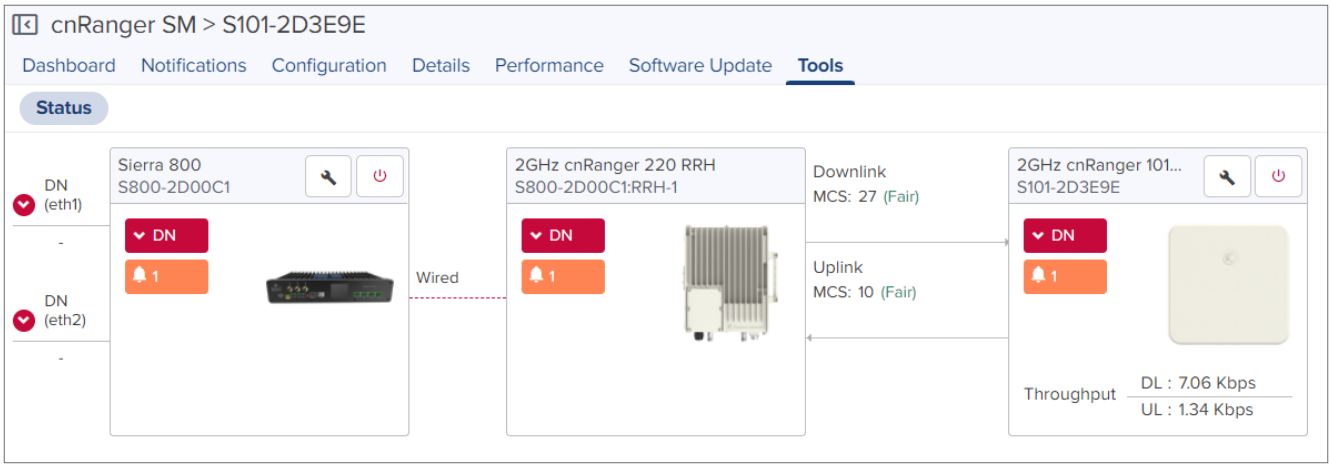
cnRanger BBU

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.



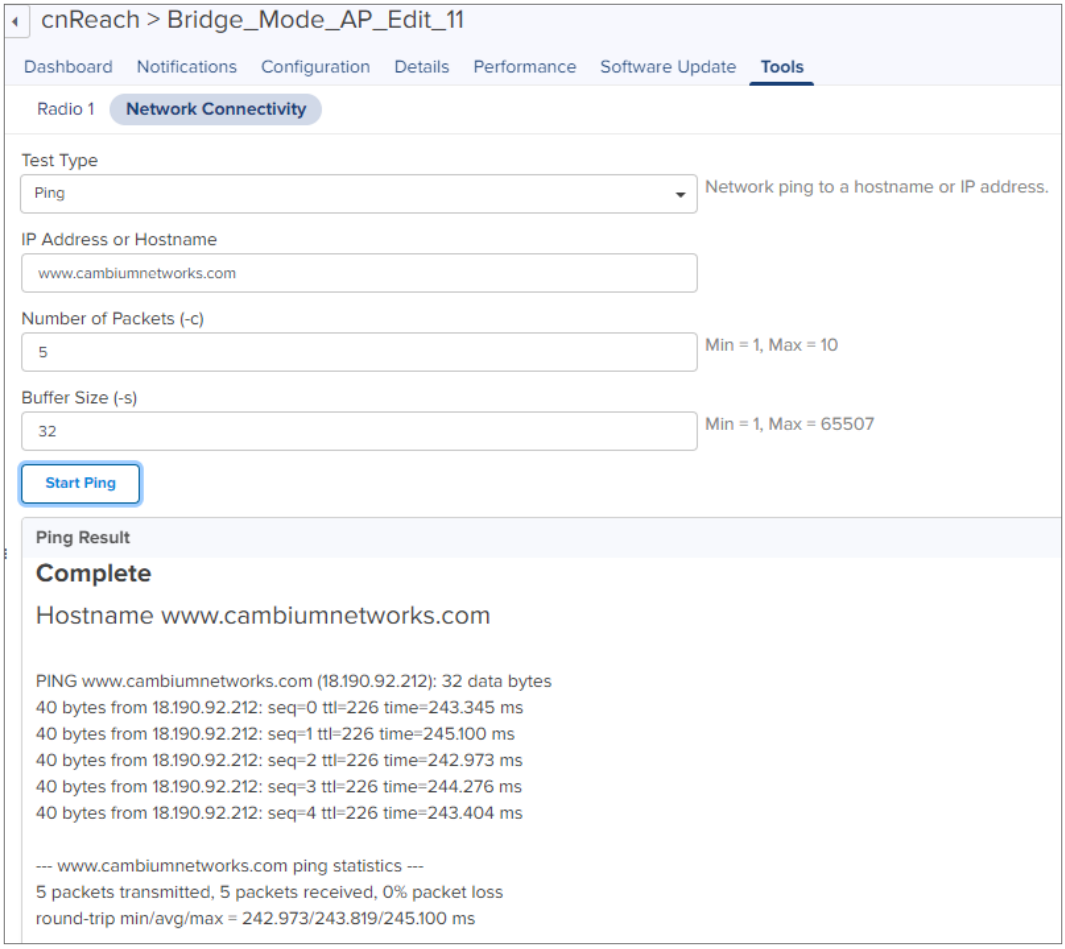
cnReach Tools

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

Table 30 *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 183 *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:

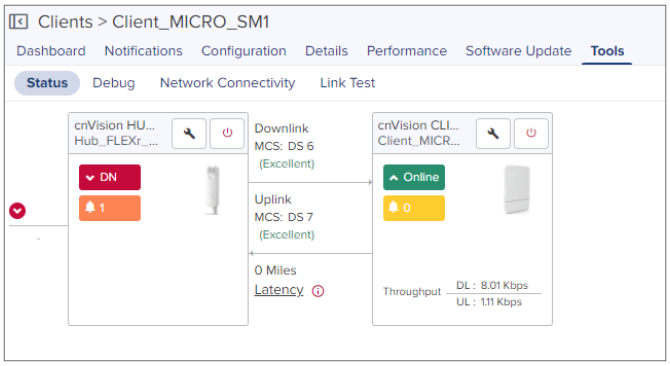
Table 31 *cnVision Tools*

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 31 *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 184 *cnVision Tools*



Edge Controller Tools

For details on Tools section, refer to Edge Controller User Guide.

Enterprise Wi-Fi Tools

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

Note

Both IPv4 and IPv6 addresses are supported for all the troubleshooting operations.

The operations of Enterprise Wi-Fi are listed below:

Table 32 *Enterprise Wi-Fi Tools*

Tools	Description
Debug	Displays the log details.
Flash LEDs (only Enterprise Wi-Fi devices)	Flash LED indicates that a device is ready to receive the signal.
Network Connectivity	Executes Ping, DNS, or Traceroute tests.
Packet Capture	Lists packet capture details. **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	Wi-Fi performance measures the backhaul speed across devices with respect to cnMaestro.

Figure 185 *Enterprise Wi-Fi Tools*

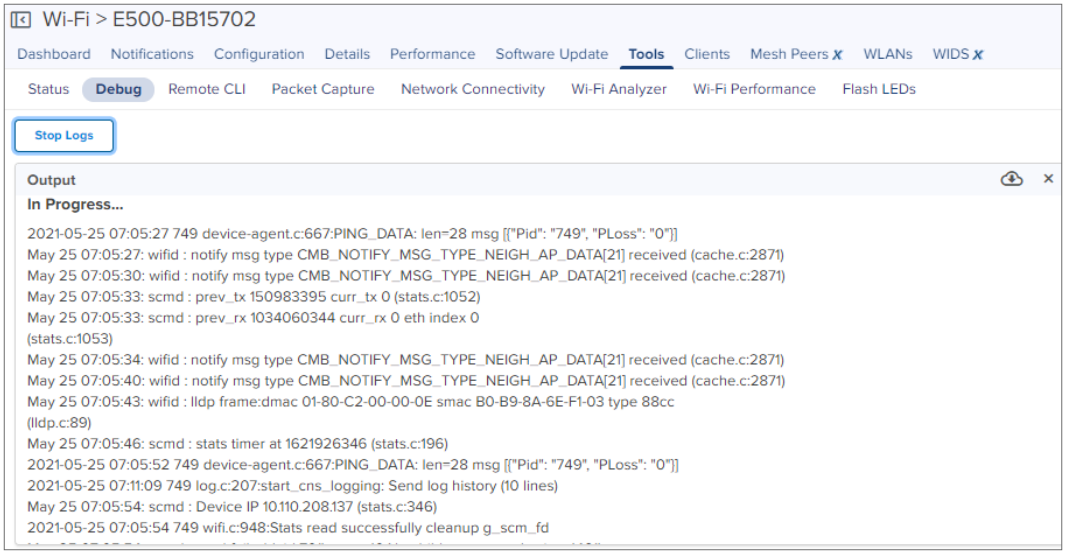


Figure 186 *Enterprise Wi-Fi Packet Capture*

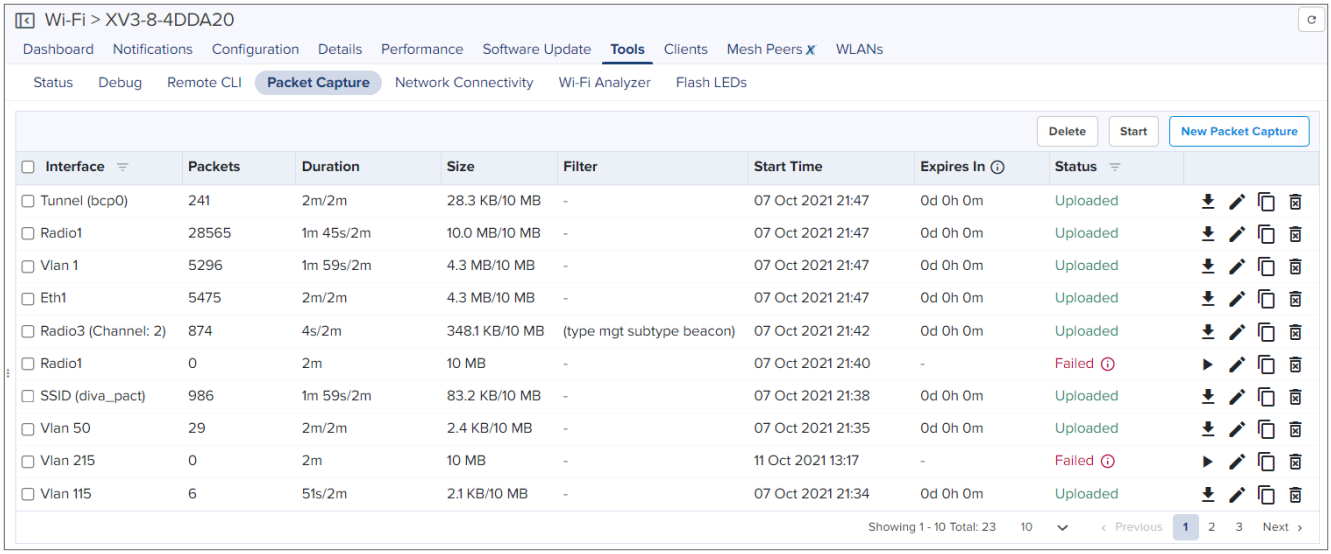


Figure 187 *Enterprise Wi-Fi Remote CLI Tools*

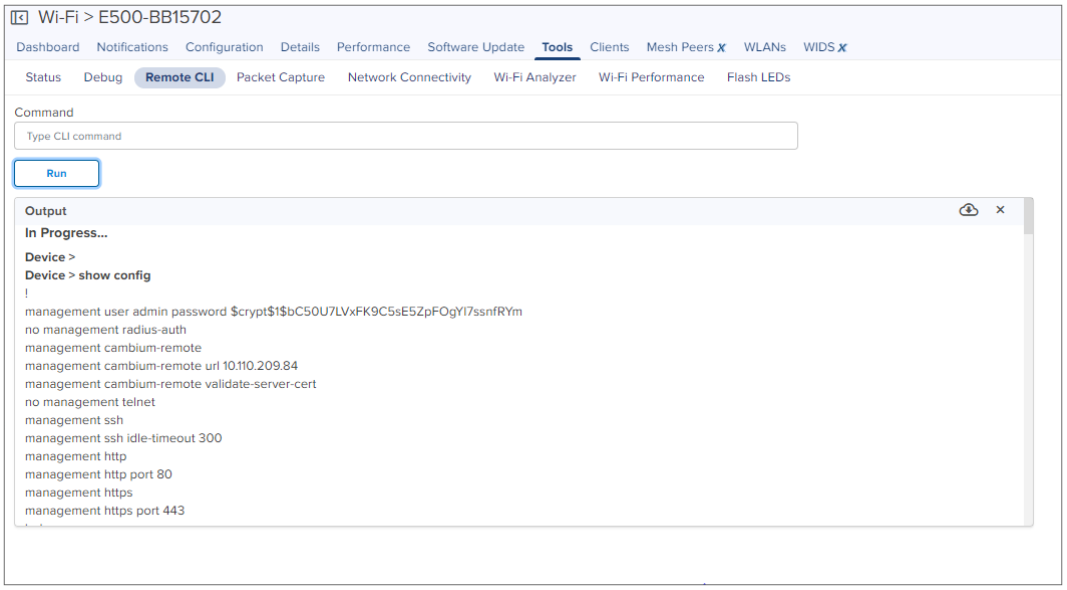
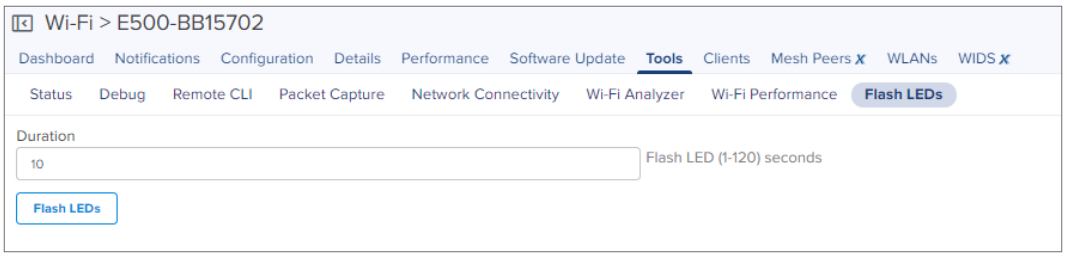


Figure 188 *Flash LEDs*

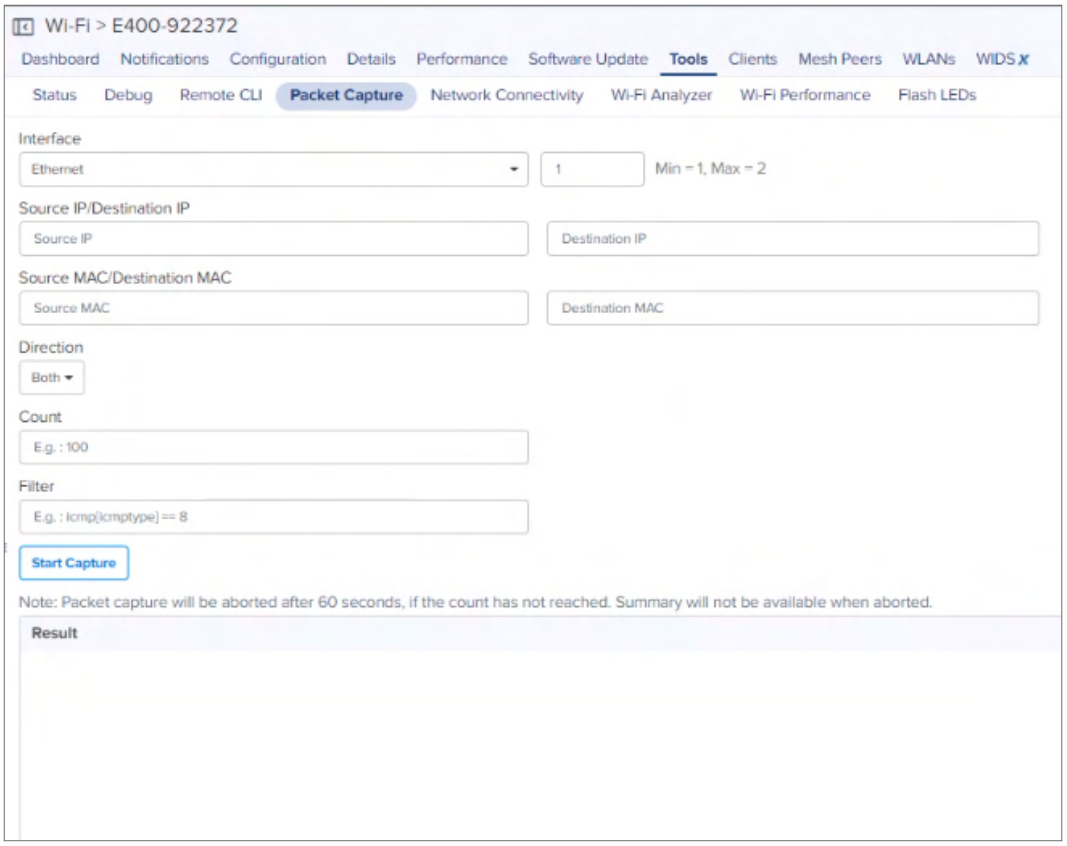


Packet Capture

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**.

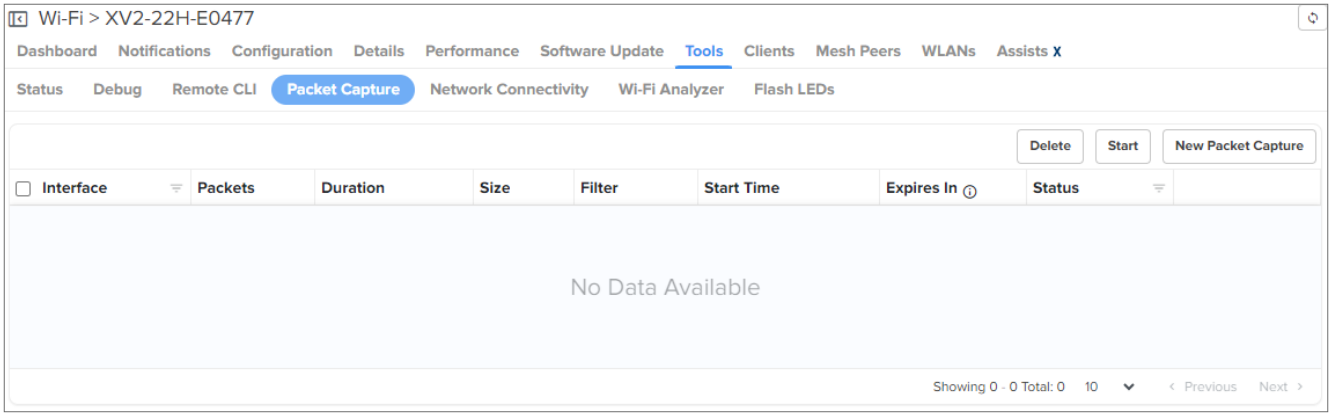


Table 33 *Packet Capture fields*

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

Table 33 *Packet Capture fields*

Field	Description
	• Ethernet • PPPoE • 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

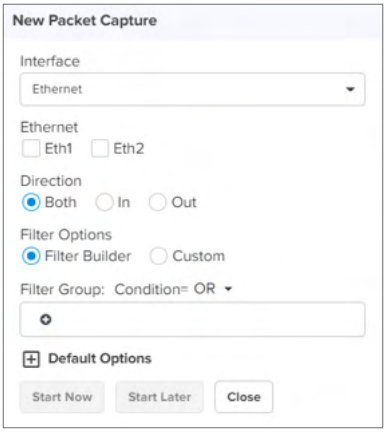
Configuring a new packet capture

Perform the following steps to start a new packet capture:

Note

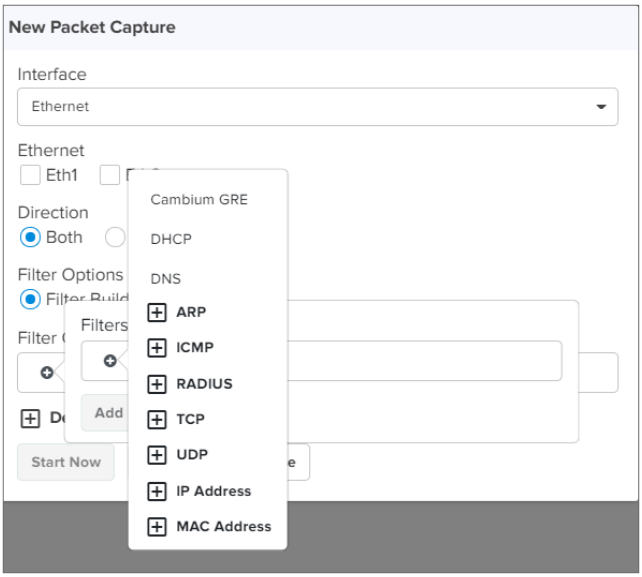
- Filter options vary for different interfaces (Radio, Wireless LAN, VLAN, SSID, TUNNEL, BRIDGE, and PPPoE. Radio, SSID has wireless 802.11 filters, other interfaces has wired 802.3 filters).
- User can also add custom filters if needed.
- Packet Capture on **Radio** interface is available only for online Enterprise Wi-Fi XV-Series and XE-Series.

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

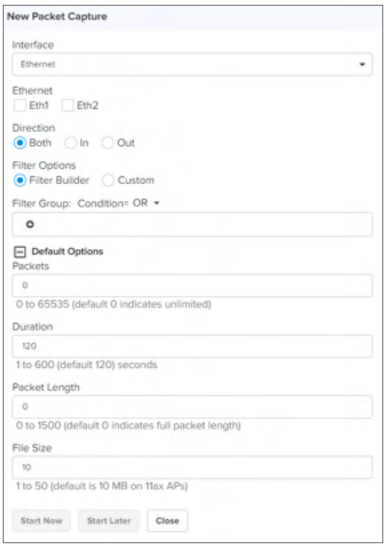


2. Select the **Interface** type from the dropdown.
3. Select **Ethernet** as **Eth1** or **Eth2**.
4. Choose the **Direction** as **Both**, **In**, or **Out**.
5. Select **Filter options** as **Filter Builder** or **Custom**.

   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**.



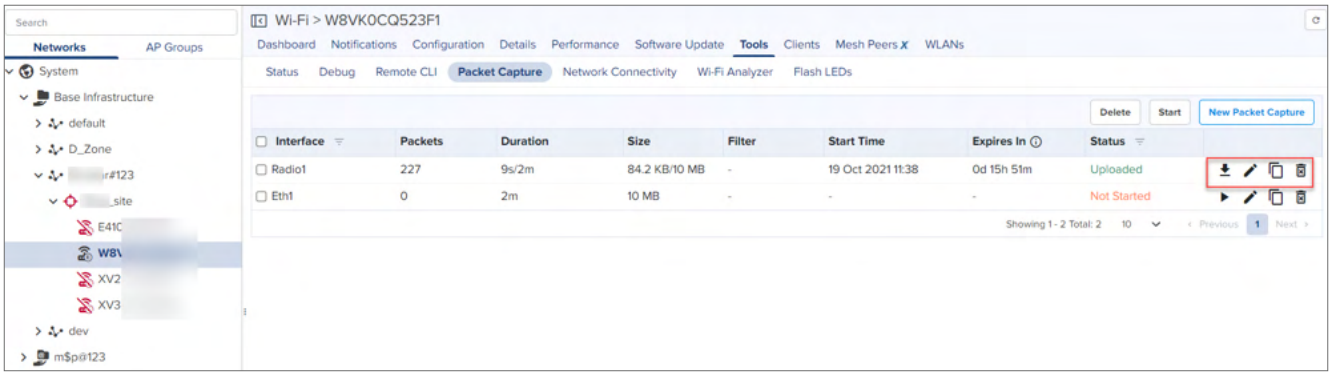
7. Click **Start Now** to capture the packets immediately, or start the capture later by selecting **Start Later** option. The progress of packets captured can be seen in the **Status** field.
8. Click the download (⬇) icon to download the capture in **PCAP** file format.



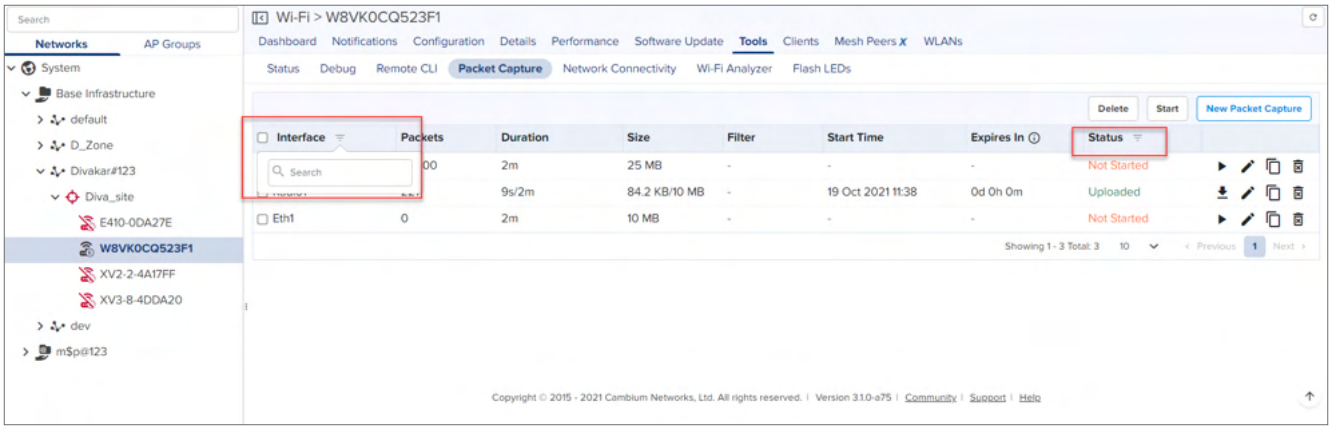
Note

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.



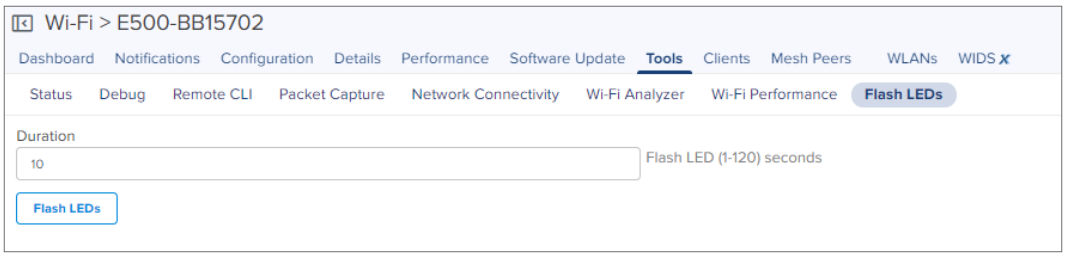
The user can search the packet capture by **Interface** type and **Status.**



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 189 *Flash LEDs*



ePMP Tools

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

Table 34 *ePMP Tools*

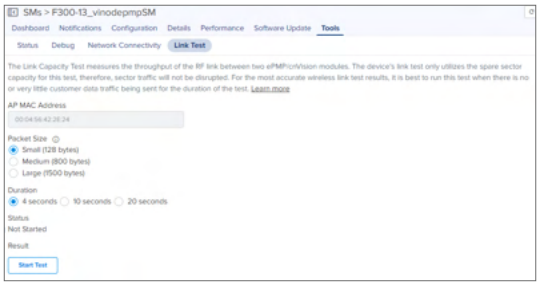
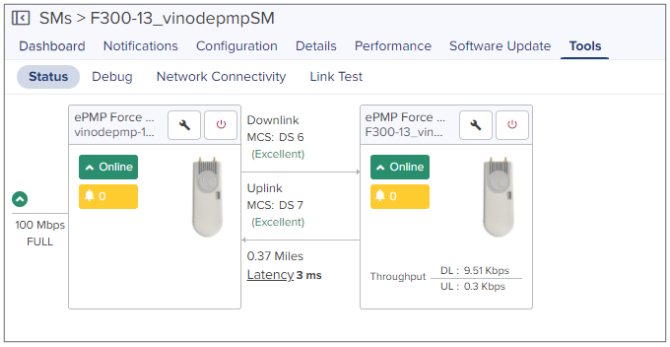
Field	Description
Debug	Displays the log details.
Link Test	The Link Capacity Test measures the throughput of the RF link between two ePMP modules. ePMP Link Test only utilizes the spare sector capacity for this test, therefore, sector traffic will not be disrupted. For the most accurate wireless link 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. ◦ **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.
Subscriber Modules	Displays the Subscriber Modules details.

Figure 190 *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 35 *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 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 191. **Figure 191** *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.

Table 35 *PMP Tools*

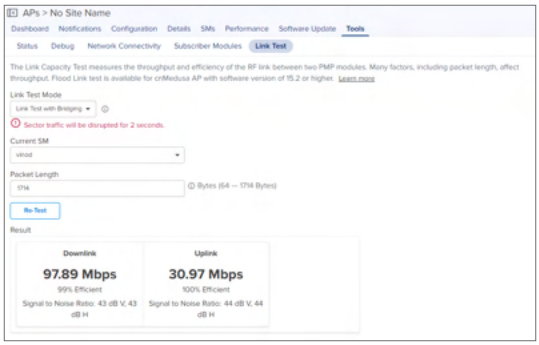
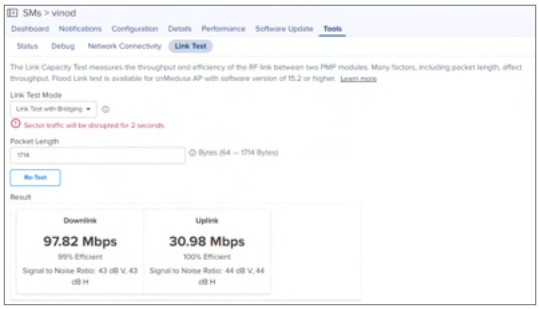
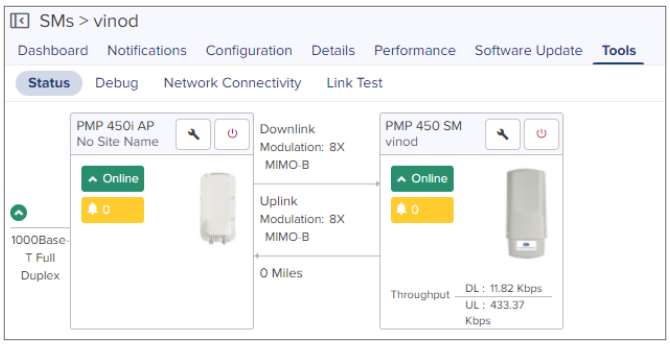
Field	Description
	• **Link Test with Bridging and MIR:** Bridges the traffic during test and also adheres to any MIR (Maximum Information Rate) settings for the link. • **Extrapolated Link Test**: Estimates the link capacity by sending few packets and measuring link quality. Displays the link related 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. 
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 192 *PMP Tools*

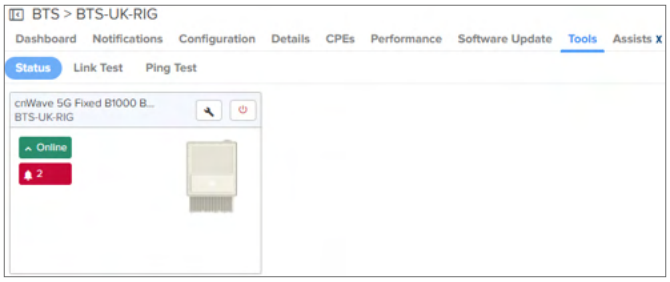


cnWave 5G Fixed Tools

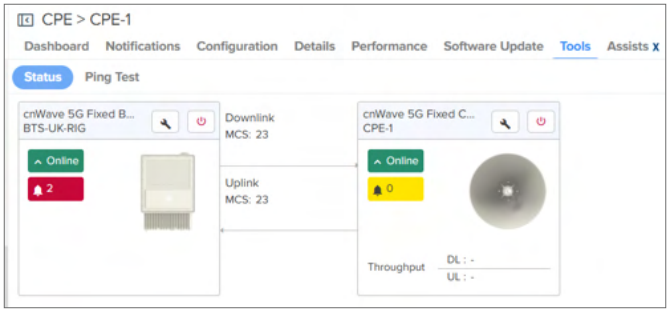
For cnWave 5G Fixed products (BTS and CPE), the **Tools** page in cnMaestro contains the following tabs:

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

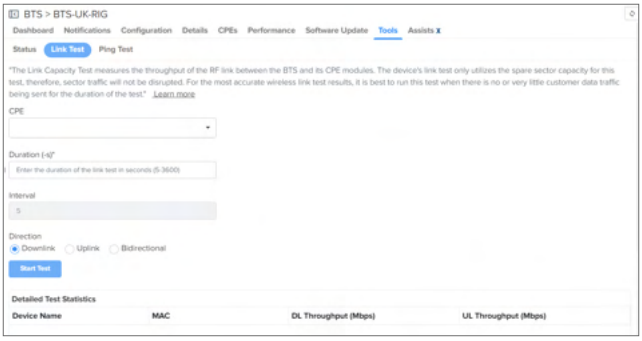
The **Link Test** tool is applicable only to the BTS device. The **Link Test** Page allows you to test the links (uplink, downlink, or both) and analyze the link performance for a CPE (s). The test output helps in managing the traffic and troubleshooting the links for the selected CPE (s).

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 36 *Parameters on the Link Test page*

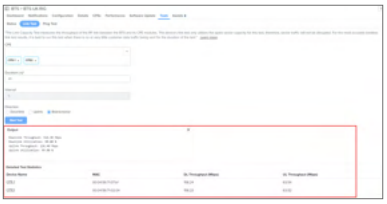
Parameter	Description
CPE	Name of the CPE device (s) for which you want to conduct the link capacity test. From the **CPE** dropdown list, select a CPE name or the required multiple CPE names. You can also search for the required CPE name or select all using this dropdown list.
Duration	Duration (in seconds) of the transmission of the traffic that you want to test. This parameter supports the value from 5 - 3600 seconds.
Interval	Time interval (in seconds) at which the test output is updated. This is a read-only parameter. Default value: 5 seconds **Note**: If you set a value between 5 and 60 seconds in the **Duration** field, the output is updated every 5 seconds. Similarly, if you set a value between 61 and 3600 seconds, the output is updated every 60 seconds.
Direction	Direction of the transmission of the traffic that you want to test. This parameter supports the following options: • 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.

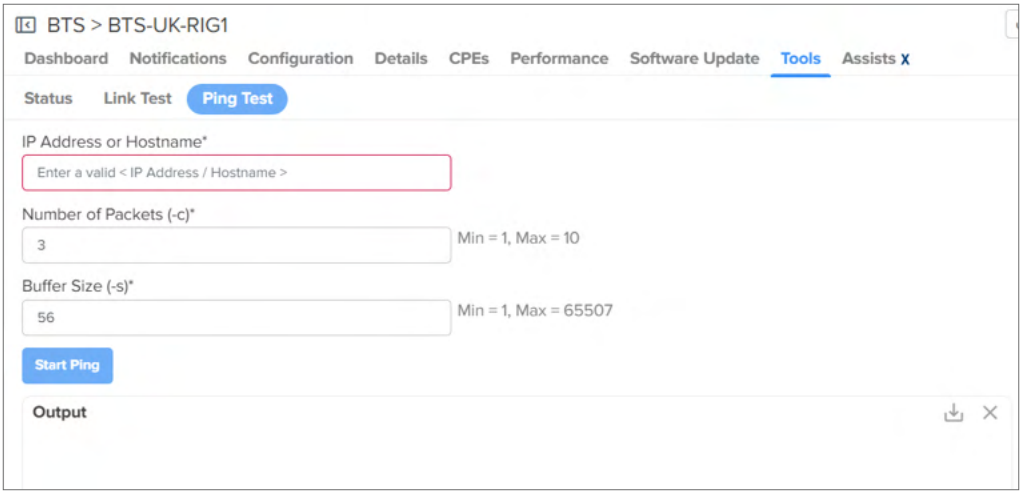
Ping Test

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 37 *Parameters on the Ping Test page*

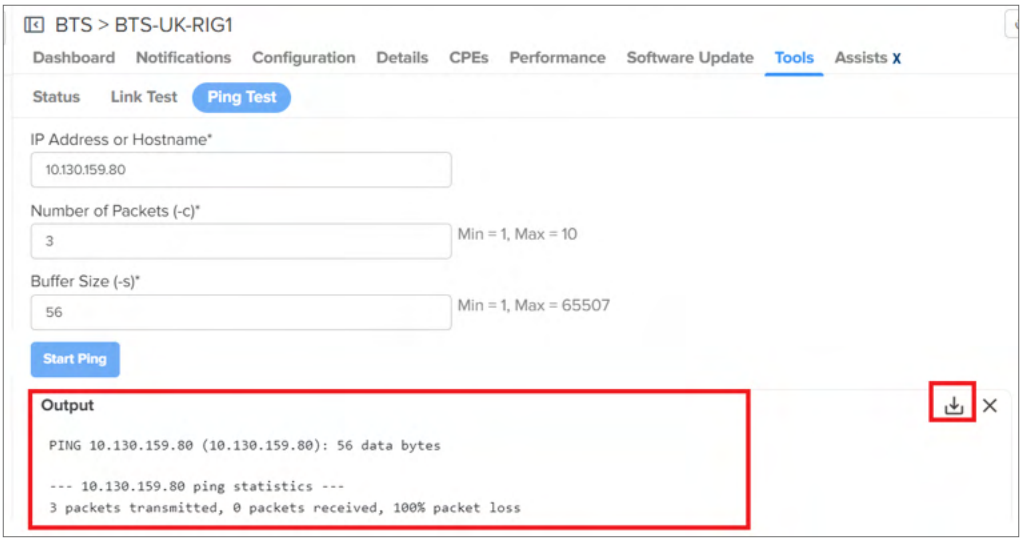
Parameter	Description
IP Address or Hostname	The valid IP address or a DNS name of the required network or destination. Type an appropriate value in the text box. This is a mandatory parameter.
Number of Packets (-c)	Number of ping packets that has to be sent to the network. Default value: 3 This parameter supports minimum one packet and maximum 10 packets. This is a mandatory parameter.
Buffer Size (-s)	Number of data bytes that have to be sent to the network.

Table 37 *Parameters on the Ping Test page*

Parameter	Description
	Default value: 56 data bytes, which are translated into 64 ICMP data bytes when combined with the 8 bytes of ICMP header data. This parameter supports a minimum of one data byte and maximum of 65507 data bytes. This is a mandatory parameter.

3. Click **Start Ping**.

   The **Output** section displays the test result, as shown below. You can click **Stop Ping** to stop the test.



Note

Similarly, you can run the ping test tool for CPE in the **Monitor and Manage** > **BTS network** > **CPE name** > **Tools** > **Ping Test** page.

4. Use the download icon in the Output section to download the test result.

RV22 Home Mesh Tools

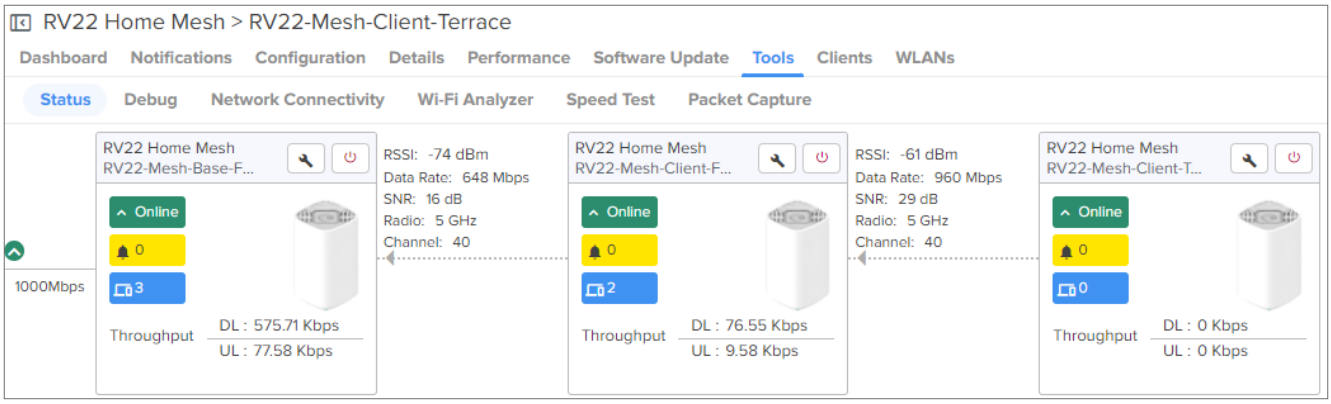
cnMaestro provides the following tools to troubleshoot and debug RV22 Home Mesh routers:

- Status
- Debug
- Network Connectivity
- Wi-Fi Analyzer
- Speed Test
- Packet Capture

To access these tools, navigate to **Monitor and Manage >** <RV22-router-name> **> Tools**.

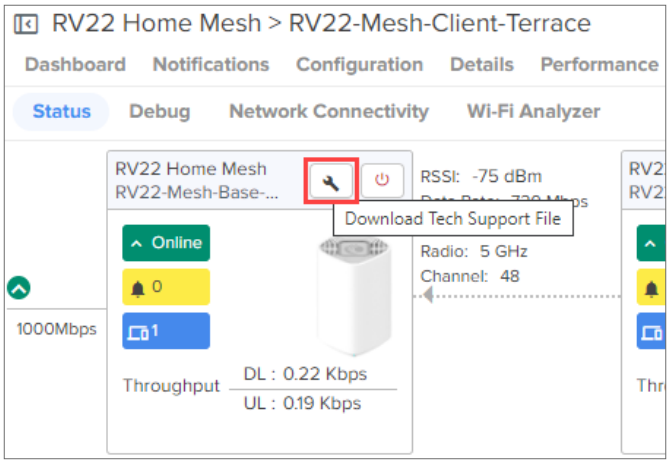
Status

To view the status of the link between the RV22 Home Mesh base and client routers, access the **Status** page under **Monitor and Manage >** <RV22-router-name> **> Tools.**



Downloading tech support file

To download the tech support file, on the **Status** page, click the **Download Tech Support File** ( ) icon.

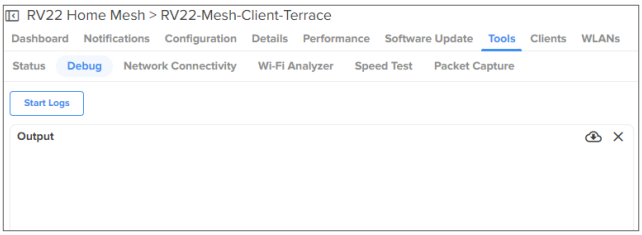


Debug

Displays log information of the RV22 Home Mesh router. To view the debug information:

1. Navigate to **Monitor and Manage >** <RV22-router-name> **> Tools** > **Debug**.
2. Click **Start Logs**.

   The log information is displayed in the **Output** window.



Network Connectivity

Provides network connectivity information of the RV22 Home Mesh routers.

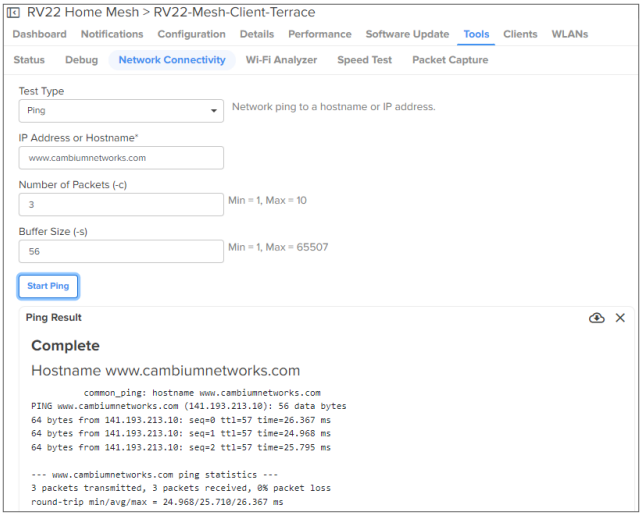
The following connectivity tests are available:

- Ping
- DNS Lookup
- Traceroute

To test network connectivity of the router:

1. Navigate to **Monitor and Manage >** <RV22-router-name> **> Tools** > **Network Connectivity**.
2. Select the test type and provide the corresponding parameters required for the test.
3. Click **Start Test**.

   cnMaestro initiates the test and displays the result in the **<Test Type> Result** window as shown below.



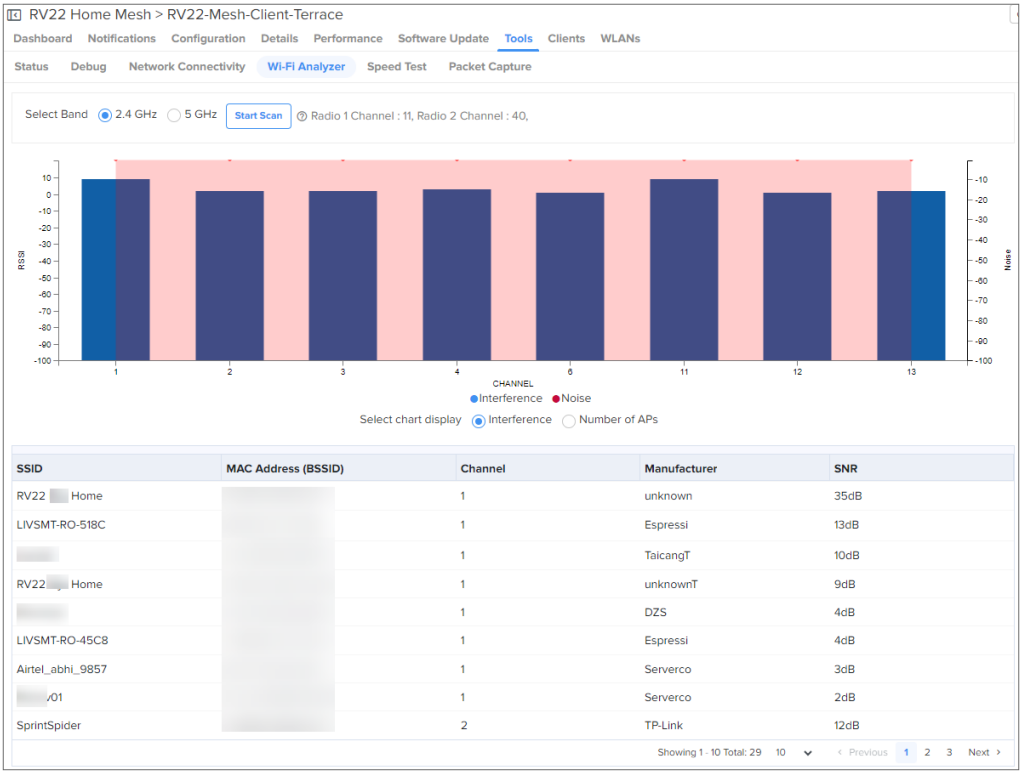
Wi-Fi Analyzer

Displays radio traffic and signal information for the selected band. It displays the interference and noise measured for the selected band.

To view the Wi-Fi Analyzer details:

1. Navigate to **Monitor and Manage >** <RV22-router-name> **> Tools** > **Wi-Fi Analyzer**.
2. Select the required band (2.4 or 5 GHz).
3. Click **Start Scan**.

cnMaestro analyzes the band and displays the result in table as shown below.



Speed Test

Displays the internet speed provided by the RV22 Home Mesh router.

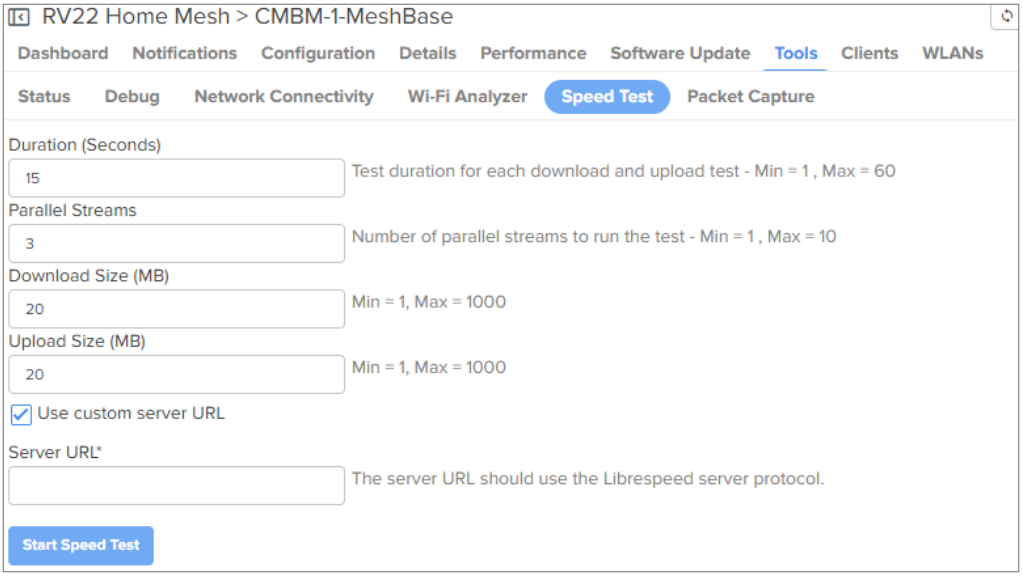
To know the speed of the router:

1. Navigate to **Monitor and Manage >** <RV22-router-name> **> Tools** > **Speed Test**.
2. Provide the details in the fields provided.
3. To use a custom server for testing, select the **Use custom server URL** checkbox and mention the URL in the **Server URL** parameter.

   The custom server URL must use the LibreSpeed server protocol.
4. Click **Start Speed Test**.

   cnMaestro checks the speed and displays both download and upload speeds in megabytes per second

(MBps).



Packet Capture

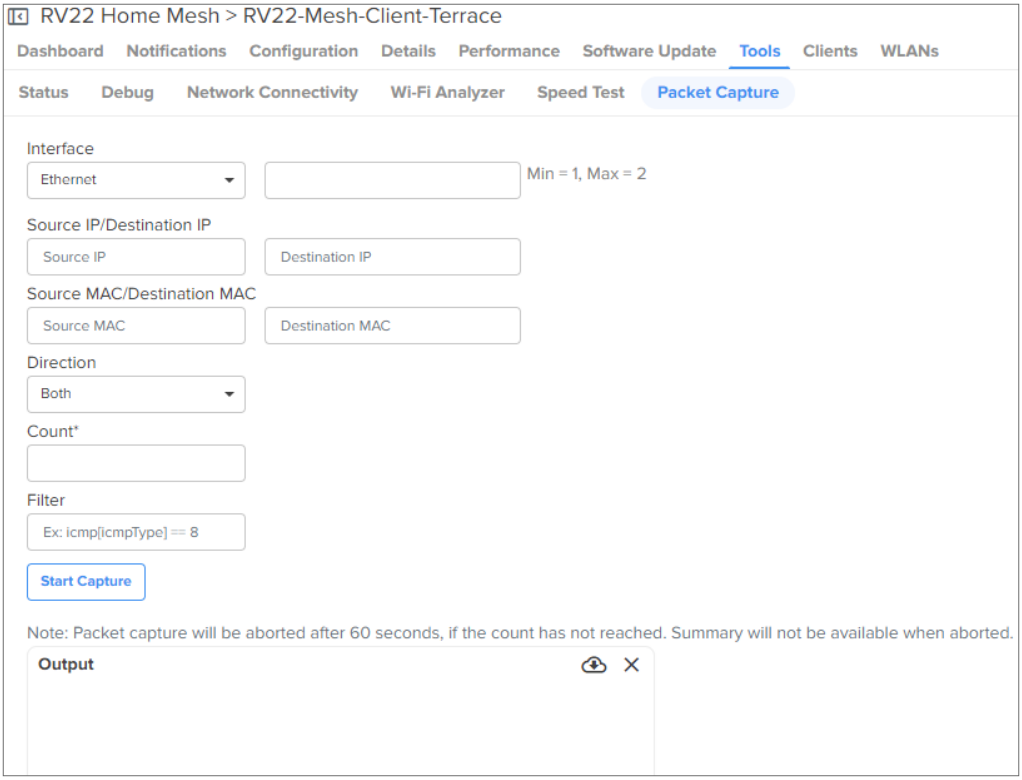
Packet Capture allows the user to capture all packets on a specified interface.

To capture packet data:

1. Navigate to **Monitor and Manage >** <RV22-router-name> **> Tools** > **Packet Capture**.
2. Select the required interface and provide the source and destination IP address or MAC address.
3. Provide the number of packets to be captured.
4. Click **Start Capture**.

   cnMaestro displays the information in the **Output** window.

5. To download the PCAP file, click the download ( ) icon.



Wireless Intrusion Detection System (WIDS)

Note

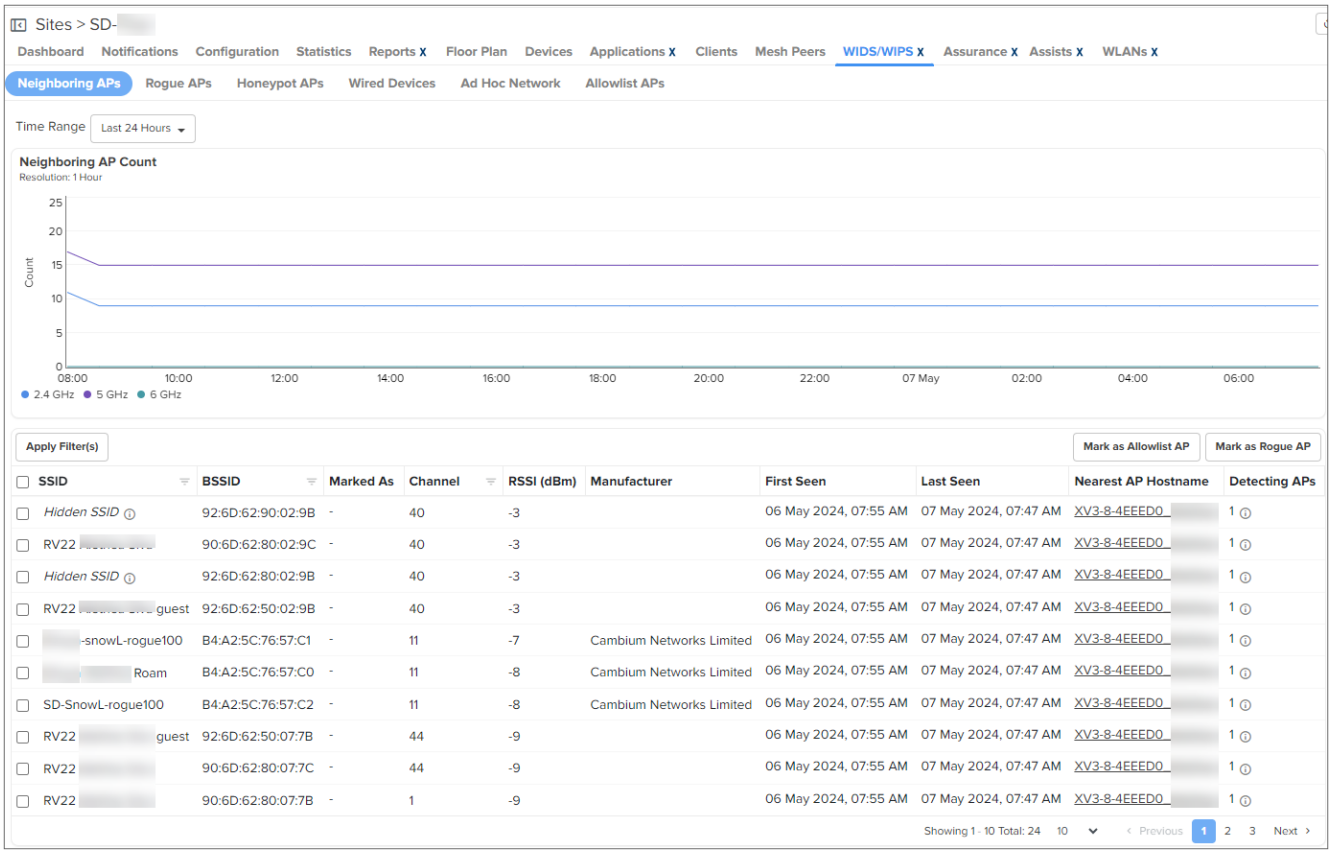
This is a beta feature.

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:

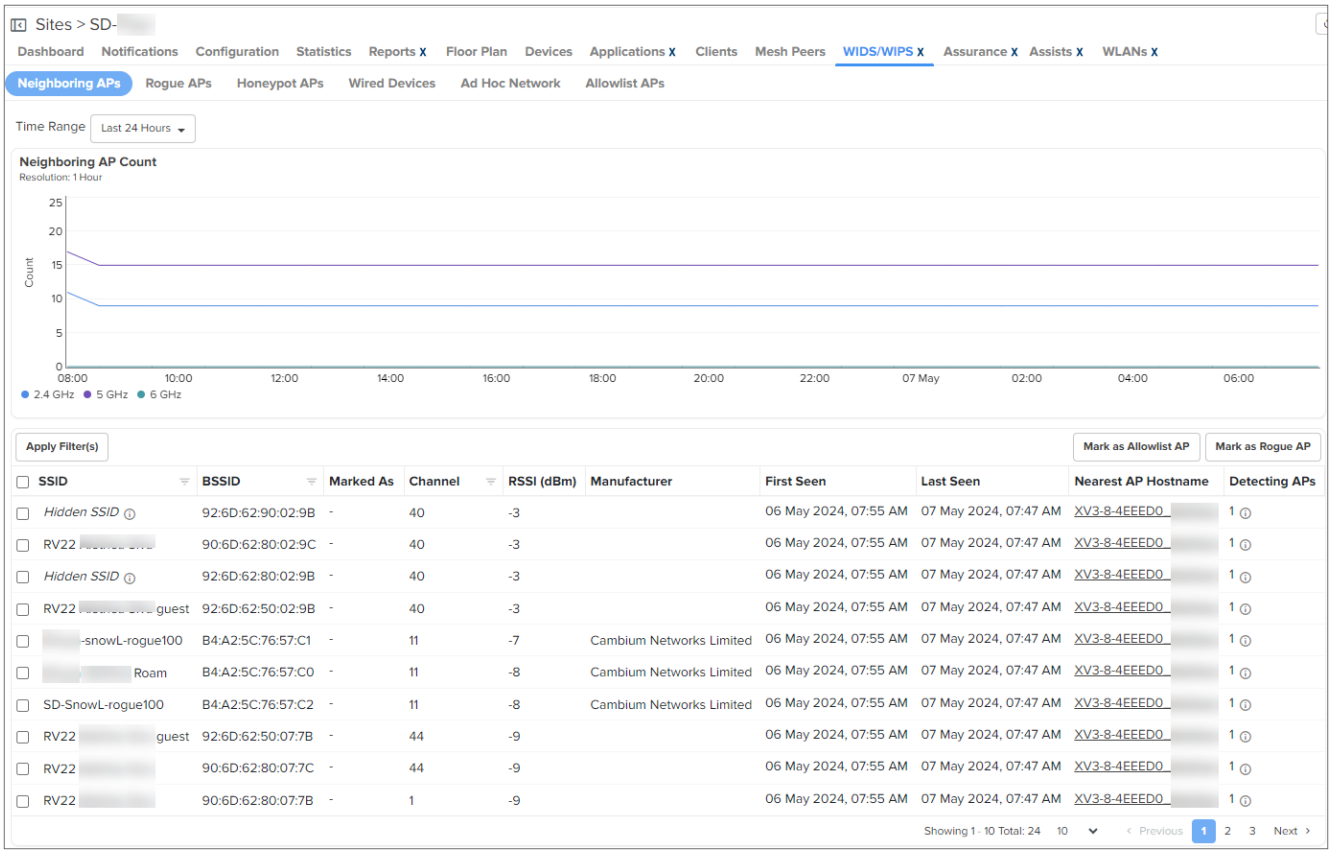
- Neighboring APs
- Rogue APs
- Honeypot APs
- Wired Devices
- Ad Hoc Network
- Allowlist APs

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.

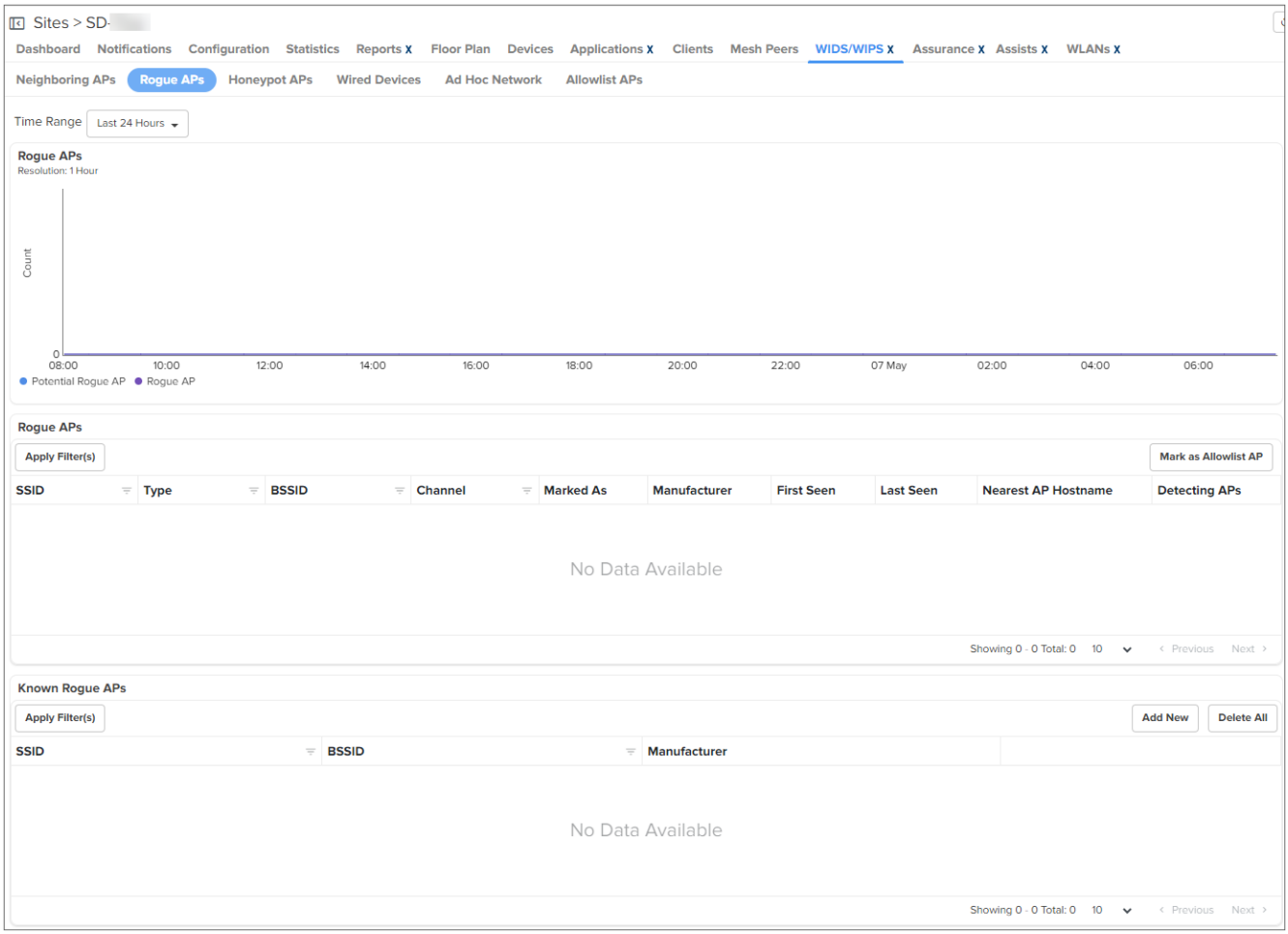
The following Neighboring APs parameters are displayed:

Table 38 *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 39 *Rogue APs parameters*

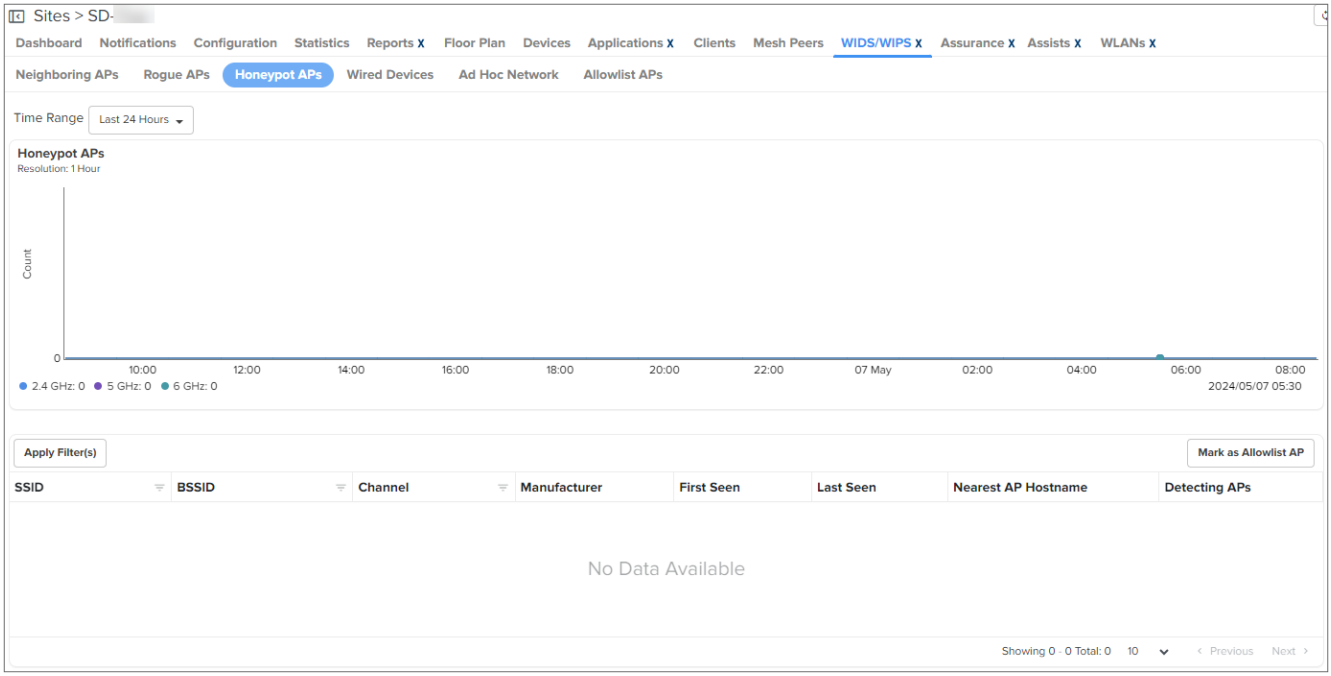
Field	Description
SSID	SSID of the rogue AP.
Type	Indicates the type of the rogue AP. Following are the supported values: • Rogue AP • Potential Rogue AP
BSSID	AP MAC address.
Channel	Channel in which the rogue AP operates.
Marked As	Indicates whether the rogue AP has been marked as an allowlist AP or 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 39 *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.



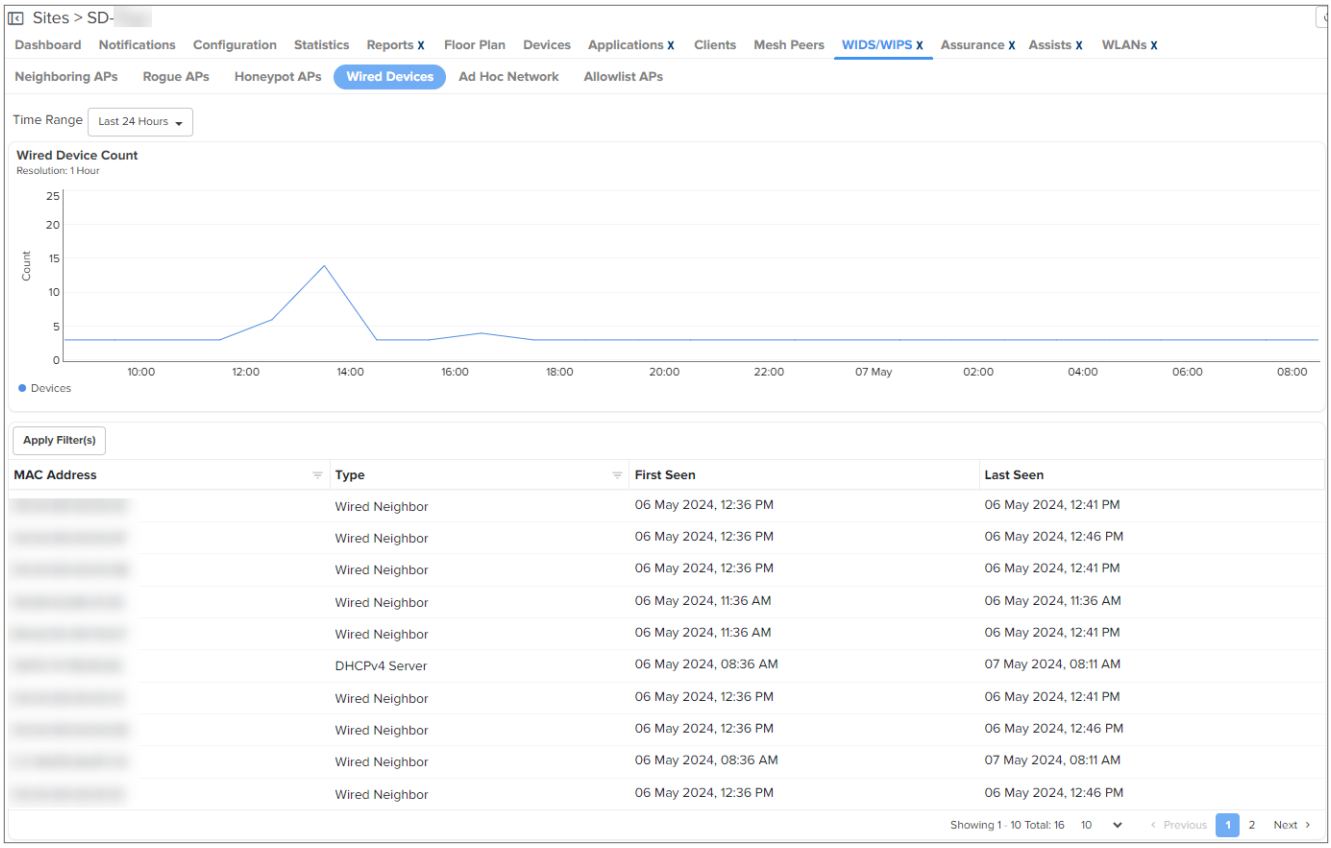
The following parameters related to Honeypot APs are displayed:

Table 40 *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.



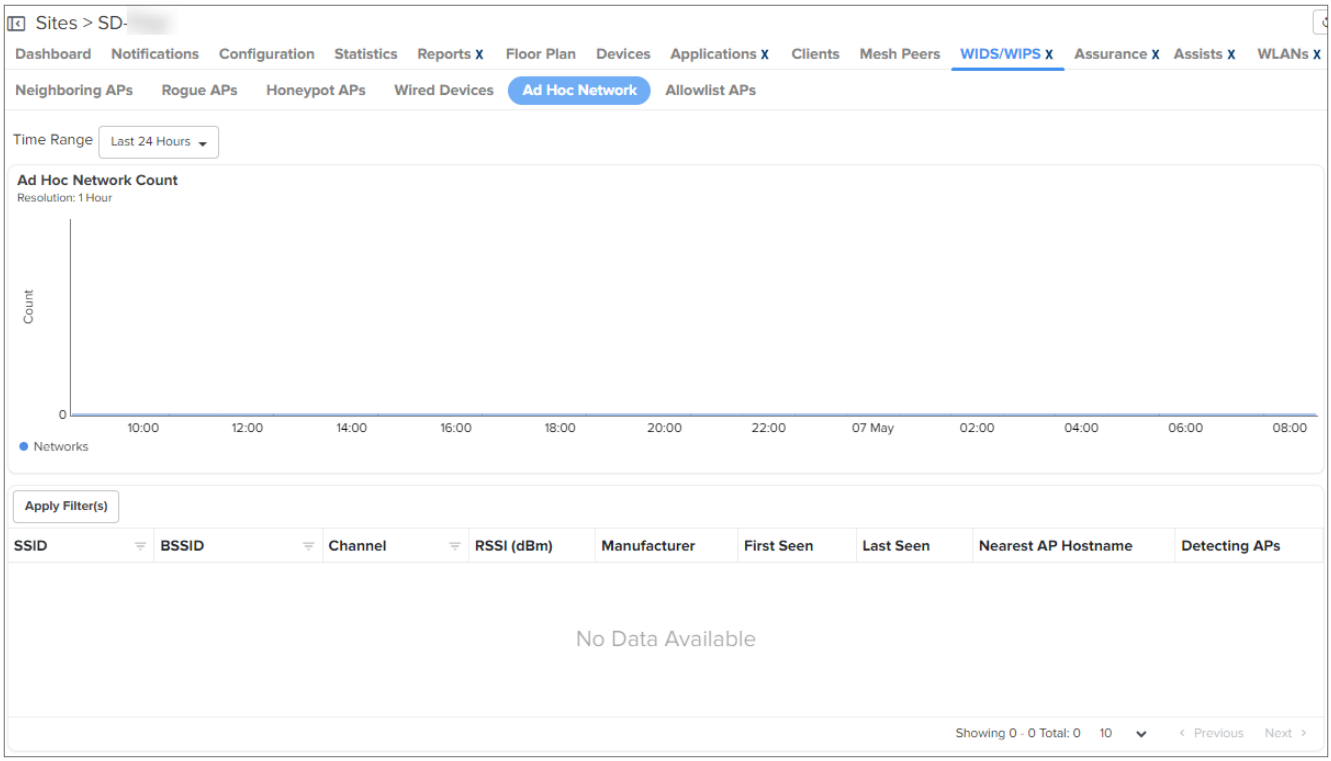
The following parameters related to Wired Devices are displayed:

Table 41 *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 42 *Ad Hoc Networks parameters*

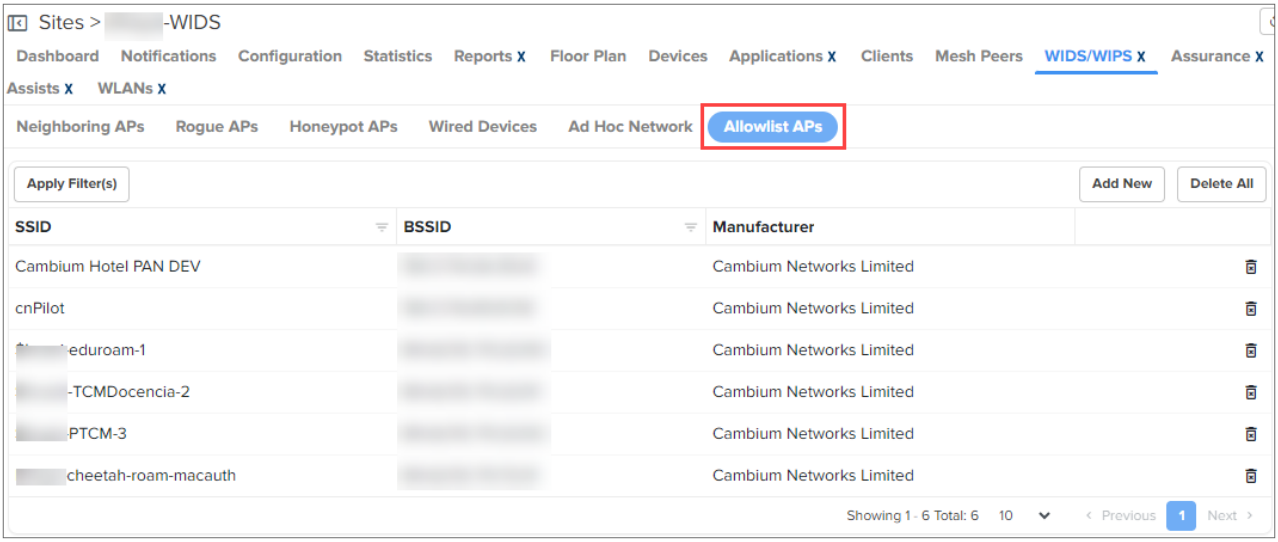
Field	Description
SSID	The name of the ad hoc wireless network.
BSSID	The MAC address of the ad hoc network.
Channel	The radio frequency channel on which the ad hoc network operates.
RSSI (dBm)	The received signal strength indication, measured in decibels relative to one milliwatt (dBm), of the ad hoc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

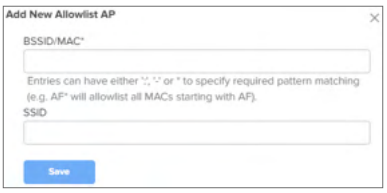
Allowlist APs allow administrators to configure the SSID and MAC addresses of authorized access points, providing control over permitted devices in the network infrastructure.

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 43 *Allowlist APs parameters*

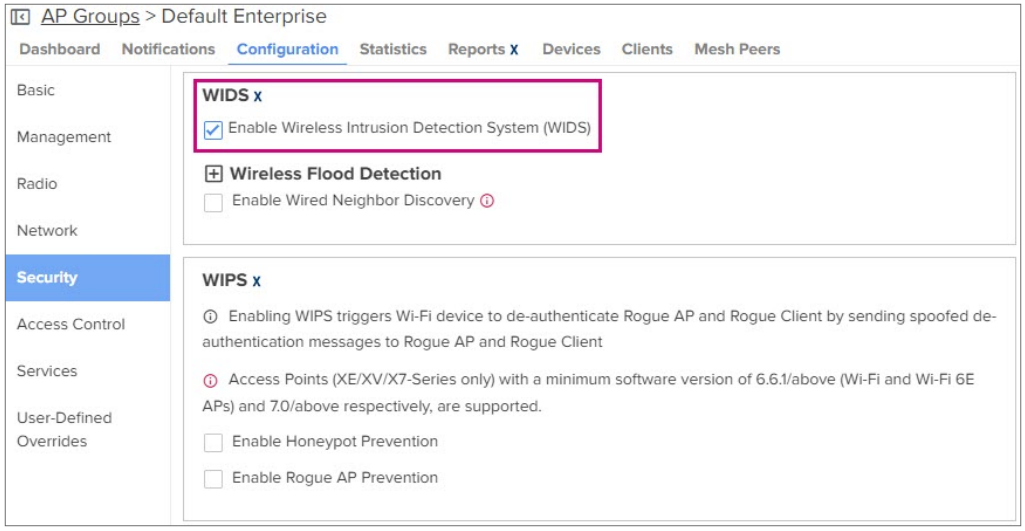
Field	Description
SSID	The name of the wireless network.
BSSID	The MAC address of the AP.
Manufacturer	The manufacturer of the AP.
Delete All	Allows to delete all Allowlist APs in the list.

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.

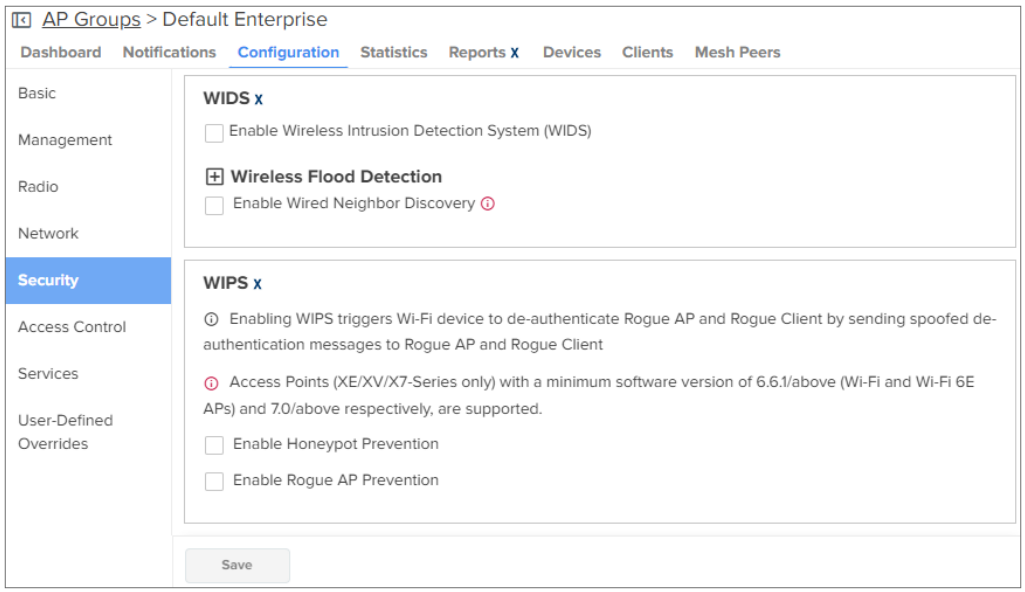
3. Select the **Enable Wireless Intrusion Detection System (WIDS)** checkbox.



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.



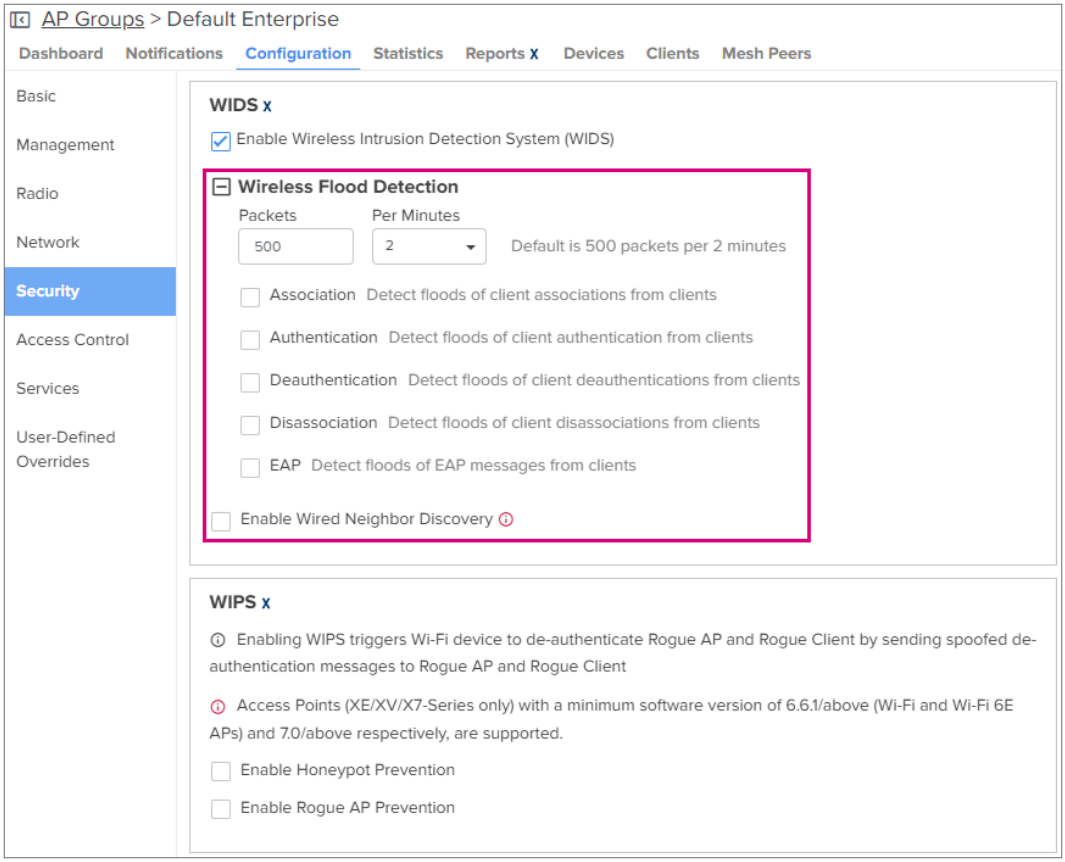
Wireless Flood Detection

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 44 *Wireless Flood Detection parameters*

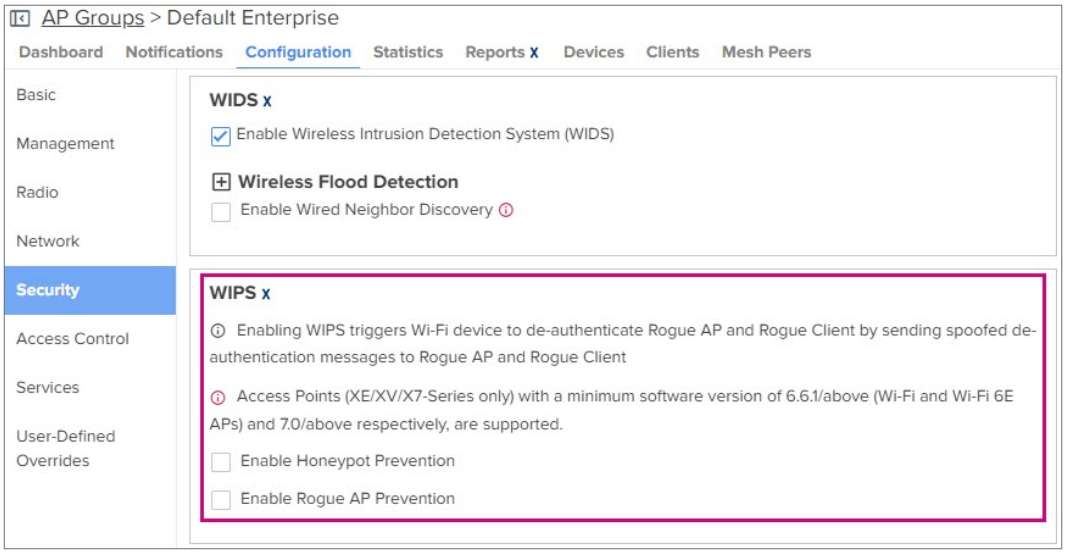
Field	Description
Association	Detect floods of client associations from clients.
Authentication	Detect floods of client authentication from clients.
Deauthentication	Detect floods of client deauthentications from clients.
Disassociation	Detect floods of client disassociations from clients.
EAP	Detect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



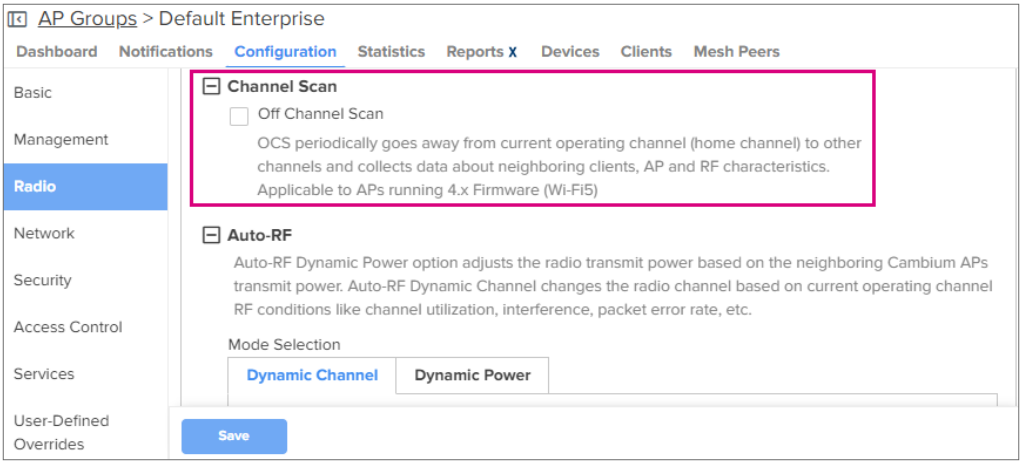
Off Channel Scan (OCS)

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**.

Network Service Edge (NSE)

Network Service Edge (NSE) delivers advanced security, routing and SD-WAN policies for small and medium enterprises. NSE is managed using the cloud-hosted cnMaestro (a management solution from Cambium Networks).

The NSE platform consists of the following devices:

- NSE3000

  NSE3000 is a cloud managed SD-WAN security gateway with multiple WANs, 2 x 1 Gbps SFP / RJ45 and 4 x 1 Gbps RJ45 ports, and offers reliable connectivity with WAN throughputs of up to 1 Gbps.

- NSE4000 (newly added platform)

  NSE4000 is a cloud managed SD-WAN security gateway with multiple WANs, 2 x 10 Gbps SFP+ and 8 x 2.5 Gbps RJ45 ports, and offers secure throughput of 3.2 Gbps and Layer-3 Firewall throughput of 10 Gbps.

This section describes the following tabs available in cnMaestro for NSE platforms:

- Dashboard
- Notifications
- Configuration
- Security
- Network
- Tools
- Clients
- Certificate

Dashboard

Dashboard widgets provides you a comprehensive overview of NSE device and network health. The dashboard displays **Details** of NSE device, **Total WAN Throughput**, number of **LAN Clients & VPN Sessions**, **Alarms**, **WAN Interface Metrics, Threats by Category**, **Threats by Location, Threats and Vulnerabilities** categorized as **Critical, Major** and **Minor**, **Port Status**, **Top Vulnerabilities**, **Top Vulnerable Clients**, **Top Active Alarms**, **WAN Throughput: Uplink and WAN Throughput: Downlink**, and **Clients and VPN Sessions**.

Figure 193 *The NSE dashboard page*



Notifications

Notifications consist of Alarms, Alarms History, and Events. They are synchronous messages that provide real-time system status.

Figure 194 *The Notifications page*

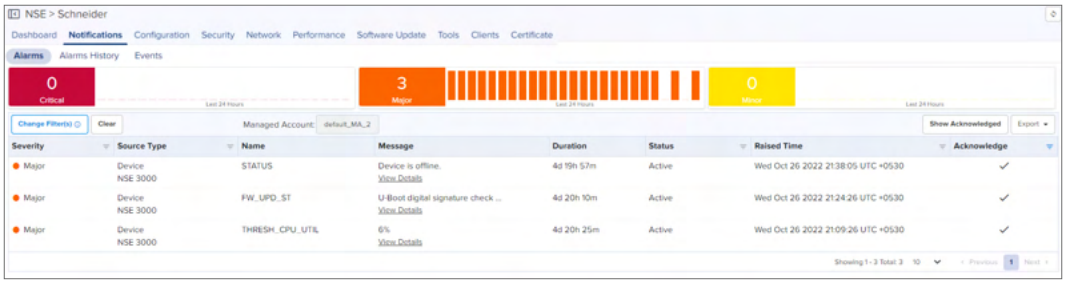


Table 45 *Notification overview*

Type	Description
Alarms	Alarms have a state and persist as long as the problematic activity continues; they reflect the current health of the devices in the network. The inactive alarms are removed from the alarms page after 10 minutes.
Alarms History	Expired Alarms are added to the Alarm History. The Alarm History displays historical active alarm counts. The history contains both the outstanding (active) and inactive alarms.
Events	Events are stateless, transient messages that occur in response to an input or action, such as if the CPU exceeds a threshold or a device association fails. Events are fire-and-forget; they are stored in an Event Table and provide a history of device activity.

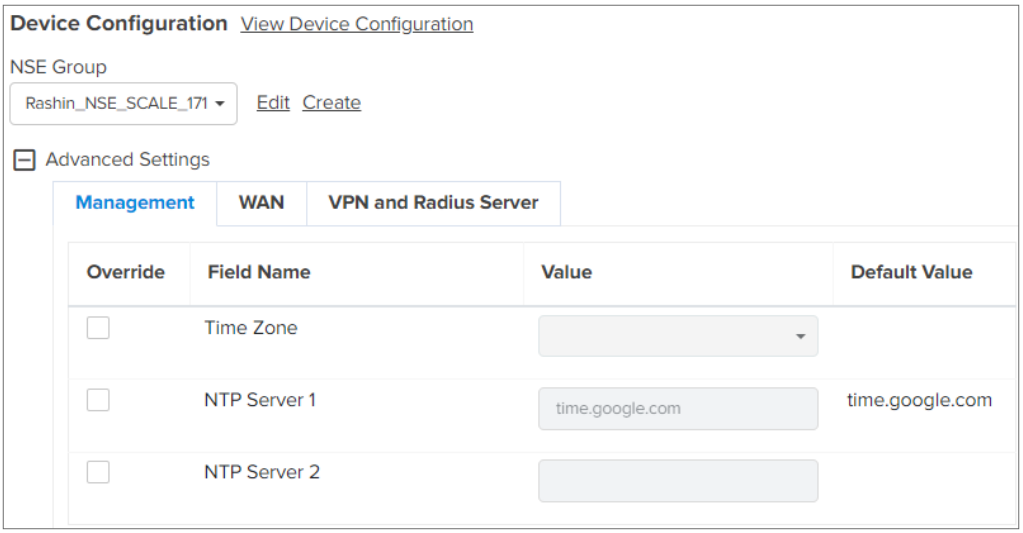
Configuration

The Configuration page allows you to configure the following for a device:

- Advanced Settings
- Factory Reset
- User-Defined Overrides
- Configuration Lock

To apply the Configuration Method, perform the following:

1. Navigate to the **Configuration** page.
2. In the **Device Configuration** section, select an NSE group from the **NSE Group** dropdown list.

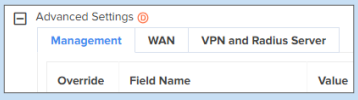


To view the jobs, click **View Configuration Jobs** or navigate to **Administration** > **Jobs** > **Configuration Update**.

Advanced Settings

Note

The **Advanced Settings** option is deprecated from cnMaestro release version 5.1.1 onwards. This option will be completely removed from the UI in future releases.



In the **Advanced Settings** you can configure the following tabs:

- Management
- WAN
- VPN and Radius Server

Management

1. In the **Management** tab, select the **Field Name** to override the settings.



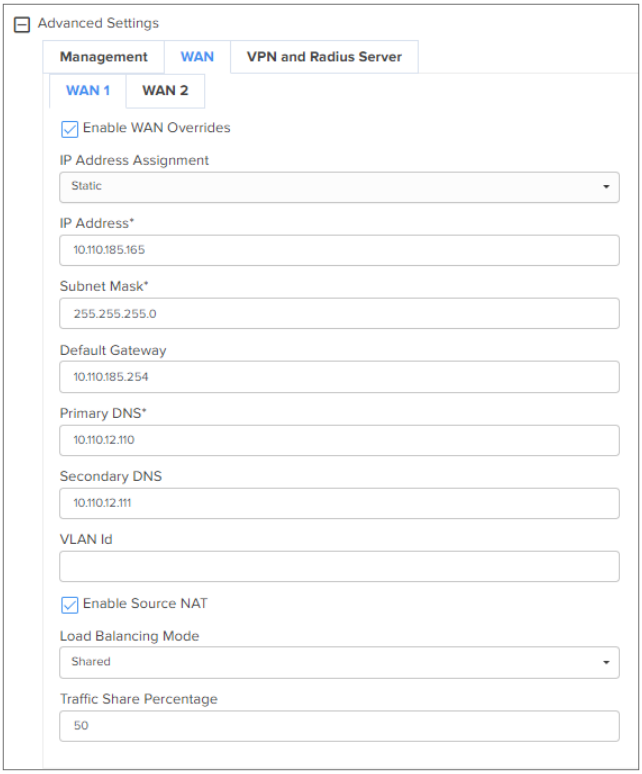
2. Click **Apply Configuration**.

WAN

In the **WAN**, you can override settings for **WAN 1** and **WAN 2.**

WAN 1

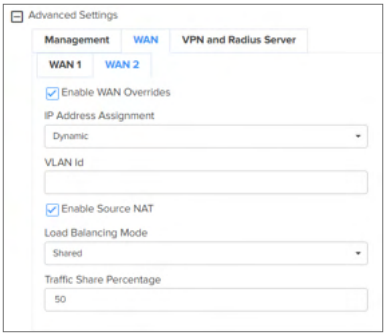
1. Select **Enable WAN Overrides** option.



2. Select the fields to override.
3. Click **Apply Configuration**.

WAN 2

1. Select **Enable WAN Overrides** option.

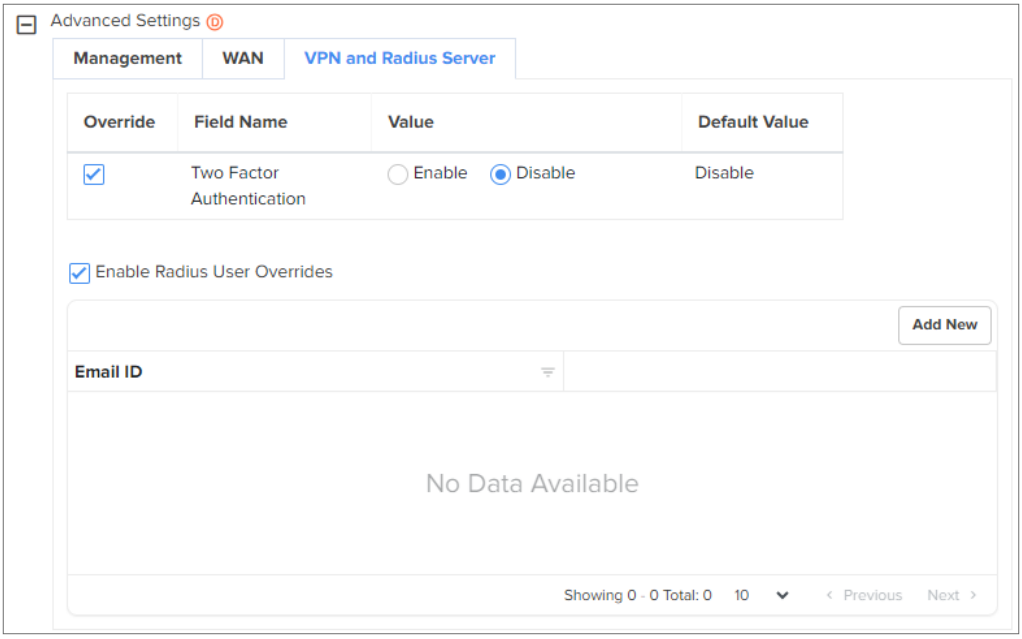


2. Select the fields to override.
3. Click **Apply Configuration**.

VPN and Radius Server

In the **VPN and Radius Server** tab you can override the Two Factor Authentication and RADIUS User settings.

1. To enable two factor authentication, first select the **Two Factor Authentication** checkbox.



2. Select the **Enable** or **Disable** option.
3. To add RADIUS users, select the **Enable Radius User Overrides** checkbox.
4. To add a new RADIUS user, click **Add New**.

   The Add Radius user window is displayed.

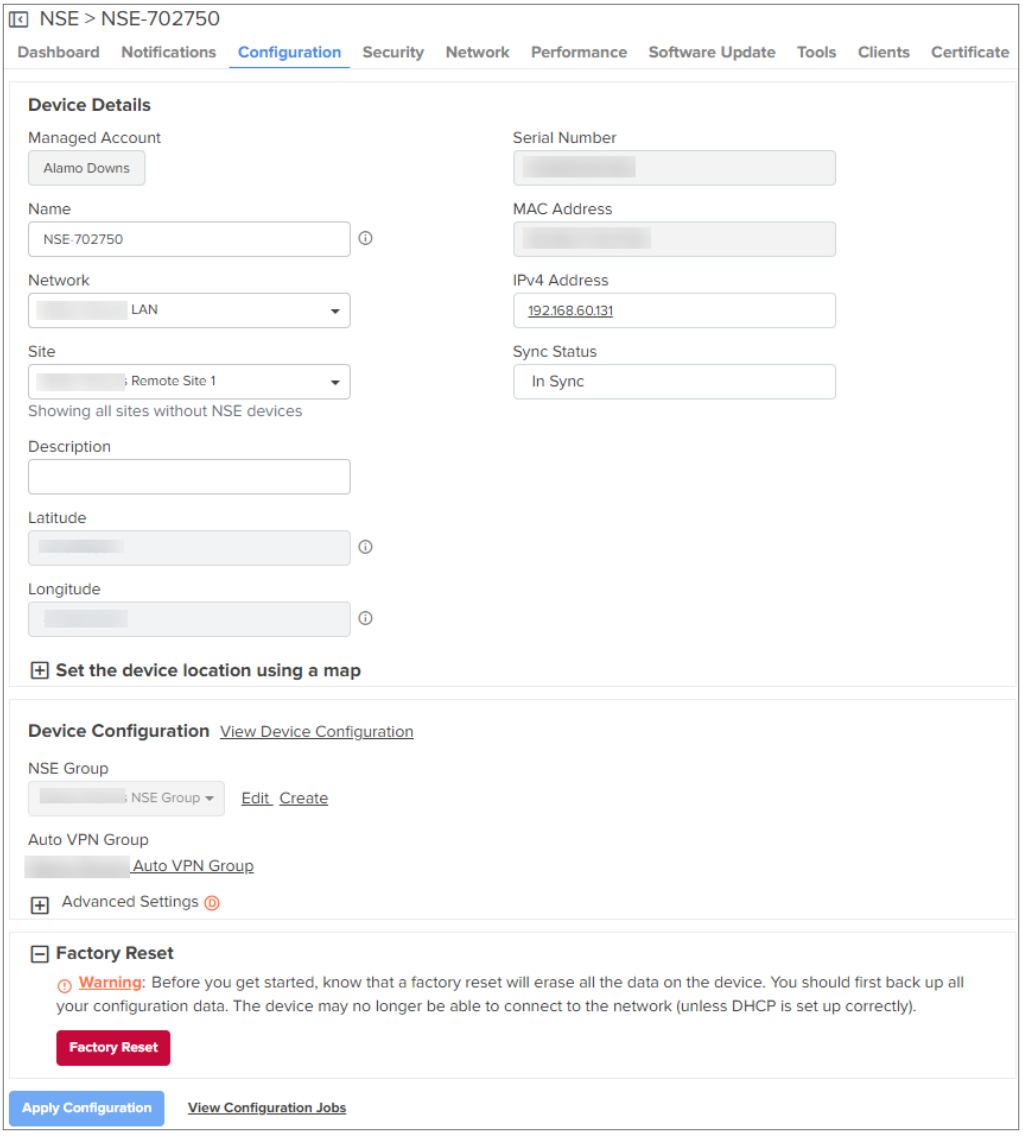


5. Add the **Email ID** and **Password** for the RADIUS user.
6. To enable two factor authentication for the this RADIUS user, select the **Enable 2FA** checkbox.
7. Click **Add**.
8. Click **Apply Configuration**.

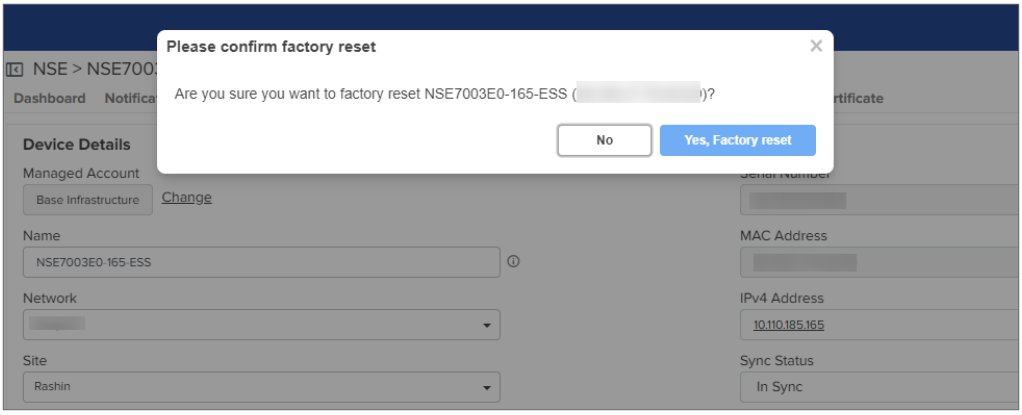
Factory Reset

To erase all the configuration on the device and bring the device back to the default factory configuration, follow these steps:

1. Navigate to the **NSE > Configuration** page and click Factory Reset.



2. In the confirmation window that appears, Click **Yes, Factory Reset**.



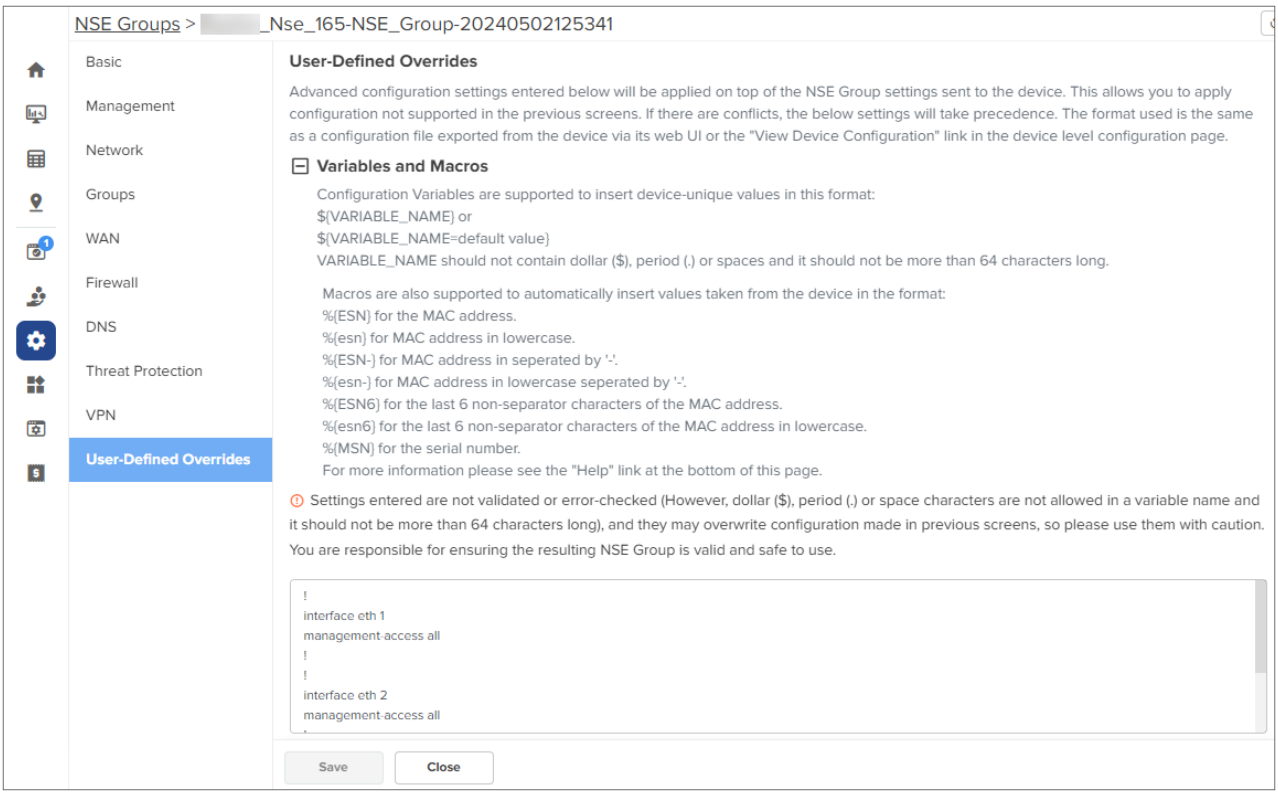
User-Defined Overrides

User-Defined Overrides are appended to the NSE groups before the configuration is applied to the device. This allows setting configuration parameters which are not supported by GUI.

To configure overrides based on your customized requirements by using variables and macros, follow these steps:.

1. Navigate to **NSE Profiles** > **NSE Groups** > **<NSE-group-name>** page > **User-Defined Overrides** section.
2. Define your overrides in the text box.

Figure 195 *The User-Defined Overrides page*



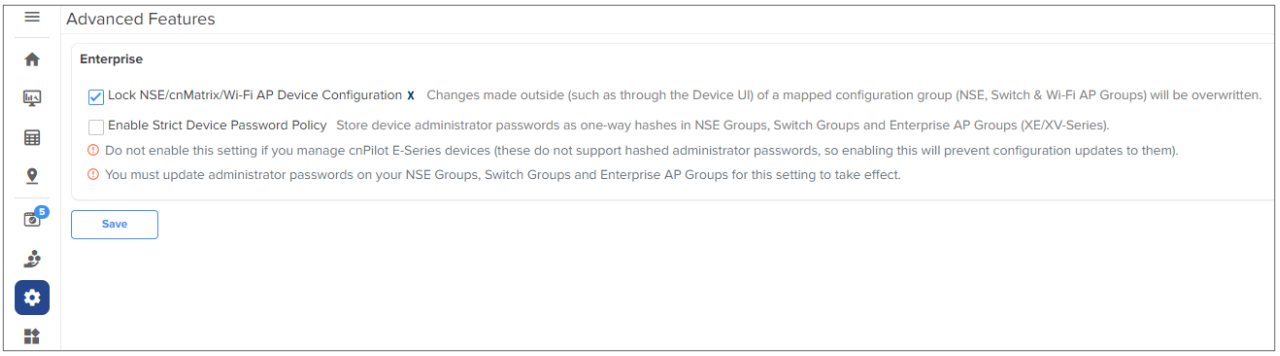
3. Click **Save**.

Configuration Lock

Configuration Lock forces the configuration on NSE and cnMaestro to be in sync always. If there is any configuration change done directly on the device, then cnMaestro tracks that device and triggers a configuration sync job to bring back the device to same configuration which is applied from the NSE Group.

To enable the configuration lock, follow these steps:

1. Navigate to the **Configuration** > **Advanced Features**.
2. Select the **Lock NSE/cnMatrix/Wi-Fi AP Device Configuration** checkbox.



3. Click **Save**.

Security

The **Security** page allows you to report the vulnerability and threats detected by the device.

Threats

The threat page displays **Threats by Location, Total Threats,** and threat categories based on **Critical, Major, Minor,** and origin of the threat (country of origin). The bar graph on the left displays the count based upon the threats by category. The pie chart displays the percentage of threats with respect to other threats. The per day bar chart displays the threat count aggregated on per day basis.

1. Navigate to **NSE** > **Security** > **Threats**.
2. Select **Time Range** from the dropdown.
    - Last 24 hours
    - Last 7 Days
    - Last 30 Days (Only when NSE Security Plus is enabled)

The threat page displays **Threats by Location, Total Threats,** and threat categories based on **Critical, Major, Minor,** and origin of the threat (country of origin). The bar graph on the left displays the count based upon the threats by category. The pie chart displays the percentage of threats with respect to other threats. The per day bar chart displays the threat count aggregated on per day basis.

Figure 196 *The Threats page*

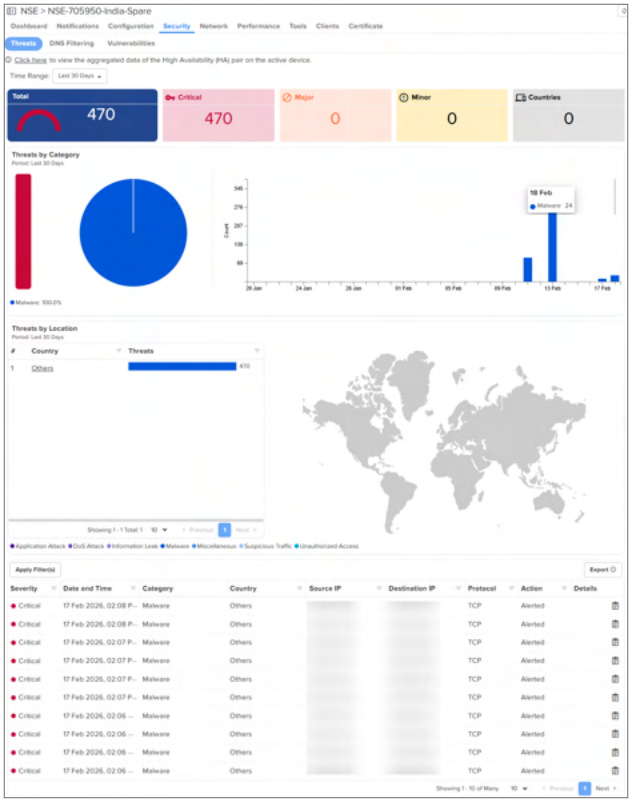


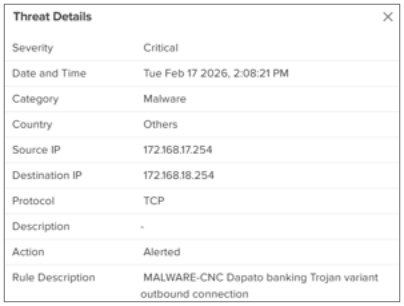
Table 46 *Parameters on the Threats page*

Parameter	Description
Severity	The severity of threat such as Critical, Major, and Minor.
Date and Time	The date and time when the threat occurred.
Category	Displays any of the following categories of threat: • Application Attack • DoS Attack • Information Leak • Malware • Miscellaneous • Suspicious Traffic • Unauthorized Access
Country	The source country of the threat is displayed for threats that originate from WAN to LAN.
Source IP	Source IP address of the flow which resulted in the threat.
Destination IP	Destination IP address of the flow which resulted in the threat.
Protocol	Protocol used in delivering the threat. **Note** This column is applicable only to NSE devices running version 2.1 and higher.

Table 46 *Parameters on the Threats page*

Parameter	Description
Action	Action taken by NSE when the threat arrived. **Note** This column is applicable only to NSE devices running version 2.1 and higher.
Details	Displays the above details in a single window in addition to a description of the threat. When you click the icon, the **Threat Details** window appears, as shown in Figure 197. **Note** The Protocol, Action, and Rule Description fields are applicable only to NSE devices running version 2.1 and higher.
Export	Export the threat details to a CSV file. A maximum of 50,000 entries are supported in the X account and 20,000 in the Essentials account.

Figure 197 *Threats > Threat Details window*



DNS Filtering

Note

- DNS filtering is applicable only to NSE devices running version 2.1 and higher.
- DNS filtering is not supported in Essentials account when the **Security Plus** mode is disabled.

The DNS Filtering page displays details of all instances where NSE has blocked access to websites. The data is shown for 24 hours, 7 days, or a maximum of 30 days.

The data can be exported to a CSV file and a maximum of 50,000 entries are supported.

To view the DNS Filtering page, complete the following steps:

1. Navigate to **NSE** > **<Device>** > **Security** > **DNS Filtering**.
2. Select **Time Range** from the dropdown.
    - Last 24 hours
    - Last 7 Days
    - Last 30 Days

Figure 198 *DNS Filtering page*

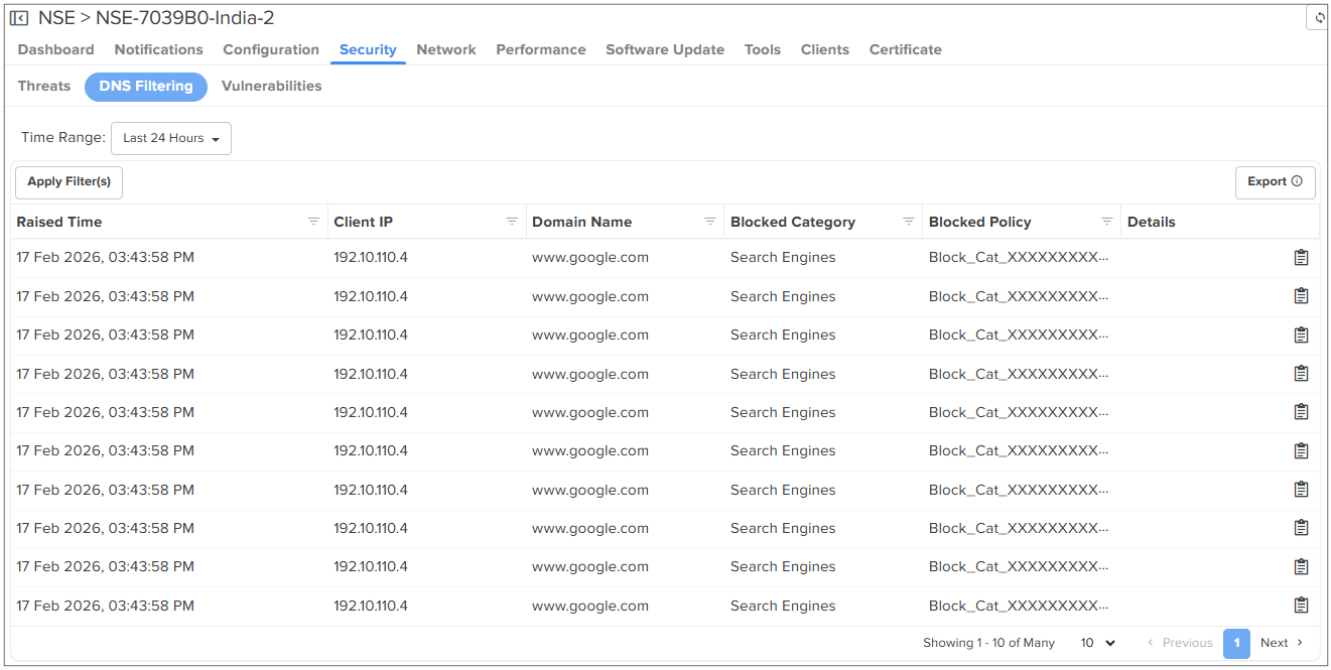


Table 47 *Parameters on the DNS Filtering page*

Parameter	Description
Raised Time	The date and time when the filtering occurred.
Client IP	IP address of the client trying to access the blocked website.
Domain Name	Domain name or URL that was blocked.
Blocked Category	Category to which the domain name is classified as.
Blocked Policy	DNS filtering policy that NSE applied to block the client fro accessing the website.
Details	Displays the above details in a single window. To view the DNS Filtering Details window, as shown in Figure 197, click the details ( ) icon.
Export	Export the threat details to a CSV file. A maximum of 50,000 entries are supported in the X account and 20,000 in the Essentials account.

Figure 199 *DNS Filtering > Threat Details window*



Vulnerabilities

The Vulnerabilities page displays **Total Vulnerabilities, Unique Critical, Unique Major, Unique Minor,** and **Vulnerable Clients.**

Figure 200 *The Vulnerabilities page*

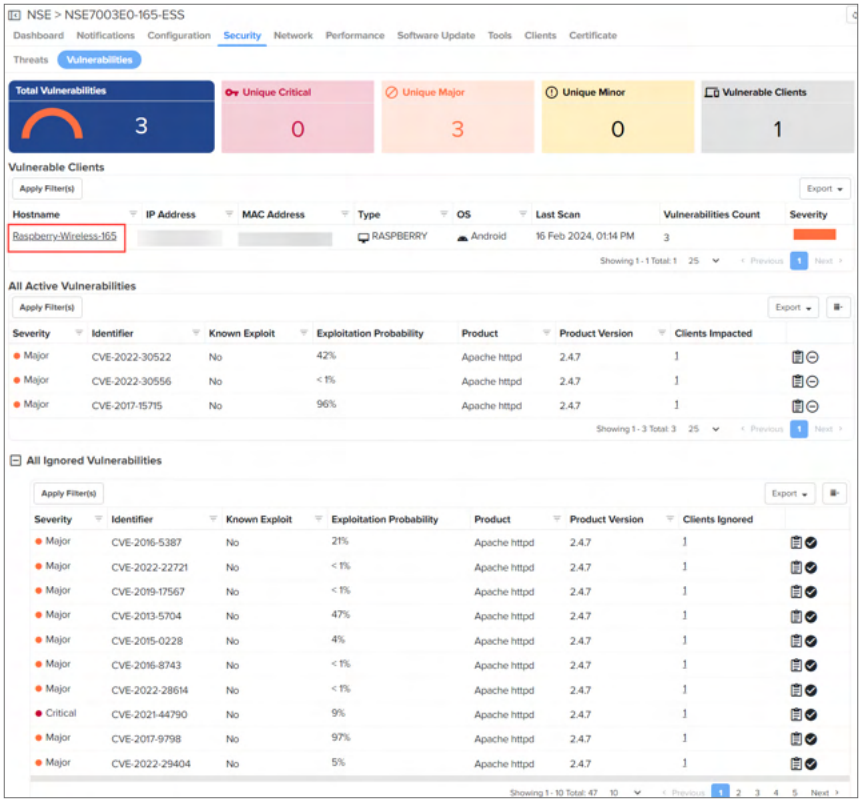


Table 48 *Parameters on the Vulnerabilities page*

Parameter	Description
Vulnerable Clients	
Hostname	Hostname of the client. When you click the hostname, you can view the vulnerabilities discovered by the NSE for the client, as shown in Figure 224.
IP Address	Source IPv4 address of the vulnerable client.
MAC Address	MAC address of the client.
Type	Type of client. For example, Computer, or Switch.
OS	Operating system running on the client. For example, Windows, or macOS.
Last Scan	Date and time of the last security scan performed on the client.
Vulnerabilities Count	Number of vulnerabilities found on the client during the security scan.
Severity	Level of severity assigned to each vulnerability, such as Critical, Major, or Minor.
Export	Exports a list of vulnerable clients. The following options are supported: • **Export page as CSV** • **Export all as CSV**
All Active Vulnerabilities	
Severity	The severity level of the vulnerability: • Critical

Table 48 *Parameters on the Vulnerabilities page*

Parameter	Description
	• Major • Minor
Identifier	CVE ID number for the discovered vulnerability.
Service	Service of the vulnerability.
Port	Port number of the service.
Known Exploit	Indicates whether the vulnerability is exploited in the wild and is present in the Known Exploited Vulnerabilities (KEV) catalog. For information on KEV catalog, see Known Exploited Vulnerabilities Catalog.
Exploitation Probability	The probability (in percentage) that a vulnerability will be exploited in the next 30 days. A higher value indicates a higher probability of the vulnerability being exploited. For information on Exploit Prediction Scoring System (EPSS), see Exploit Prediction Scoring System.
Product	Name of the product.
Product Version	Version of the product.
Clients Impacted	Number of clients impacted by the vulnerability. When you click the number in the **Clients Impacted** column, a window appears as shown in Figure 201.
Details	Displays the above details in a single window in addition to a short description of the vulnerability. A short description typically includes essential information, such as details on how an attacker can potentially exploit the vulnerability and which product versions are affected by it. When you click the Details ( ) icon, the **Vulnerability Details** window appears, as shown in Figure 202. When you click the CVE Identifier link, you can access detailed information about a specific vulnerability in the National Vulnerability Database (NVD) page, as shown in Figure 203.
Ignore	An option to ignore vulnerability(s). When you click the ignore ( ) icon, a window appears, as shown in Figure 205. To ignore vulnerability(s), select the required vulnerability(s), provide your reason in the **Reason** field, and then click **Ignore** button. The ignored vulnerability(s) are included in **All Ignored Vulnerabilities** section.
Export	Exports a list of all active vulnerabilities. The following options are supported: • **Export page as CSV** • **Export all as CSV**
All Ignored Vulnerabilities	
Severity	The severity level of the vulnerability: • Critical • Major

Table 48 *Parameters on the Vulnerabilities page*

Parameter	Description
	• Minor
Identifier	CVE ID number for the discovered vulnerability.
Service	Service of the vulnerability.
Port	Port number of the service.
Known Exploit	Indicates whether the vulnerability is exploited in the wild and is present in the Known Exploited Vulnerabilities (KEV) catalog. For information on KEV catalog, see Known Exploited Vulnerabilities Catalog.
Exploitation Probability	The probability (in percentage) that a vulnerability will be exploited in the next 30 days. A higher value indicates a higher probability of the vulnerability being exploited. For information on Exploit Prediction Scoring System (EPSS), see Exploit Prediction Scoring System.
Product	Name of the product.
Product Version	Version of the product.
Clients Ignored	Number of clients ignored. When you click the number in the **Clients Ignored** column, a window appears as shown in Figure 206.
Details	Displays the above details in a single window in addition to a short description of the vulnerability. A short description typically includes essential information, such as details on how an attacker can potentially exploit the vulnerability and which product versions are affected by it. When you click the Details ( ) icon, the **Vulnerability Details** window appears, as shown in Figure 202. When you click the CVE Identifier link, you can access detailed information about the specific vulnerability in the National Vulnerability Database (NVD) page, as shown in Figure 203.
Re-activate	An option to reactivate the ignored vulnerability(s). When you click the Reactivate ( ) icon, a window appears, as shown in Figure 207. To reactivate an ignored vulnerability(s), select the vulnerability(s) and then click **Re-activate** button. The reactivated vulnerability(s) are included in **All Active Vulnerabilities** section.
Export	Exports a list of all ignored vulnerabilities. The following options are supported: • **Export page as CSV** • **Export all as CSV**

Figure 201 *A window with impacted clients*



Figure 202 *The Vulnerability Details window*

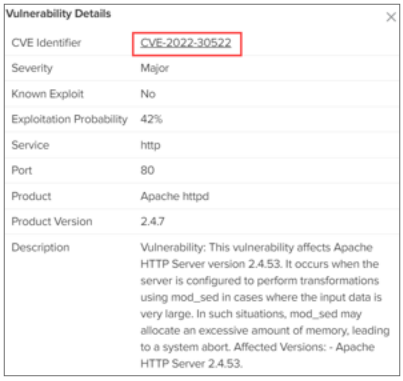
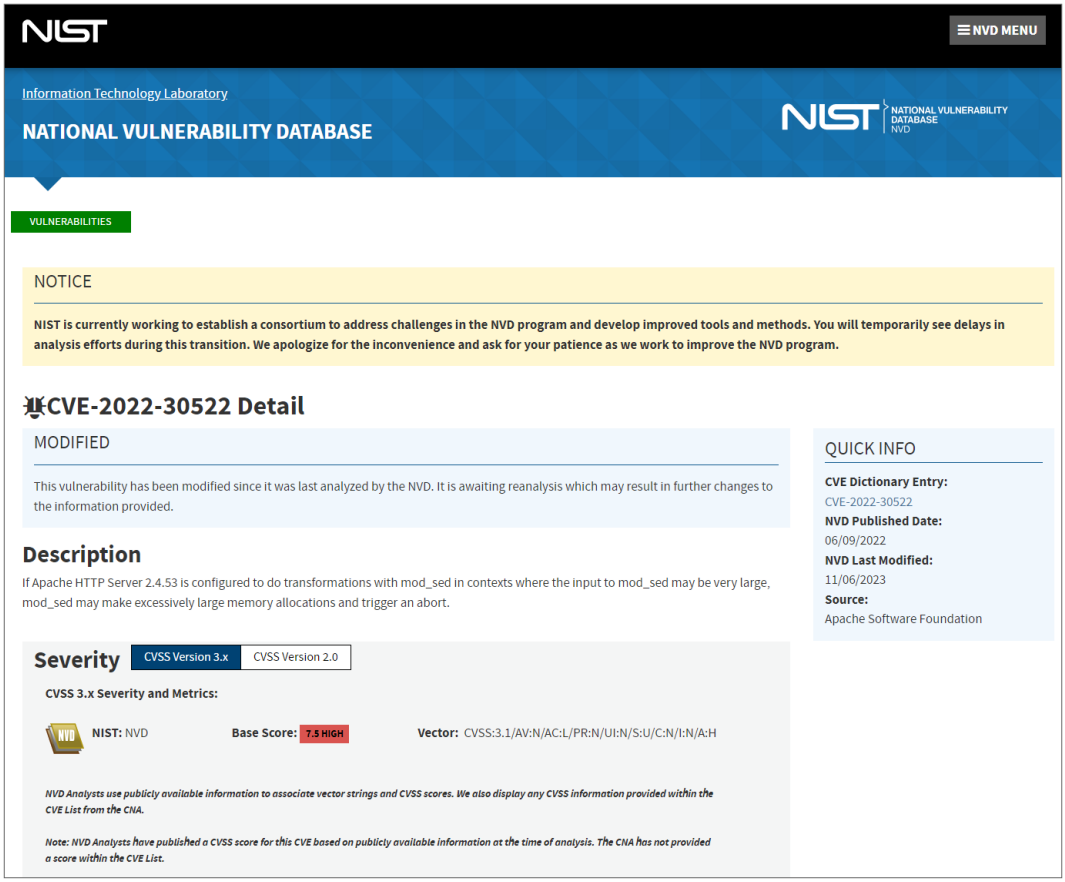


Figure 203 *The NVD page*



You can refine your search results using **Apply Filter(s)** option as shown in Figure 204.

Figure 204 *Apply Filter(s) option*

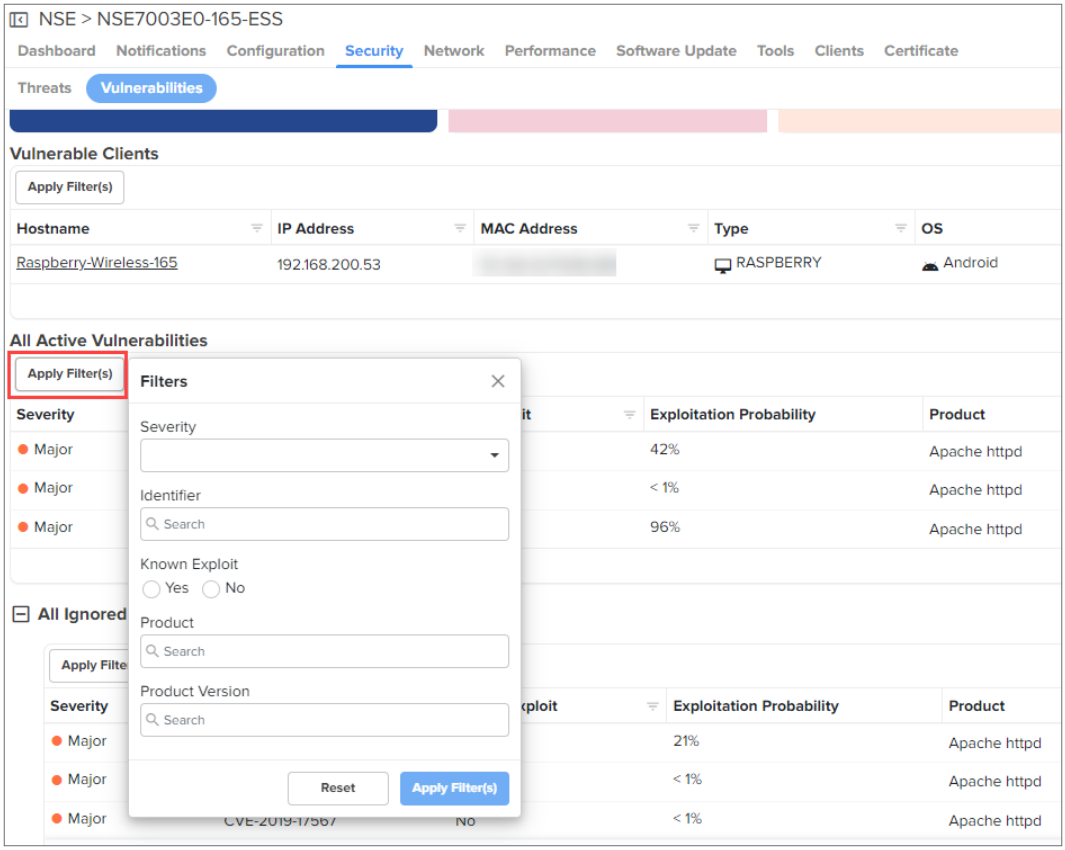


Figure 205 *A window with an option to ignore the client(s)*



Figure 206 *A window with ignored clients*

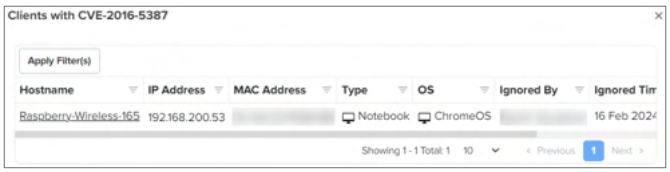
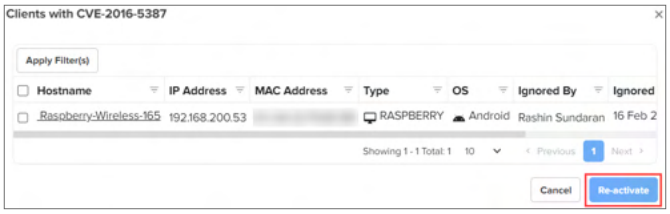


Figure 207 *A window with an option to reactivate*



Network

Network page displays information about onboard DHCP servers, route table, WAN and Starlink statistics, and VPN sites.

- LAN
- Routes
- WAN
- VPN Sites
- Tailnet
- Starlink
- Cellular WAN
- Firewall Counters

LAN

LAN page displays **Subnet** and **DHCP Leases**. You can **Apply Filters** for the table header to search for a specific parameter in the table.

Figure 208 *The LAN page*

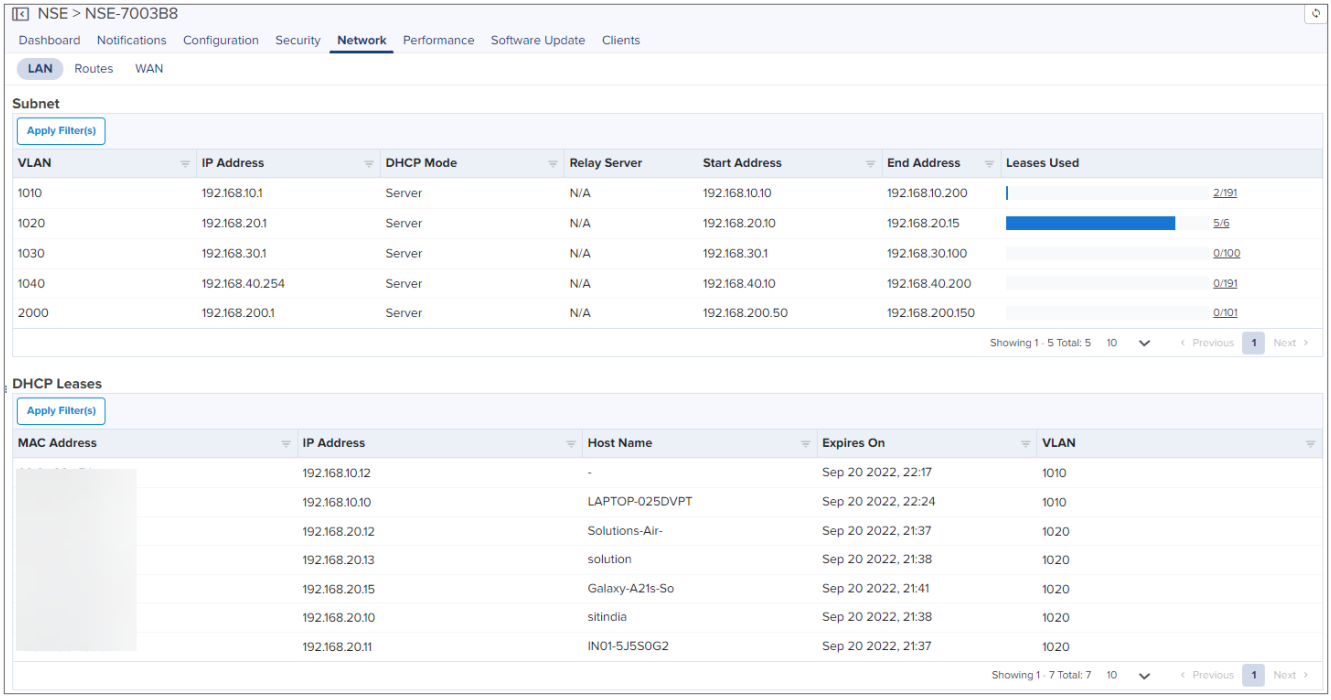


Table 49 *Parameters displayed in LAN*

Parameter	Description
Subnet	
VLAN	VLAN ID.
IP Address	Static IP address of the VLAN interface.

Table 49 *Parameters displayed in LAN*

Parameter	Description
DHCP Mode	Status of the DHCP server mode enabled or disabled.
Relay Server	Status of the relay server mode enabled or disabled.
Start Address	DHCP pool start IP address.
End Address	DHCP pool end IP address.
Lease Used	Active IP address issued by the DHCP server.
DHCP Leases	
MAC Address	MAC address of the client.
IP Address	The leased IP address to the client.
Host Name	The hostname of the client.
Expires On	The duration for the leased IP.
VLAN	The VLAN ID assigned to the client.

Routes

Routes page displays layer 3 routing table of the device. You can **Apply Filters** for the table header to search for a specific parameter in the table.

Figure 209 *The Routes page*

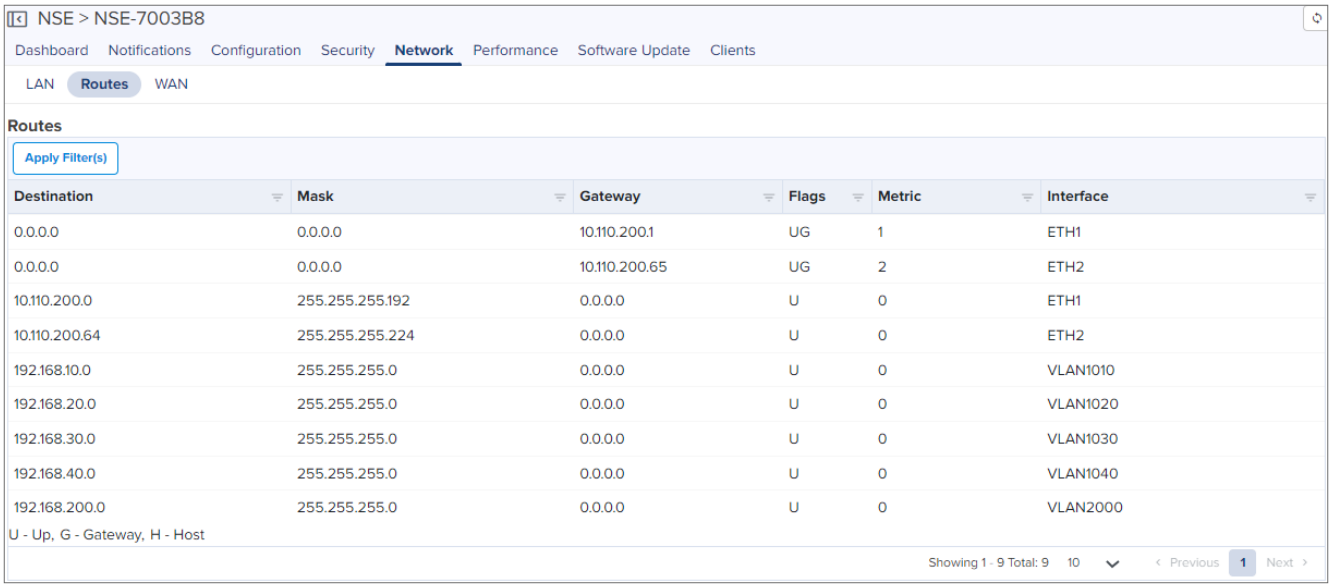


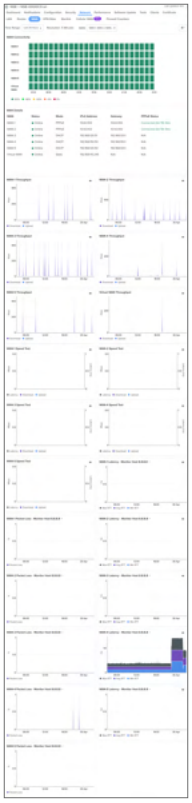
Table 50 *Parameters on the Routes page*

Parameter	Description
Routes	
Destination	Destination address of the routes.
Mask	Subnet mask of the specific route.
Gateway	Default gateway of the routes.
Flags	Flags of the routes.
Metric	Metric of the routes.
Interface	Interface of the routes.

WAN

WAN page displays **WAN Connectivity, WAN Details,** graphical representation of **Speed Test, Throughput, Latency,** and **Packet loss** in **WAN-1, WAN-2**, and **Virtual WAN** in the selected **Time Range** (Last 24 hours or Last 7 Days)**.**

Figure 210 *The WAN page*



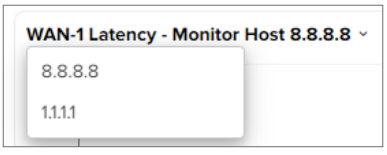
- **WAN connectivity**: Provides the status of the periodic health check of WAN links.

  Select the required WANs from the WAN drop-down, to display the details.

- **WAN speed test**: Provides the status of the MAX uplink and downlink bandwidth of the WAN link.
- **WAN throughput**: Provides the usage of WAN uplink and downlink over a period of time.

  This graph is supported for Virtual WAN also.

- **WAN Latency - Monitor Host**: Displays the latency based on maximum, minimum, and average round trip time (RTT) of monitor hosts for each of the WAN links configured. If there are more than one monitor hosts, you can view the details for each of the hosts by selecting the host from the dropdown list.



- **WAN Packet Loss - Monitor Host**: Displays the packet loss (in percentage) experienced by monitor hosts for each of the WAN links configured.

WAN Details

Note

For Virtual WAN, only **Status** and **IPv4 Address** details are displayed.

Table 51 *Parameters displayed on the WAN Details section*

Parameter	Description
WAN Details	
WAN	Name of the WANs configured on the device. • For NSE3000, it can be WAN 1 to 4 • For NSE4000, it can be WAN 1 to 5 • Virtual WAN
Status	Status (online or offline) based upon the periodic WAN link health check.
Mode	Mode as DHCP or Static.
IPv4 Address	IPv4 address of the WAN.
Gateway	Default gateway address of the WAN interface.
PPPoE Status	Status of the PPPoE server.

VPN Sites

The VPN Sites page displays the network traffic and connection details as shown in Figure 211.

Figure 211 *The VPN Sites page*

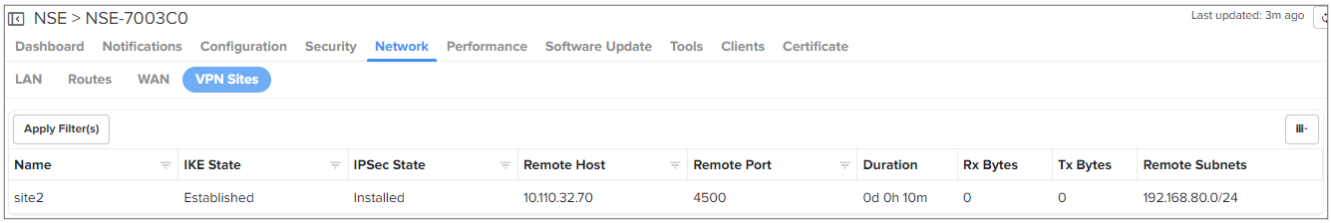


Table 52 *Parameters displayed on the VPN Sites page*

Parameter	Description
VPN Sites	
Name	Name of the VPN site.
IKE State	Current state of IKE protocol.
IPSec State	Current state of IPSec protocol.
Remote Host	IP address of the remote VPN endpoint.
Remote Port	Port number of the remote VPN endpoint.
Duration	Duration of the VPN connection.
Rx Bytes	Number of bytes received by the local VPN endpoint from the remote VPN endpoint.
Tx Bytes	Number of bytes transmitted by the local VPN endpoint to the remote VPN endpoint.
Remote Subnets	IP address ranges assigned to the remote VPN endpoint's network.

Tailnet

The Tailnet page displays information about the Tailnet tunnel activity across all peers. Tailscale network and its latency to different regions, and a list of Tailnet peers.

To view the details, make sure the **Tailscale** configuration under **NSE Groups** > **VPN** is enabled and the corresponding parameters are configured correctly.

For parameter information, see Tailscale configuration.

Note

Tailnet page and the corresponding Tailscale configuration are supported only when NSE **Security Plus** mode is enabled.

Figure 212 *Tailnet page*

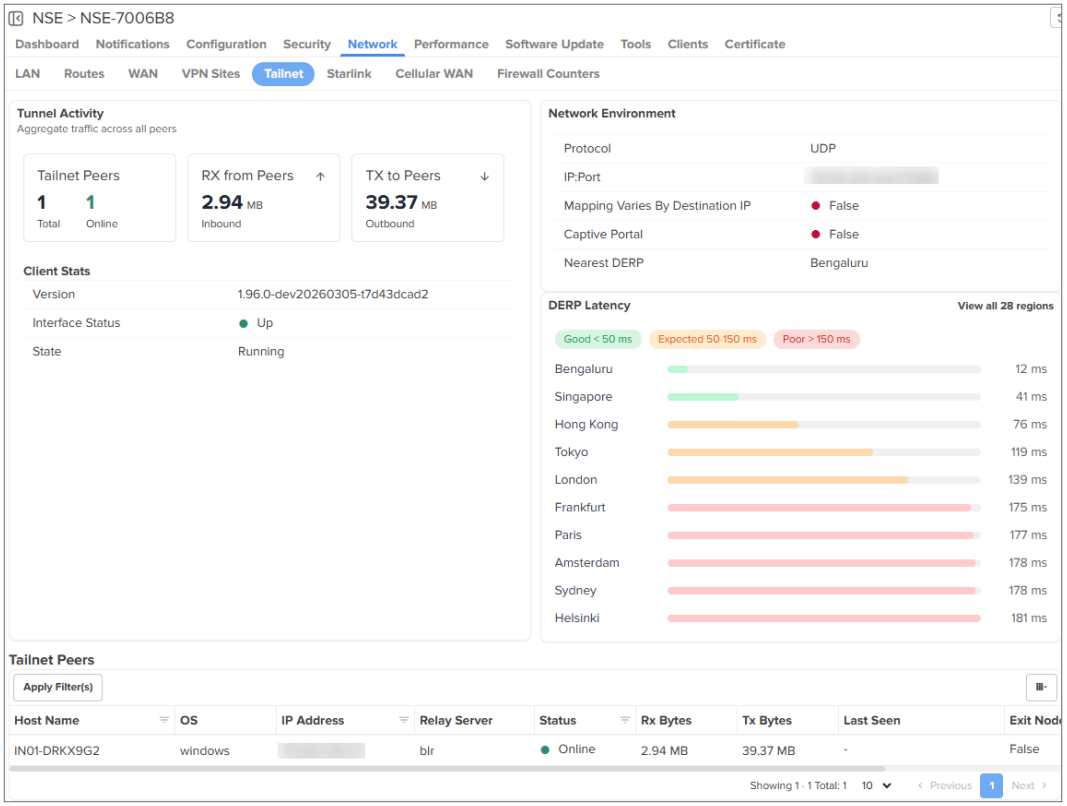


Table 53 *Parameters displayed on the Tailnet page*

Parameter	Description
Tunnel Activity—Displays information about the Tailnet tunnel, its peers, and the total traffic.	
Tailnet Peers	Total number of Tailnet peers and the number of peers that are online.
RX from Peers	Total data received from the Tailnet peers.
TX to Peers	Total data sent to the Tailnet peers.
Client Stats	Displays the following client information: • Version • Interface Status—Up or down • State

Parameter	Description
Network Environment—Displays connectivity details using protocol and IP-port mapping.	
Protocol	Protocol used for peer connectivity. (UDP or TCP).
IP:Port	IPv4 address and port number of the device.
Mapping Varies By Destination IP	Indicates whether the mapping is performed based on the destination IP address.
Captive Portal	Indicates whether the traffic is routed to a captive portal or not.
Nearest DERP	Specifies the name of the nearest Designated Encrypted Relay for Packets (DERP) region.
DERP Latency	Displays the latency from the client to available DERP regions. • Poor (In red color): > 150 ms • Expected (In yellow color): 50-150 ms • Good (In green color): < 50 ms The table lists the top 10 regions with the lowest latencies. Click **View all <number of regions> regions** for the complete list.
Tailnet Peers	Lists the details of available Tailnet peers.

Starlink

The Starlink page displays performance and alignment data of Starlink service.

To view the details, make sure the following points are adhered to:

- Starlink detection is enabled on the **WAN** configuration page.
- Starlink Dish IP address is configured correctly.

Figure 213 *Starlink page*

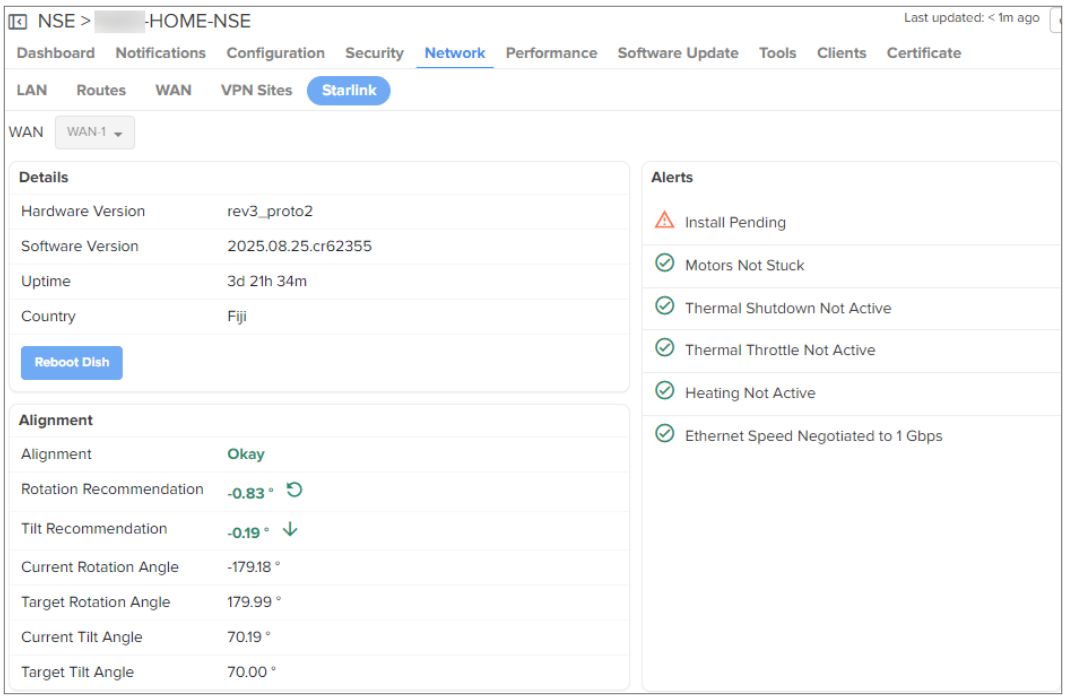




Table 54 *Parameters displayed on the Starlink page*

Parameter	Description
Details—Displays version and location details about the Starlink dish	
Hardware Version	Device hardware version currently running on the Starlink dish.
Software Version	Software version currently running on the Starlink dish.
Uptime	Duration, in the `DDDd Hh MMm` format, for which the dish has been turned on.
Country	Name of country where the Starlink dish is located.
Reboot Dish	Click to reboot the Starlink dish from cnMaestro UI.
Alerts—Displays the various alerts generated by the dish. • —Indicates lower priority alerts. • —Indicates higher priority alerts.	
Alignment—Displays the status of the alignment along with recommendations for correcting the alignment.	
Alignment	Specifies if the status of dish alignment. The following values are supported: • **Okay**—Displayed in green color. • **Misaligned**—Displayed in red color. • **Determining**—Displayed in orange color.
Rotation Recommendation	Indicates the recommended rotation angle, in degrees. The angle may be one of the following options:

Parameter	Description
	• Positive rotation angle—Represented by the clockwise symbol • Negative rotation angle—Represented by the anticlockwise symbol
Tilt Recommendation	Indicates the recommended tilt angle, in degrees. The tilt angle may be one of the following options: • Positive tilt angle—Represented by the clockwise symbol • Negative tilt angle—Represented by the anticlockwise symbol
Current Rotation Angle	Specifies the current rotation angle, in degrees.
Target Rotation Angle	Specifies the target rotation angle, in degrees.
Current Tilt Angle	Specifies the current tilt angle, in degrees.
Target Tilt Angle	Specifies the target tilt angle, in degrees.
Graphs—Graphical representation of dish throughput, latency, and data drop rate for the last 12 hours.	
Throughput	Displays the uplink and downlink data (in kbps) of the Starlink dish for the last 12 hours.
Latency	Displays the Starlink dish latency (in ms) for the last 12 hours.
Drop Rate	Displays the percentage of dropped data packets for the last 12 hours.

Cellular WAN

Cellular WAN integration adds monitoring and configuration support for cellular uplinks in cnMaestro. It enables visibility and management of cellular WAN interfaces along with wired and Starlink connections.

Note

- Cellular WAN is supported only on NSE devices running version 2.2 and higher.
- Cellular WAN data supports a maximum of two SIM cards.
- To view the details, make sure the **Uplink Type** parameter under **NSE Groups** > **WAN** is configured as **Cellular** and the corresponding parameters are configured correctly.

  For parameter information, see WAN.

Figure 214 *Cellular WAN page*

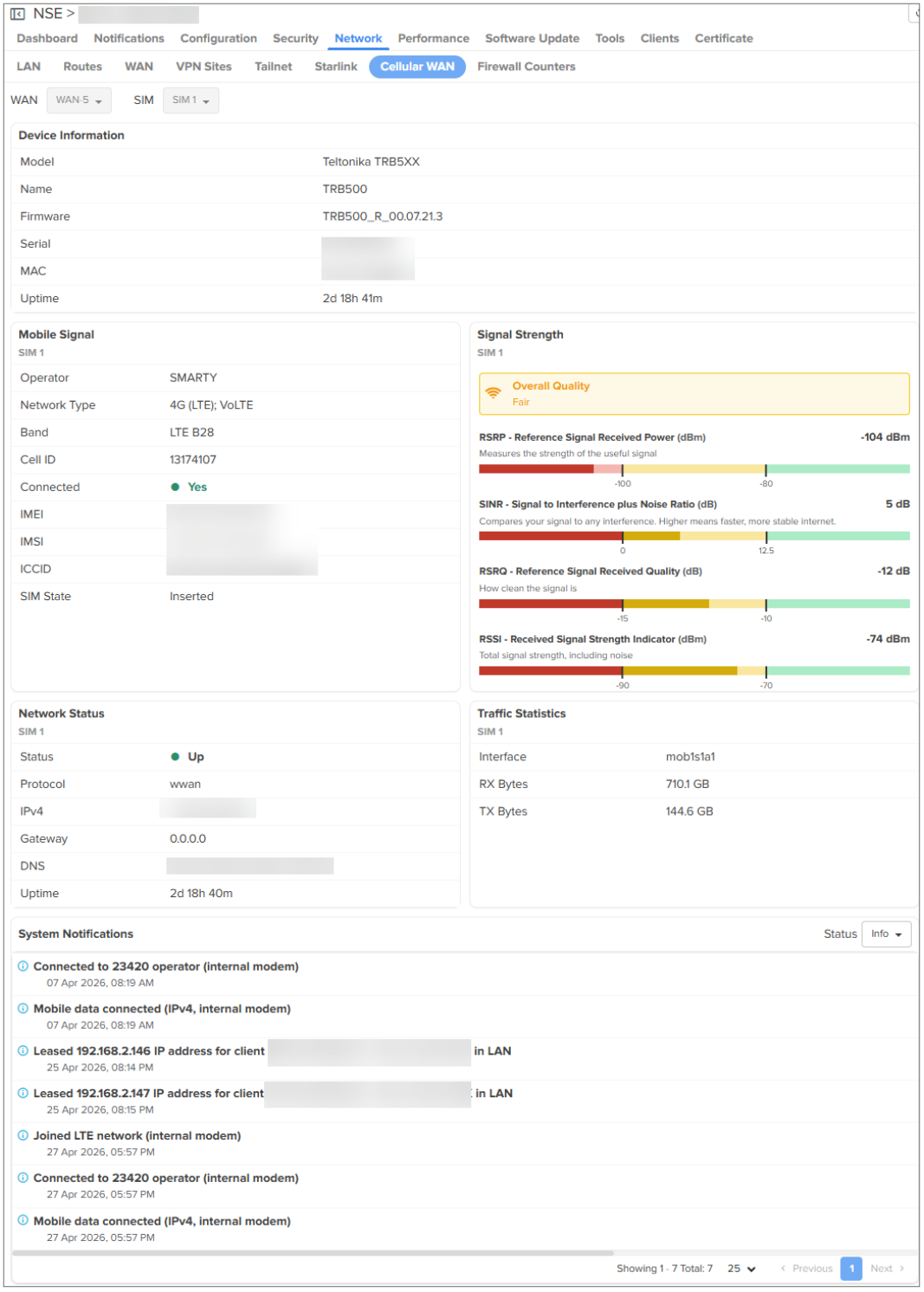


Figure 215 *Cellular WAN page when configuration is disabled*

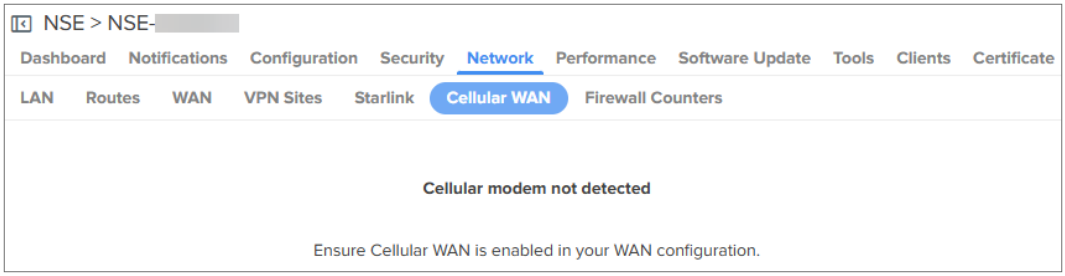


Table 55 *Parameters displayed on the Cellular WAN page*

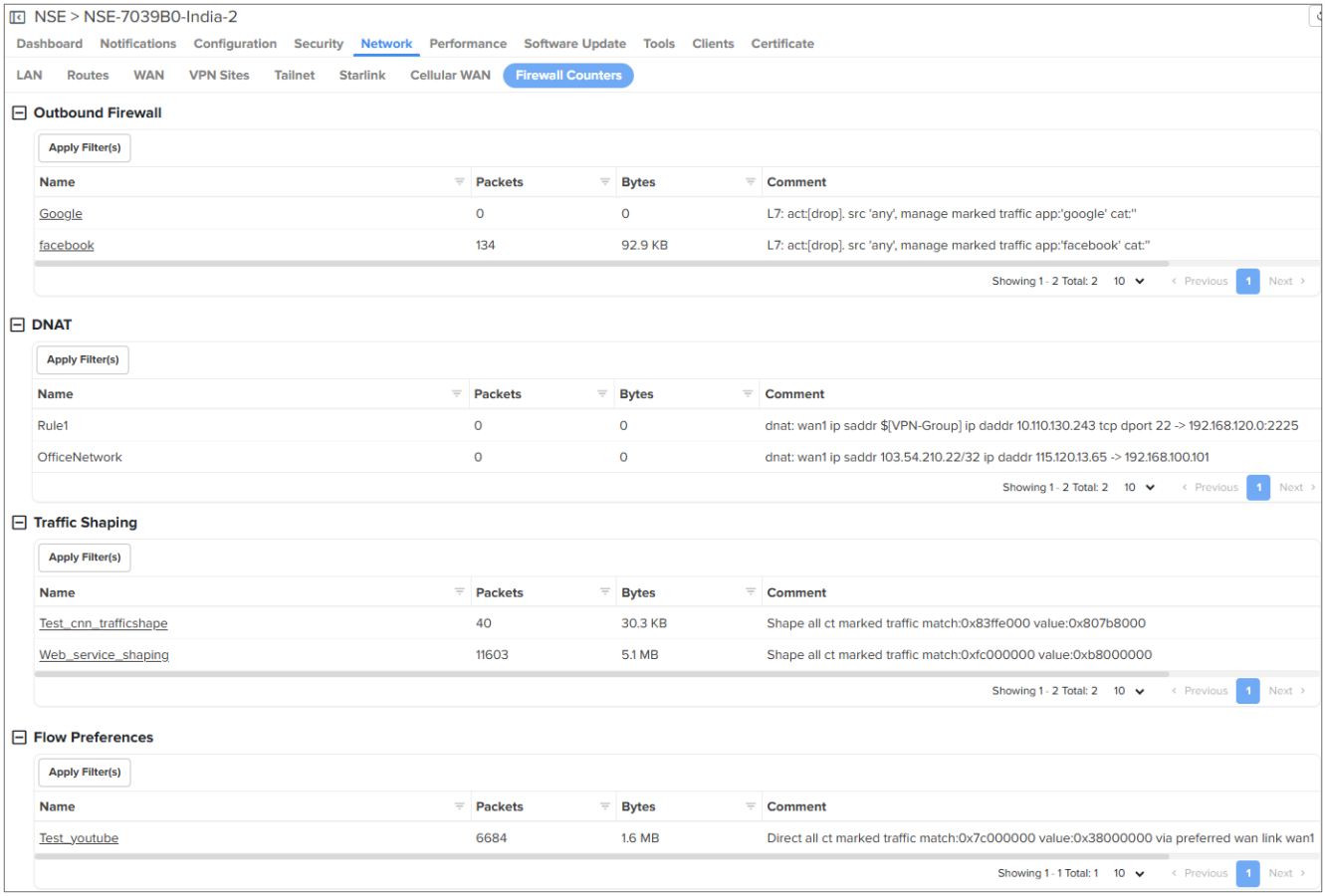
Parameter	Description
WAN	WAN interface for which you want to view the data.
SIM	SIM card for which you want to view the data.
Device Information—Displays cellular WAN device information.	
Model	Model name of the cellular WAN device.
Name	Name provided for the device.
Firmware	Firmware version installed on the device.
Serial	Serial number of the device.
MAC	MAC address of the device
Uptime	Duration (in the DDd HHh MMm format) for which the device is switched on.
Mobile Signal—Displays the details of the operator and mobile signal for the selected SIM card.	
Operator	Mobile network provider that the SIM card is currently connected to.
Network Type	Type of network the SIM is using.
Band	Radio frequency band on which the SIM is communicating with the mobile network.
Cell ID	Unique cellular tower ID that the SIM is currently connected to.
Connected	Indicates whether the SIM card is connected to the cellular network or not.
IMEI	International Mobile Equipment Identity (IMEI) Unique number assigned to the device's hardware.
IMSI	International Mobile Subscriber Identity (IMSI) Unique ID stored on the SIM that is used to identify the user.
ICCID	Integrated Circuit Card Identification (ICCID). Unique serial number of the SIM card.
SIM State	Current status of the SIM card,
Signal Strength	Displays the overall signal strength as poor, fair, or green depending on the following signal strength parameters (along with exact values): • **RSRP - Reference Signal Received Power (dBm)**—Measures the strength of the useful signal ◦ Poor (In red color): < -100 dBm ◦ Fair (In yellow color): -100 to -80 dBm ◦ Good (In green color): > -80 dBm • **SINR - Signal to Interference plus Noise Ratio (dB)**—Compares your signal to any interference. Higher means faster, more stable internet.

Parameter	Description
	◦ Poor (In red color): < 0 dB ◦ Fair (In yellow color): 0 to 12.5 dB ◦ Good (In green color): > 12.5 dB • **RSRQ - Reference Signal Received Quality (dB)**—Displays signal quality by combining signal strength and interference ◦ Poor (In red color): < -15 dB ◦ Fair (In yellow color): -15 to -10 dB ◦ Good (In green color): > -10 dB • **RSSI - Received Signal Strength Indicator (dBm)**—Displays total signal strength, including noise ◦ Poor (In red color): < -90 dBm ◦ Fair (In yellow color): -90 to -70 dBm ◦ Good (In green color): > -70 dBm
Network Status—Displays the status of the network for the selected SIM card.	
Status	Indicates the status of the network.
Protocol	Displays the network protocol used.
IPv4	Displays the device IPv4 address assigned by the network.
Gateway	Displays the Gateway address used by the network.
DNS	Displays the DNS server address.
Uptime	Displays the device up time (in the DDd HHh MMm format).
Traffic Statistics—Displays the traffic details for the selected SIM card.	
Interface	Displays the interface used.
RX Bytes	Displays the total number of received data.
TX Bytes	Displays the total number of transmitted data.
System Notifications	Displays the alerts and notifications reported by the device for the following severities: • All • Info • Notice • Error • Warning • Critical • Alert **Note**: A maximum of 250 notifications are displayed.

Firewall Counters

The Firewall Counters page provides statistical tracking metrics associated with firewall-related rules configured on the devices using cnMaestro. The statistics provide a basic view of the implementation of rules and if the rules are active.

Figure 216 *Firewall Counters page*



The statistics displayed here is temporary and the data is reset when the NSE device is restarted or when the configuration is updated on the device.



Note

If there is a mismatch between the cnMaestro and the device configuration, clicking the rule link displays an error that the rule is not present.

For example, if the rule is updated or renamed and the configuration is not synced with the device, then the error message is displayed.

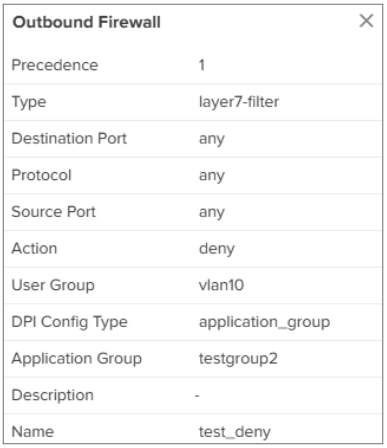
The page includes the following sections:

- **Outbound Firewall**—Lists all the outbound filter rules and displays the total number and size of packets (in bytes) transferred for each outbound filter rule applied on clients traffic.

  These rules are configured under the **NSE Groups** > ***<Group-name>*** > **Firewall** > **Outbound Filter Rules** section.

  To view the information about the rule, click the link corresponding to the rule. The rule window appears:

Figure 217 *Outbound Firewall rule information window*



- **DNAT**—Displays the total number and size of packets (in bytes) transferred for each of the Destination Network Address Translation (DNAT) rules configured.

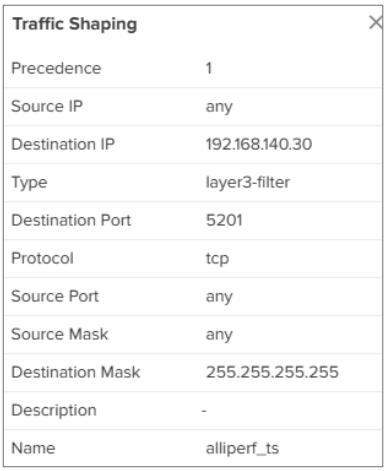
  These rules are configured under the **NSE Groups** > ***<Group-name>*** > **Firewall** > **Port Forward Rules**, **NAT One-to-One**, and **NAT One-to-Many** sections.

- **Traffic Shaping**—Displays the total number and size of packets (in bytes) transferred for each of the traffic shaping rules configured.

  These rules are configured under the **NSE Groups** > ***<Group-name>*** > **WAN** > **Traffic Shaping** section.

  To view the information about the rule, click the link corresponding to the rule. The rule window appears:

  Figure 218 *Traffic Shaping rule information window*



- **Flow Preferences**—Displays the total number and size of packets (in bytes) whenever traffic passes through the configured applications or IP addresses on the specified WAN.

  These rules are configured under the **NSE Groups** > ***<Group-name>*** > **WAN** > **Flow Preferences** section.

  To view the information about the rule, click the link corresponding to the rule. The rule window appears:

Figure 219 *Flow Preferences rule information window*

Flow Preferences	
Source IP	172.24.40.0
Destination IP	192.168.140.30
Type	layer3-filter
Destination Port	any
Protocol	any
Source Port	any
Source Mask	255.255.255.0
Destination Mask	255.255.255.255
Name	sendiperf
Description	-
Policy	flexible
WAN	wan2

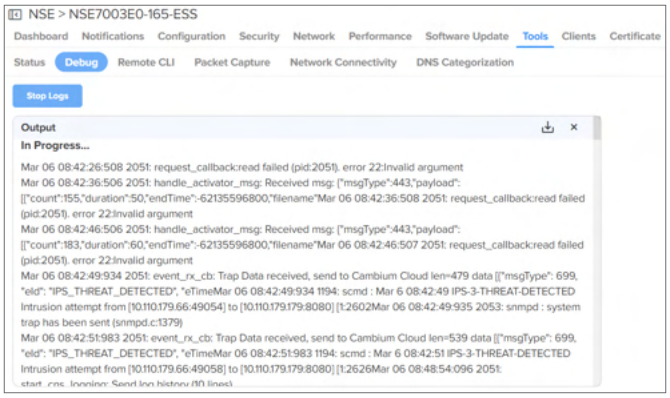
Debug Tools

You can capture logs, run remote CLI commands to see stats in real time, run traceroute, ping to check the reachability, and run live packet capture on the NSE devices on the selected interface.

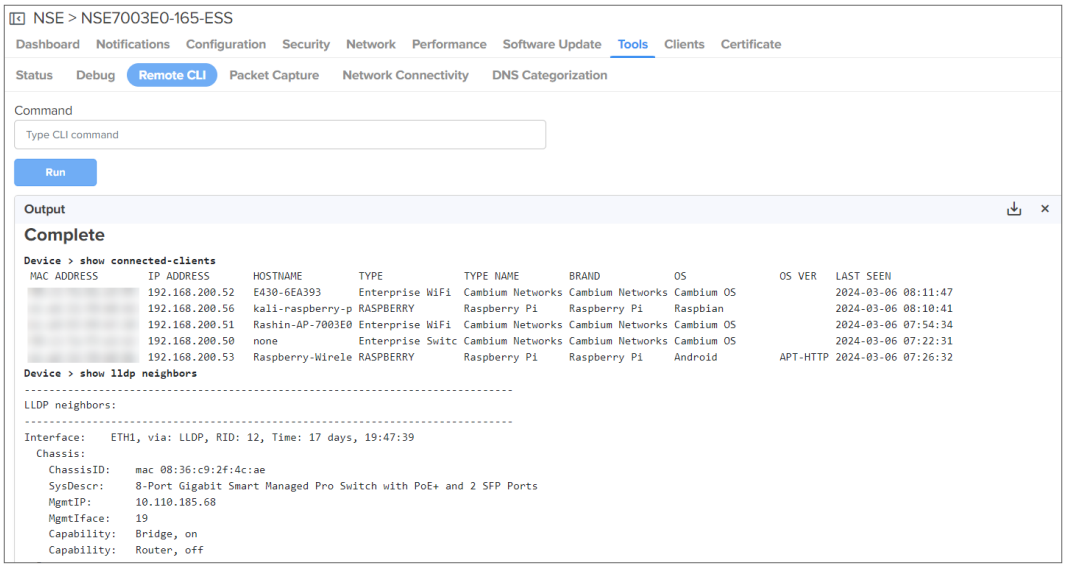
To display the NSE device status, navigate to **NSE** > **Tools** > **Status** page.



To access the logs, navigate to **NSE** > **Tools** > **Debug** tab and click **Start Logs**:

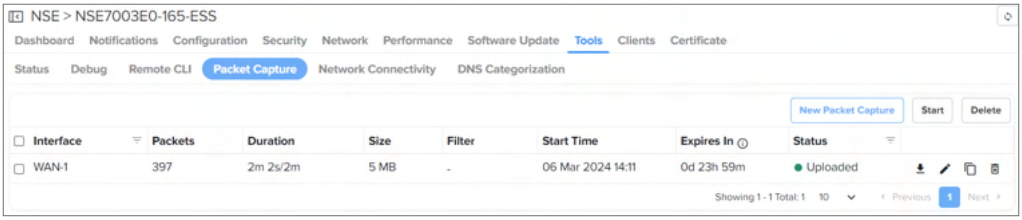


To run CLI commands, navigate to **NSE** > **Tools** > **Remote CLI** page, enter the **Command** and then click **Run**:

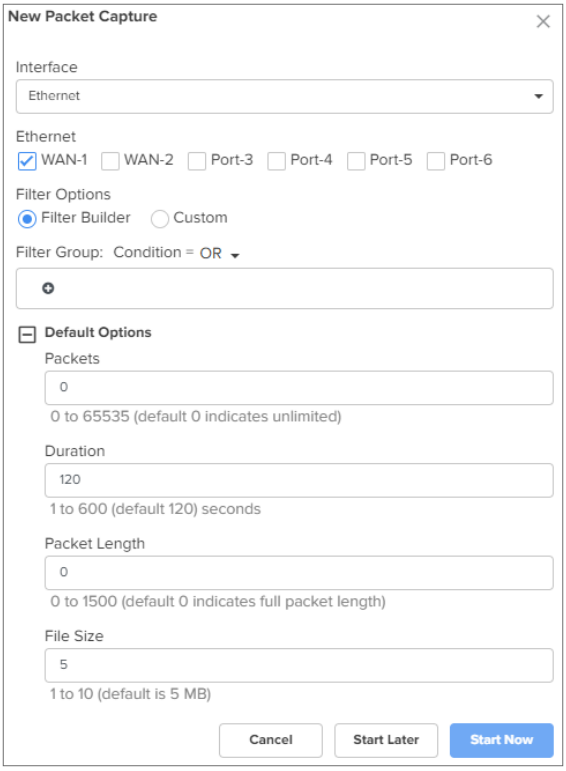


To run packet capture on the NSE device, navigate to **NSE > Tools > Packet Capture** page and follow these steps:

1. Click **New Packet Capture** and complete the details.



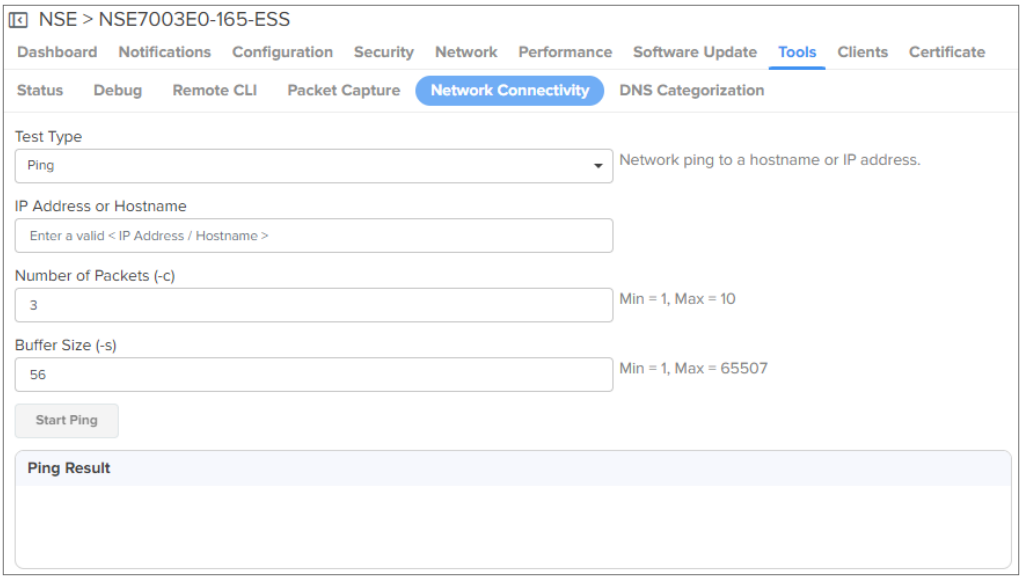
The New Packet Capture window is displayed.



2. Click either **Start Now** or **Start Later** and then click **Close**.

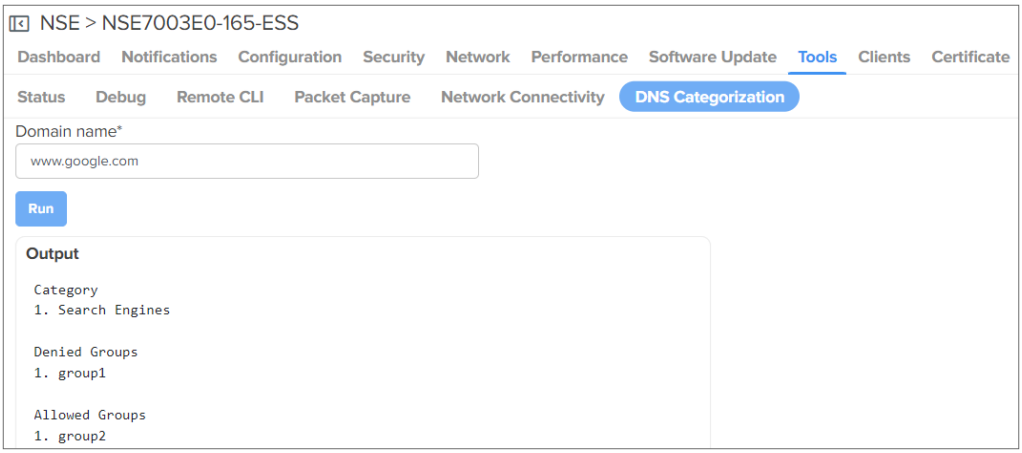
3. If you had clicked **Start Later**, you can start the packet capture by clicking the right pointed triangle in the right most column of the interface details list.

   To check the network connectivity, navigate to **NSE > Tools > Network Connectivity** page, complete the details, and then click **Start Ping**:



   To access DNS categorization, navigate to **NSE** >**Tools** > **DNS Categorization.**

   The DNS categorization tool is used to determine the category of the domain under which the queried domain falls. It is employed in scenarios where the administrator knows the specific domain and wants to ascertain which category to select while configuring the DNS filter. Additionally, it indicates whether the queried domain is permitted or denied for the specified group configured on the box.



Clients

The Clients page displays information depending on the system, network. or the device level from where you are accessing the page.

- Device-level information
- Network- and Site-level information
- Clients > Dashboard

Device-level information

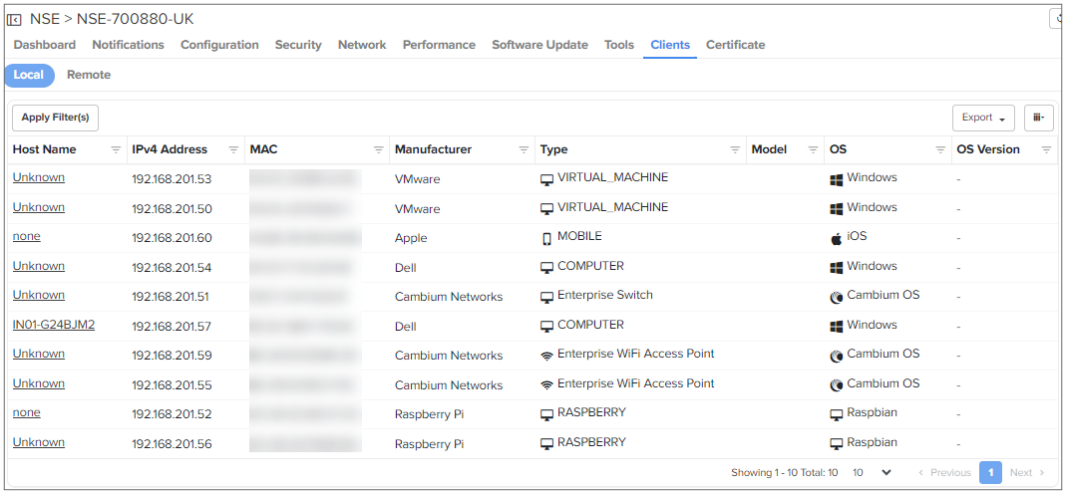
Clients page at the device-level displays the Local and Remote clients (VPN clients) connected to the NSE device.

Note

You can connect up to 1000 clients on the LAN side of NSE. The clients can be either wired clients or wireless clients.

Local

The Local page displays the total client count which are connected to the NSE on the LAN side. Using device finger printing NSE provides **Device Type**, **Device OS**, and **OS Version**.



Click **Host Name**. It navigates to detailed Client Dashboard as shown in Figure 223.

Remote

The **Remote** page displays client count (vpn client) connected on the WAN side.

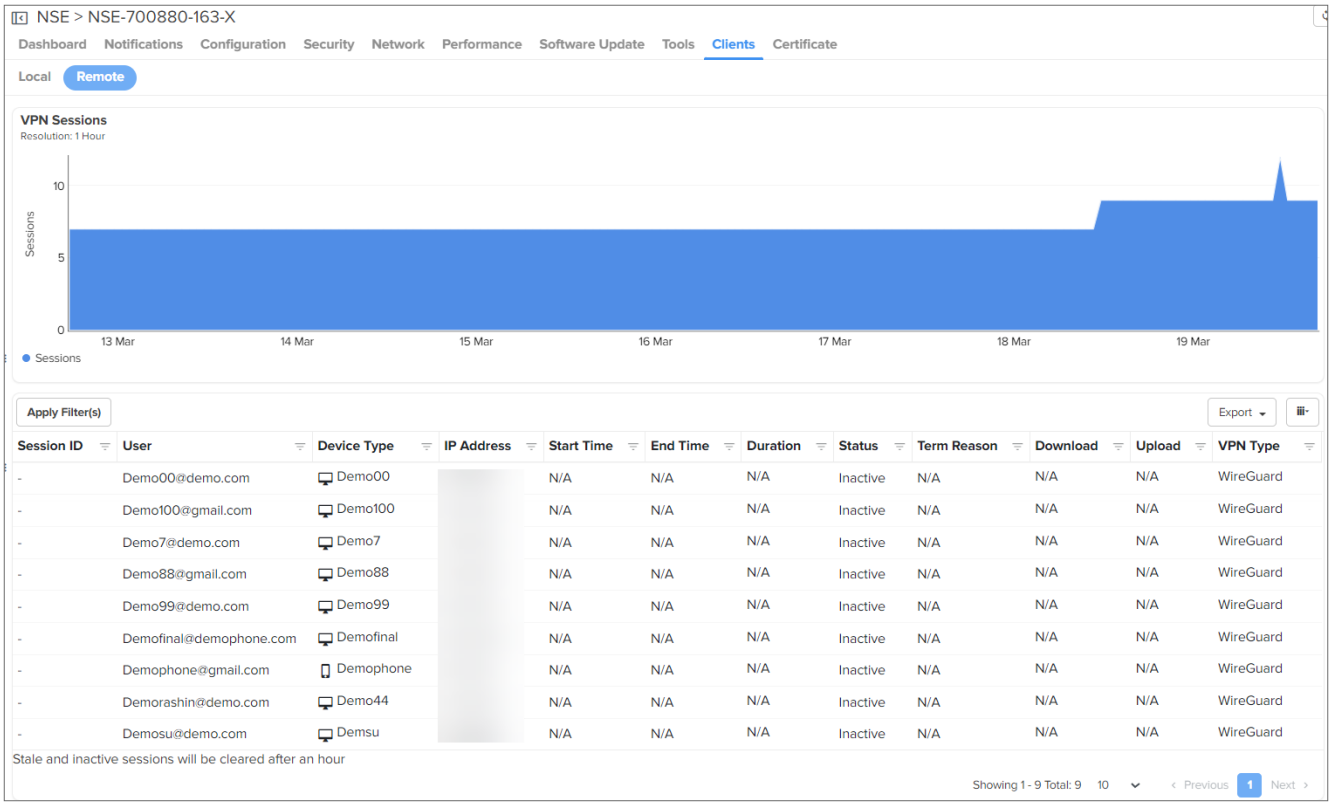


Table 56 *Parameters displayed in VPN sessions*

Parameter	Description
VPN Sessions	
Session ID	ID of the session. **Note**: The session ID is displayed only for **IPSec IKEV2** and **L2TP over IPSec** VPN types.
User	VPN user name.
Device Type	Type of device.
IP Address	IP Address assigned to the VPN client.
Start Time	VPN session start time.
End Time	VPN session end time.
Duration	Total session duration.
Status	Session status as active or inactive.
Term Reason	Terminated reason of the session disconnected or timeout.
Download	Total download by the VPN user.
Upload	Total upload by the VPN user.
VPN Type	Type of VPN. The following options are supported: • **WireGuard** • **IPSec IKEV2** • **L2TP over IPSec**

Network- and Site-level information

The Clients page at the Network- and Site-level displays the details of all the connected wireless and wired clients, and all unconnected clients.

- Wireless Clients
- Wired Clients
- Unconnected Clients

Wireless Clients

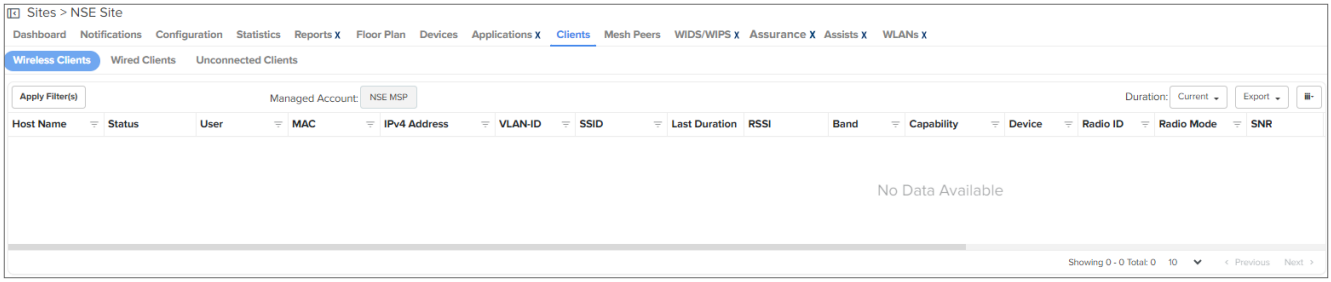
The **Clients** > **Wireless Clients** page at the Network- and Site-level displays the following details:

- **General**
  - Device
  - Device MAC
  - Host Name
  - Last Duration
  - Last Seen
  - Manufacturer
  - OS
  - Status
  - User
- **Guest Access**
  - Auth Status
  - Authentication Type
  - Client Type
  - Download Quota
  - Download Quota Balance
  - Guest Access Type
  - Session Expiry
  - Total Quota
  - Total Quota Balance
  - Upload Quota
  - Upload Quota Balance
- **Network**
  - IPv4 Address
  - IPv6 Address

- MAC
- VLAN-ID

- **Wireless**
  - Band
  - Capability
  - Download
  - Radio ID
  - Radio Mode
  - RSSI
  - SNR
  - SSID
  - Upload

Figure 220 *Site > Clients > Wireless Clients*



Wired Clients

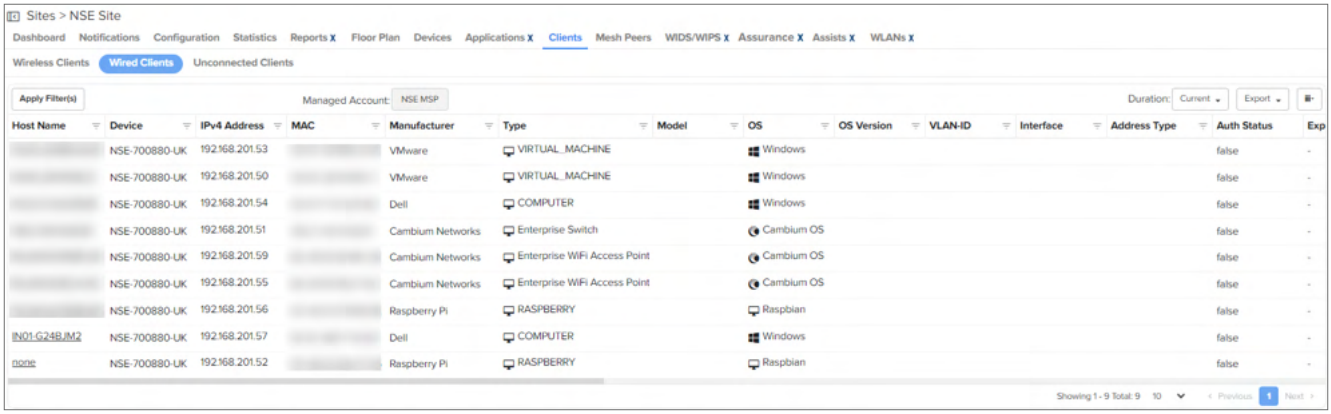
The **Clients** > **Wired Clients** page at the Network- and Site-level displays the following details:

- **General**
  - Address Type
  - Device
  - Device MAC
  - Download
  - Expires
  - Host Name
  - Last Duration
  - Last Seen
  - Manufacturer
  - Model
  - OS
  - OS Version
  - Status

- Type
- Upload

- **Guest Access**
  - Auth Status
  - Authentication Type
  - Client Type
  - Download Quota
  - Download Quota Balance
  - Guest Access Type
  - Portal Mode
  - Session Expiry
  - Total Quota
  - Total Quota Balance
  - Upload Quota
  - Upload Quota Balance
- **Network**
  - Interface
  - IPv4 Address
  - MAC
  - VLAN-ID

Figure 221 *Site > Clients > Wired Clients*



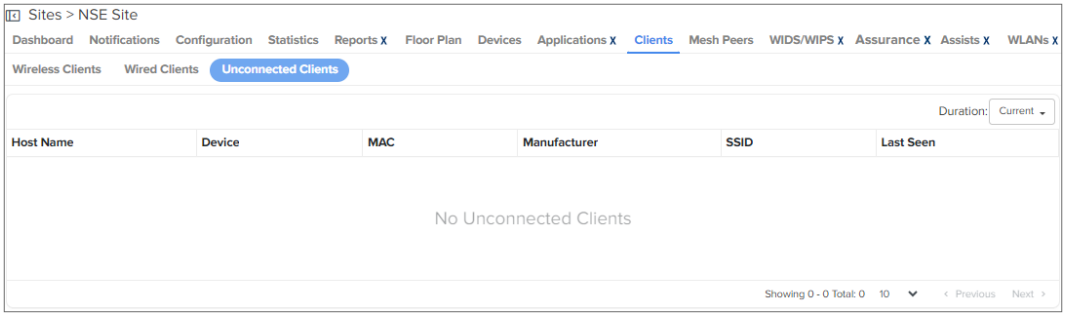
Unconnected Clients

The **Clients** > **Unconnected Clients** page at the Network- and Site-level displays the following details:

- Host Name
- Device
- Last Seen
- MAC (address)

- SSID
- Manufacturer

Figure 222 *Site > Clients > Unconnected Clients*

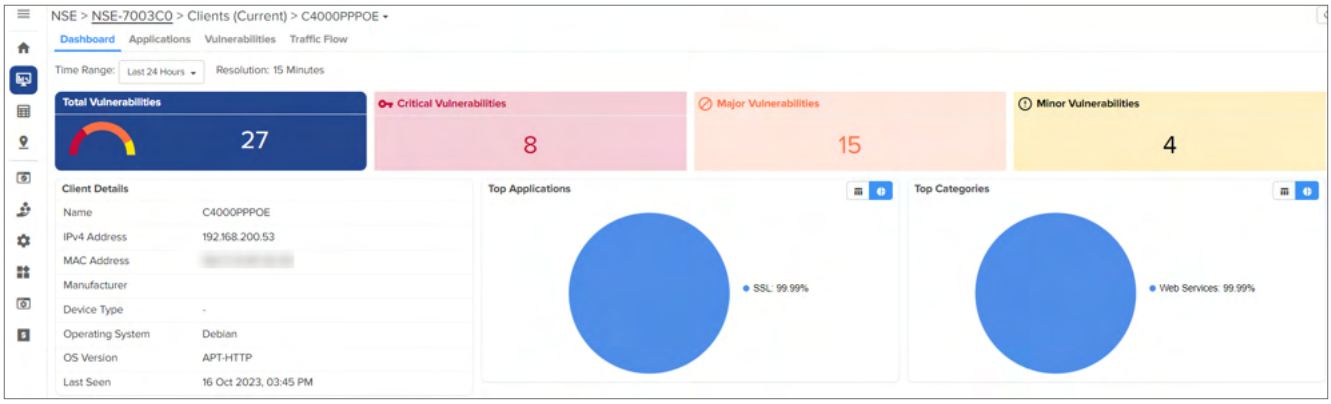


Client-level information

Clients > Dashboard

Dashboard provides overview of the wired and wireless clients usage. Click the pie chart to view specific application usage.

Figure 223 *Client Dashboard*



The following parameters are displayed for NSE Clients:

- Total Vulnerabilities
- Critical Vulnerabilities
- Major Vulnerabilities
- Minor Vulnerabilities
- Client Details
- Top Applications
- Top Categories

Clients > Applications

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



The Application data can be presented most for 24 hours, 7 days, or 30 days.

Note

The NSE devices support up to 256000 concurrent connections.

- **Top Application**: Represent the most used application by the client.
- **Total Bytes**: Represents the sum of Uplink and Downlink traffic across all applications used by the client.
- **Top Category**: Category of the top application used by the client.

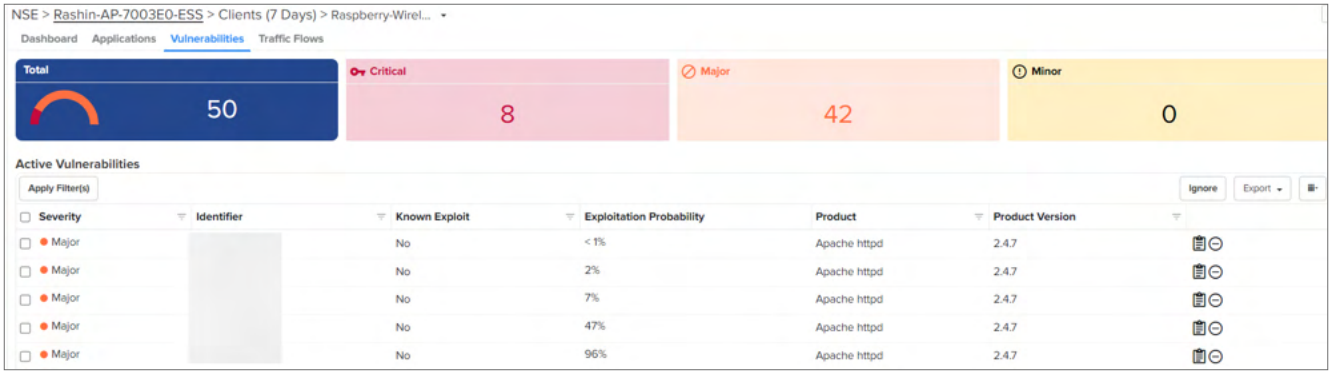
Table 57 *Parameters on the Applications page*

Field	Description
Application Name	Name of the application.
Category	Category of the application.
Downlink	Total number of downlink bytes during the selected period.
Uplink	Total number of uplink bytes during the period selected.
Total Bytes	Total amount of application data (uplink plus downlink).
Usage	The percentage of usage by this application in comparison to all applications.

Clients > Vulnerabilities

The **Vulnerabilities** page displays the vulnerabilities discovered for the client by the NSE. Vulnerabilities are categorized as Minor, Major, and Critical.

Figure 224 *Vulnerabilities dashboard*



Clients > Traffic Flows

Traffic flows can be referred to as a current snapshot of existing flows. The flow direction can be either LAN to WAN or WAN to LAN.

Note

The NSE devices support up to 256000 concurrent connections.

The **Traffic Flows** page displays the active connections or flows of a client, as shown in Figure 225.

Figure 225 *The Traffic Flows page*



Table 58 *Parameters on the Traffic Flows page*

Parameter	Description
Source IP	Source IP address of the device or endpoint, based on the flow direction. If the flow direction is from LAN to WAN, the source IP address is the source IP address of the device. If the flow direction is from WAN to LAN, the source IP address is the source IP address of the endpoint to which the device has connection to.
Source Port	Source port number.
Destination IP	Destination IP address of the device or endpoint, based on the flow direction. If the flow direction is from LAN to WAN, the destination IP address is the destination IP address of the endpoint. If the flow direction is from WAN to LAN, the destination IP address is the destination IP address of the device.
Destination Port	Destination port number.
Application	Name of the application.
Tx Packets	Transmitted packets.
Tx Bytes	Transmitted bytes.
Rx Packets	Received packets.

Table 58 *Parameters on the Traffic Flows page*

Parameter	Description
Rx Bytes	Received bytes.
TTL	Time to live. Time period during which a session or connection is active.
NAT'ed IP	IP address after the Network Address Translation (NAT) process.
NAT'ed Port	Port number after the NAT process.
Direction	Direction of the communication, indication whether it is incoming or outgoing. Outgoing: LAN to WAN Incoming: WAN to LAN
State	Current state of a connection. The following connection states are valid only if the protocol is TCP. • SYN_SENT • SYN_RECV • ESTABLISHED • FIN_WAIT • CLOSE_WAIT • LAST_ACK • TIME_WAIT • CLOSE
Protocol	Name of the protocol, such as TCP, UDP, ICMP, or any.

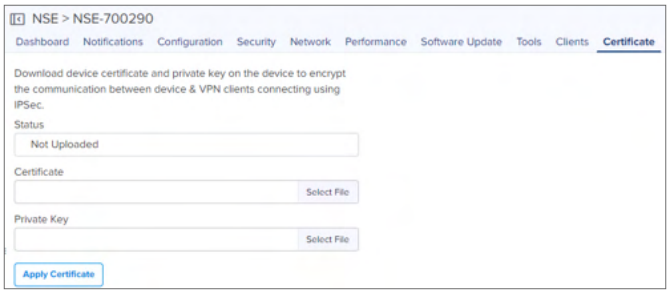
Certificate

To secure the communication between an NSE device and the VPN clients, you can encrypt the communication. To apply the encryption certificate, navigate to **NSE > Certificate**, upload the certificate and the key files, and then click **Apply Certificate**.

Note

Only certificates with **.der** and **.pem** file extensions are accepted.

Figure 226 *The Certificate page*



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 227 *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

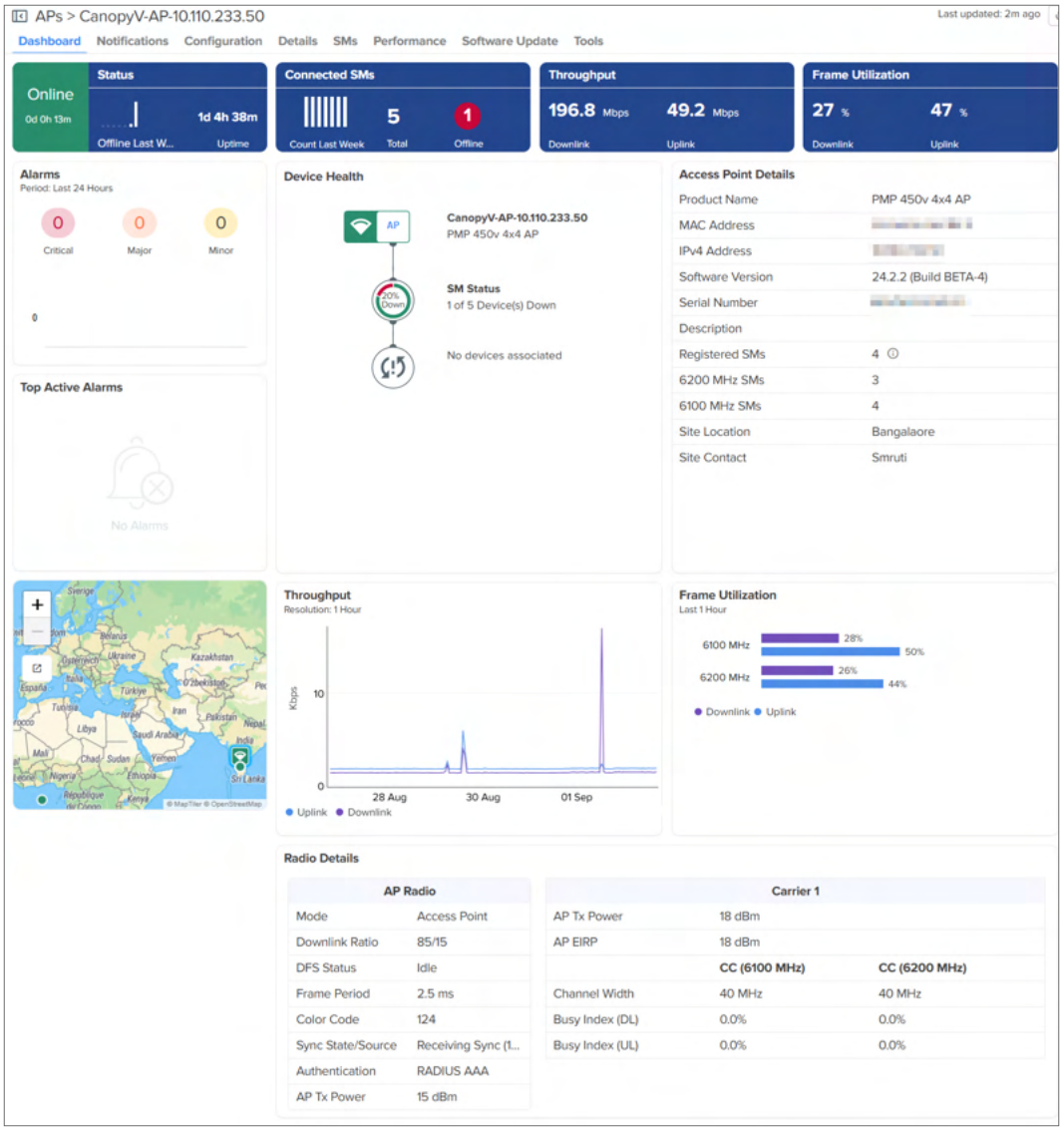
For more details about the difference between Carriers and CCs, refer to Configuring Radio Parameters in the PMP 450 Series Configuration Guide.

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.

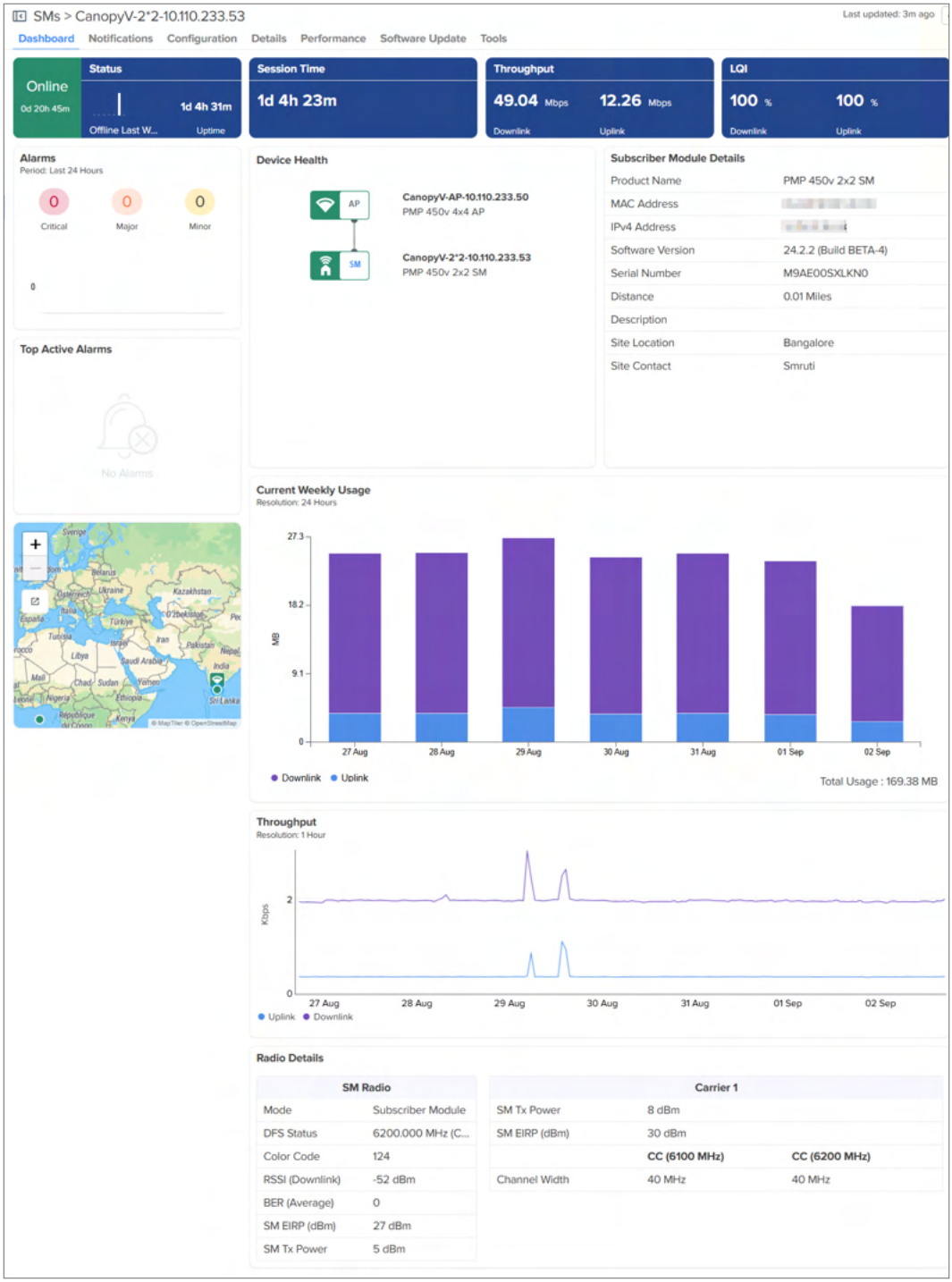
Figure 228 *PMP 450v 4x4 AP/BHM dashboard*



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.

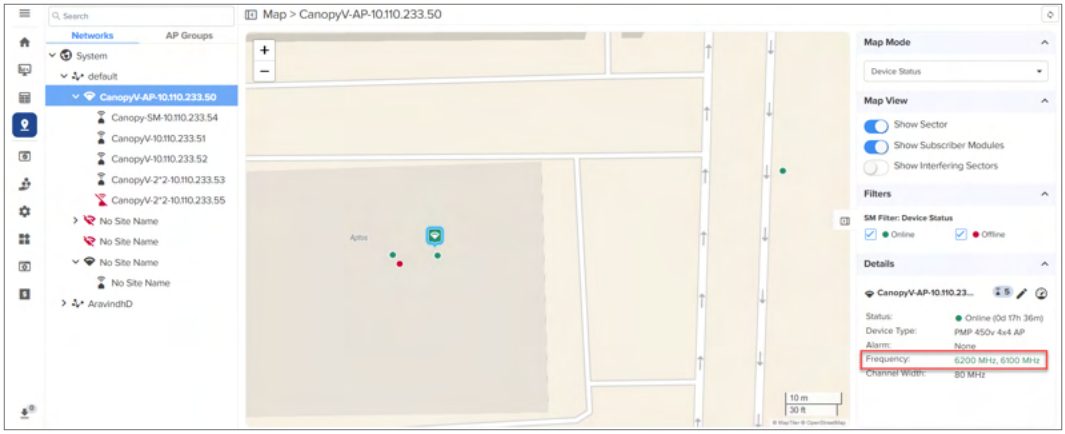
Figure 229 *PMP 450v 4×4 SM/BHS and PMP 450v 2×2 SM/BHS dashboard page*



PMP 450v 4×4 AP/BHM Map View

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

Figure 230 *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
- WLANs Dashboard

Wi-Fi Monitoring

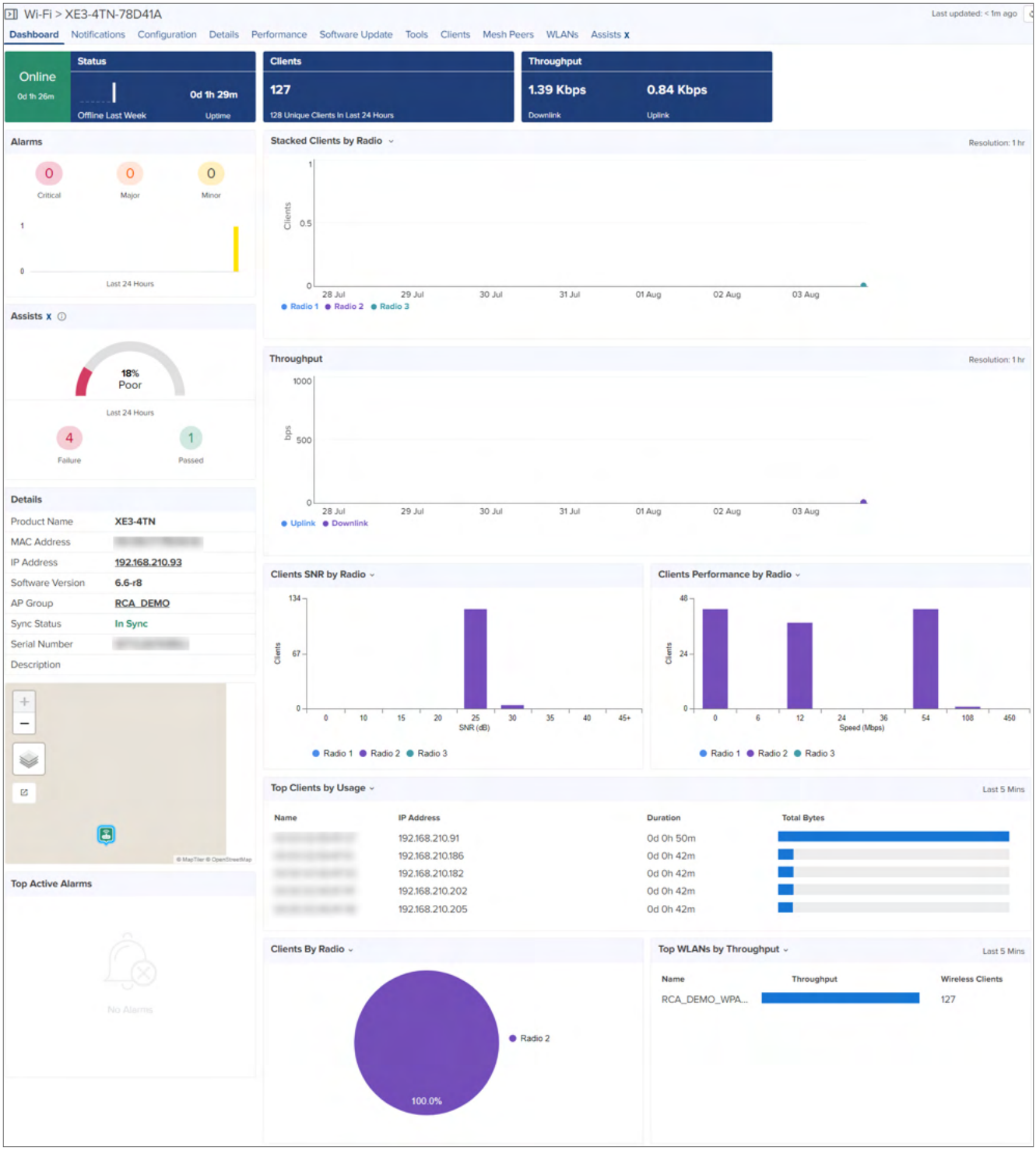
The Wi-Fi Monitoring pages include the following:

- Dashboard
- Clients
- Details
- Mesh Peers

Dashboard

The cnPilot Dashboard displays **Stacked Clients by Radio, Stacked Clients by Band, Clients by Radio, Clients by Band, Details, Status, Throughput, Top Active Alarms, Top Clients by Usage, Top Clients by Session, Top WLANs by Clients,** and **Top WLANs by Throughput**.

Figure 231 *Device > Dashboard*



Clients

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

Note

- Clients' historical data is available at the System-, site-, and AP-level for 24 Hours, 7 Days, and 30 days for cnMaestro X users.

- This is applicable for Wireless Clients and Unconnected Clients only.

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 Address
- Manufacturer
- Radio ID
- RSSI
- SSID
- Upload

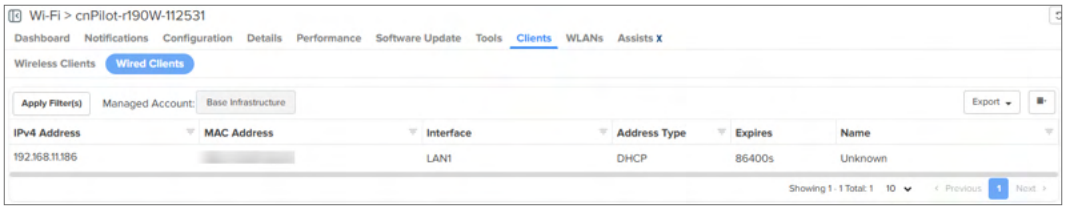
Figure 232 *cnPilot Home: Device > Clients > Wireless Clients*



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 Address
- Name

Figure 233 *cnPilot Home (R-Series): Device > Wired Clients*

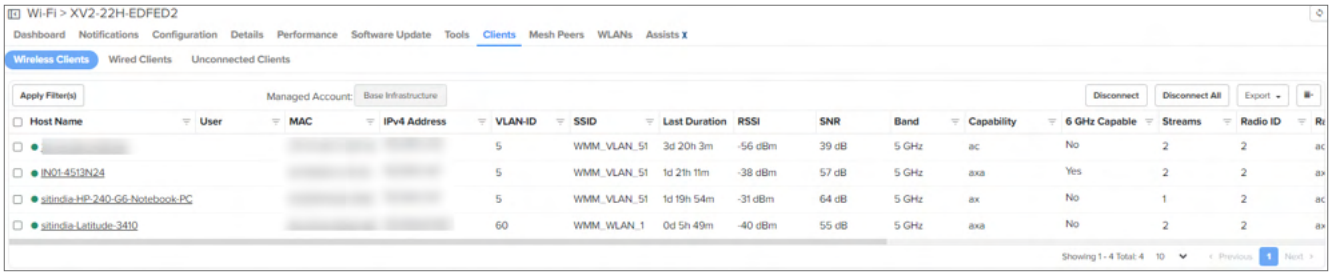


The following parameters are displayed for wireless clients connected to Enterprise Wi-Fi APs (E-, XE-, XV-, and X7-Series):

- 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 234 *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 235 *Enterprise Wi-Fi: Device Wired Clients*

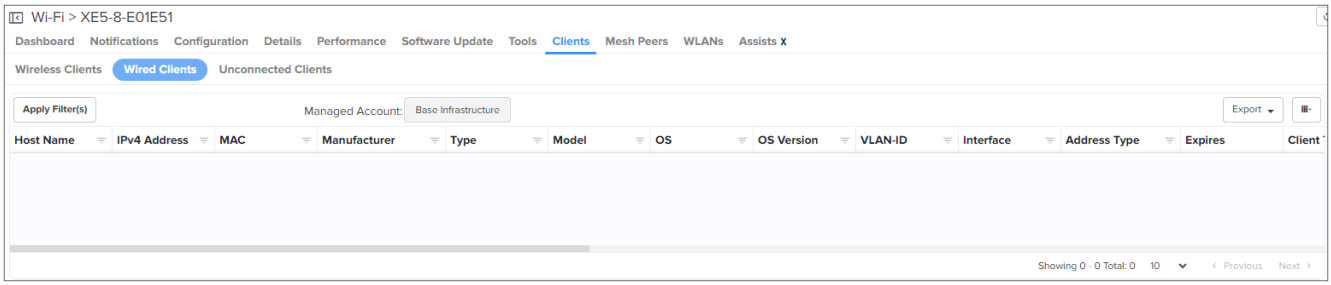
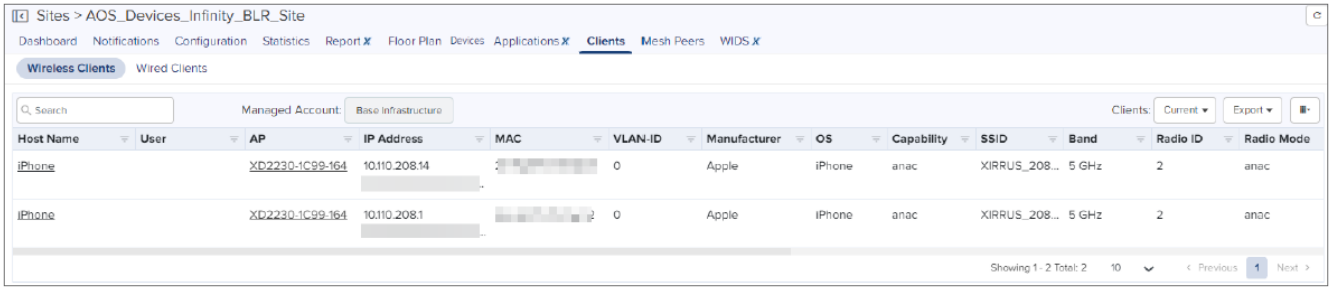


Figure 236 *Enterprise Wi-Fi (Xirrus-Series) Wireless Clients*



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):

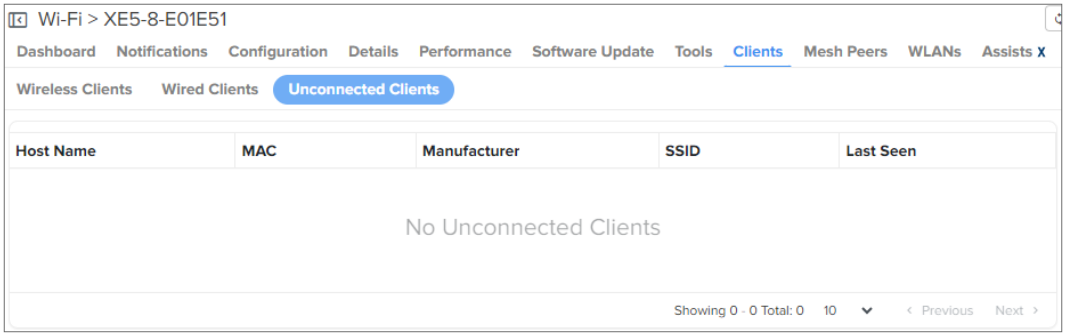
Note

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

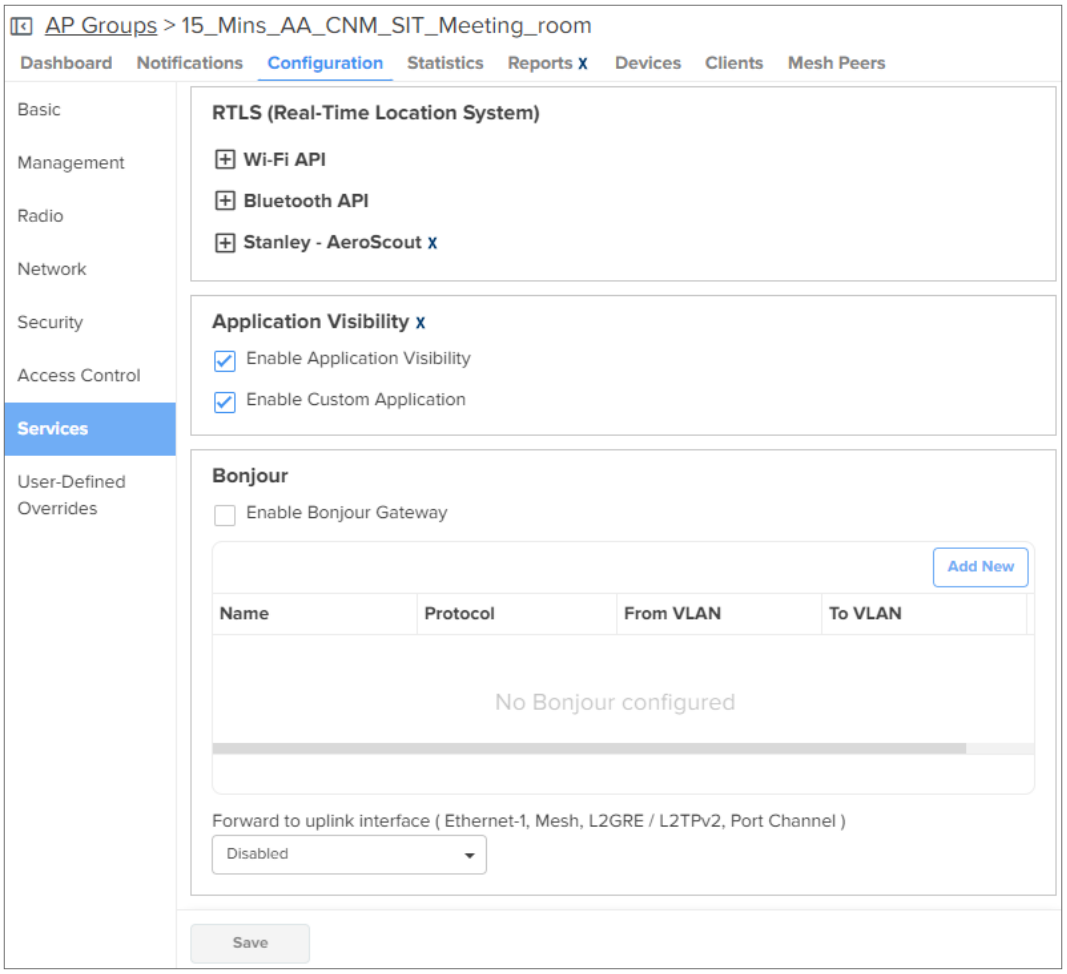
- Host Name
- MAC
- Manufacturer
- SSID
- Last Seen

Figure 237 *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.



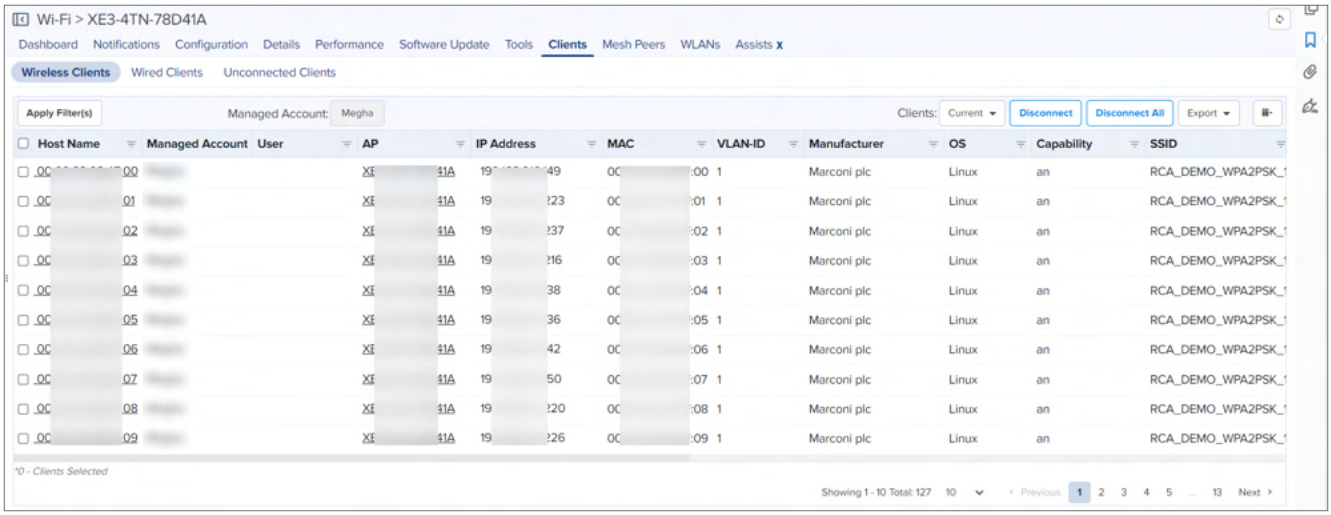
The Client Dashboard displays the details of the clients connected to the Wi-Fi device.

Note

- Enable the **Application Visibility** feature to view **Application** page. It is supported only for XE, XV, X7 series devices.
- **Dashboard** is supported for all cnPilot devices.
- The historical clients data is available for 24 hours, 7 days, and to a maximum of 30 days for

cnMaestro X users.

Figure 238 *XE, XV, and X7 Series: Device Dashboard Wireless Clients*



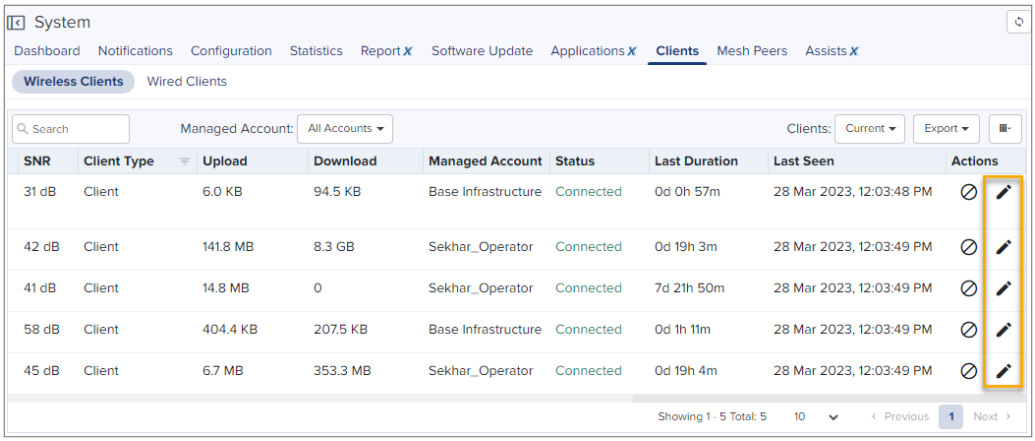
To view the **Dashboard**, navigate to **Clients** > **Wireless Clients** and click a value in the **Host Name** column.

A detailed **Client Dashboard** page is displayed.

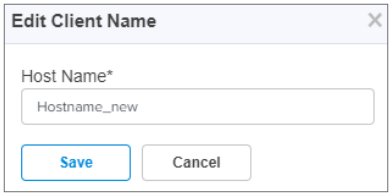
Renaming Client Host-names

You can assign friendly host-names for the clients. To edit the host-name of connected wired or wireless client, follow these steps:

1. Navigate to **Clients** > **Wireless Clients** or **Wired Clients** tab.



2. Scroll to the right most side of the clients list and click on the **Edit** icon under the **Actions** column.
3. In the **Edit Client Name** pop-up window, enter a friendly name for the client.



4. Click **Save**.

The new host-name is displayed in all the places such as the Client Dashboards, Audit logs, and Reports.

Application Visibility

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

The Application data is available for a duration of 24 hours, 7 days, and 30 days at all levels—System, MSP, Network, Site, and AP.

- **Top Application**: displays the most used application by traffic.
- **Total Bytes**: displays the sum of the uplink and downlink traffic across applications.
- **Top Category**: displays the most used application category.
- **Top Client**: displays the client that has utilized the most traffic.

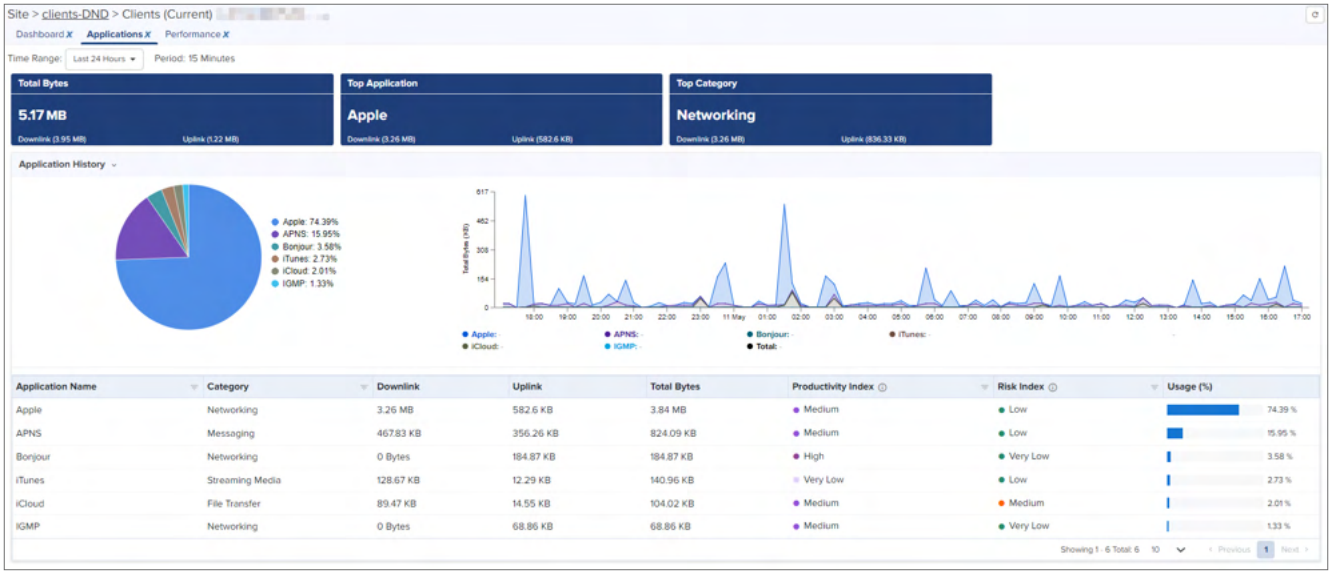
> **Note**
>
> - The graphical Client Dashboard is only available in cnMaestro X.

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.

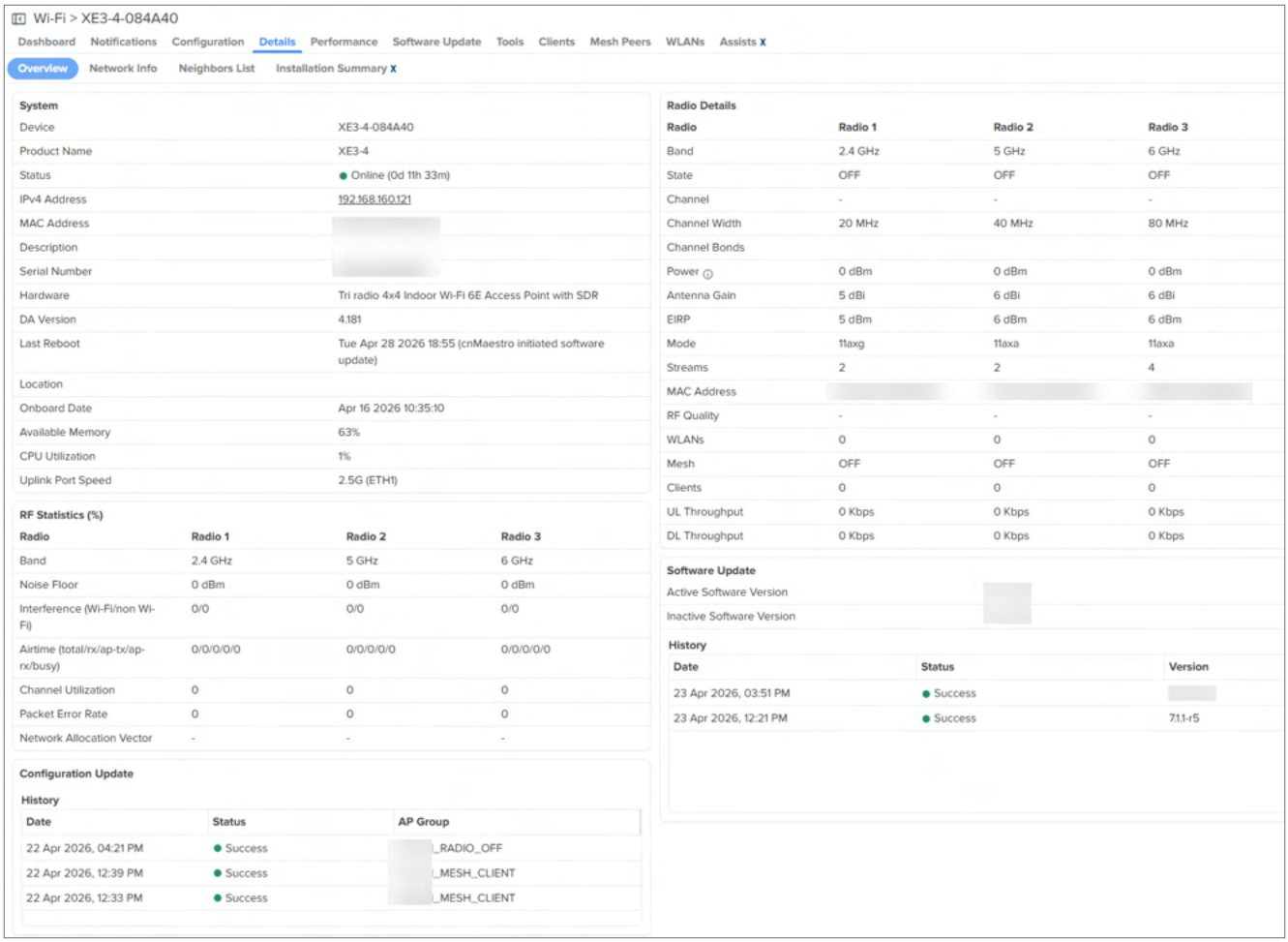
Table 59 *Application fields*

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.



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.

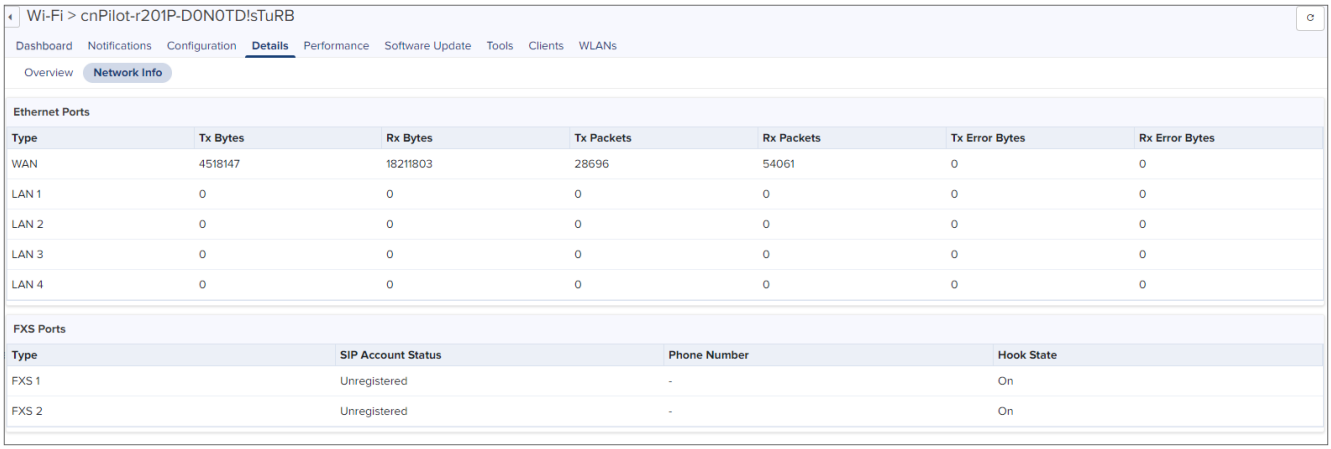
Network Info

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

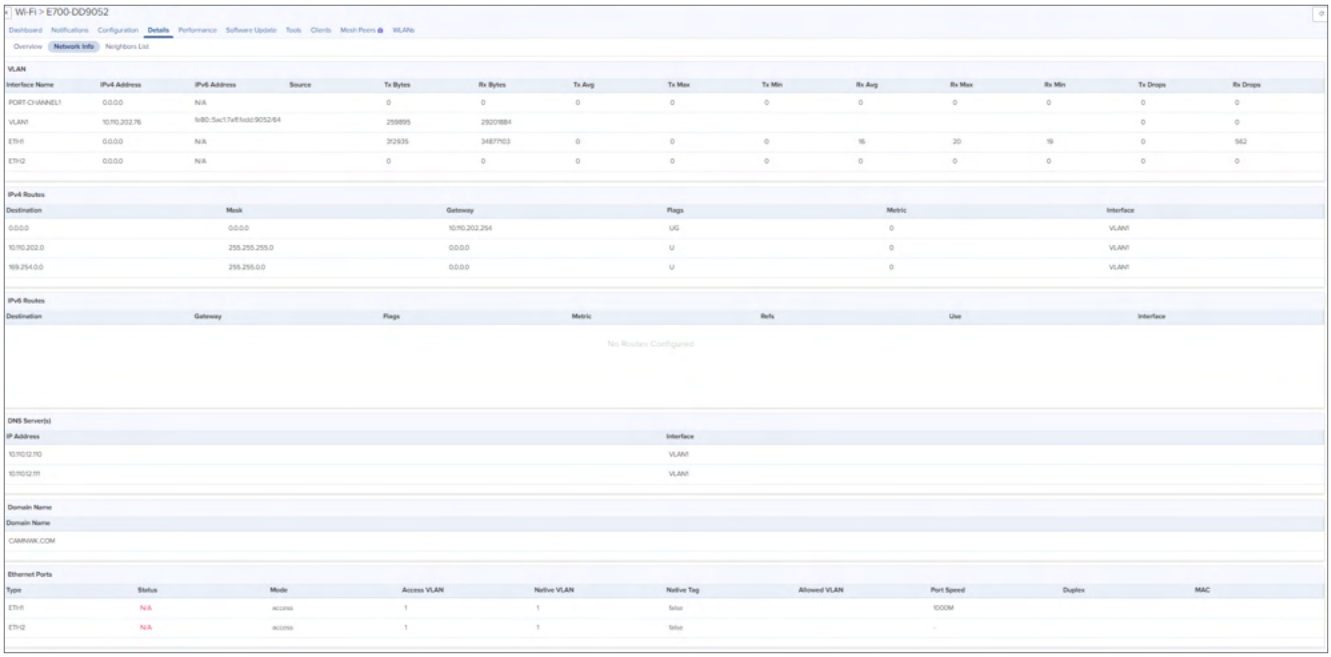
- Hook State
- Phone Number
- SIP Account Status
- Type

Figure 239 *cnPilot Home: Device > Details > Network Info*

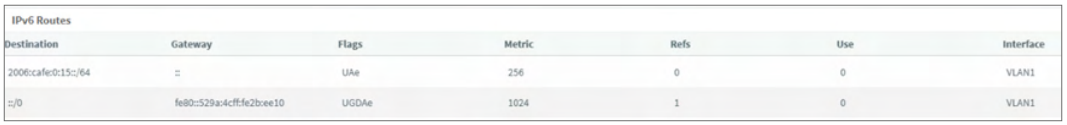


- Ethernet Ports
- PPPoE
- Routes
- Tunnels
- VLAN Pool

Figure 240 *Enterprise Wi-Fi: Device >Details > Network Info*



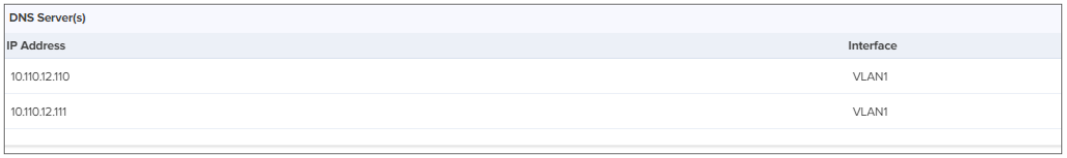
IPv6 Routes



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

The following parameter details are displayed in E-Series:

- Port
- Rx Broadcasts
- Rx Frames
- Rx Frames Oversize
- Rx Frames Undersize
- Rx Frames with Error
- Rx Octets
- Tx Broadcasts
- Tx Frames
- Tx Octets

Figure 241 *Enterprise Wi-Fi (Xirrus-Series): Device > Dashboard > Network Info*

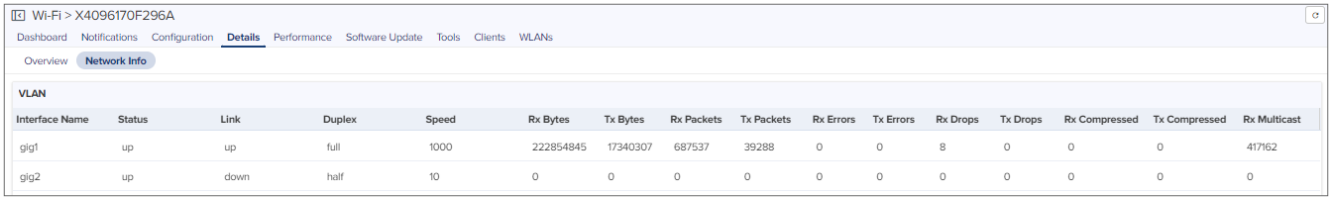
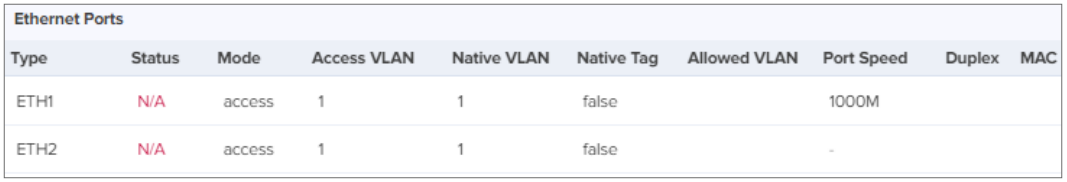


Figure 242 *PTP 650/670/700: Device >Details > Network Info*



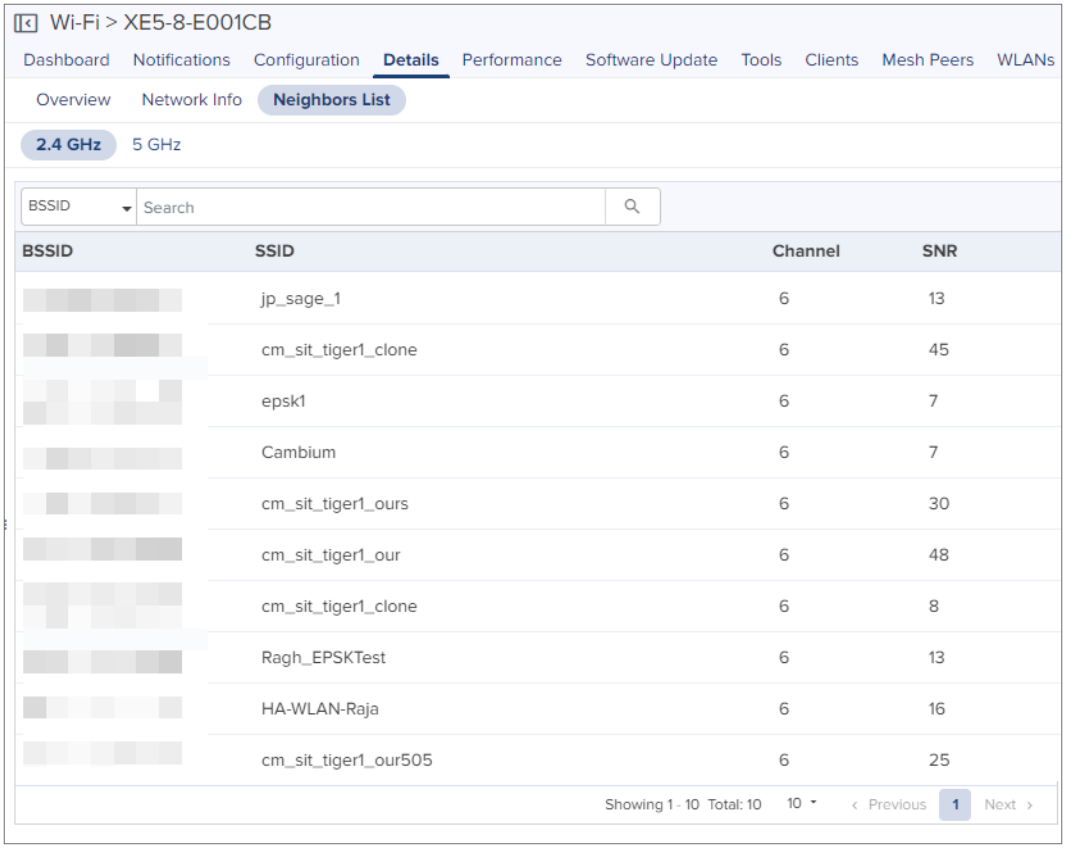
Ethernet Ports

Type	Status	Mode	Access VLAN	Native VLAN	Native Tag	Allowed VLAN	Port Speed	Duplex	MAC
ETH1	N/A	access	1	1	false		1000M		
ETH2	N/A	access	1	1	false		-		

Neighbors List

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

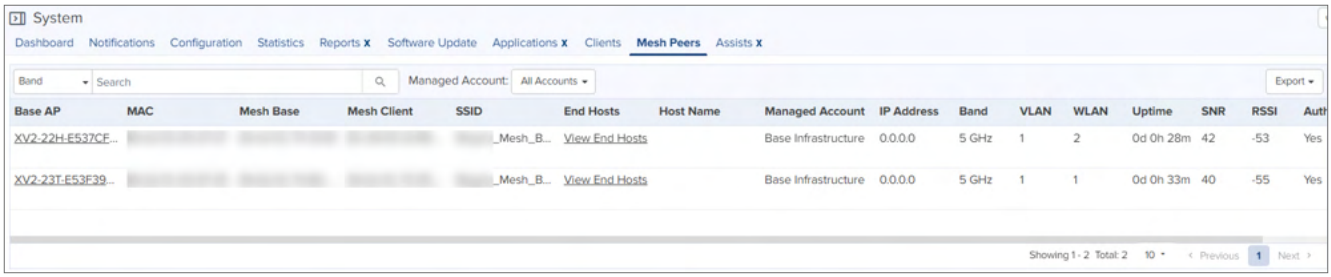
Figure 243 *Neighbors List*



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 244 *Device > Mesh Peers*



Roaming History for Mesh Peers

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

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

A detailed Information and Roaming History window pops up.

Figure 245 *Mesh Peers > Host Name > Information*

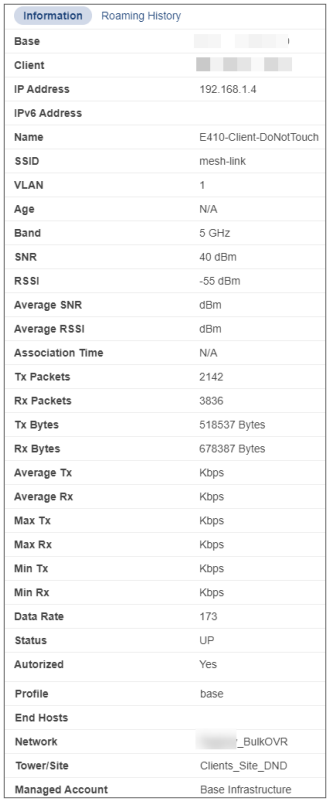
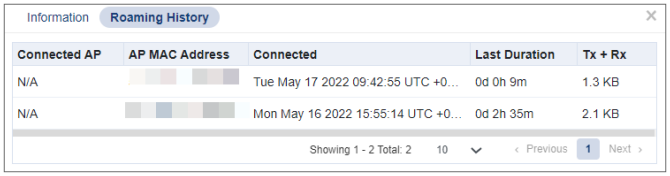
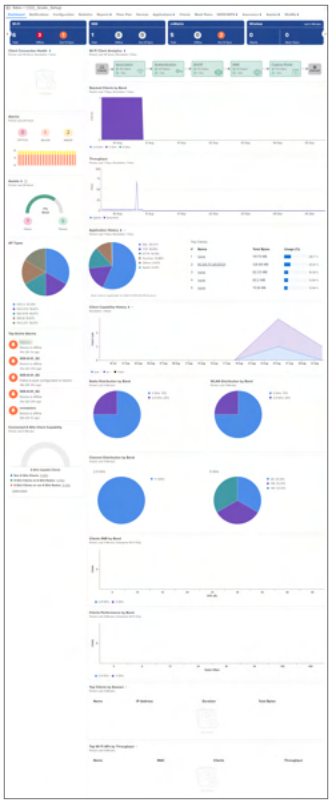


Figure 246 *Mesh Peers > Host Name > Roaming History*



Site Dashboard

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



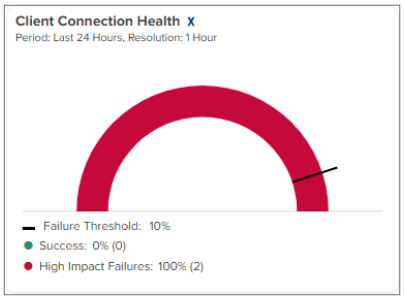
The Site Dashboard displays the following graphics:

- Client Connection Health X
- Wi-Fi Client Analytics X
- Assists X
- Alarms
- Top Active Alarms
- AP Types
- Stacked Clients by Band
- Channel Distribution by Band
- Clients Performance by Band (Enterprise Wi-Fi)
- Clients SNR by Band (Enterprise Wi-Fi)
- Connected 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

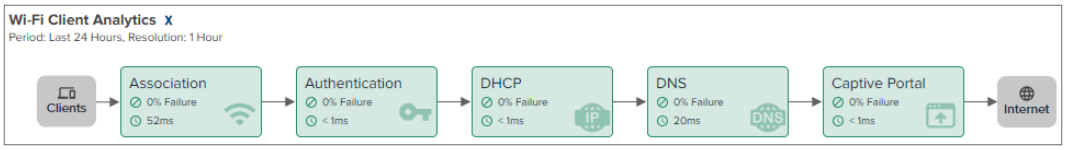
Displays the percentage of success and failed client connections in that site.



Wi-Fi Client Analytics X

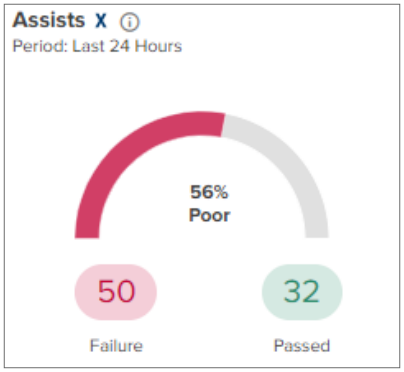
Displays the failure percentage in each stage of the client connection to the AP and subsequent network access.

For more information, refer to Assurance X.



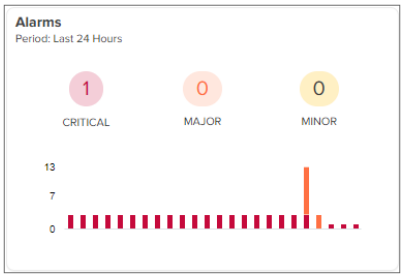
Assists X

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.



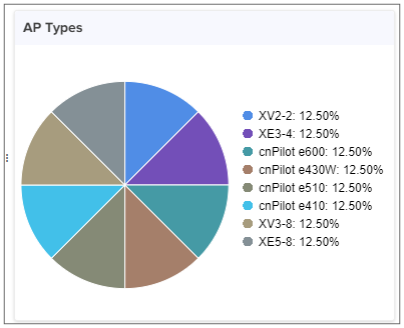
Top Active Alarms

Displays the topmost active alarms raised in that Site.



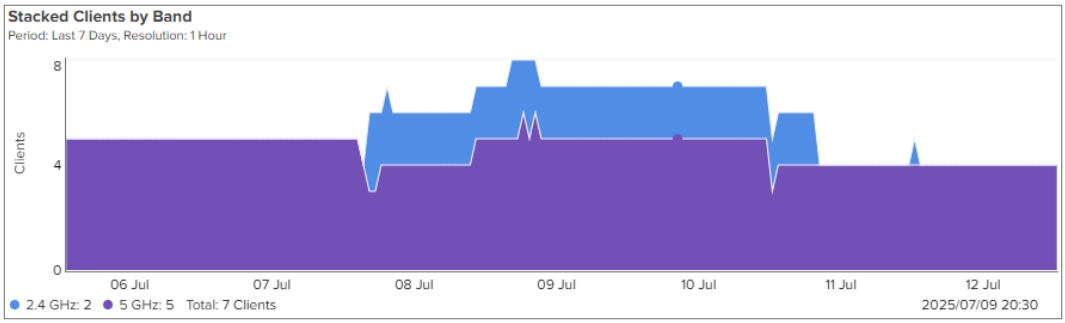
AP Types

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



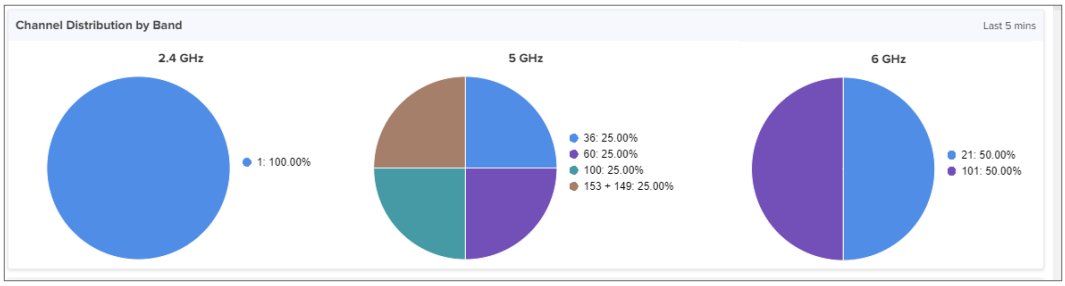
Stacked Clients by Band

Displays the number of clients connected to the APs per radio band that is supported.



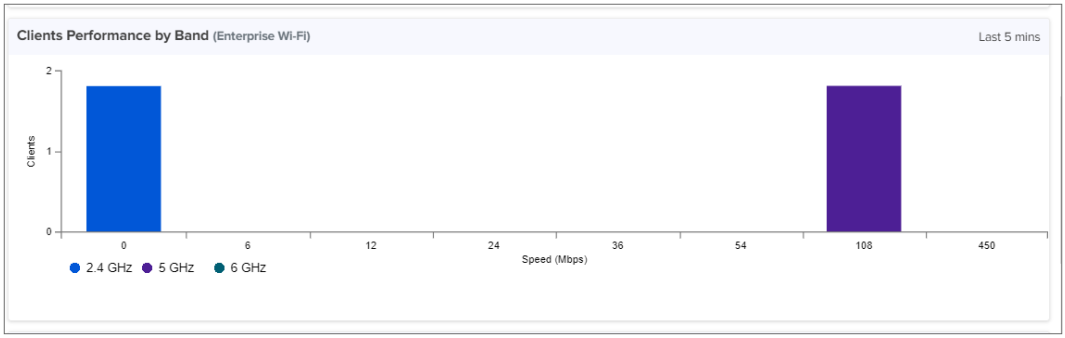
Channel Distribution by Band

Channel distribution displays usage of channels in 2.4 GHz, 5 GHz and 6 GHz. This helps in planning and implementing WLANs within a high-density environment. It displays the usage details for last 5 minutes.

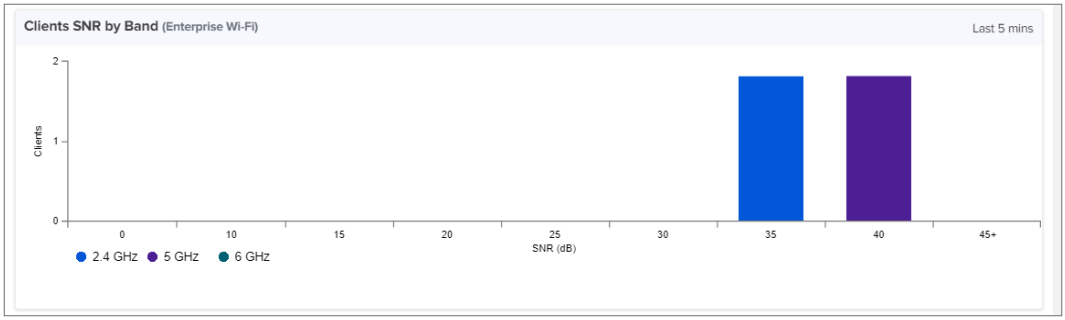


Clients Performance by Band (Enterprise Wi-Fi)

Clients performance details is displayed for last 5 minutes.



Clients SNR by Band (Enterprise Wi-Fi)



Connected 6 GHz Client Capability

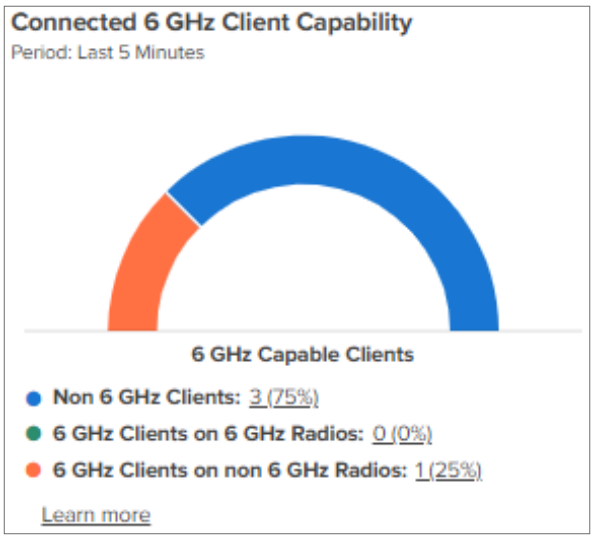
The Connected 6 GHz Client Capability widget presents a point-in-time view of Wi-Fi 6 GHz clients associating to non-6 GHz radios. These clients may experience better service if SDR radios are upgraded from 5 GHz to 6 GHz. A high percentage of 6 GHz capable clients connecting to non-6 GHz radios is an 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 247 *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 (NSE/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.

Clicking on the clients in the **Top Clients** sections displays the Site-specific **Client Dashboard** page. For more details, refer to Viewing a client or host-specific connection or disconnection event.



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 248 *Clients History in line chart*

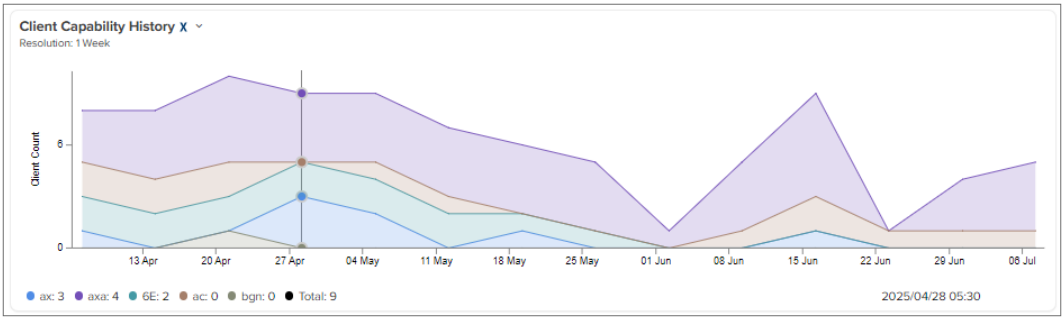
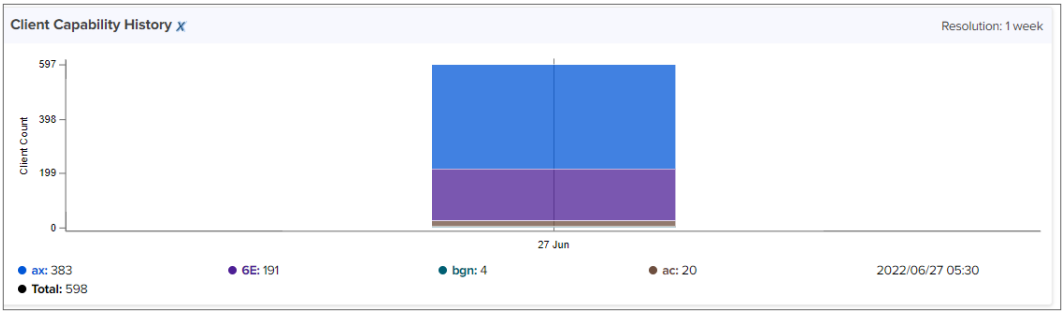
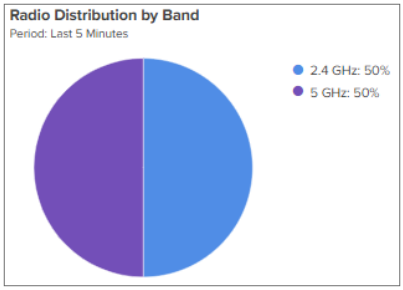


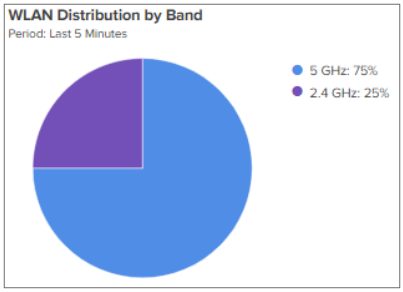
Figure 249 *Clients History in bar chart*



Radio Distribution by Band



WLAN Distribution by Band



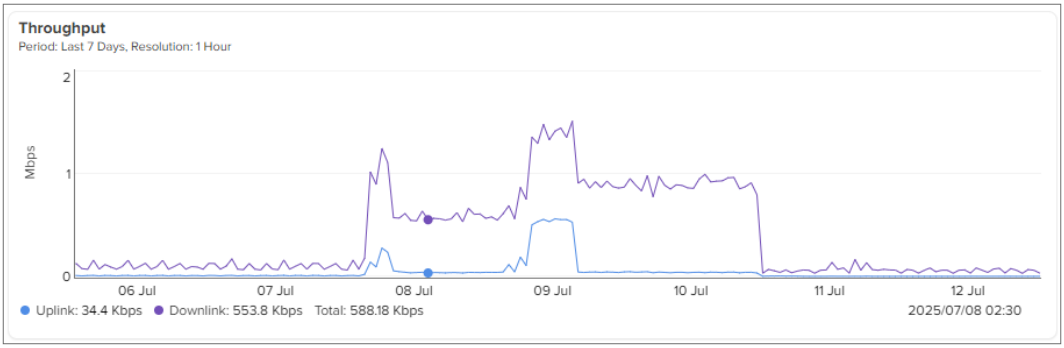
Throughput

Displays aggregated throughput for all the clients.



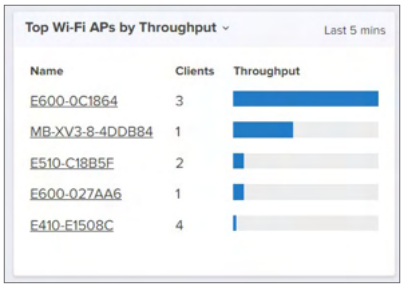
Throughput Graph

Throughput graph displays client traffic for the last week.



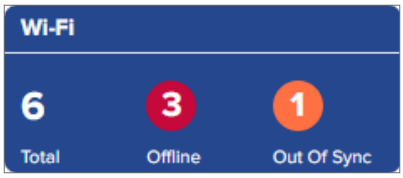
Top Wi-Fi APs by Throughput or Clients

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.

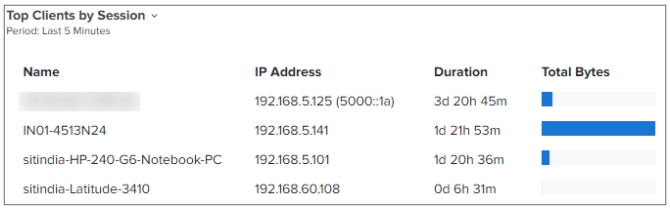


- **Total**—Click the number to display the **Sites** > **Devices** > **List** page with the device type filter applied.
- **Offline**—Click the number to display the **Sites** > **Devices** > **List** page with the **Status** filter applied as **Offline**.
- **Out Of Sync**—Click the number to display 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**.

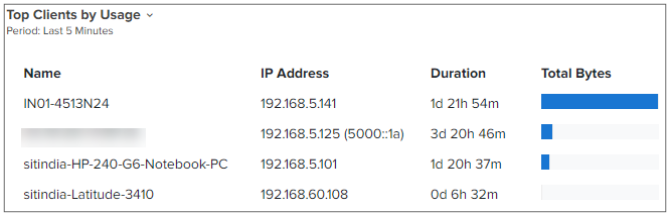
Top Clients by Session

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.

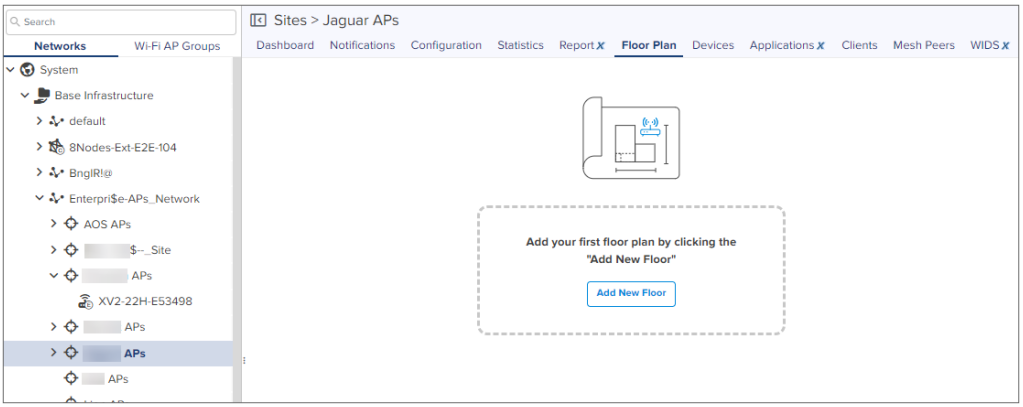
To create a floor plan, perform the following steps:

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.

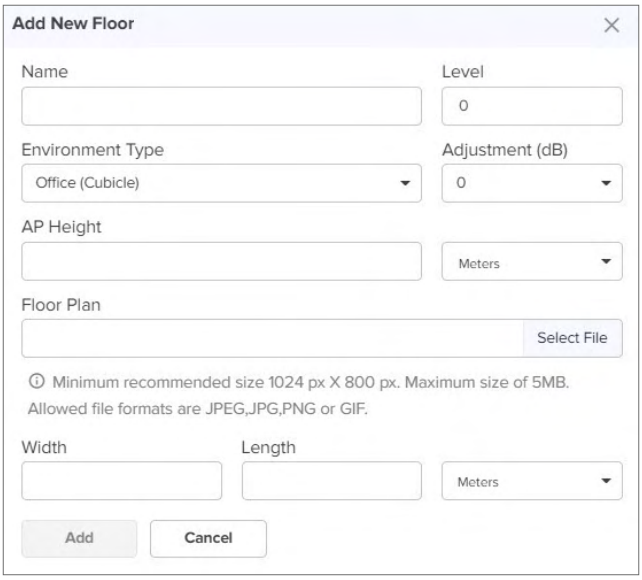


Table 60 *Fields in Floor Plan*

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.

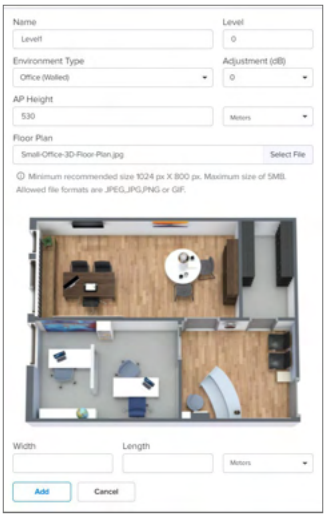
Note

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

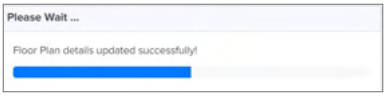


Note

- 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 more than one floor plan.
- You cannot duplicate the floor level for other floor plans.
- If the devices are in a default location and upgraded to 3.1.1, the devices are moved to the **Unmapped Devices** option.

The right pane of the Floor Plan window provides details of uploaded floor plans, such as Floor View, Map Opacity, Radio Details, Filters, and the devices in the floor plan.

Figure 250 *Configure Floor Plan*

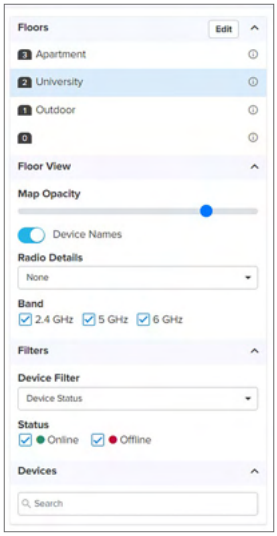


Table 61 *Fields to configure floor plan page*

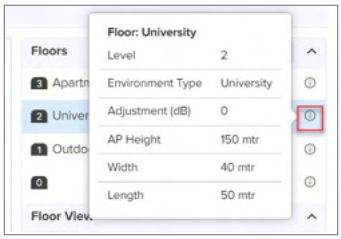
Field	Description
Floors	Indicates the floor level. The following actions are available: • Click **Add** to add new floor level. Drag and drop the selected devices from the right pane to the required floor level. If multiple floor levels are available, then select required floor level from the dropdown. • 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 61 *Fields to configure floor plan page*

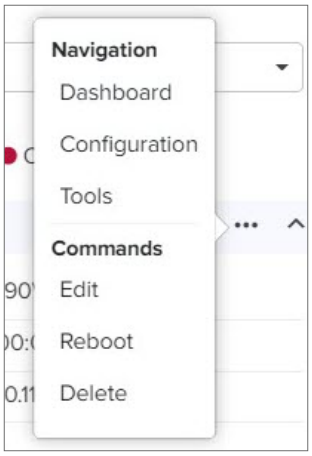
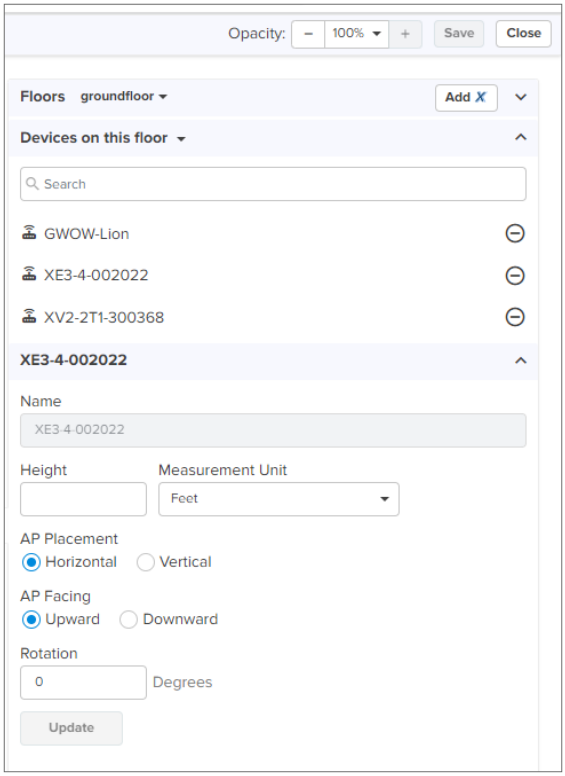
Field	Description
Filter	Filter devices by Device Status, Channel, and Power.
Devices	View and edit the device details. The following actions are available: • Select the device on the floor plan or type the device name in the search field. • Click the eye icon ( ) to **Show** or **Hide** the device on 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 61 *Fields to configure floor plan page*

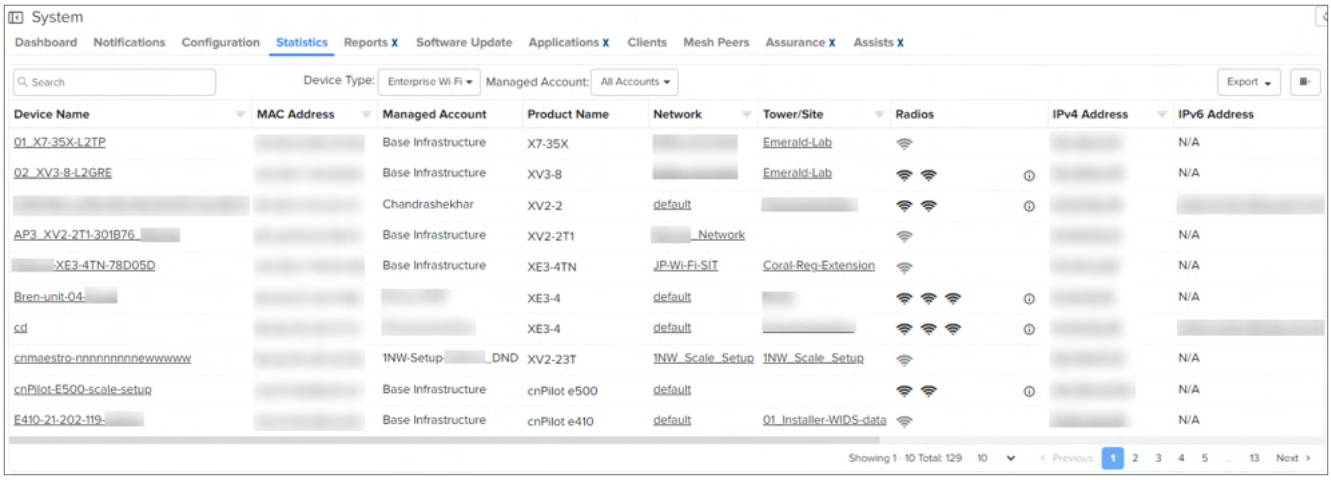
Field	Description
	 Edit the **AP Placement**, **AP Facing** and **Rotation** options. • Click **Update** and **Save.** • Click **Remove** (⊖) icon to remove device from the floor plan. • Click **Save**.

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

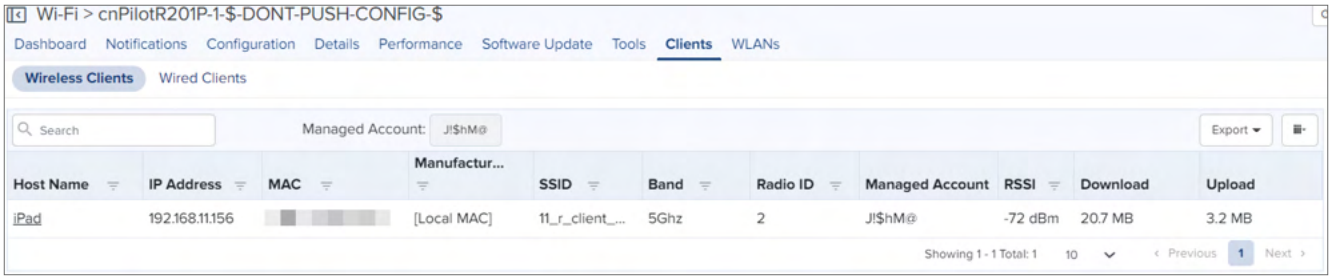


Wireless Clients

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.



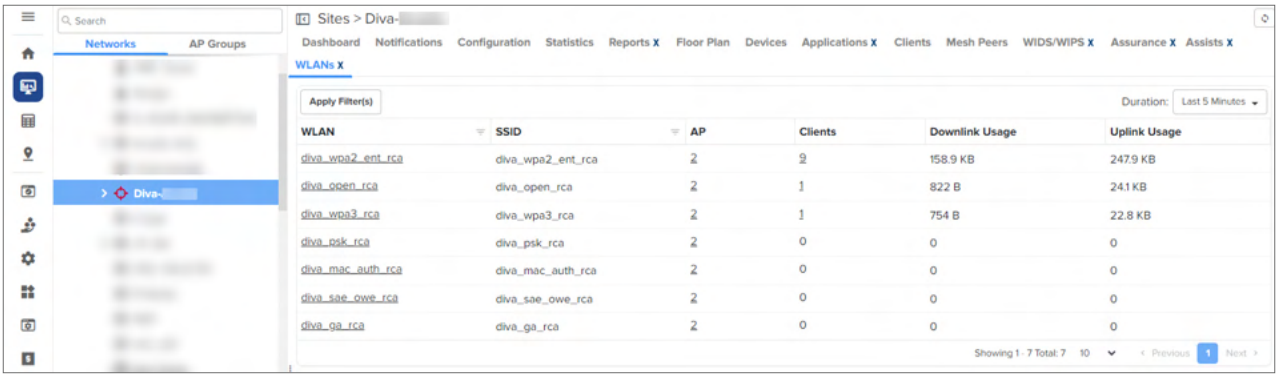
WLANs Dashboard

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 251 *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.

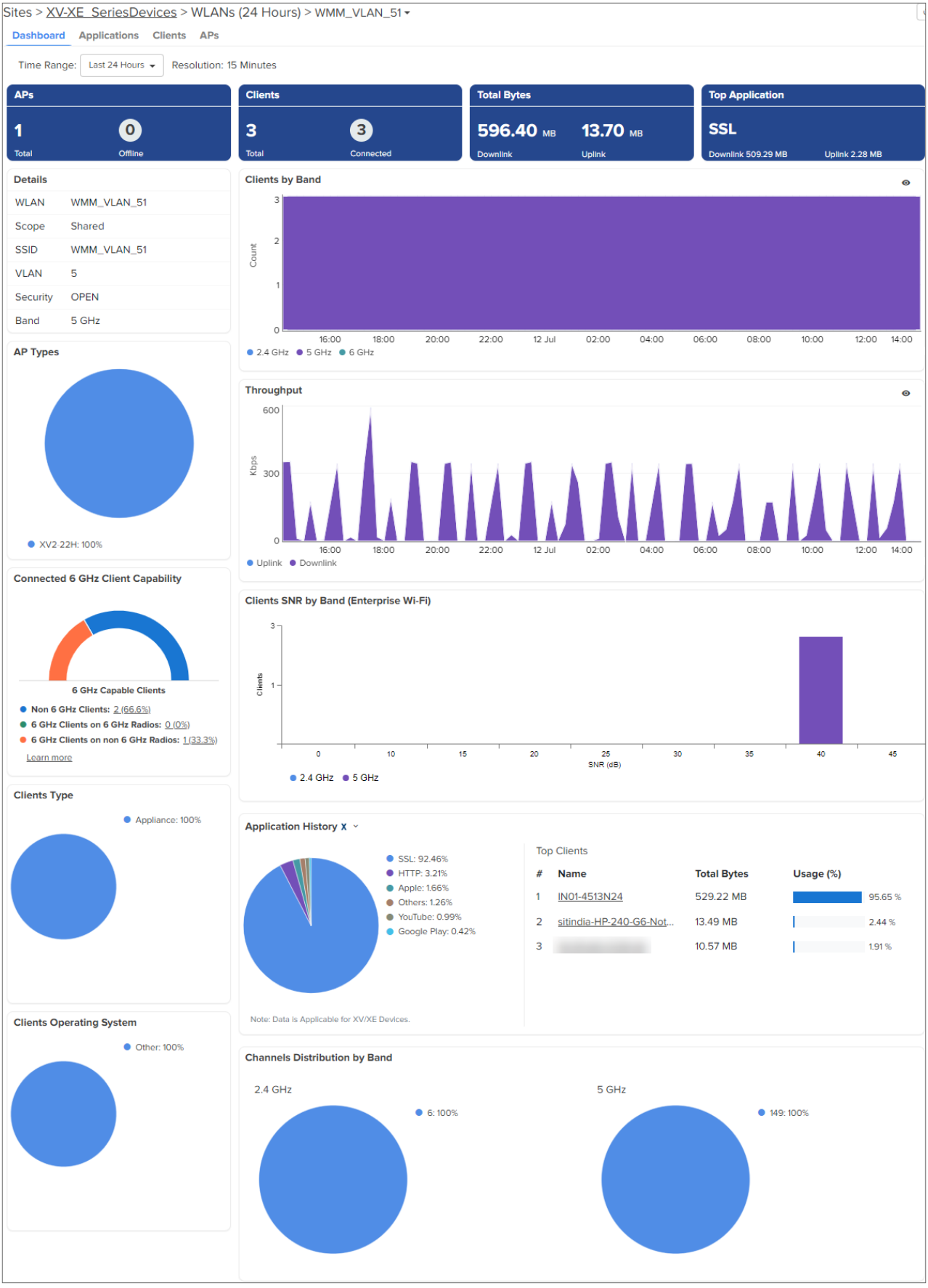
- Click a WLAN in the WLANs page to view the WLAN-specific dashboard.

  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 252 *WLAN-specific Dashboard*



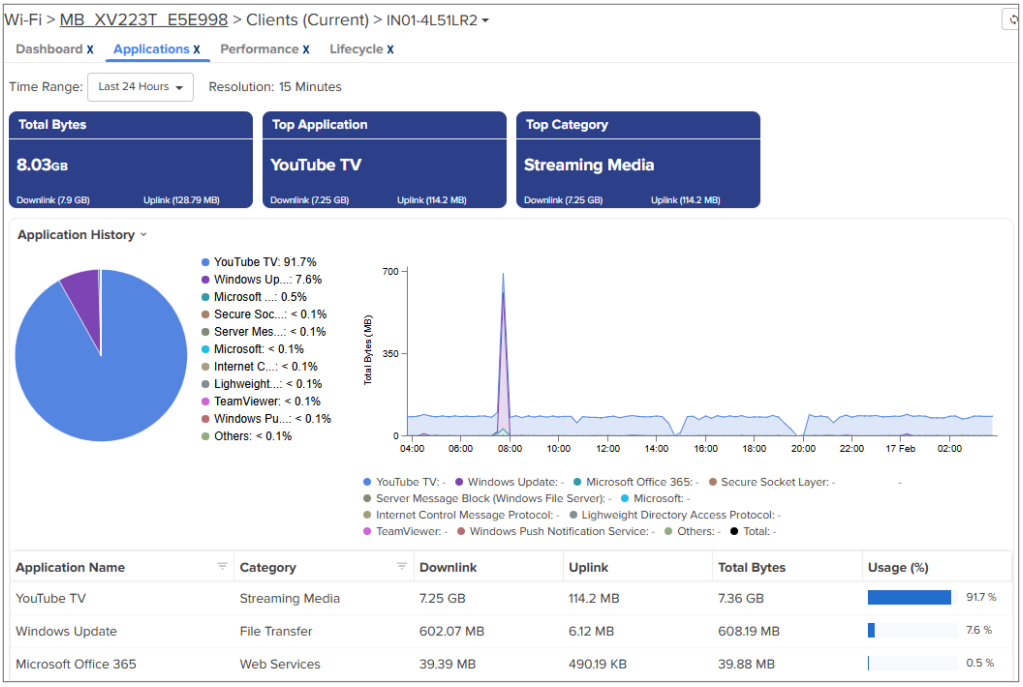
- To view the details of the applications accessed through this WLAN, click the **Monitor and Manage** > ***<Site-Name>*** > **WLANs**[X] > <WLAN-Name> > **Applications** tab.

  The **Applications** dashboard displays both a graphical data and details in a table with the following fields:

Table 62 *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.

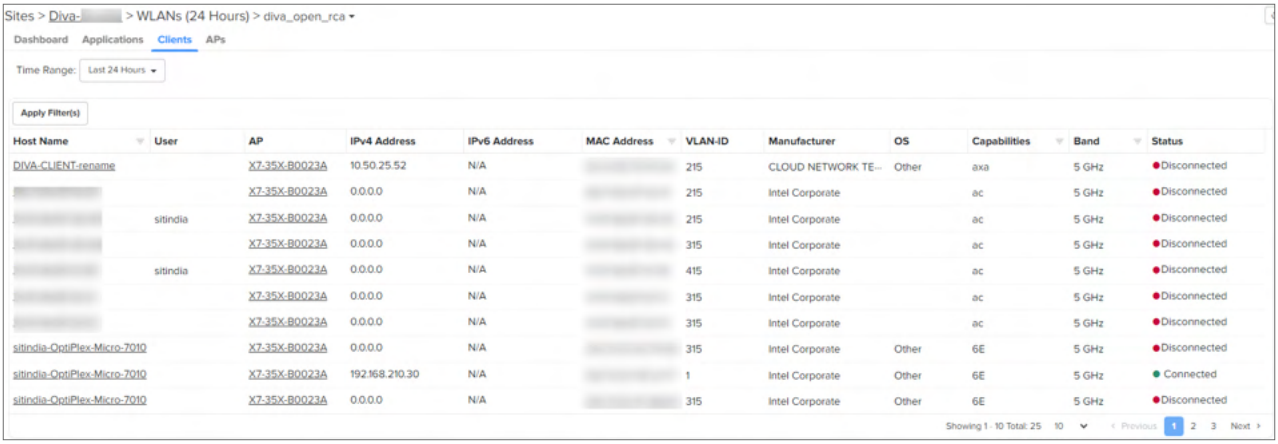
Figure 253 *WLAN-specific Application Dashboard*



- 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 254 *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 255 *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 256 *Fiber OLT dashboard*



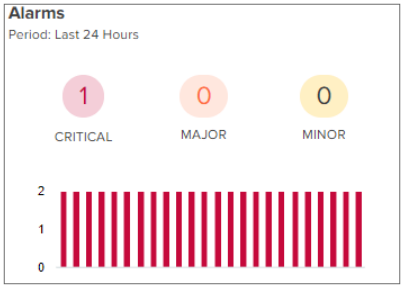
Dashboard has the following elements:

- 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

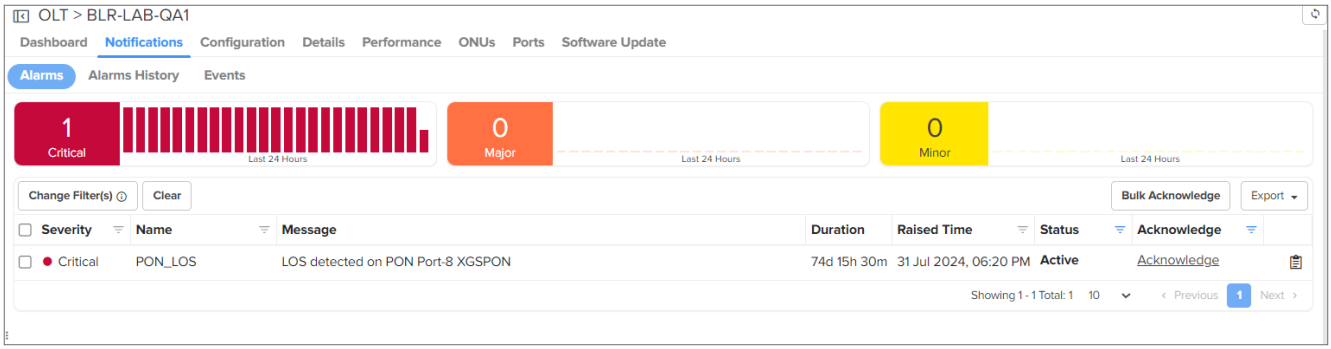
Alarms

Displays the critical, major, and minor alarms. Figure 257 shows the status of the alarms.

Figure 257 *Alarms*



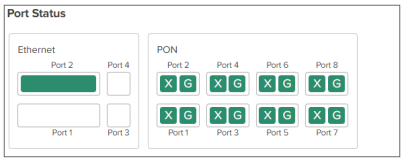
To view the detailed information, click on the respective alarm count.



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.

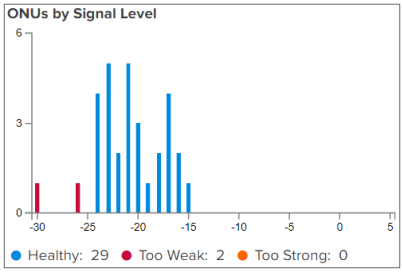
Figure 258 *Port status*



ONU by Signal Level

Displays the signal level received by the ONU.

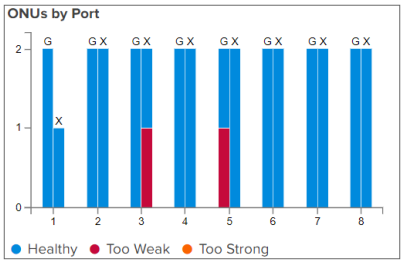
Figure 259 *ONU by signal level graph*



ONU by Signal Level per Port

Displays the number of ONU connected and their corresponding power levels.

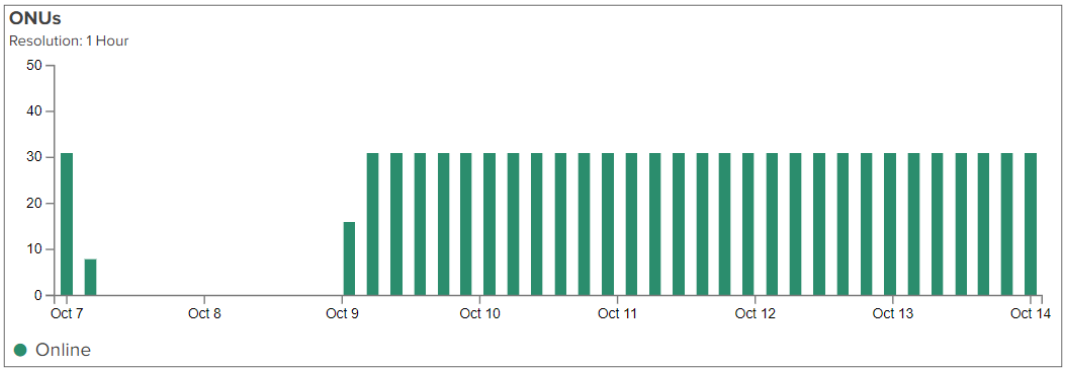
Figure 260 *ONU by signal level per port*



ONUs

Displays the number of ONUs connected to the OLT.

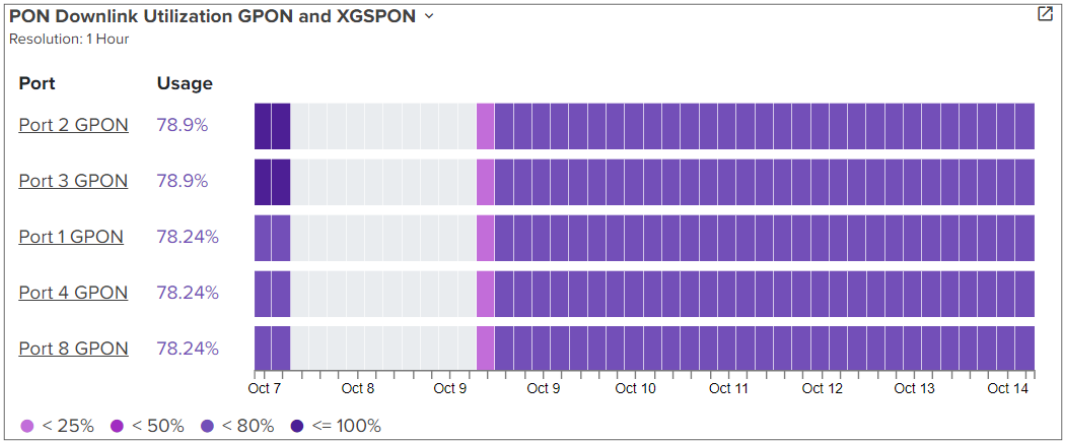
Figure 261 *ONU*



PON Downlink Utilization

Displays the utilization of GPON and XGS-PON.

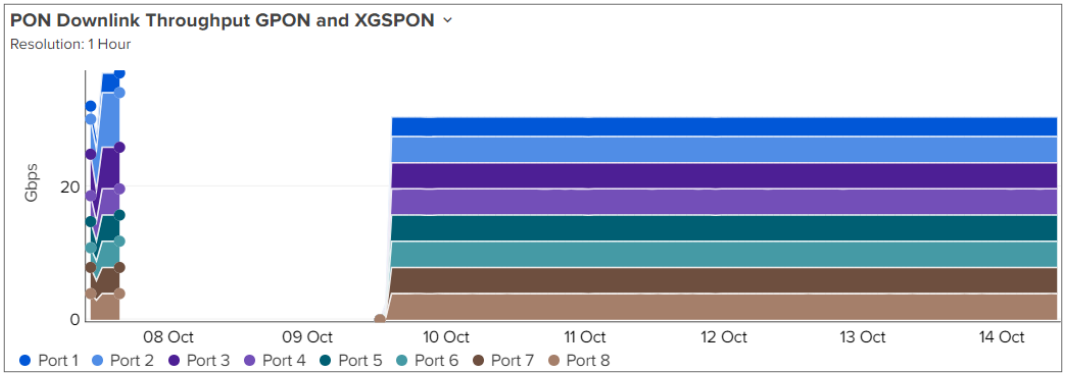
Figure 262 *PON Downlink Utilization*



PON Downlink Throughput

PON Downlink throughput displays the downlink throughput information of GPON and XGS-PON.

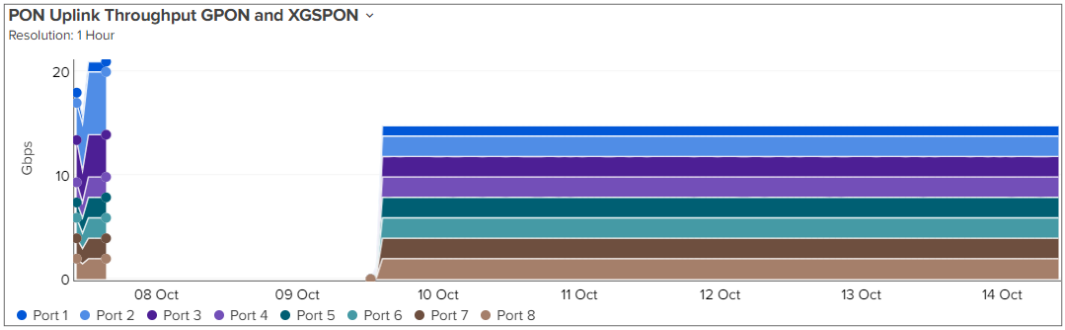
Figure 263 *PON Downlink Throughput*



PON Uplink Throughput

Displays the uplink throughput information of GPON and XGS-PON.

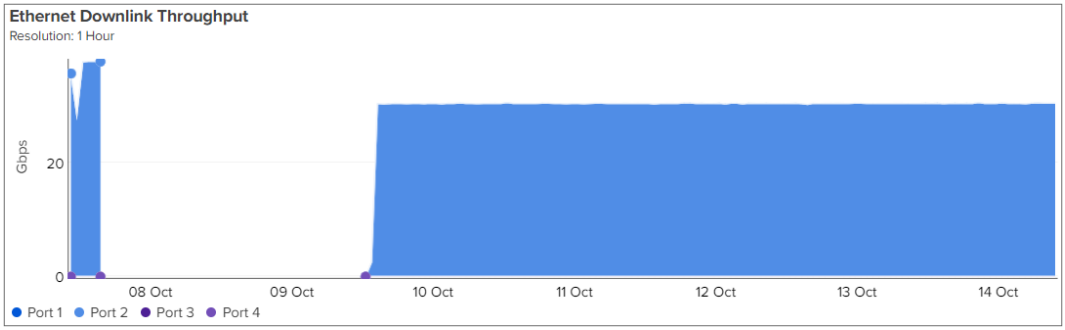
Figure 264 *PON Uplink Throughput*



Ethernet Downlink Throughput

Displays the Ethernet Downlink information of GPON and XGS-PON.

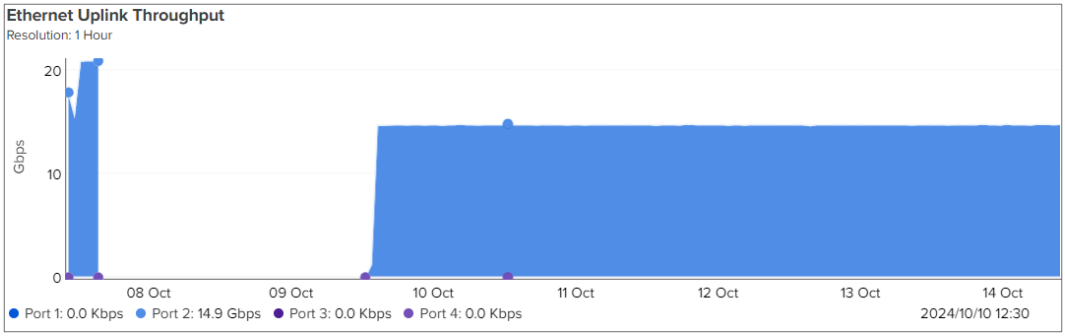
Figure 265 *Ethernet Downlink throughput*



Ethernet Uplink Throughput

Displays the Ethernet Uplink information of GPON and XGS-PON.

Figure 266 *Ethernet Uplink Throughput*



Notifications

Displays the alarm information of the OLT.

Figure 267 *Notifications*

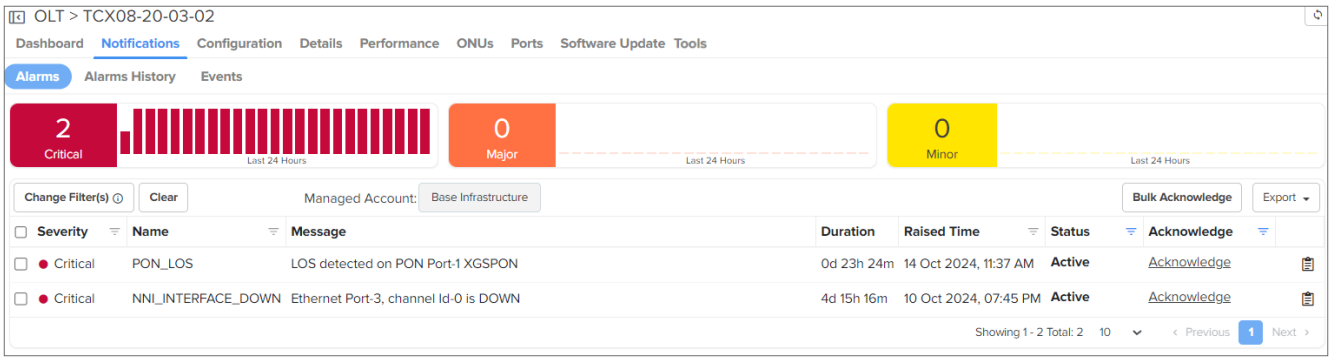


Table 63 *Parameters on the Notifications page*

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 268 *Configuration*

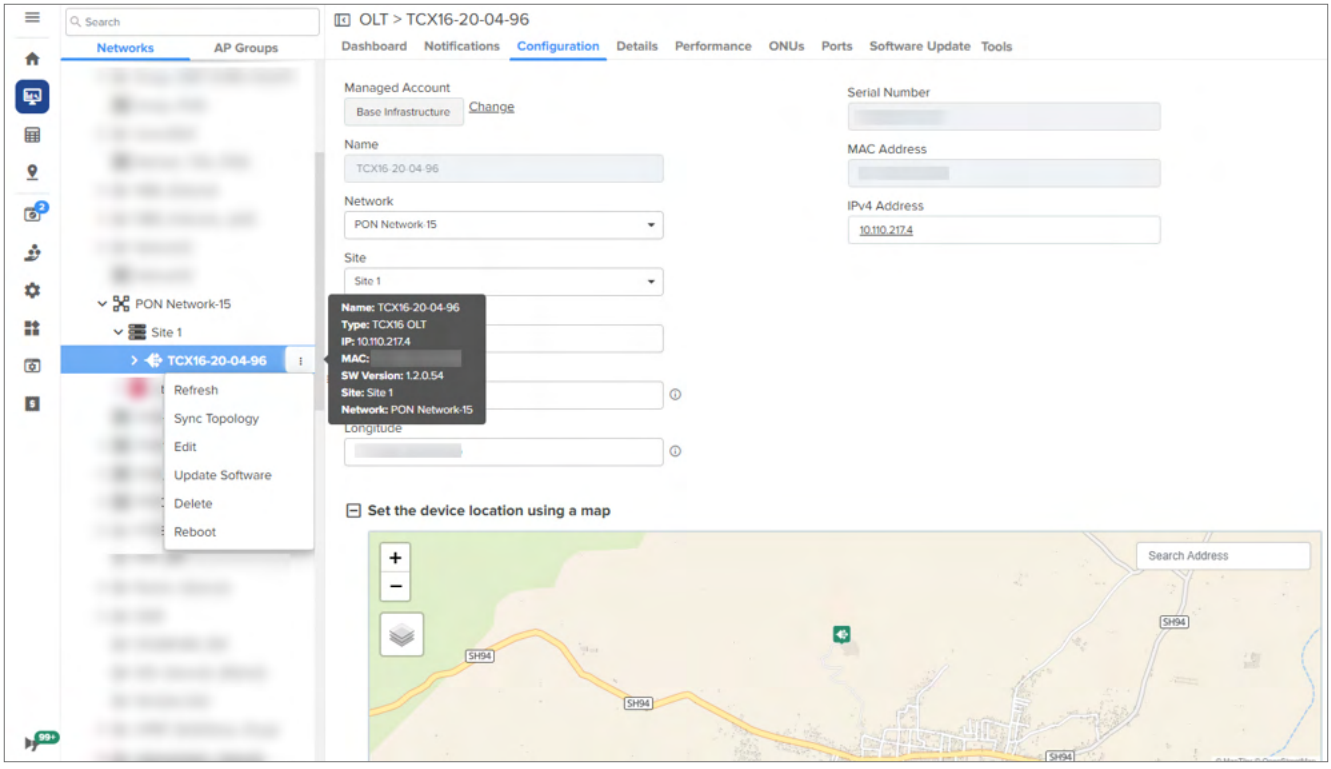


Table 64 *Parameters on the Configuration page*

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 269 *Details*

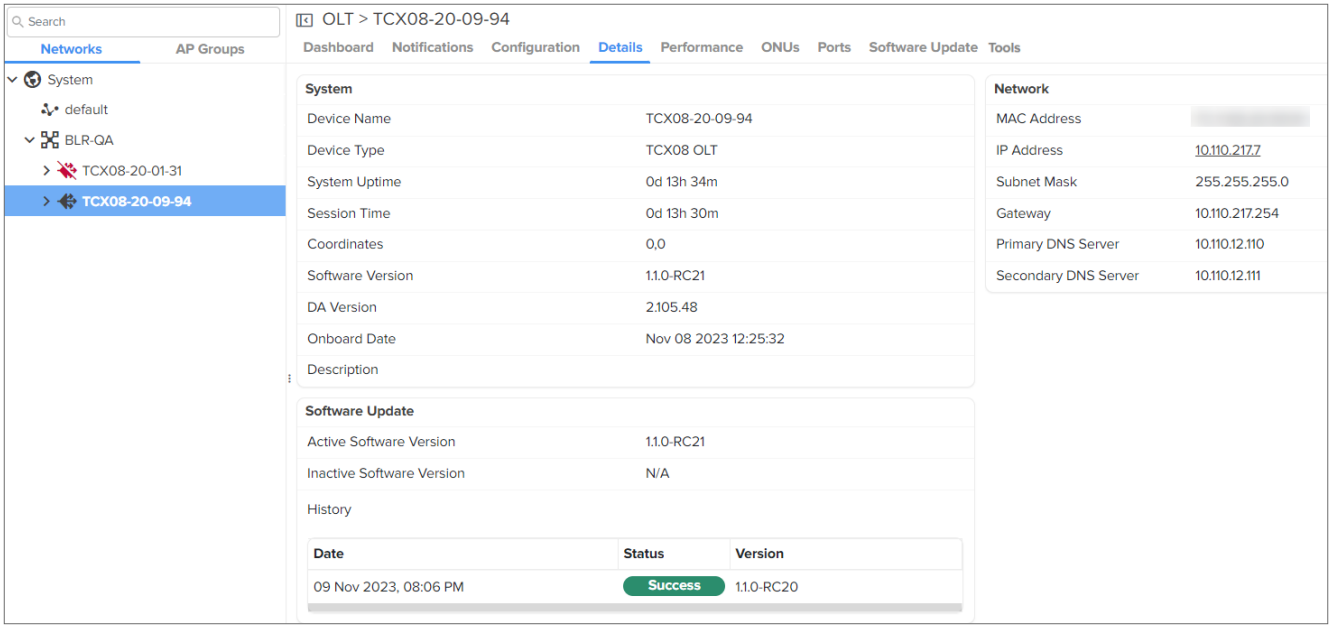


Table 65 *Parameters on the Details page*

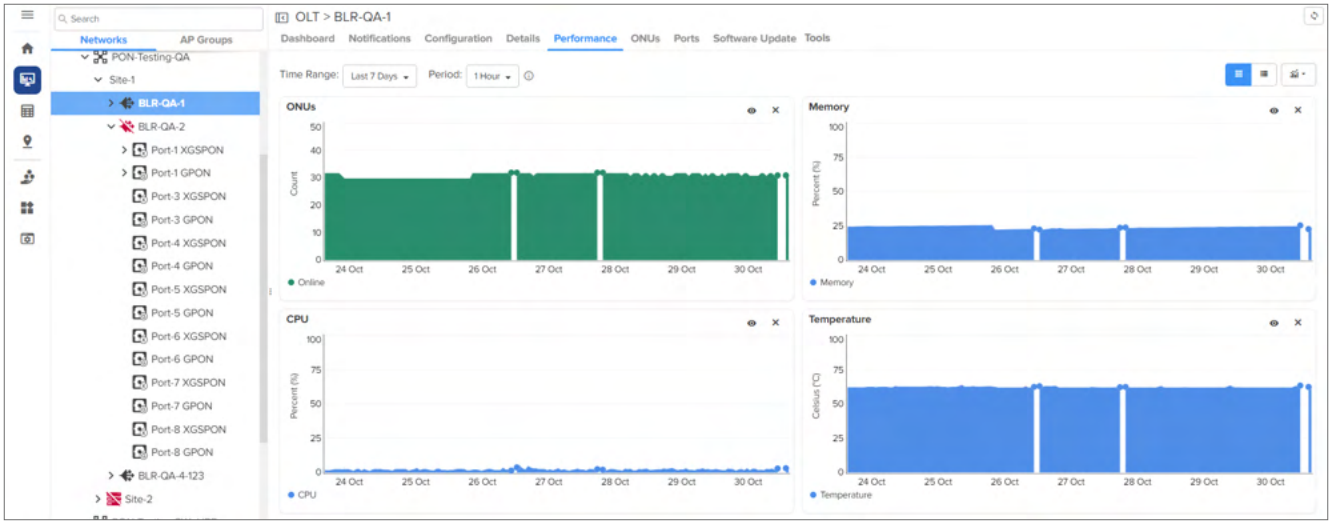
Parameter	Description
System	
Device Name	Name of the device.
Device Type	Type of the device. This parameter supports the following device types: • OLT • ONU

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 270 *Performance*



ONUs

Displays the number of ONUs connected to the OLT and their information.

Figure 271 *ONUs*

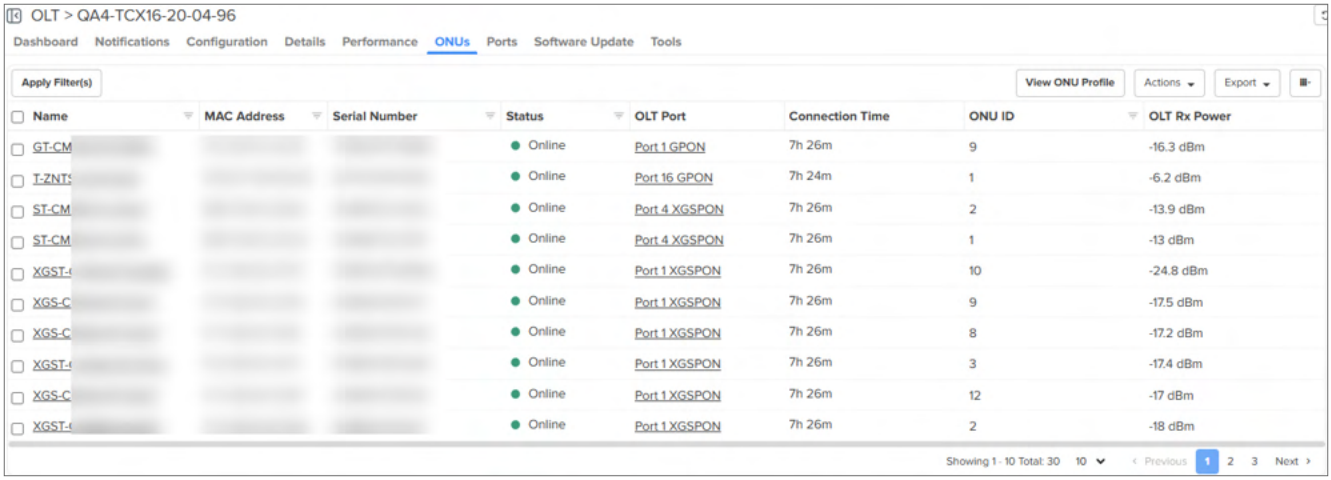


Table 66 *Parameters on the ONUs page*

Parameter	Description
Name	Name of the ONU. Click the **Name** to view the ONU-specific Dashboard page as shown in Figure 274.
MAC Address	MAC address of the ONU.
Serial Number	Serial number of the ONU.
Status	Status of the ONU.
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 ONU.

Viewing and updating ONU profile

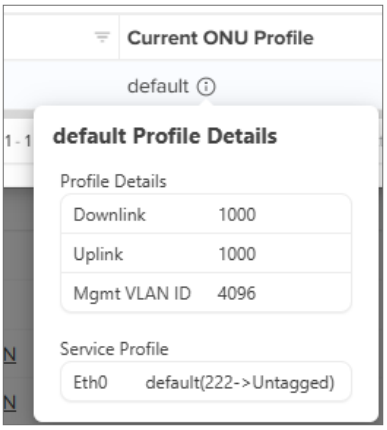
To view and update ONU profiles, complete the following steps:

1. To view the profile, on the **ONUs** page, select the ONUs whose profile you want to view and click **View ONU Profile**.

   The View ONU Profile window is displayed.

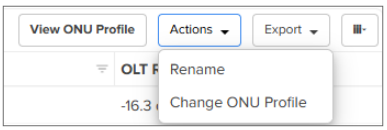


2. Under the **Current ONU Profile** column, hover the cursor over the info (ⓘ) icon, the current ONU profile details are displayed.



3. To change the ONU profile, click **Change ONU Profile**.

   You can also directly change the ONU profile by selecting the ONUs and clicking **Actions** > **Change ONU Profile** on the ONUs page.

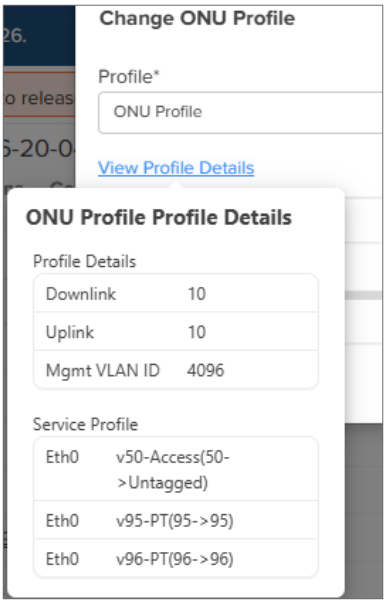


   The Change ONU Profile window is displayed.



4. Select the required profiles available for the OLT to which the ONU is connected from the Profile dorpdown list.
5. After you select the profile, you can view the profile details by clicking **View Profile Details**.

   The ***<profile-name>*** **Profile Details** window is displayed.

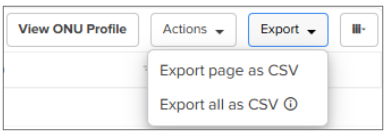


6. Click **Update**.

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

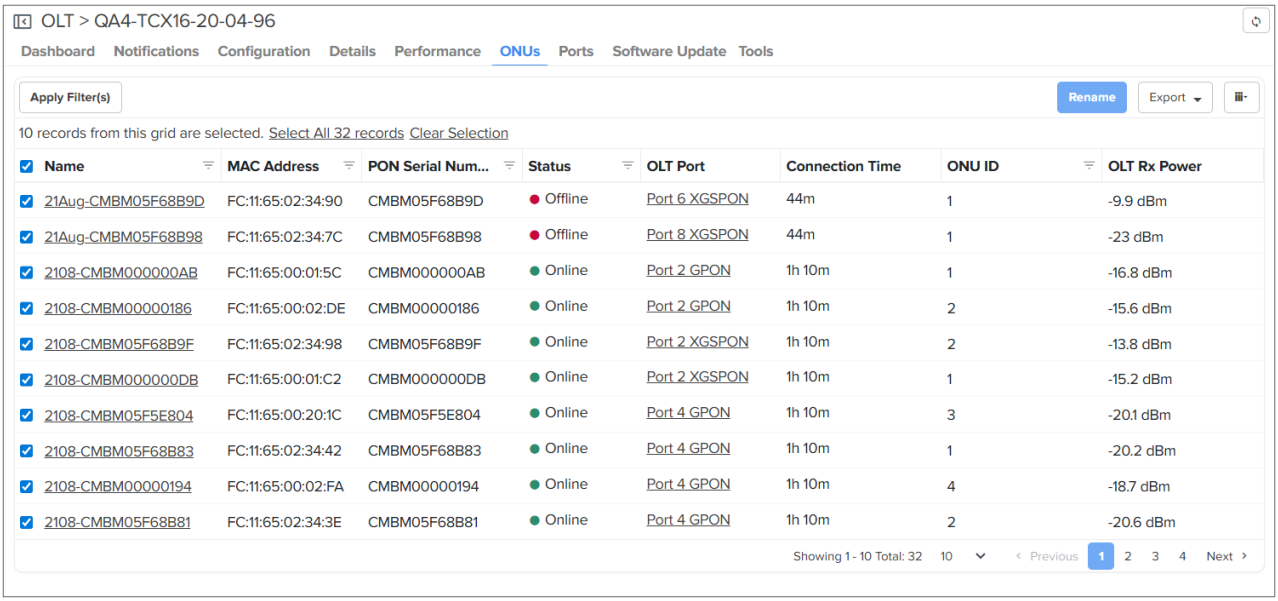
Bulk rename of ONUs is supported on OLTs running version 1.3.0 or higher.

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.



3. Click **Actions** > **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 272 *Ports*

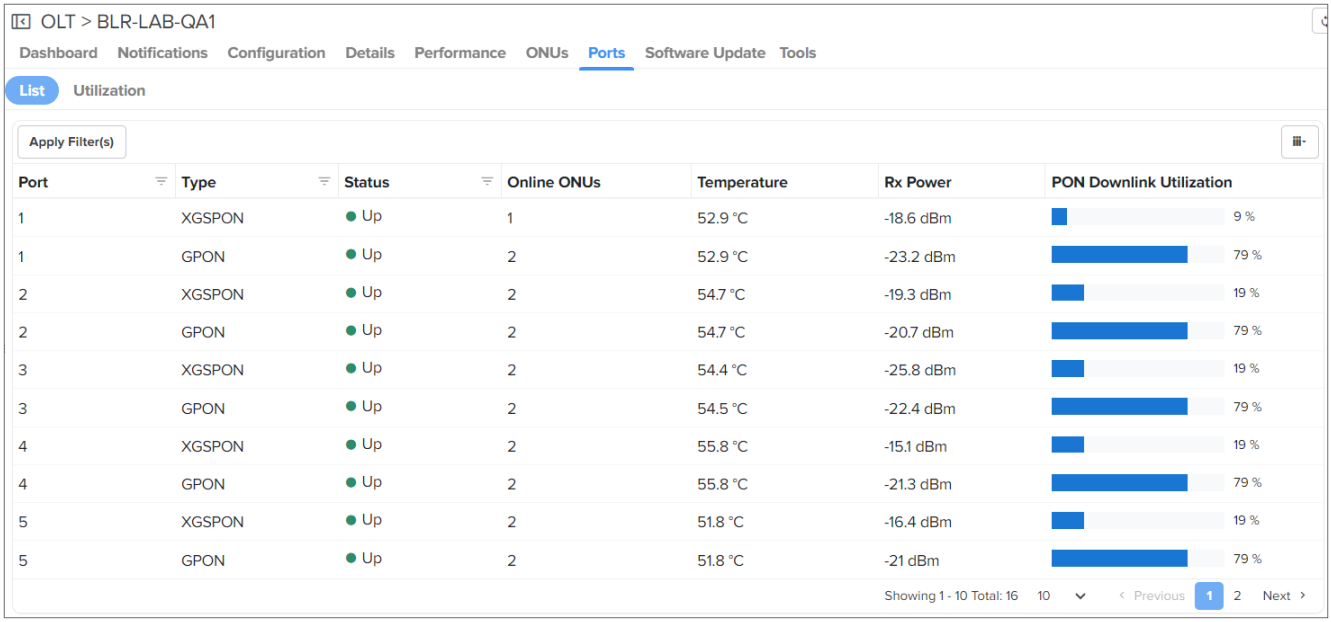
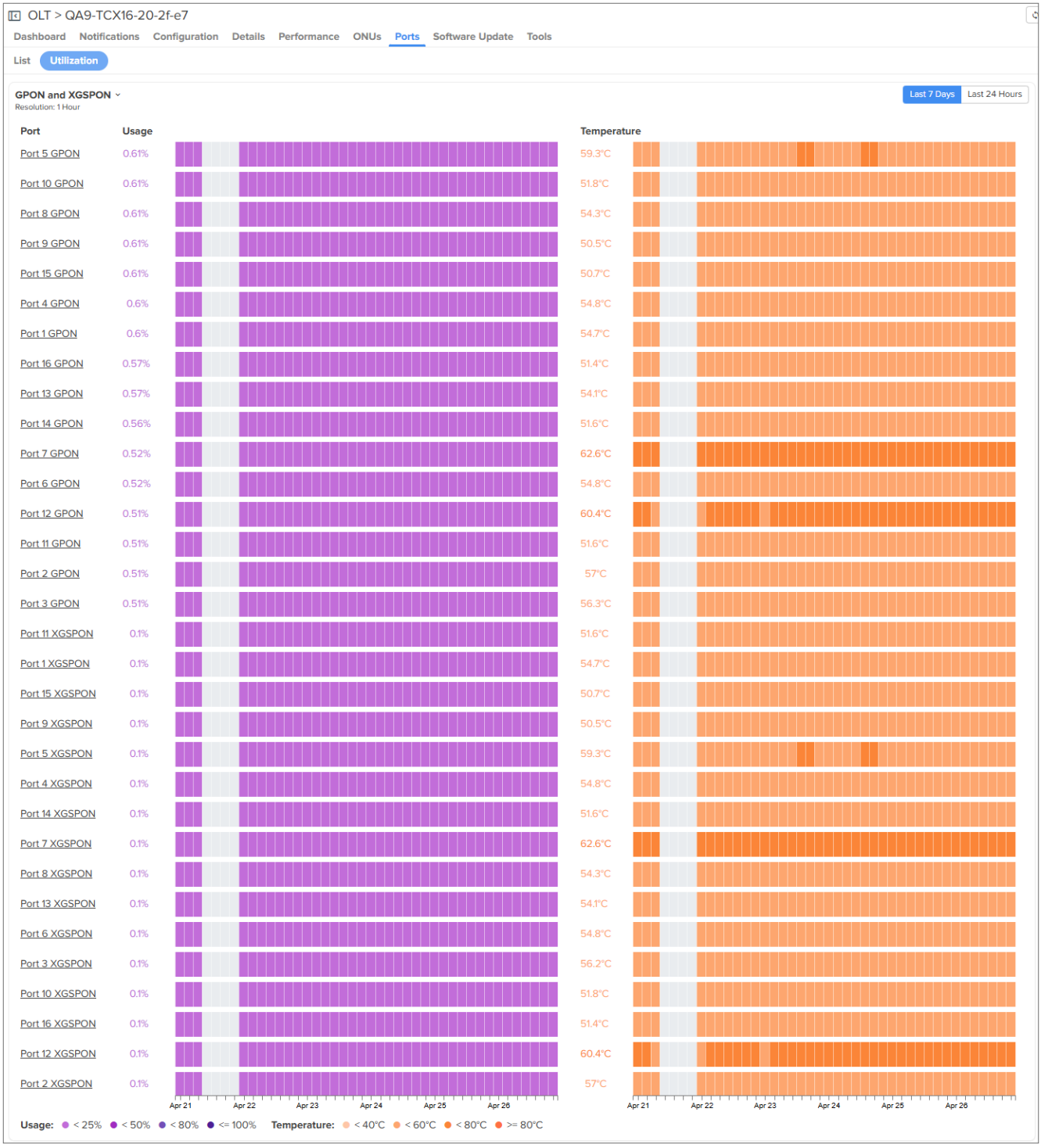


Figure 273 *Ports utilization*



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)**.

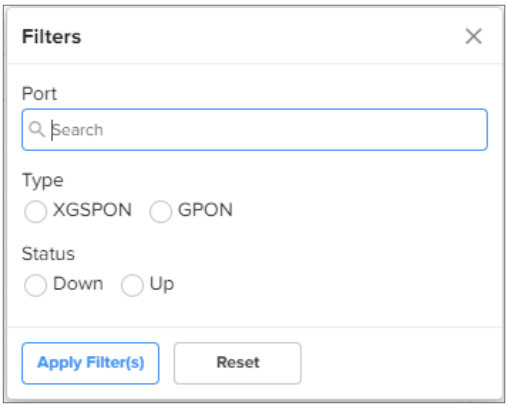


Table 67 *Parameters on the Ports page*

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.

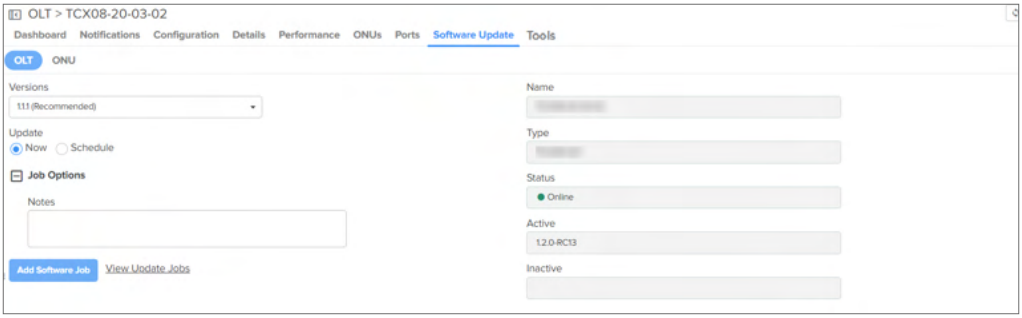
OLT Software Update

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:

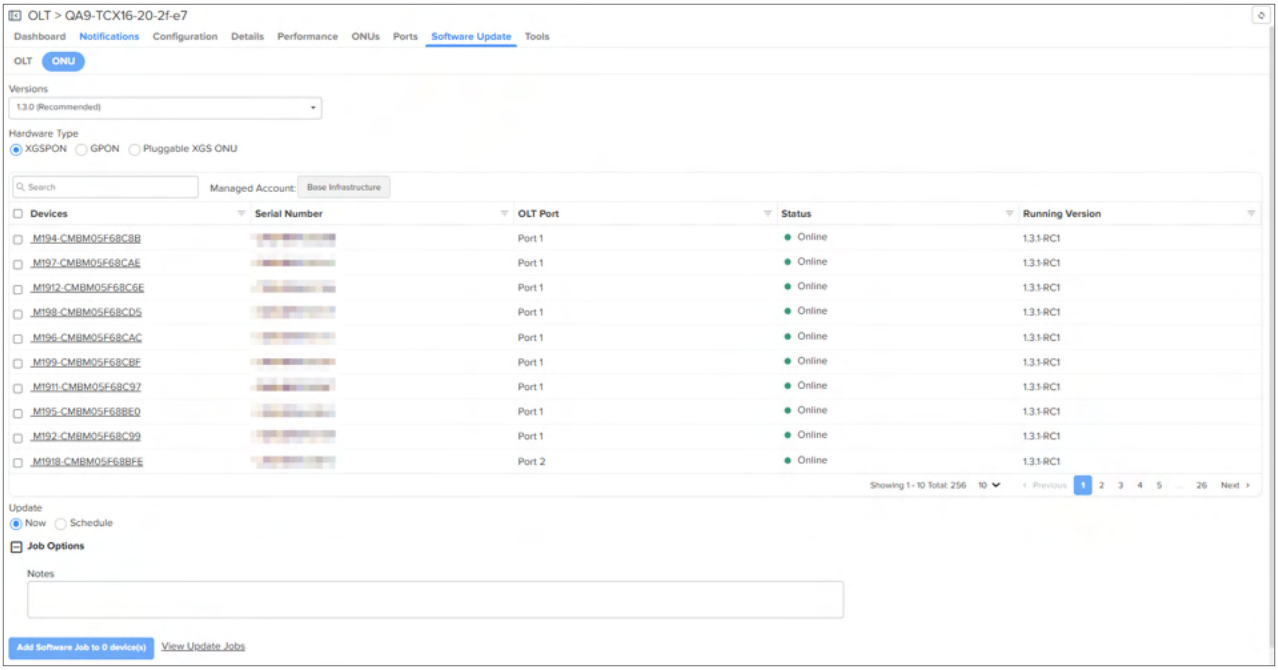
1. Download the latest firmware from Cambium Networks Support Site.
2. Navigate the **Monitor and Manage** > **<Site-Name>** > **OLT** > **Software Update** tab.

   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

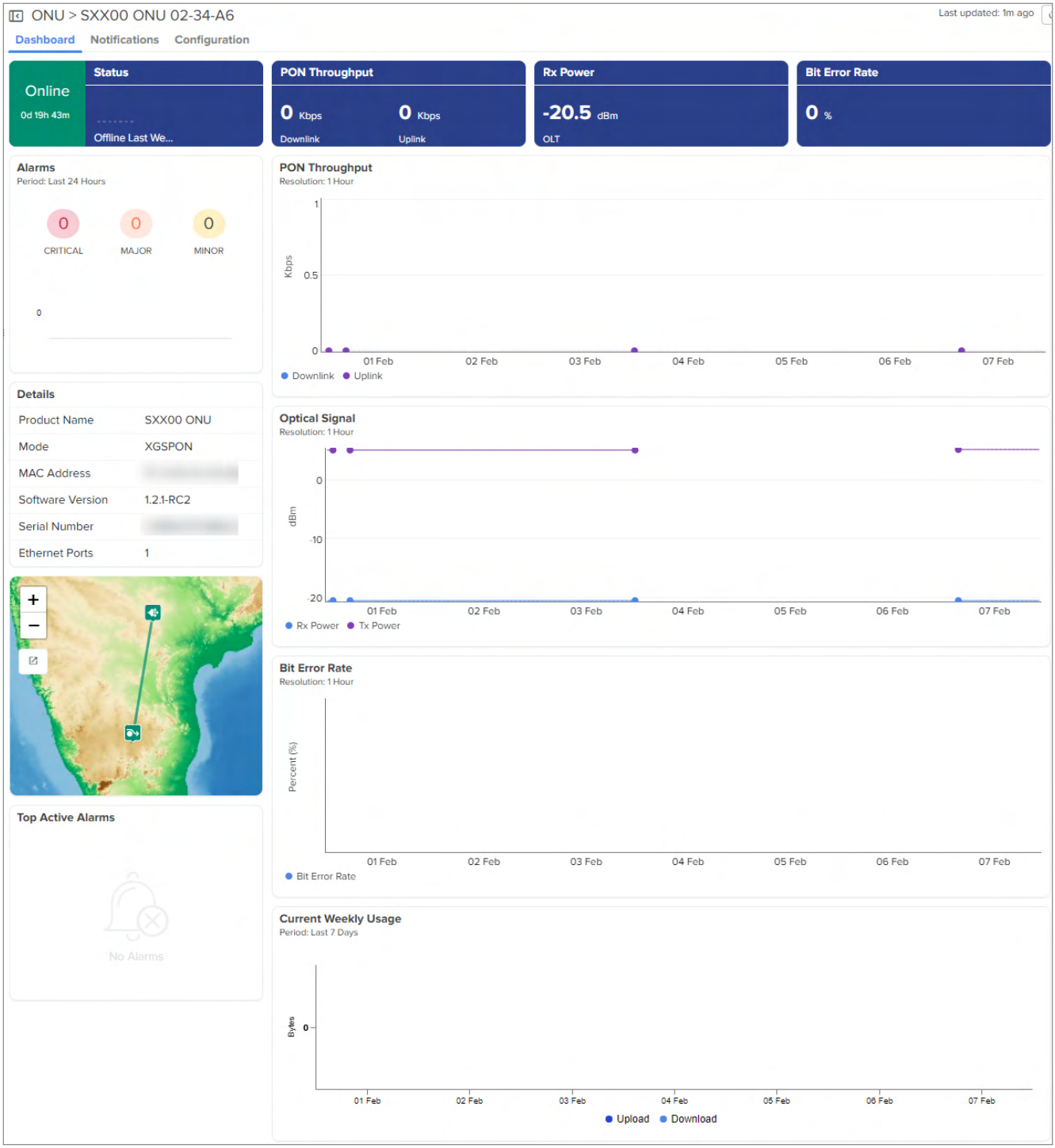
Note

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

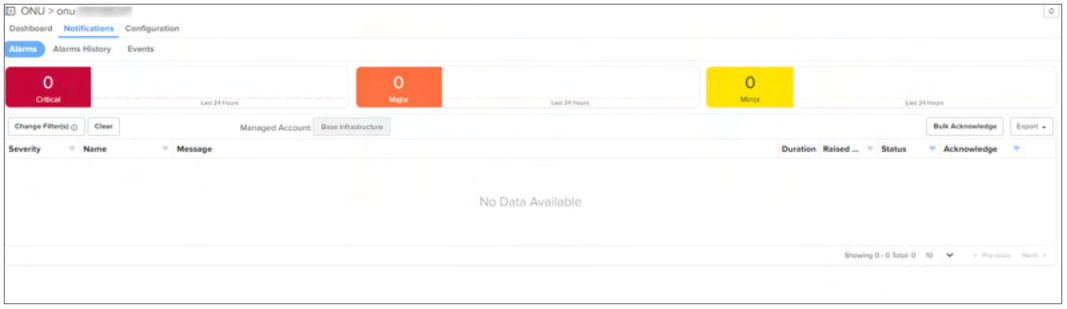
Figure 274 *ONU Dashboard*



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 275 *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 276 *ONU Configuration*

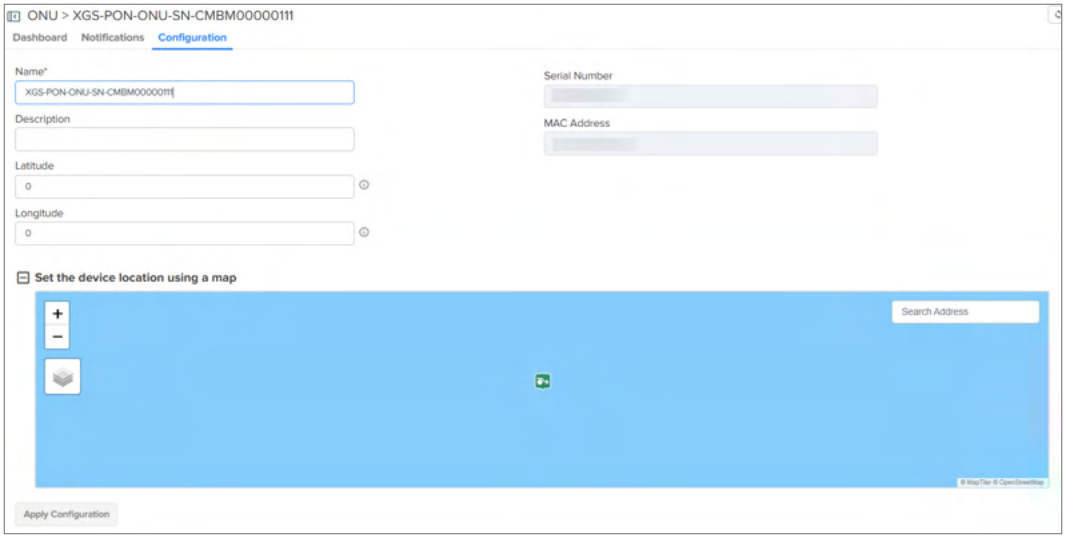


Table 68 *Parameters on the Configuration page*

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 277 *Inventory page at the System-level*

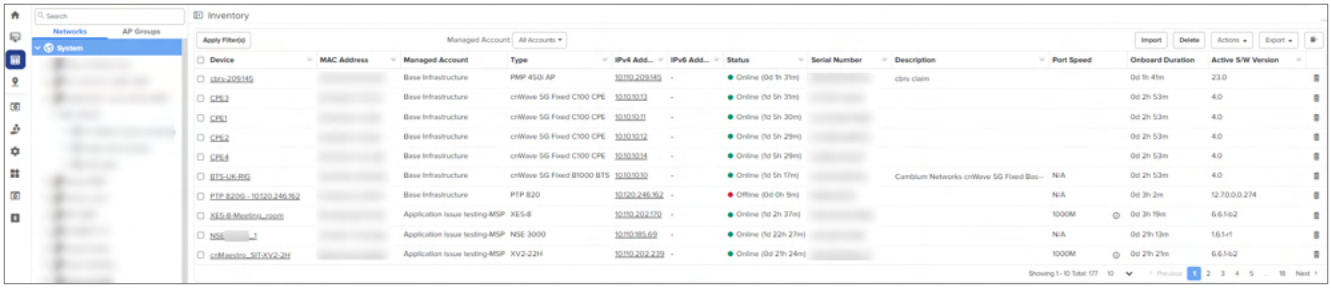


Figure 278 *Inventory page at the Site-level*



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

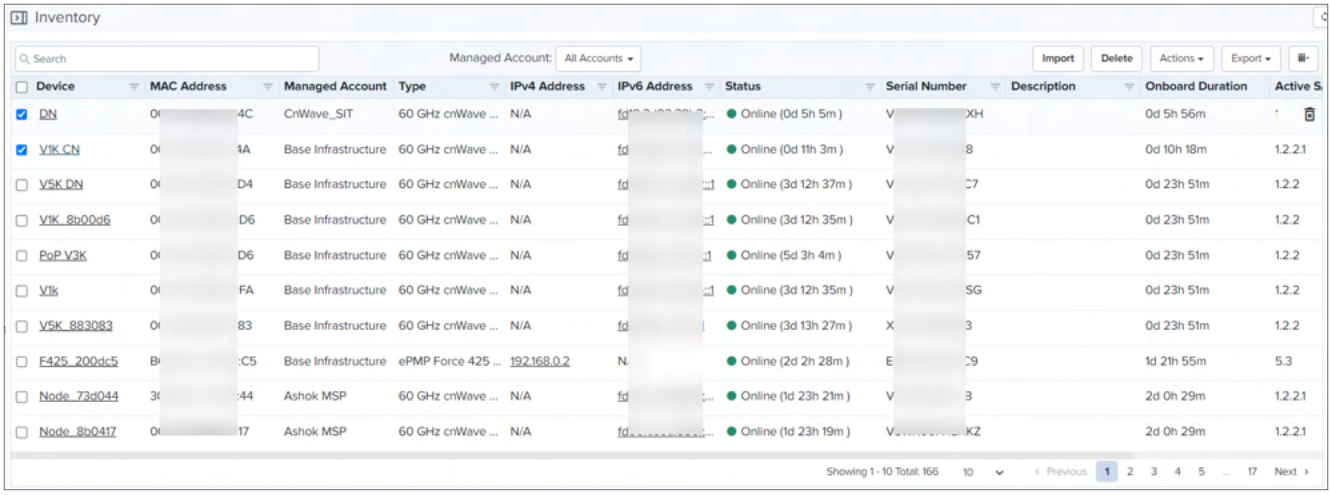
Inventory export is supported for PON devices starting from version 5.2.1.

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 279 *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.

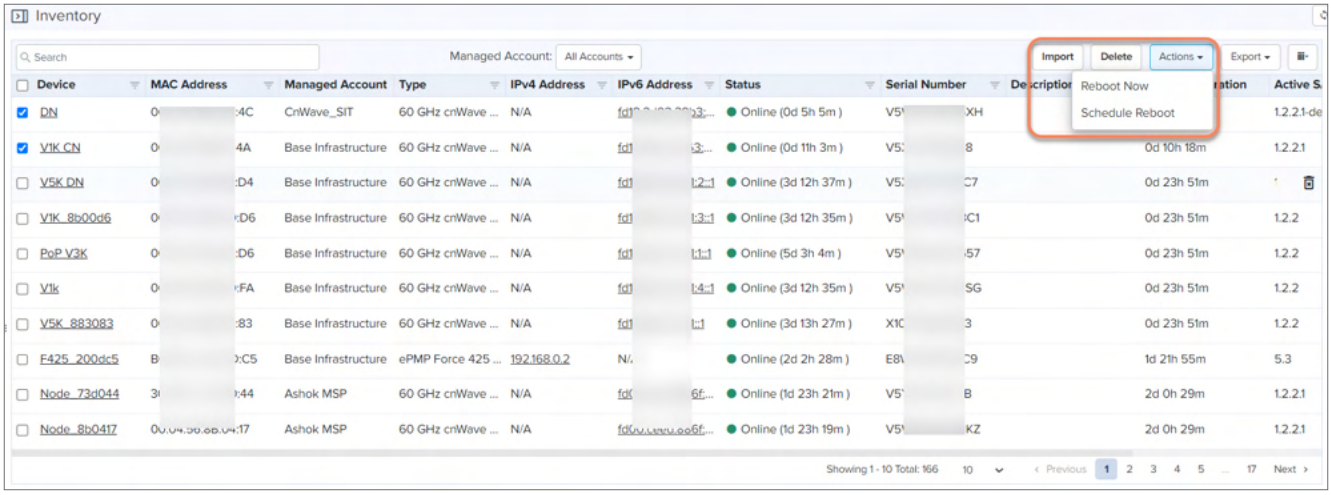
After deleting devices in bulk, you can view the status in the **Administration** > **Jobs** > **Actions** page.

For more information about deleting devices in bulk, see Deleting Devices in Bulk.

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 280 *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.

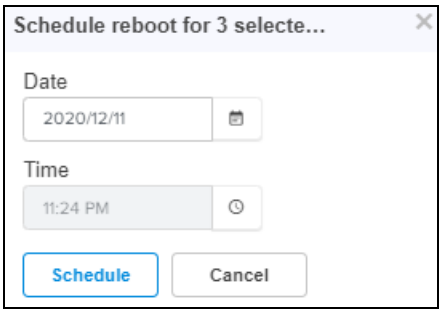
3. Click **Actions** and choose **Reboot Now**.

Schedule Reboot

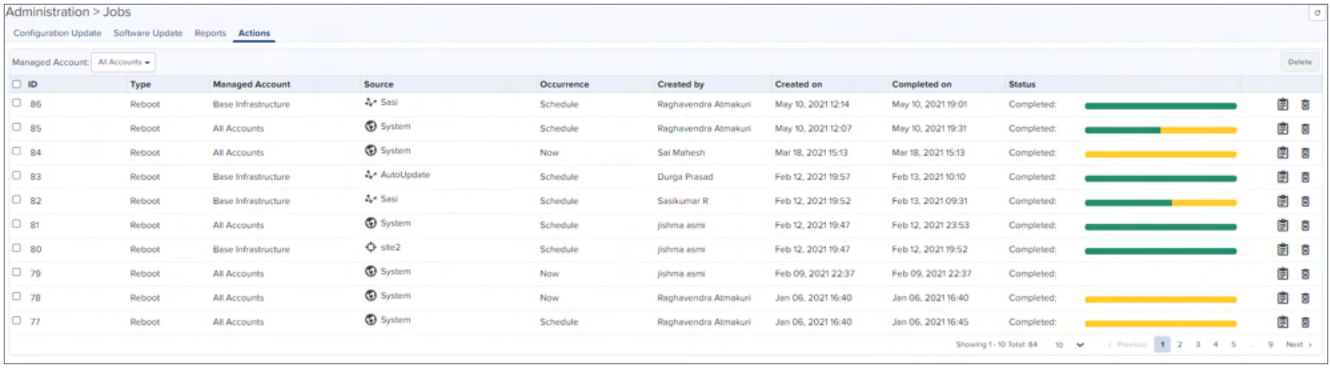
Schedule a reboot of the device(s) by selecting **Schedule Reboot** from **Actions** dropdown.

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:

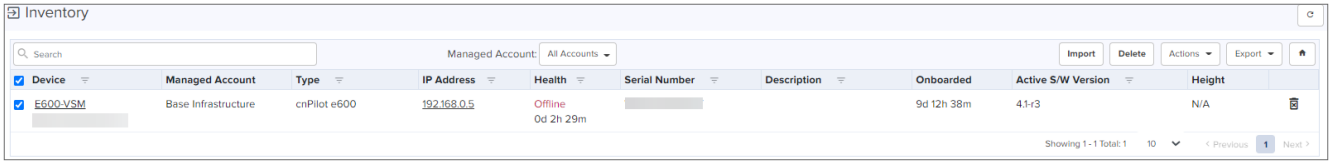
- Azhimuth
- Beamwidth
- Elevation

- Height
- Latitude
- Longitude

The following parameters are supported for ePMP/PMP SM is in the CSV file:

- Latitude
- Longitude

Figure 281 *Import Device Configuration*

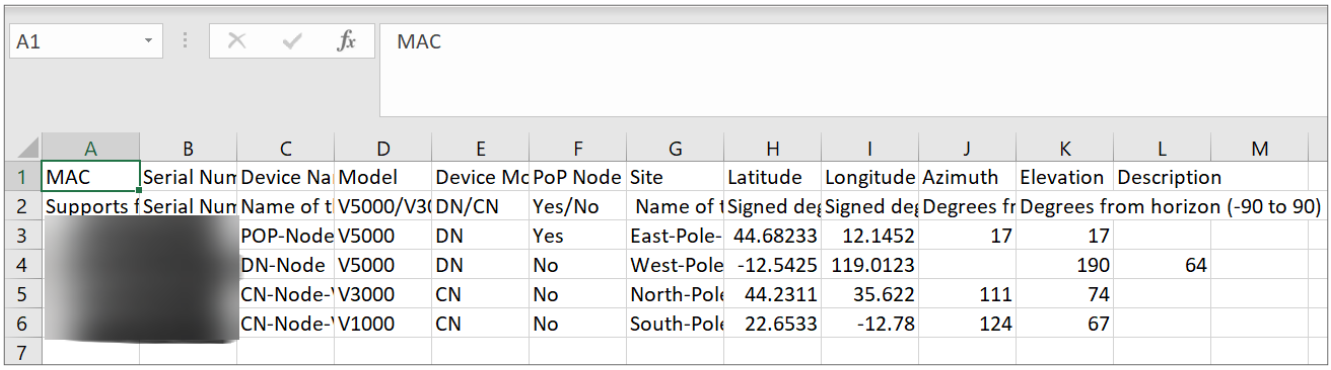


Sample Configuration File

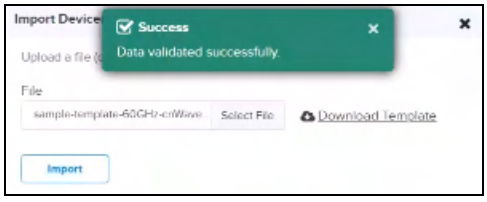
MAC	LATITUDE	LONGITUDE	AZIMUTH	ELEVATION	BEAM WIDTH	HEIGHT	HEIGHT UNIT
Supports formats with ':', '-', 'no space', upper and lower case.	Signed degrees format (DDD.ddd).	Signed degrees format (DDD.ddd).	Degrees from North (0 to 360)	Degrees from horizon (-90 to 90)	Degrees from 1 to 360	Min=0, Max=5	Meters/Feet
[redacted]	16	19	17	17	130	1500	Feet
[redacted]	-90	119.0123	190	64	120	1000	feet
[redacted]	79.0123	11	111	74	112	110	Meters
[redacted]	-44	-12.78	124	67	177	190	meters

Sample Configuration File (60 GHz cnWave)

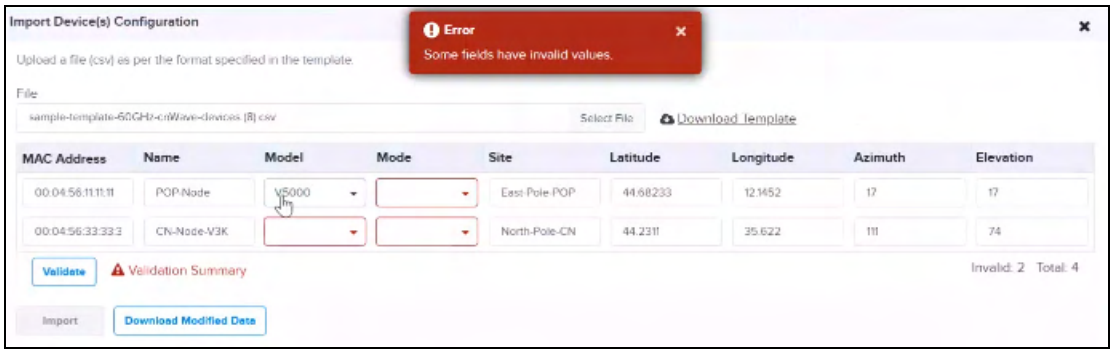
Figure 282 *Sample Configuration file: 60 GHz cnWave*



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:

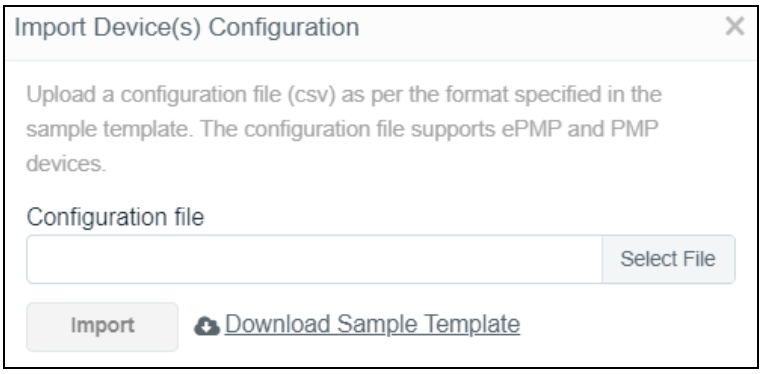
1. Click **Download Sample Template** or prepare a sheet in CSV file format with necessary column details.
2. Upload a configuration file (CSV) using the format specified in the sample template.

Note

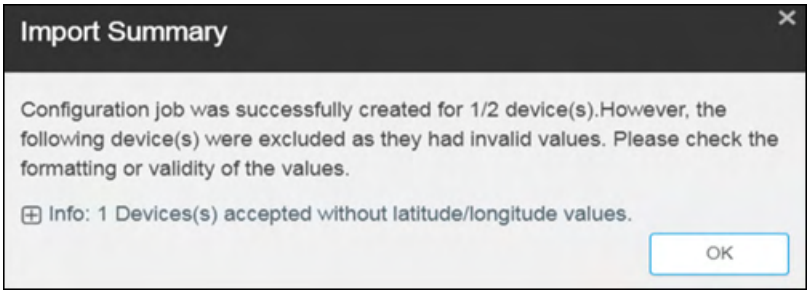
You must know the MAC address of the device to push the configuration.

3. Click **Import**.

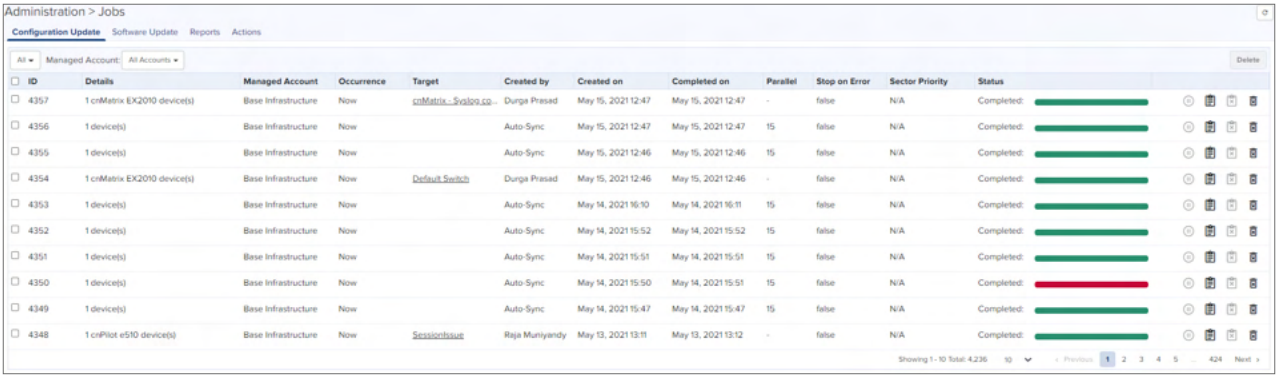
Figure 283 *Uploading Configuration file*



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 69 *Importing Error*

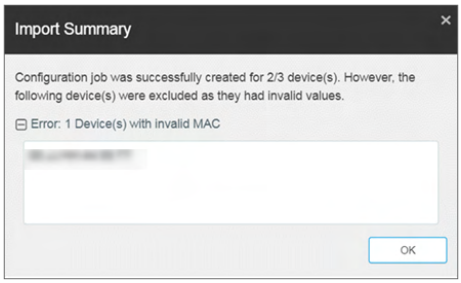
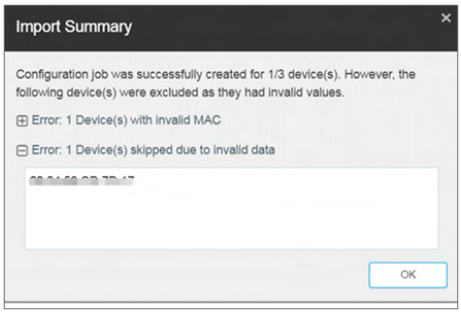
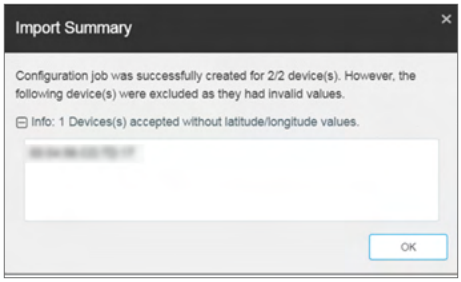
Error	Description
{Count of Devices} Device(s) with invalid MAC	This error is displayed if the uploaded CSV file contains an invalid MAC Address. 
{Count of Devices} Device(s) skipped due to invalid data	This error is displayed if the uploaded CSV file contains invalid Data or data not relevant for Latitude, Longitude, Azimuth, Height, and Elevation. 
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	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.

Table 69 *Importing Error*

Error	Description
values	

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.

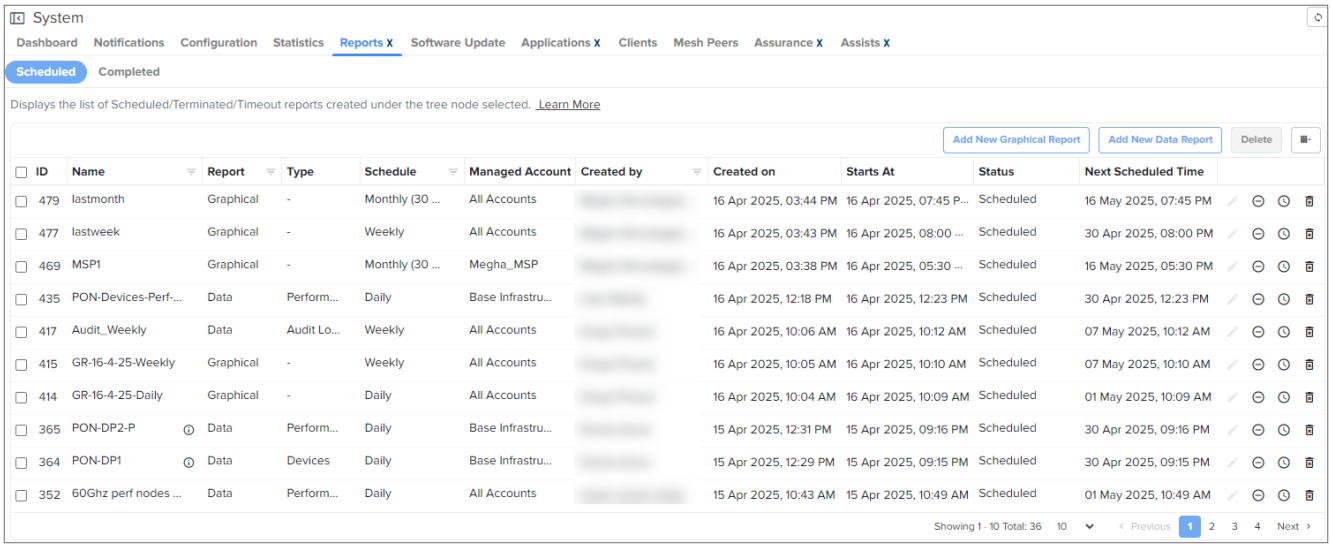
Scheduled Reports include the Scheduled, Terminated, and Timeout status in the Status column. **Completed Reports** include the Completed and Failed status is the Status column. Data reports are displayed only in a tabular format while graphical reports include charts and graphs.

Note

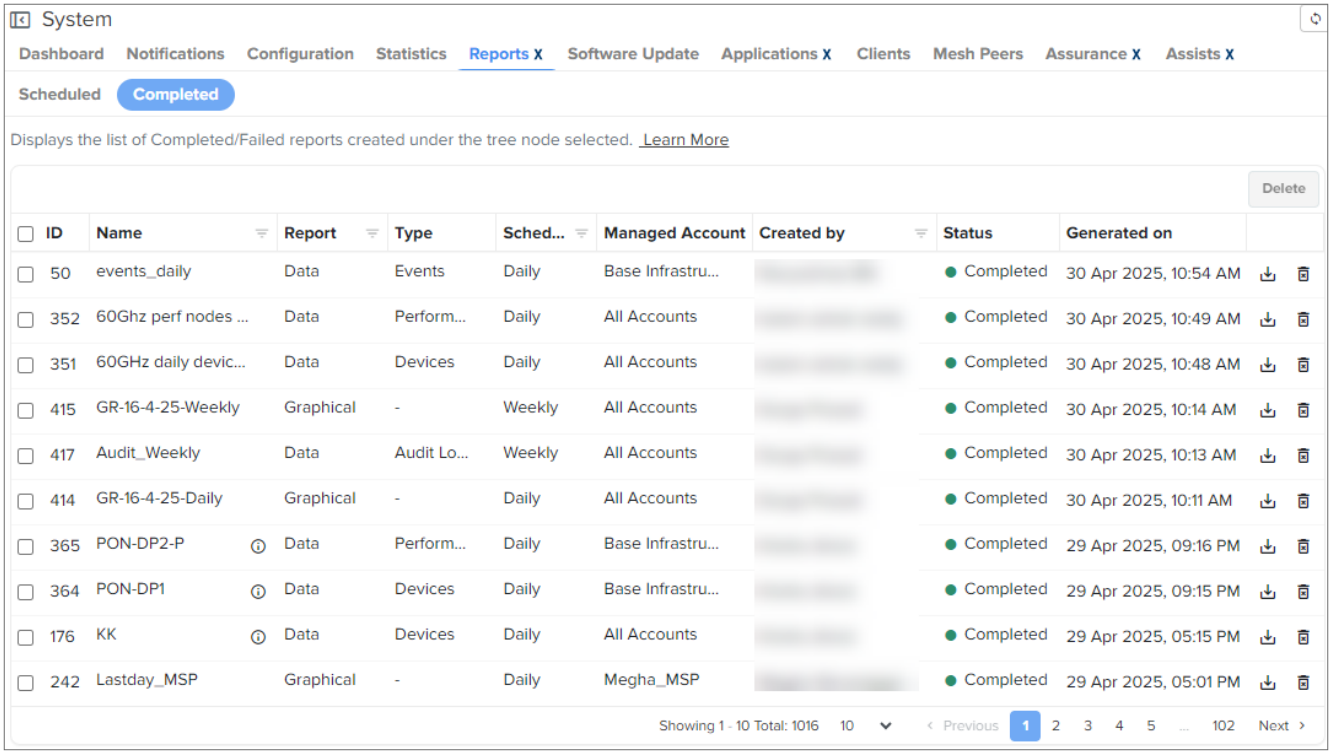
You can schedule and view reports (data and graphical) at the following levels in cnMaestro:

- 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

- Guest Access Login Events
- Reports jobs

Note

cnMaestro supports 14 months of historical data for the following devices:

- cnPilot Home (R-Series)
- Enterprise devices (Enterprise Wi-Fi and cnMatrix)
- IIoT devices

cnMaestro supports 26 months of historical data for the following devices:

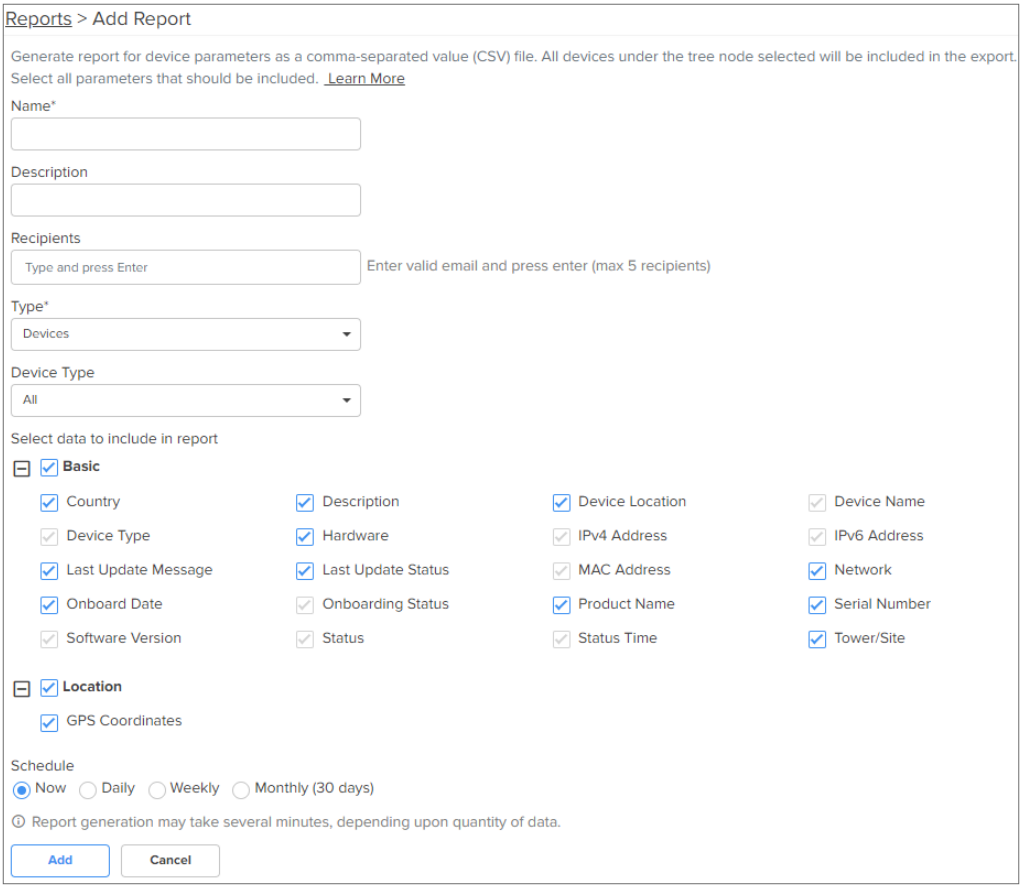
- Fixed Wireless

Devices Report

Devices Reports are generated as CSV files and include all devices under the selected tree node.

To generate Devices Reports, perform the following steps:

1. Navigate to **Reports** > **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.

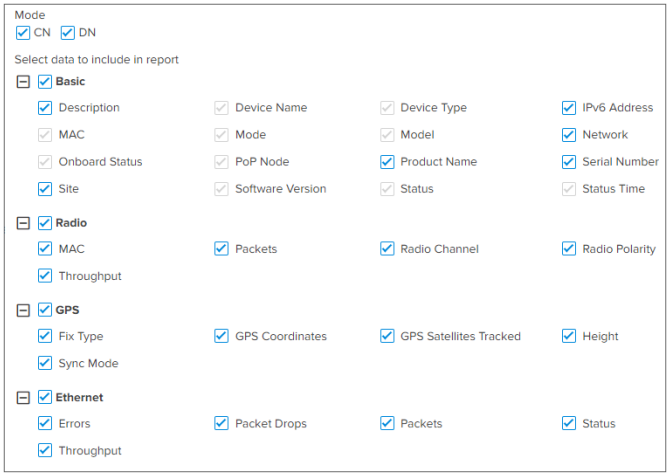
The device data parameters exported for the following devices are listed below:

- 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
- RV22 Home Mesh

If 60 GHz cnWave device is selected as **Device Type**, then the following parameter sections are available:

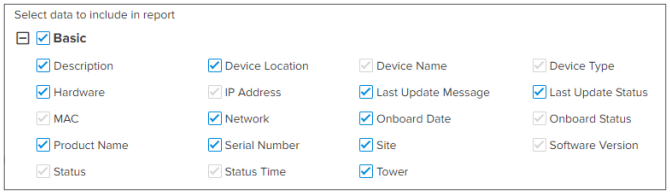
- Mode (CN or DN)
- Basic
- Ethernet
- GPS
- Radio

Figure 284 *Device Report: 60 GHz cnWave*



If cnMatrix is selected as the **Device Type**, then **Basic** data export parameters will be exported.

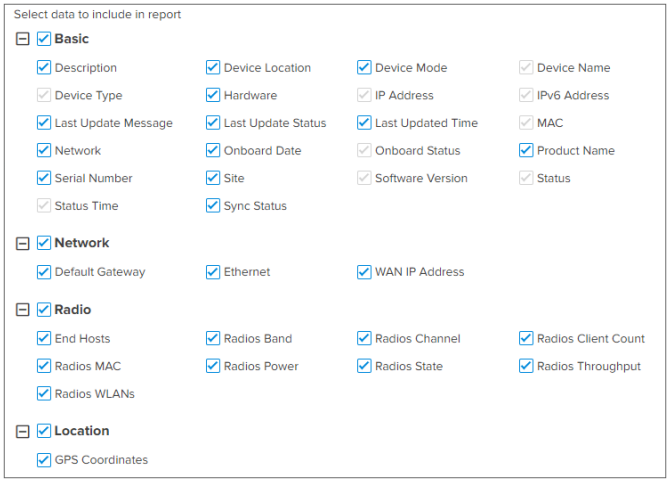
Figure 285 *Device Report: cnMatrix*



If cnPilot Home (R-Series) is selected as the **Device Type**, then the following parameter sections are available:

- Basic
- Location
- Network
- Radio

Figure 286 *Device Report: cnPilot Home (R-Series)*

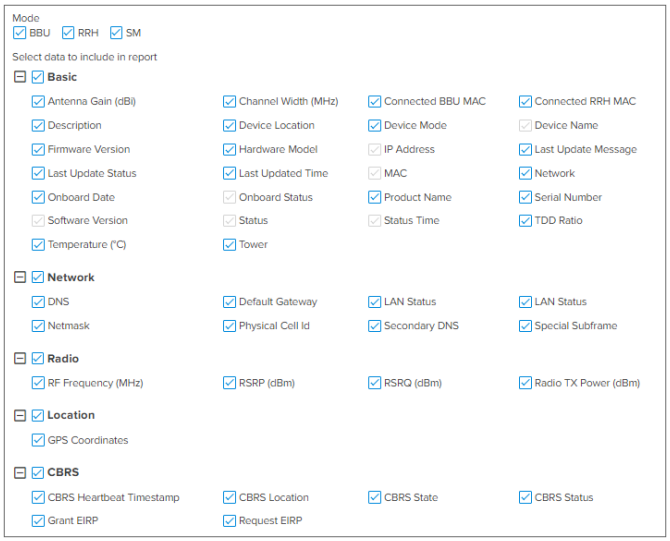


If cnRanger is selected as the **Device Type**, then the following parameter sections are available:

- Basic
- CBRS

- Location
- Network
- Radio

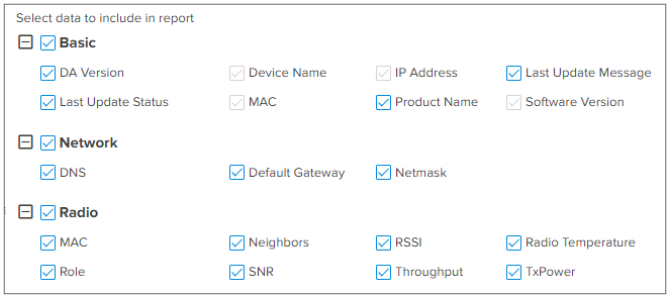
Figure 287 *Device Report: cnRanger*



If cnReach is selected as the **Device Type**, then the following sections are available:

- Basic
- Network
- Radio

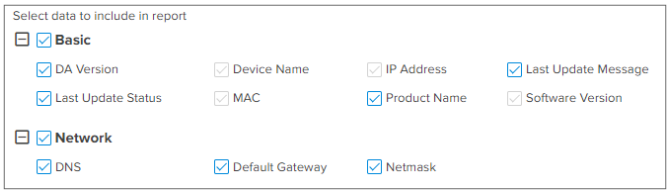
Figure 288 *Device Report: cnReach*



If cnReach XIO is selected as the **Device Type**, then the following sections are available:

- Basic
- Network

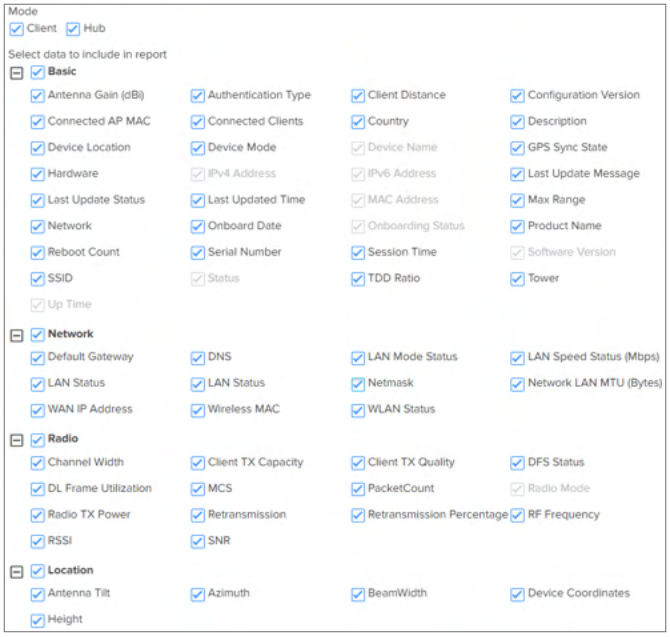
Figure 289 *Device Report: cnReach XIO*



If cnVision is selected as the **Device Type**, then the following sections are available:

- Mode (Client or Hub)
- Basic
- Location
- Mode
- Network
- Radio

Figure 290 *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

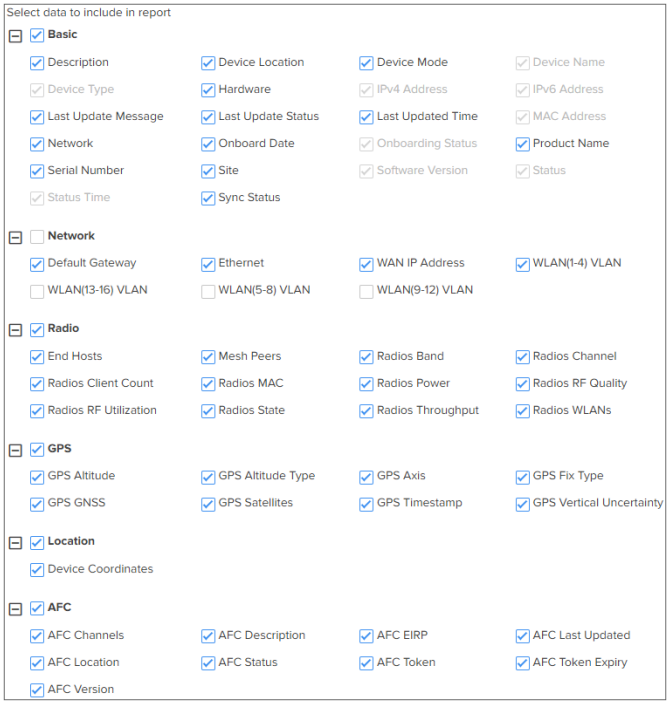
Figure 291 *Device Report: cnWave 5G Fixed*



If Enterprise Wi-Fi is selected as the **Device Type**, then the following sections are available:

- AFC
- Basic
- GPS
- Location
- Network
- Radio

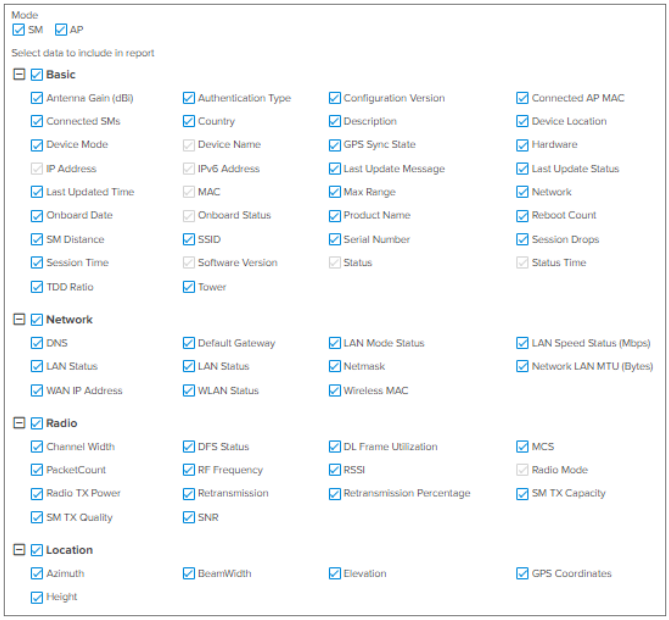
Figure 292 *Device Report: Enterprise(Wi-Fi)*



If ePMP is selected as the **Device Type** then the following sections are available:

- Mode (AP or SM)
- Basic
- Location
- Network
- Radio

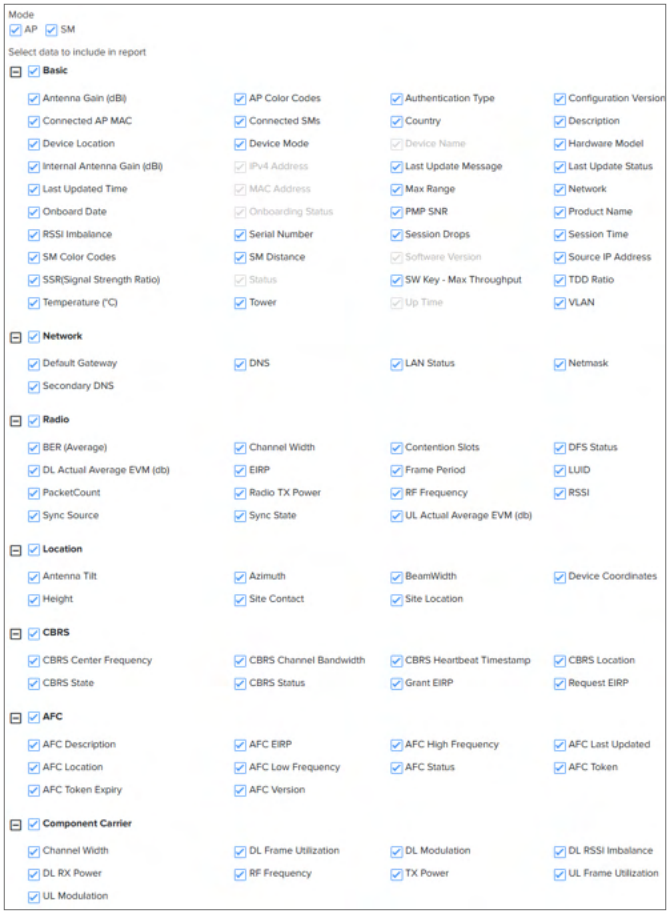
Figure 293 *Device Report: ePMP*



If PMP is selected as the **Device Type**, then the following sections are available:

- Mode (AP or SM)
- AFC
- Basic
- CBRS
- Component Carrier
- Location
- Network
- Radio

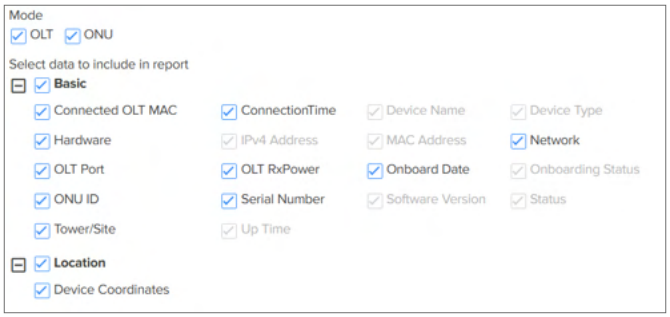
Figure 294 *Device Report: PMP*



If PON is selected as the **Device Type**, then the following sections are available:

- Basic
- Location

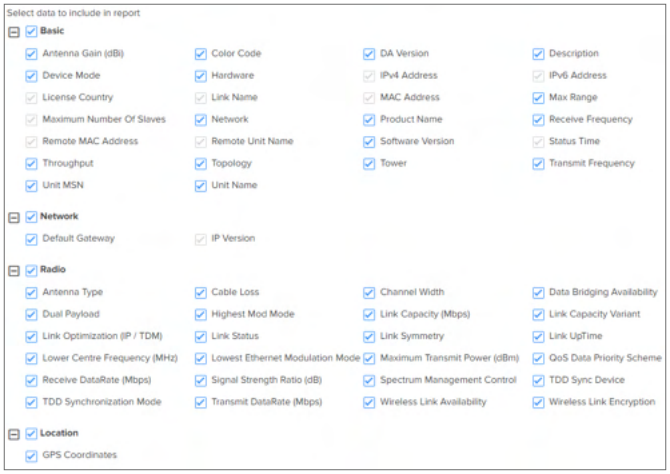
Figure 295 *Device Report: PON*



If PTP 650/670/700 is selected as the **Device Type**, then the following sections are available:

- Basic
- Location
- Network
- Radio

Figure 296 *Device Report: PTP 650/670/700*



If PTP 820/850 is selected as the **Device Type**, then the following sections are available:

- Basic
- Radio

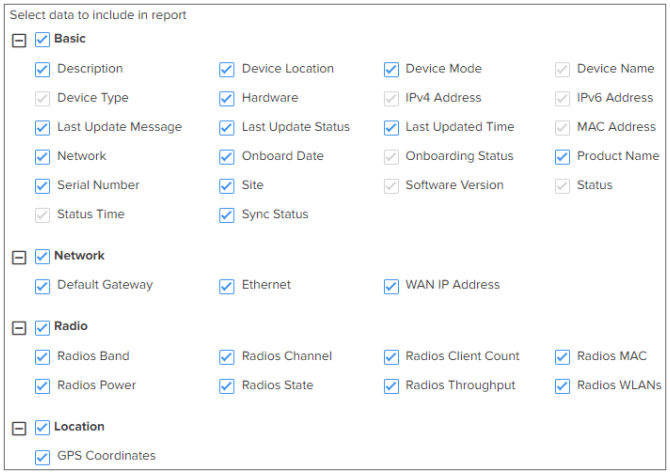
Figure 297 *Device Report: PTP 820/850*



The following sections are available for RV22 Home Mesh routers:

- Basic
- Location
- Network
- Radio

Figure 298 *Device Report: RV22 Home Mesh*



Note

Reports are available for each of the following hierarchical nodes in the tree:

- System
- Managed Account
- Network
- Tower
- Site
- AP Group

Audit Logs Report

Note

Audit log data is available for a maximum of 90 days.

The Audit logs report generates, in the CSV format, the cnMaestro audit log data that is available on the **Administration** > **Audit Logs** X page.

To generate the Audit Logs report, perform the following steps:

1. Navigate to **Reports** X > **Scheduled** tab.
2. Click **Add New Data Report**.

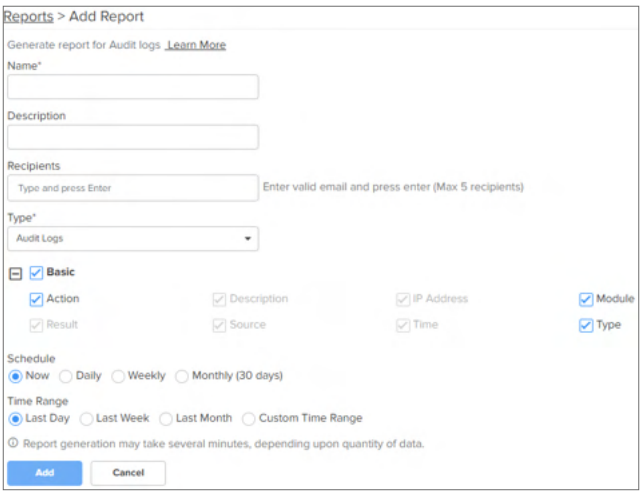
   The Add Report page appears.
3. Enter a **Name** and **Description** for the report.
4. Enter email addresses (maximum of 5) in the **Recipients** field to send reports.
5. Select the **Report Type** as Audit Logs.
6. Select data parameters to include in the report.

   Select the required checkboxes.
7. Select the following options:

- Schedule type (Now, Daily, Weekly, or Monthly (30 days))
- Time Range (Last Day, Last Week. Last Month, or Custom Time Range (up to a maximum of 90 days))

8. Click **Add**. The report is saved and listed in the **Scheduled Reports** page.

Figure 299 *Audit Logs Report*



Performance Report

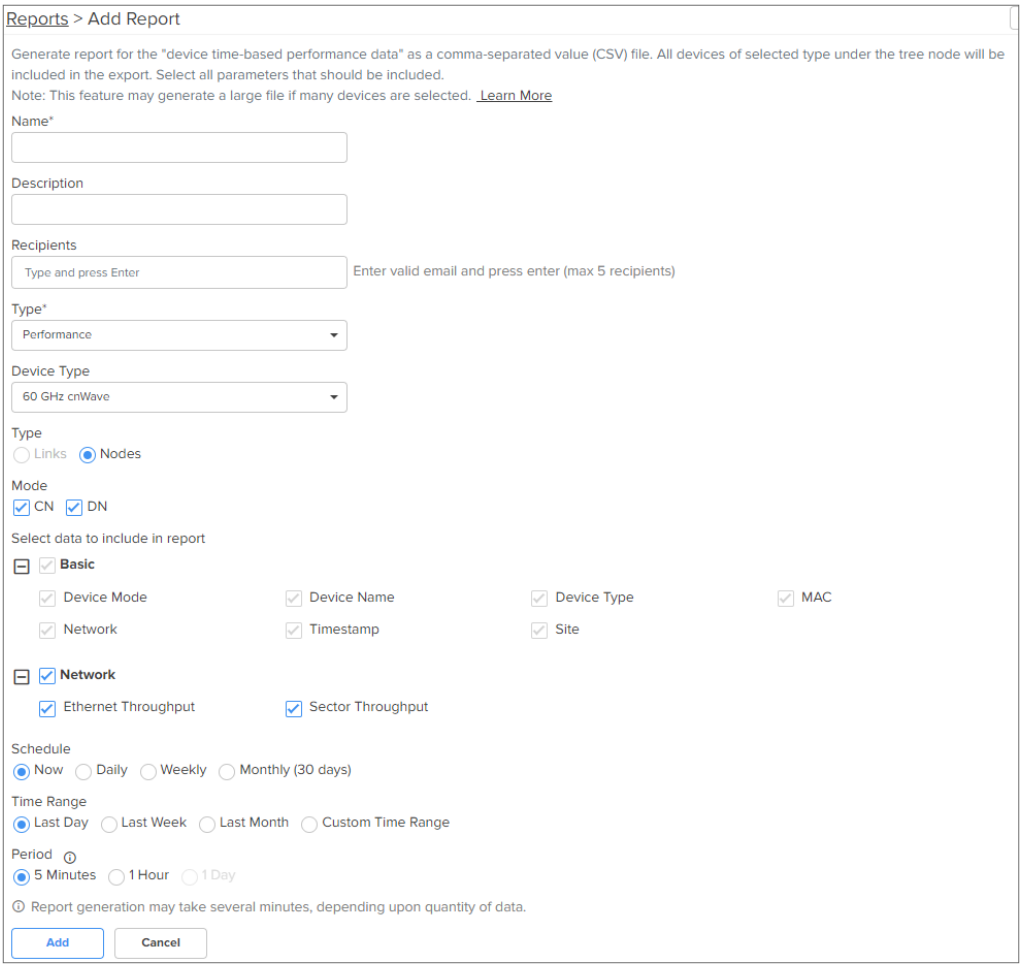
The Performance Report generates device time-series performance data as a comma-separated value (CSV) file. All devices of selected type under the tree node will be included in the export.

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 300 *Performance Report: 60 GHz cnWave (Links Type)*

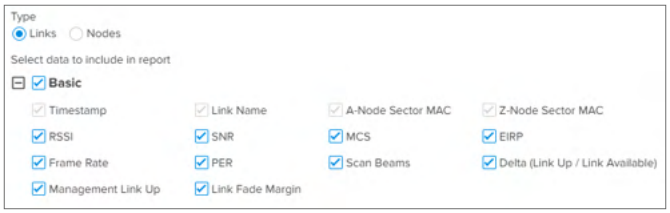
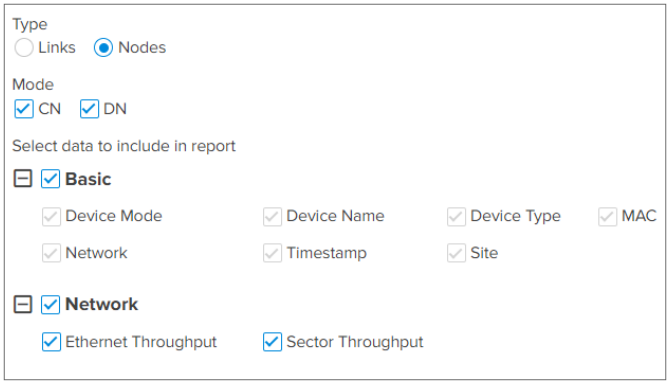
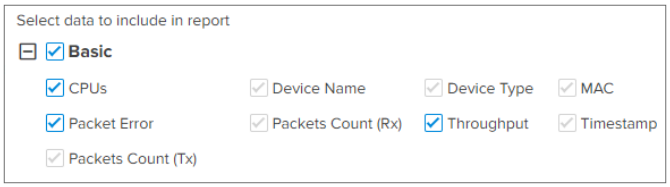


Figure 301 *Performance Report: 60 GHz cnWave (Node Type)*



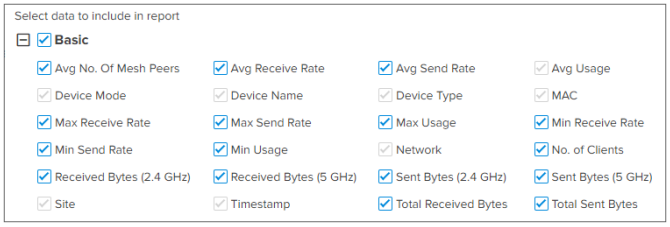
cnMatrix Performance Report

Figure 302 *Performance Report: cnMatrix*



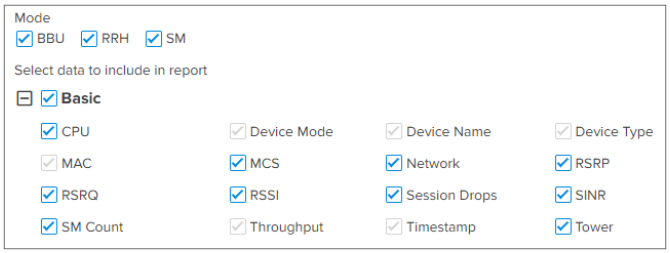
cnPilot Home (R-Series) Performance Report

Figure 303 *Performance Report: cnPilot Home (R-Series)*



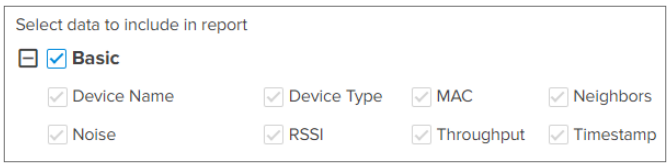
cnRanger Performance Report

Figure 304 *Performance Report: cnRanger*



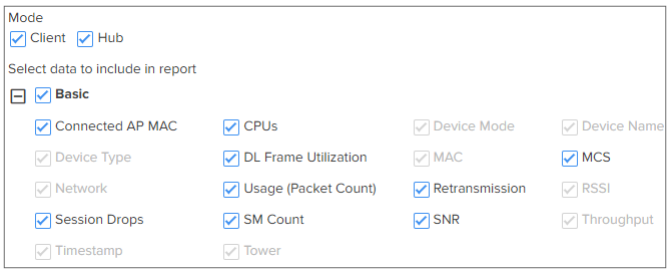
cnReach Performance Report

Figure 305 *Performance Report: cnReach*



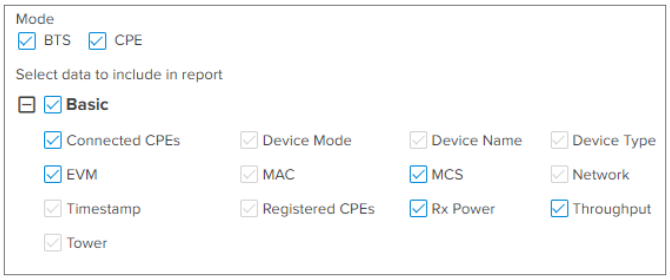
cnVision Performance Report

Figure 306 *Performance Report: cnVision*



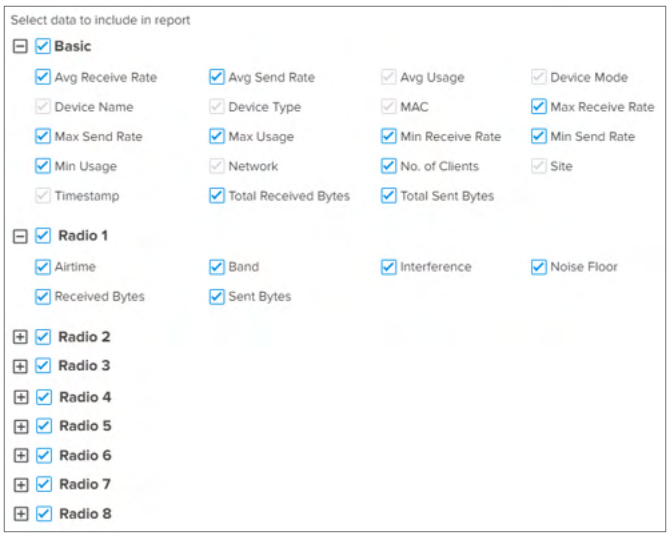
cnWave 5G Fixed Performance Report

Figure 307 *Performance Report: cnWave 5G Fixed*



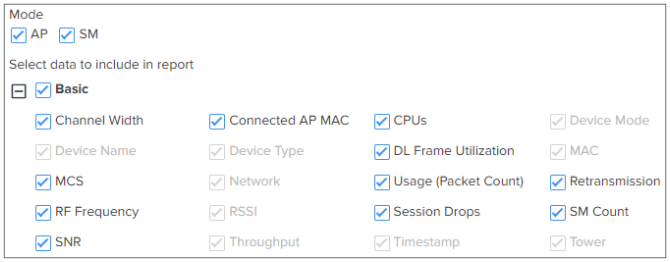
Enterprise Wi-Fi Performance Report

Figure 308 *Performance Report: Enterprise Wi-Fi*



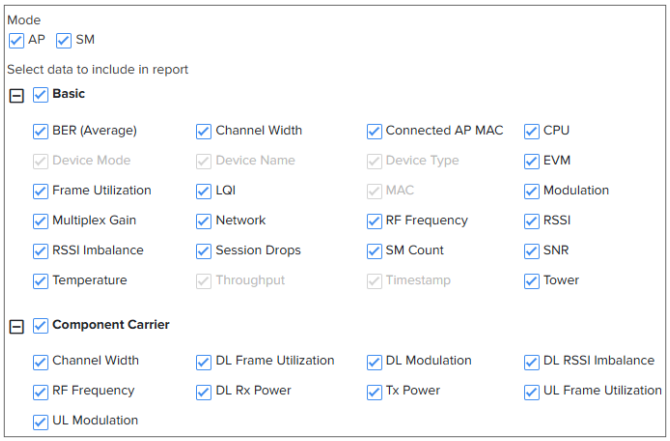
ePMP Performance Report

Figure 309 *Performance Report: ePMP*



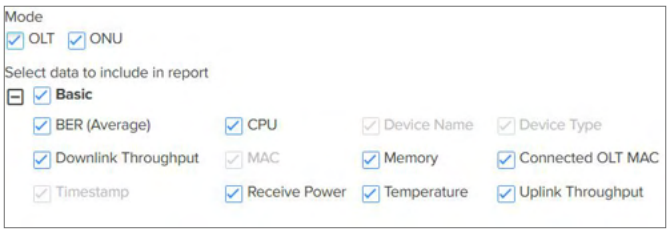
PMP Performance Report

Figure 310 *Performance Report: PMP*



PON Performance Report

Figure 311 *Performance Report: PON*



The modulation mappings for the PMP device are as follows:

Figure 312 *Mapping PMP*

Value	Description
-1	N/A
0	1X MIMO-A
1	2X MIMO-A
2	3X MIMO-A
3	4X MIMO-A
4	2X MIMO-B
5	3X MIMO-B
6	4X MIMO-B
7	5X MIMO-B
8	6X MIMO-B
9	7X MIMO-B
10	8X MIMO-B

Figure 313 *PMP 450m*

Value	Description
0	N/A
1	1X MIMO-A
2	2X MIMO-A
3	3X MIMO-A
4	4X MIMO-A

Figure 314 *PMP 450m*

Value	Description
0	N/A
2	2X MIMO-B
3	3X MIMO-B
4	4X MIMO-B
5	5X MIMO-B

Value	Description
6	6X MIMO-B
7	7X MIMO-B
8	8X MIMO-B

Figure 315 *PMP 430*

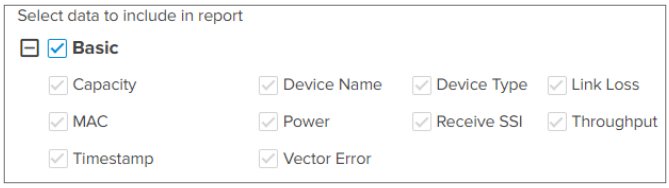
Value	Description
-1	N/A
0	1X SISO
1	2X SISO
2	3X SISO

Figure 316 *PMP 450v*

Value	Description
0	N/A
2	2X MIMO-B
3	3X MIMO-B
4	4X MIMO-B
5	5X MIMO-B
6	6X MIMO-B
7	7X MIMO-B
8	8X MIMO-B

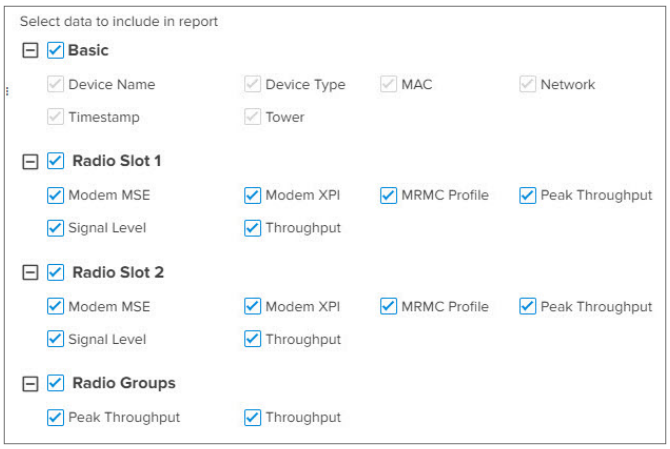
PTP 650/670/700 Performance Report

Figure 317 *Performance Report: PTP 650/670/700*



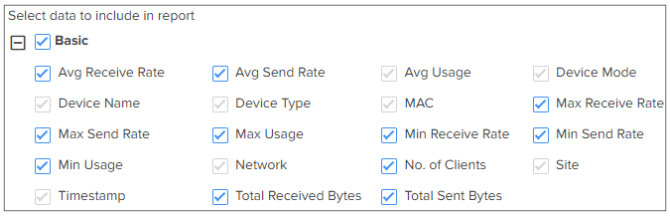
PTP 820/850 Performance Report

Figure 318 *Performance Report: PTP 820/850*



RV22 Home Mesh Performance Report

Figure 319 *Performance Report: RV22 Home Mesh*



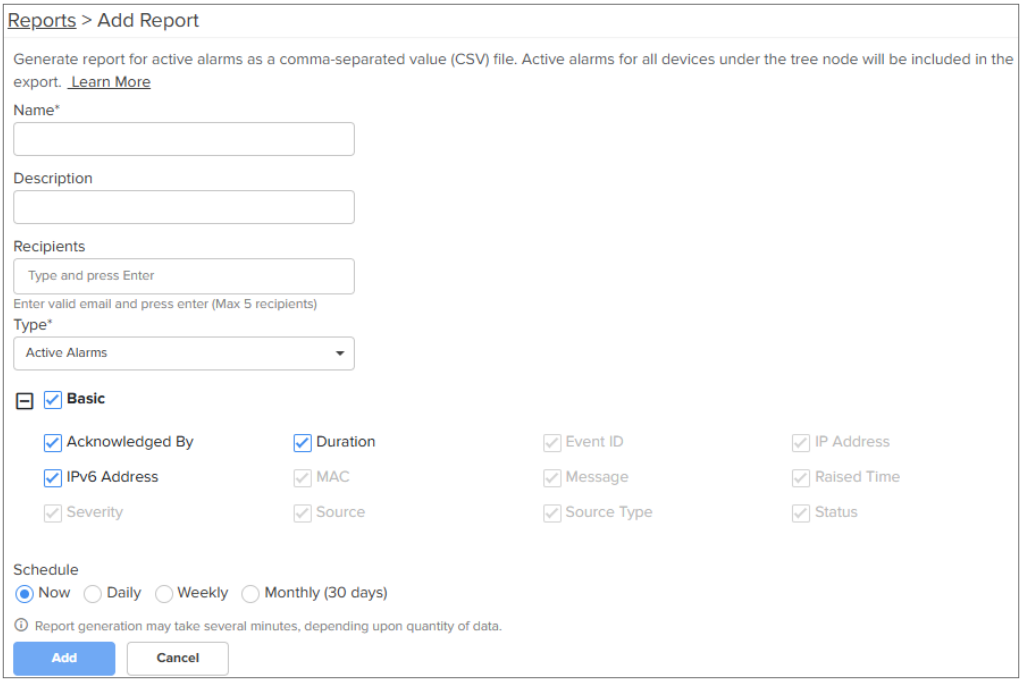
Active Alarms Report

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** > **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.



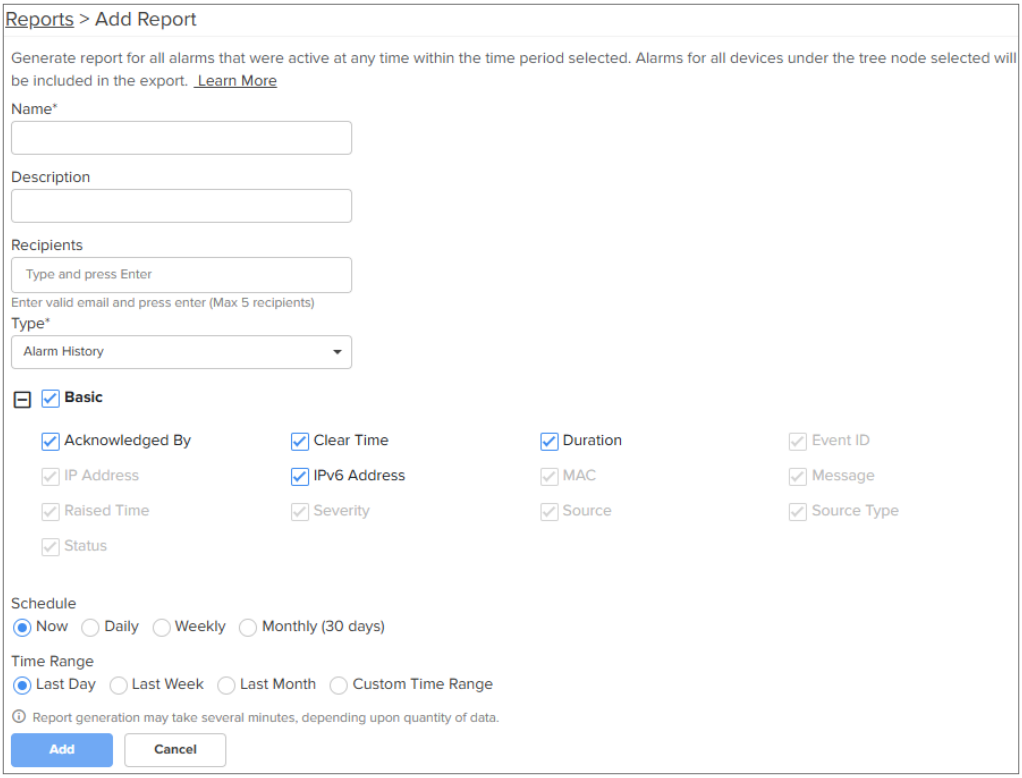
Alarm History Report

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** > **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.



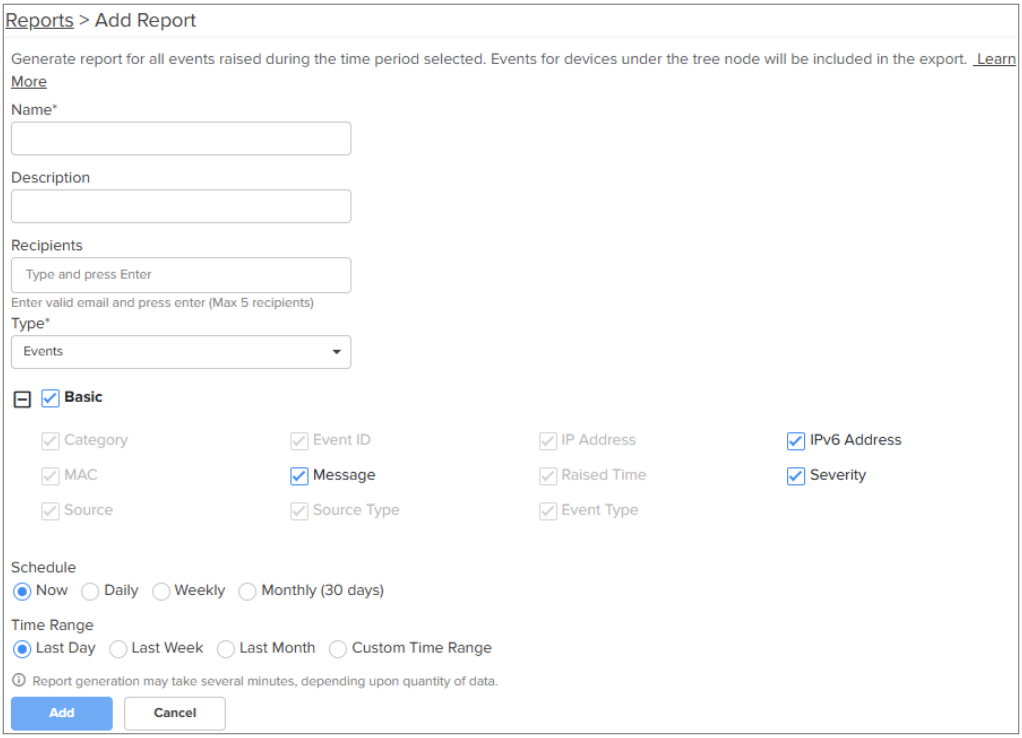
Events Report

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** > **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

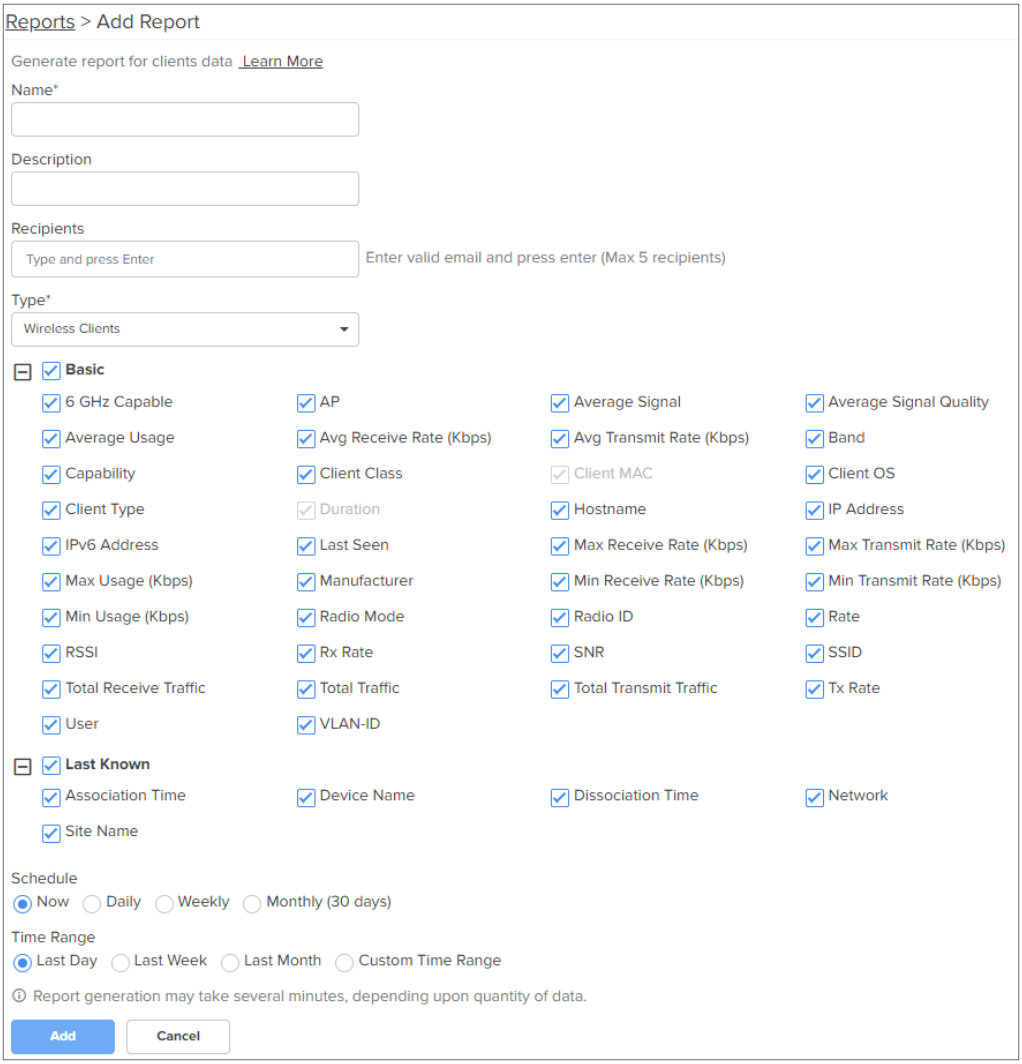
Client Data is available for the last day, last 24 hours, last week, and a maximum of 30 days.

To generate the Wireless Clients reports, perform the following steps:

1. Navigate to **Reports** > **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, Weekly, or Monthly (30 days))
   - Time Range (Last Day, Last Week. Last Month, or Custom Time Range (up to a maximum of 30 days))
8. Click **Add**. The report is saved and listed in the **Scheduled Reports** page.

Figure 320 *Wireless Clients Report*



Wi-Fi Events Report



Note

Wi-Fi events data is available for a maximum of seven days.

The Wi-Fi Events report generates the Wi-Fi events data that is available on the **Notifications** > **Wi-Fi Events** page.

To generate the Wi-Fi Events reports, perform the following steps:

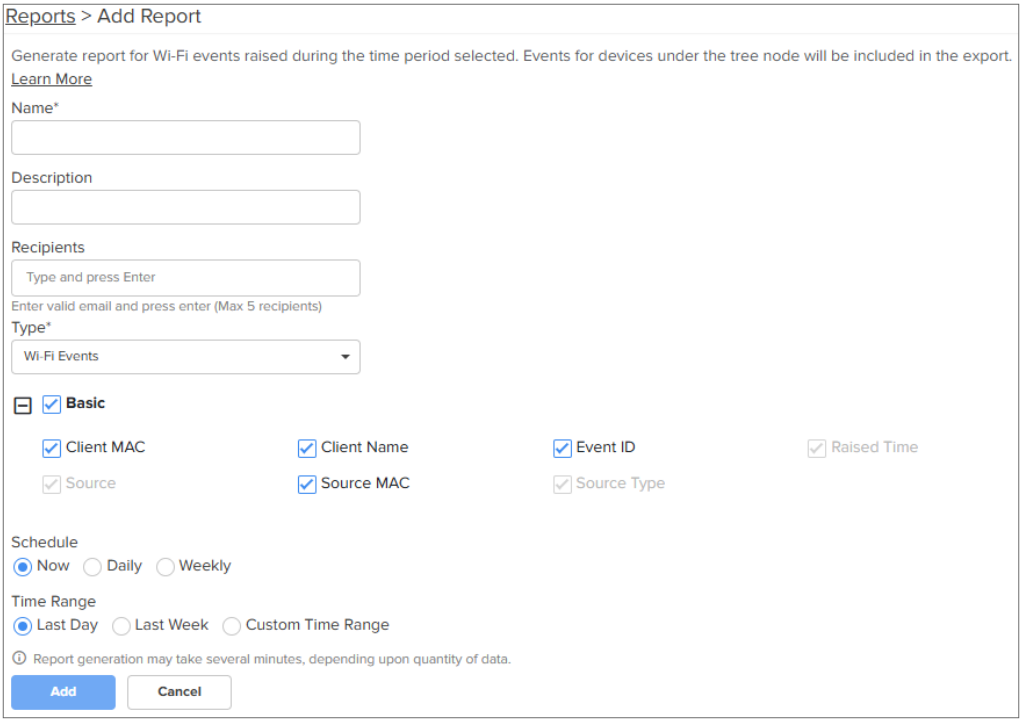
1. Navigate to **Reports** > **Scheduled** tab.
2. Click **Add New Data Report**.

   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 321 *Wi-Fi Events Report*



Guest Access Login Events

The Guest Access Login Events represent Wi-Fi guest access logins.

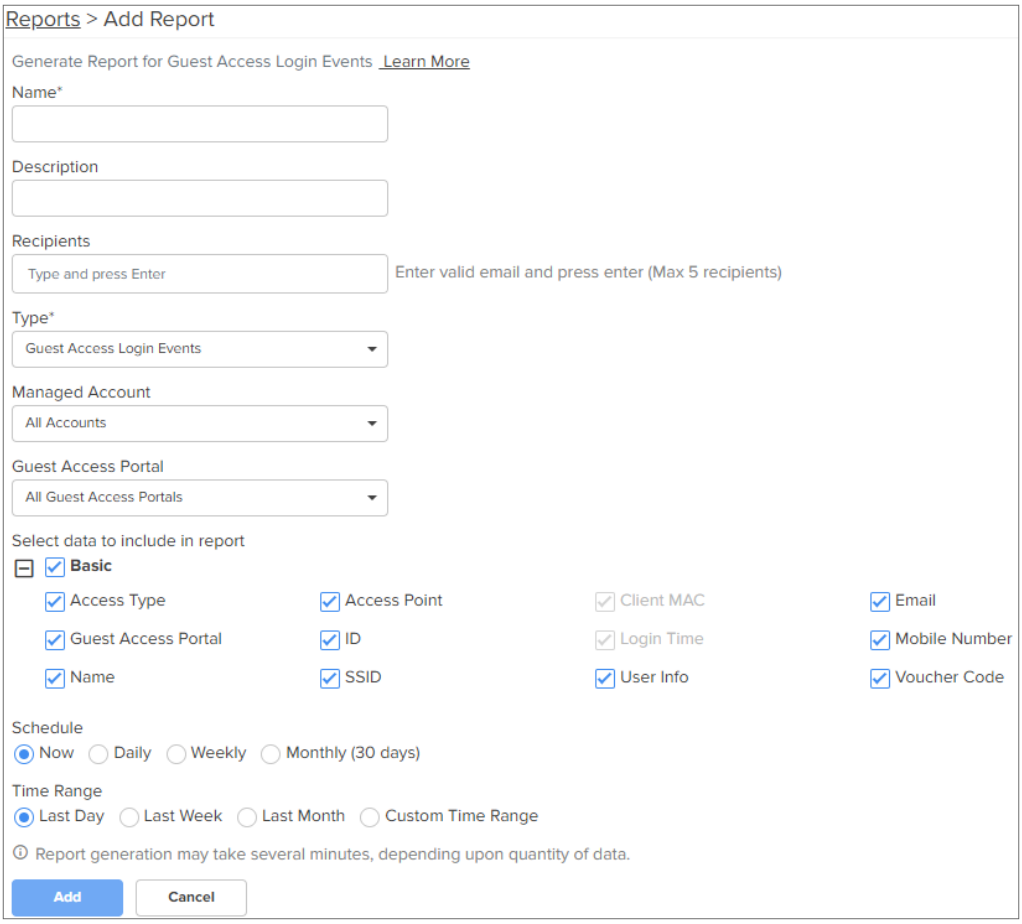
> **Note**
>
> - Guest access report can be generated only at the system level.
> - Guest access login data is available for a maximum of 90 days.

To generate the Guest Access Login Events report, perform the following steps:

1. Navigate to **Report X > Scheduled** tab.
2. Enter a **Name** and **Description** for the report.
3. Enter email addresses (maximum of 5) in the **Recipients** field to send reports.
4. Select the **Report Type** as Guest Access Login Events.
5. Select the **Managed Account**, if applicable.
6. Select the **Guest Access Portal**, if applicable.
7. Select data parameters to include in the report.
8. Select the following options:

- Schedule type (Now, Daily, Weekly, or Monthly (30 days))
- Time Range (Last Day, Last Week. Last Month, or Custom Time Range (up to a maximum of 90 days))

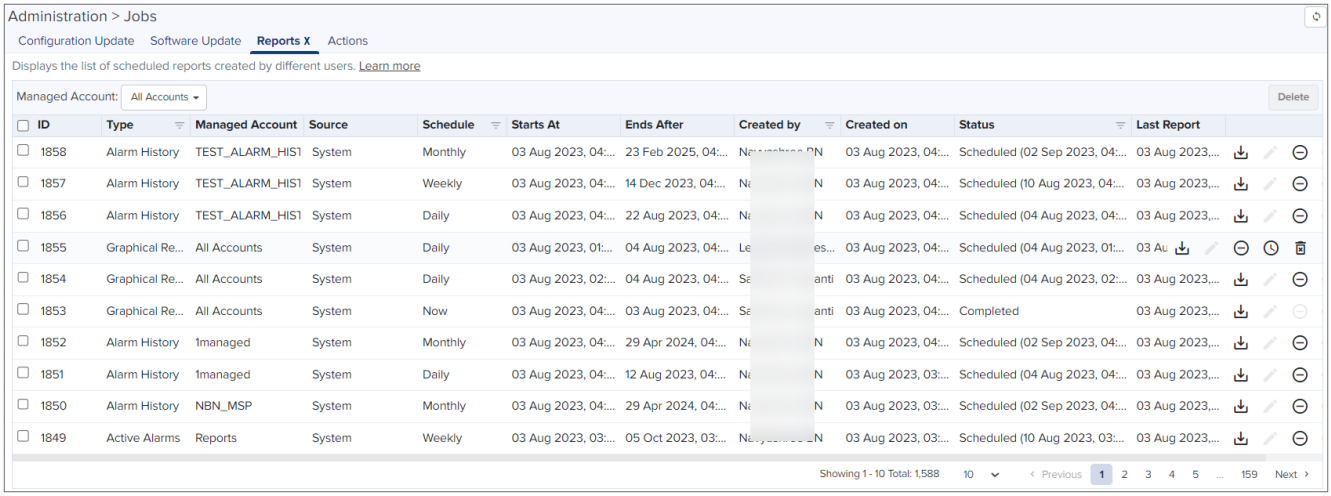
9. Click **Add**. The report gets added to the **Scheduled Reports** page.



Reports jobs

The report jobs displays the list of scheduled jobs created by different users. To view jobs, navigate to **Administration** > **Jobs** > **Reports**.

Figure 322 *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 323 lists the Graphical Reports widgets available in cnMaestro and the version they were introduced in.

Figure 323 *List of Graphical Reports widgets available*

Name of Widget	Version Introduced
Assurance	
Assurance: Top Access Points Reporting Client Disconnections—Top APs reporting client disconnections	4.1.0
Assurance: Top Client Connection Failures—Top client connection failure types by number of failures	4.1.0
Assurance: Top Affected Client OS by Failure Count	5.2.0
Assurance: Top Affected Client Types by Failure Count	5.2.0
Access Points	
Top Access Points by Traffic Usage—Top APs by traffic usage	5.1.0
Clients	
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

Name of Widget	Version Introduced
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
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:

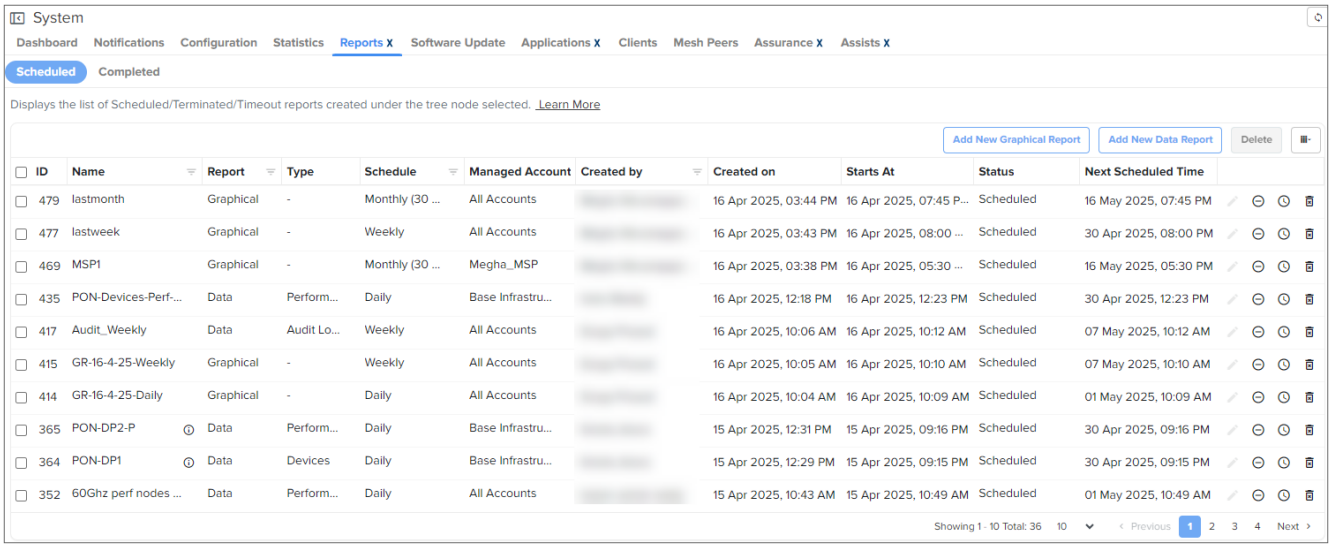
1. Create a template using the widgets listed above.
2. Select a level of the hierarchy on which to apply the template.
3. Schedule the report to either execute one-time or periodically.

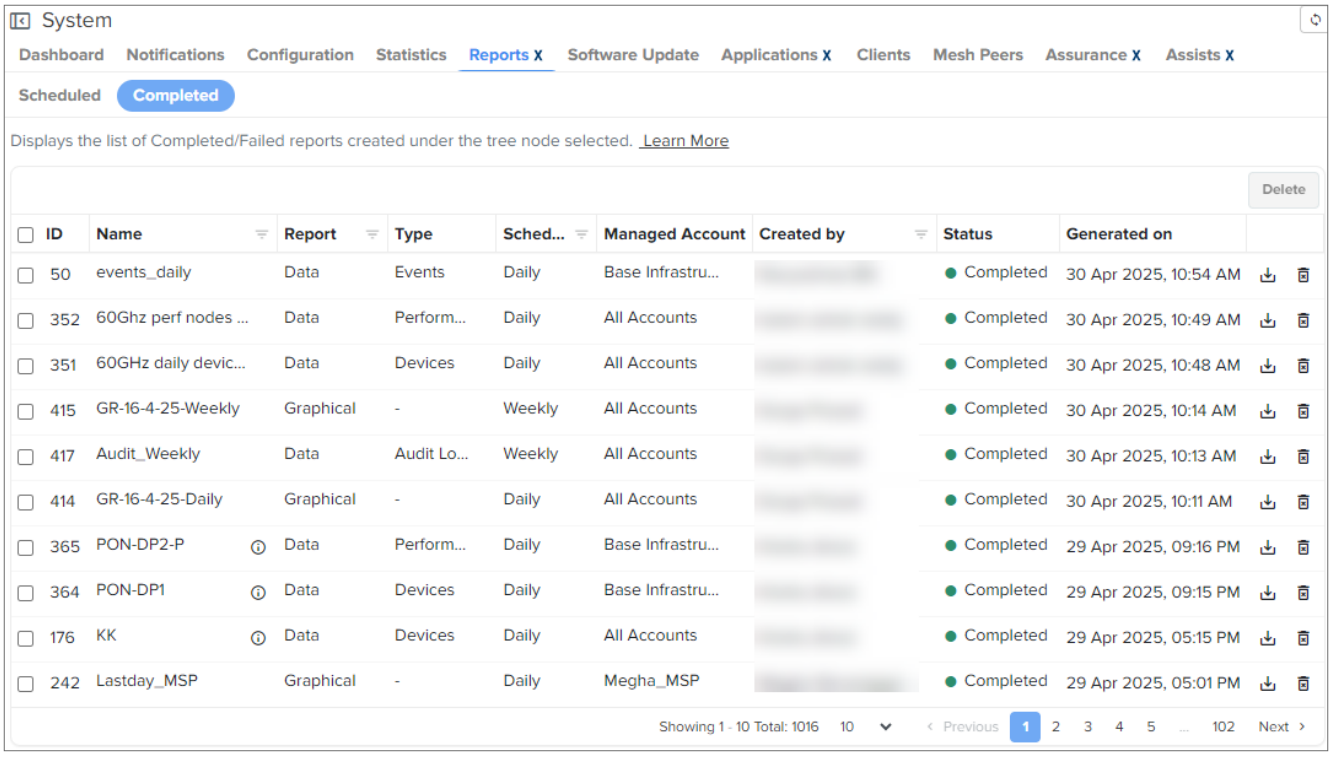


Note

- 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).





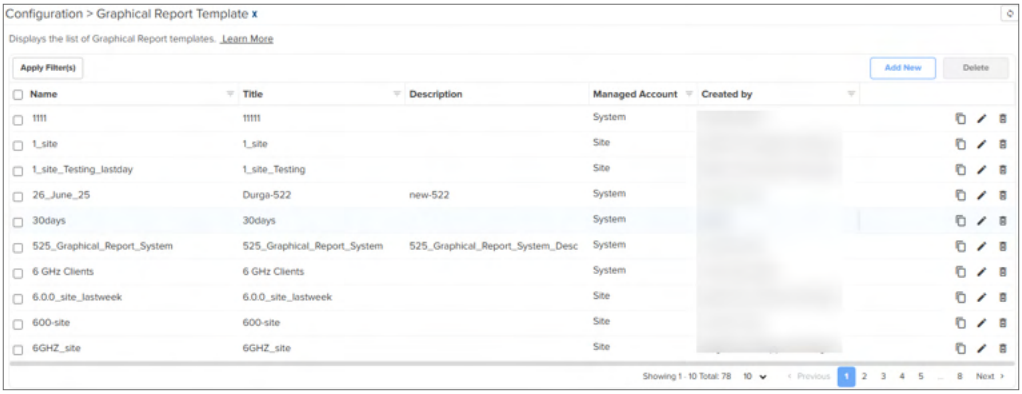
Refer to the following topics to create templates and schedule reports:

- Create Graphical Report Templates
- Generate Reports Based on Templates

Create Graphical Report Templates

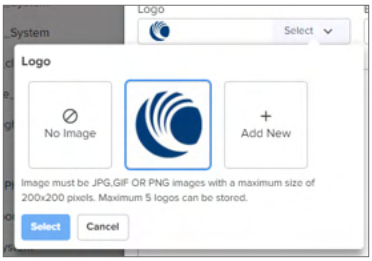
To create a graphical report template, complete the following steps:

1. Navigate to **Configuration > 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**.



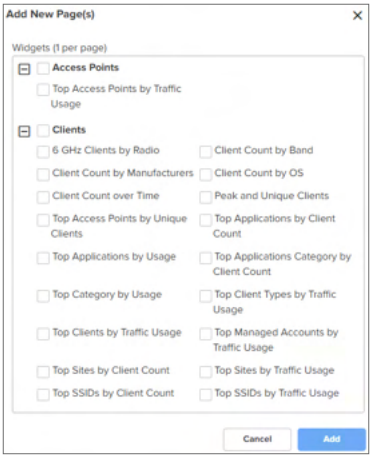
   - **Brand Image**—To select an existing brand image, click the down arrow, and then click **Select**. You can also add a new brand image by clicking **Add New**.
   - **Themes**—Select a theme for the title page of the report as either **Vertical Lines**, **Brand Box**, or **Plain**.



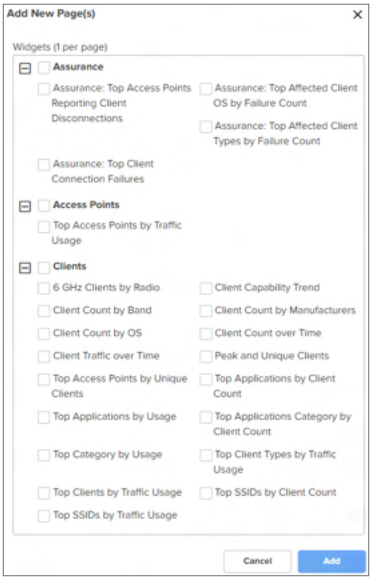
   - **Theme Color**—Select the Theme Color by clicking the desired colored square.
4. Click **Add**.

   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:

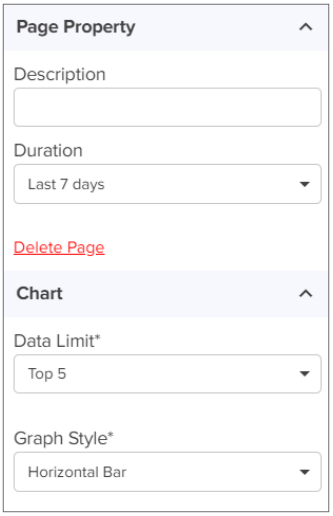


6. Select the checkbox for one or more Widgets and click **Add**. Each page can have only one widget. Drag and drop the pages in the left pane to rearrange the widgets.

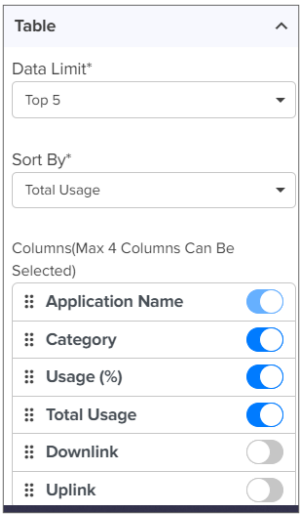


7. For each page, select the page properties in the right pane. They differ based on widget and options that you have chosen.

   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:

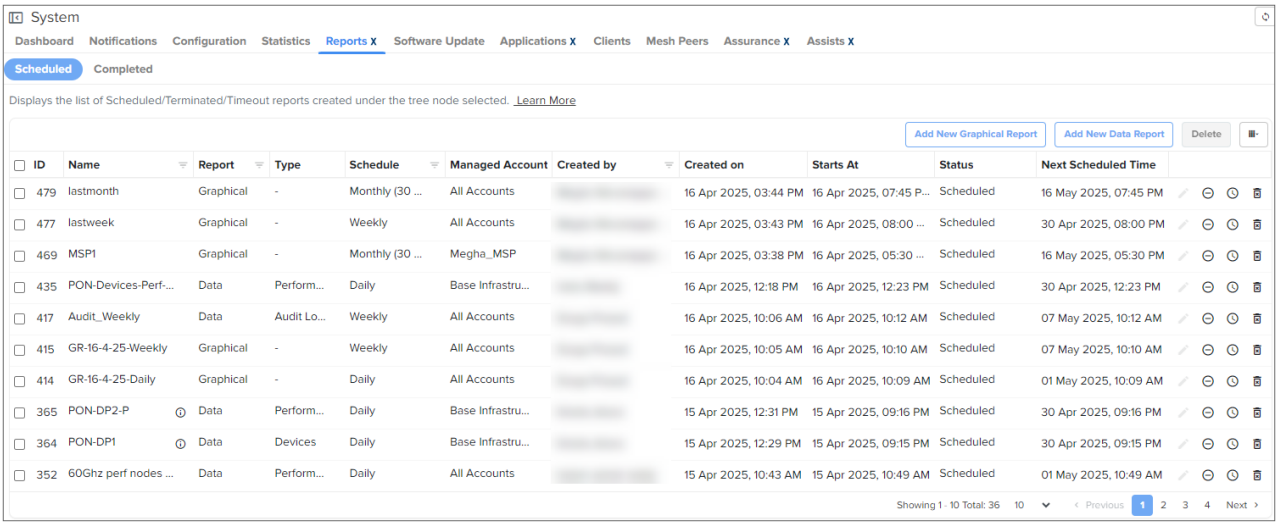
- **Title**—Title for the report.
- **Description**—Detailed information about the report criteria.
- **Duration**— Time interval. For example, **Last Day** or **Last 7 Days**.
- **Chart/Graph Style**— Type of graph. For example, **Horizontal Bar** or **Pie Chart**
- **Data Limit**—Volume of data to 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**.

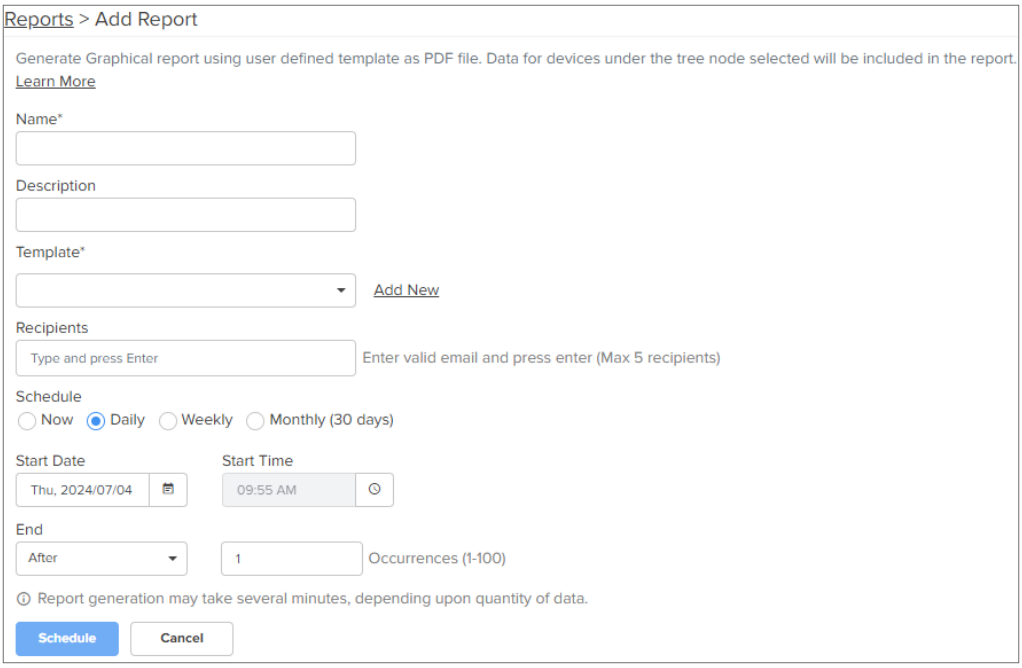
Generate Reports Based on Templates

To add a new report, follow the steps below:

1. Navigate to **Monitor and Manage** > **System** or **Site** > **Reports** > **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
- NSE 3000 Configuration
- Configuring Advanced Features
- Managing Home Mesh Router

Software Update

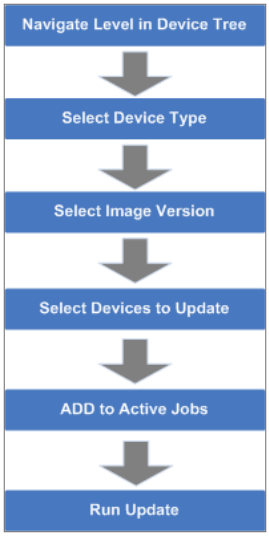
The **Software Update** tab displays the device update details. This section includes the following:

- Software Update Overview
- Create Software Update Job
- Software Update Jobs and Parameters
- Viewing Running Jobs in header

Software Update Overview

The Software Update feature allows users to deploy the latest software images to devices. Software updates can be started at any level in the Device Tree. Updates are created as Jobs and placed into the Jobs Queue. When the update is ready to run, it can be started. The process flow of Software Update is shown below:

Figure 324 *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

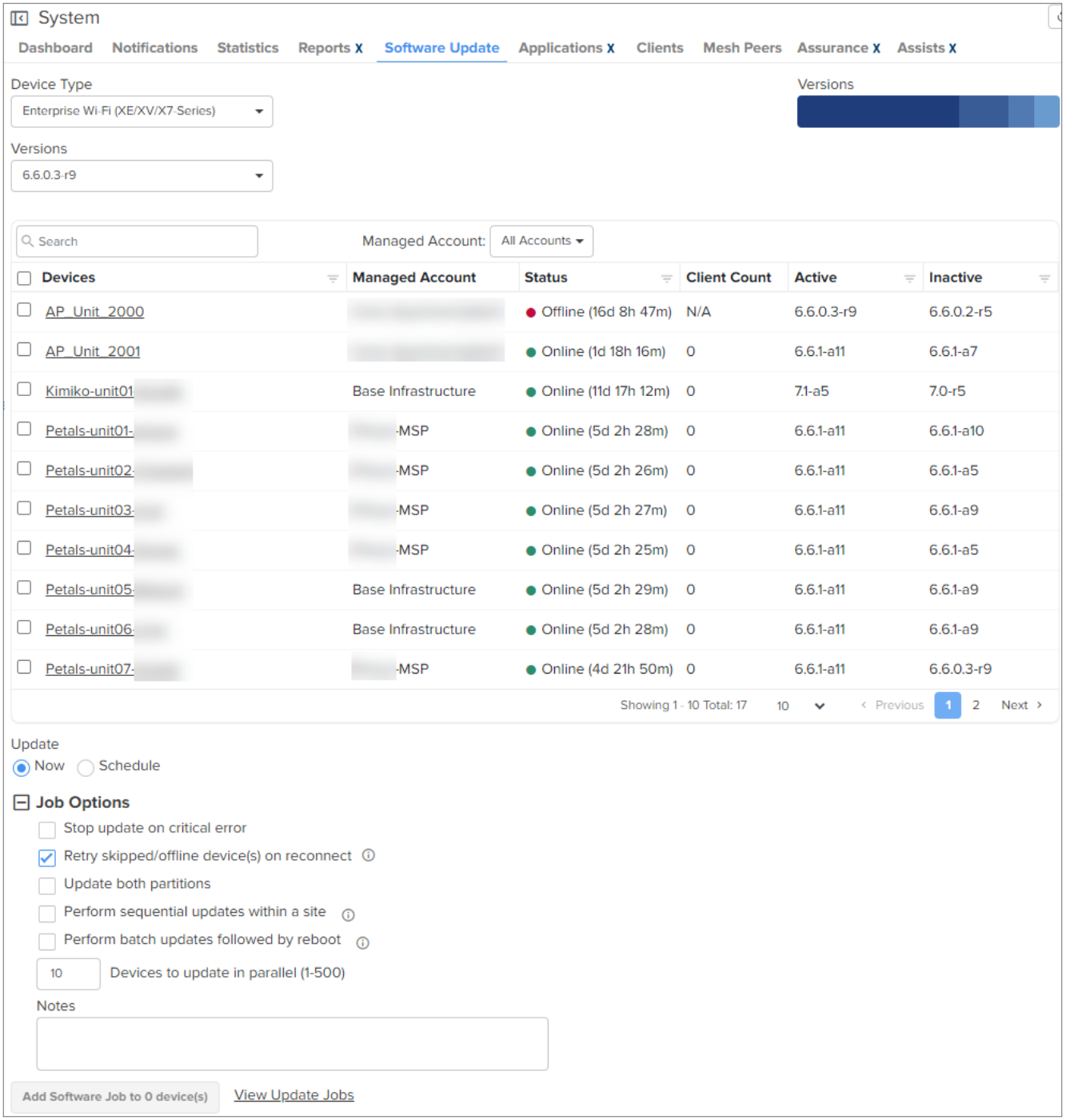
Once the device type is chosen, the UI displays the most recent software release version for that device type. It also displays a breakdown of the different software versions currently installed on the devices.

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 325 *Software Update: Enterprise Wi-Fi*



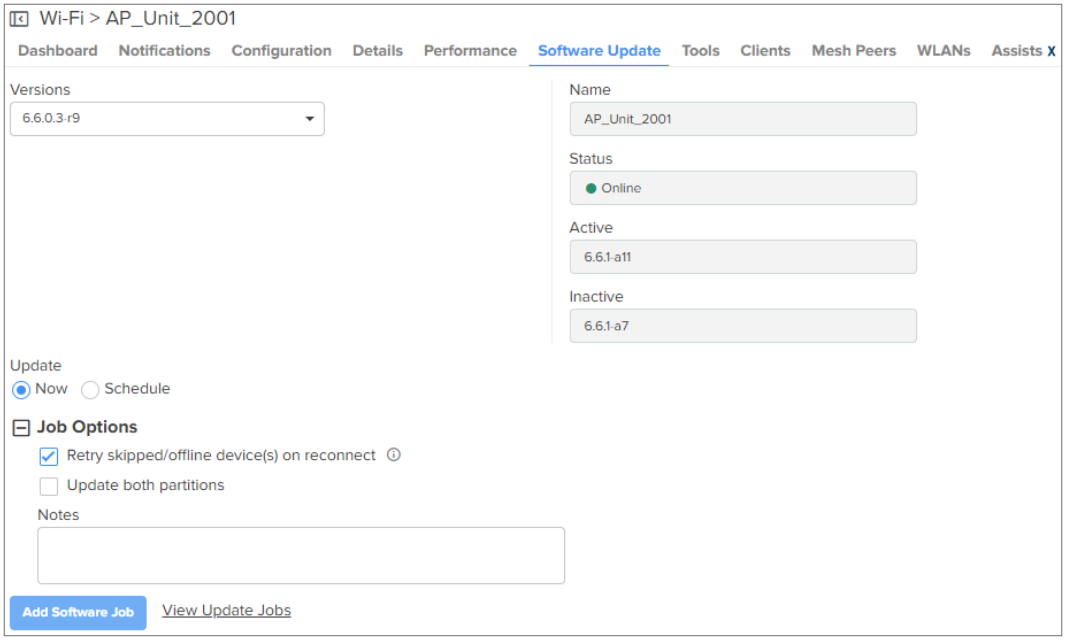
Note

- **Update both partitions** option is available at System/Network/Site/Device levels. It is only available for the devices that support it.
- **Perform sequential updates within a site** option is available at System/Network/Site level except the Device level.

If the **Update both partitions** option is enabled/ disabled, the device level of the Software Update will be displayed as follows:

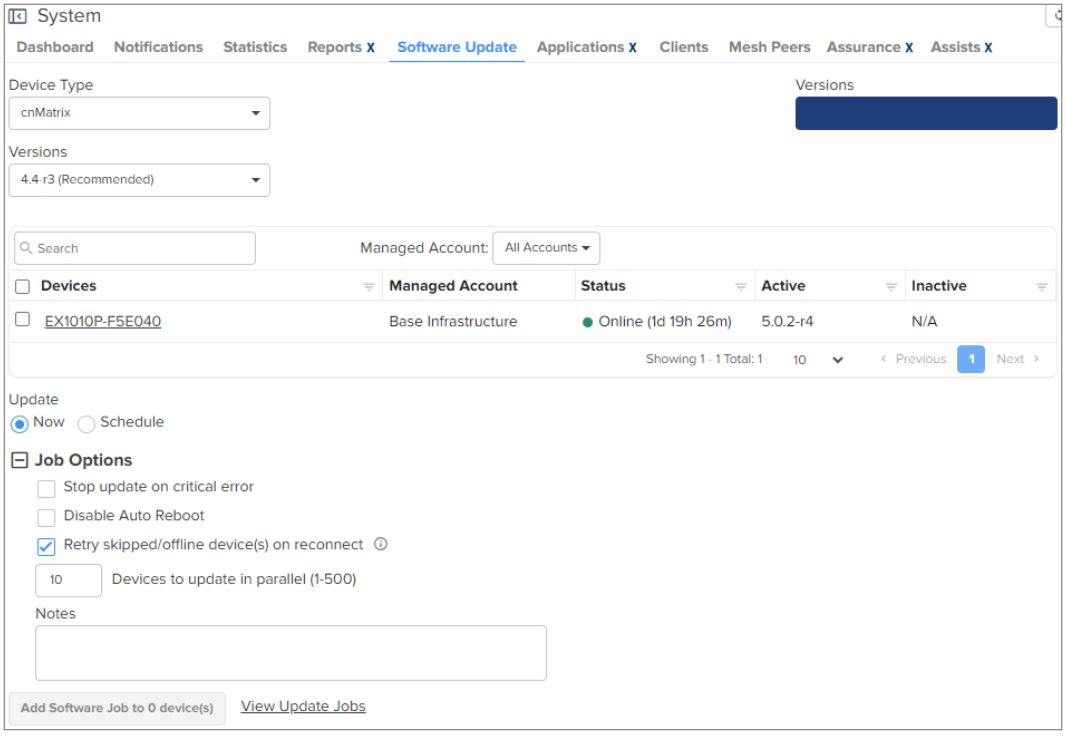
- **Enable**: Tp
- Selected target image will be upgraded in only active portion of the device.

Figure 326 *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 327 *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 328 *Software Update: cnRanger*

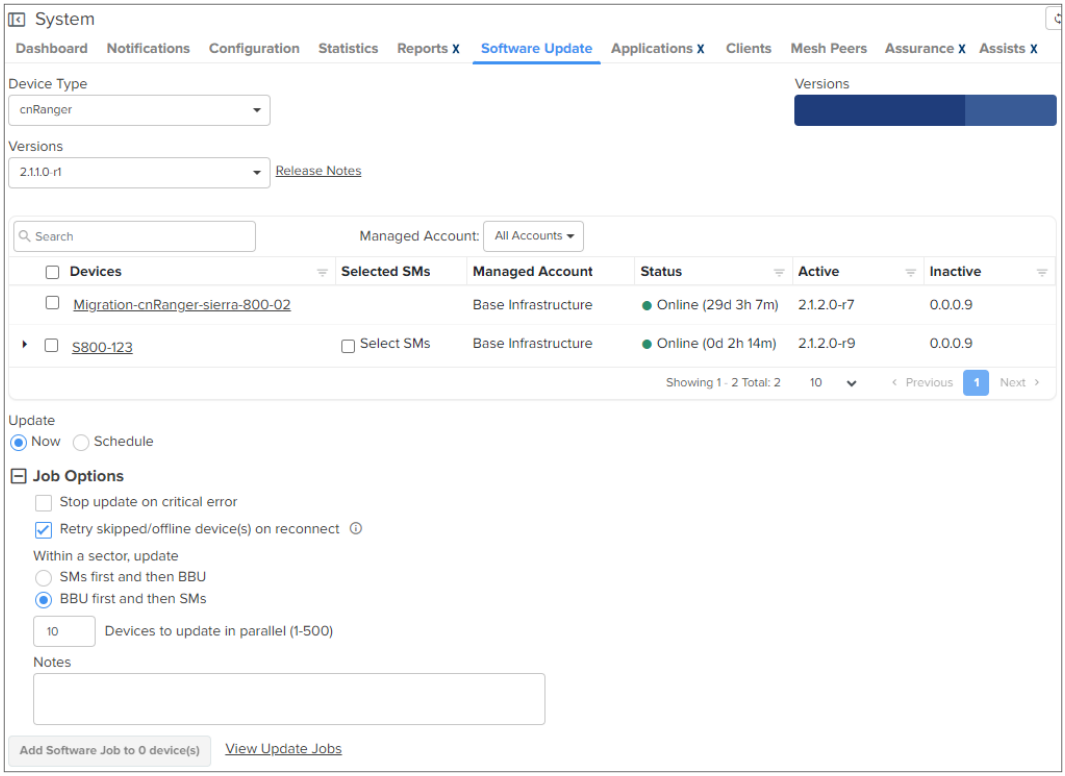


Figure 329 *Software Update: 60 GHz cnWave*

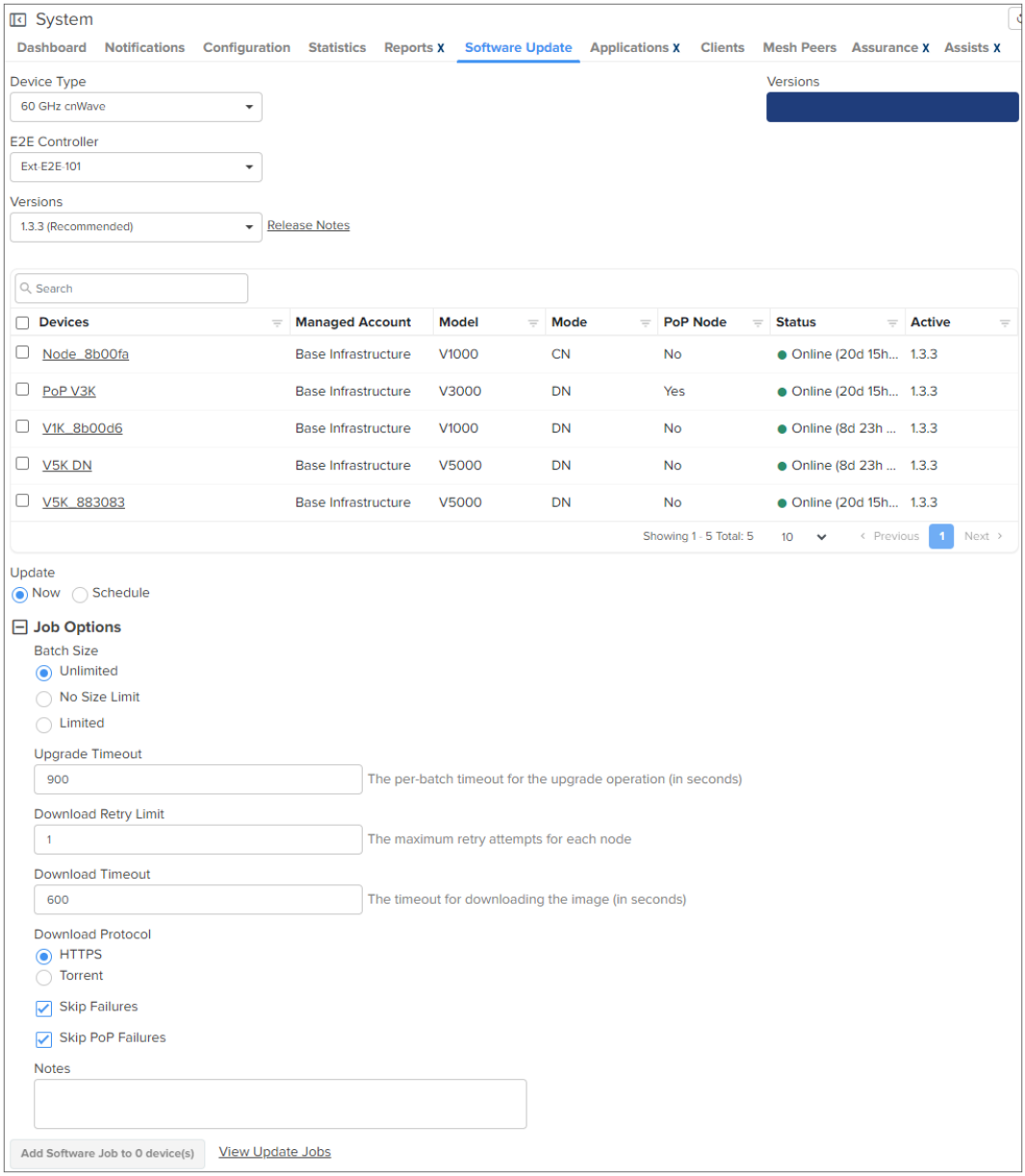
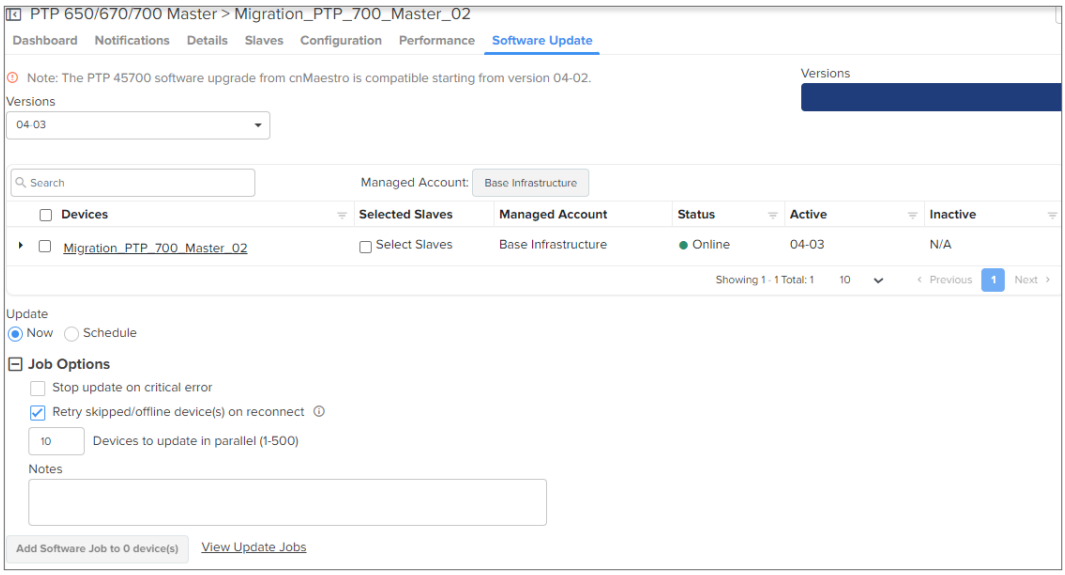


Figure 330 *Software Update: PTP 670/700*



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.

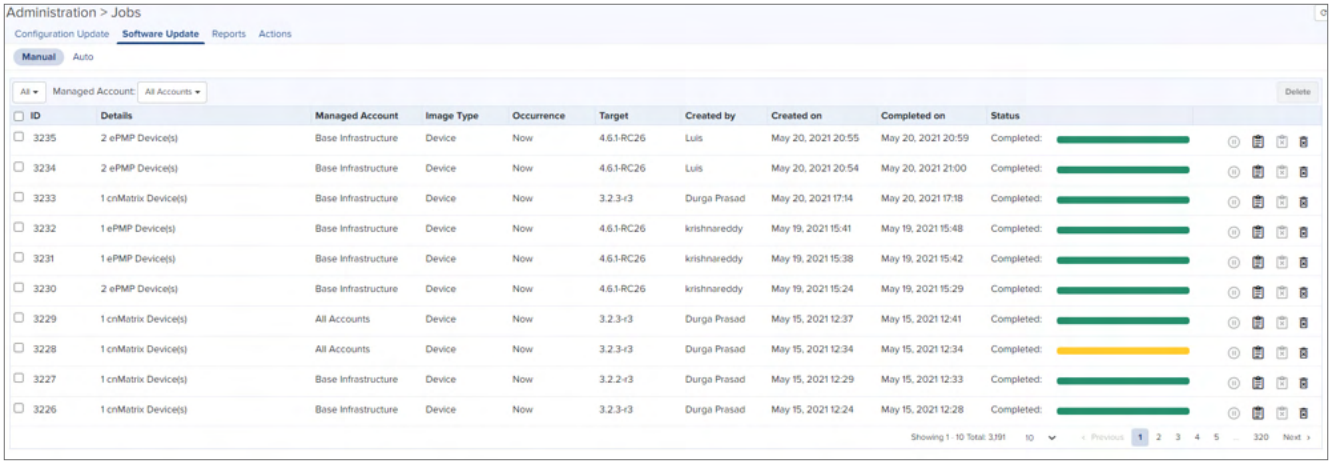
Software Update

The software version on the devices can be automatically updated to the preferred version when the device first contacts cnMaestro.

Enable the automatic update of device software as follows:

1. Navigate to **Administration** > **Jobs** > **Software Update** page**.**
2. Select the **Manual** or **Auto** page for updating the device software feature.
3. Choose the software version depending on the device type.
4. Click **Start.**

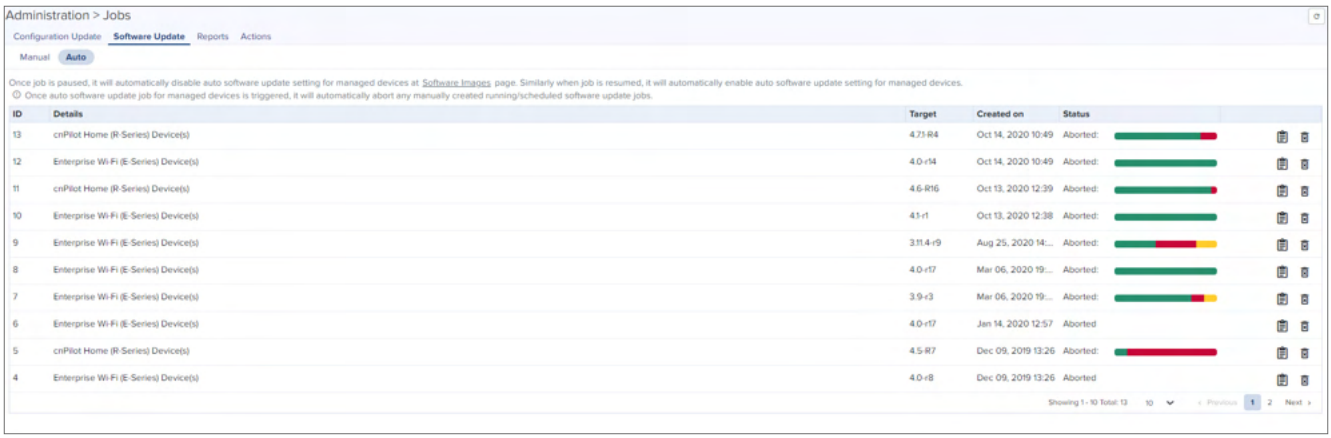
Figure 331 *Manual update*



Note

A Manual Update can be aborted at any point of time by clicking the Abort.

Figure 332 *Auto update*



Note

Auto update can't be manually aborted.

You need to download the new image version released from the Support Site. For more details refer to Managing Device Software Images.

Device Table

Select the devices to upgrade in the Devices Table.

Note

- You can upgrade a device only when status is Up. If you try to upgrade a device when it is Down, you will receive a message the selected device is down.
- If the device is under the Auto Software Upgrade, the manual software update is not possible.

The following parameters are visible (though some are only available for certain device types).

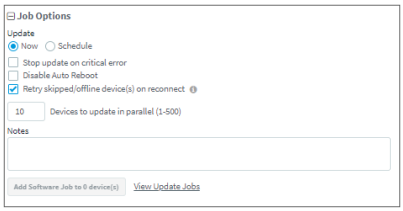
Table 70 *Parameters in Device Table*

Parameter	Description
Current Version	The version of the active software image running on the device.
Devices	The names of available devices in a system. The list is pre-filtered based upon the node selected in the Device Tree.
Selected SMs	If the AP is selected, the corresponding SMs will also be selected.
Status	The status of a particular device in a system. Devices that are not connected cannot 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 333 *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. NSE
   m. PMP (Sectors)
   n. PON
   o. PTP 670/700
   p. PTP 820/850
   q. RV22 Home Mesh
3. Select the software image to update from the **Versions** dropdown list.
4. Select checkbox for the devices to update.
5. Expand the **Job Options** section and configure the required parameters.

   The job options available vary for different devices.
6. Click **Add Software Job to** <Number of devices> **device(s)**.

Software Update Jobs and Parameters

The Software Update Jobs table lists all currently running, queued, and completed jobs. The jobs can be triggered immediately, or they can be run later.

(**Administration** > **Jobs** > **Software Update** tab.)

The following table displays the list of parameters in the **Software Update Jobs** tab:

Table 71 *Parameters in Software Update Jobs*

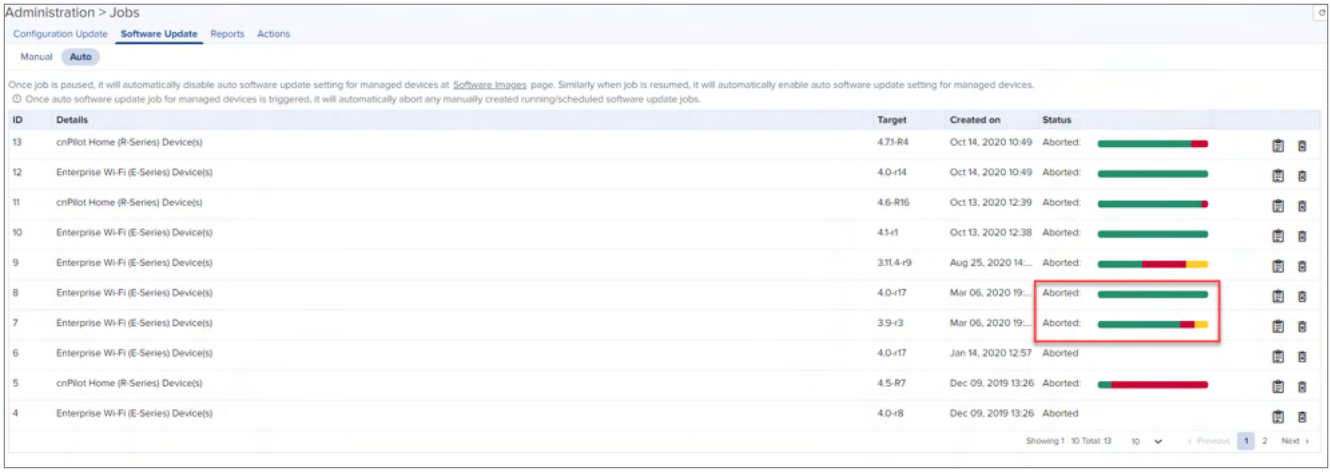
Parameter	Description
Action	Use the **Start** or **Delete** button to manage the upgrade process. After the upgrade has started, the **Pause** button will stop new upgrades from the beginning. If the upgrade process fails or the upgrade has been paused, you can restart the process by clicking the **Resume** button.
Created By	The user who has created this job.
Created On	Date and time the job is created.
Details	Count of devices and date and time the upgrade process is initiated.
ID	Identification number of the active job.
Image Type	Displays **Device** for Device Firmware Upgrade.
Occurrence	Displays **Now** and **Scheduled** depending upon the job options selected during Software Update Job.
Parallel	Number of devices to start in parallel.
Sector Priority	For cnVision, ePMP/PMP, the priority of AP/SM to start.
Status	Status of update.
Stop on Error	Stop the job on an error in any device update.
Target	Target software version to upgrade.
By selecting the **Show More** icon, you can view the following parameters:	
Device	Device for which the upgrade is initiated.
Message	The message that is displayed after the update.
Original Version	The current software image version of the device.
Result	The upgrade status of the device.
Status	Status of the device.

The user can filter the jobs based on the running status. The user can also filter the devices in a particular job based on the parameters mentioned in the above table.

Abort Software Job

Abort operation will skip devices that are waiting for an update to begin. Devices already being updated may continue, but cnMaestro will stop tracking their progress. Aborting a Software Job puts the device into a "Completed" state that cannot be manually restarted by the user. The "pending" devices will not begin their updates.

Figure 334 *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

Fixed Wireless Configuration

This chapter provides the following information:

- Overview
  - Configuration Templates
  - Configuration Variables
  - Macros
  - Variable Caching
  - Device Type-Specific Configurations
  - Variable validation

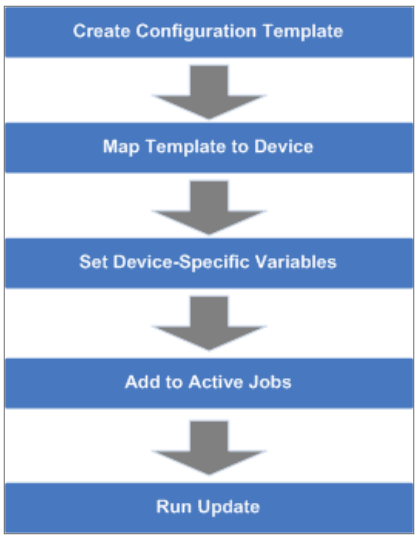
    - Sample Templates
    - Template file creation
- Template
    - BTS and CPE Configuration
    - Configuration Template for PTP 820/850
- By selecting the Custom option under the Template type filter All Default templates will be hidden.
- Configuration Jobs
- Configuration Update at Onboarding

Overview

Template configuration is supported for ePMP, PMP, cnWave 5G Fixed devices. Templates are textual representations of device settings that contain a full or partial configuration. When a template is applied to a device, the only parameters changed are those in the template.

The process flow of the basic template configuration is shown below:

Figure 335 *Basic Template Configuration Flow*



Configuration Templates

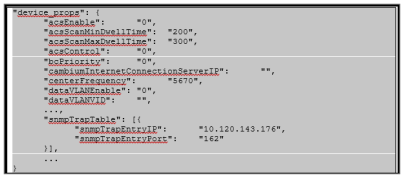
Templates can be pushed to a device manually through a configuration job. This is accomplished in the configuration management page. Templates can also be applied prior to onboarding, in which they would be provisioned in the Onboarding Queue.

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 336 *Sample ePMP Template*



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:

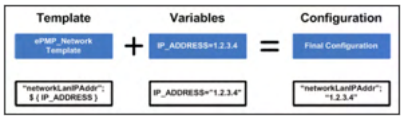
“networkLanIPAddr”: ${IP ADDRESS="10.1.1.254"},

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 337 *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

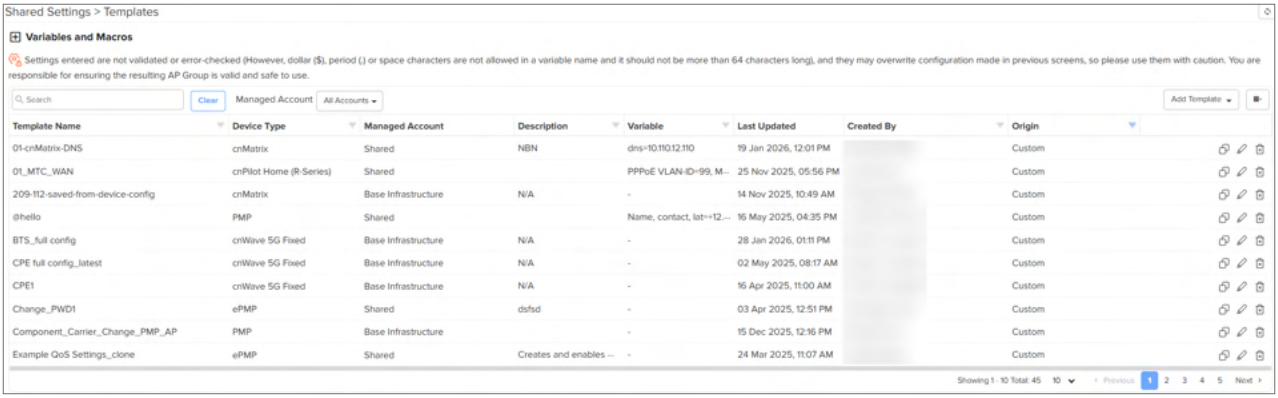
The typical process for creating your own configuration templates is below:

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.

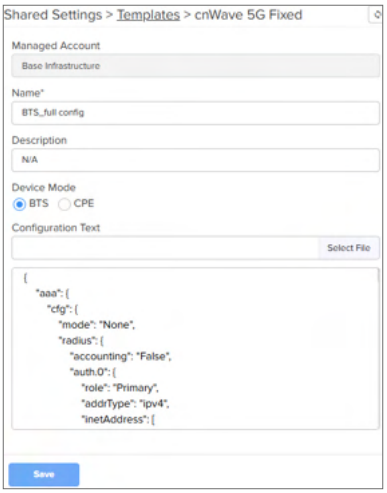
Template

To create a configuration template:

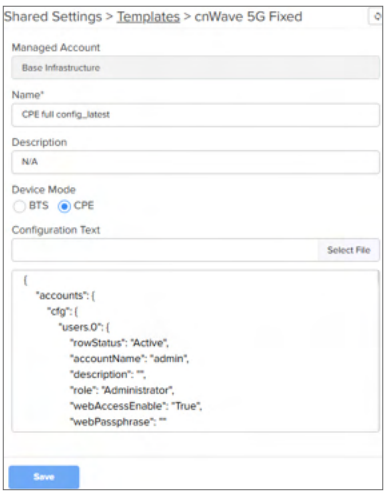
1. Navigate to **Configuration > Templates** in the main menu.



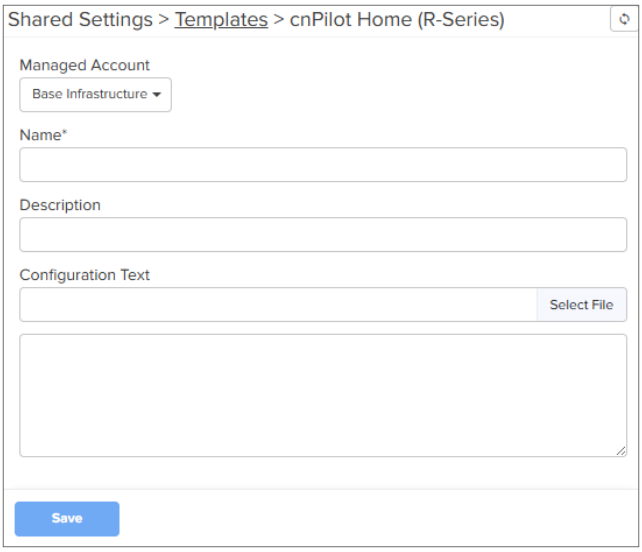
The following template is for BTS:



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.

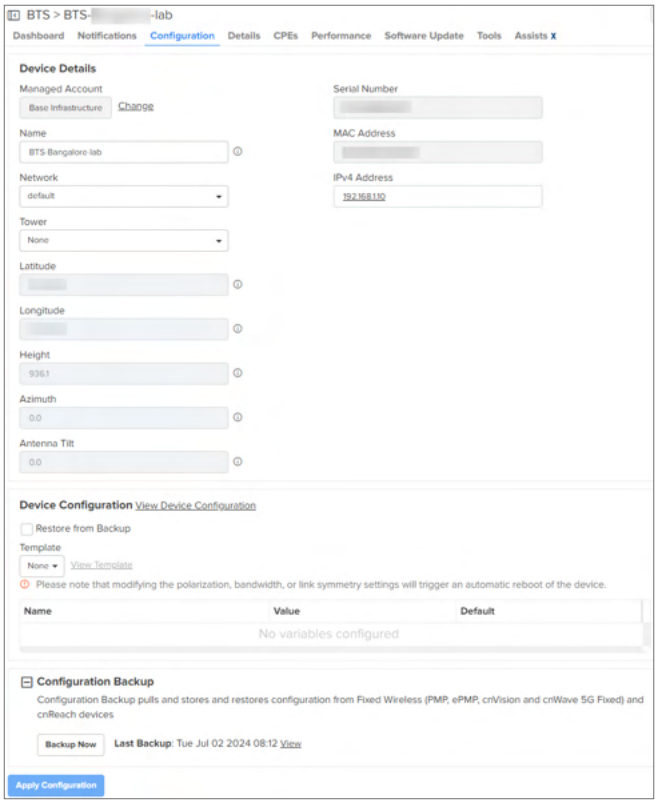
5. After clicking **Save**, the template will be available in the selection menu on the configuration and onboarding pages, as long as the device type and model match the device selected.
6. By selecting the Custom option under the Template type filter All Default templates will be hidden.

Note

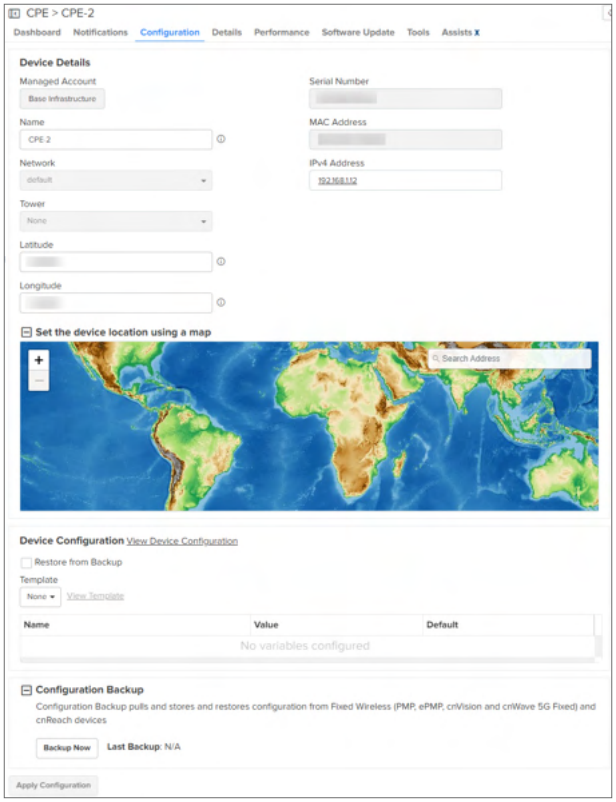
When you navigate to the Template page default template type filter will be custom. User needs to select **All** or **Default** to view other templates.

BTS and CPE Configuration

To configure BTS, navigate to **Monitor and Manage** > **BTS** > **Configuration**.



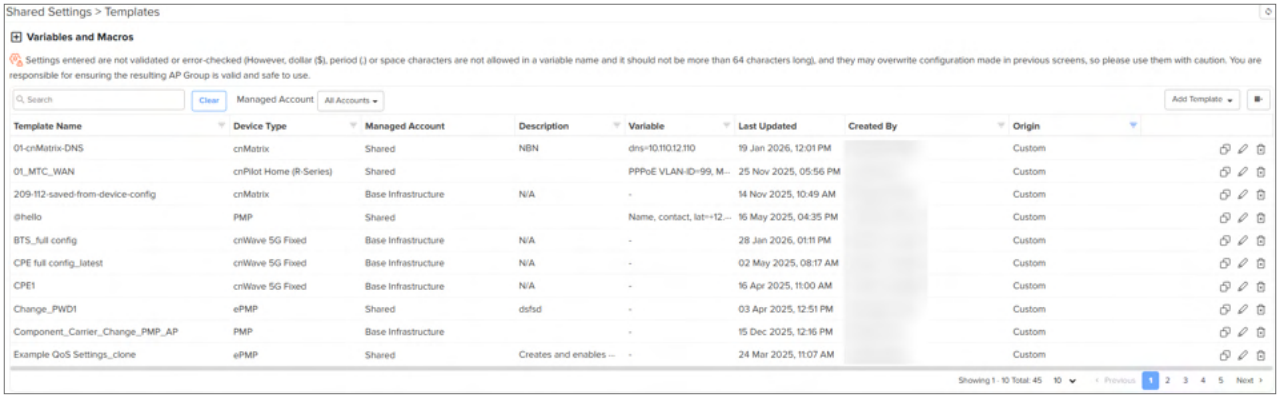
To configure CPE, navigate to **Monitor and Manage** > **BTS** > **CPE** > **Configuration**.



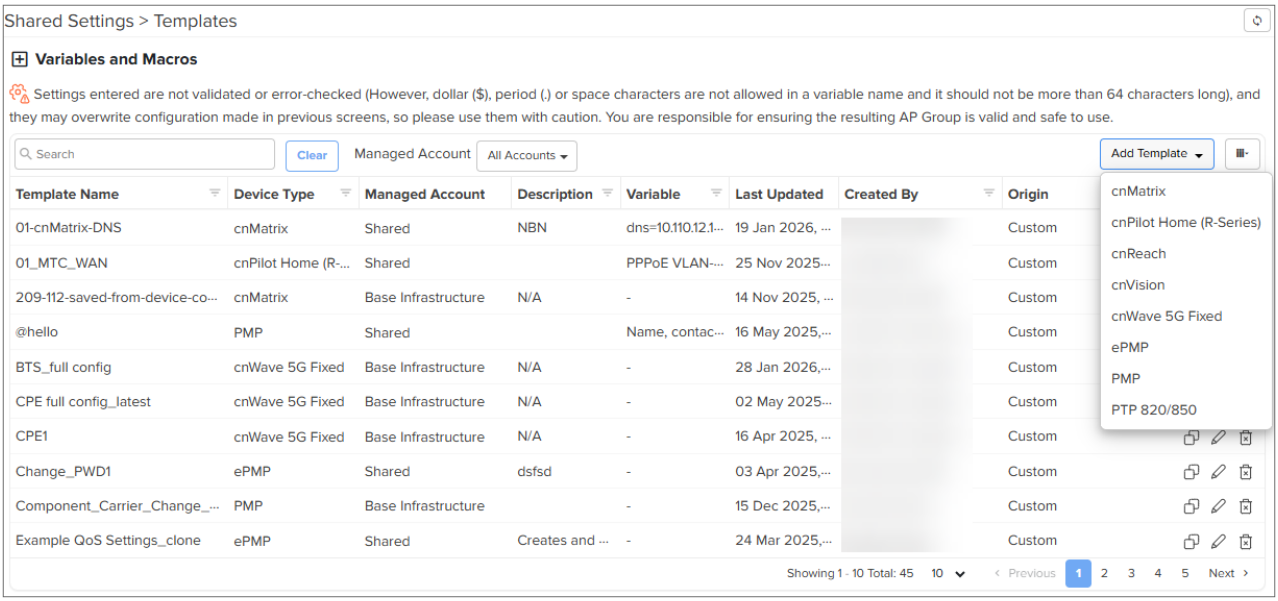
Configuration Template for PTP 820/850

To create a configuration template of PTP 820/850 device, perform the following steps:

1. Navigate to **Configuration > Templates** in the main menu.



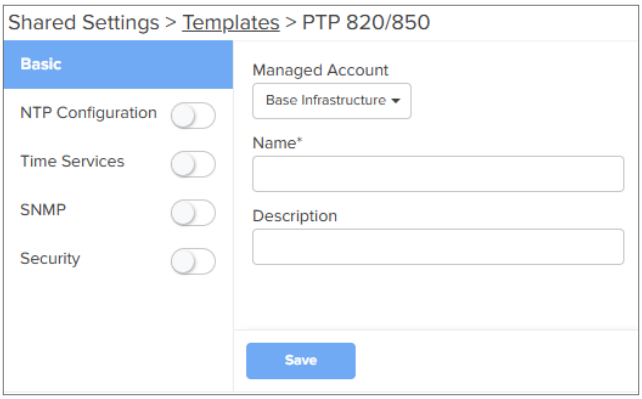
2. In the **Add Template** dropdown, select PTP 820/850.



The **Basic** template page appears.

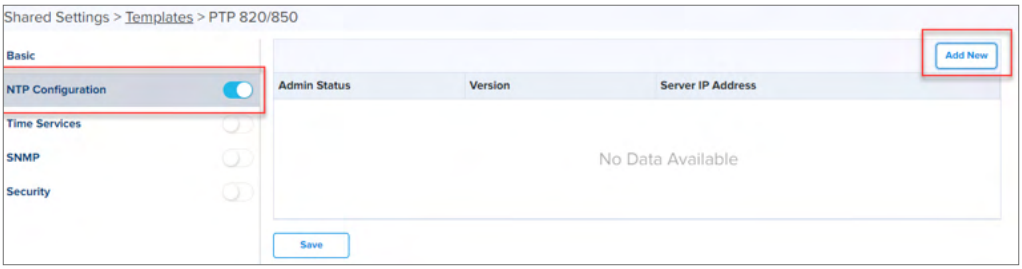
3. In the **Basic** page, enter **Name** and **Description** and click **Save**.

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.



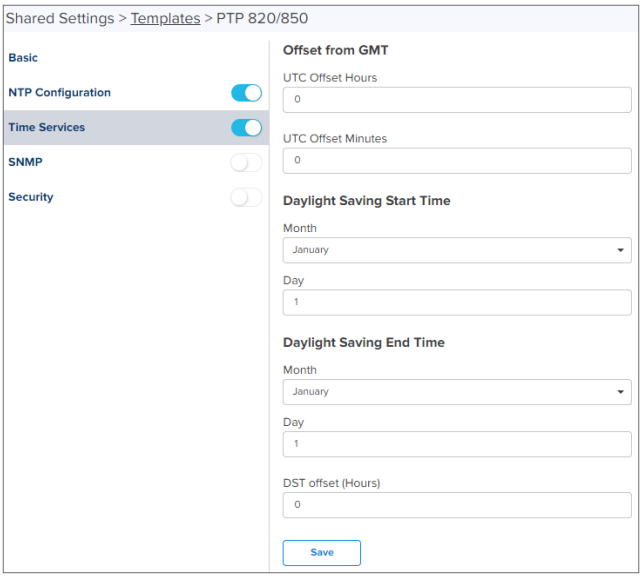
2. Select **Admin Status** from dropdown.
3. Select **Version** from dropdown.
4. Enter **Server IP Address**.
5. Click **Save.**

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

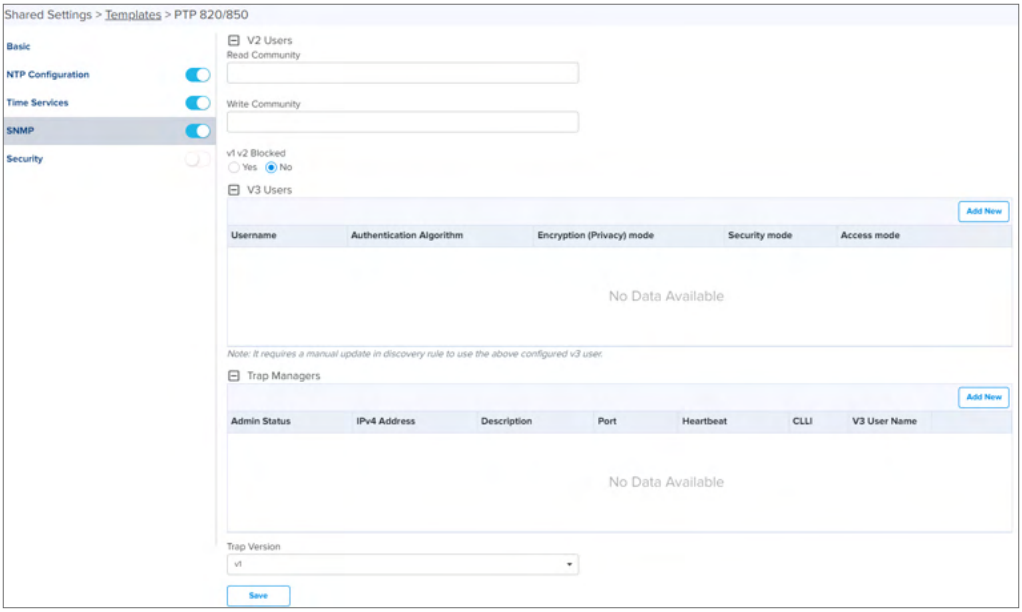
1. Enter the values for the following fields:
   - Offset from GMT
   - Daylight Saving Start Time
   - Daylight Saving End Time



2. Click **Save**.

SNMP

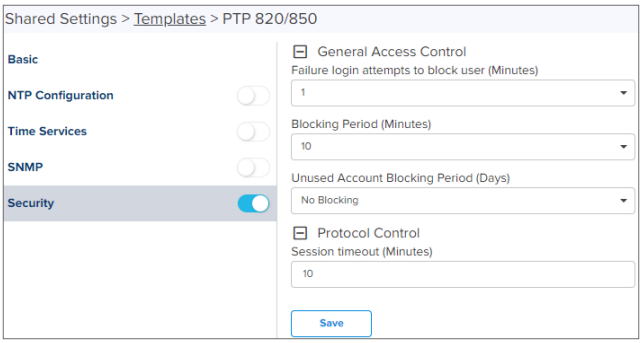
1. Enter the details for **V2 Users**, add **V3 Users** and **Trap Managers**, and select **Trap Version**.



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 72 *Device Table parameters*

Parameter	Description
Devices	The names of available devices in a system. The list is pre-filtered based upon the node selected in the Device Tree.
Network/Tower	The network and the tower on which the device is located.
Status	The status of a particular device in a system. Devices that are “Down” can not have images pushed to them.

Note

- You can only push configuration to a device when its status is **Up**.
- The user should validate the configuration before pushing it to the device from cnMaestro.

Options

Stop all Configuration on a Critical Error

If one of the configuration updates fails, then do not start any additional updates and instead pause the update job. All existing, concurrent updates will be allowed to proceed until completion. The administrator will be able to continue the update where it left off.

Parallel Upgrades

Define how many configuration updates to perform in parallel.

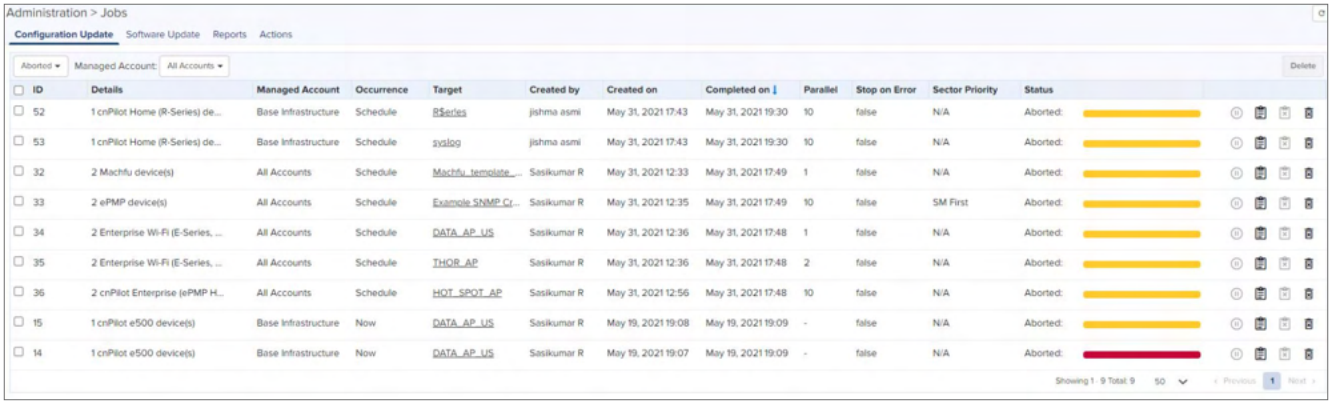
Update Ordering

Allows you to specify update ordering within a Fixed Wireless sector. Options are SMs first and then AP or AP first and then SMs.

Abort Configuration

Abort operation will skip devices that are waiting for update to begin. Devices already being updated may continue but cnMaestro will stop tracking their progress. Aborting a Configuration Job puts the device into a complete state that cannot be manually restarted by the user. The pending devices will not begin their updates.

Figure 338 *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**.

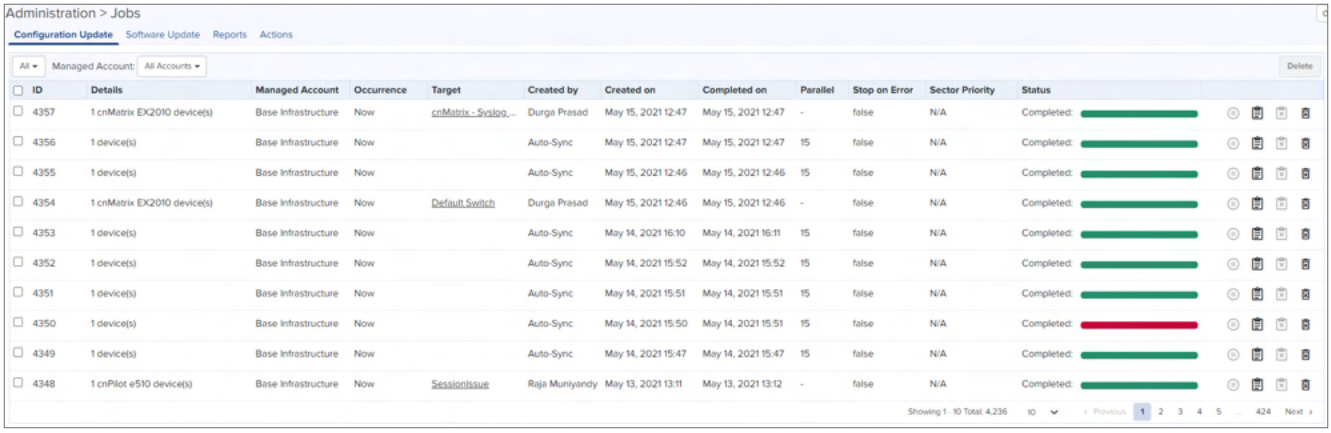
Note

- 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 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:



Note

cnMaestro X account user can run any number of **Jobs** in parallel.

The following table displays the list of parameters in the **Jobs** tab:

Table 73 *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

Table 73 *Configuration Update parameters*

Parameter	Description
	Resume button.
Created By	The user who has created this job.
Created On	Date and time on which the job is created.
Details	Count of devices and date and time the upgrade process is initiated.
ID	Identification number of the active job.
Parallel	Number of devices to start in parallel.
Sector Priority	For ePMP/PMP, cnRanger, cnVision Hub/Client, the priority of AP/BBU/SM to start.
Status	Status of update.
Stop on Error	Stop the job, if any device in middle finds any error.
Target	Target software version to upgrade.
By selecting the **Show More** icon, you can view the following parameters:	
Device	Device for which the upgrade is initiated.
Message	The message displayed after the update.
Result	The upgrade status of the device.
Status	Status of the device.
Mode	SM or AP mode selected.
Network	Type of Network.
Tower	Name of the Tower.

Configuration Update at Onboarding

Administrators can apply the configuration to devices during the onboarding process: Prior to approving the device in the Onboarding Queue, the configuration template and variables can be specified. These will then be pushed to the device during onboarding. For more details on onboarding, see Device Onboarding.

Wi-Fi Configuration

Wi-Fi configuration is handled through AP Groups or Templates, which Fixed Wireless devices, such as ePMP and PMP, exclusively use Templates. This section will focus exclusively on AP Groups.

This chapter provides details on the following sections:

- Enterprise Wi-Fi AP
- Factory Reset
- Association ACL
- Access Control Policies
- Custom Applications

Enterprise Wi-Fi AP

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
- cnPilot Home (cnPilot R-series devices)
- Enterprise Wi-Fi (Xirrus-Series)
- RV22 Home Mesh Routers

These four hardware types map to the following AP group types:

- Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)
- Enterprise Wi-Fi (Xirrus-Series)
- cnPilot Home (R-Series)
- RV22 Home Mesh

Multiple AP Group types are needed, because the features available across the groups are different.



Note

Wi-Fi devices can alternately be configured using a template mechanism, in which a subset of configuration is pushed to the device manually through a user-defined template of parameters. See the section on Templates for more information. Template configuration and AP Group configuration cannot be used simultaneously.

Configuring Enterprise Wi-Fi APs using Wi-Fi Profiles

Wi-Fi devices are configured by creating an AP Group, mapping it to 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.

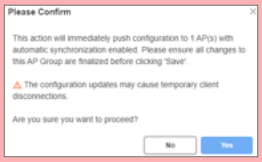


Warning

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 339 *Warning when modifying WLAN*

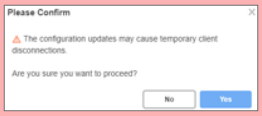


- Auto Sync is enabled and if no devices are present in the AP Group:

  OR

  Auto Sync is disabled and regardless of devices present or not in the AP Group:

  Figure 340 *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 341 *Basic: cnPilot Home (R-Series)*

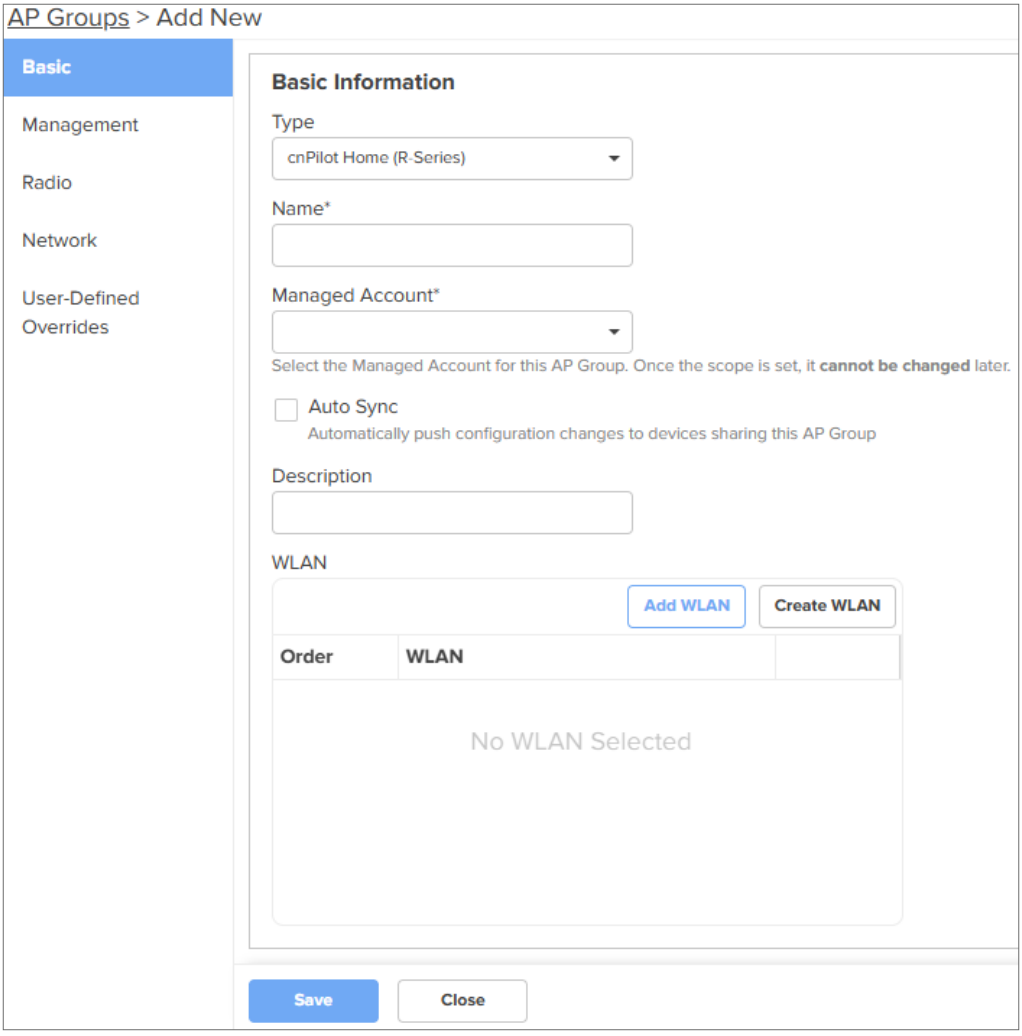


Figure 342 *Basic: Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)*

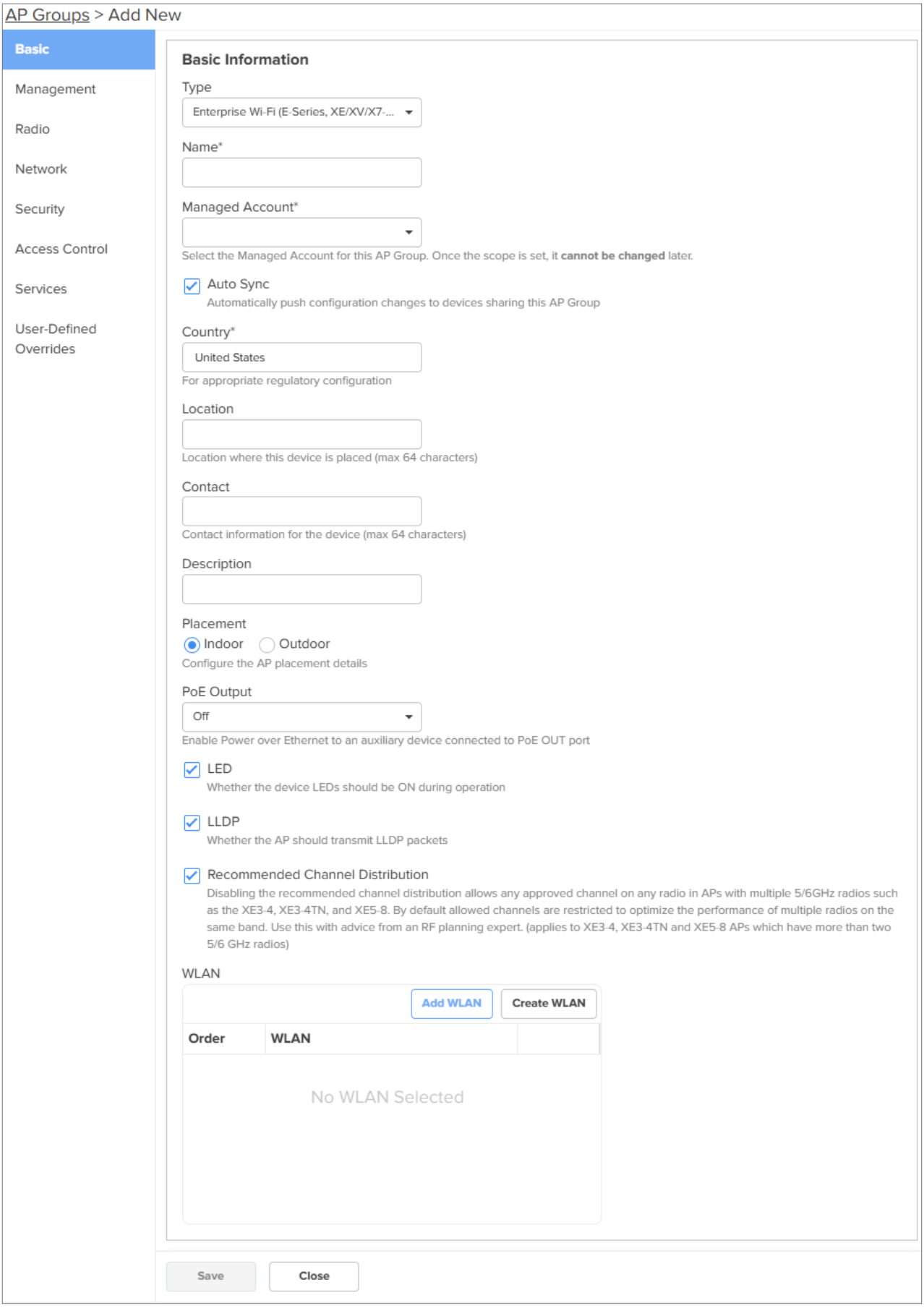
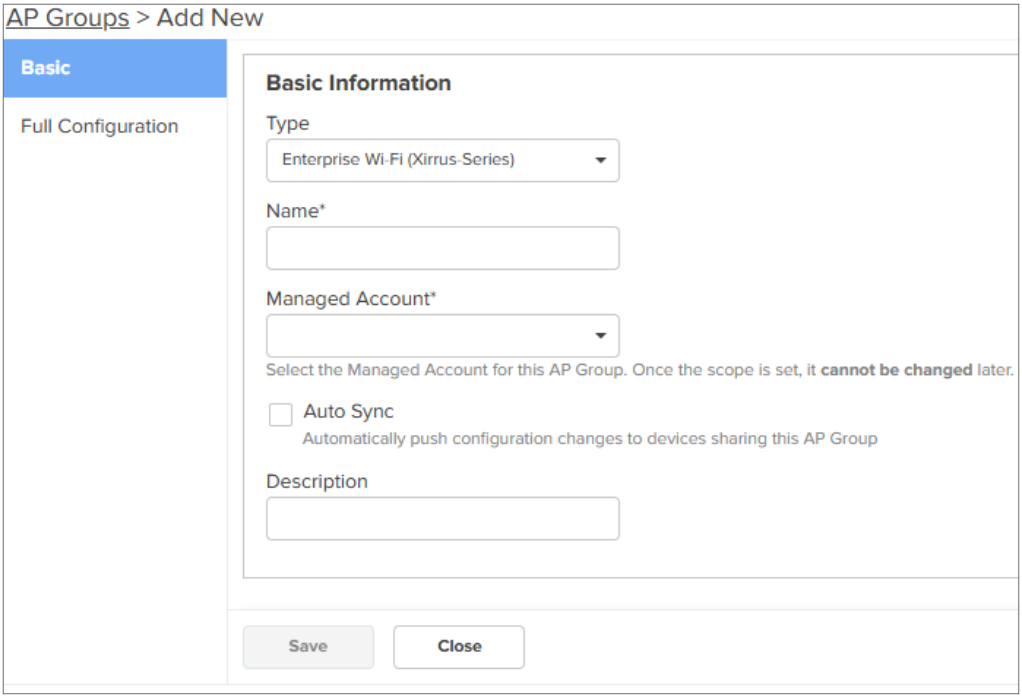
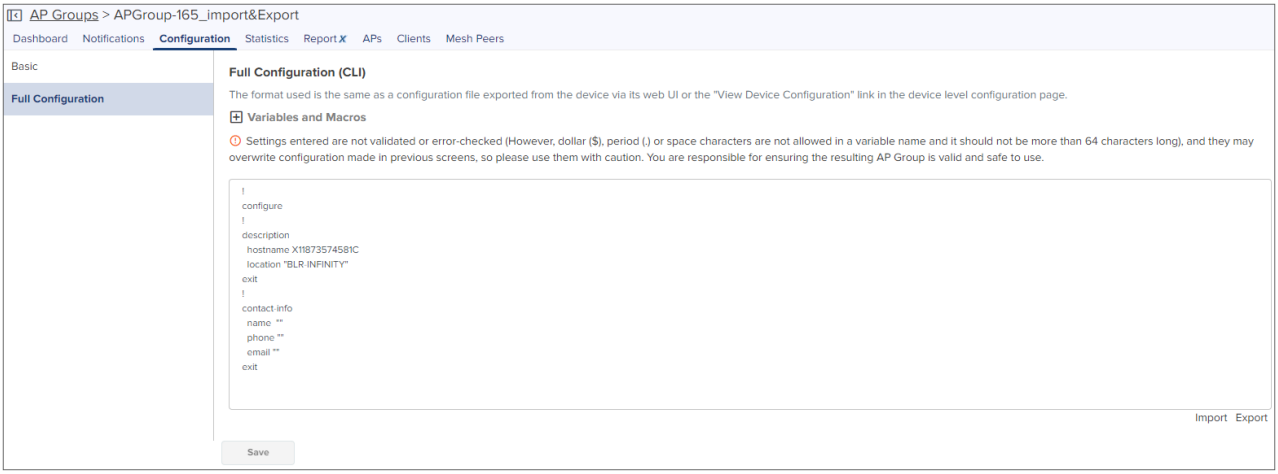

AP Groups > Add New
Basic
Management
Radio
Network
Security
Access Control
Services
User-Defined Overrides
Basic Information
Type
Enterprise Wi-Fi (E-Series, XE/XV/X7-...
Name*
Managed Account*
Select the Managed Account for this AP Group. Once the scope is set, it cannot be changed later.
Auto Sync
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 343 *Basic: Enterprise Wi-Fi (Xirrus-Series)*



The Xirrus AP Group embeds a Full Configuration of CLI commands.

Figure 344 *Full Configuration: Enterprise Wi-Fi (Xirrus-Series)*



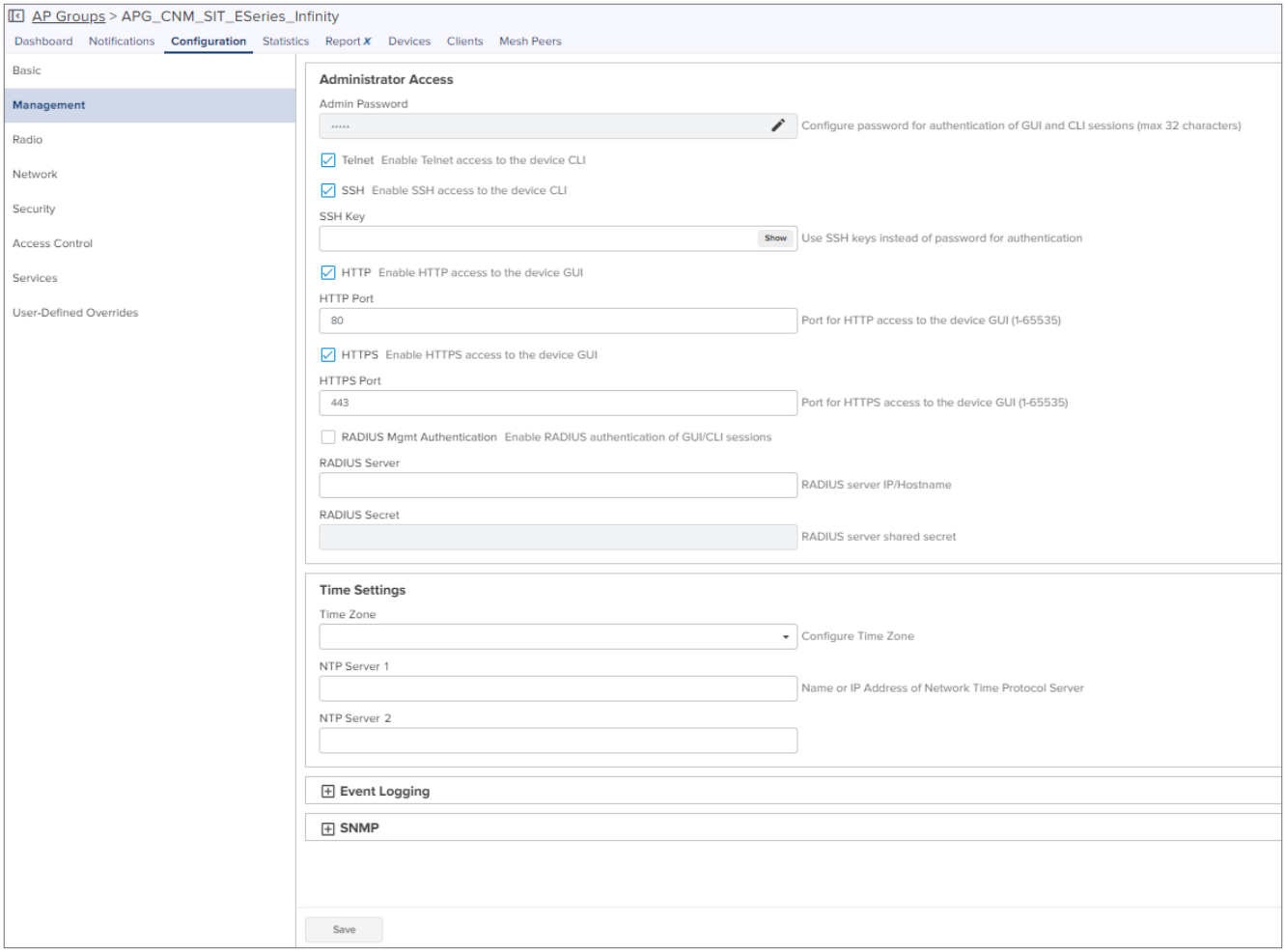
Management

The **Management** page allows to configure the **Administrator Access, Time Settings, Event Logging** and **SNMP.**

Note

Enterprise Wi-Fi AP uses the AES-128 algorithm for encryption and SNMPv3 password configuration parameter is used for encryption and authentication.

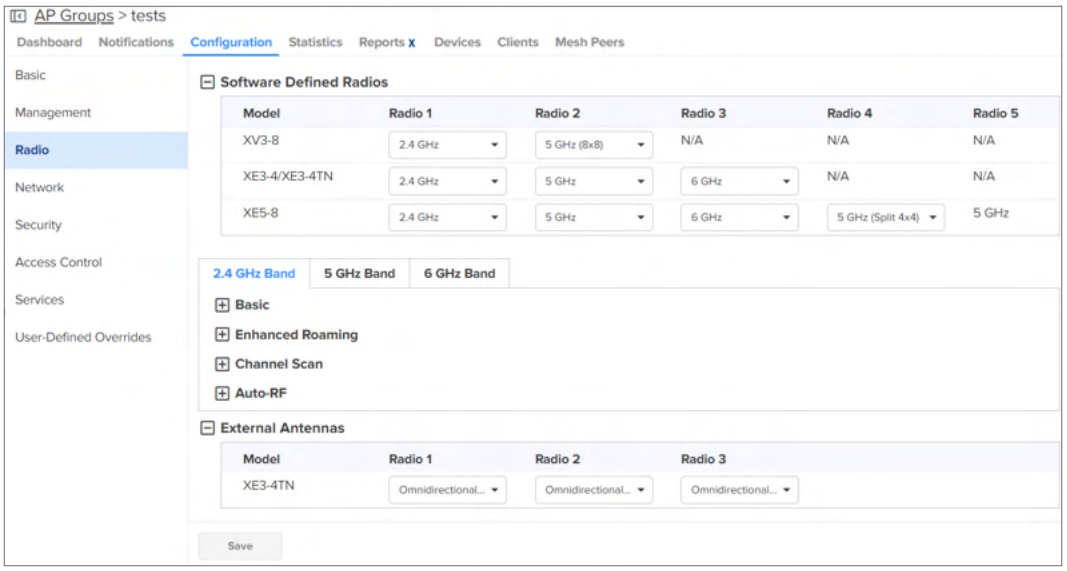
Figure 345 *Management: Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)*



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 346 *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 346. The other radio bands for which the devices can be configured are as shown in Table 74.

Table 74 *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 75 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		
X7-55X	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

Models	Radios	Supported Radio Bands	Channel Specification		
			Channel width	Default Channel width	Supported channel list
X7-56X	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
* 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 75 *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:

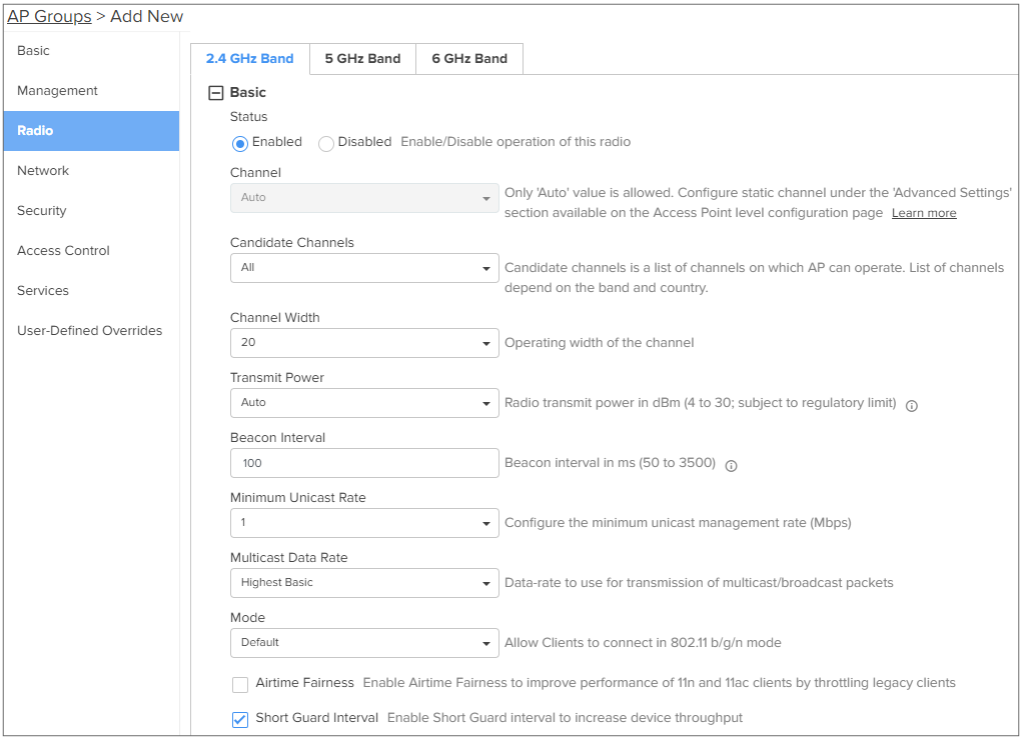
```
!
no channels-distribution
!
```

5. Click **Save**.

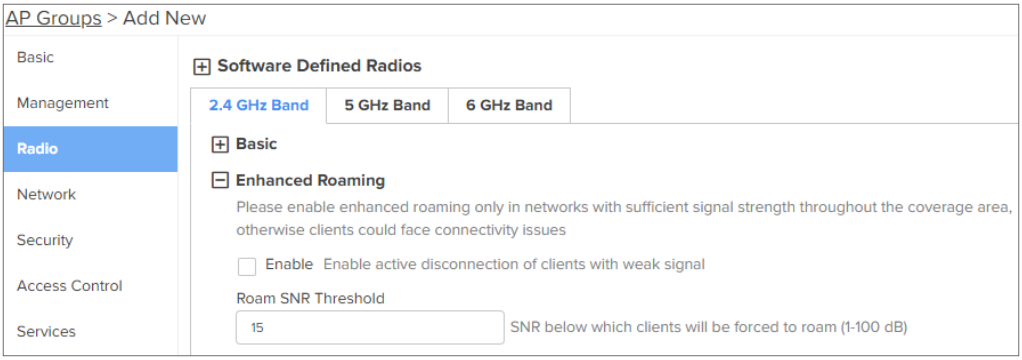
1. In the **Radio** tab, you can configure **Software Defined Radios** for the required **Model** as shown in Table 74.

   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 347 *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

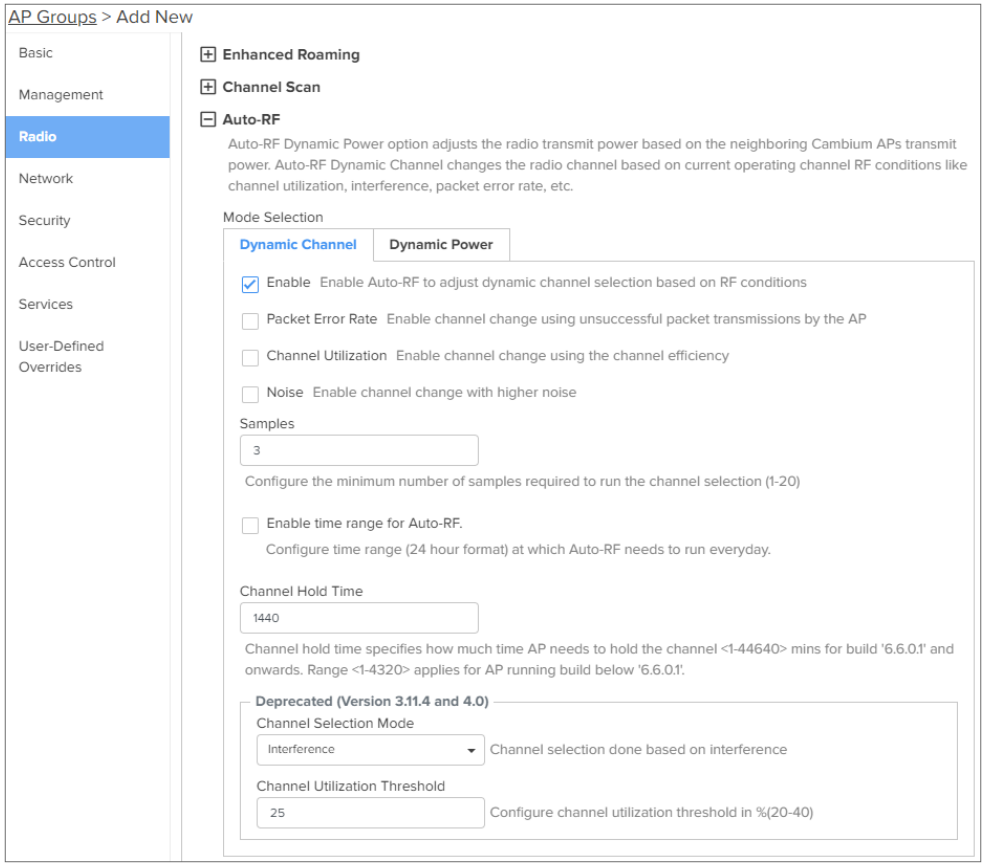
Enable **Enhanced Roaming** only in networks with sufficient signal strength throughout the coverage area, otherwise clients could face connectivity issues.

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

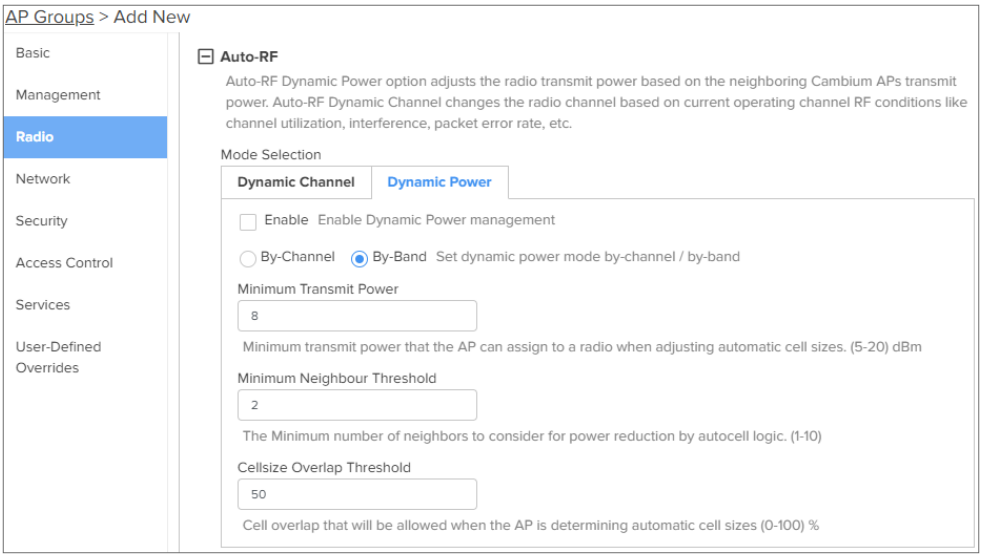
The **Channel Hold Time** parameter specifies the time (in minutes) for which the AP will hold the channel.

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 348. This customization helps in achieving optimal wireless network performance customized for specific deployment scenarios.

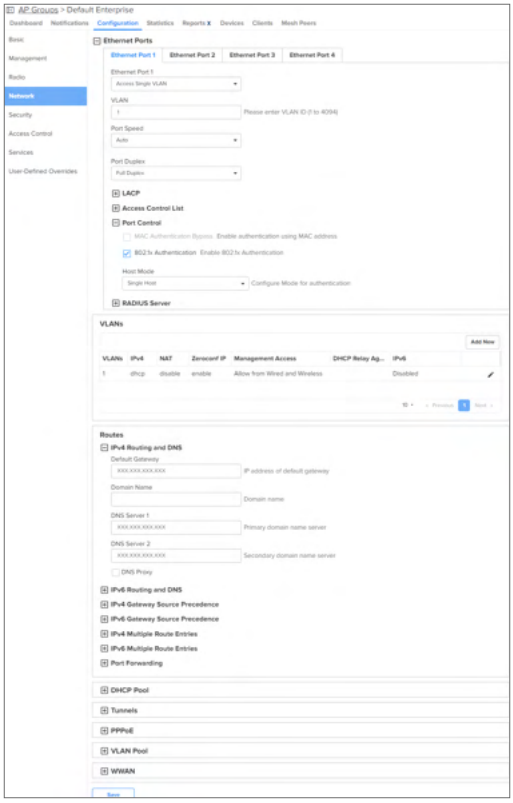
Figure 348 *External Antennas for XE3-4TN APs*



Network

The **Network** page allows to configure **Ethernet Ports**, **VLANs**, **Routes** for IPv4 and IPv6, **DHCP Pool, Tunnels, PPPoE , VLAN Pool,** and **WWAN**.

Figure 349 *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 350 *WLAN Concentrator > L2GRE parameters*

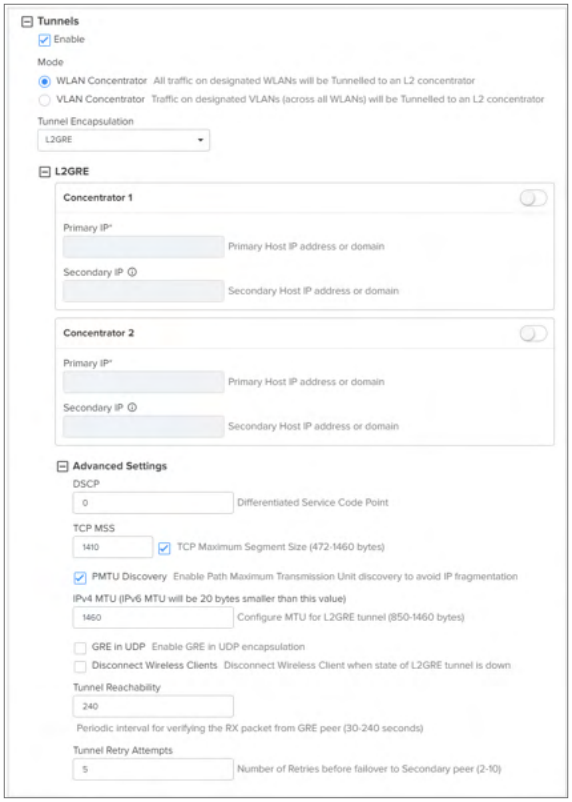


Figure 351 *WLAN Concentrator > L2TP parameters*

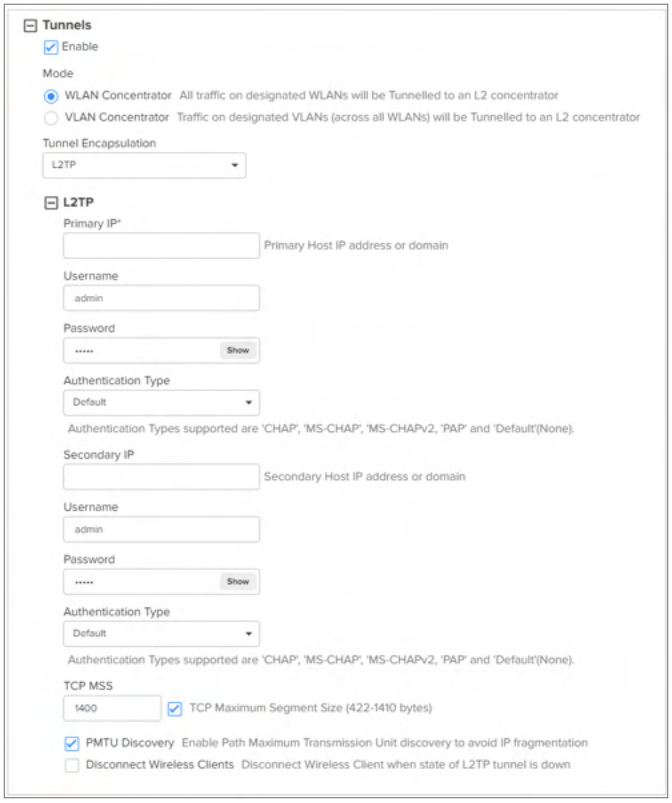


Figure 352 *VLAN Concentrator—Only L2GRE parameters*

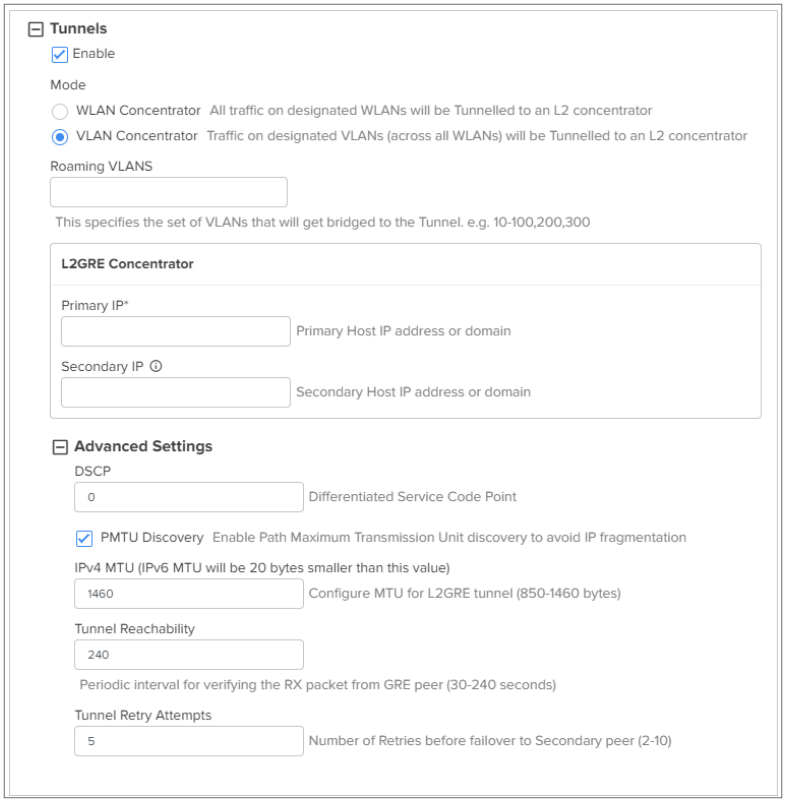


Table 76 *Tunnels parameters*

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 77 *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.



Note

- In the current release, IPv6 functionality is supported only for cnPilot Enterprise devices.
- IPv6 functionality is supported on cnPilot from System Release 4.0.

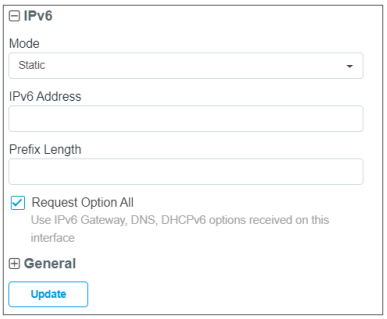
Configuring IPv6

To configure IPv6, perform the following:

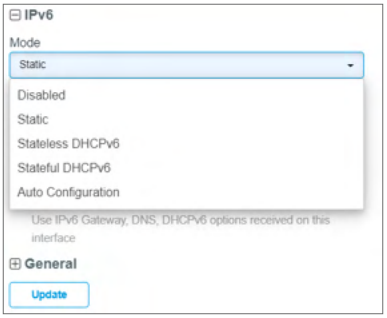
1. Navigate to **Configuration Wi-Fi Profiles** > **AP Groups** tab.
2. Select **Network** tab and click **Edit VLAN**.



3. Click the (+) plus sign next to **IPv6** option.



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**.

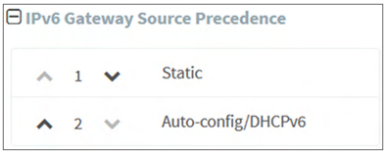


   If **Static** is selected, provide the following details:

   - **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**.

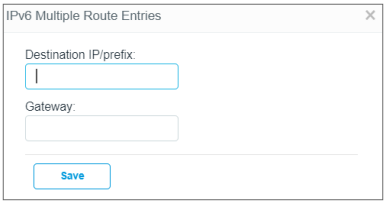


To create a new static Route,

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)

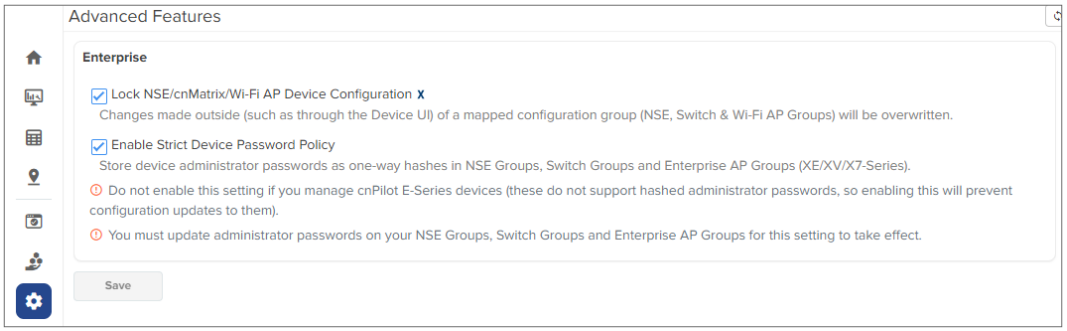
3. Recovery (maximum of one Mesh Recovery is selected)
4. WLANs with Mesh Mode Off (total WLAN limit including Mesh WLANs)

Note

Maximum of 16 WLAN policies are supported for E-Series and XV-Series devices. 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.

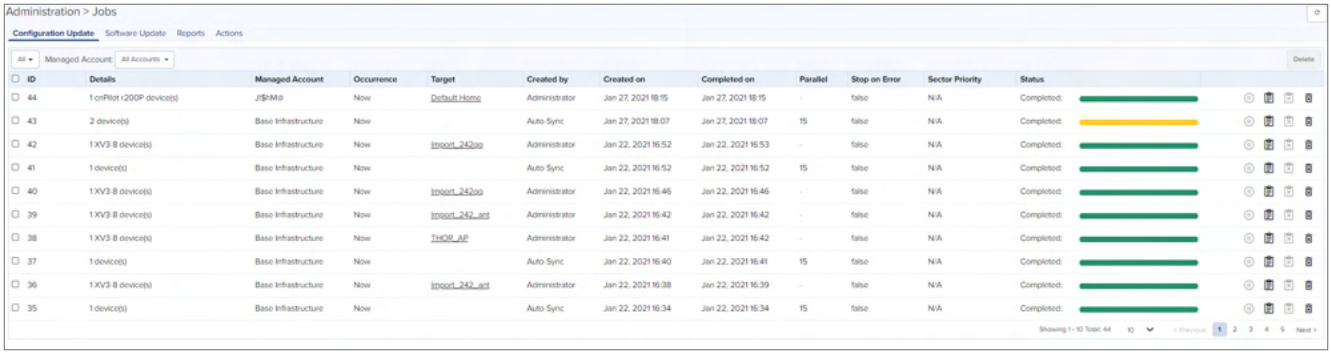


To enable this feature, perform the following steps:

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.

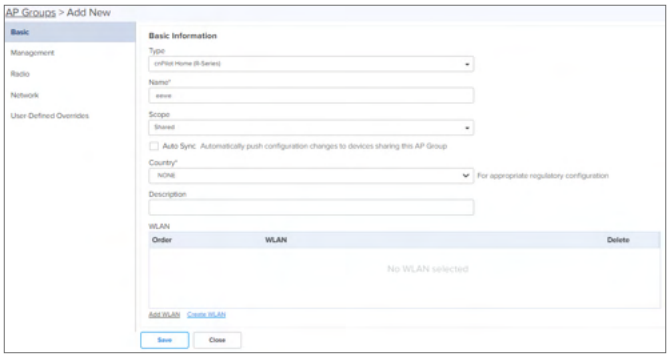


Retrying configuration

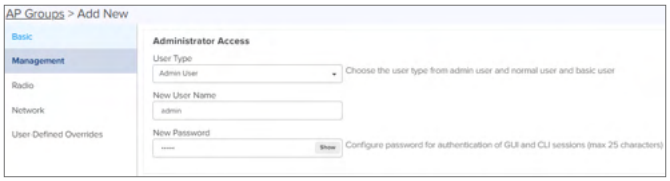
When the user applies an AP Group to the device, and the Job is skipped because the device is Offline, the reason for the skip will be displayed as **Device was offline** in the **Jobs** page. When device comes up and connects to cnMaestro, an **Auto-Sync** job pushes the AP Group to the device. (It 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

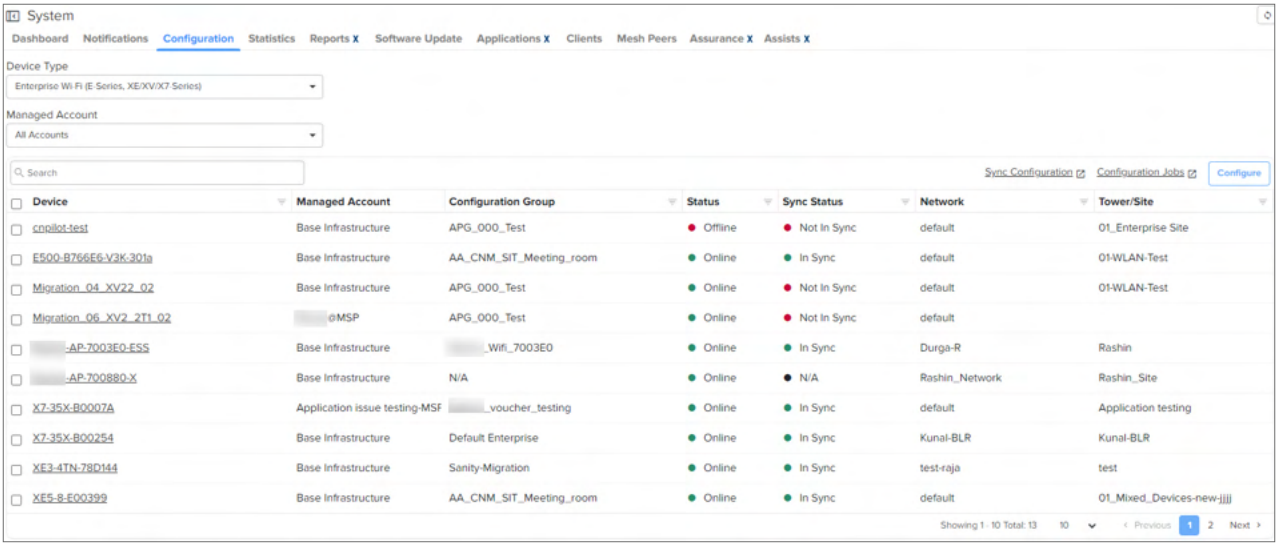
Default User Name: **admin** can be used after the upgrade.

Apply AP Group to Device

A Configuration Job can be created as follows:

1. Navigate to **Monitor and Manage > System > Configuration**.

   Figure 353 *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 354 *Configuration page: Enterprise Wi-Fi (E-Series, XE,/XV/X7-Series)*



   Figure 355 *Configuration page: cnPilot Home (R-Series)*

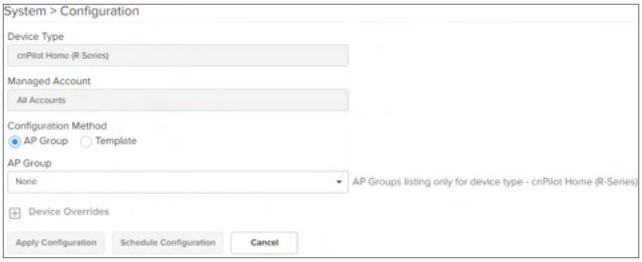
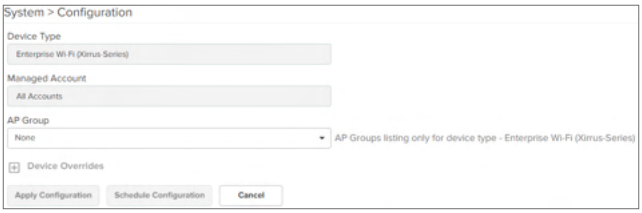


   Figure 356 *Configuration page: Enterprise Wi-Fi (Xirrus-Series)*



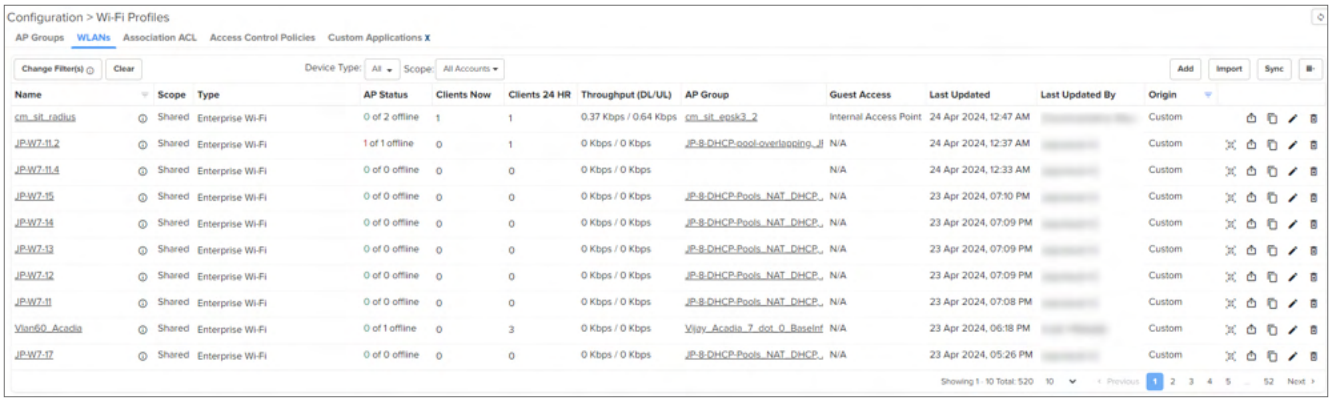
5. Select the AP group from the **AP Group** dropdown list.
6. Click **Apply Configuration.**

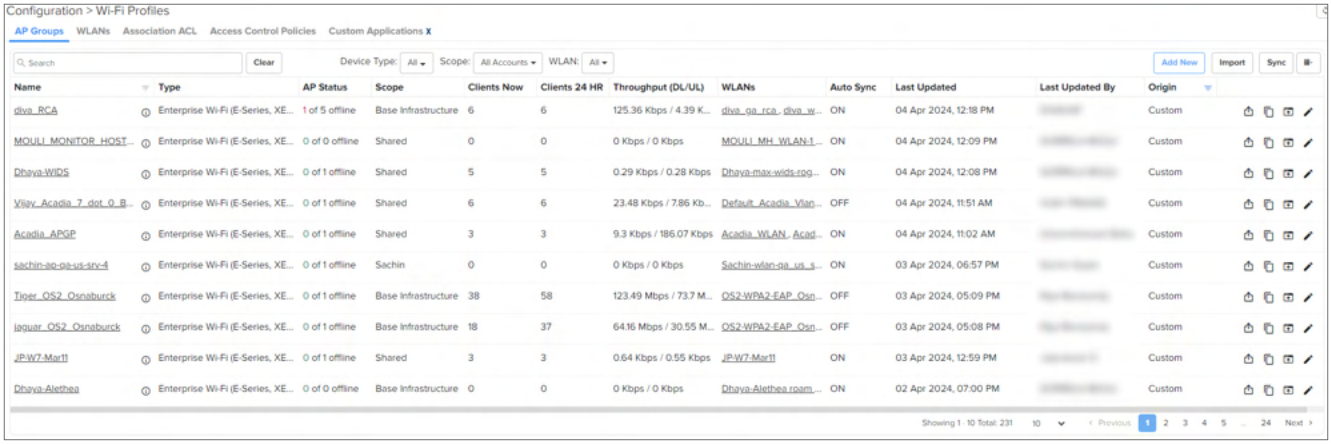
AP Group and WLAN Import/Export

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 the **WLAN** tab select **New**.

As with AP Groups, WLANs are separated into cnPilot Home and Enterprise Wi-Fi. You can configure WLAN, RADIUS, Guest Access, Usage Limits, Scheduled Access, and Access parameters with Enterprise Wi-Fi WLANs. With the cnPilot Home WLANs, you can configure SSID, Scheduled Access, and Access parameters.

Note

- Special characters can be used to create AP Group and WLAN names (Eg: a-zA-Z_-*&%#@!<>.() []^~`$1234567890). The user can also rename the AP group and WLAN names, if required.
- The MAC authentication fallback feature works only when Guest Access is configured with RADIUS authentication under **WLANs** > **Guest Access** > **Access Policy** > **RADIUS**.

To create a WLAN, perform the following steps:

1. Navigate to **Configuration > Wi-Fi Profiles**.
2. Select **WLANs** tab and then click **Add**.
3. Enter **Type, Name**, and WLAN parameters.
4. Ensure **WPA2 PSK** is enabled in **Security** dropdown.

Note

- WPA3 security standard is not supported on Enterprise Wi-Fi 5 APs (version 4.x.)

- To support ePSK with WPA3, you must select either the **WPA2/WPA3 Pre-shared Keys** or **WPA3 Pre-shared Keys** option in the **Security** dropdown list, and configure ePSK passphrase.
- ePSK support with WPA3 requires a cnMaestro X subscription.
- When the **Security** parameter is configured with the **WPA2 Pre-Shared Keys** option, 6 GHz clients connect to the AP using the secure Simultaneous Authentication of Equals (SAE) method.

For information on client (WPA2 and WPA3-compliant) registration with ePSK passphrase, see ePSK registration for WPA3 clients.



The following table lists the description of the basic and advanced parameters available in the WLAN tab:

Table 78 *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 (Access Profile Mode)

Parameters	Description	Range	Default
	• **Off**: Mesh support disabled on WLAN profile.		
VLAN	Segregates wireless station traffic from AP traffic in the network. Wireless stations obtain an IP address from the subnet configured in the VLAN field of the WLAN profile.	1-4094	1
Security	Determines key values that are encrypted based on the selected algorithm. Following security methods are supported: • **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.	-	Open

Parameters	Description	Range	Default
	 **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 ePSK registration for WPA3 clients. • **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.		

Parameters	Description	Range	Default
	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 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.		

Parameters	Description	Range	Default
	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
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 79 *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	–	Disabled

Parameters	Description	Range	Default
	This feature is disabled for this WLAN. • Radius Based The user is expected to configure WPA2 Enterprise for this mode to support. During the association phase, AP obtains pool name from RADIUS transaction and based on the present distribution of wireless station across VLANs, AP selects appropriate VLAN and wireless station requests an IP address from the VLAN selected by Enterprise Wi-Fi AP device. • Static For this mode to support, the user requires to configure VLAN Pool details available under **Configure** > **Network** > **VLAN pool**. During the association phase, AP obtains pool, and based on the present distribution of wireless station across VLANs, AP selects appropriate VLAN and wireless station requests an IPv4/IPv6 address from the VLAN selected by the Enterprise Wi-Fi AP device.		
Max Clients	This specifies the maximum number of wireless stations that can be associated with a WLAN profile. This varies based on the Enterprise Wi-Fi AP device model number. Refer to for more details.	1-512 (Refer)	256
UAPSD	When enabled, Enterprise Wi-Fi AP devices support WMM Power Save / UAPSD. This is required where applications such as VOIP Calls, Live Video streaming are in use. This feature helps to prioritize traffic. Below is the default traffic priority followed by the Enterprise Wi-Fi AP device.  	–	Disabled
QBSS	When enabled, appends QBSS IE in Management frames. This IE provides information on channel usage by AP, so that smart wireless stations can decide better AP for connectivity. Station count, Channel utilization, and Available admission capacity are the information available in this IE.	–	Disabled
DTIM interval	This parameter plays a key role when power save supported mobile stations are part of the infrastructure. This field when enabled controls the transmission of Broadcast and Multicast frames.	1-255	1
Monitored Host			
Host	This feature is required where there is an interrupted backbone network. Enterprise Wi-Fi AP device monitors the reachability of hostname/IP configured in this parameter and modifies the state of WLAN.	-	Disabled

Parameters	Description	Range	Default
Interval	The frequency of monitoring the network health based on the status of the keep-alive mechanism w.r.t configured monitored host.	60-3600 sec	300
Attempts	The number of packets in the keep-alive mechanism to determine the status.	1-20	1
DNS Logging Host	By enabling this feature, the Administrator can monitor the websites accessed by wireless stations connected to WLAN profile.	–	Disabled
Connection Logging Host	When enabled provides information of all IP connections accessed by a wireless station that is associated with WLAN and logs the connection data seamlessly onto an external syslog server.	–	Disabled
Band Steering	This feature when enabled steers wireless stations to connect to 5GHz. There are three modes supported by Enterprise Wi-Fi devices. The mode can be selected based on either deployment or wireless station type. Below is the order of modes, which forces the wireless station to connect to the 5 GHz band. • 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	–	Disabled

Parameters	Description	Range	Default
	• 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		
Tunnel Mode	This option is enabled when user traffic is tunneled to the DMZ network either using L2TP or L2GRE.	–	Disabled
Fast-Roaming Protocol	One of the important aspects to support voice applications on a Wi-Fi network (apart from QoS) is how quickly a client can move its connection from one AP to another. This should be less than 150 ms to avoid any call drop. This is easily achievable when the WPA2-PSK security mechanism is in use. However, in enterprise environments, there is a need for more robust security (the one provided by WPA2-Enterprise). With WPA2-Enterprise, the client exchanges multiple frames with the AAA server, and hence depending on the location of the AAA server the roaming time will be above 700 ms. 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**	–	Disabled

Parameters	Description	Range	Default
	• Support for WPA2 authentication method		
802.11v	Provision to enable 802.11v BSS Transition Management.	–	Disabled
PMF (802.11w)	802.11w also termed as Protected Management Frames (PMF) Service, defines encryption for management frames. Unencrypted management frames make wireless connection vulnerable to DoS attacks as well as they cannot protect important information exchanged using management frames from eavesdroppers.	–	Optional
SA Query Retry Time	The legitimate 802.11w client must respond with a Security Association (SA) Query Response frame within a pre-defined amount of time (milliseconds) called the SA Query Retry time.	100-500	100ms
Association Comeback Time	This value is included in the Association Response as an Association Comeback Time information element. AP will deny association for the configured interval.	1-20	1 Sec

5. Click **Save**.

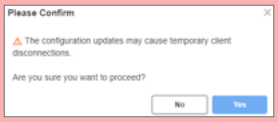
Note

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 357 *Warning when modifying WLAN*



ePSK registration for WPA3 clients

Note

ePSK support for WPA3 clients requires a cnMaestro X subscription.

For the ePSK feature, when you configure WPA3-WPA2 (mixed mode)-PSK or WPA3-PSK as the WLAN security, the clients connection in the WPA3 mode must go through an additional registration phase. This is different from the flow when you configure WPA2-PSK as the WLAN security, where users can authenticate by using only a passphrase.

When clients use WPA3-PSK security, Simultaneous Authentication of Equals (SAE) is the authentication mechanism. Here an extra authentication is added, which is more secure than WPA2. For WPA2-PSK clients, the passphrase is matched against a database to identify the user. However, this is not possible for WPA3-PSK clients because of the extra authentication in WPA3-SAE. When WPA2-PSK security is used, the Pairwise Master Key (PMK) is the same for every connection made by the client. This is due to the underlying weaknesses in WPA2-PSK, which make it easier to validate the passphrase. In contrast, when WPA3-PSK security is used, a new PMK is generated each time a client joins the network. Therefore, registration will help us to know the passphrase upfront

when a client tries to connect. This mandates the users to register themselves with the ePSK passphrase to bind the client MAC with the passphrase to successfully connect to the Wi-Fi network.

For WPA3 clients to connect to the network using ePSK flow:

1. First connect to the WLAN with the WLAN passphrase.

   A simple password is recommended to be configured, for example, `signmeup`, or any other appropriate passphrase.

2. Register themselves with the WPA3-ePSK unique passphrase.

   After the MAC binding is complete, users can use the WPA3-ePSK unique passphrase for subsequent WLAN connections.

This section describes the following topics:

- ePSK with WPA3 feature recommendations
- Scenarios while registering clients
- Configuring ePSK registration for WPA3 clients
- Registration flow screenshots
- Recommended best practices

ePSK with WPA3 feature recommendations

The following are the recommendations for this feature:

- This feature is supported only on cnMaestro Cloud 5.1.0 onwards.
- Supported AP firmware version is 6.6.1 or 7.0 and above.
- Security mode must be configured to either **WPA2/WPA3 Pre-shared Keys** or **WPA3 Pre-shared Keys**.
- APs must be managed from cnMaestro Cloud for client registration.
- The WLAN VLAN must be able to provide DHCP to clients and must have internet connectivity.
- This feature is not supported on Enterprise Wi-Fi 5 APs and Xirrus APs.

Scenarios while registering clients

When a client connects to the WLAN, the following scenarios are possible:

- When a client connects for the first time using WPA2 security and ePSK passphrase (either on 2.4 GHz or 5 GHz radios), the AP performs an ePSK lookup. The following are the outcome:
  - If a match is found, the MAC binding is created with the respective ePSK key.

    AP shares this MAC binding information with the other APs in the network.
  - If a match is not found, the connection fails.
- If the WPA2 client is connected using the WLAN passphrase, client registration steps are performed to bind the passphrase to the client.
- When a client connects for the first time using WPA3 security, the following two possibilities may occur:
  1. If MAC binding is not available for the client on the AP, the following procedure must be completed for successful registration of clients:

a. User must authenticate using the configured WLAN passphrase, for example, `signmeup`.

   If the user tries to sign in with some other password other than the configured WLAN password (`signmeup`), the connection fails.

b. If the connection with the configured password (`signmeup`) is successful, the AP redirects the client to the registration page.

   This is the only traffic allowed for the client with this WLAN passphrase.

c. User must now enter the configured ePSK passphrase and register.

   The AP redirects the client to the registration page with instructions.

d. Users must select the checkbox after reading the instructions (provided for different clients, such as Android, Windows, and iOS), and then disconnect from the network.

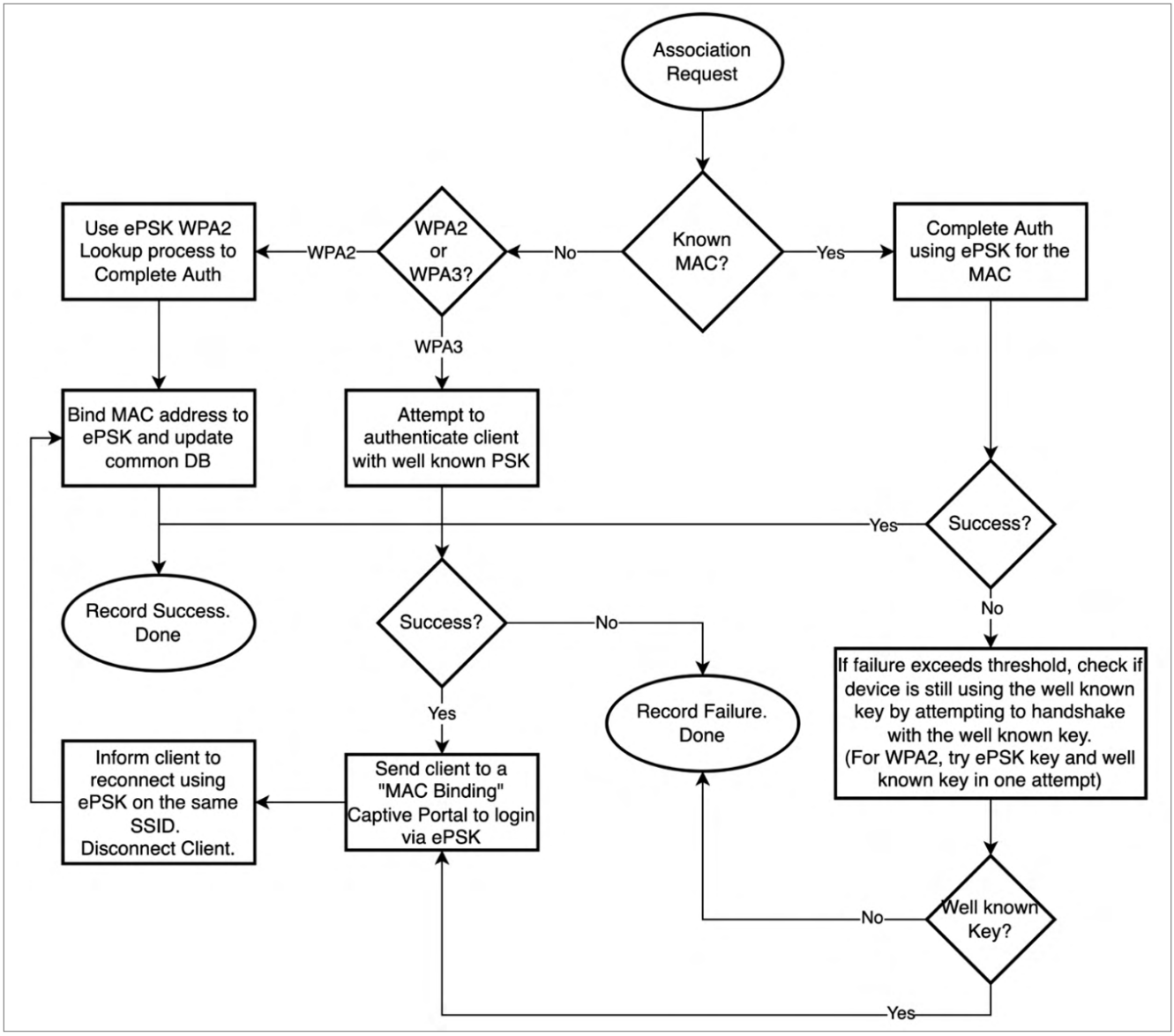
e. User must forget the WLAN/SSID and reconfigure using the ePSK passphrase.

   User then reconnects with ePSK passphrase and gets authenticated.

For a more detailed information, see Registration flow screenshots.

2. When MAC binding is available for the client on the AP, users can authenticate the client with the passphrase present in the MAC binding, that is the ePSK passphrase.

Figure 358 *Client registration flow for WPA3 clients*



Configuring ePSK registration for WPA3 clients

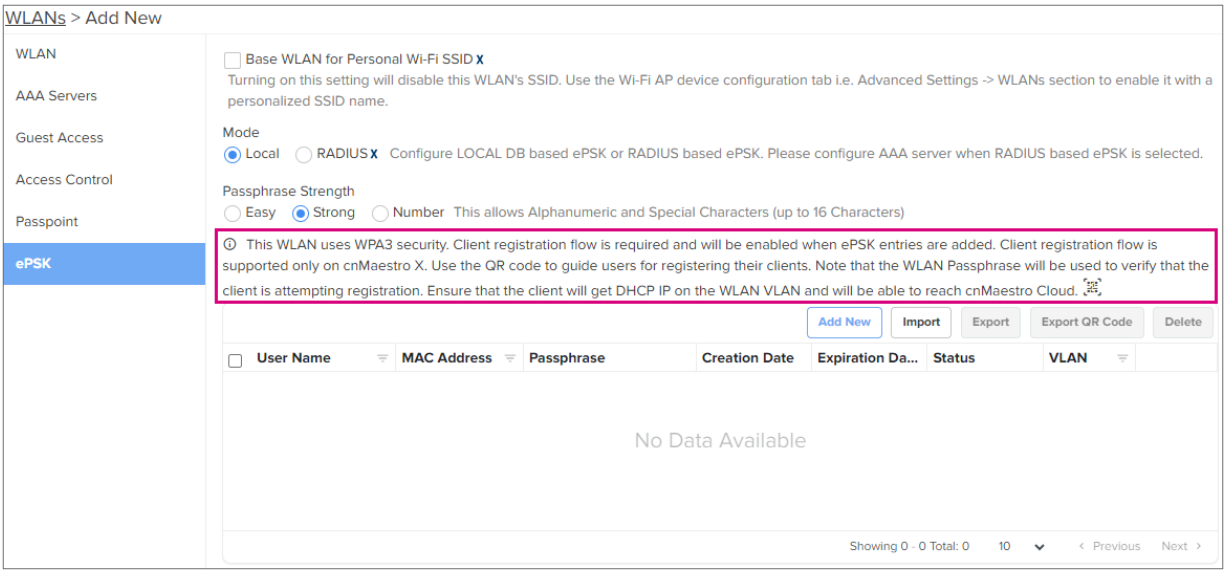
To enable WPA3-ePSK registration, you must create a WLAN profile and add ePSK entries in the ePSK grid.

To create WLAN profile and add ePSK entries, complete the following steps:

1. Navigate to **Configuration** > **Wi-Fi Profiles** page.
2. Select **WLANs** tab and click **Add**.
3. Select **Enterprise Wi-Fi** from the **Type** dropdown list and configure the WLAN parameters.
4. In the **Basic Settings** section, ensure either the **WPA2/WPA3 Pre-shared Keys** or **WPA3 Pre-shared Keys** option is selected in the **Security** dropdown list.
5. Enter the WLAN passphrase.
6. Click **Save**.

- When ePSK passphrase is not configured in the **WLANs** > **ePSK** page, the following message is displayed explaining the registration flow.

Figure 359 *Message on the ePSK page when no ePSK entries are added*



- For existing WLANs where ePSK entries are present and when **WPA2/WPA3 Pre-shared Keys** or **WPA3 Pre-shared Keys** option is selected in the **Security** dropdown list, the following messages appear respectively

Figure 360 *When **WPA3 Pre-shared Keys** option is selected*

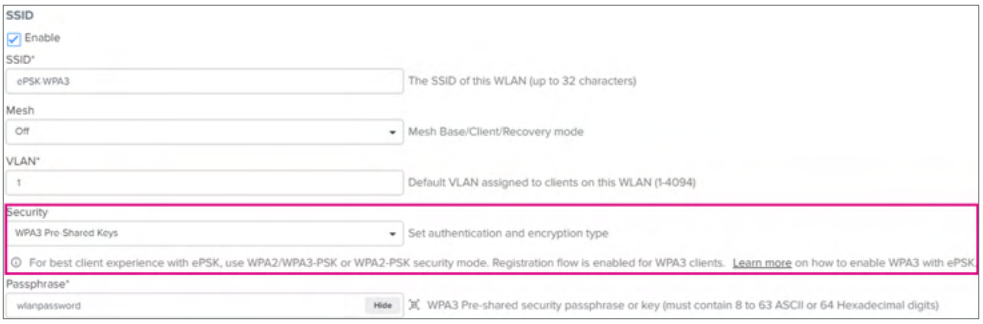
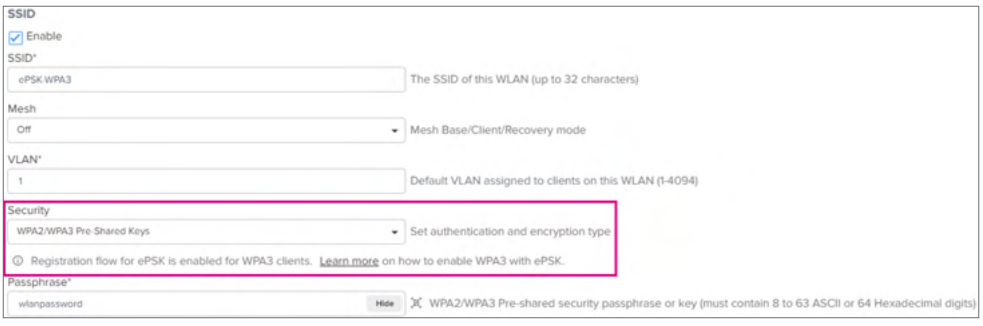


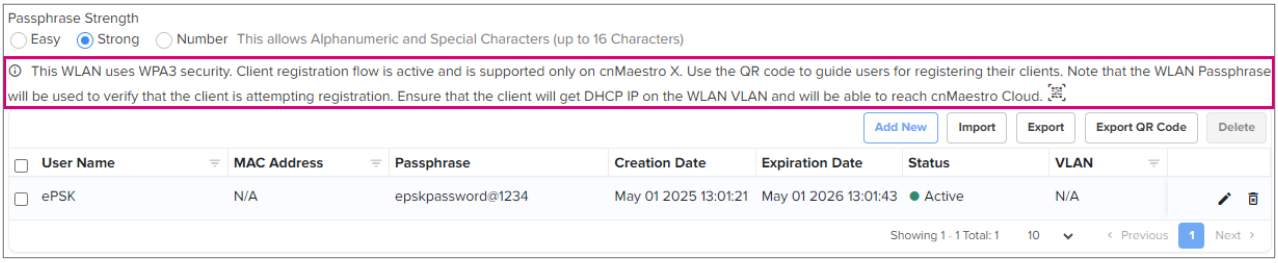
Figure 361 *When **WPA2/WPA3 Pre-shared Keys** option is selected*



7. Click the **ePSK** tab and add the passphrase.

   After the ePSK passphrase is added, the following message is displayed explaining the registration flow.

Figure 362 *Message on the ePSK page when ePSK entries are added*



8. To download the QR code for the WLAN and the ePSK passphrase, click **Export QR Code**.

   The QR code is downloaded in a PDF file as shown below.

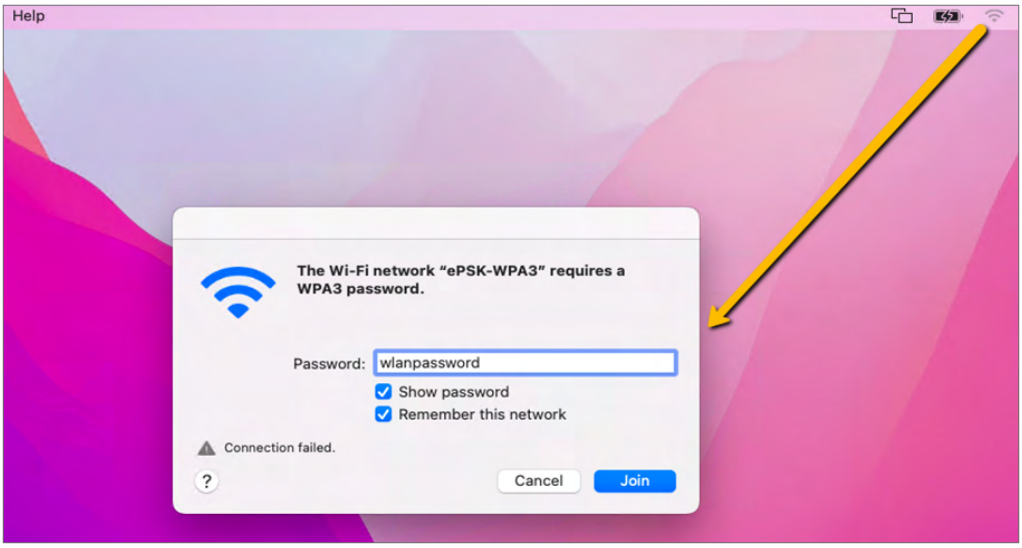


Registration flow screenshots

To register the clients to the network using the ePSK passphrase, users must complete the following steps:

1. Connect the client to the network using the WLAN passphrase.

   Figure 363 *Using WLAN passphrase for connecting to network*

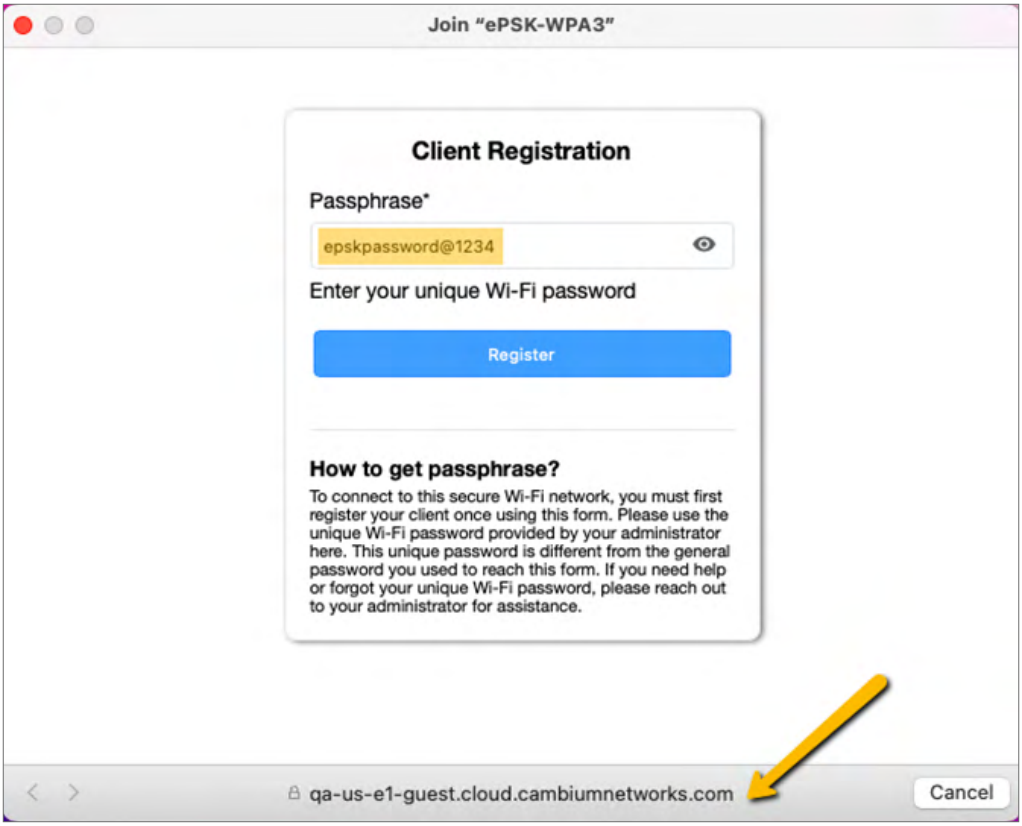


2. Click **Join**.

Clients are redirected to the **Client Registration** page for providing the ePSK passphrase.

3. Enter the ePSK passphrase in the **Passphrase** field and click **Register**.

Figure 364 *Using ePSK passphrase for connecting*



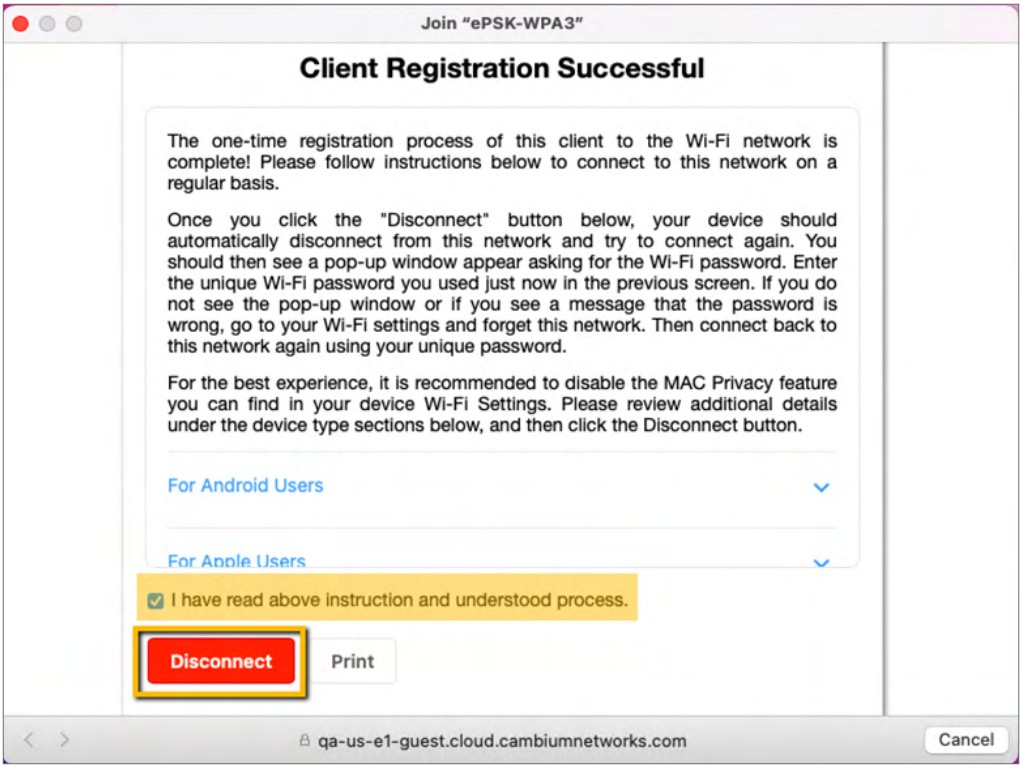
The registration success page is displayed along with a set of instructions.

4. Read the instructions (provided for different devices, such as Android, Windows, and iOS) and select the checkbox for confirmation.

   The instructions provide details of the next steps for different devices.

   The **Disconnect** button is enabled.

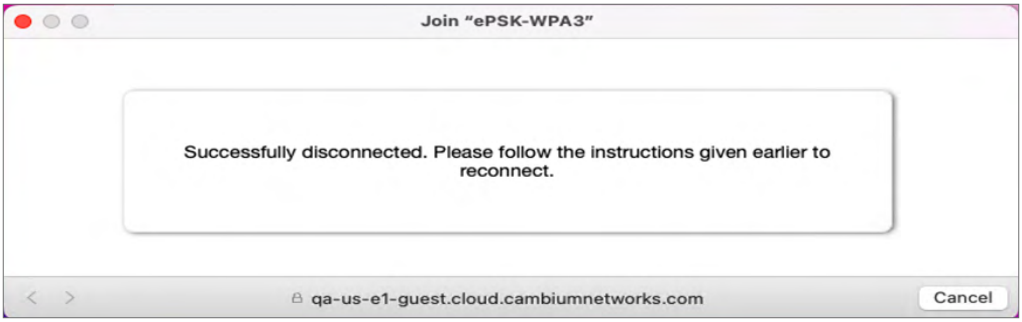
Figure 365 *Registration success page with instructions*



5. Click **Disconnect**.

   The client is disconnected and a disconnect success message is displayed.

Figure 366 *Disconnect success page*



6. Reconnect to the network using the ePSK passphrase that you provided in the **Client Registration** page earlier.

   The client connects to the network with the mapped VLAN.

Figure 367 *Using ePSK passphrase for connecting to network*



Recommended best practices

Following are some of the best practices you can follow while configuring ePSK registration for WPA3 clients:

- WPA3 PSK is not recommended for unmanaged (BYOD) clients (For example, multi-dwelling unit (MDU), hospitality, and educational institutions).

  In MDUs, with IoT clients, making WPA3 mandatory with a single SSID may not be a successful deployment.
- WPA2/WPA3 PSK is recommended for unmanaged clients and to transition from the current (WPA2-PSK).
- Most of the WPA3-capable clients favor WPA3 PSK when available. This behavior is different among other clients, where some fallback to WPA2 and some which do not.
- When the SSID is mapped to 2.4 GHz and 5 GHz radios, WPA2 PSK or WPA2/WPA3 PSK security is recommended.
- When the SSID is mapped to 2.4 GHz, 5 GHz, and 6 GHz radios, or only the 6 GHz radio, then WPA3 PSK security is recommended.

Creating an ePSK WLAN

To create an ePSK WLAN, perform the following steps:

1. Navigate to **Configuration** > **Wi-Fi Profiles** or WLAN page in the Wireless LAN View.
2. Select **WLANs** tab and click **Add**.

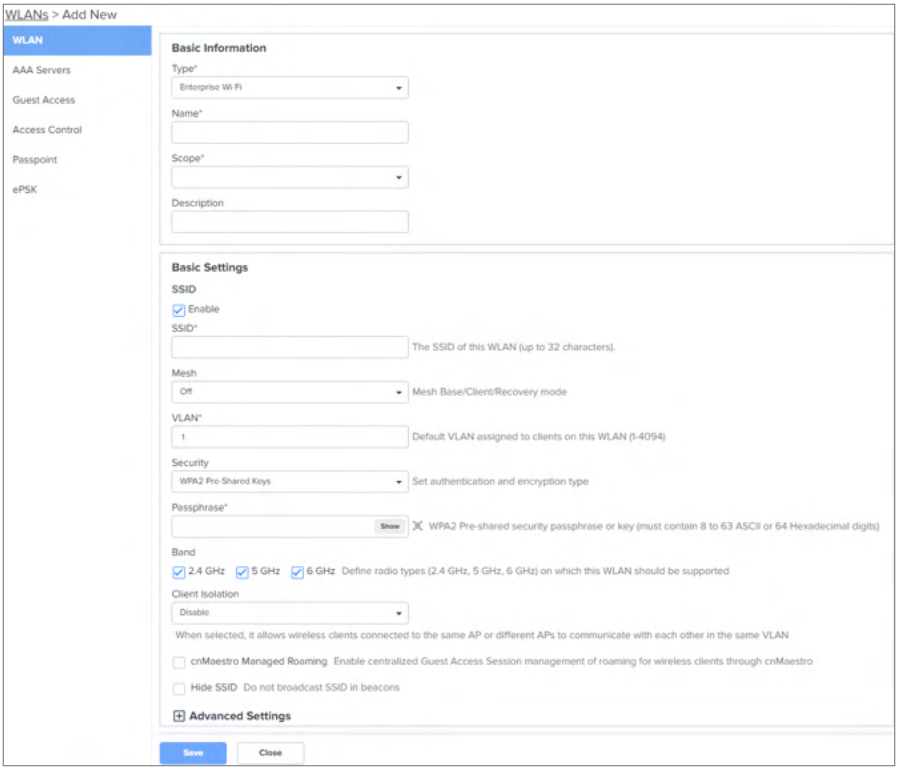
As with AP Groups, WLANs are separated into cnPilot Home (R-Series), Enterprise Wi-Fi, and RV22 Home Mesh types. You can configure WLAN, RADIUS, Guest Access, Usage Limits, Scheduled Access, and Access parameters with Enterprise Wi-Fi WLANs. With the cnPilot Home WLANs, you can configure SSID, Scheduled Access, and Access parameters.

Note

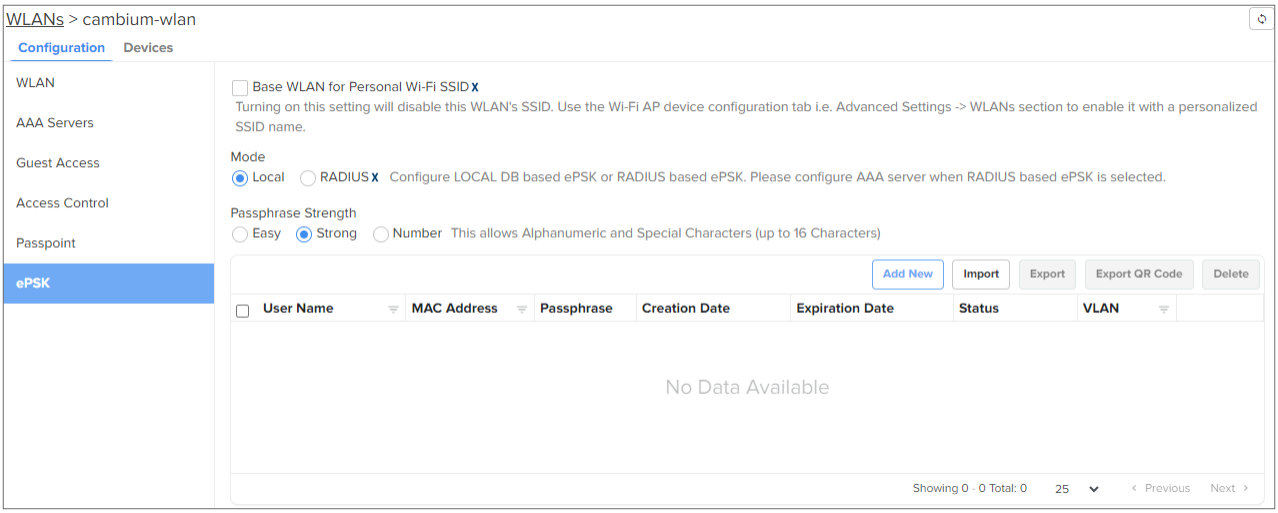
- The special characters can be used to create AP Group and WLAN names (Eg: a-zA-Z_-*&%#@!<>.() []^~`$1234567890). The user can also rename them if required.
- By default, password will not be configured. User has to configure the password for WLAN.

To create WLAN policy, perform the following steps:

1. Navigate to **Configuration** > **Wi-Fi Profiles**.
2. Select **WLAN** tab and click **Add**.
3. Select **Enterprise Wi-Fi** from the **Type** dropdown list and enter details in the **Basic Information** section.
4. In the **Basic Settings** section, ensure the **WPA2 Pre-Shared Keys** option is selected in the **Security** dropdown list.



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**).

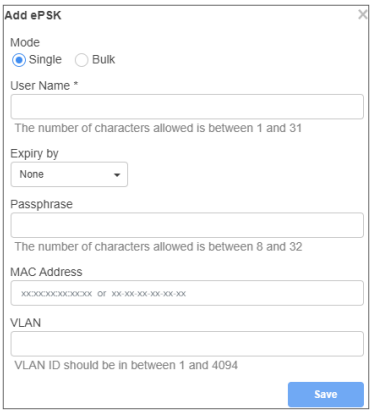


7. Click **Add New**.

   The **Add ePSK** window is displayed.

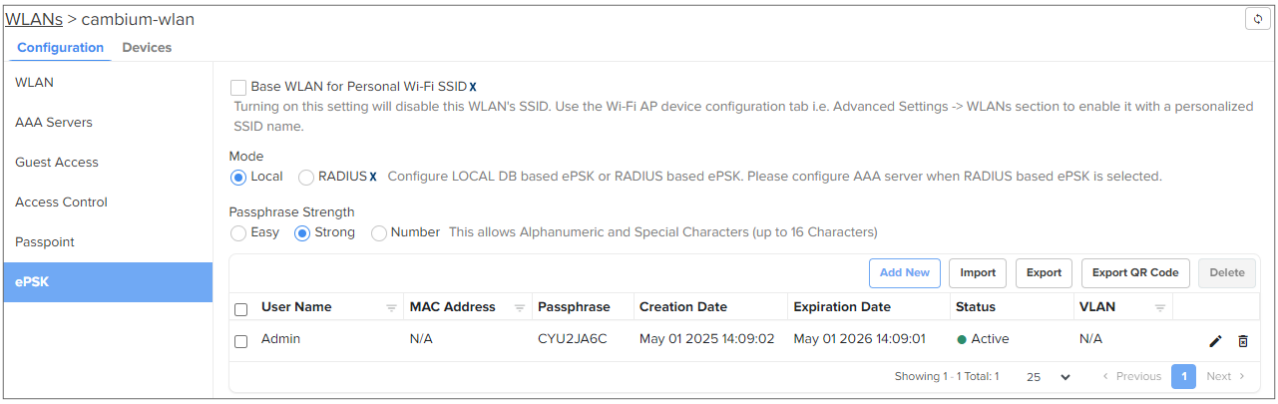
8. Select the **Mode** parameter as one of the following:

   - **Single**: In the single mode, only one entry is created. Only the **User Name** parameter is mandatory and the others are optional.



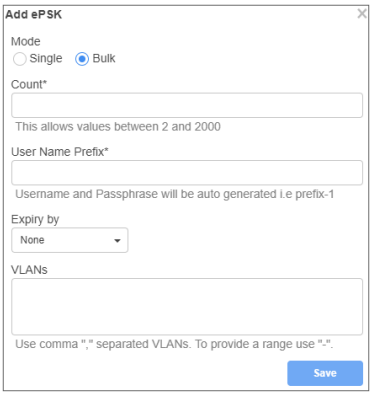
Note

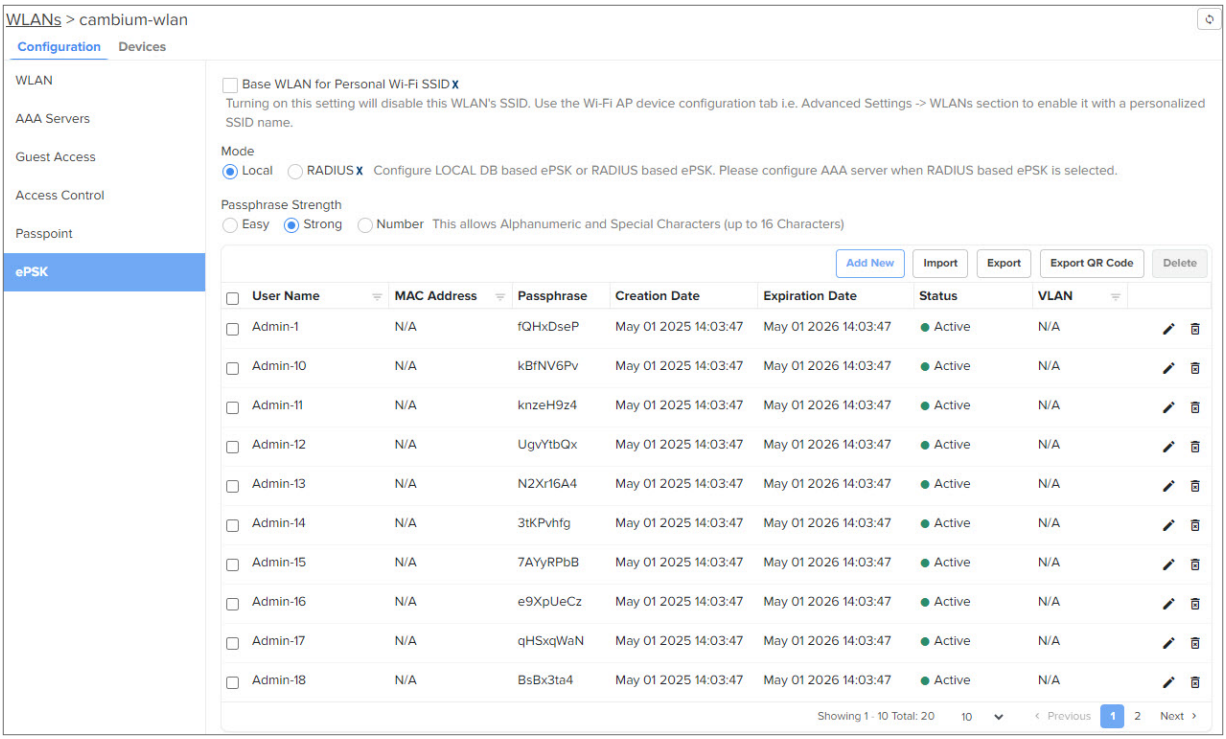
Passphrase is optional and unless manually configured, it will be automatically generated based on the selected **Passphrase Strength**.



   - 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 368 *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.

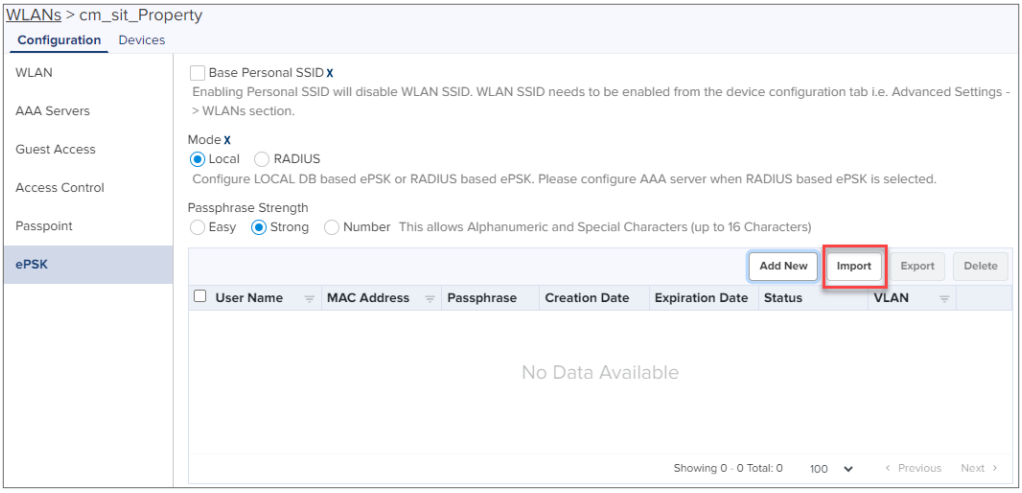
To configure personal Wi-Fi on the AP, complete the following steps:

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.

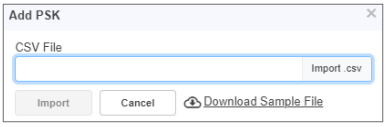
By default, this feature is disabled. Once enabled, the **Enable** checkbox (under **WLANs > WLAN > Basic Settings > SSID**) is cleared. Also, the local and RADIUS ePSKs are disabled.

Import ePSK

1. Click **Import**.

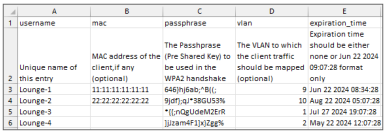


2. Select **Import.csv** file.



Alternatively, one can import a CSV file containing a list of ePSK entries. A sample file format is available from the Import dialog.

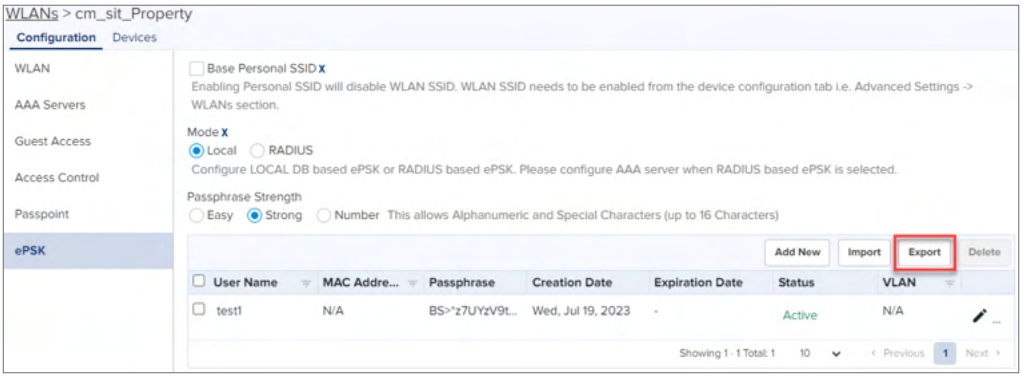
3. Click **Download Sample File**, to view sample ePSK Excel sheet.

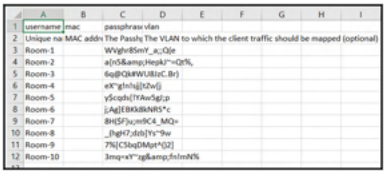


	A	B	C	D	E
1	username	mac	passphrase	vlan	expiration_time
2	Unique name of this entry	MAC address of the client,if any (optional)	The Passphrase (Pre Shared Key) to be used in the WPA2 handshake	The VLAN to which the client traffic should be mapped (optional)	Expiration time should be either none or Jun 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*38GUS3%	10	Aug 22 2024 05:07:28
5	Lounge-3		*(;nQgUdeM2Er9	1	Jul 27 2024 19:07:28
6	Lounge-4		)jjzam4F1)xjZg&%	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
- American Bandwidth
- Google Orion
- Helium
- WayFi
- WBA OpenRoaming Demo
- XNET

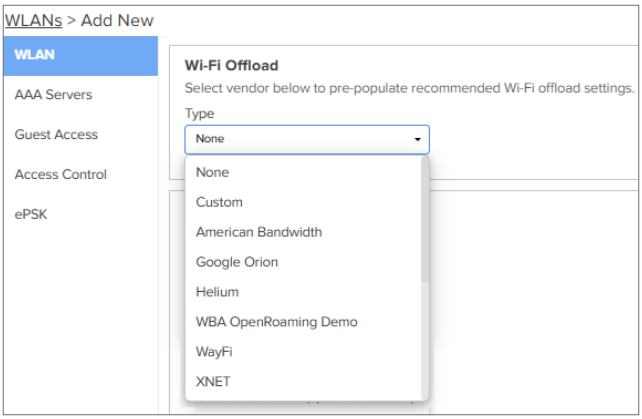
In addition to the above vendors, Cambium also supports custom Wi-Fi offloading configuration.

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 369 *WLANS > Wi-Fi Offloading*

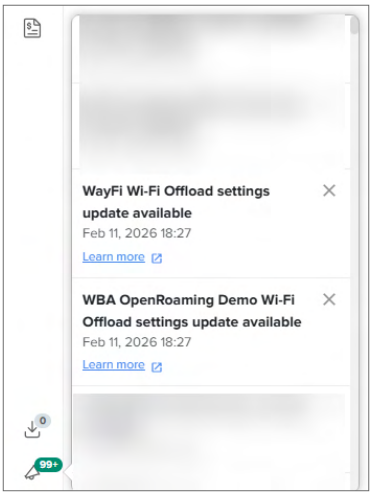


5. When a vendor updates the configuration, then cnMaestro displays notifications in the following locations:

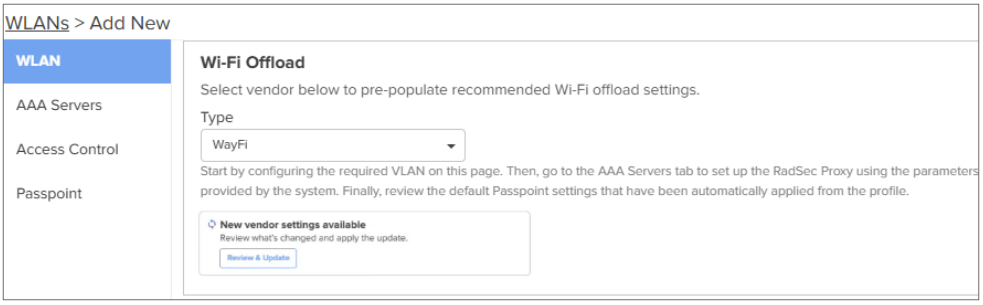
   Note

   Notifications will only appear if that particular vendor configurations is configured for that account.

   - Notifications window

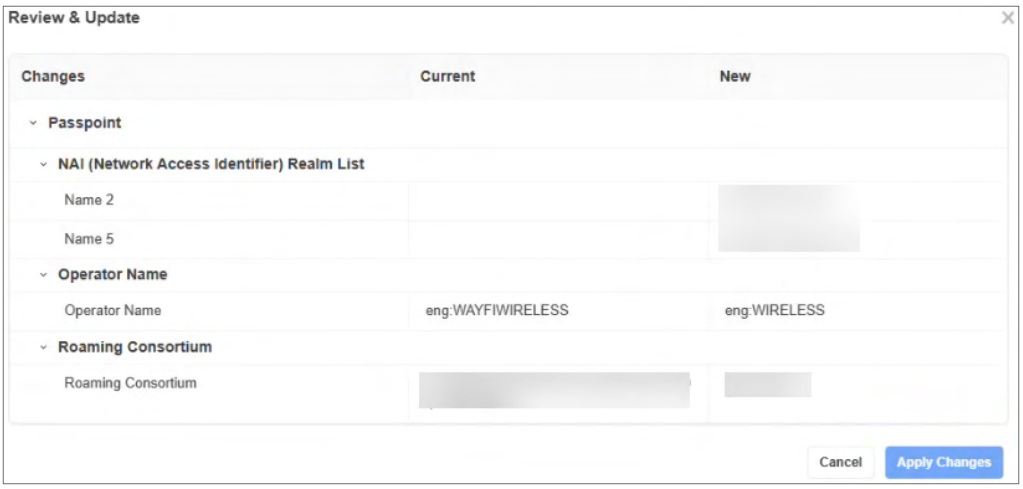


- **WLANs** page



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.

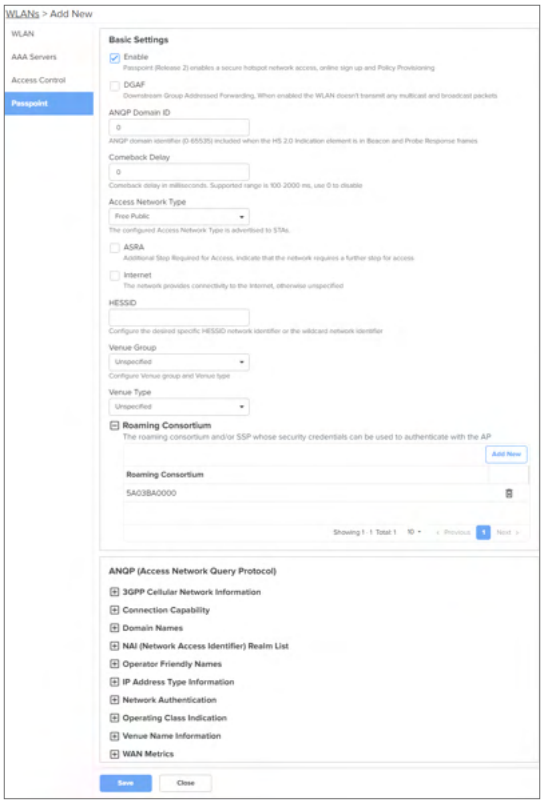
Table 80 *Passpoint parameters*

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		

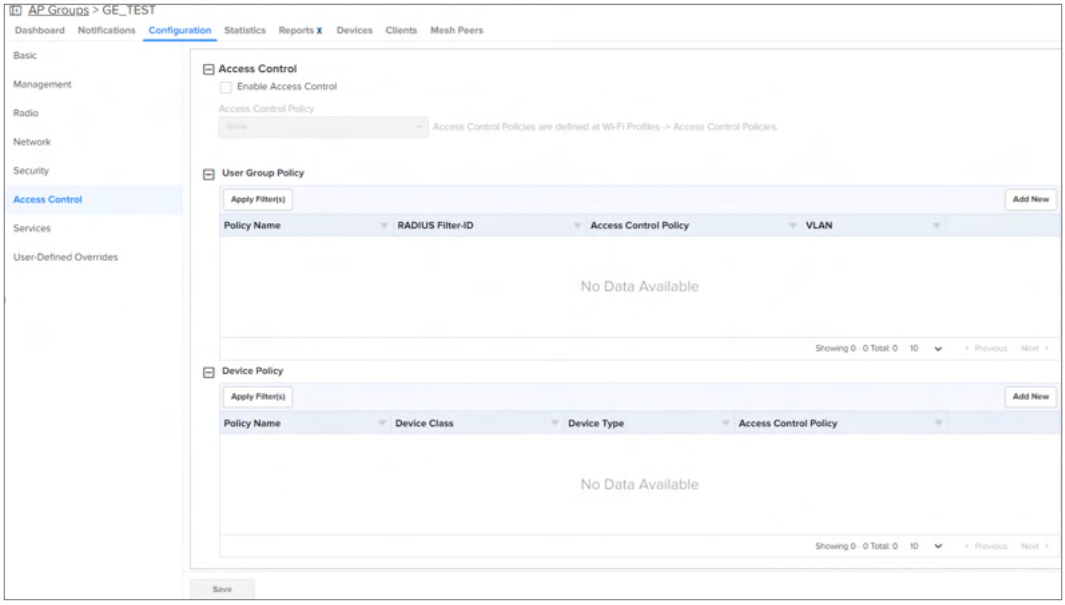
Figure 370 *Passpoint parameters*



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 371 *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 372.

Figure 372 *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 372. This provides a comprehensive view of the policies and rules within the network.

User Group Policy

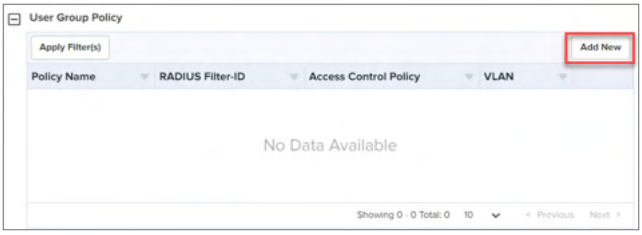
User Group Policy enables users to categorize into specific roles with customized access permissions and restrictions, facilitating fine-tuned control over network access.

Adding a new User Group Policy

To add a new User Group Policy, perform the following steps:

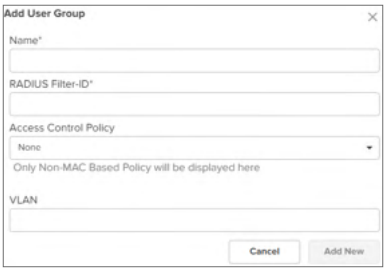
1. Navigate to **Configuration** > **Access Control** page.
2. Click **Add New** in the top right corner of the User Group Policy as shown in Figure 373.

Figure 373 *User Group Policy*



3. Complete the details in the **Add User Group** pop-up window as shown in Figure 374.

Figure 374 *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

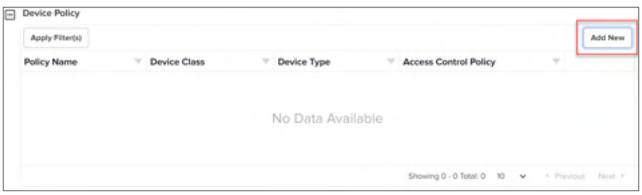
Device Policy allows users to apply specific rules and access control policies based on the type and characteristics of devices, offering customized control over device behavior within the network.

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 375.

Figure 375 *Device Policy*



3. Complete the details in the **Add Device Policy** pop-up window as shown in Figure 376.

Figure 376 *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/Disabling SSID and Passphrase. These items can be configured in the Device Configuration page, which can be selected by choosing **Manage > Configuration** in the menu, and then selecting the device in the tree to update.

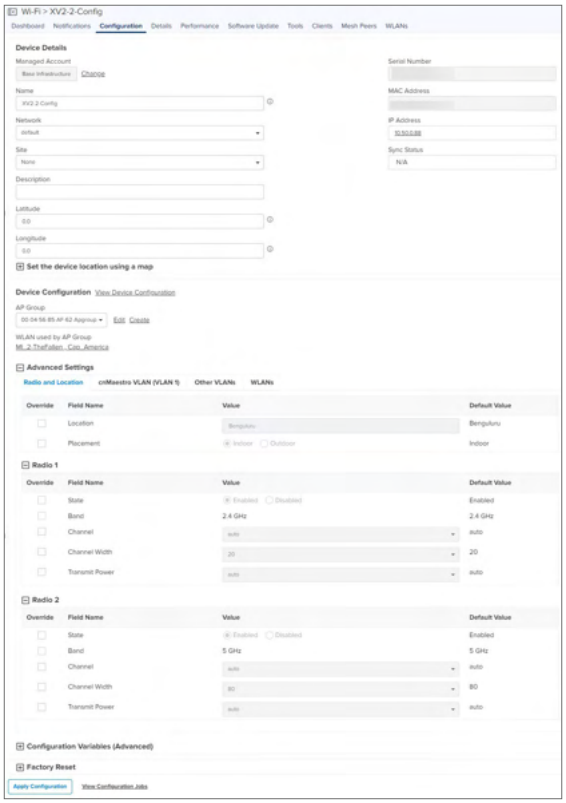
You can then choose/change different values from AP Group to be overridden. The icon to the left of a field must be selected first to override that parameter. After specifying override parameters, select **Apply Configuration** on the bottom right to save your changes to the server and create a job to push the new values to the device. This option is also applicable for Onboarding process queue.

Advanced Settings

By default, Enterprise Wi-Fi devices have **Auto-set from device** enabled. This option reads several network related configuration fields from the device and uses those as override values to prevent overwriting values that would disconnect the device.

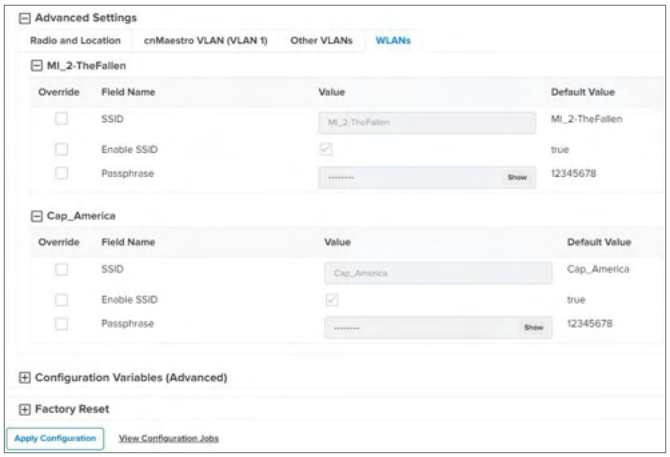
Modify the **Advanced Settings** section on the Access Point level configuration page as below:

- Add option to override Dual 5 GHz Radio setting for XV3-8 APs below the Placement field.
- If the Dual 5 GHz Radio feature is **Enabled**, then show the settings to override/configure the 3rd 5 GHz radio.
- If the Dual 5 GHz Radio option is enabled, then allow channel range > = 100 for Radio 2 and 36 – 64 for Radio 3.



Note

XE3-4TN features a radio antenna override option.



User-Defined Overrides

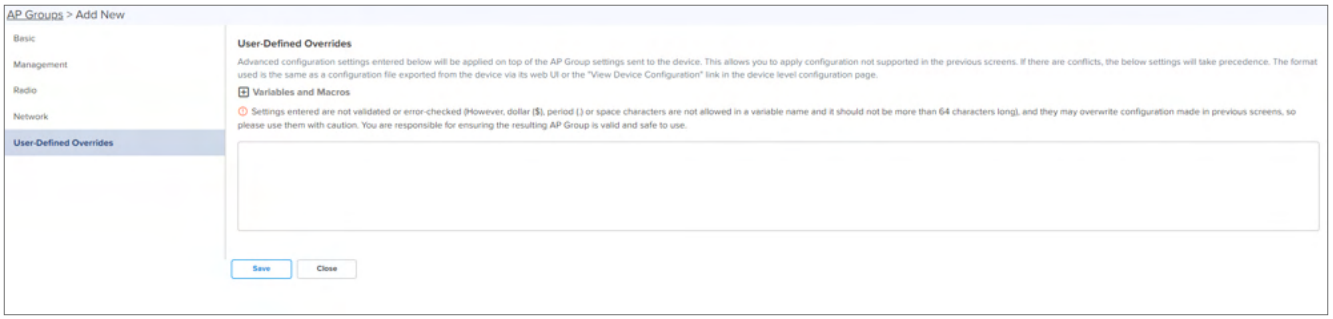
User-Defined Overrides can be entered into the end of an AP Group configuration. They will be appended to the AP Groups before the configuration is applied to the device. This allows setting configuration parameters which are not supported by GUI; this is an advanced operation that should rarely be used. 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.

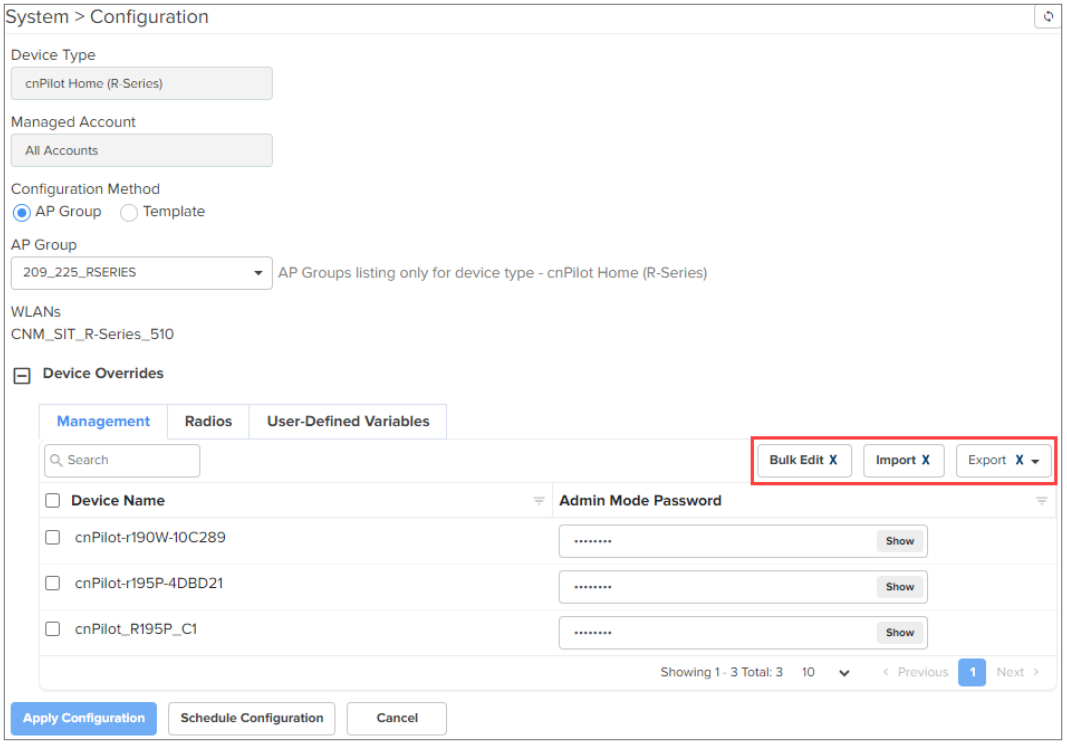
Note

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
- Wi-Fi Configuration

Figure 377 *Bulk Override: cnPilot (R-Series)*

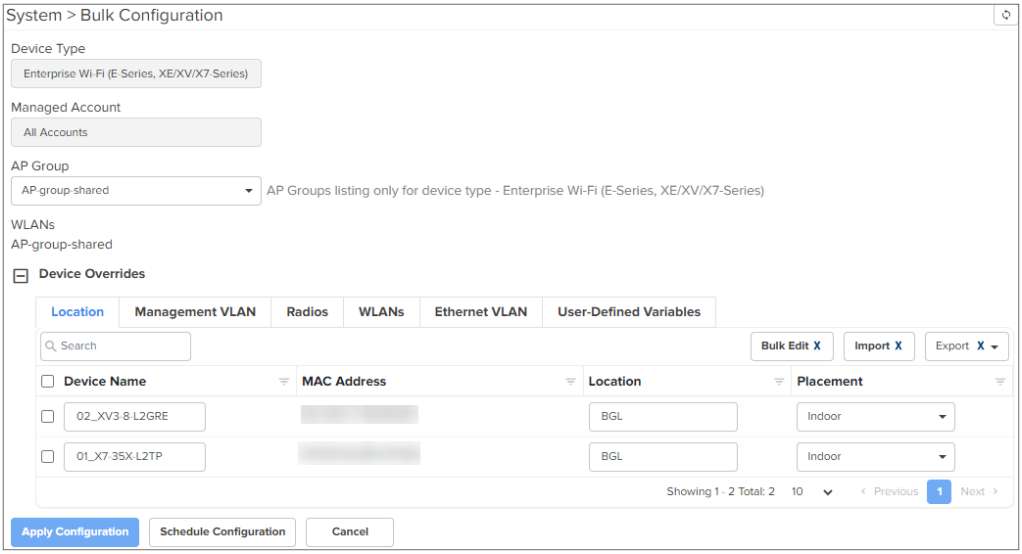


The user can override the following configurations in Enterprise Wi-Fi (E-Series, XV-Series):

- Location
- Management VLAN
- Radios
- WLANs

- Ethernet VLAN
- User-Defined Variables

Figure 378 *Bulk Override: Enterprise Wi-Fi (E-Series, XE-Series, XV-Series)*



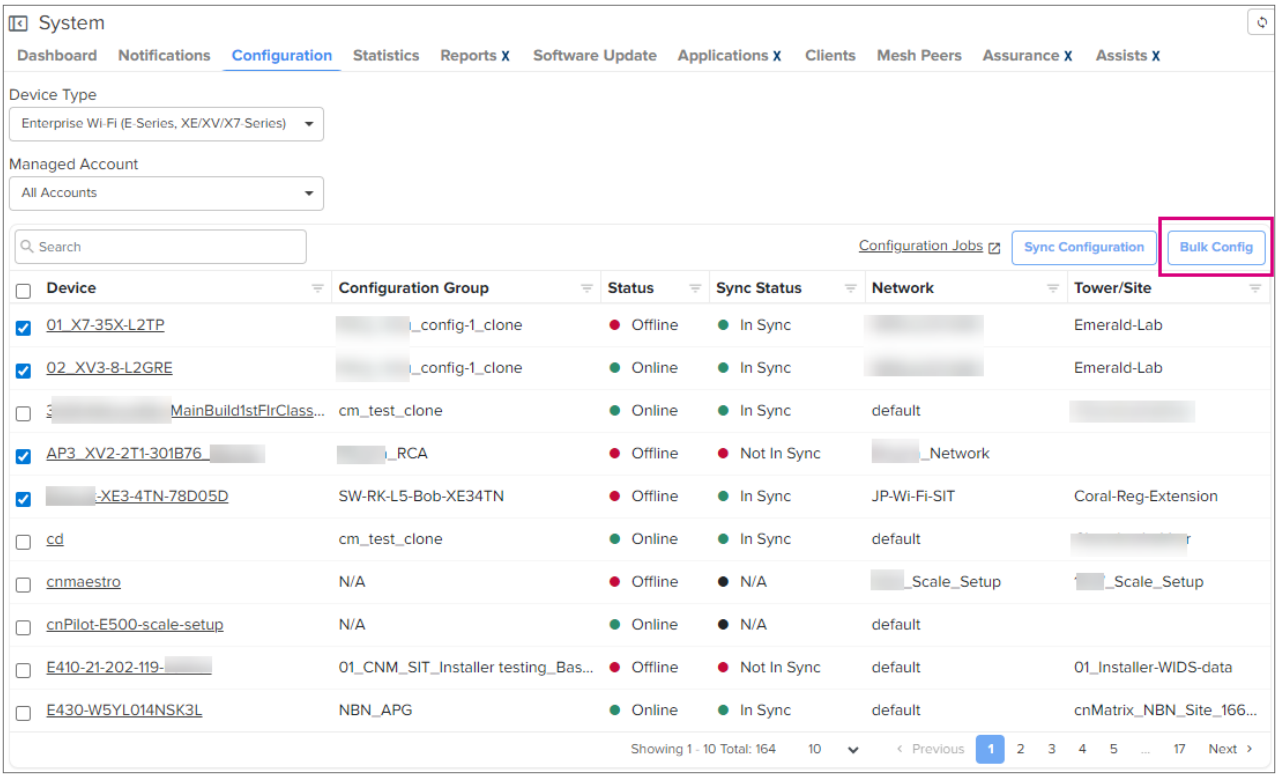
Note

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:

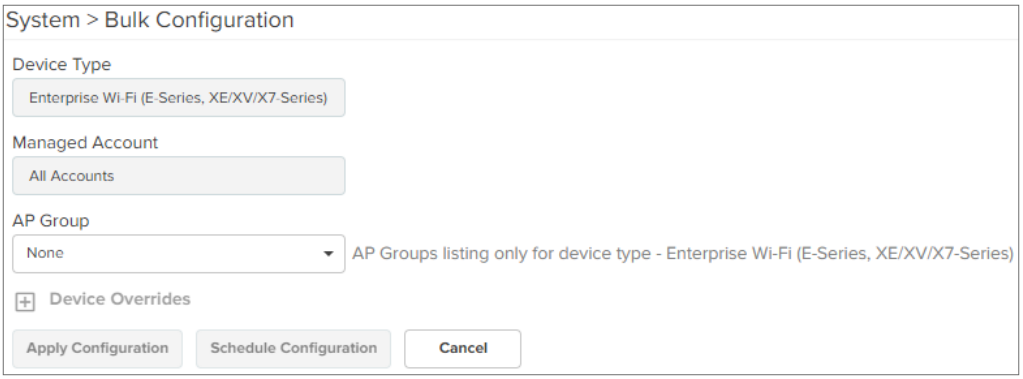
1. Navigate to **Monitor and Manage > System > Configuration.**
2. Select **Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)** from the **Device Type** from the dropdown.
3. Select the checkboxes corresponding to the devices you want to configure and click **Bulk Config**.

   To select all devices, select the checkbox next to the **Device** column name.

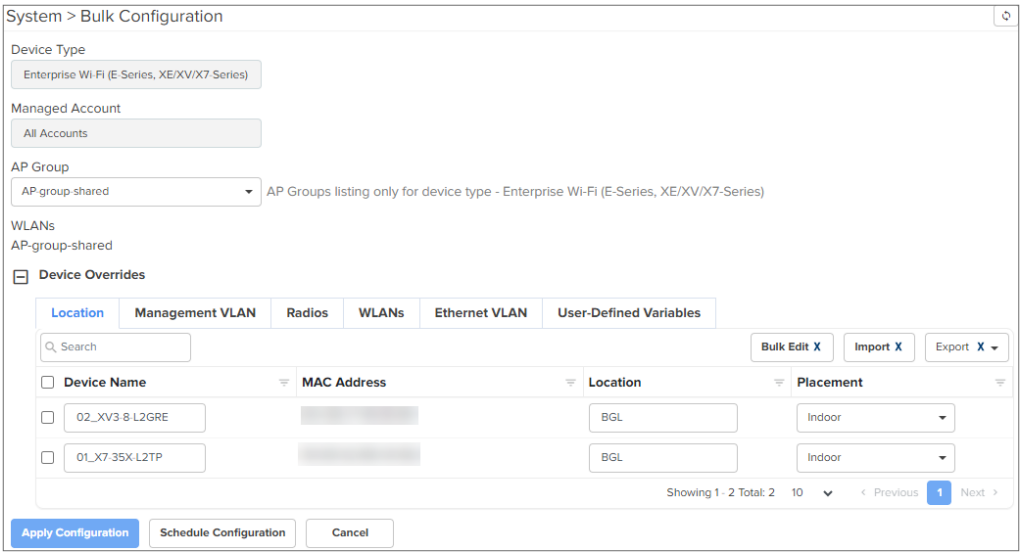


The **System** > **Bulk Configuration** page is displayed.

4. Select an appropriate AP group from the dropdown if **None** is selected by default.



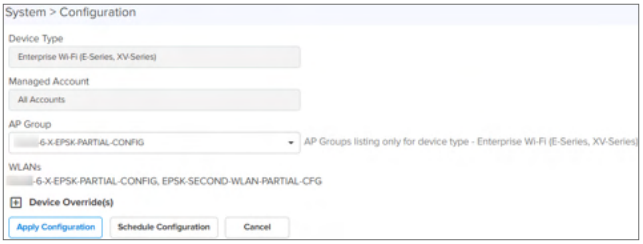
5. Expand the **Device Overrides** section by clicking the plus (+) icon.



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**.



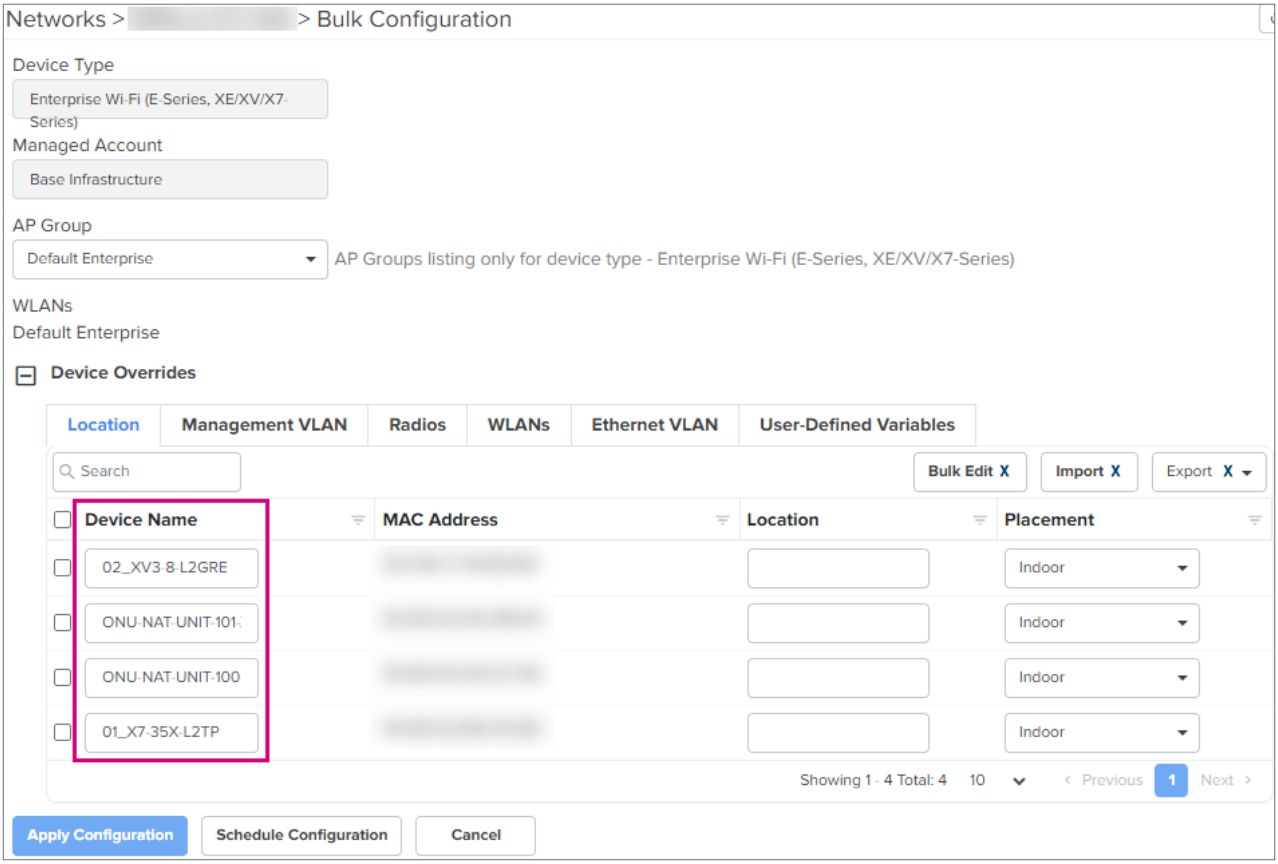
Location

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.**



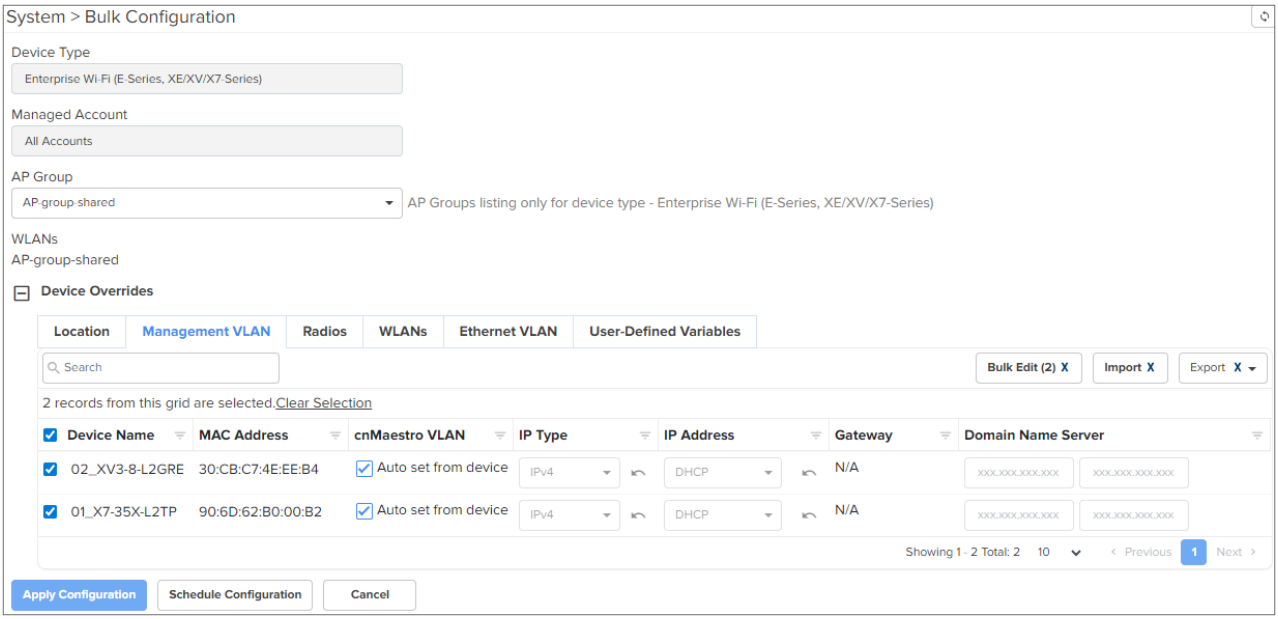
4. **Override Location** window appears, edit the configuration details and click **Save**.



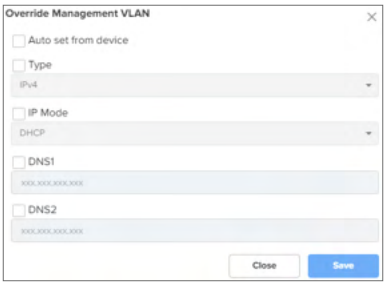
5. Click Save.

Management VLAN

1. In the **Management VLAN** tab, select the devices from the list and click **Bulk Edit**.



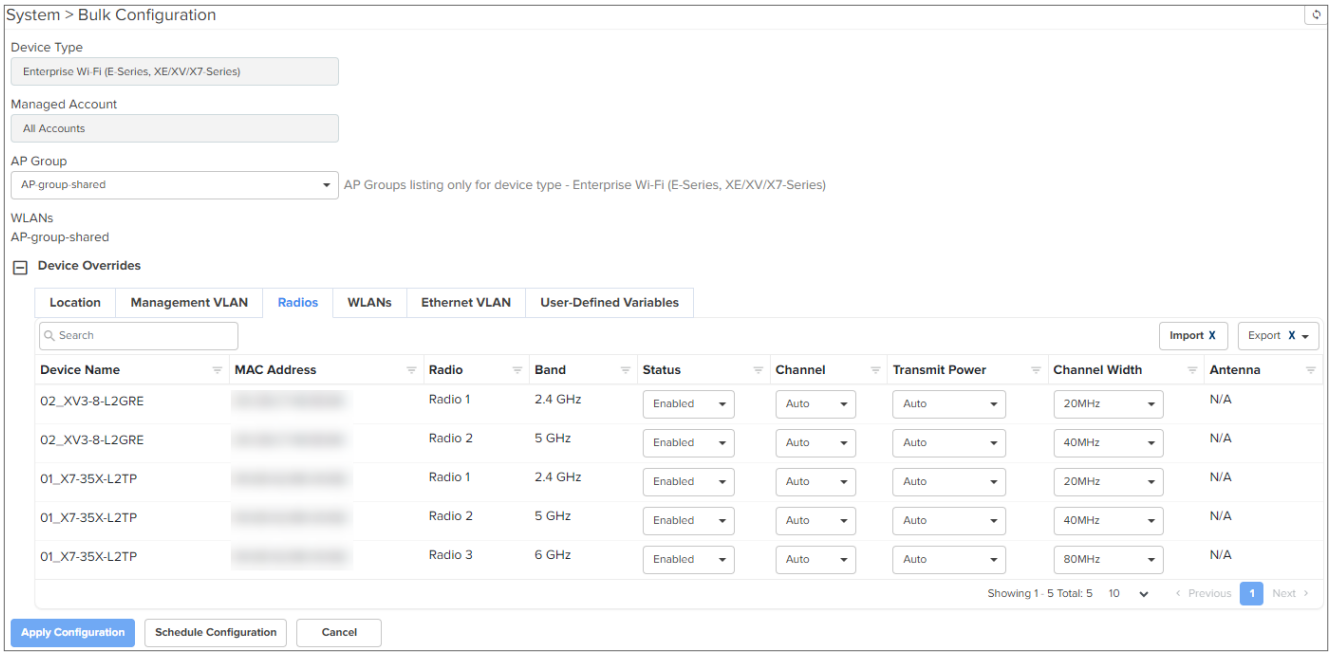
2. In the **Override Management VLAN** window appears.



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.



Note

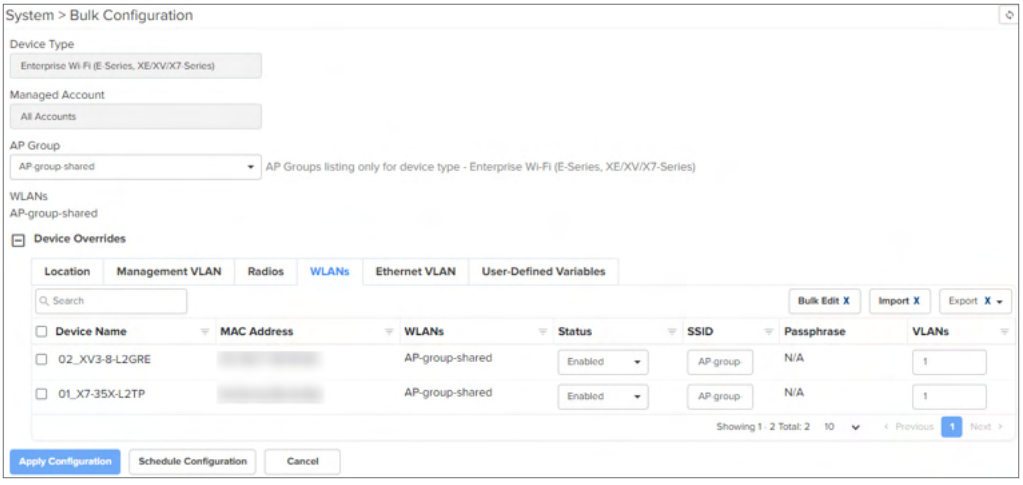
Bulk Edit tab is removed from Radio configuration from 3.1.1 release.

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.

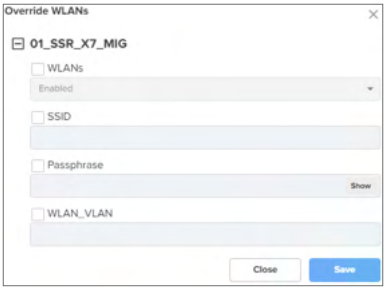
WLANs

1. In the **WLANs** tab, select the WLAN of the devices from the list.



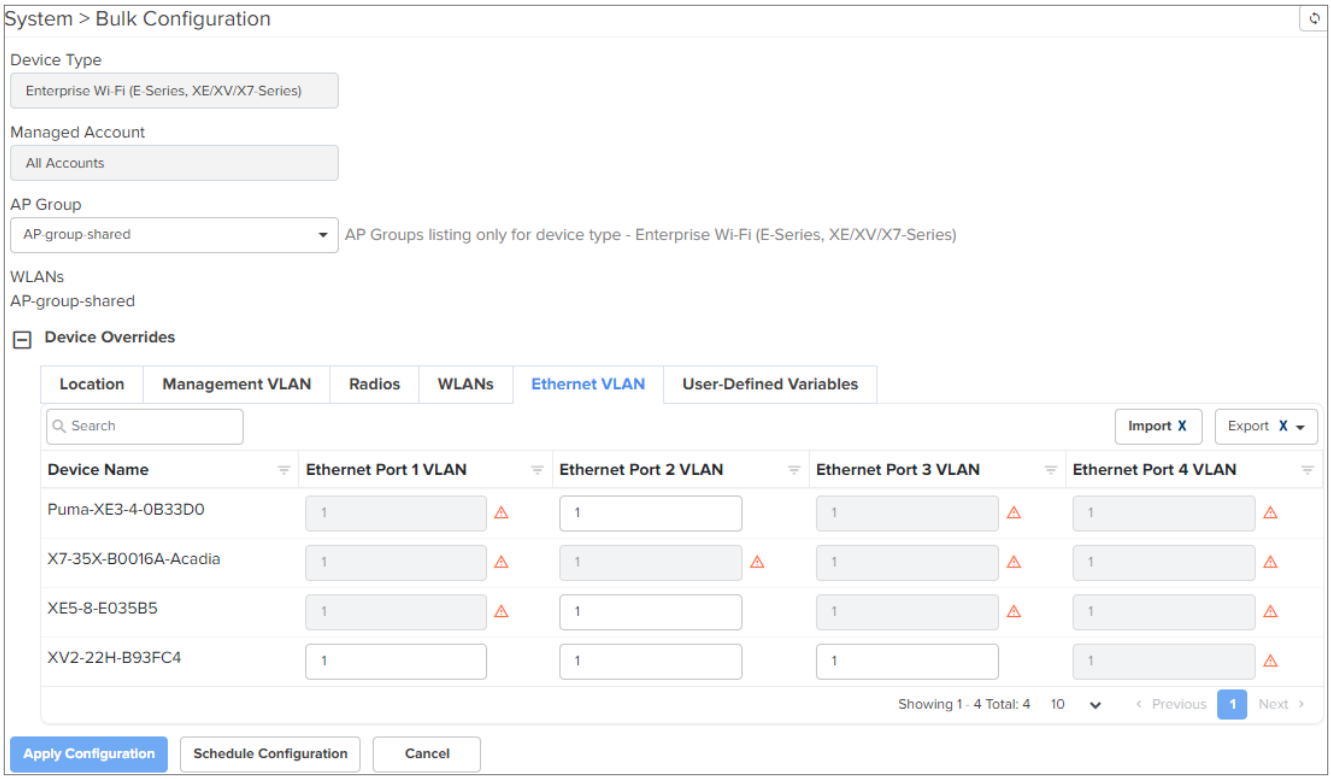
2. Click **Bulk Edit**.

3. **Override WLANs** window appears, edit the configuration details and click **Save**.



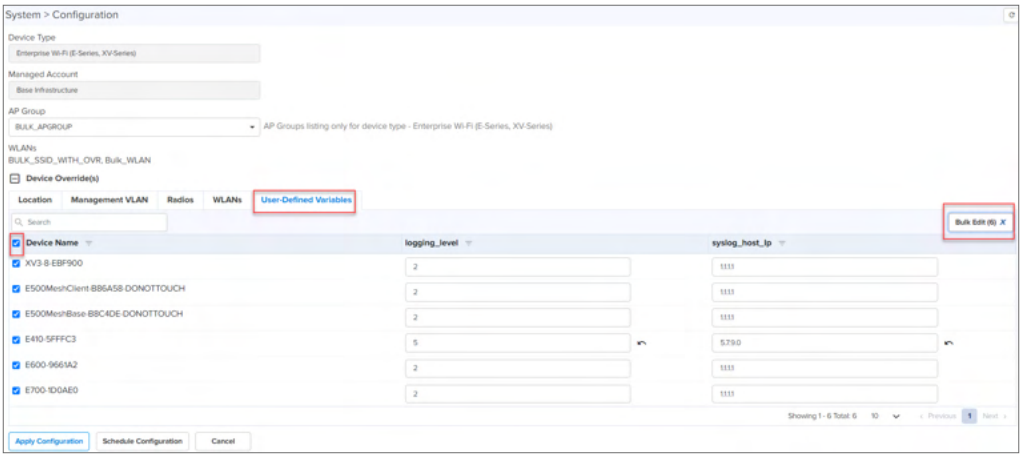
Ethernet VLAN

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.



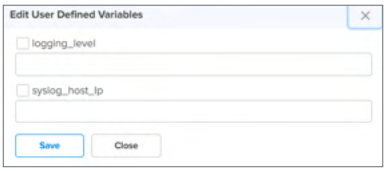
User-Defined Variables

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

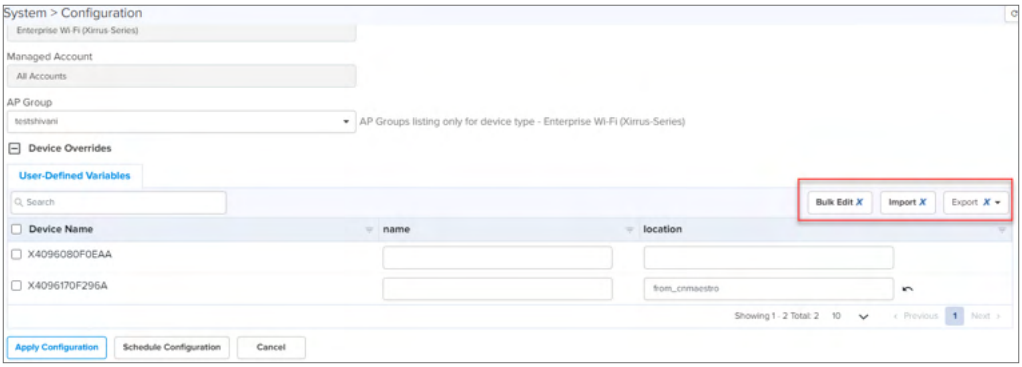
For Bulk overrides to be enabled in **User-Defined Overrides** tab, you must define the overrides in the **User-Defined Overrides** section of AP groups. For more details, see User-Defined Overrides

4. Click **Apply Configuration** to start immediately, or click **Schedule Configuration** to schedule later.

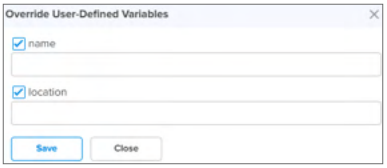
The user can override for the following configurations in Enterprises Wi-Fi (Xirrus-Series):

- User-Defined Variables

Figure 379 *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)

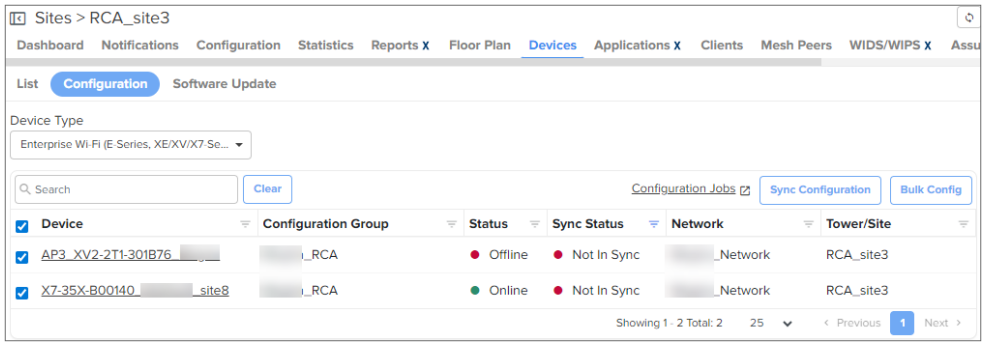
Steps to sync configuration

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**.

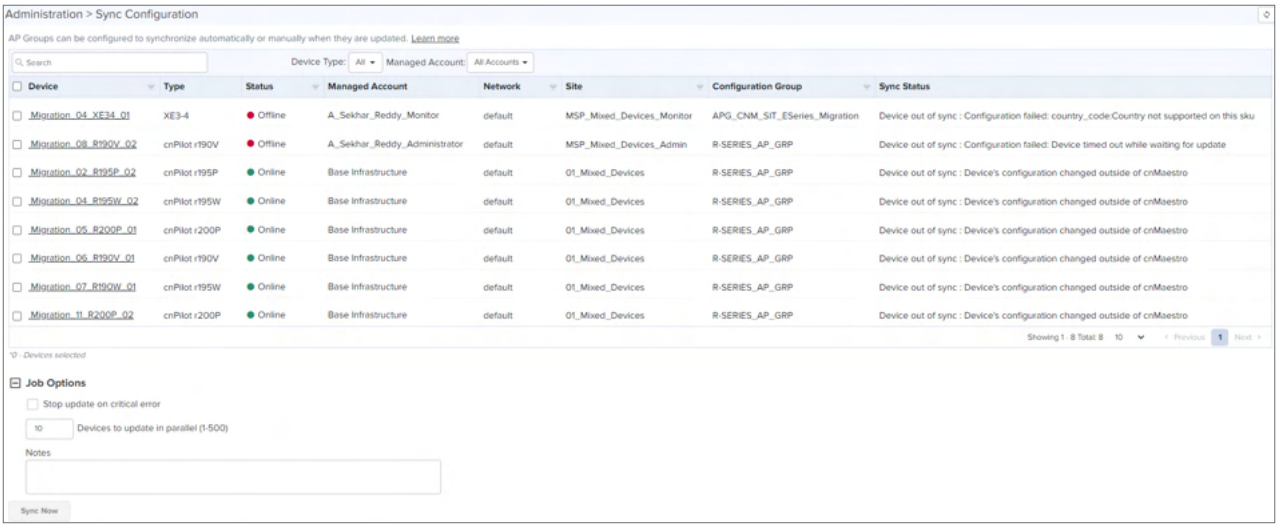
Figure 380 *Site-level out of sync devices*



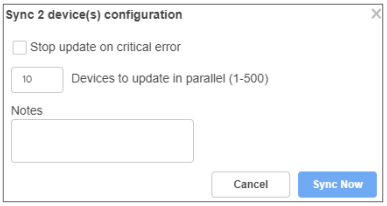
- **Administration** > **Sync Configuration**.

  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

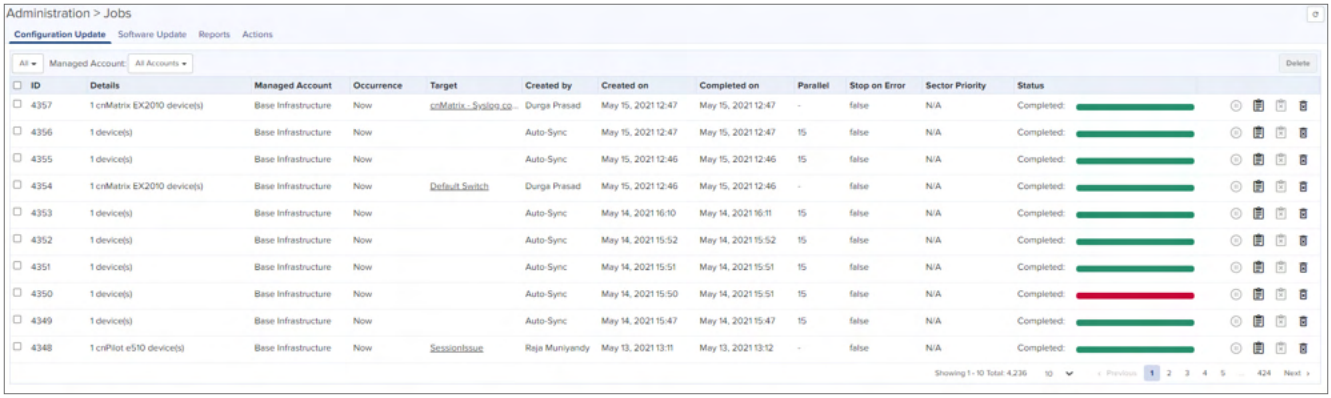
same device.

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

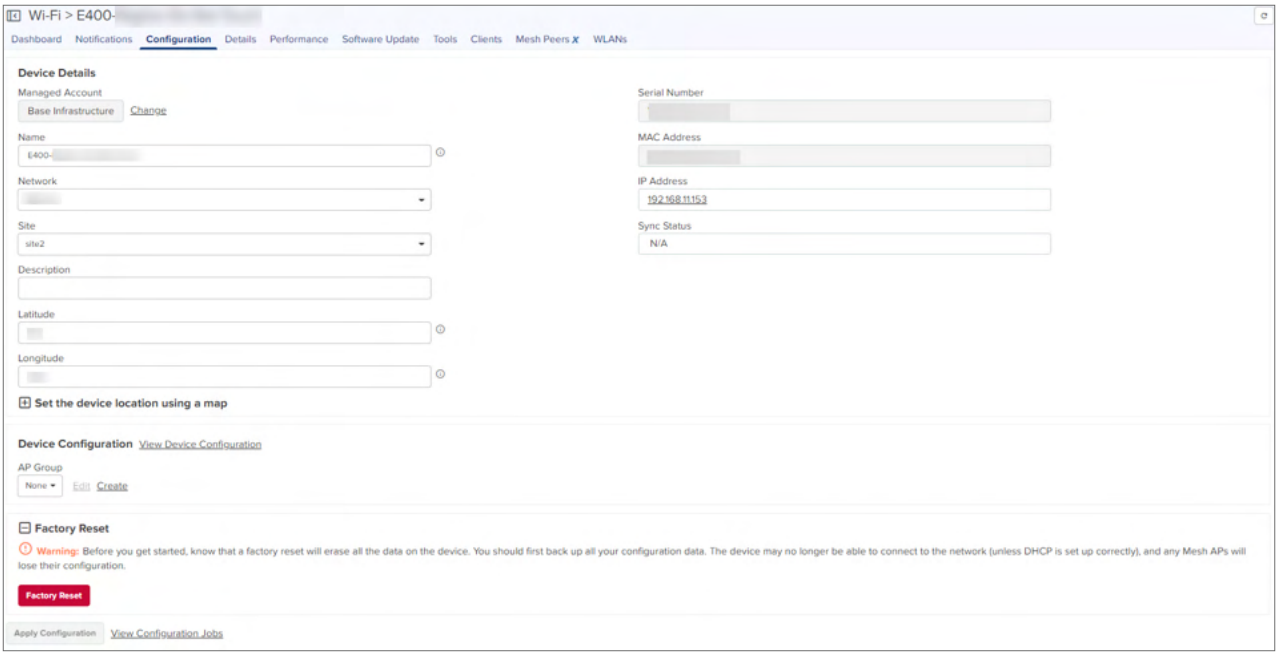
- Configuration jobs skip offline devices. With manual synchronization, they need to be synchronized by the administrator.
- For more information on Wi-Fi AP configuration, refer to the following URLs:
  - Unique per-Device values in Profiles Using User-Defined Overrides
  - AP Groups and Overrides for 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.

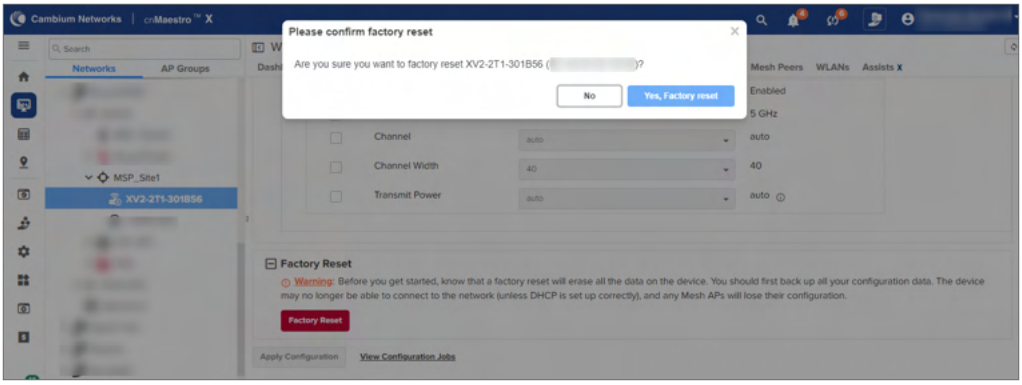
To factory reset the device perform as follows:

1. Navigate to the **Configuration** page of the device.
2. Select **Factory Reset.**

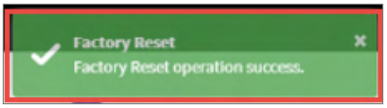


3. Click **Factory Reset**.

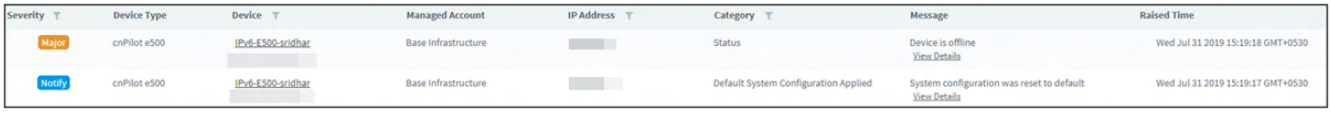
   It displays **Please confirm factory reset** message as shown below:



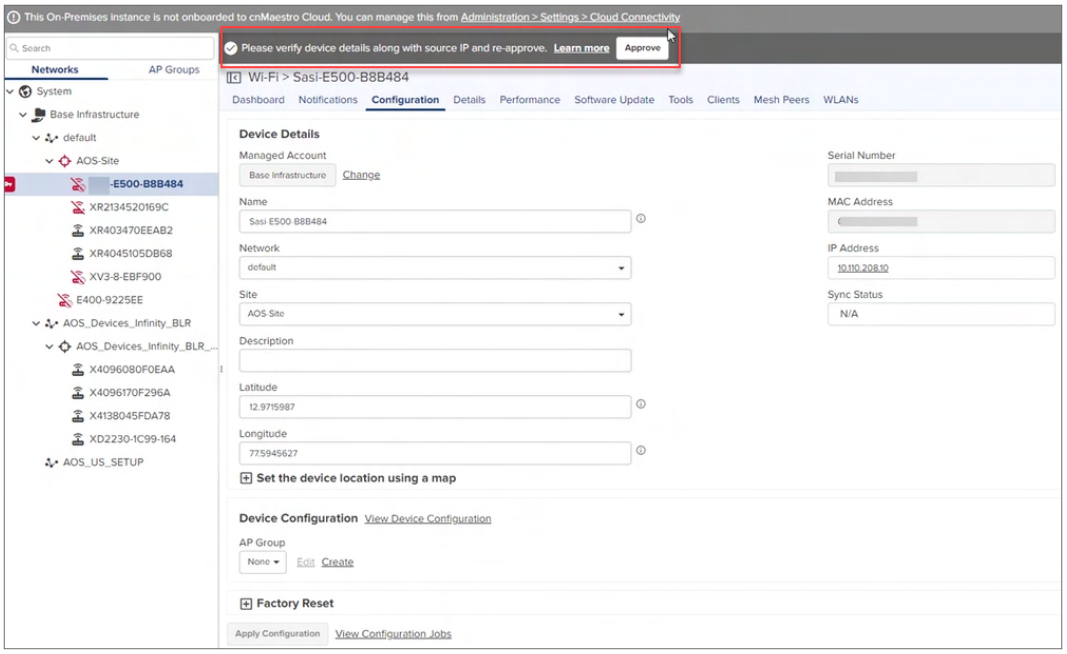
4. Click **Yes, Factory reset** option.



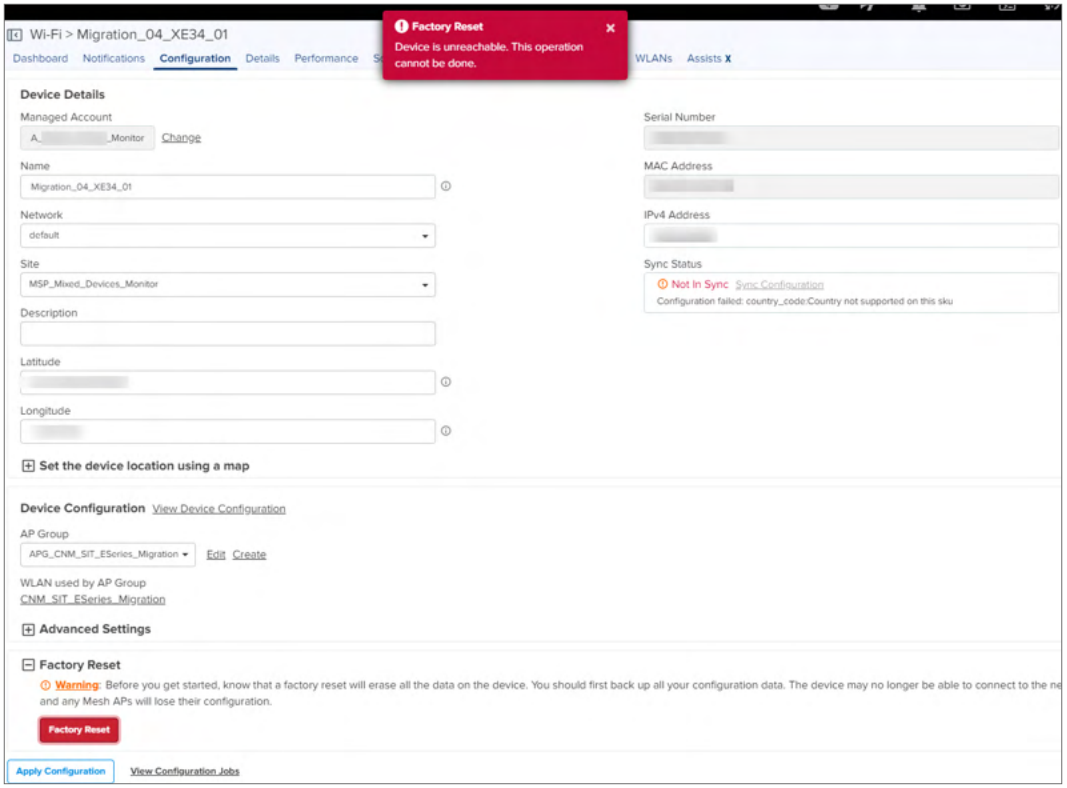
If the Factory Reset is successful, the following message is displayed on the **Notifications** tab.



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

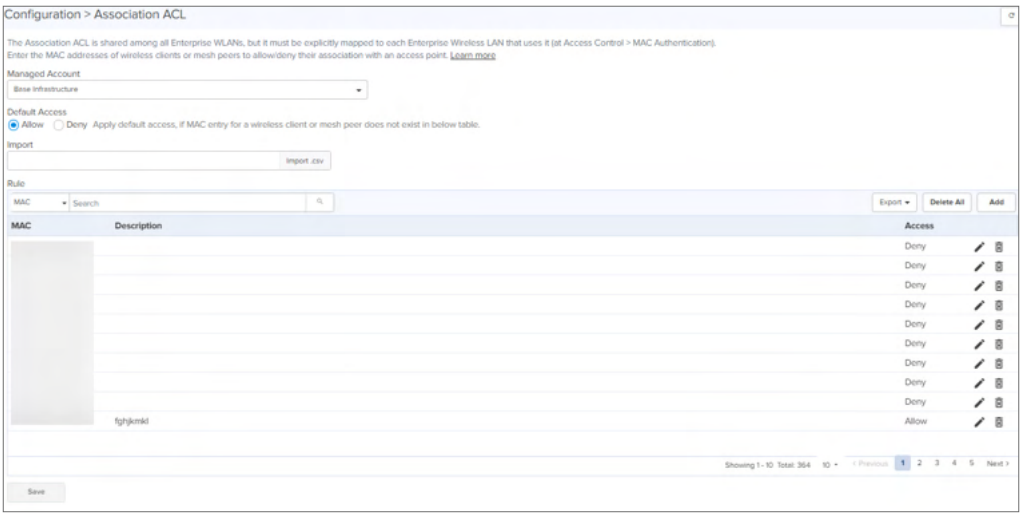
When a client tries to connect to an AP, the following occurs:

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.

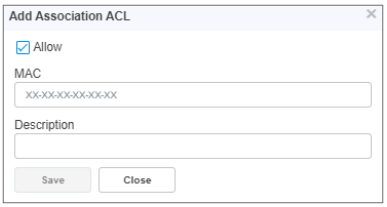
Configuring Association ACL

To configure the Access Control List (ACL) in cnMaestro:

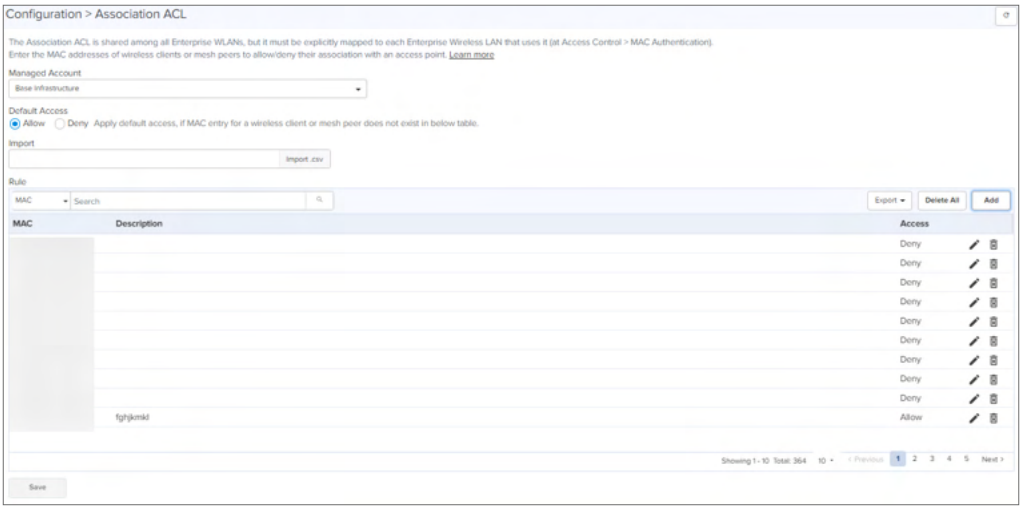
1. Navigate to **Configuration** > **Wi-Fi Profiles** > **Association ACL** tab**.**
2. Click **Add.**



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.

Access Control Policies

This feature allows you to configure policies that define who can connect to the network, and how or when they are allowed to connect and access a specific device. The policies are a set of conditions, constraints, and settings.

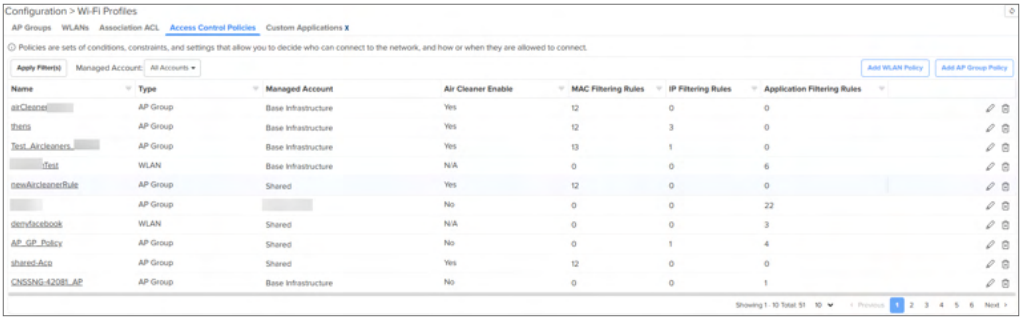
The policies can be configured on both AP Group level and WLAN level, AP Group policies have more priority than WLAN Access Control policies.

On both AP group policy and WLAN policy, we can have L2, L3 and L3 Rules. The configuration rules are processed in following priority: MAC Filters followed by IP and Application Filters.

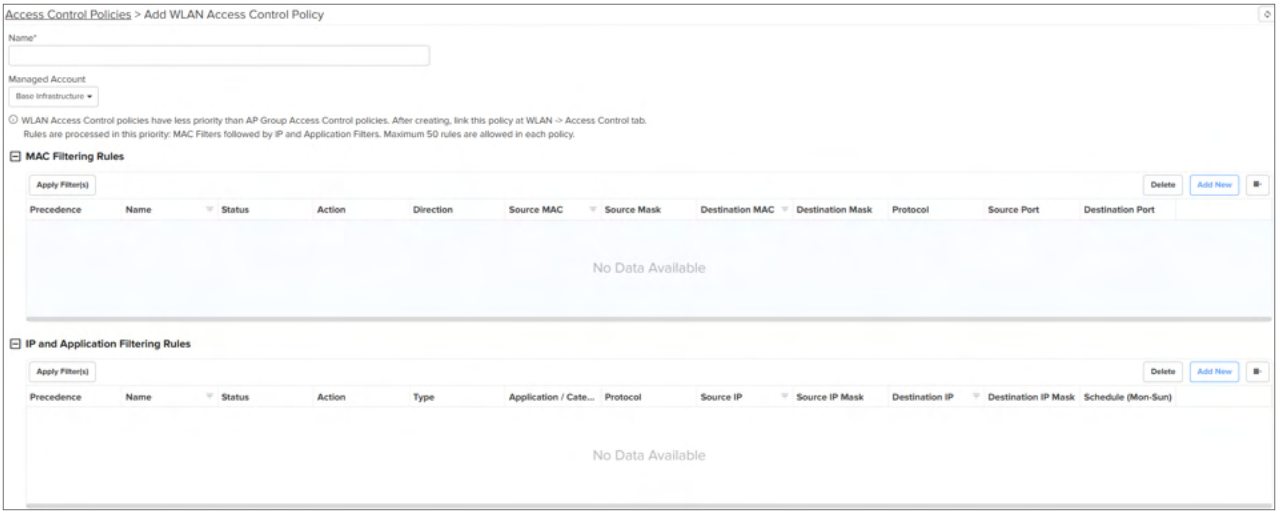
Configuring Access Control Policies for AP Groups and WLANs

To configure the Access Control Policies:

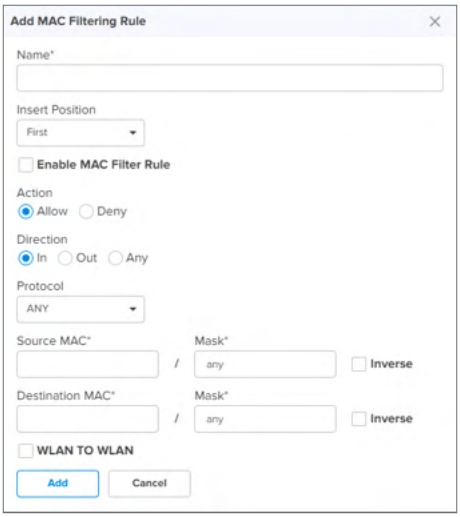
1. Navigate to **Configuration > Wi-Fi Profiles > Access Control Policies** tab**.**



2. Click **Add WLAN Policy** or **Add AP Group Policy**.



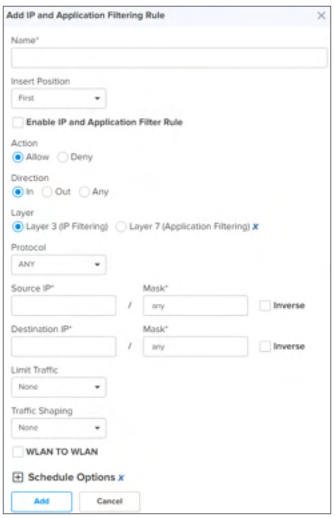
3. Enter a **Name** for the policy.
4. Select the **Managed Account** from the dropdown list.
5. For AP Groups, **Enable Air Cleaner**.
6. Click **Add New** in the top right corner of the **MAC Filtering Rules** list and complete the details in the **Add MAC Filtering Rule** pop-up window.



7. Click **Add New** in the top right corner of the **IP and Applications Filtering Rules** list and complete the details in the **Add IP and Application Filtering Rule** pop-up window.

Note

The **Layer 7 (Application Filtering)** option is a cnMaestro X feature.



8. After adding all the required rules, click **Add**.
9. Navigate to **WLAN** > **Access Control** or **AP Group** > **Access Control** tab and link this policy.

Note

- AP Group Access Control Policies are applied at the device level.
- WLAN Access Control policies have less priority than AP Group Access Control policies.

Custom Applications X

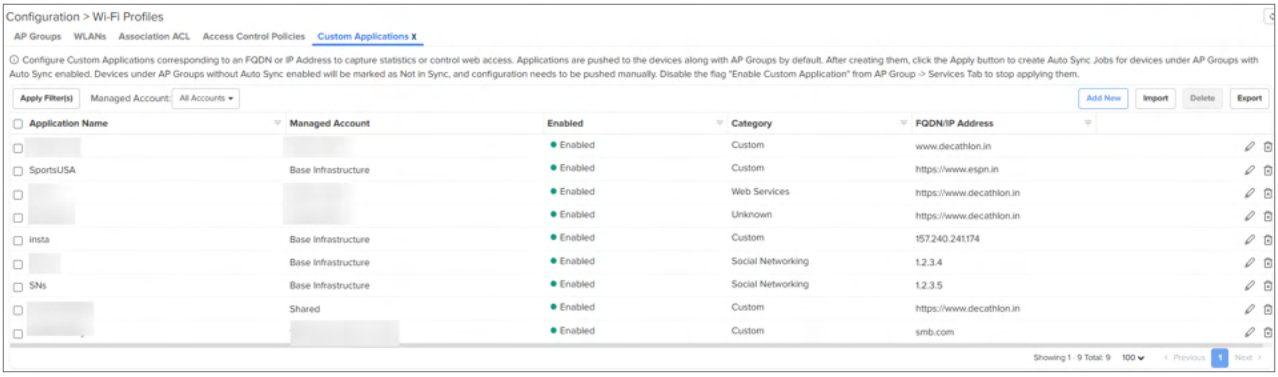
Custom applications allow you to configure applications with a specific IP address or a domain name, and apply filter rules, such as enable or disable traffic from these applications. By default, these applications are applied on the devices along with the AP group configuration.

After creating the custom application, when you click **Apply**, cnMaestro creates a job for devices in the AP group that has auto sync enabled. Devices in AP groups that do not have auto sync enabled, are marked as **Not in Sync**, and users must manually apply the configuration on to the devices.

To disable cnMaestro from applying the custom application configuration on the devices, clear the **Enable Custom Application** checkbox from the **AP Groups** > **Services** tab > **Application Visibility** X section.

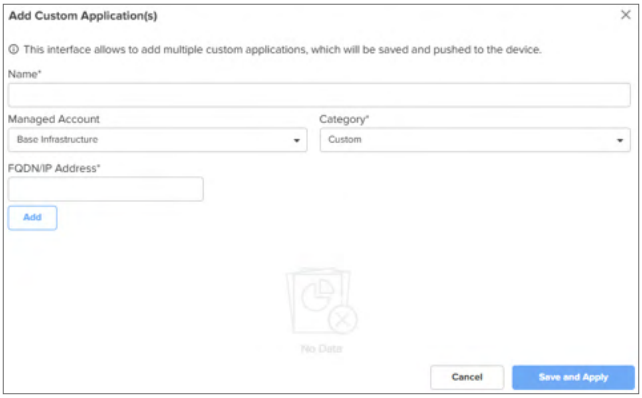
To add a new custom application, complete the following steps:

1. Navigate to **Configuration** > **Wi-Fi Profiles** > **Custom Applications** X.



2. Click **Add New** on the **Custom Applications** X page.

   The **Add Custom Application(s)** window is displayed.



   Configure the following parameters:

Table 81 *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

Table 81 *Custom Application Parameters*

Parameter	Description
	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

cnMatrix switches simplify the network deployment and operation. cnMaestro provides management, configuration, control, and security services for cnMatrix with deployment options such as Policy-Based Automation (PBA) to simplify core operations and improve network security. Central to cnMaestro's orchestration of cnMatrix devices is the concept of Switch Profiles.

Port Templates allow users to create and reuse predefined port configurations across multiple ports within a Switch Group.

This chapter describes the following topics of the Switch Profiles:

- Switch Groups
- Port Templates

Switch Groups

A Switch Group represents a virtual stack of switches, independent of their locations or networks. The Switch Group functionality enables users to manage multiple switches with the same configuration.

Configuration is common to all switches belonging to a Switch Group:

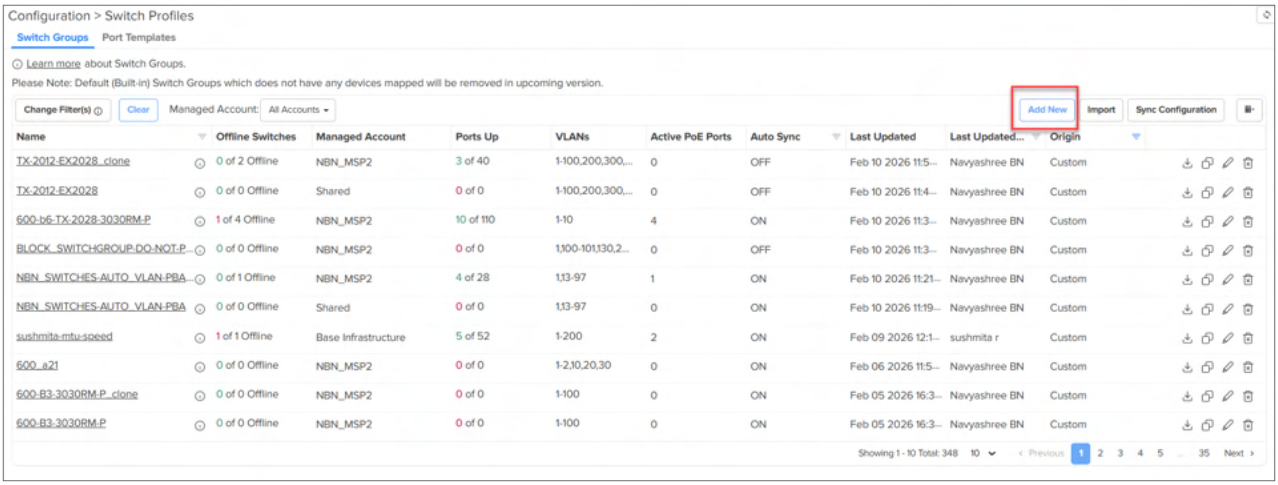
- Configuration changes are synchronized and applied to all the switches in a Switch Group.
- A subset of configuration attributes can be overruled for an individual switch.
- Switch Ports across all physical switches are associated with a Switch Group and can be simultaneously bulk edited.

This section contains the following topics:

- Synchronize (Sync) Configuration
- Policy Based Automation (PBA)
- Devices
- Ports Stack
- Device Details

The process for creating a new switch group configuration is as follows:

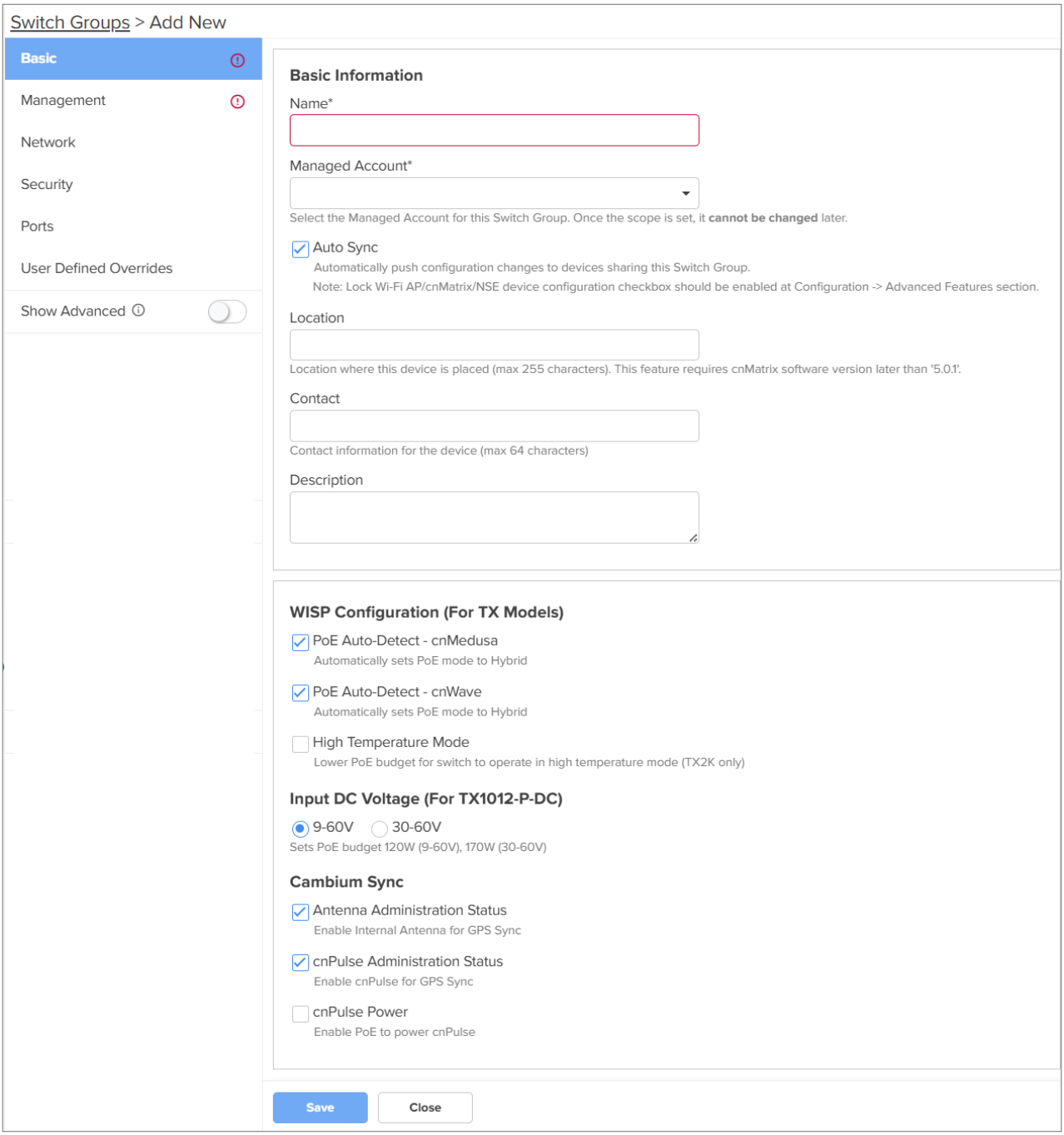
1. Navigate to **Configuration** > **Switch Profiles** > **Switch Groups** tab.
2. Click **Add New**.



Note

To edit the Configuration of an existing switch group, click the edit ( ) icon, navigates to Switch Group Configuration page.

3. Configure the following tab parameters to create a Switch groups:
4.
   - Basic
   - Management
   - Network
   - Security
   - 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

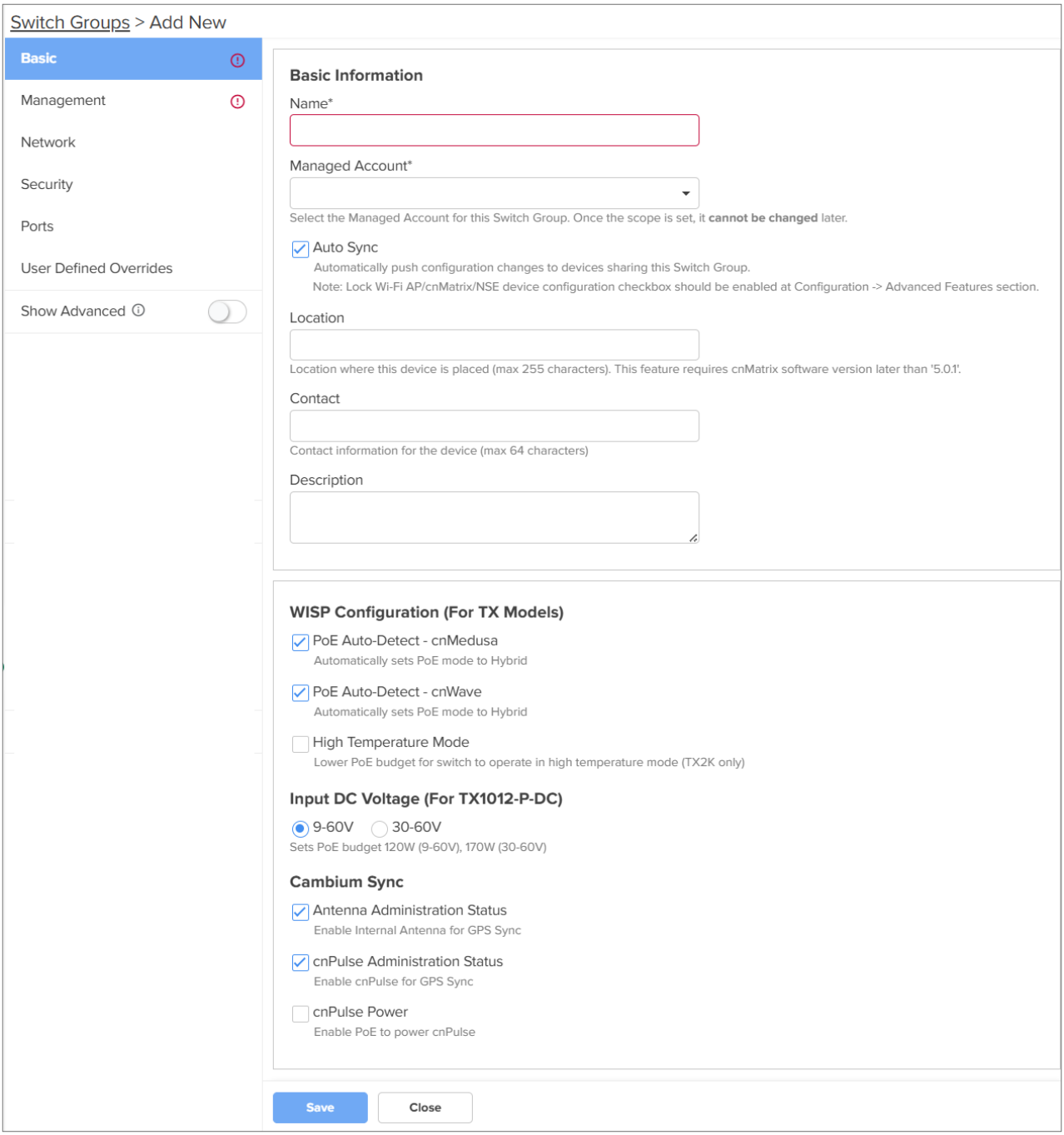
The Basic tab provides options to the user to configure the device name as well as other standard values used to identify a switch.

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.

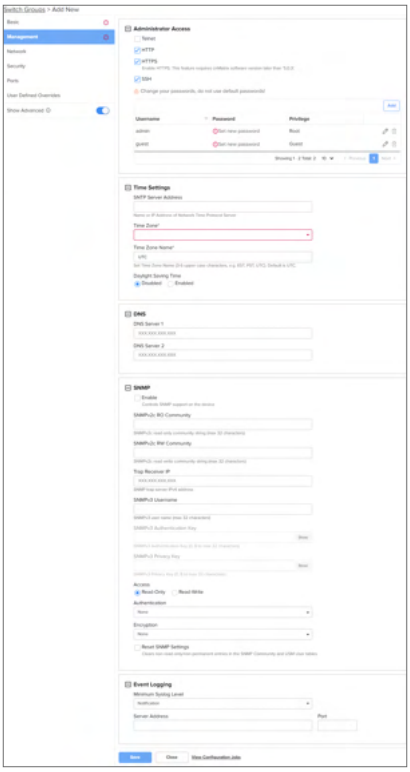


3. Click **Save**.

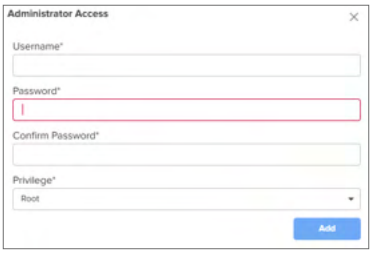
Management

The **Management** page allows you to configure Administrator Access, Time Settings, DNS, and Event Logging.

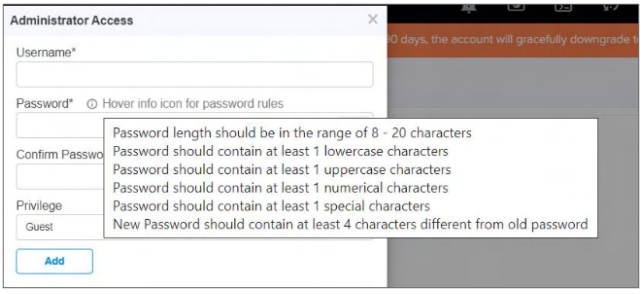
1. Navigate to **Switch Groups** > **Management** page.
2. If required, enable the **Daylight Saving Time** and enter the details.



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.

    By default, SNMP is disabled. To enable SNMP, toggle the **Show Advanced** option to the on position.

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

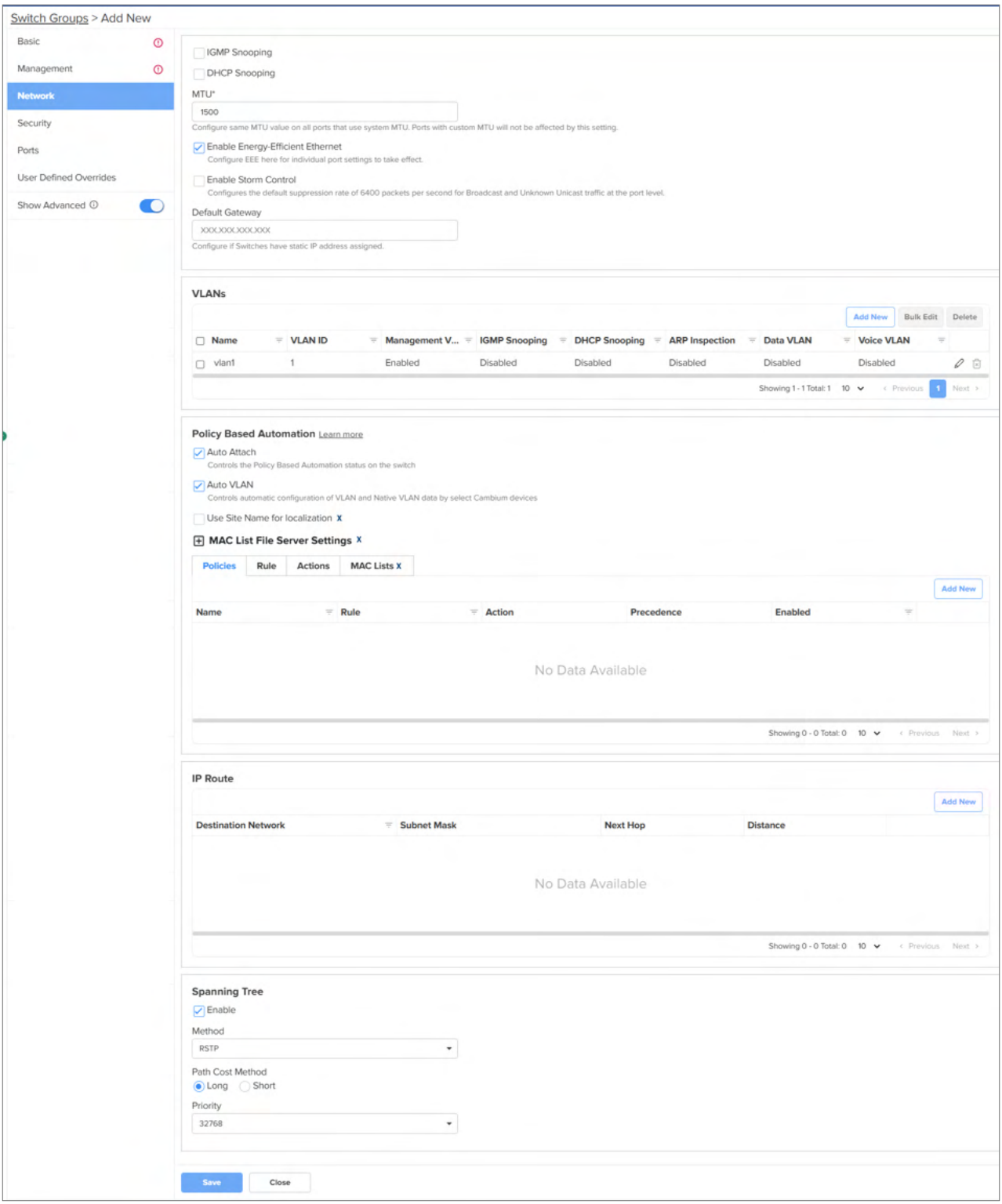
The Network page allows the user to configure VLANs, PBA, IP Route, and Spanning Tree details.



Note

From release 3.0.4 cnMatrix Switches supports MSTP Mode and Path Cost Method in Spanning Tree.

1. Navigate to **Switch Groups > Add New > Network** page.



Note

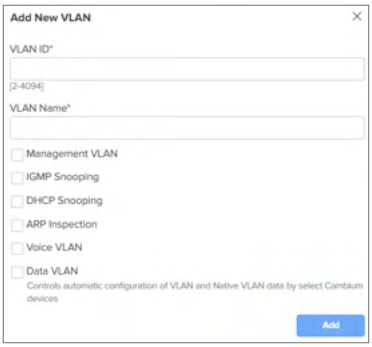
Use Site Name for localization, **MAC List File Server Settings**, and **MAC Lists** are cnMaestro X features.

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

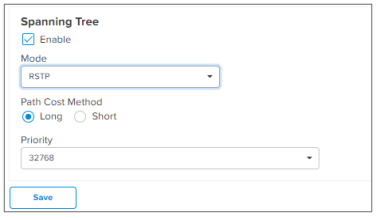
Update to apply the changes.



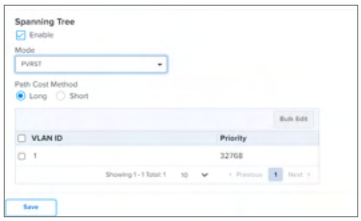
7. If required to add a new IP Route, click **Add New.**
   a. Enter the **Destination Network**.
   b. Enter the **Subnet Mask**.



   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**.

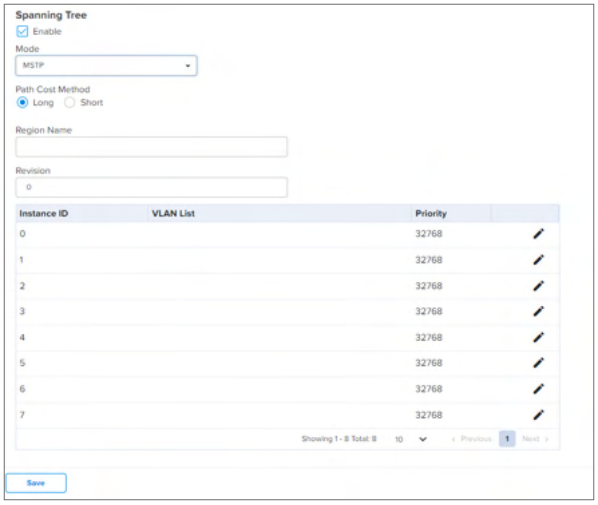


   b. Select the Mode **PVRST** from the drop down.
      - Select Path Cost Method **Long** or **Short.**
      - Select **Priority**.

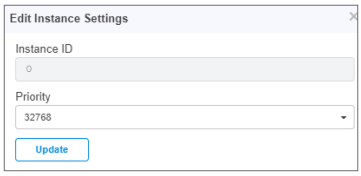


c. Select the Mode **MSTP** from the drop down.

- 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.**

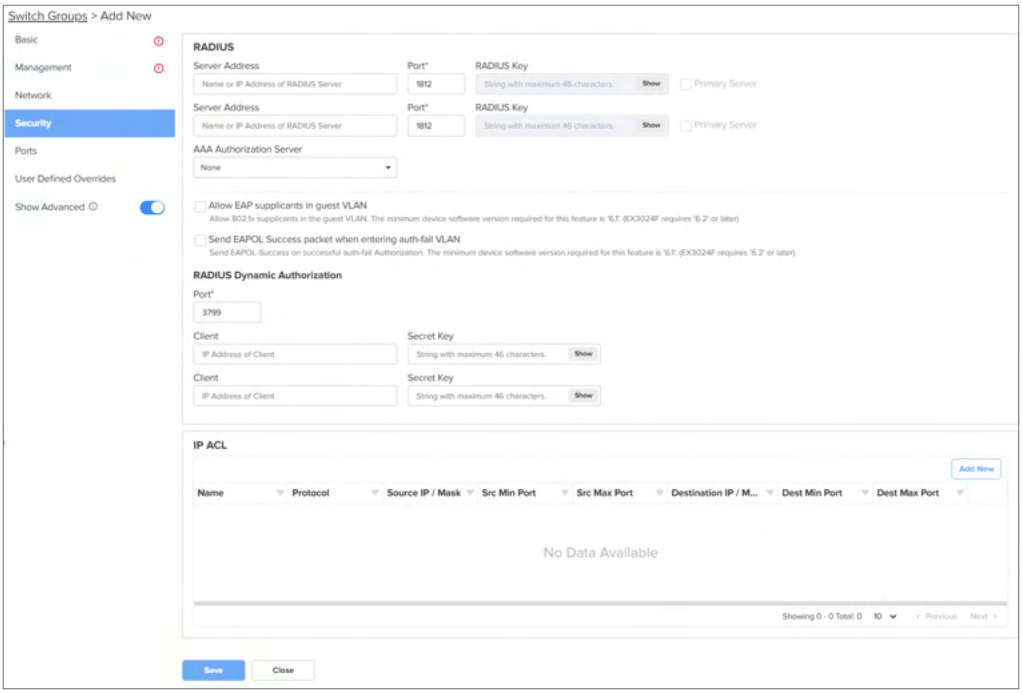


9. Click **Save.**

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**.

Port Overrides

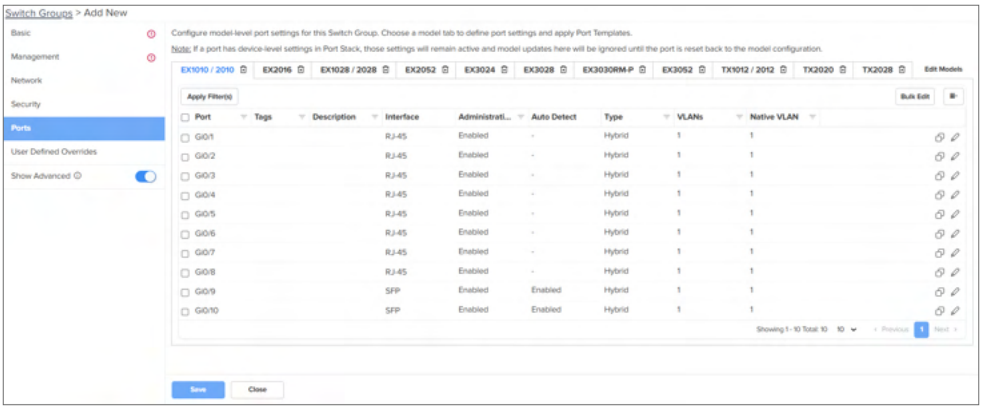
The Port Overrides section allows user to configure common port settings for each switch model in a switch group. These settings are automatically applied and shown in the **Ports** > **Port Overrides** section.

Note:

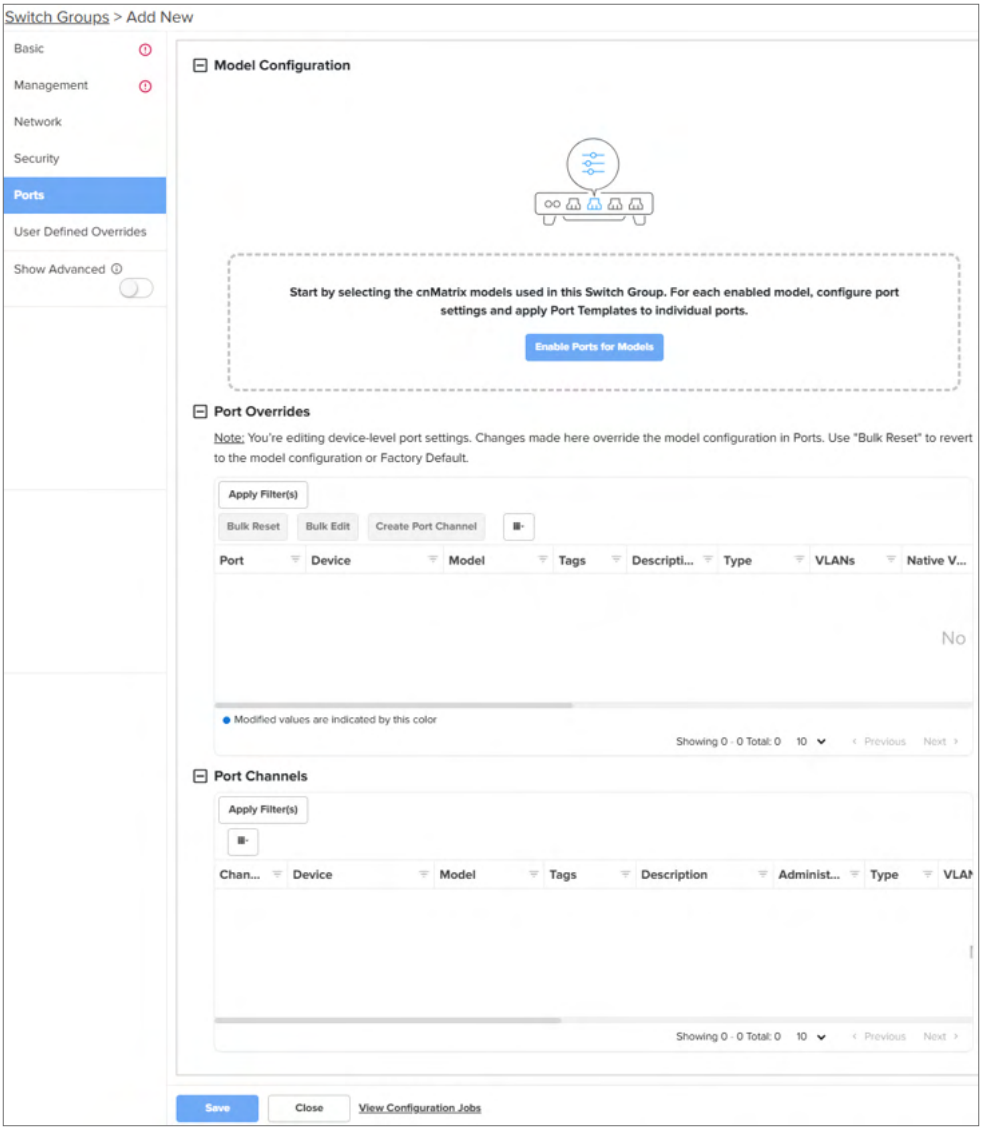
Configuration changes made in the **Port Overrides** section always take priority and override the configuration in the **Model Configuration** section.

To configure Ports, perform the following steps:

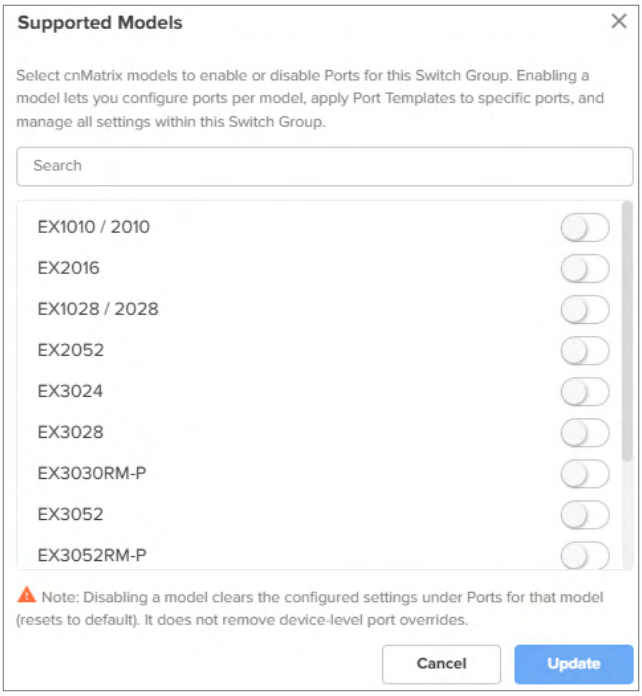
1. Navigate to **Switch Groups** > **Ports** section.
    - For new switch groups or switch groups already running the current release, Ports is available by default.



    - For existing switch groups upgraded from earlier releases, users must enable Ports before configuring port-level settings.



2. In the **Model Configuration** section, click **Enable Ports for Models**.



a. Toggle the button to enable or disable the device models for ports.

Note:

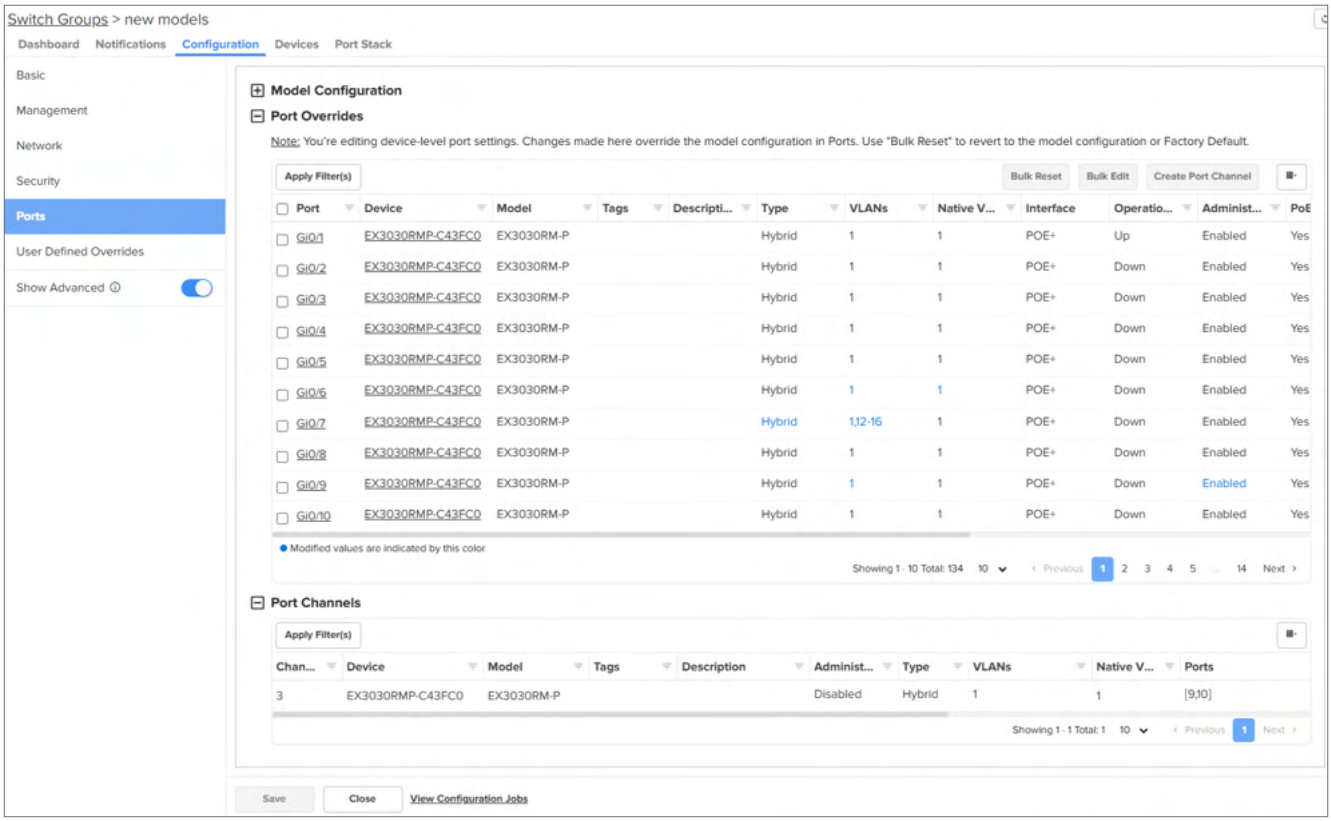
Once a device model is disabled in Ports and the changes are saved, the configuration cannot be restored. Re-enabling the model applies the default port configuration.

b. Click **Update**.

3. In the **Model Configuration** section, click icon corresponding to the tabs to delete models, or use **Edit Models** to enable or disable.
4. Click **Save**.

Port Overrides

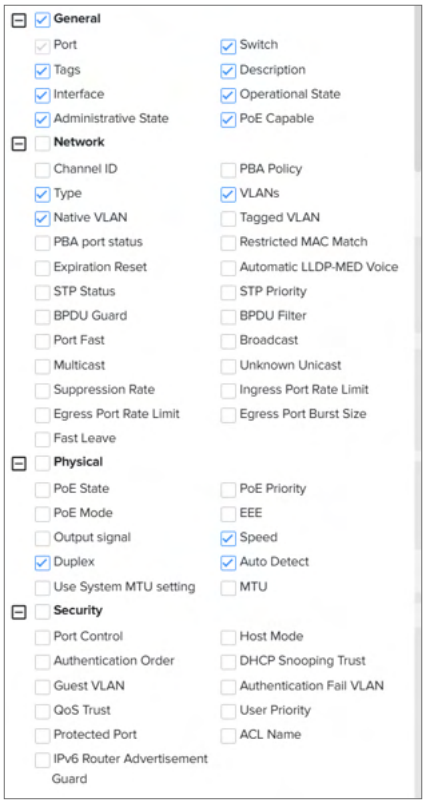
The **Ports** > **Port Overrides** section supports creating port channels, editing port configuration, and configuring port parameters.



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 **Save** 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 the **Port Overrides** section.



Click the edit (✎) icon or Port device in the list to edit the Ports Configuration details.

Note

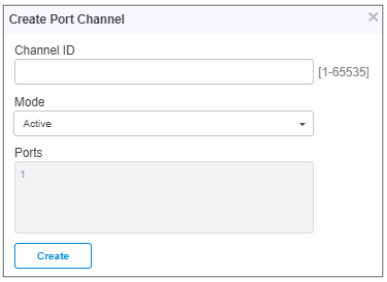
After modifying the port or channel details, you can apply the configuration to the device by clicking **Save** at the bottom of the **Switch Ports** page.

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 dropdown.
5. Click **Create**.

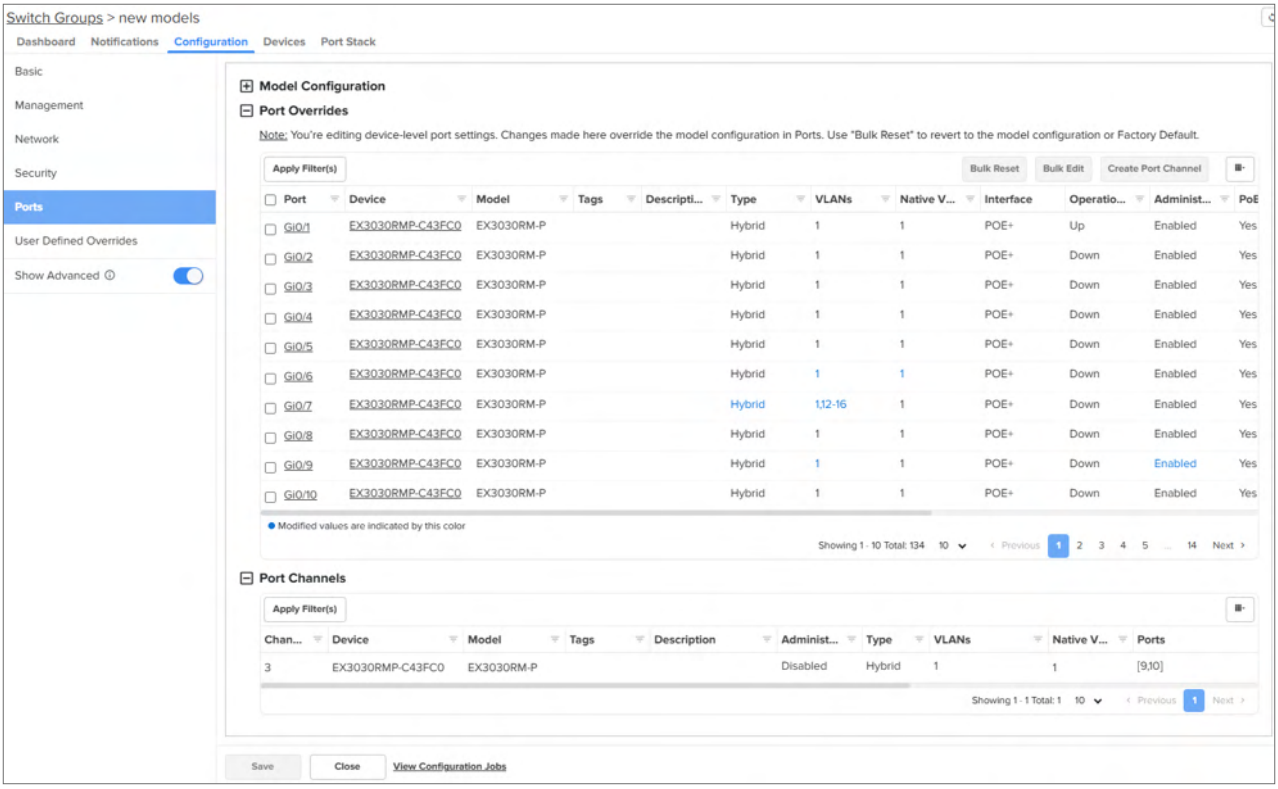
Reset

Upon Reset or Bulk Reset, the selected ports are restored to the ports configuration defined in the **Model Configuration** section, if available; otherwise, they are reset to the factory default configuration.

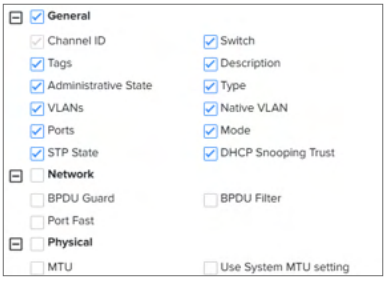
Port Channels

The **Port Channels** section displays the following fields by default:

- Channel ID, Device, Model , Tags, Description, VLANs, Native VLAN, Type, Administrative State, Mode, Ports, STP State, and STP Priority.



lick ▾ to include additional fields in **Port Channel** Detail view.



Edit Ports

Note

- Model-specific settings from templates are automatically ignored if applied to incompatible devices.
- Ports that have been modified are highlighted in blue, indicating they contain overrides different from the configuration present in the **Model Configuration**

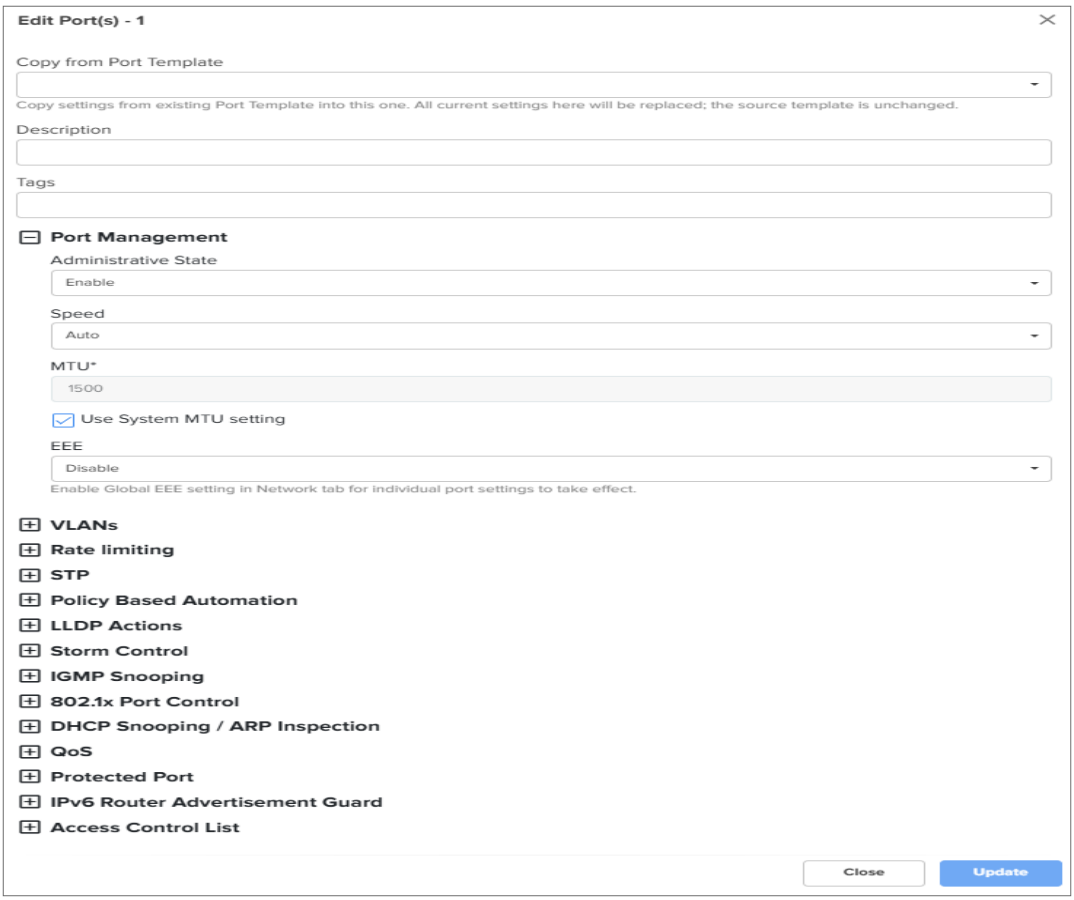
section.

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 83.
5. Click **Update**.

Clone Ports

To clone the port templates, perform the following steps:

1. In the **Model Configuration** section, click the save as port template ( ) icon corresponding to the port configuration you want to clone.

   Save as Port Template window is displayed.



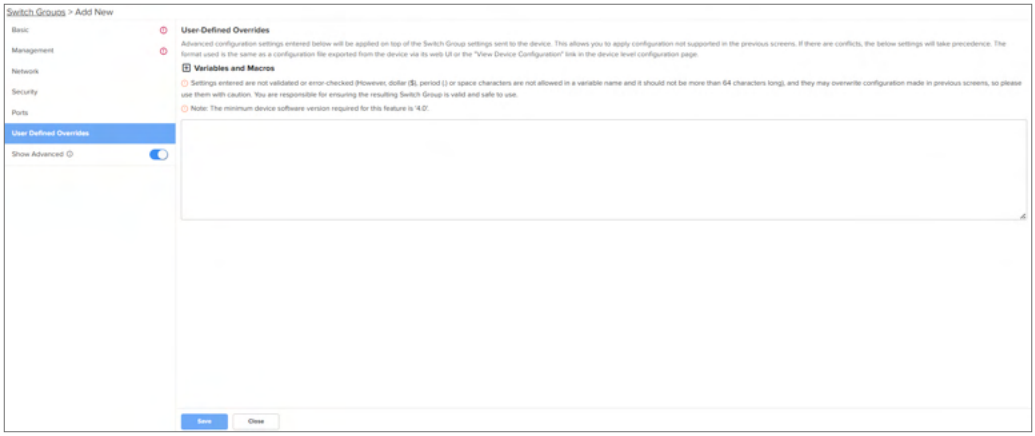
2. Enter the **Port Template Name**.
3. Enter the **Description**.
4. Click **Save**.

User-Defined Overrides

Note

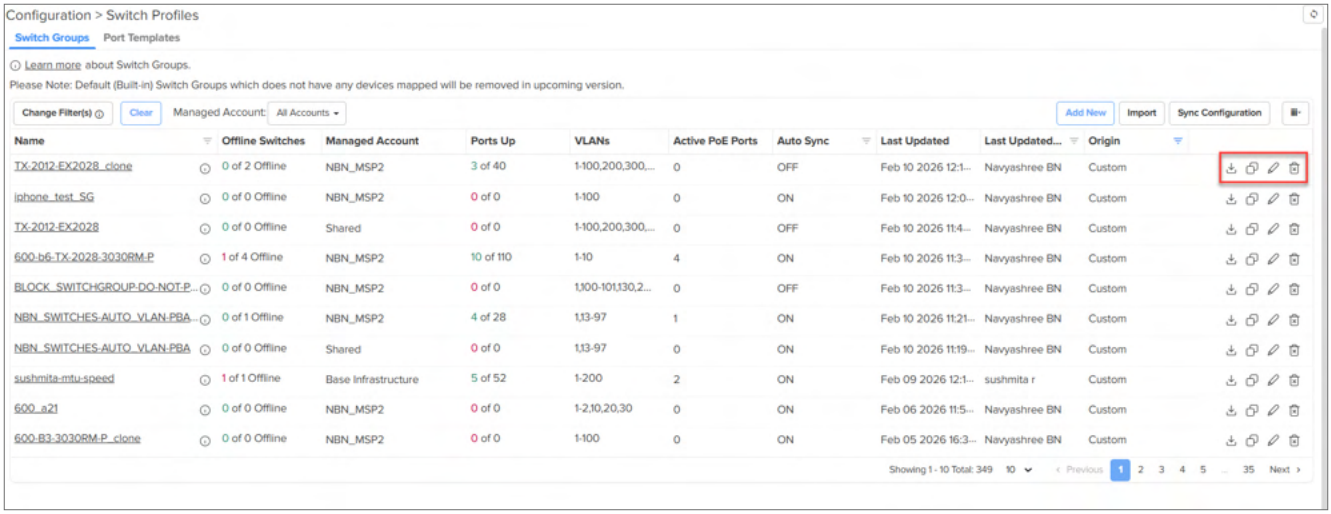
The minimum device software version supported for this feature is 4.0.

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.



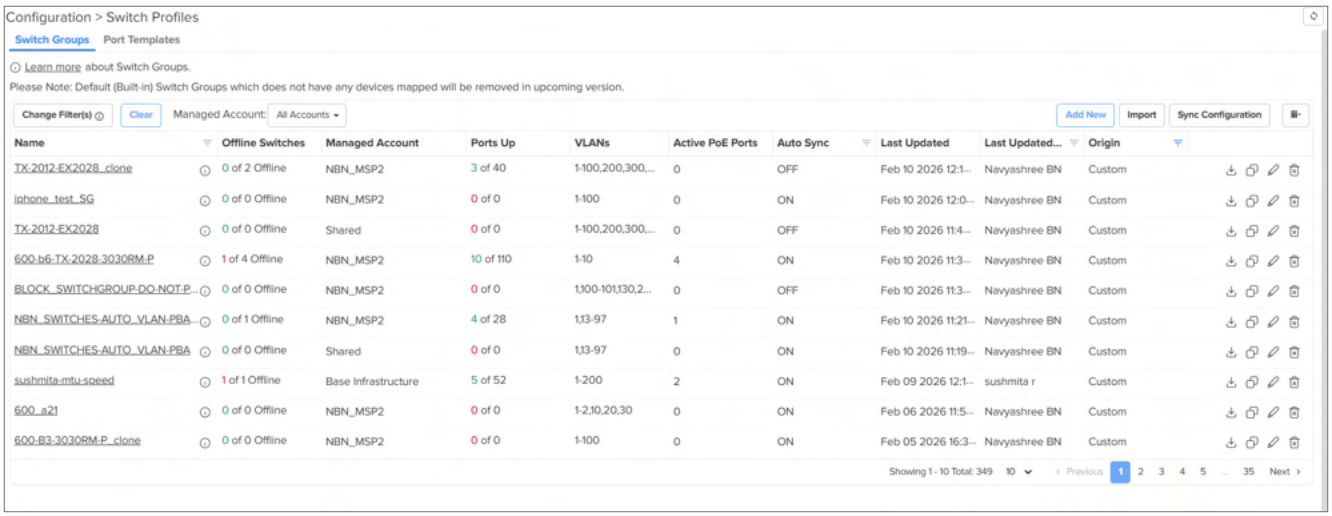
4. Click **Import.**

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.



Retry Configure

When the user tries to apply any Switch Group on the device, and if the job was skipped for the device as it was offline, the reason for the skip will be displayed as " Device was offline", in the Jobs page. In this case, when the device comes Up and connects to cnMaestro, then cnMaestro will create an Auto-sync job for that device and push the Switch Group. (It will not apply to the switch group if the "Auto-Sync" was disabled in the switch group).

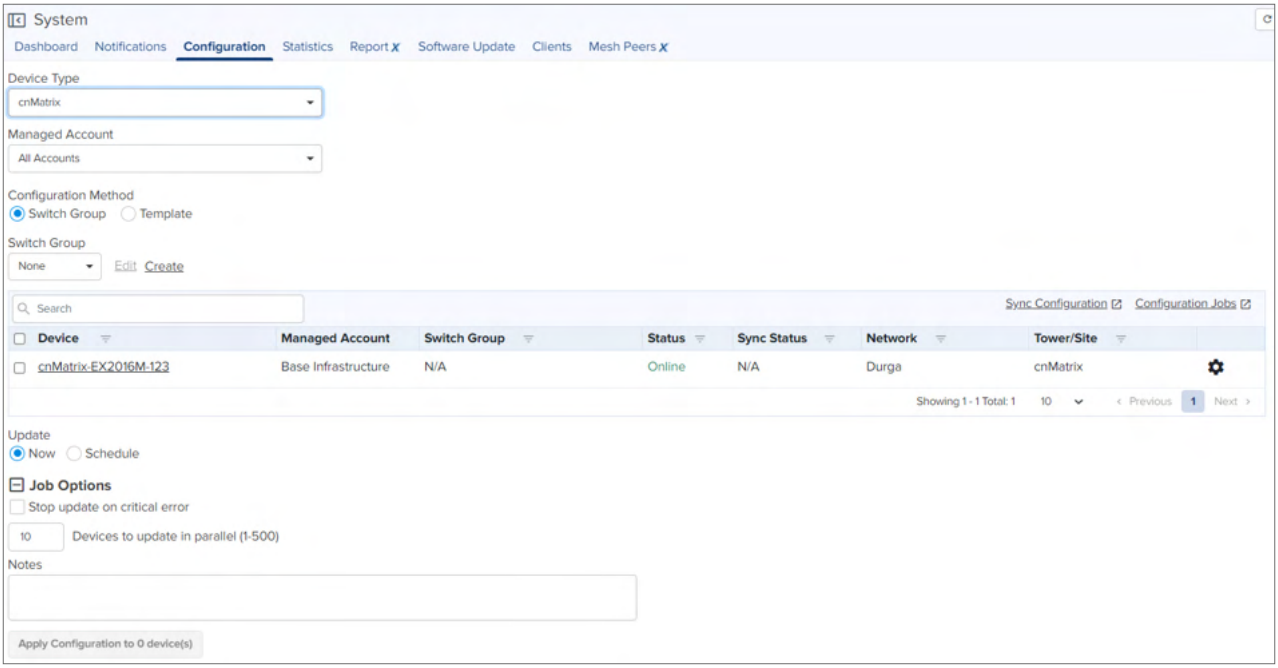
Note

The config update (auto-sync) will happen only when the **Auto-Sync** option was enabled in the Switch Groups page. If the device was skipped/failed because of any other reason other than the "Device was offline", then the device will not be updated.

Create a Configuration Job

Configuration job can be created from **System/Network/Tower/Site/Device Configuration** page. Select a device type and a set of devices along with switch groups to which they will be mapped. This can be done in three steps:

1. Select the Switch Group that needs to be pushed from 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.

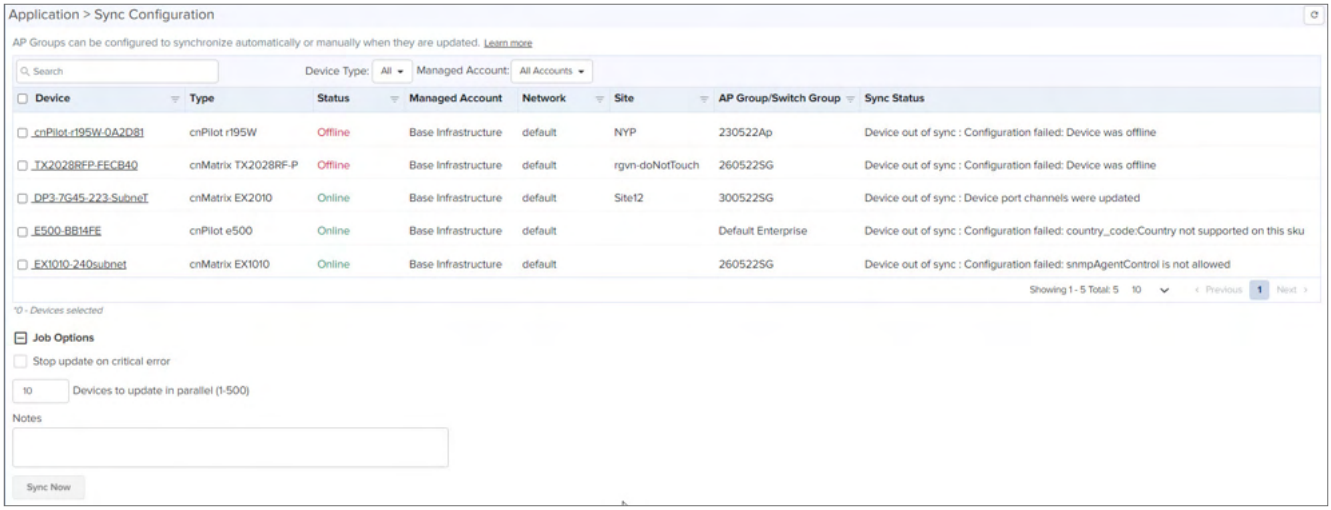
Switches by default synchronize automatically (so any change of switch group, followed by a Save, will immediately push configuration to the devices without manual intervention).

Manual Synchronization

Manual configuration synchronization allows the user to synchronize any devices with a single action rather than updating each device separately. The page is located at **Administration > Sync Configuration**.

To sync the device manually, navigate to **Administration** > **Sync Configuration**. This location can also be accessed by clicking the **Sync** button on the **Switch Groups** page.

Figure 381 *Sync Configuration page*



Sync Configuration has the following fields:

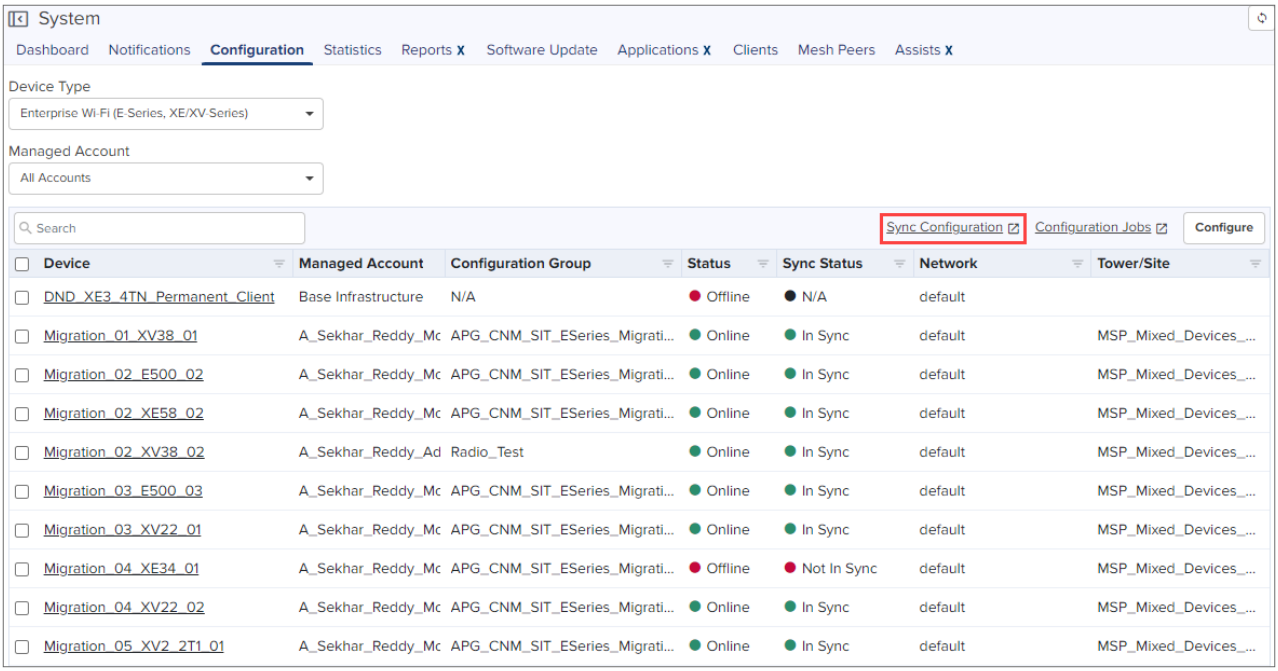
- Device (Hostname)
- Type
- Status (Online/Offline)
- Network (Network in which device is present)
- Site (Site under which device is present)
- Configuration Group (AP Group/Switch Group to which device is mapped)
- Sync Status (Sync status will tell whether job is completed or failed)

Table 82 *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.

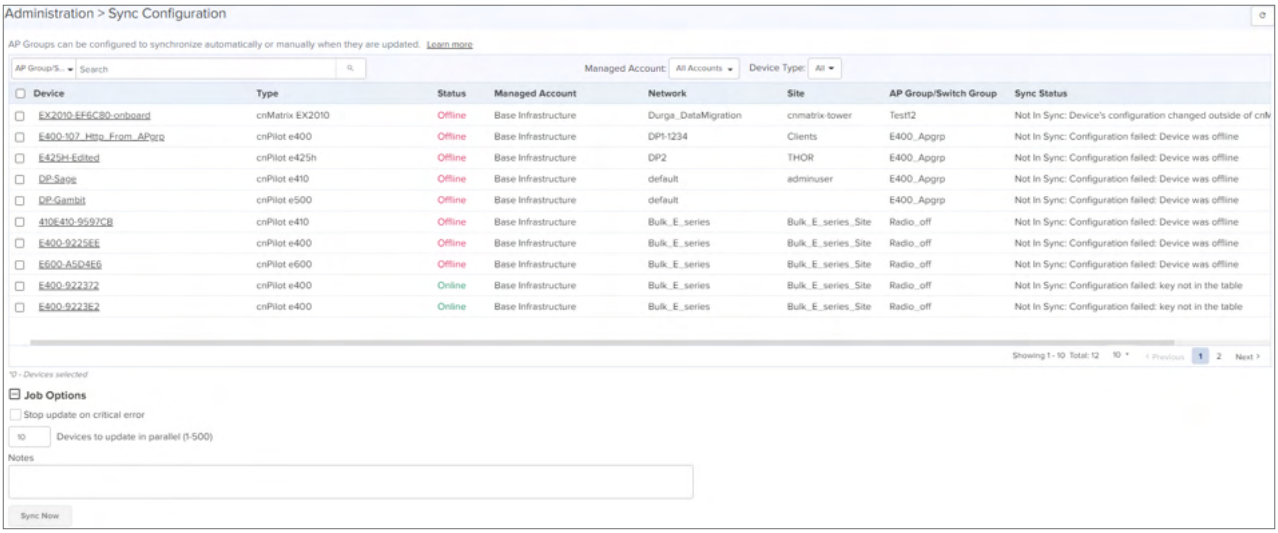
Perform the following steps to Sync Configuration:

1. Navigate to **Monitor and Manage** > **System** > **Configuration** or the **Jobs** tab.
2. Select the devices to synchronize and click **Sync Configuration.**

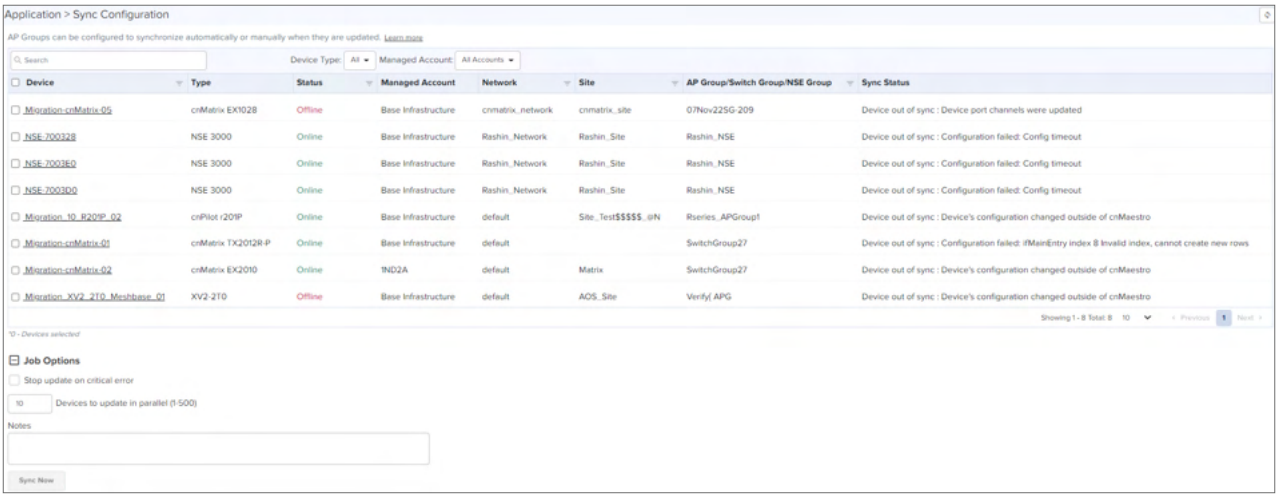


3. The **Administration** > **Sync Configuration** page is displayed.

   Select the devices to synchronize.



4. Click **Sync Now**.



User can also synchronize devices from **Administration** > **Sync Configuration**.

Note

Sync configuration can only be used if a Switch Group is already mapped to the device.

Policy Based Automation (PBA)

Cambium Networks PBA feature fully automates commonly performed operations, improving network security while eliminating potential configuration errors. It allows the user to automatically configure switch port settings based on the device connected to the port. These dynamic PBA settings remain in use for the duration of the device connection and are automatically cleared when the device disconnects from the switch.

PBA configuration is common to all switches within a Switch Group.

Note

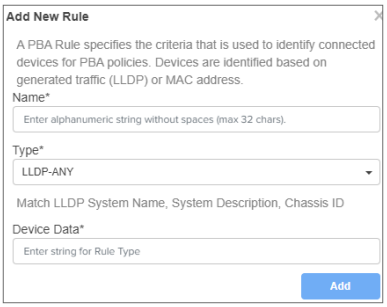
Dynamic PBA updates are indicated by asterisk * on the Switch Dashboard and on the **Switch Groups** > **Ports** > **Port Overrides** section.

Configure the PBA as follows:

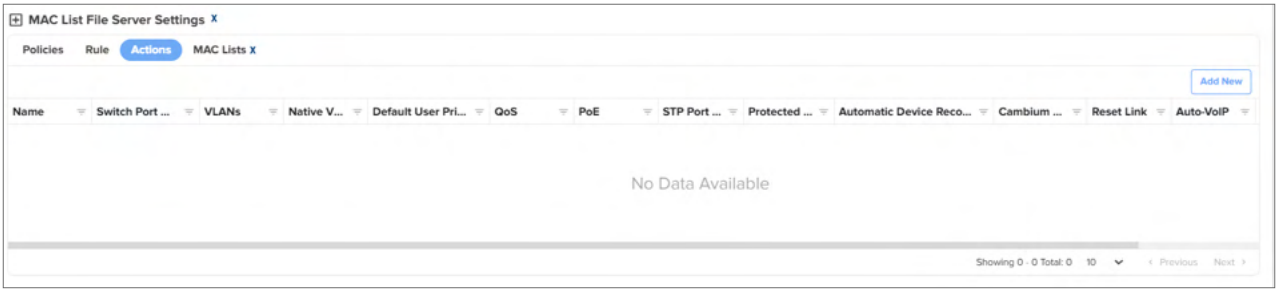
1. Navigate to **Configuration > Switch Groups > Network > Policy Based Automation.**
2. Navigate to **Rules** tab**.**



3. Click **Add New** to set the rules.



4. Click **Add**.
5. Navigate to **Actions** tab.



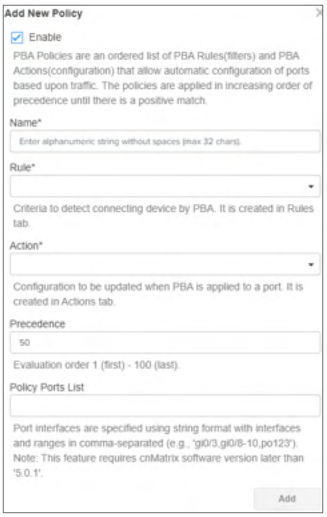
6. Click **Add New** to set the actions.



7. Click **Add**.
8. Navigate to **Policies.**

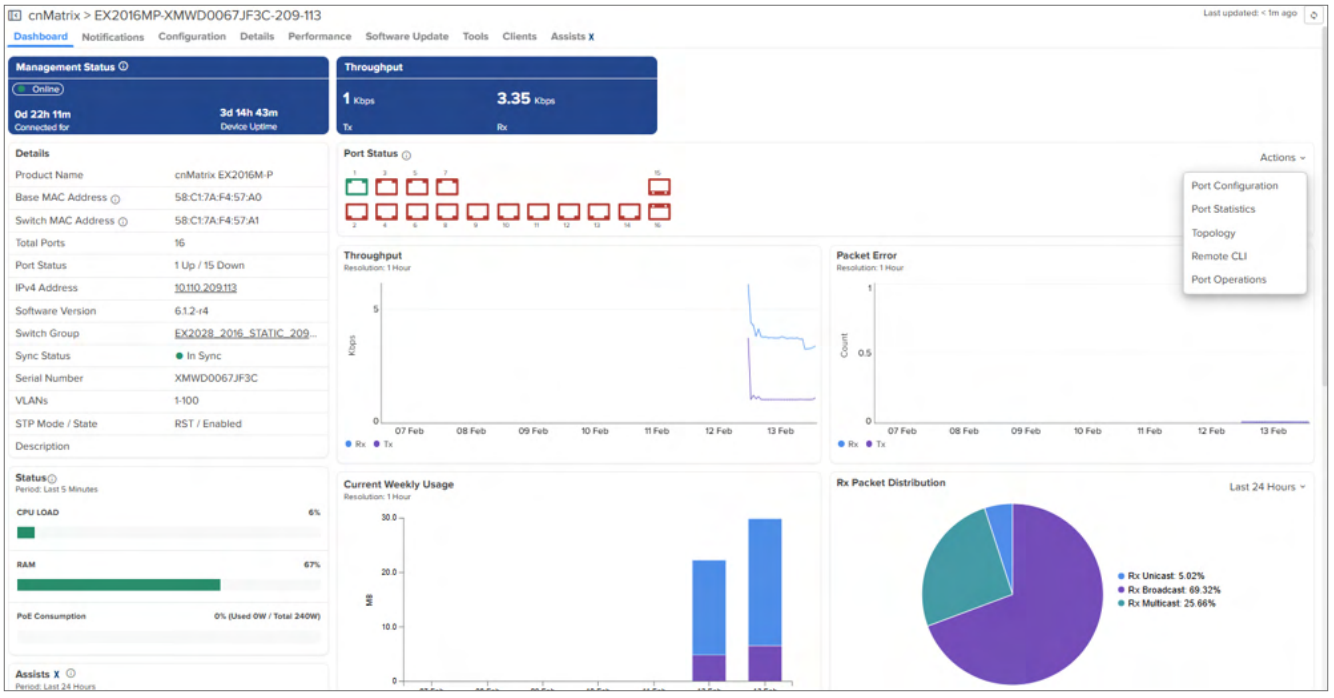


9. Click **Add New** to set the policies.



In the cnMatrix dashboard, users can navigate to the following pages using the **Action** dropdown menu in Port Status.

- Port Configuration
- Port Statistics
- Topology
- Remote CLI
- Port Operations



Devices

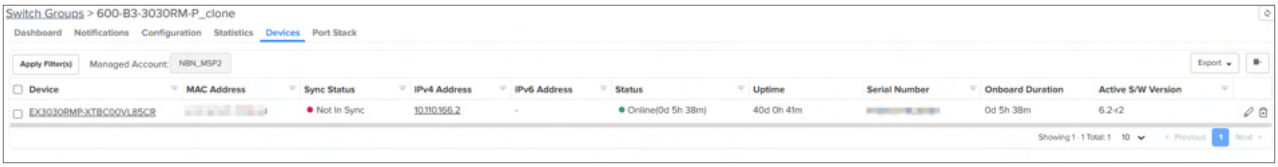
The Devices page is accessed by selecting the **Switch Groups > Devices** tab lists all of the physical switches assigned to the Switch Group. The Switch Dashboard and switch override configuration settings are accessible through this page.

Note

For configuration, a switch must belong to a Switch Group.

Configure the Switch Group as follows:

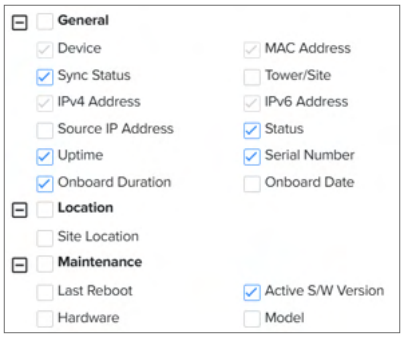
- Navigate to **Switch Groups** > select the switch from the list, and click **Devices** page to view and edit the onboarded switches.



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.

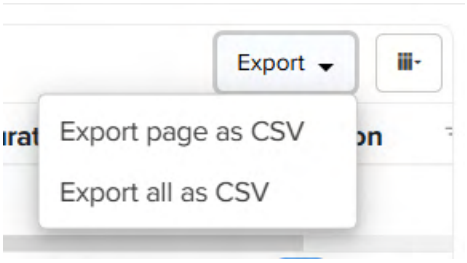
User can click on top bar to include additional fields in Devices Detail view.



Export Devices

Perform the following steps to export the Device table:

1. Click **Export**. A dialogue box appears.

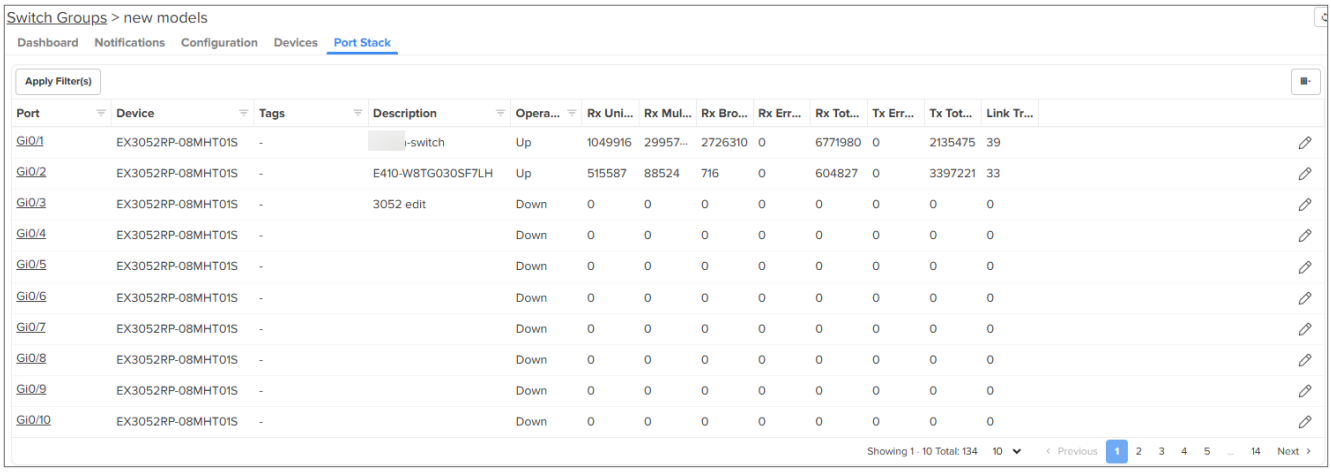


2. Select **Export page as CSV/all as CSV** and export the file.

Ports Stack

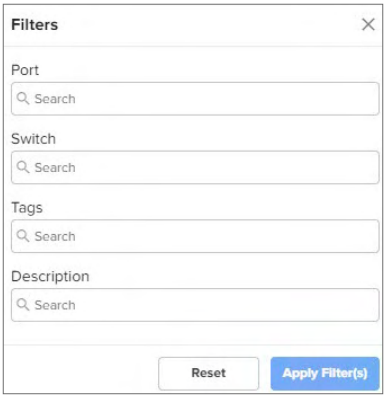
The **Ports Stack** table displays the latest data and statistics of each port stack. Port stack statistics match the Client statistics and generate the Client View.

To view the Switch Ports statistics navigate to **Configuration** > **Switch Groups** > **Port Stack**.



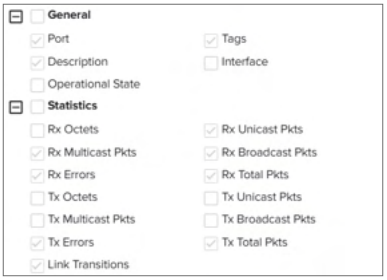
To apply filters, follow the steps below:

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)**.

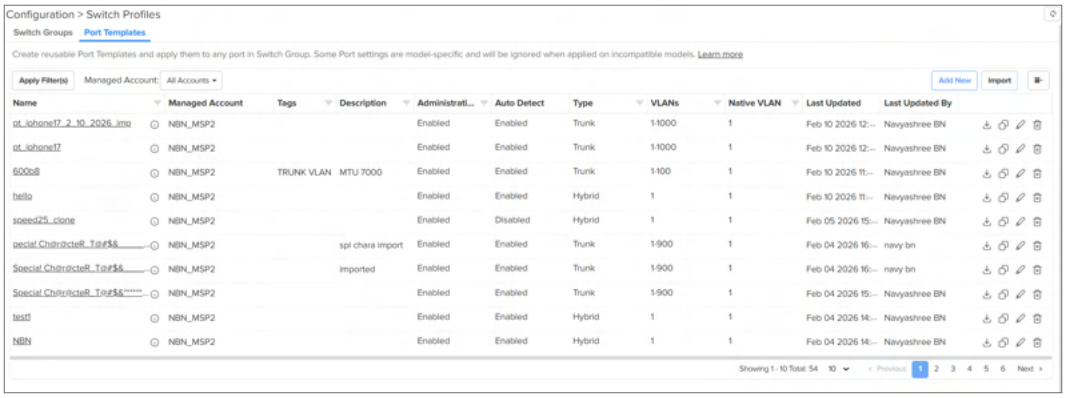
   User can click on top bar to include additional fields in **Statistics** Detail view.



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.

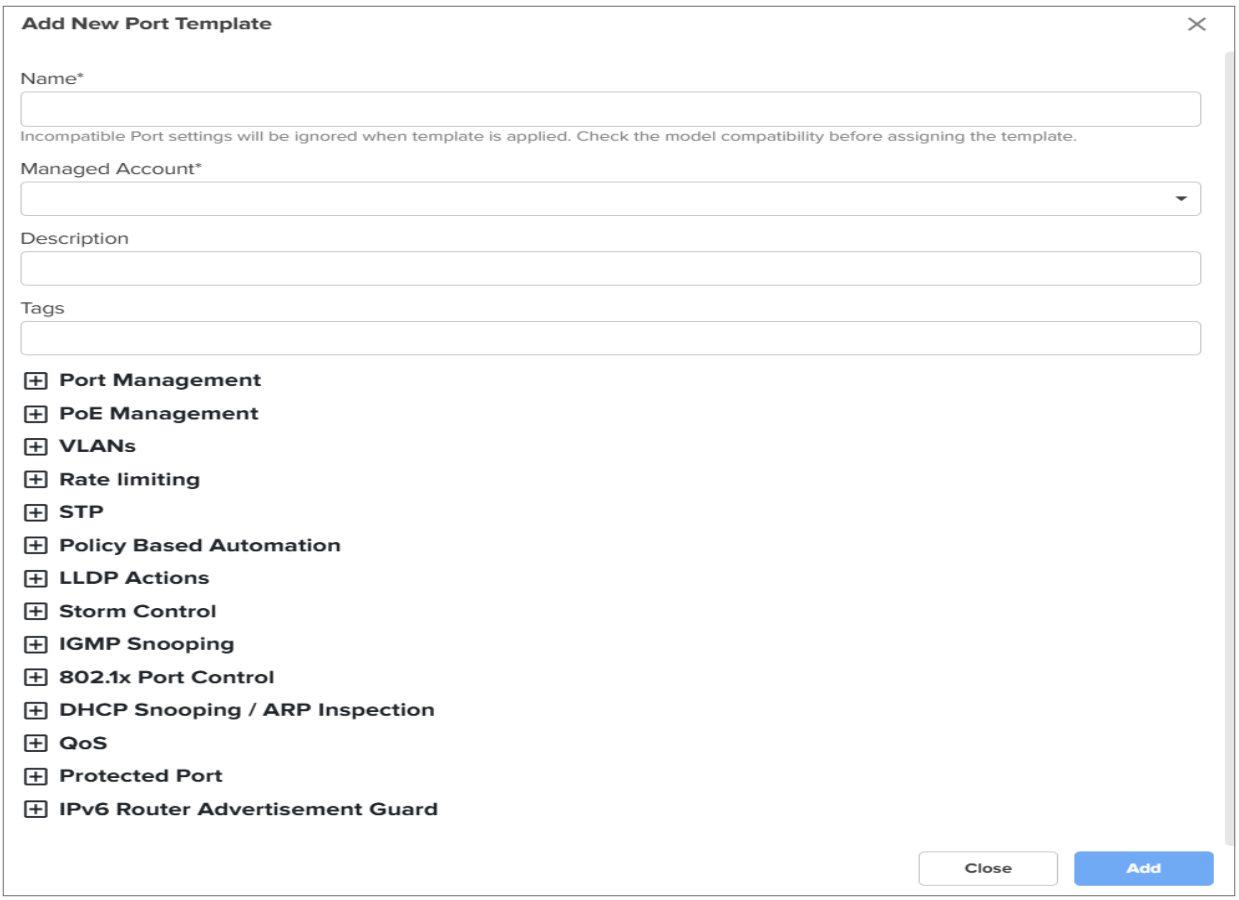
This can be used on ports section of switch group as well as **Ports Stack** tab



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 83.

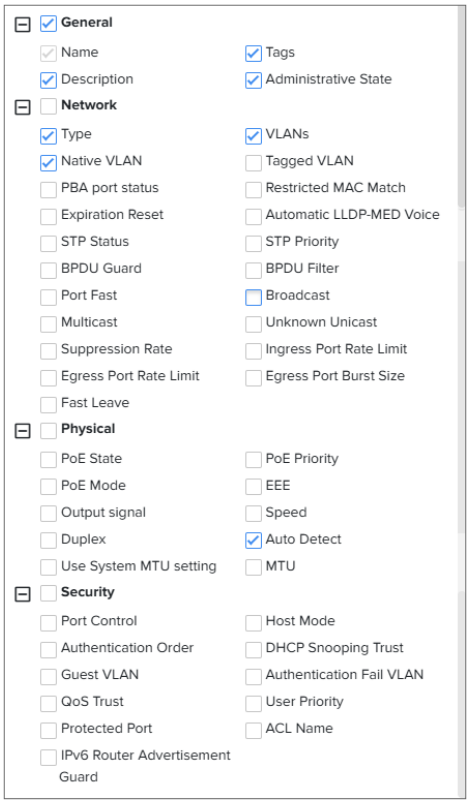
   Table 83 *Add New Port Template parameters*

Parameter	Description
Name	Specifies a unique name for the Port Template.

Parameter	Description
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, 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.

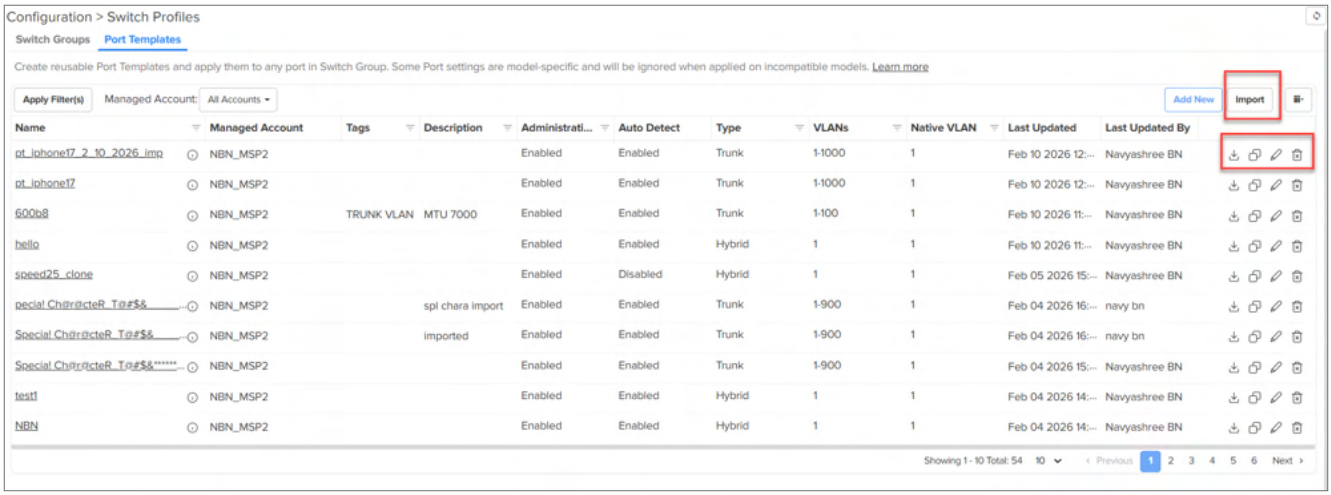
4. Click **Add**.

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.

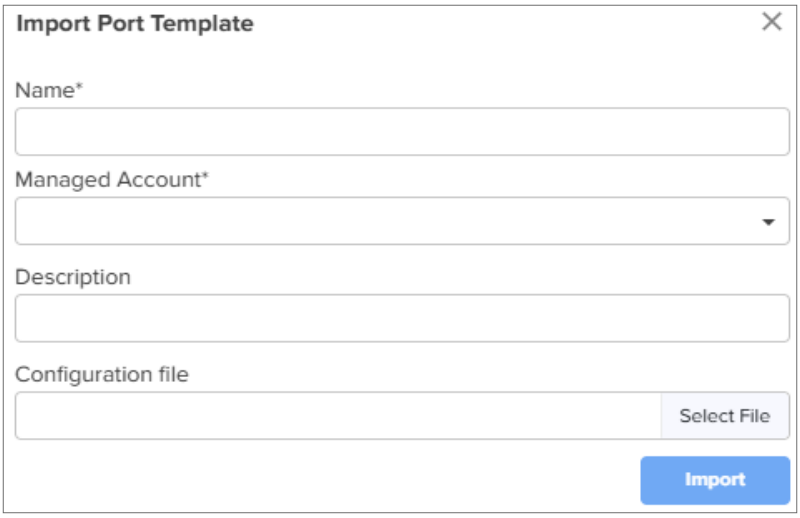


Export Port Templates

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.

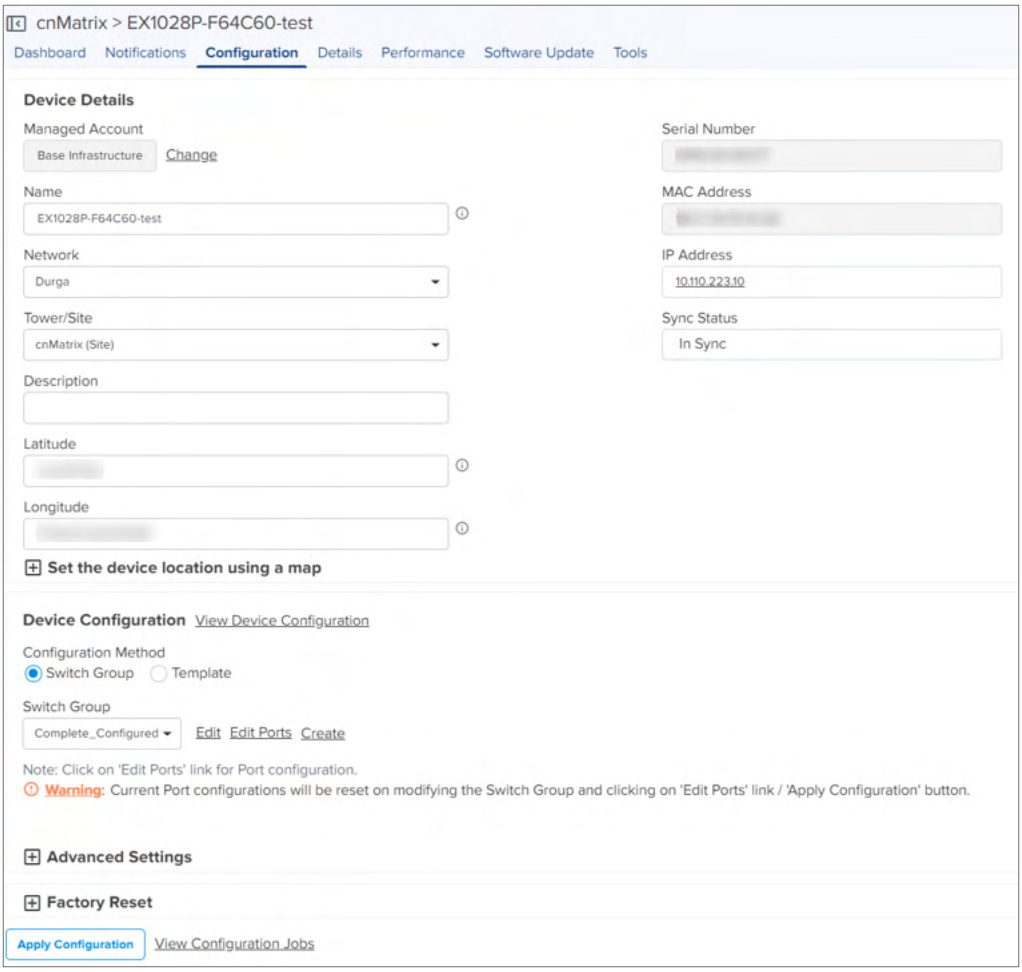
Delete Port Templates

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:

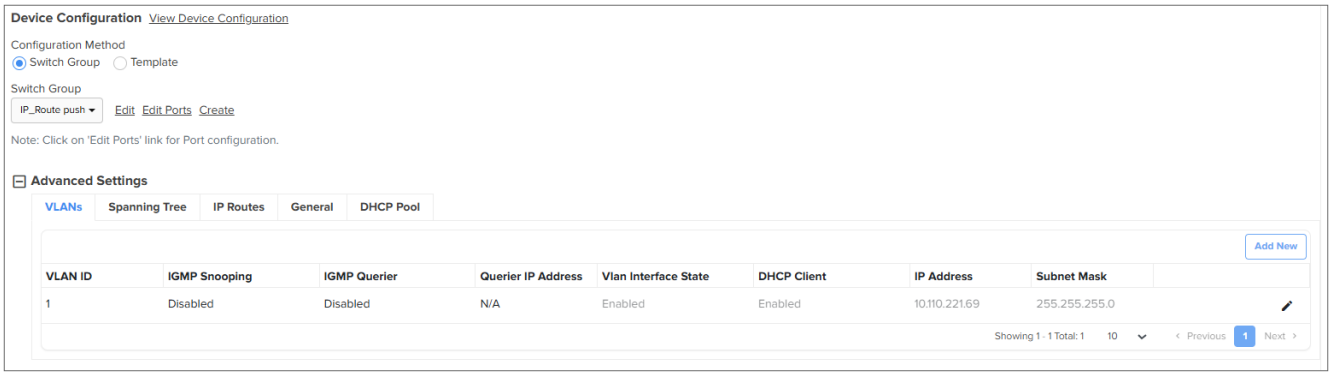
- Device Configuration
- Advanced Settings
- Factory Reset

Device Configuration

Device Configuration allows you to configure the Configuration Method as Switch Group/Template.

Switch Group Configuration Method

Enable the Switch Group and select a device from the Switch Group dropdown.



To Edit or Create a Switch Group. Refer to the Switch Groups Configuration.

Advanced Settings

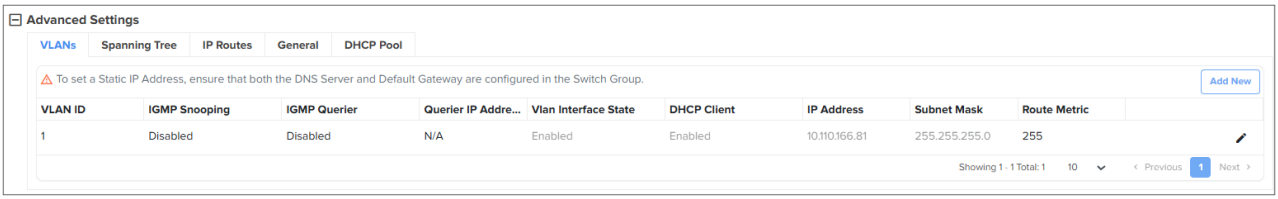
Navigate to the Advanced Settings and configure the following parameters:

- VLANs
- Spanning Tree
- IP Routes
- General
- DHCP Pool

VLANs

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.

- Click **Advanced Settings** in **Configuration** page and navigate to **VLAN Interface** tab.



- If required, click the edit (✎) icon or **Add New**.
- Enter or edit the required details and click **Add**.



Spanning Tree

Enabling the spanning tree allows the user to configure Spanning Tree to override the Switch Group settings.

If required, perform the following to configuration to override:

- Click **Advanced Settings** in **Configuration** page.
- Click **Enable Spanning Tree Overrides.**
- Select the **Spanning Tree** parameters.



Note

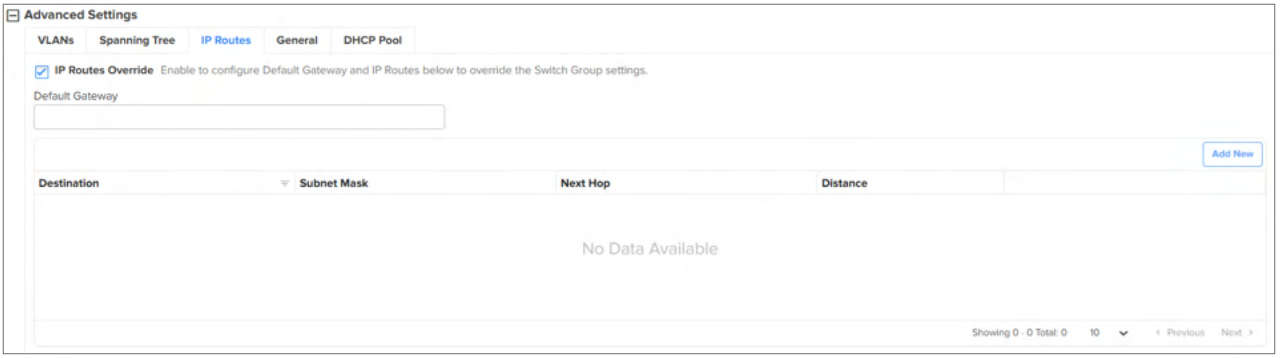
If Spanning Tree is disabled the overrides feature will be disabled on the Switch configuration.

IP Routes

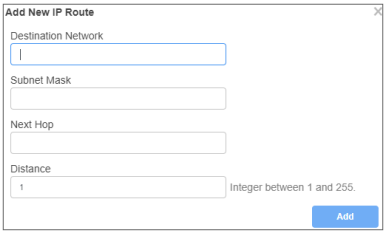
Enabling the IP Routes override allows the user to configure the Default Gateway and IP Routes to override the Switch Group.

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

General tabs allow user to configure PBA Localization settings to override the Switch Group settings.

If required, perform the following to configuration to Override:

- Click **Advanced Settings** in **Configuration** page and navigate to **General** tab.



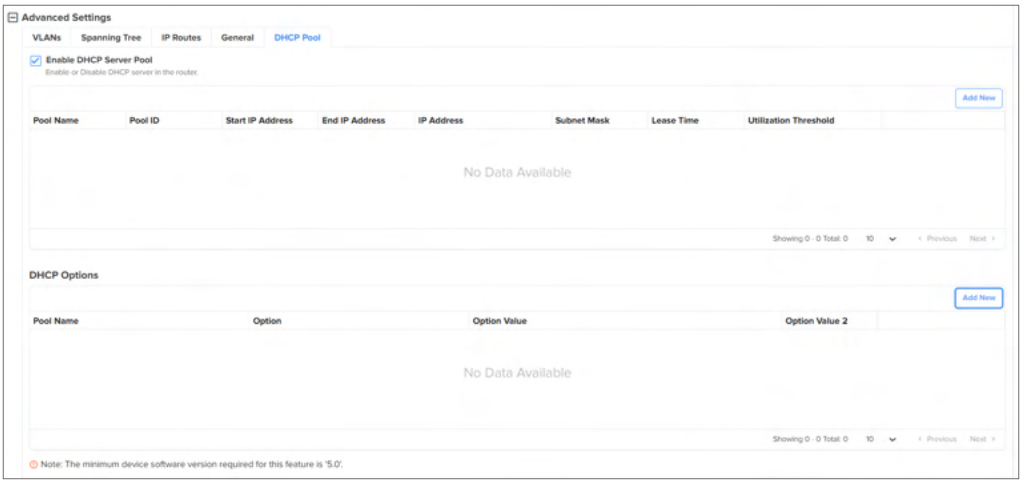
- Click **Enable PBA localization overrides**.
- Select **Use Site Name** or **Custom**.
- Enter **PBA Uplink Ports**.

DHCP Pool

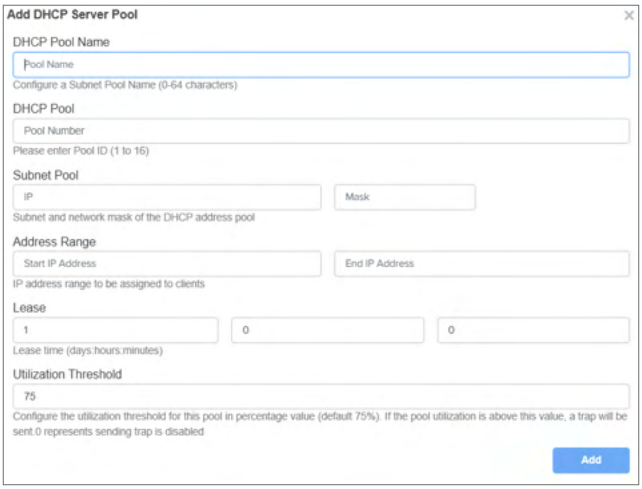
DHCP Pool tabs allow user to enable or disable DHCP server in the router.

If required, perform the following to configuration the DHCP pool:

- Click **Advanced Settings** in **Configuration** page and navigate to **DHCP Pool** tab.



- Click **Enable DHCP Server Pool**.
- If required, click **Add New** to add the new DHCP Server Pool.



- Enter the required parameters and click Add.

- If required, click **Add New** to add the new DHCP Option.

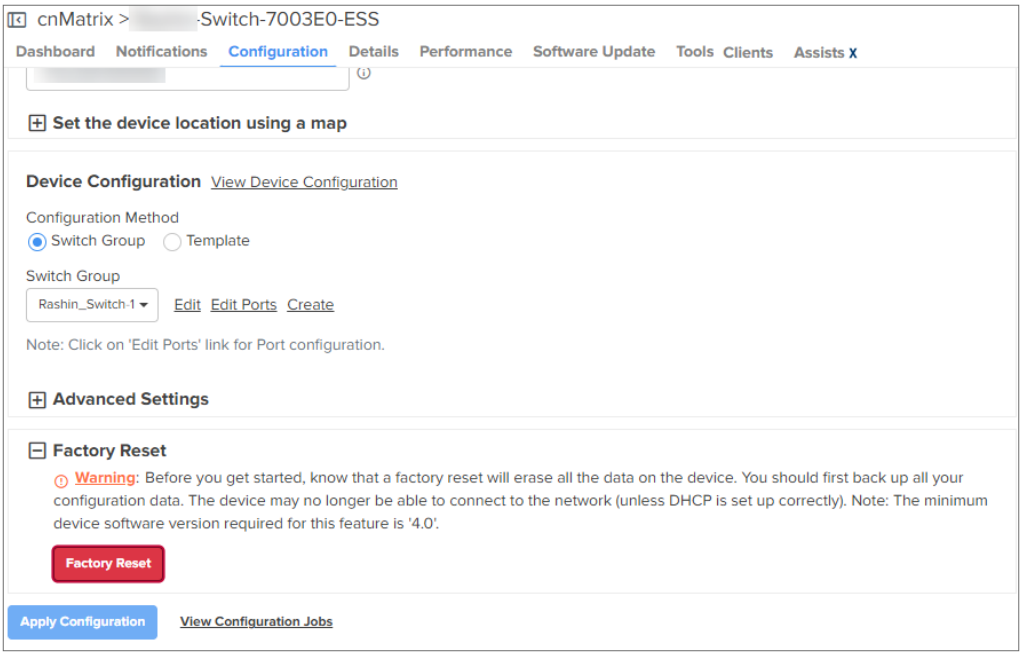


- Enter the required parameters and click Add.

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**.

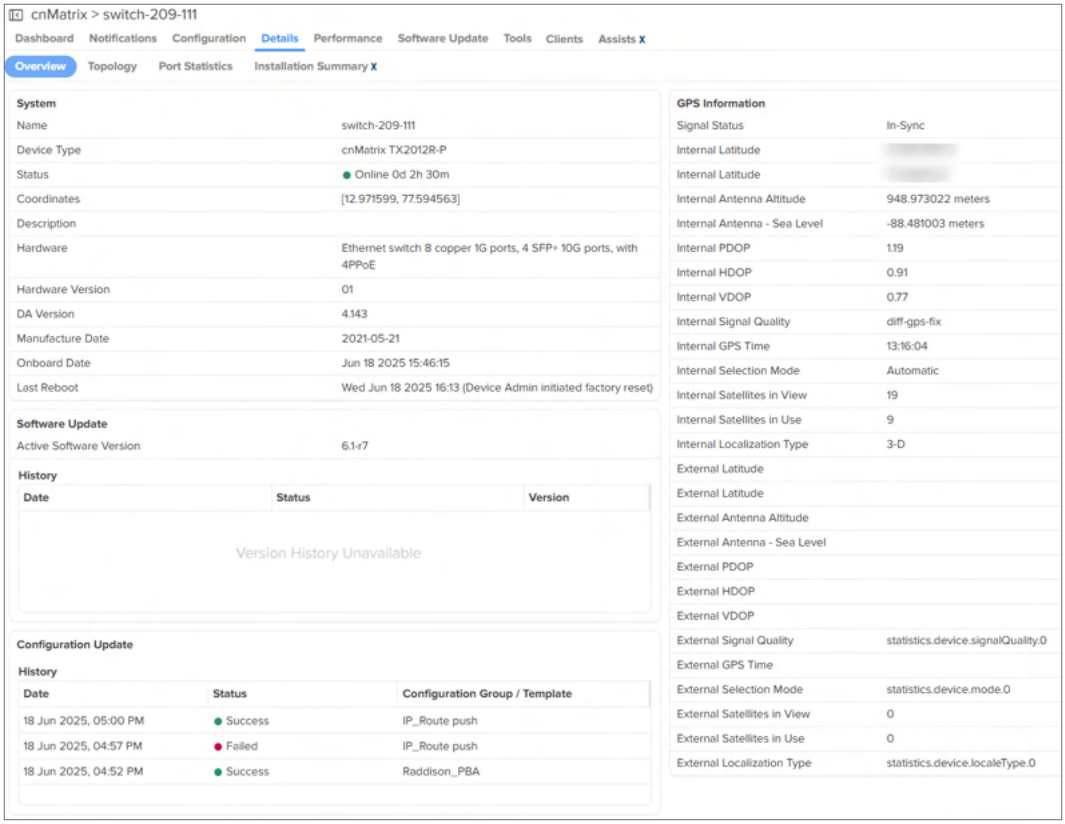


3. In the pop-up window that appears, click **Yes, Factory reset**.



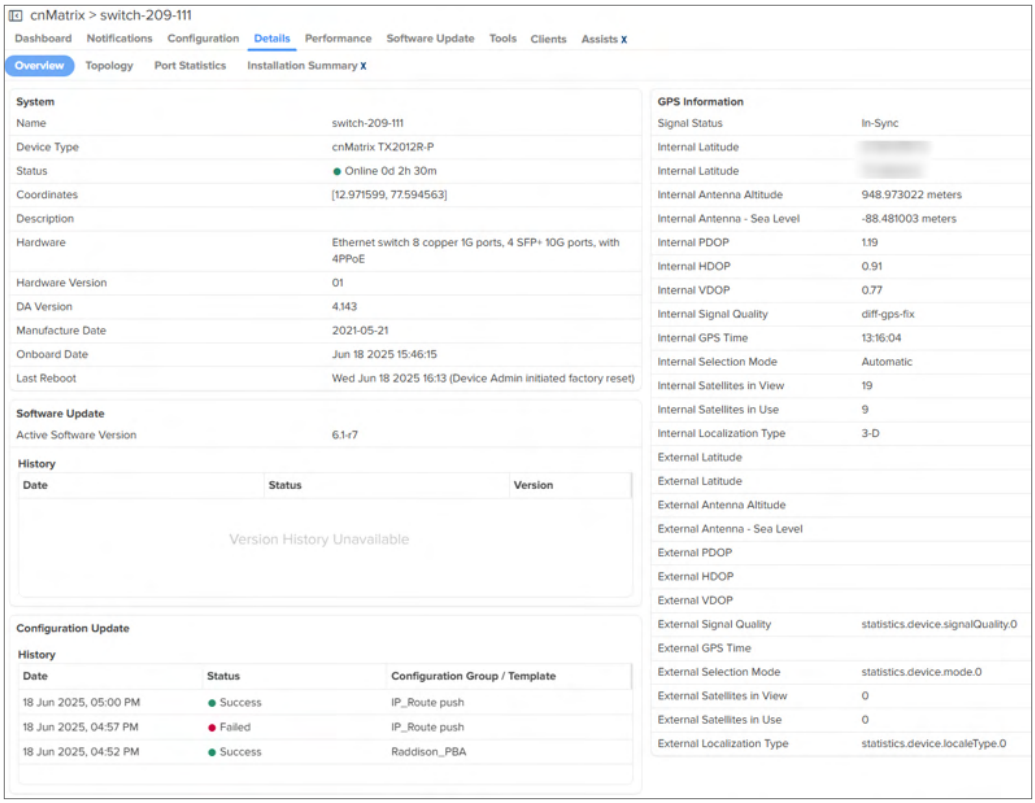
Device Details

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.



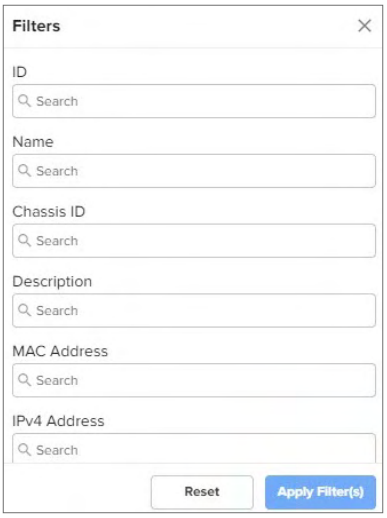
Topology

To view the details of the Topology page, navigate to the **Details** > **Topology** tab.



To apply filters, follow the steps below:

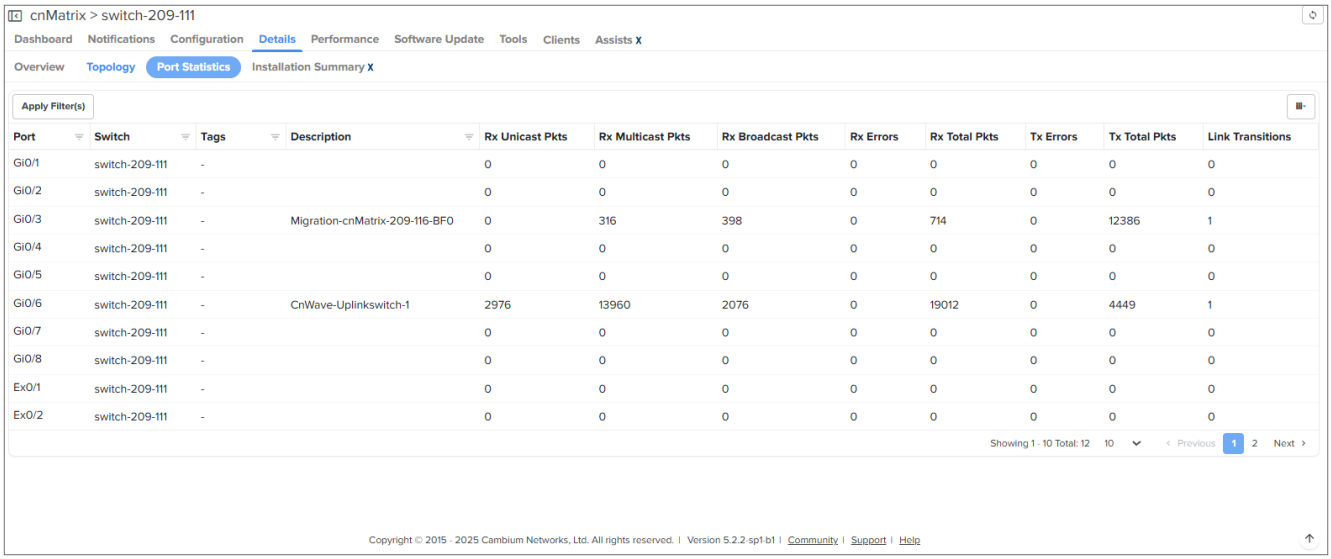
1. Click on the **Apply Filter(s)** tab.
2. A new window titled **Filters** appears.



3. Enter information in any field based on your filtering needs.
4. Click on **Apply Filter(s)**.

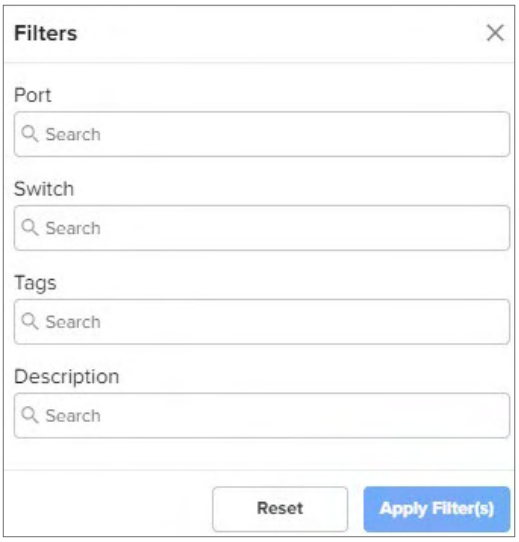
Port Statistics

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.



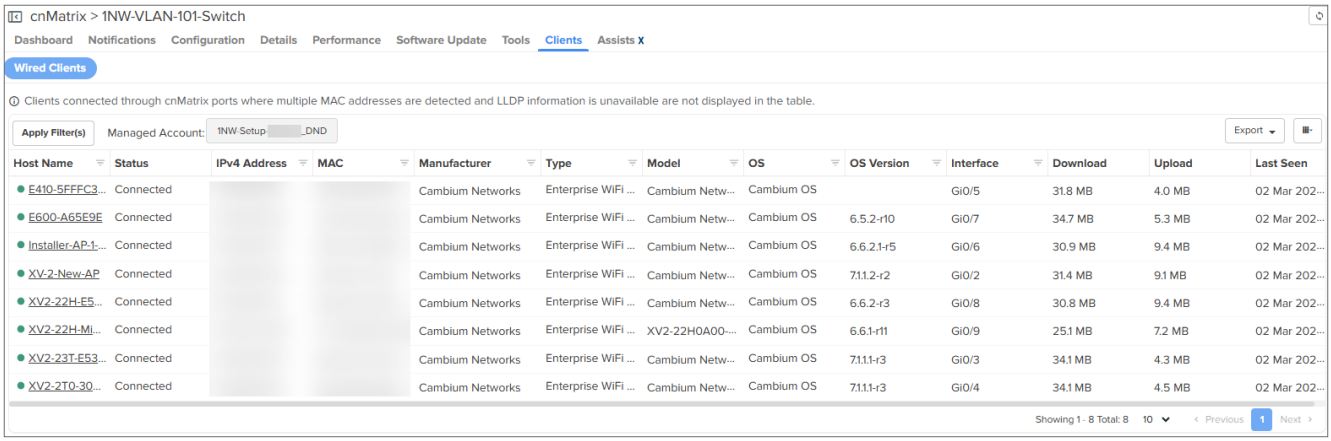
3. Enter information in any field based on your filtering needs.
4. Click on **Apply Filter(s)**.

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.

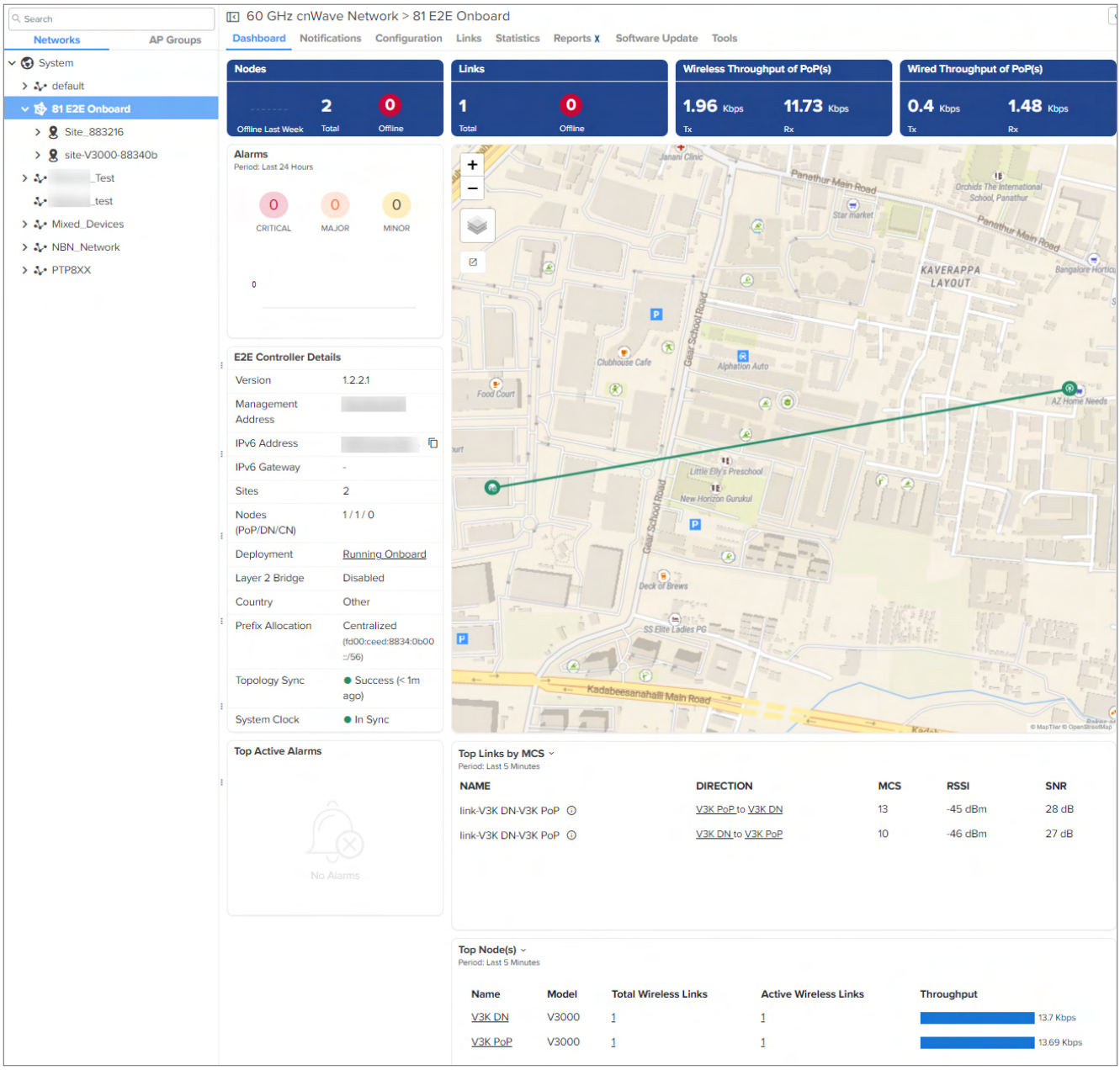
Managing E2E Network

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, Wireless Throughput of PoP(s), Wired Throughput of PoP(s), Alarms, E2E Controller Details, Top Active Alarms, Map, Top Links by MCS, Top Links by RSSI, Top Links by SNR, Top Node(s) Top PoP(s), Top DN(s),** and **Top CN(s).**



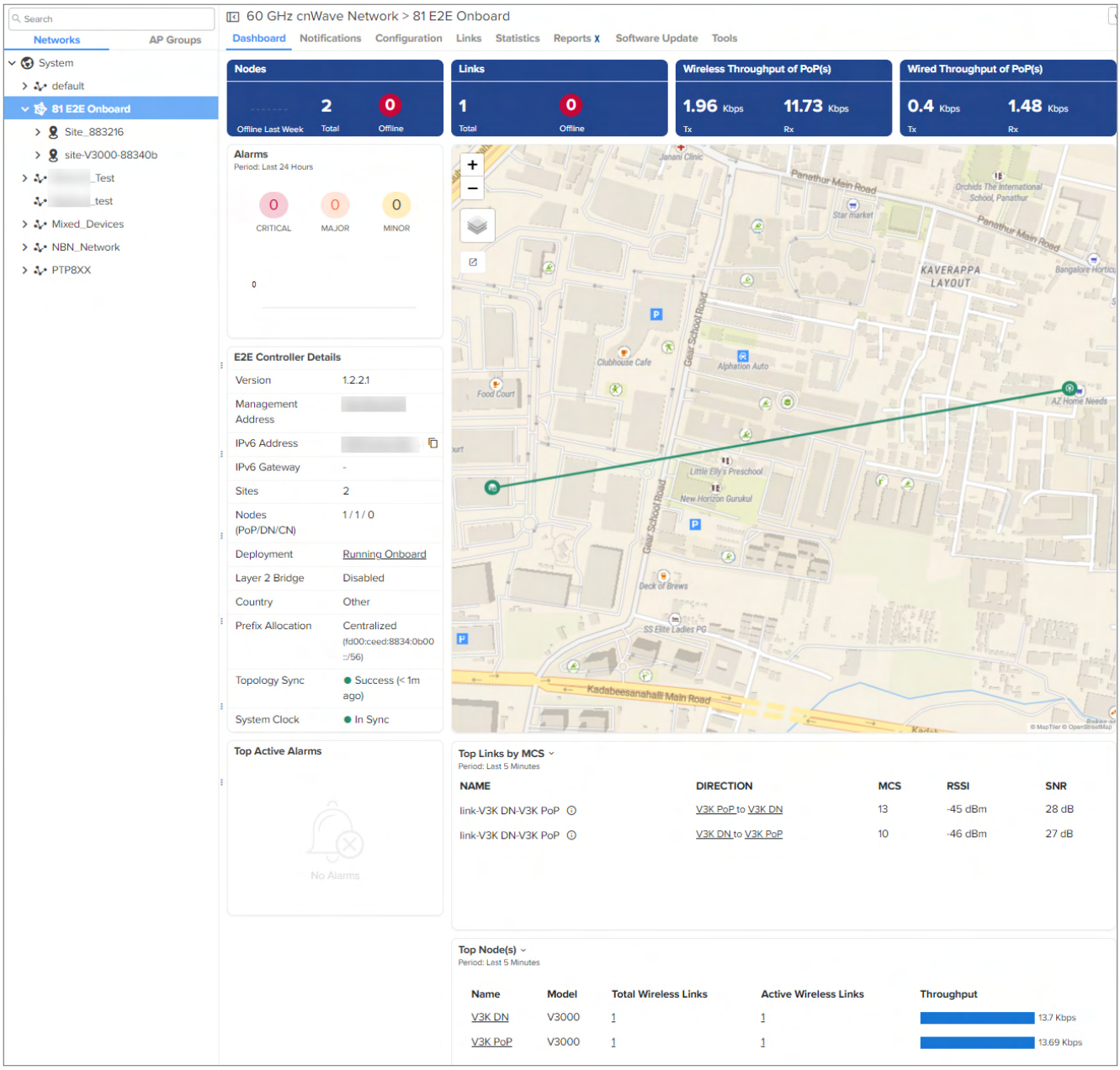
Note

Backup CN links are not shown as Offline links in links widget.

Auto Manage IPv6 Routes (E2E Controller↔ Node)

The **External E2E Network**. dashboard page displays the **Auto Manage IPv6 Routes (E2E Controller ↔ Node)** tab, if you enable **Auto Manage Routes** in the **Tools > Settings** page of **External E2E Network**.

This feature automates IPv6 routes for DNs and CNs based on status of the topology and PoP nodes. It is applicable only if PoP nodes and E2E Controller are in the same Network or containing the same prefix length.



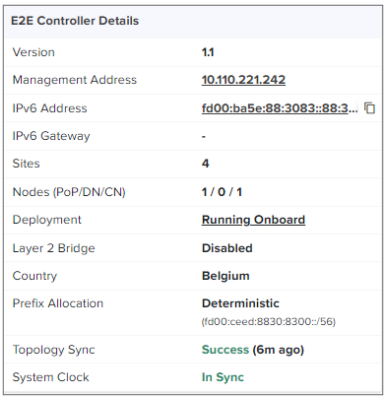
Note

Auto Manage IPv6 Routes is not applicable for Onboard E2E Controller.

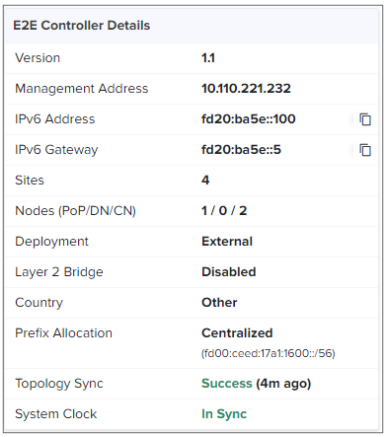
E2E Controller Details

E2E Controller Details displays the details such as **Version**, **Management Address, IPv6 Address, IPv6 Gateway, Sites, Nodes, (PoP/DN/CN), Deployment, Layer 2 Bridge, Country, Prefix Allocation, Topology Sync,** and **System Clock**

- If Onboard E2E controller is enabled in device and managed by cnMaestro, it displays deployment as **Running Onboard.**

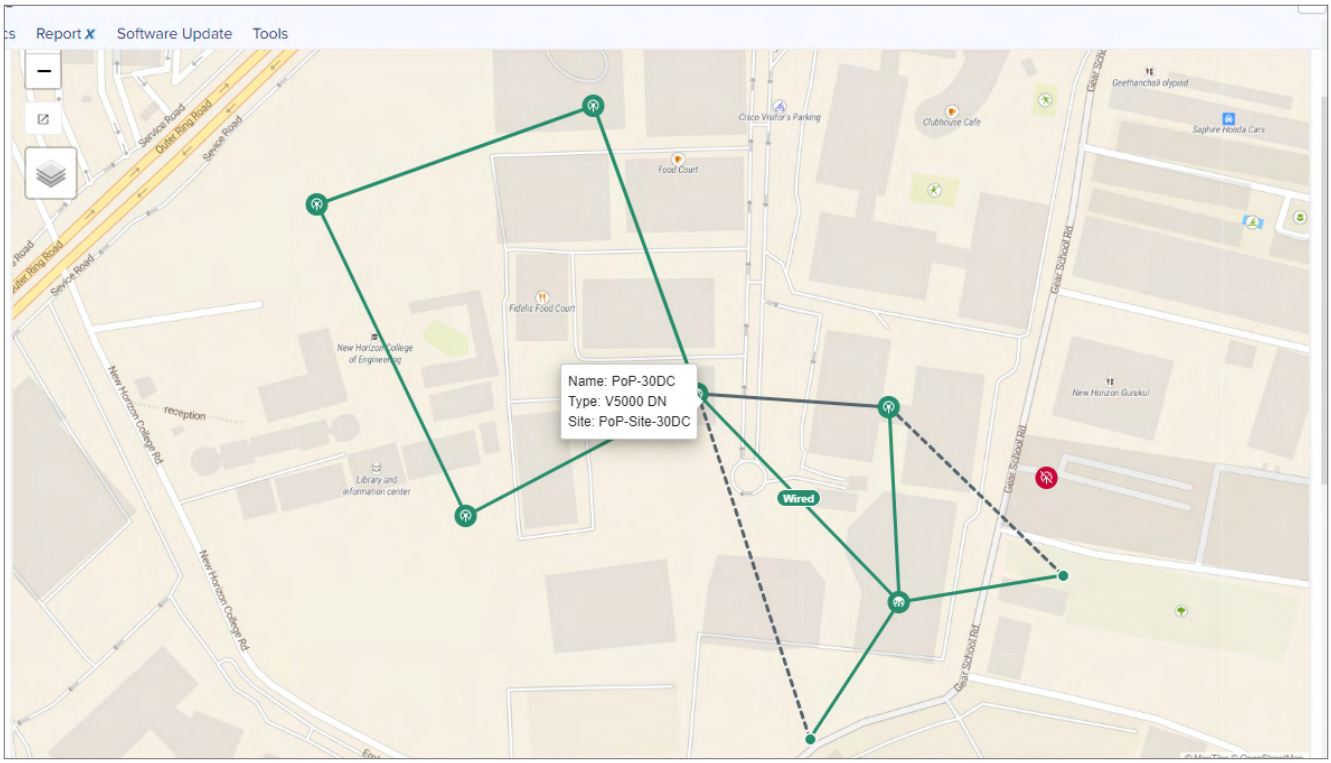


- If External E2E controller is managed by cnMaestro, it displays deployment as **External.**

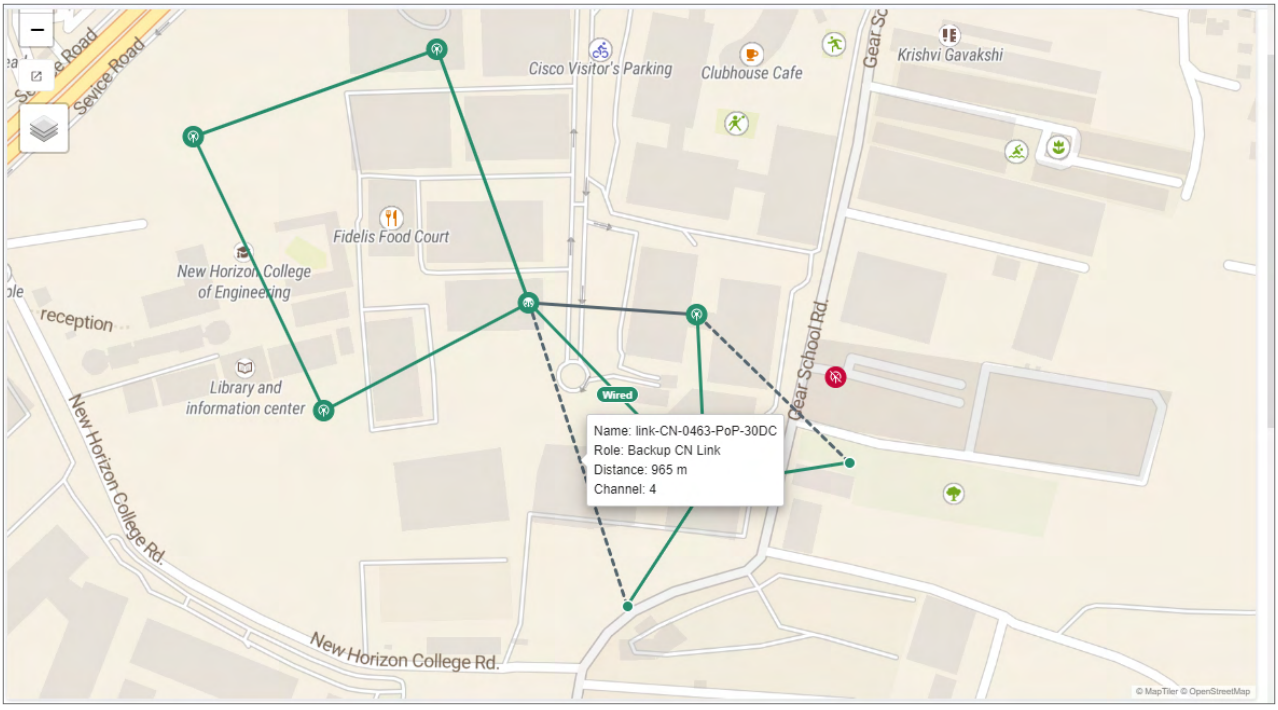


Dashboard Maps

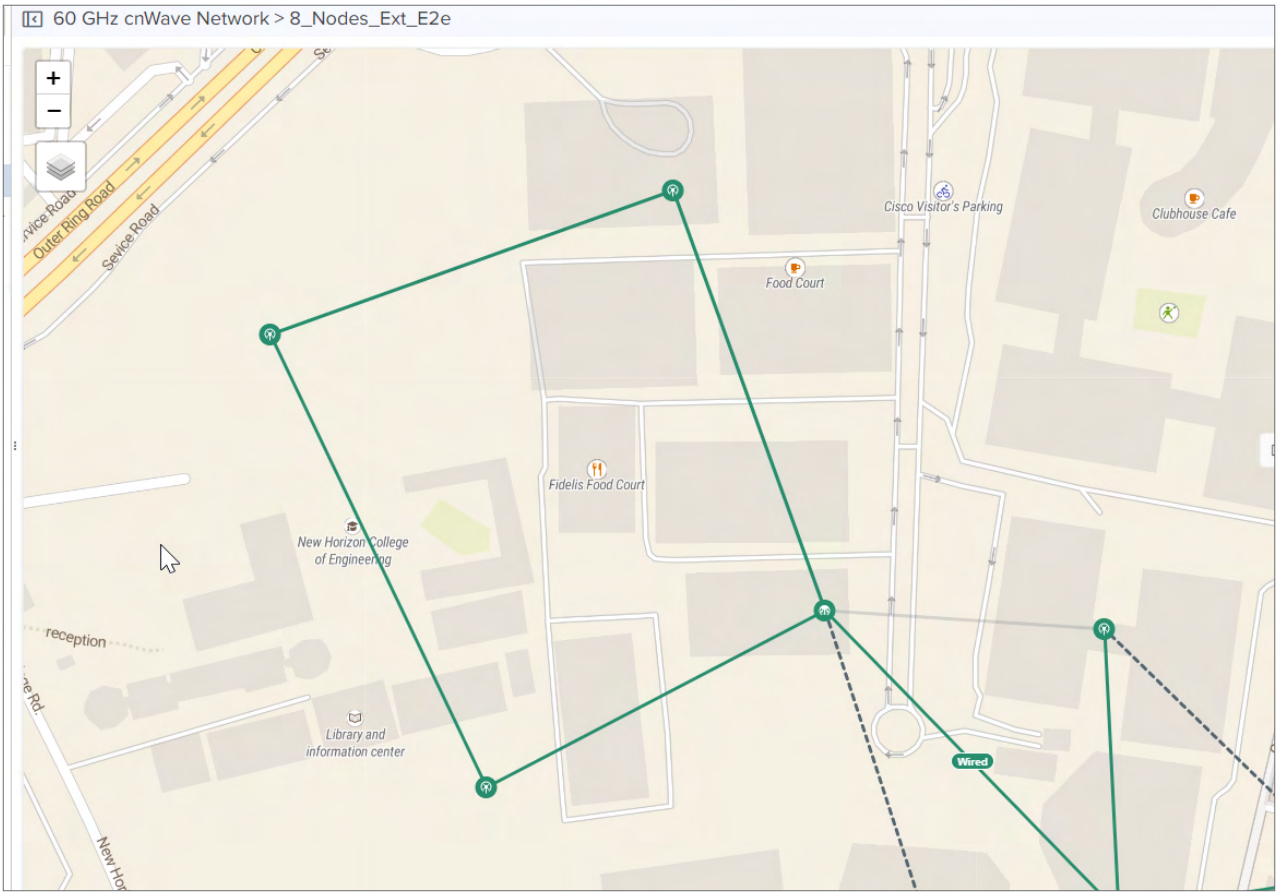
In the dashboard map, when user hovers on particular **PoP, DN** or **CN** it pops-up the device details. When user hovers on particular link it pops up the link details.



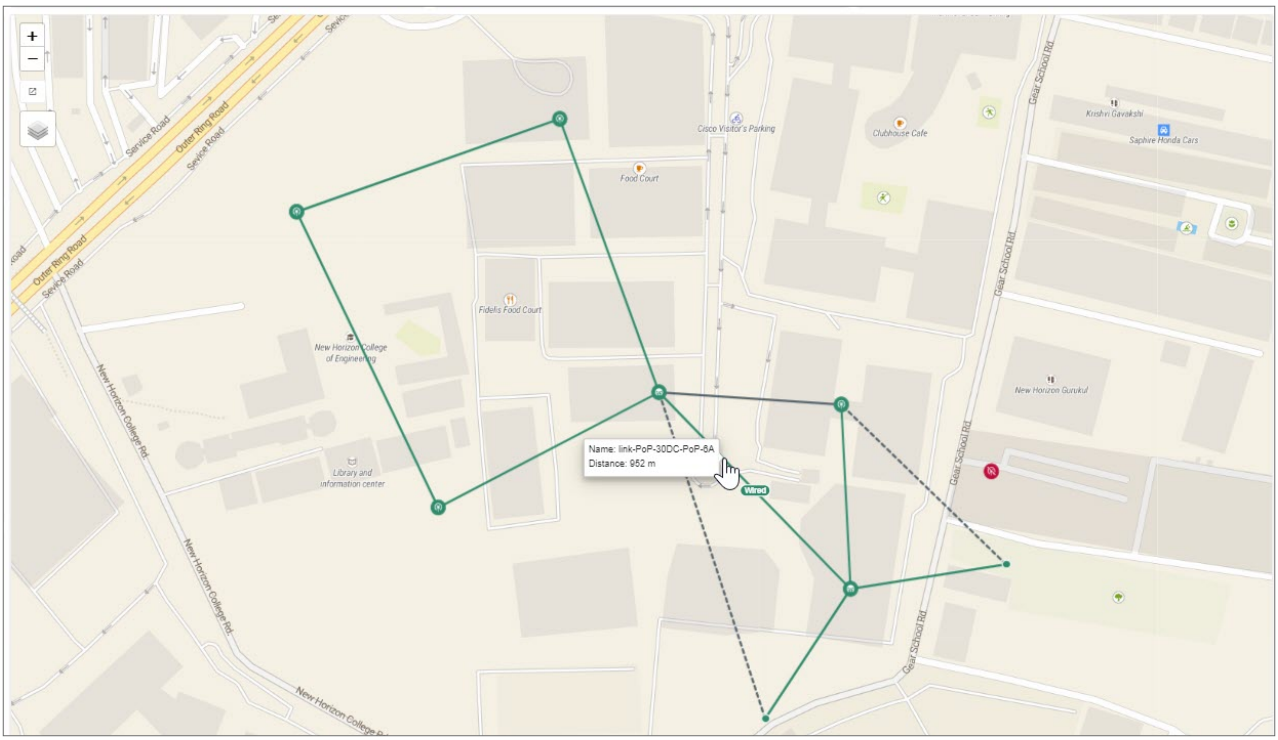
- Dotted line displays the Backup CN link between the DN and CN..



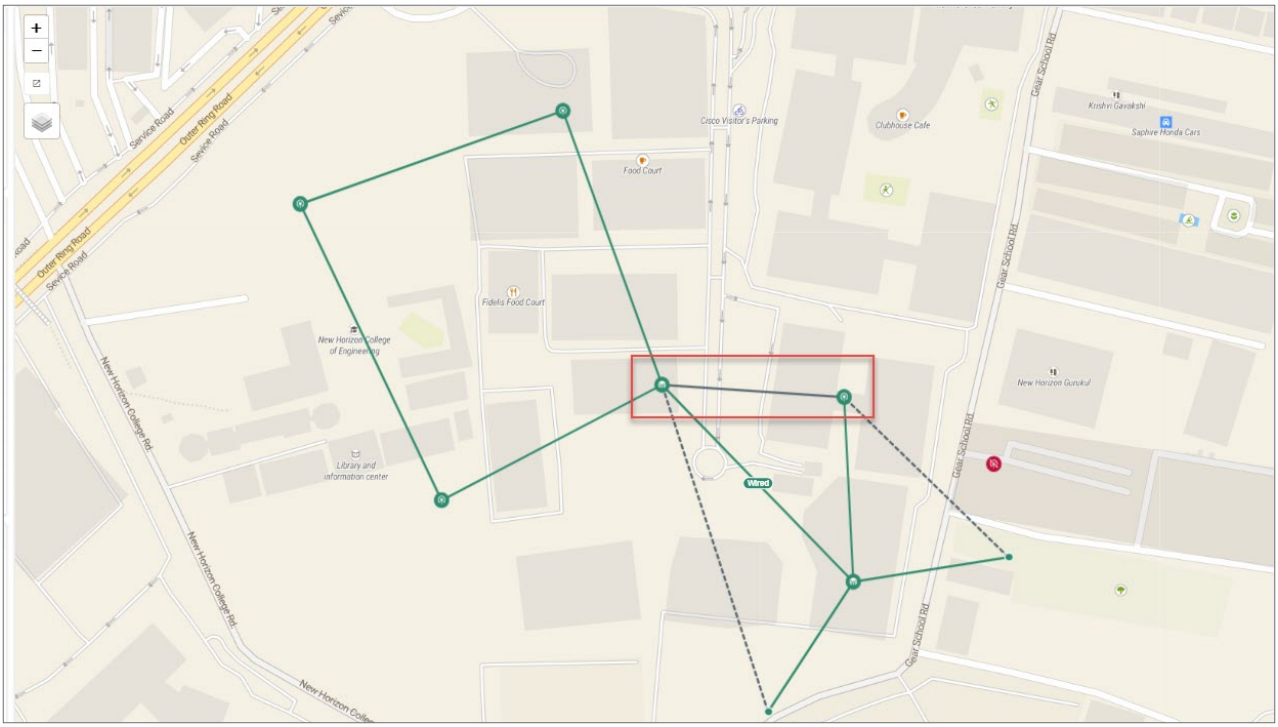
- Continuous line display the wireless link between PoP, DN, or CN..



- 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:

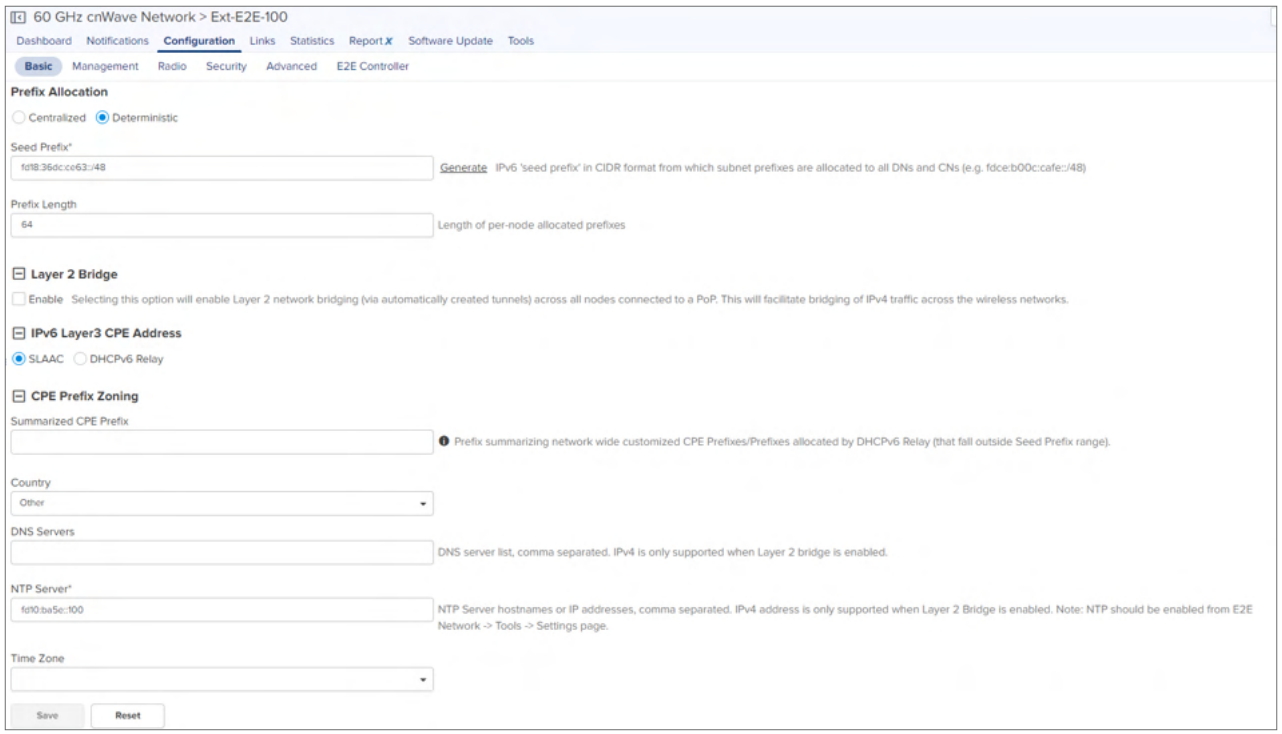
- Basic
- Management
- Radio
- Security
- Advanced
- E2E Controller
- High Availability X

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.

Note

- By default **Country** is **Other**, user can configure it.
- Enter the **Hostnames** or **IP address** of NTP server.

2. Select the **Country** from the dropdown.
3. Enter the **DNS Server.**
4. Enter **NTP Server.**
5. Select the **Time Zone** from the dropdown.

Note

By default **Wireless Scans** will be disabled.

6. Click **Save.**

Management

Management configuration allows user to configure and manage the credentials of the administrator and it allows enable **SNMP**.

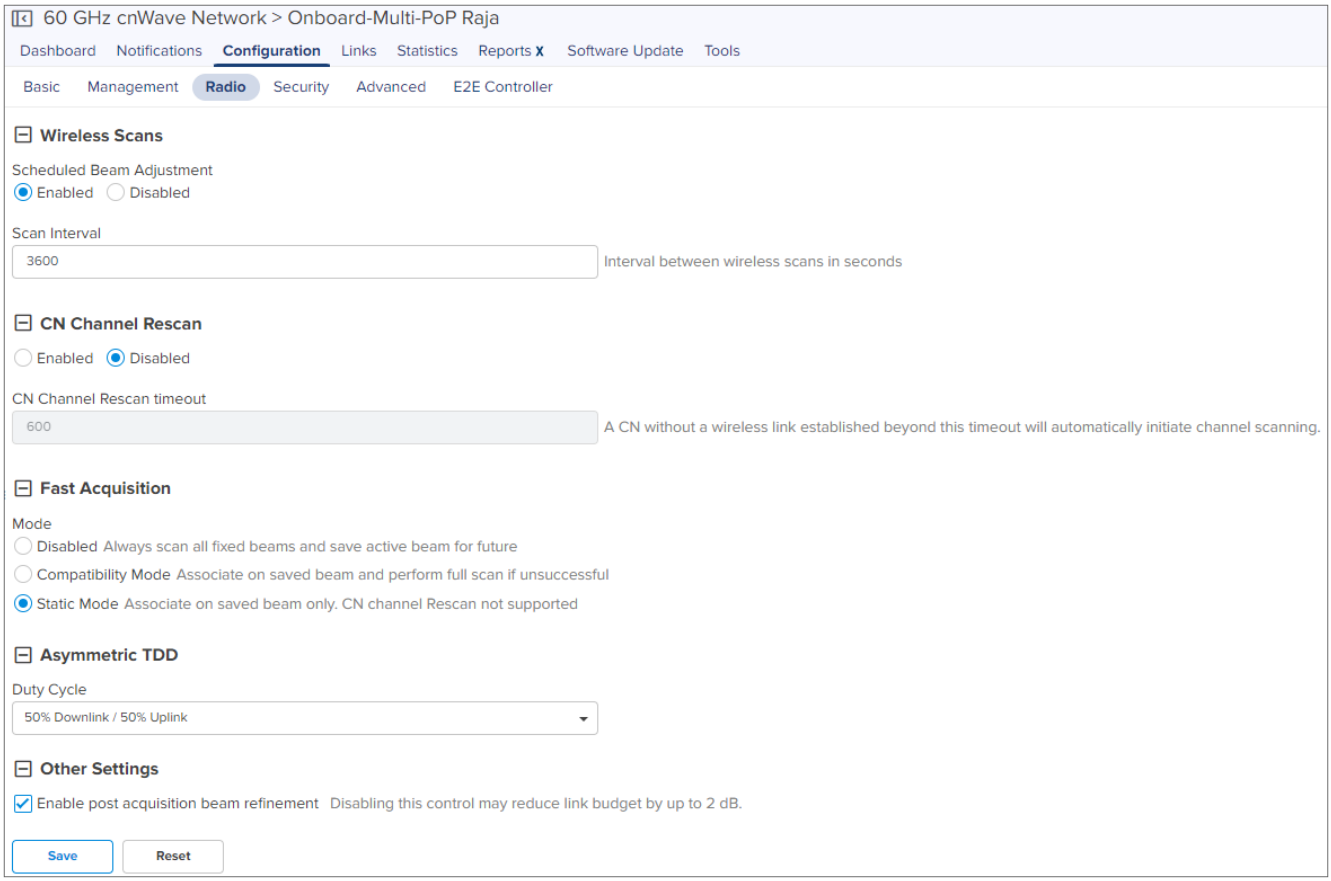
1. Navigate to **Configuration** > **Management** to set the **Device GUI Passwords** and to enable the **SNMP**.



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.

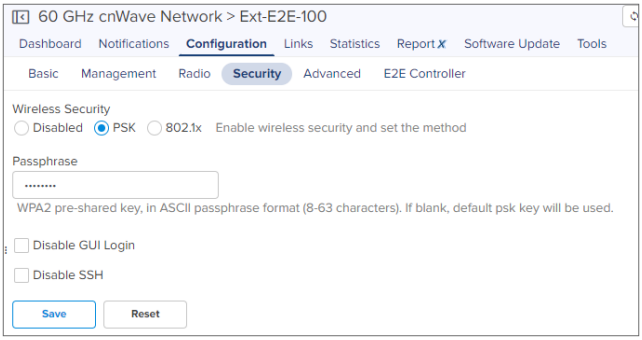
- **Asymmetric TDD**
  - **Duty Cycle**—Select a duty cycle from the dropdown list. For example:
    - **60% Downlink / 40% Uplink**—Set 60% of physical bandwidth for downloading and 40% of the physical bandwidth for uploading.
- **Other Settings**
  - **Enable post acquisition beam refinement**—Select 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**.

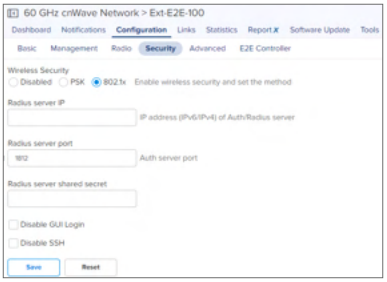
Note

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.**

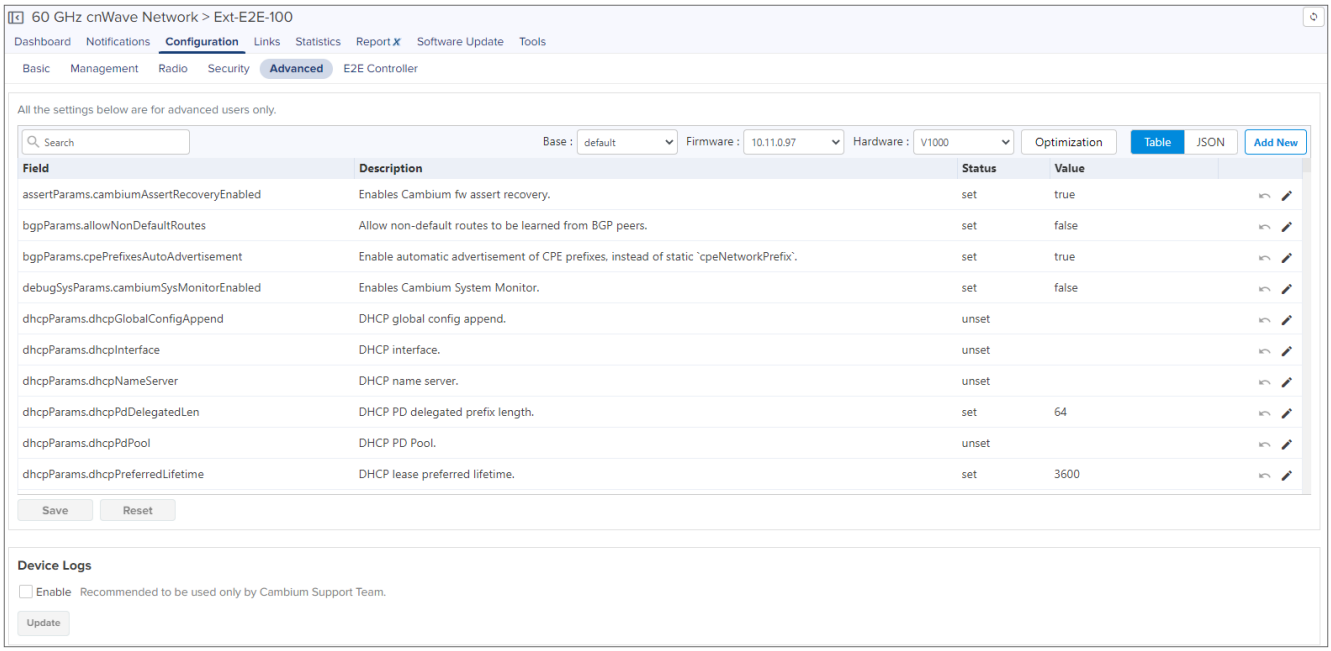
4. Enter the **Radius Server port.**
5. Enter the **Radius Server Shared Secret.**
6. Click **Save**.

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 Control Superframe Allocation
- Optimize DPA Zone Allocation
- Clear Node Auto Configuration

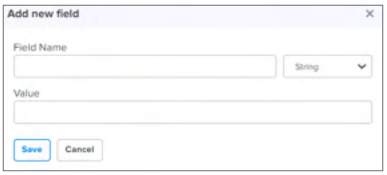


Table

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:

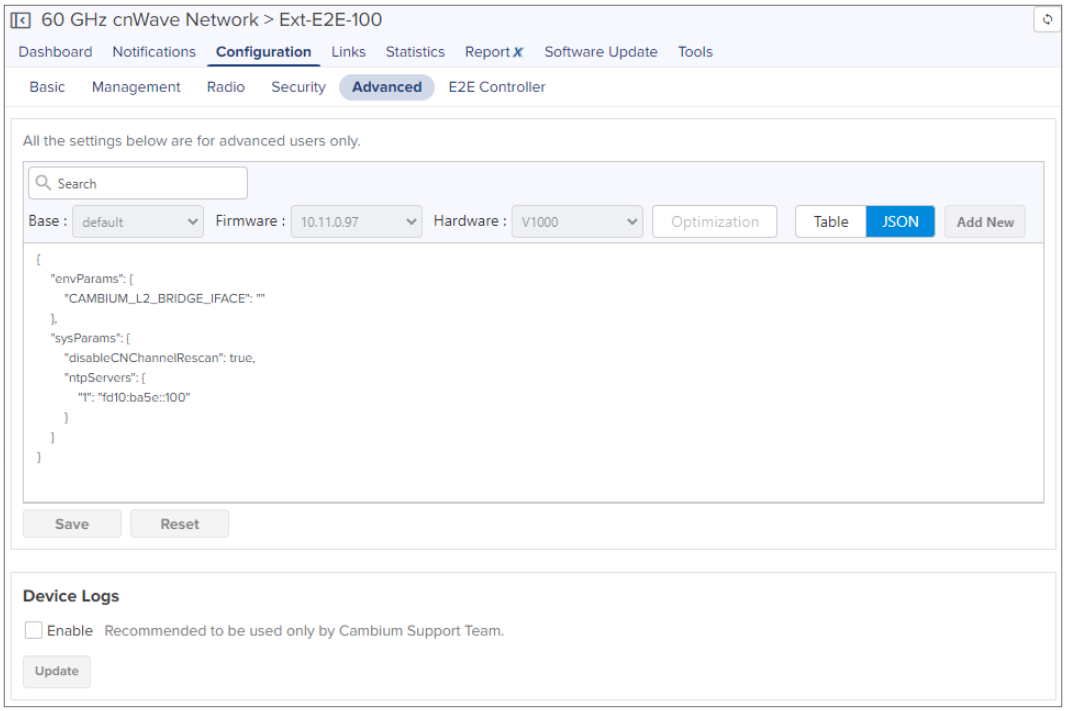
1. Navigate to **Configuration** > **Advanced.**
2. Click **Add New.**
3. Enter the **Field Name** and **Value.**



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

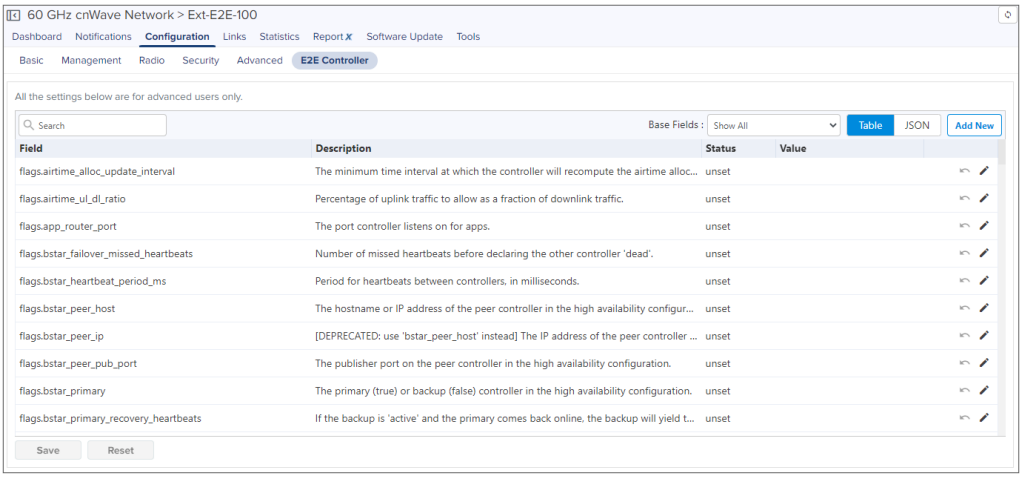
E2E Controller allows the advanced user to set the **Table** and download the **JSON** file.

Table

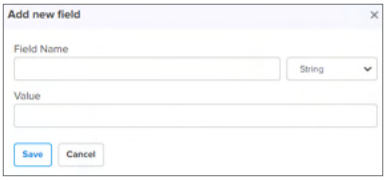
In **E2E Controller Table** user can edit or add **Field Name** and **Value.**

To Add Field:

1. Navigate to **Configuration** > **E2E Controller.**
2. Click **Add New.**



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:

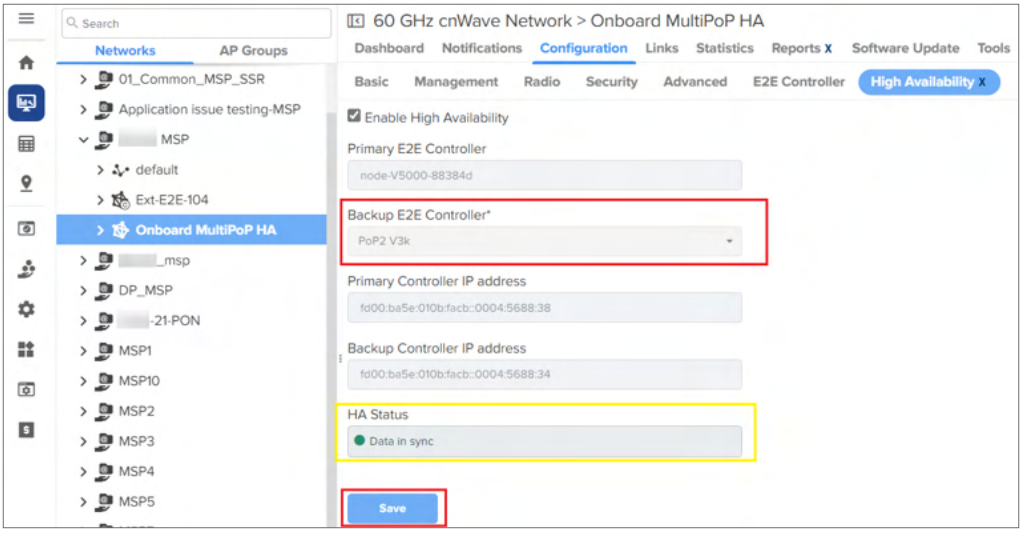
1. From the Home page of cnMaestro, navigate to **Monitor and Manage** > **E2E Network** > **Configuration** > **High Availability X**.

   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.

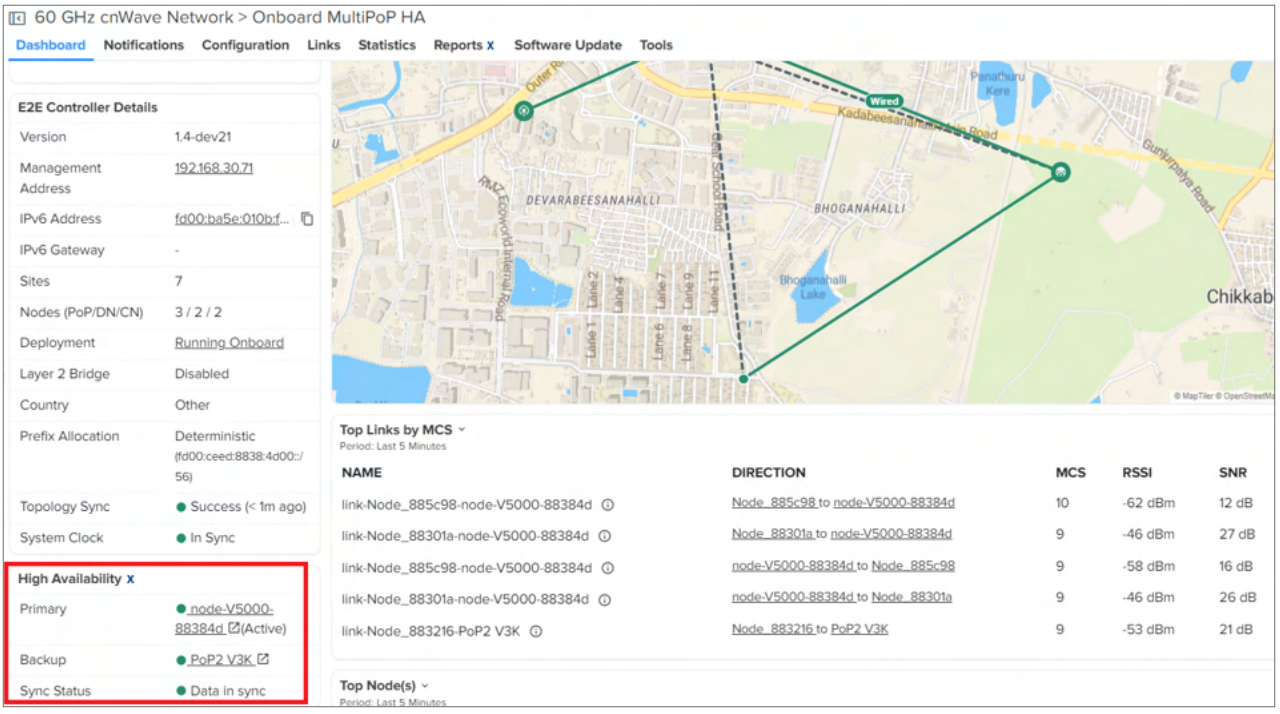
   You can check the IP addresses (read only) of primary and backup controllers.

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 84 *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.

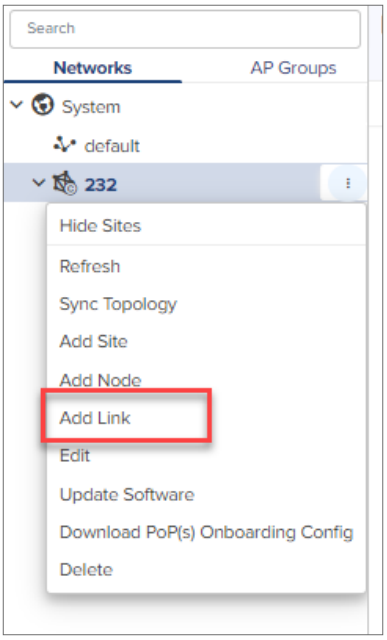
- List
- Statistics
- Events

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.

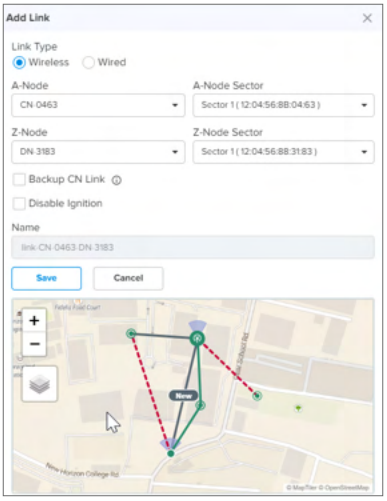
To add a link, perform the following steps:

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.

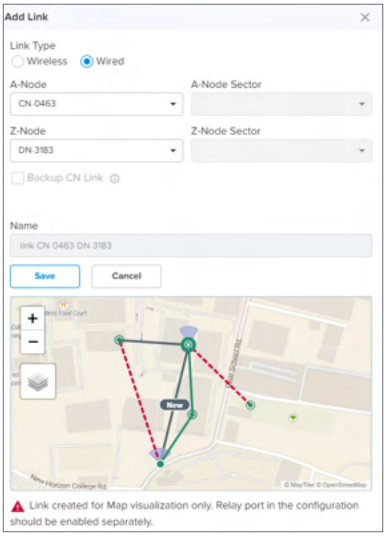
Figure 382 *Wireless link*



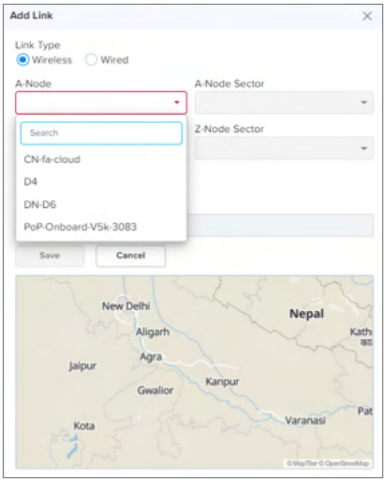
Note

In Wired Link Type, add Sector is disabled.

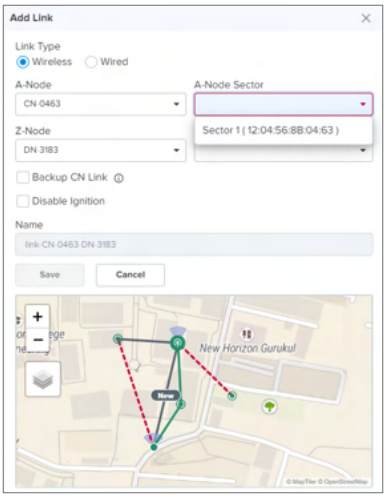
Figure 383 *Wired link*



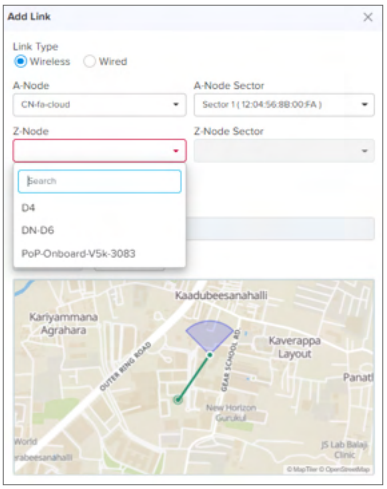
4. Select the **Node** from the dropdown in **A-Node.**



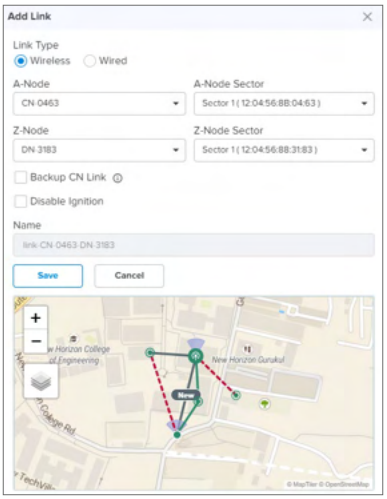
5. Select the **Sector** of the node from the dropdown in **A-Node Sector.**



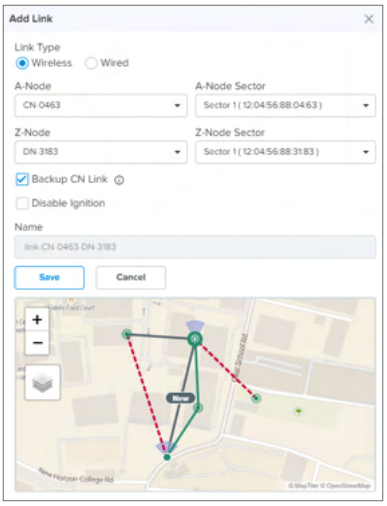
6. Select the **Node** from the dropdown in **Z-Node.**



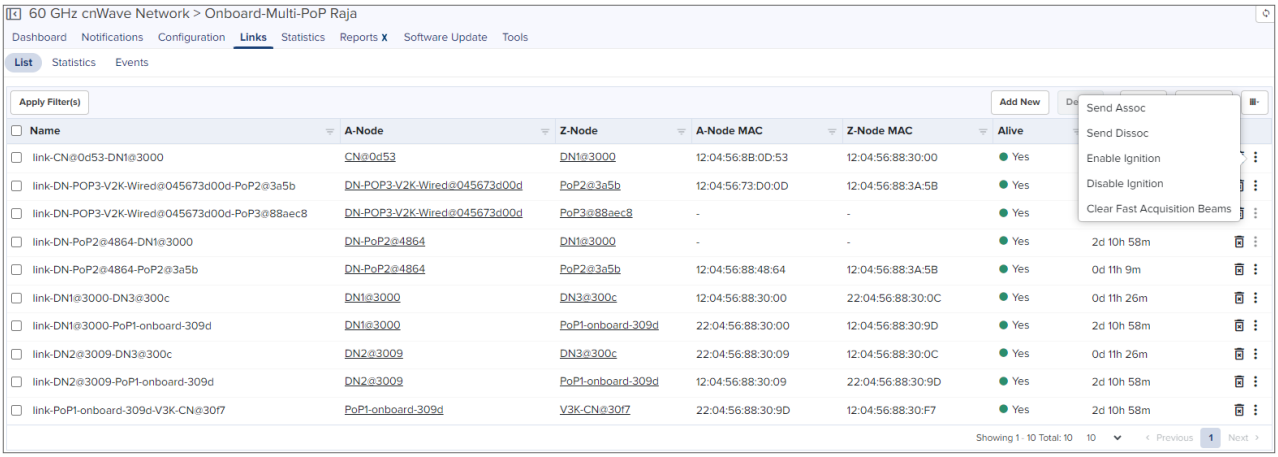
7. Select the **Sector** of the node from the dropdown in **Z-Node Sector.**



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. If user selects **Disable Ignition** option, wireless link creates with disable ignition. User need to manual select **Enable Ignition** from link options.
10. Click **Save**.
11. Once the link is successful it displays the **Alive** status as **Yes**.



Available link options are:

- Send Assoc
- Send Dissoc
- Enable Ignition
- Disable Ignition
- Clear Fast Acquisition Beams

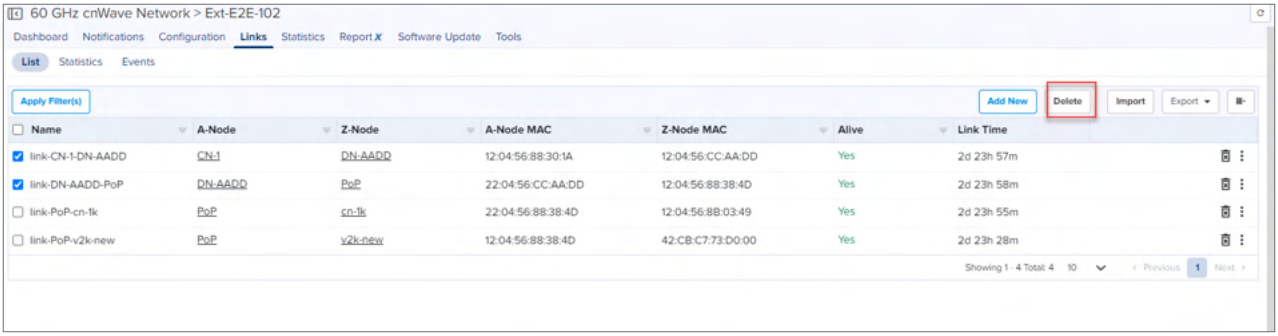
Delete Links

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.



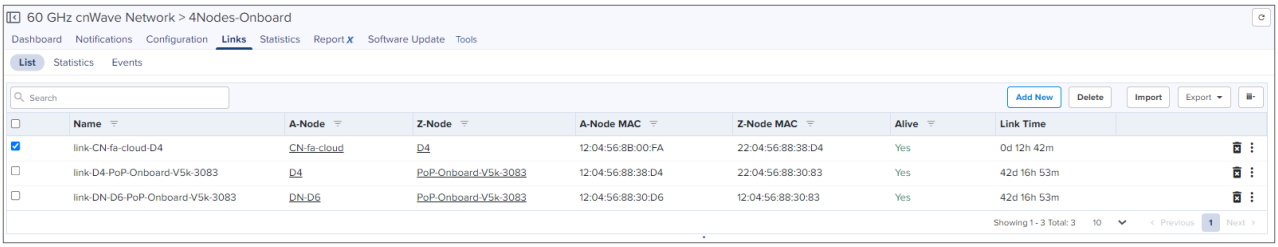
1. Click **Delete**.

Import List

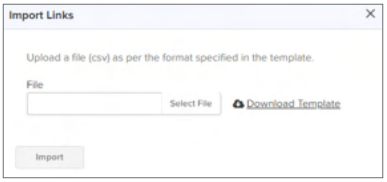
In **Links** tab you can import the E2E Controller Network Links.

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	[illegible]	wireless
4	DN1	12:04:56:31:44:55	CN1	[illegible]	wireless
5	DN1		CN2		wired
6					
7					

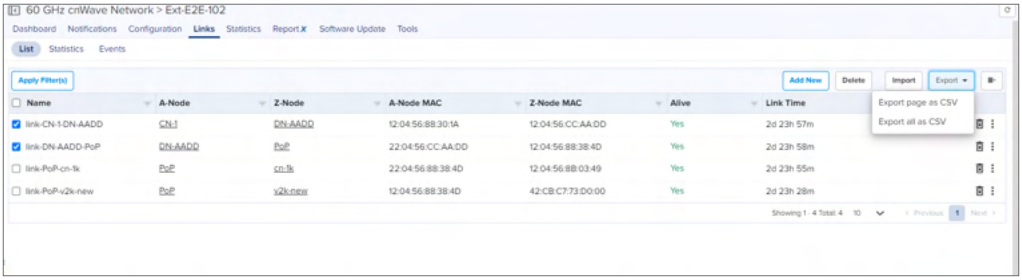
5. Select the file and click **Import**.

Export List

In **Links** tab you can export the E2E Controller Network Links.

To export the links:

1. Navigate to **Links** > **List** > select **Export.**

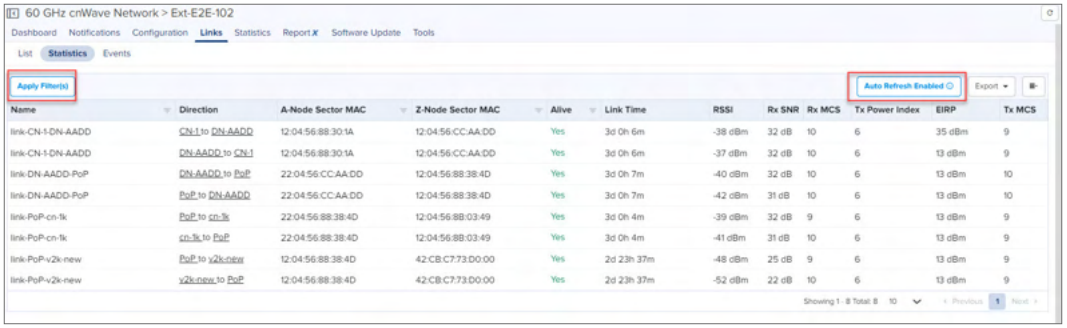


2. Data is exported in the.CSV file format as shown below.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	LINK_NAME	A_NODE_I	A_NODE_I	Z_NODE_N	Z_NODE_I	LINK_TYPE	ALIVE	IGNITION_	DISTANCE	AZIMUTH	BACKUP_C	IGNITION_	TIMESTAMP		
2	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		
3	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		
4	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		
5	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		

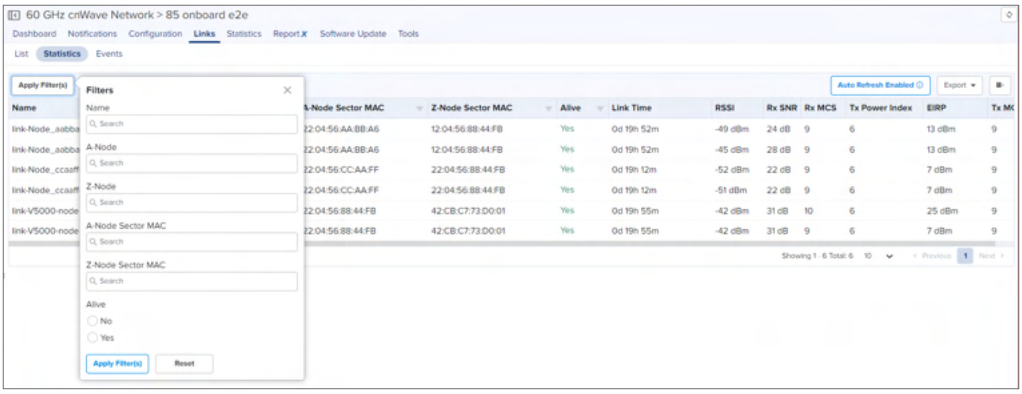
Statistics

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.

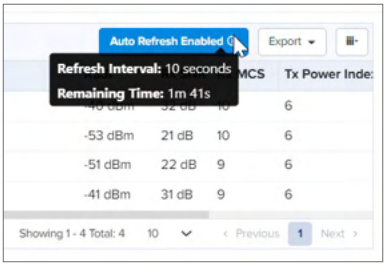


You can **Apply Filter(s)** for Name, A-Node, Z-Node, A-Node Sector MAC, Z-Node Sector MAC, and Alive. The **Auto Refresh** option allows to refresh data automatically as per Refresh Interval, which is configured for five minutes. By default, Refresh Interval is 10 seconds. This option gets disabled 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.**



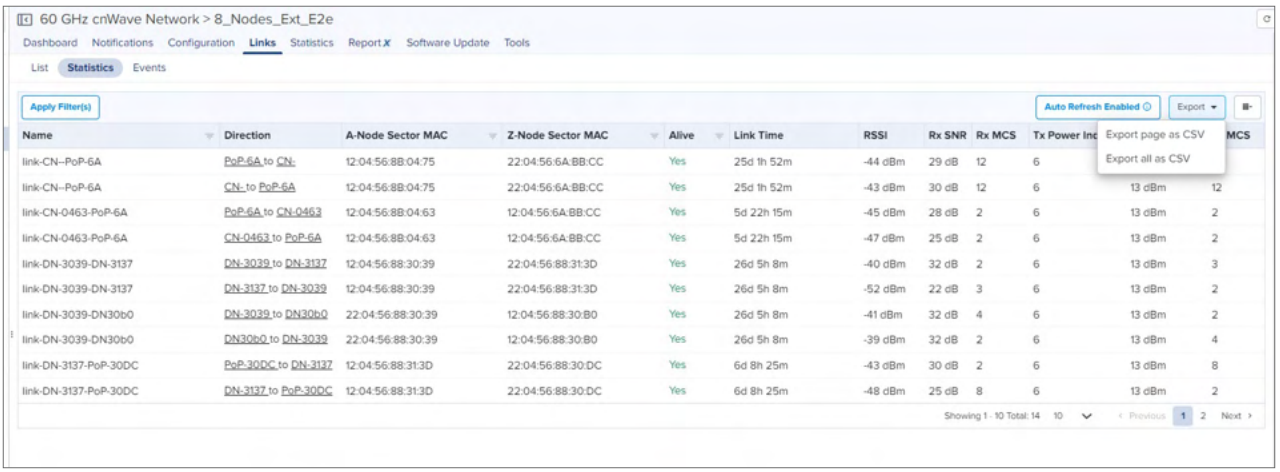
4. Click the info icon to view **Refresh Interval** and **Remaining Time**.



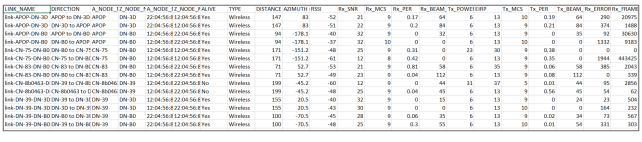
Export Statistics

To export the Statistics:

1. Navigate to **Links** > **Statistics** > select **Export.**



2. It exports .csv file format as shown below.



Events

Events provide the details of link availability, hourly link availability in percentage, link availability in different time lines, and distance of the link.

Figure 384 *Links > Events*

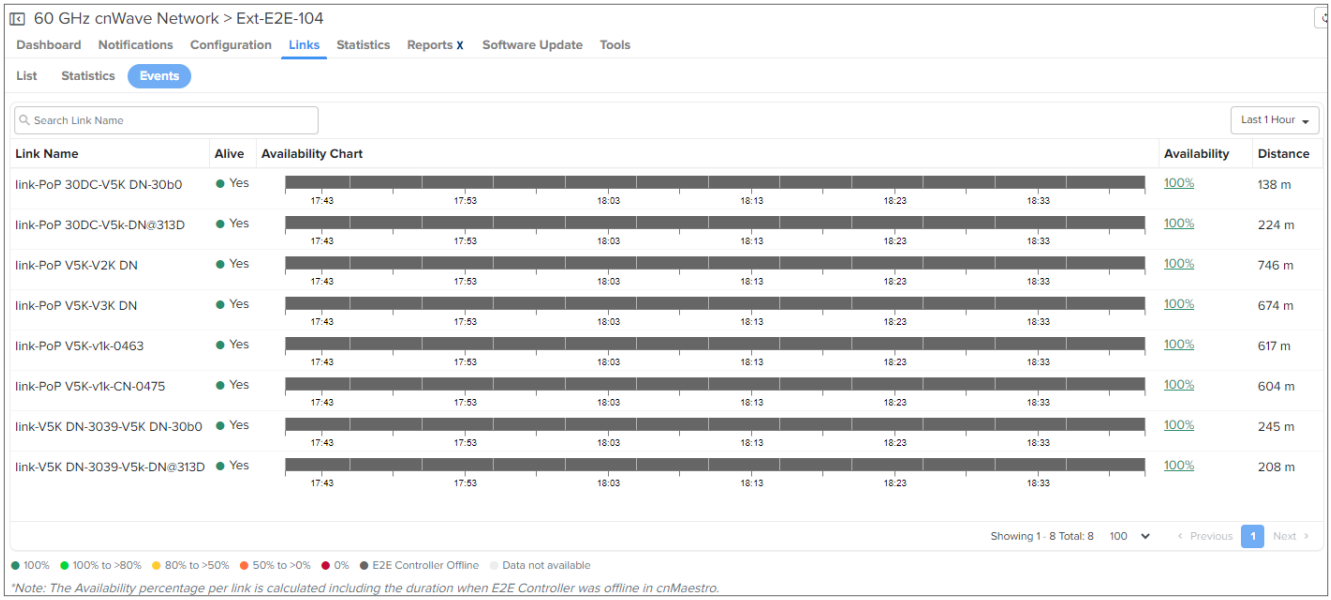
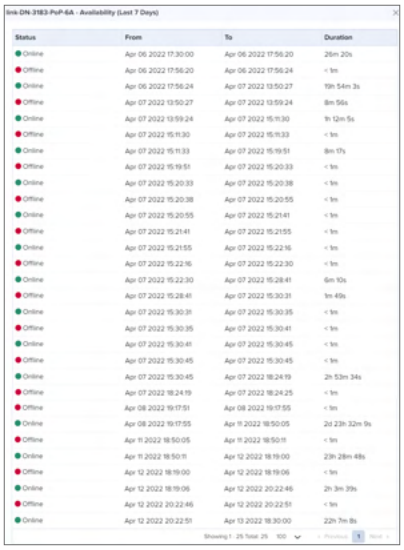


Table 85 *Events fields*

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 386. Clicking on percentage link availability displays pop-up window as shown in Figure 387 Link availability is presented in different colors in the chart as shown in Figure 385
Availability Percentage	Availability of link is shown in percentage in the Availability column as shown in Figure 386.
Distance	Distance of the link in meters.

Figure 385 *Link Availability in Percentage*





Availability percentage per link is calculated including the duration when E2E Controller was Offline in cnMaestro.

Figure 386 *Link Availability*

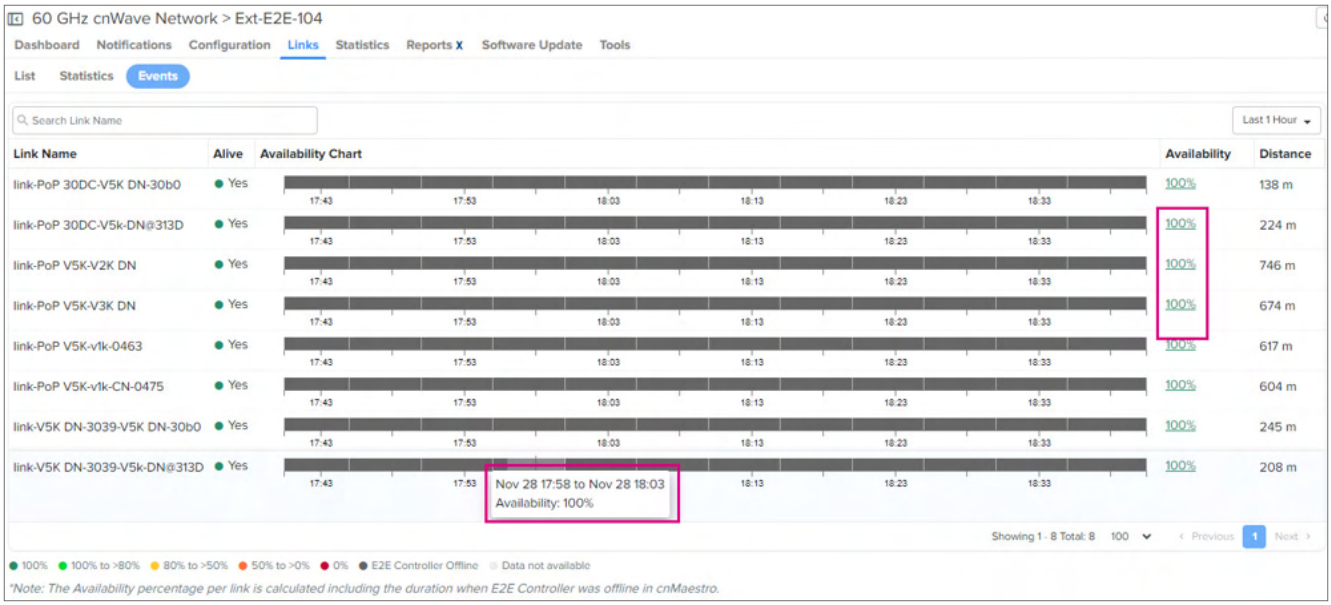
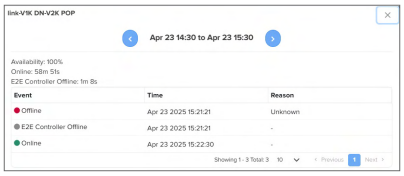


Figure 387 *Link Status*



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

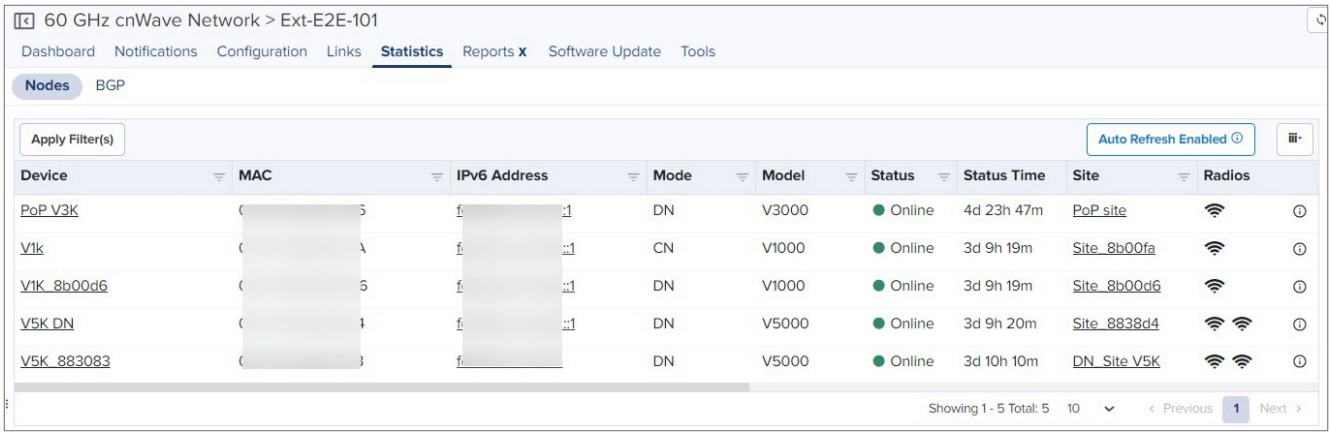
The E2E Network provides the following statistics:

- 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 388 *Nodes Statistics*



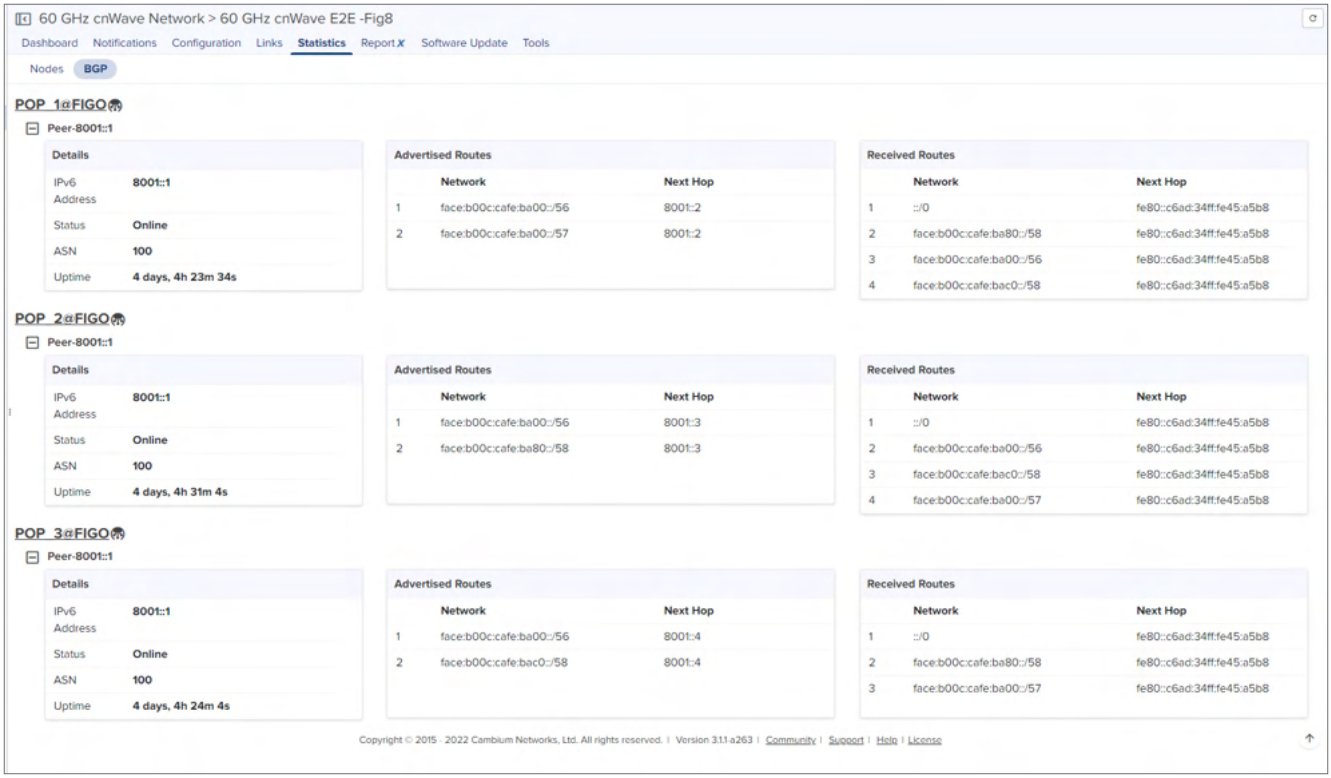
BGP

Note

BGP statistics displays only if BGP option is enabled in Routing in PoP configuration.

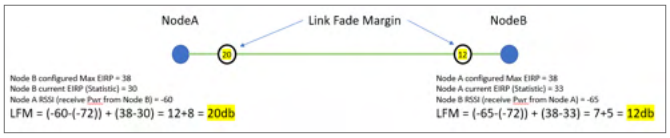
BGP provides the details of **Advertised Routes, Received Routes,** and **Peer** details.

Figure 389 *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 390 *Link Fade Margin*



Software Update

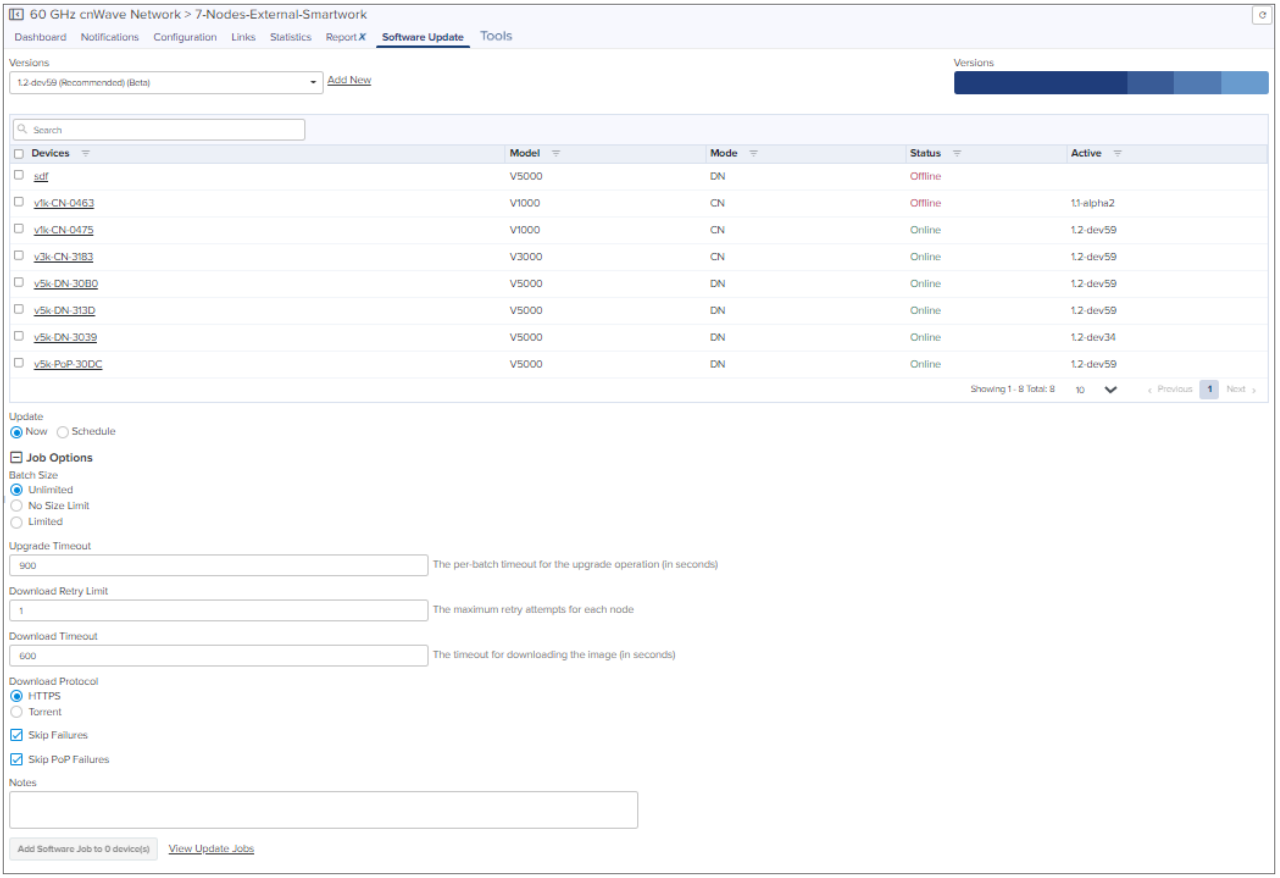
The **Software Update** tab allows to update with the latest device software.

To update the software:

1. Select the **Network** and navigate to the **Software Update** tab.
2. In **Software Update** tab select the desired Versions from dropdown in **Versions** tab.
3. Select the **Device**.
4. In **Job Options**, do the following:

- Select **Batch Size**
- Enter **Upgrade Timeout.**
- Enter **Download Retry Limit.**
- Enter **Download Timeout.**
- Select the Download Protocol as **HTTPS** or **Torrent.**
- Enable the **Skip Failures** or **Skip PoP Failures**.

5. Click **Add Software Job to device.**



Note

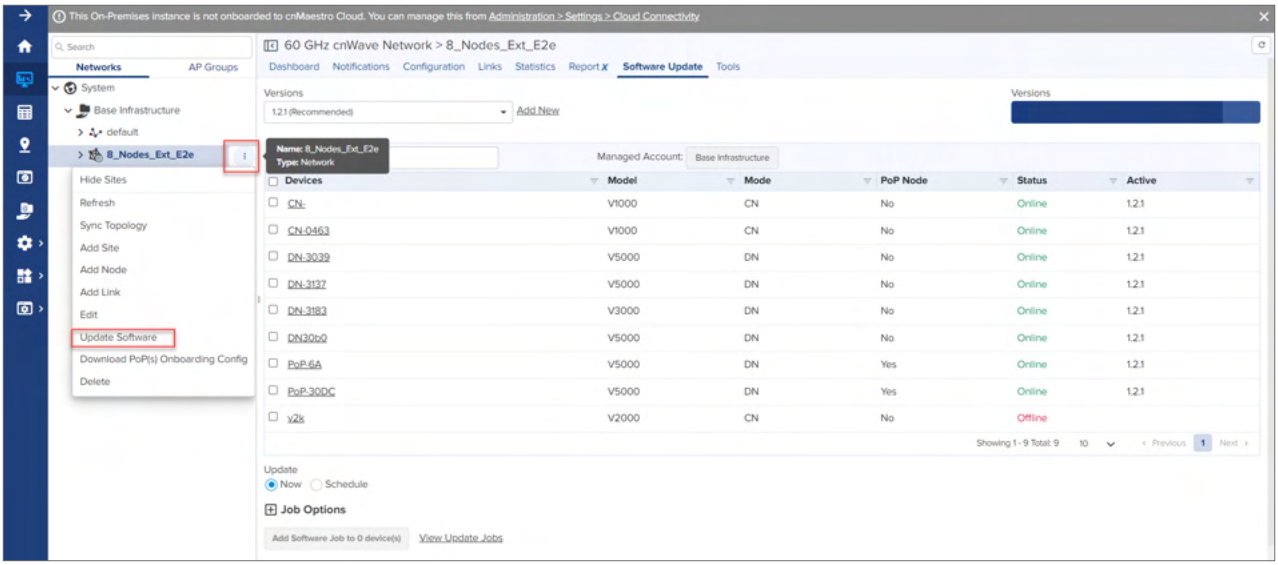
Onboard E2E controller will support only one synced image. If user needs to sync another image, select the image from **Versions** drop down and click **Sync Selected Image.**

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 86.

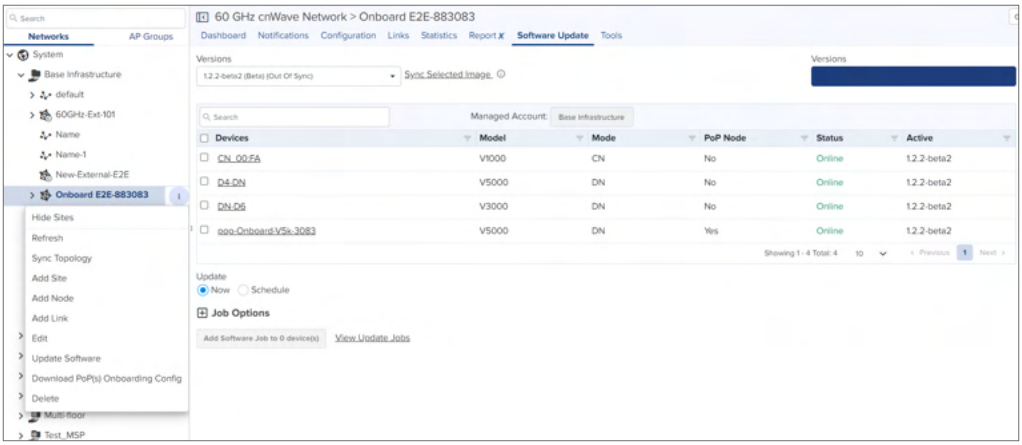
   Table 86 *Device Software Update: External E2E Controller*

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 87.

Table 87 *Device Software Upgrade: Onboard E2E Controller*

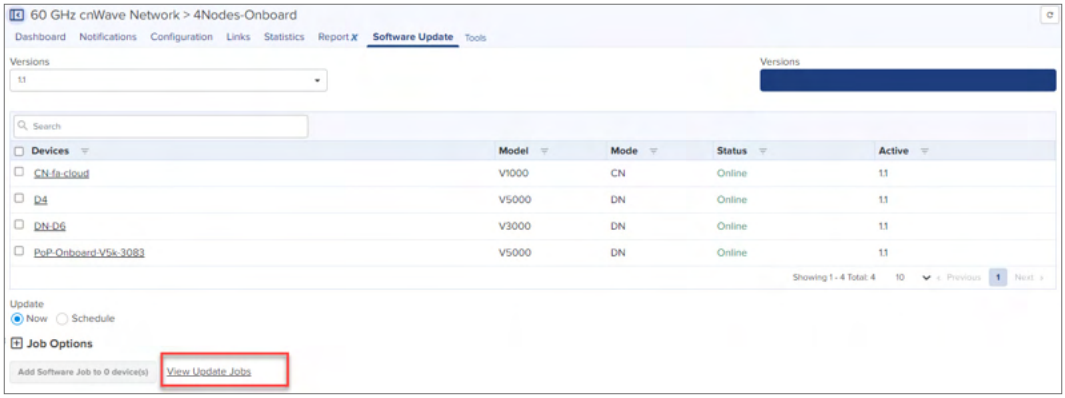
Software Upgrade	Example
If software version of Onboard PoP device is lower and upgraded to higher version then Software Upgrade is successful.	If the Onboard PoP device is running with 1.2, and selected software version is 1.2.1 or higher then Onboard PoP device is upgraded successfully.
If software 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.

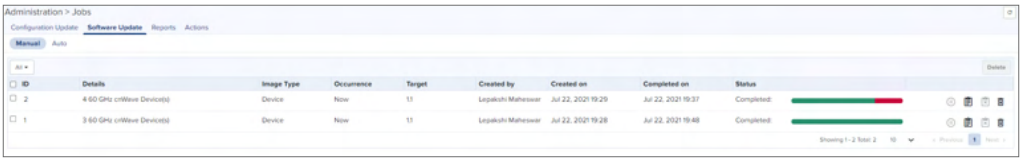
The Software Upgrade scenario for Onboard E2E Controller is explained in Table 87.

View Update Jobs

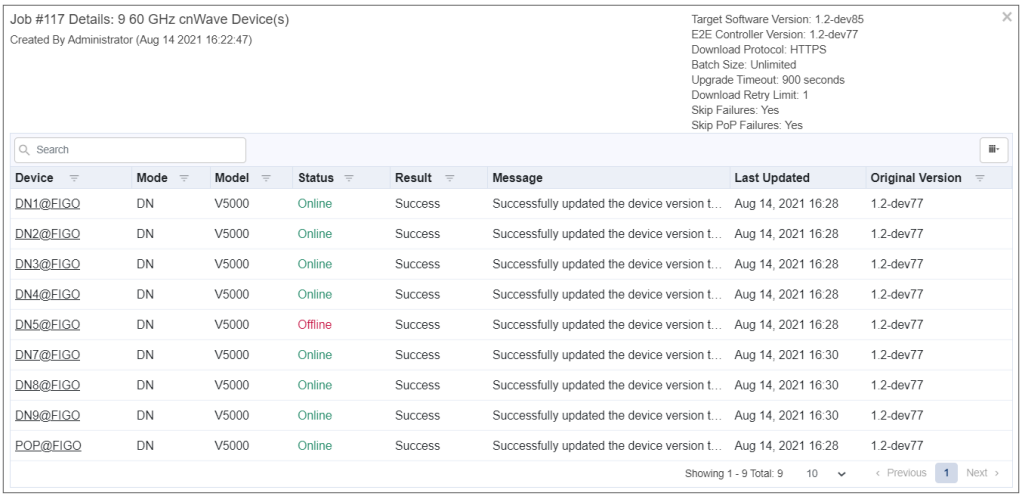
After adding the new Software Images, click **View Update Jobs.**



1. Navigate to the **Administration > Jobs > Software Update**.



2. Click **Show More** to view the Job Details.



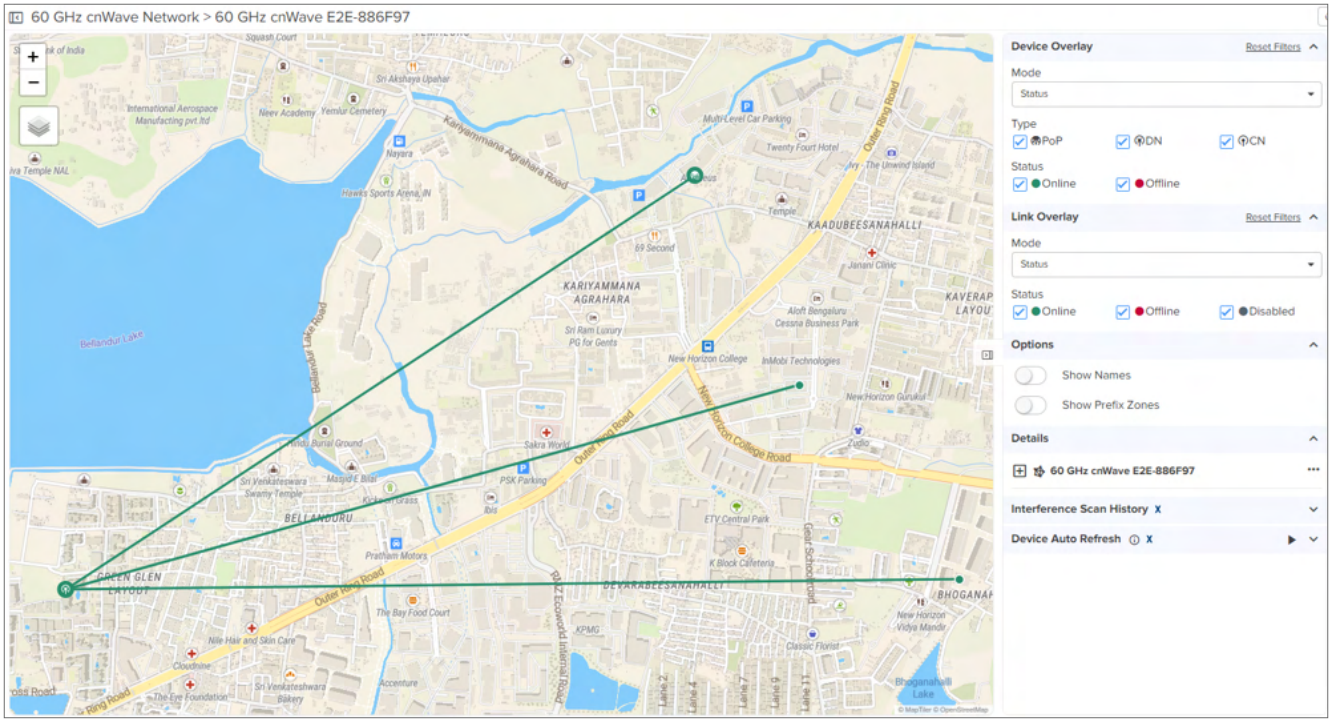
Reports

Reports page provides details on how to schedule and generate different types of data reports such as Devices, Active Alarms, Alarm History, and Events. For further details refer to Reports.

Map

The Map page shows how devices are connected in an E2E network, the state of the devices, and links in the E2E network. To view the map, select the **Map** ( ) icon in the left pane of the homepage and navigate to **E2E Network** to view the 60 GHz cnWave devices and links (as shown in Figure 391).

Figure 391 *Viewing E2E Network*



Note

Gray color lines are unmanaged links and gray color nodes are unmanaged nodes.

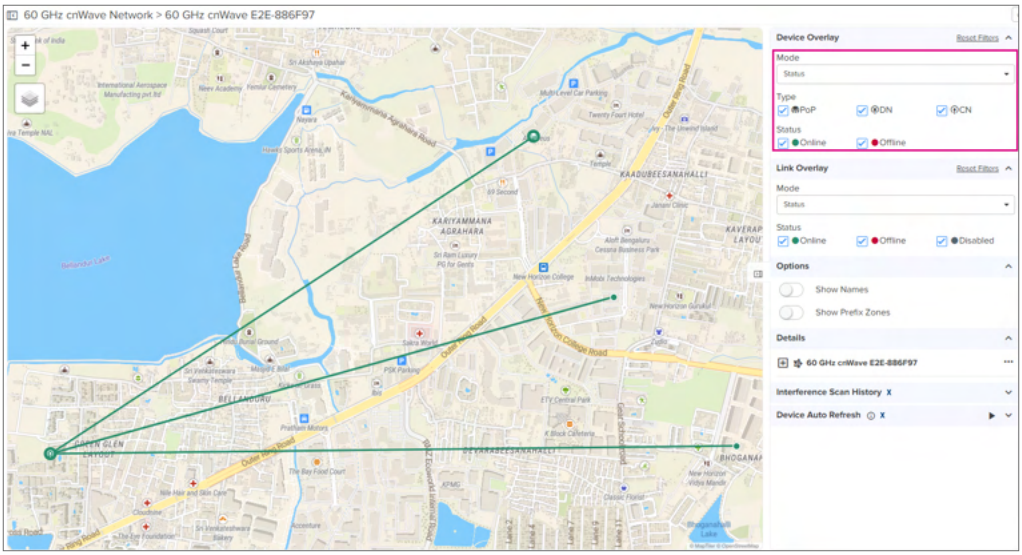
The following fields on the **Map** page provide details of the nodes and links:

- Device Overlay
- Link Overlay
- Options
- Details
- Interference Scan History X
- Device Auto Refresh

Device Overlay

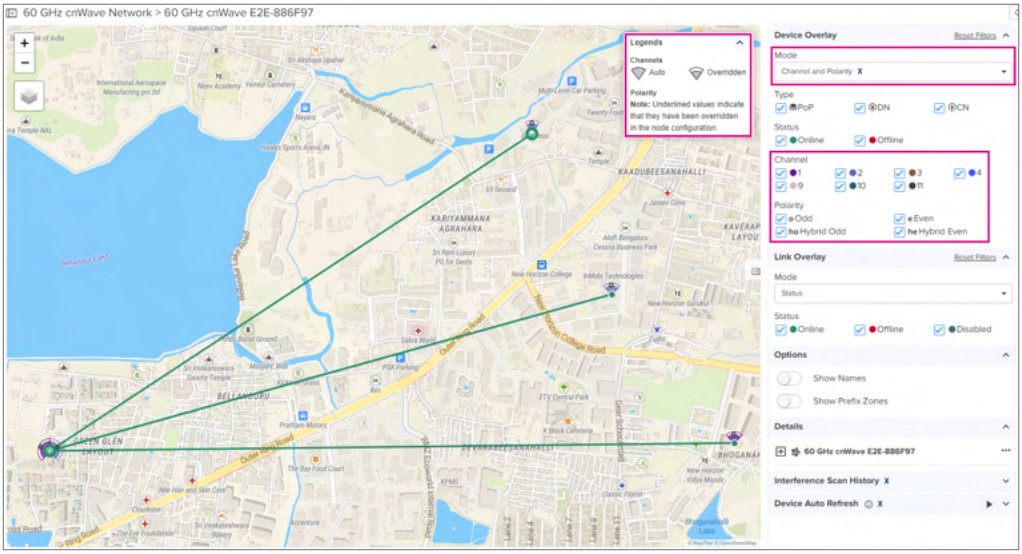
In the Device Overlay field section, complete the following steps:

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.



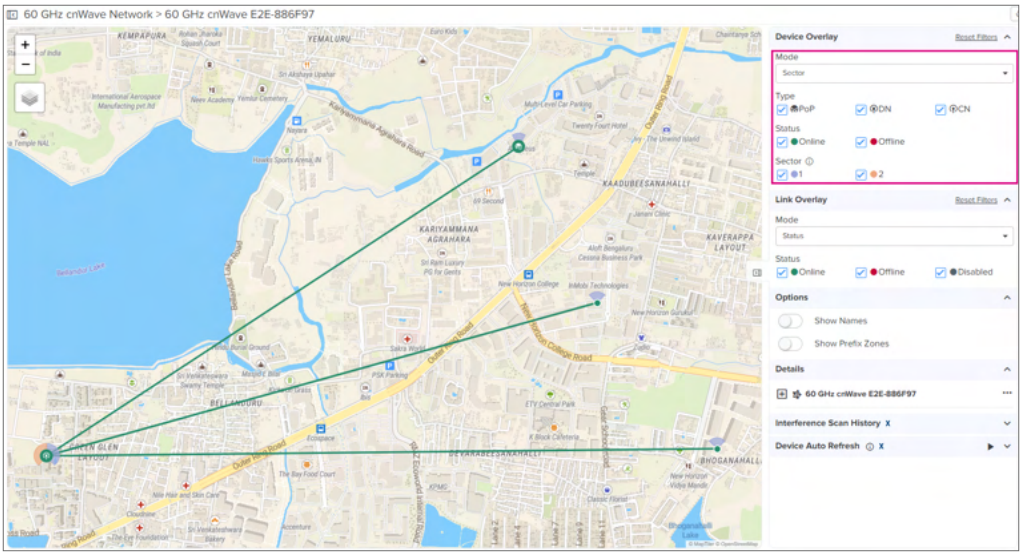
2. Select the **Mode** type as **Channel and Polarity** to view the following:

   - 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:

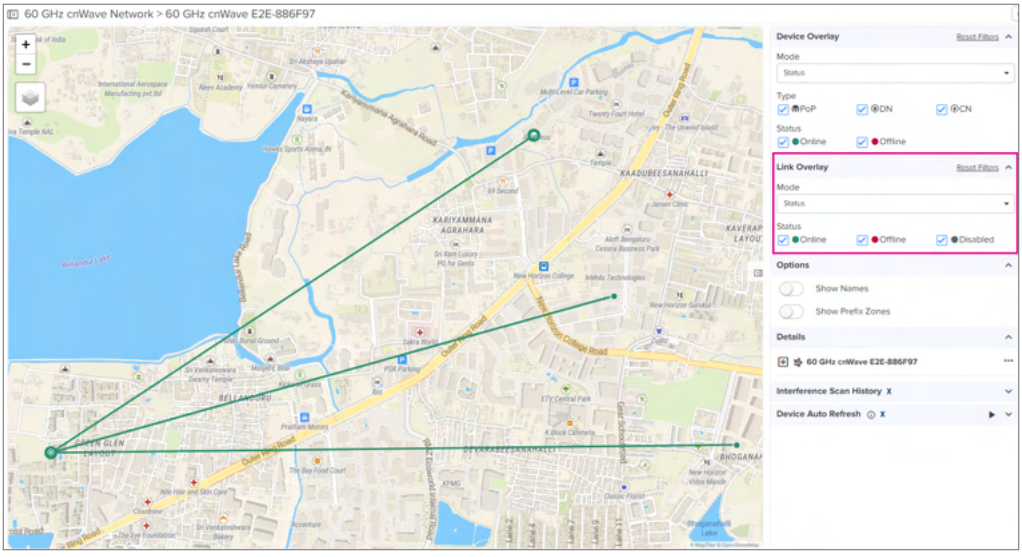


Link Overlay

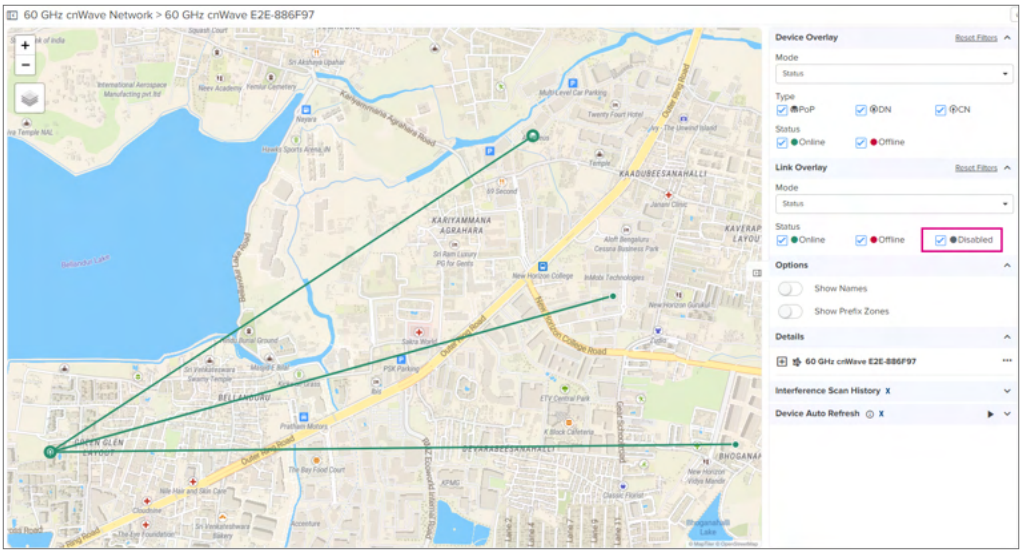
In the Link Overlay field section, complete the following steps:

1. Select the **Mode** type as **Status** to view the following:

   Status: The link status is Online or Offline.

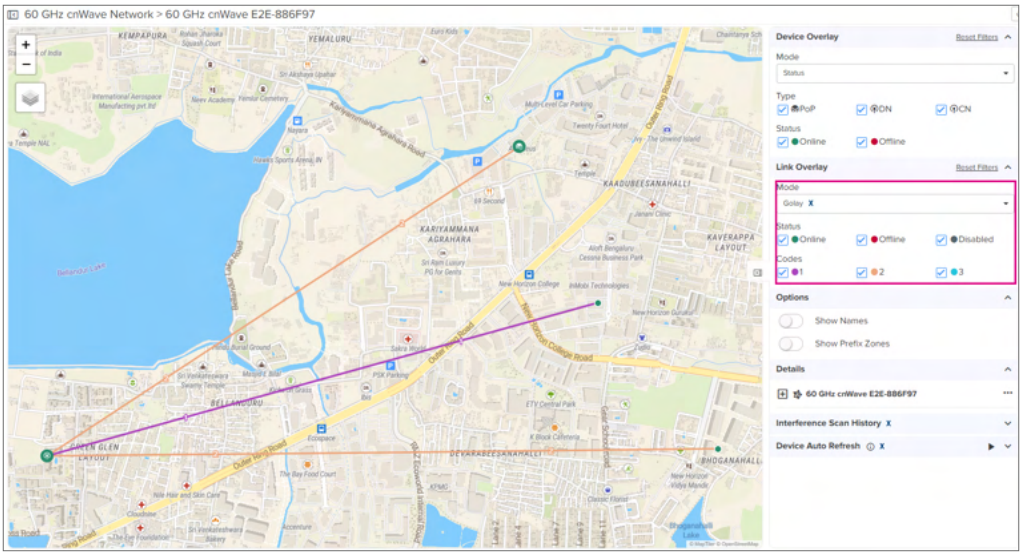


   By default the **Disabled** option is selected, which appears in light gray.



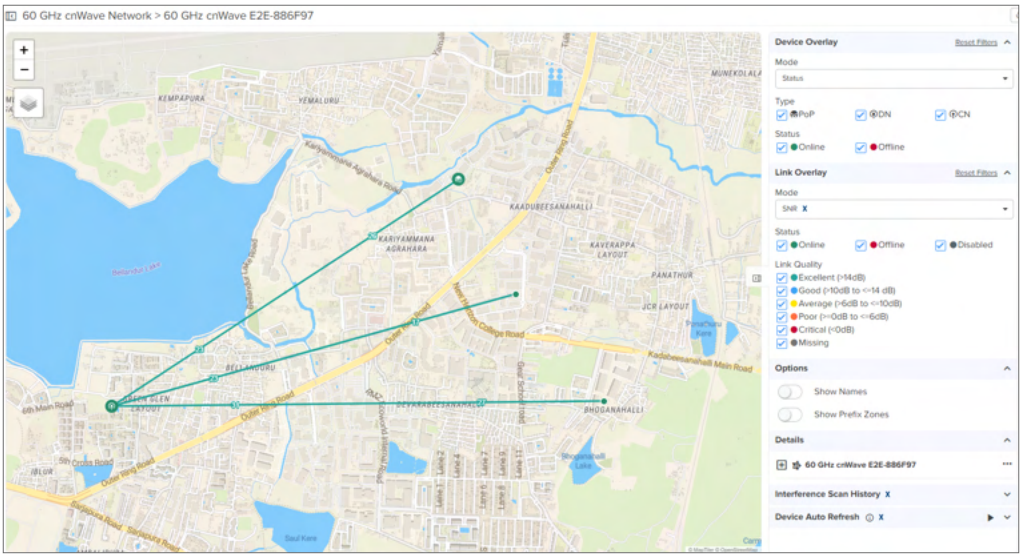
2. Select the **Mode** type as **Golay** to view codes.

   Golay: The Golay mode is represented in color codes, as shown below:



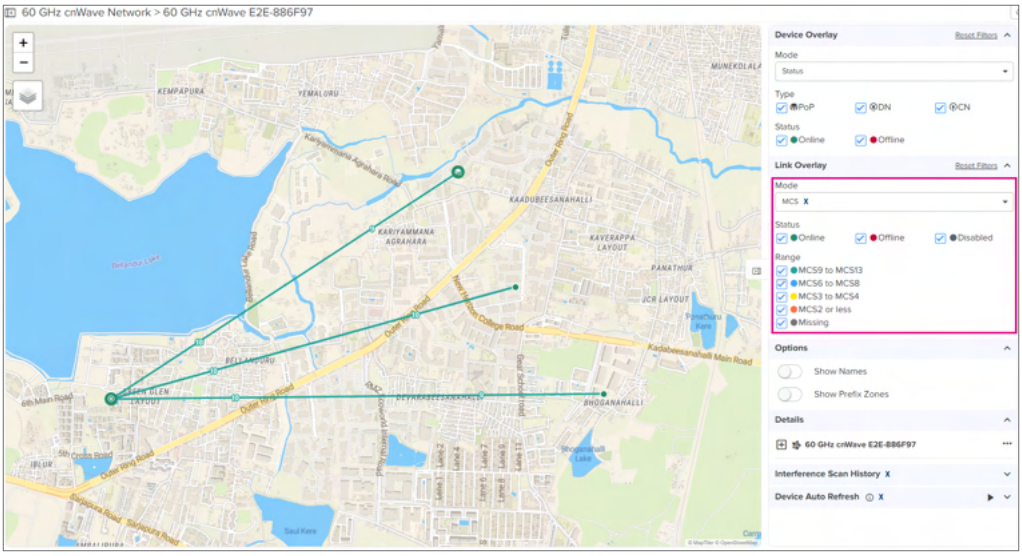
3. Select the **Mode** type as **SNR** to view link qualities.

   SNR: Shows various SNR link qualities and is represented in different colors.



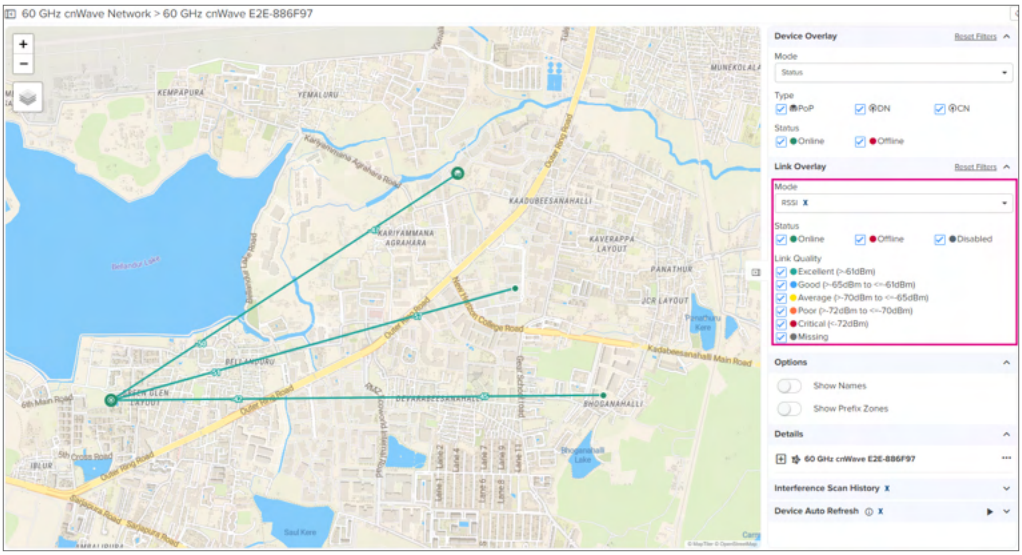
4. Select the **Mode** type as **MCS** to view link range.

   MCS: Shows the link status and various link ranges represented in different colors.



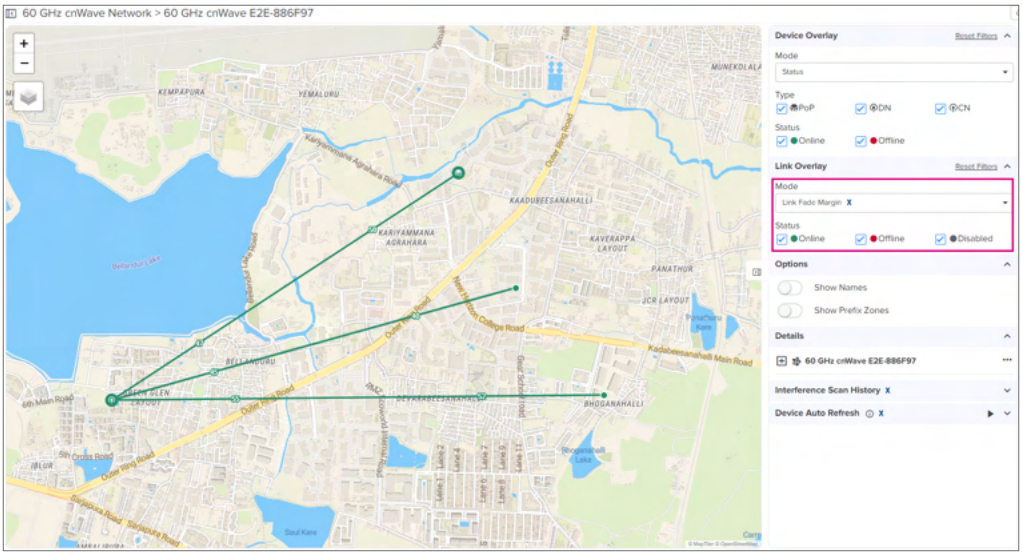
5. Select the **Mode** type as **RSSI** to view link qualities.

   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 390.



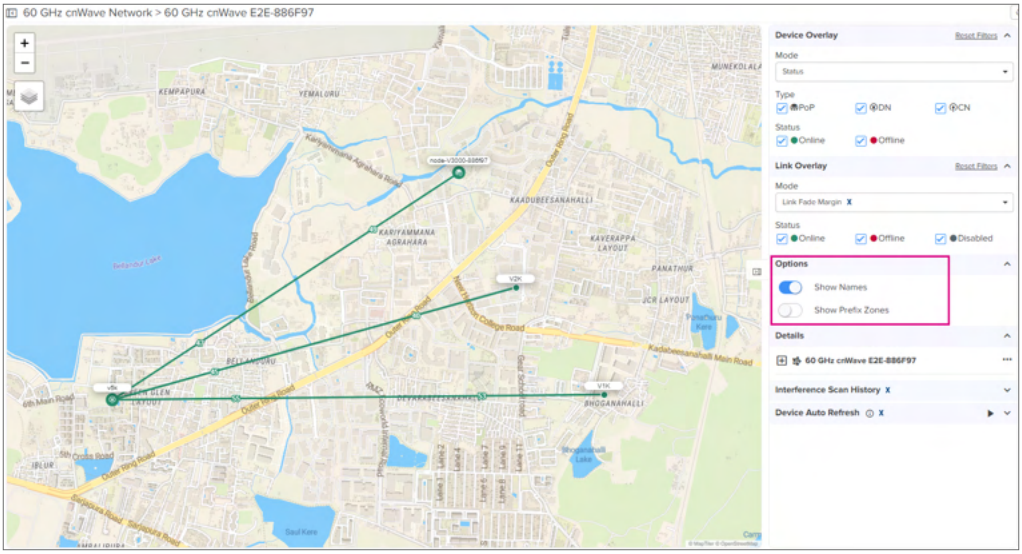
Note: Link Fade Margin is applicable only when E2E Controller and Device version are 1.2.2.

- Airtime%
- Throughput (Mbps)

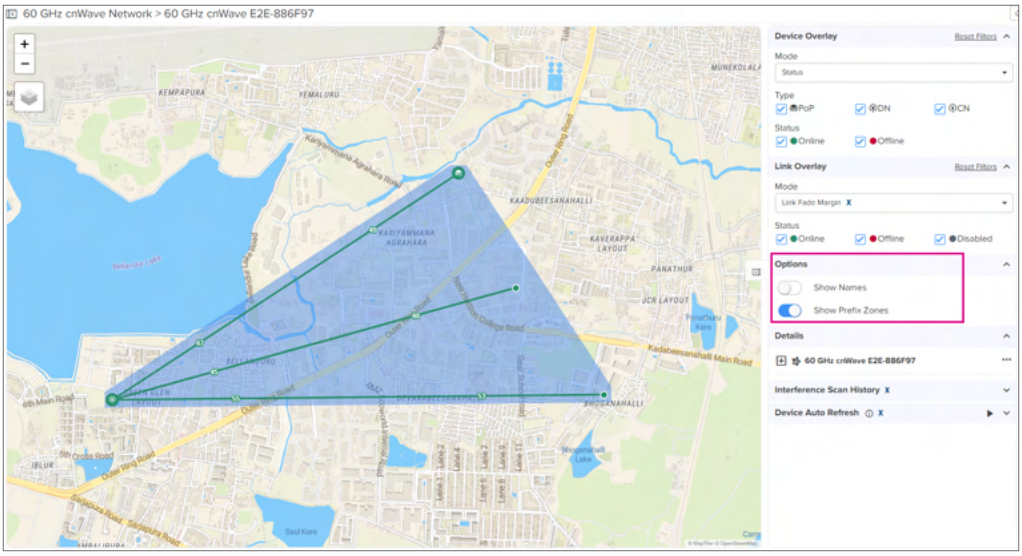
Options

The Options field supports UI controls to toggle between **Show Names** and **Show Prefix Zones**, as described**:**

- **Show Name**: shows the name of the nodes available in the E2E Network.



- **Show Prefix Zones**: shows the prefix zone of each PoP that is communicating with each other.

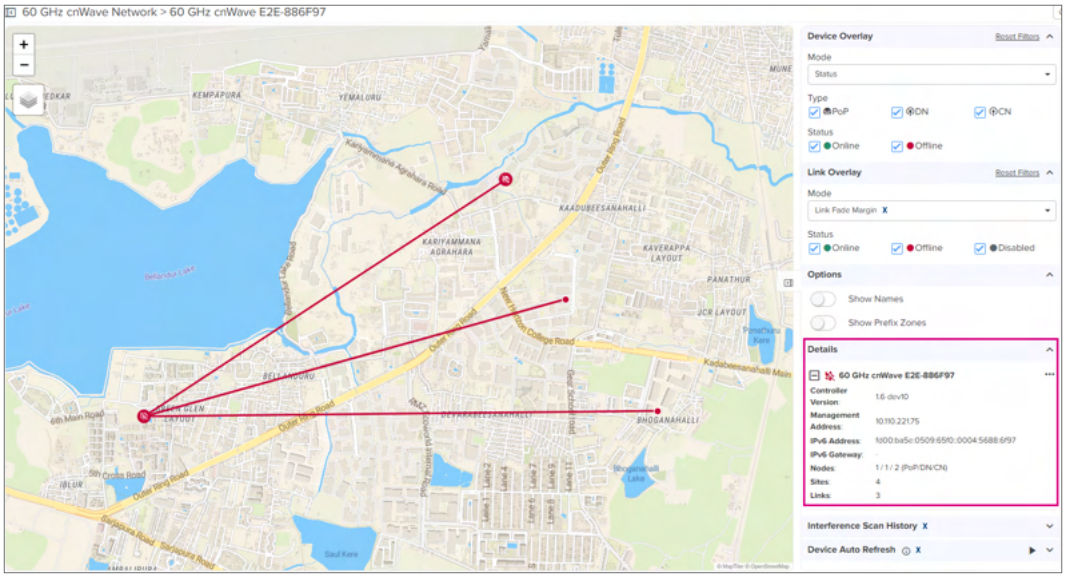


Note

Show Prefix Zones is enabled only if **Prefix Allocation** is set to **Deterministic**.

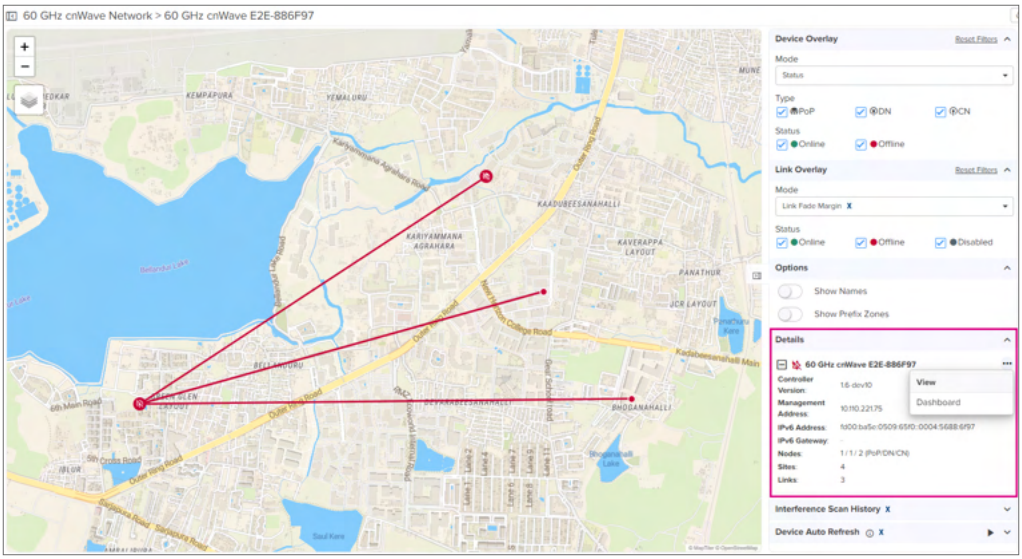
Details

The **Details** field displays the basic details of E2E Network when E2E Network is selected from the tree.



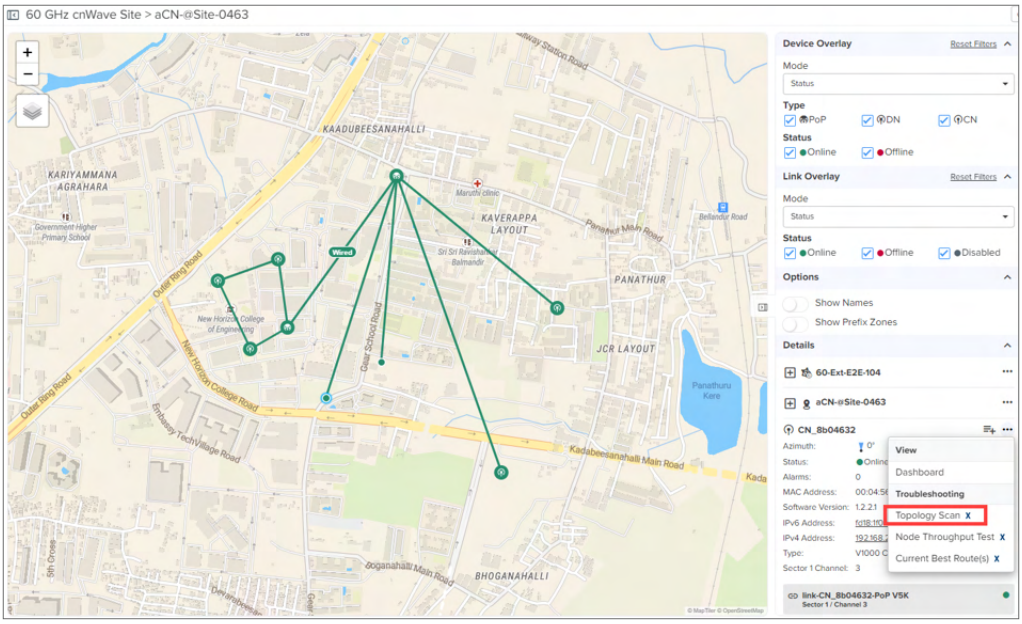
To view the details of nodes and links, complete the following steps:

1. Click the (•••) icon in the **Details** section to view E2E Network Dashboard.



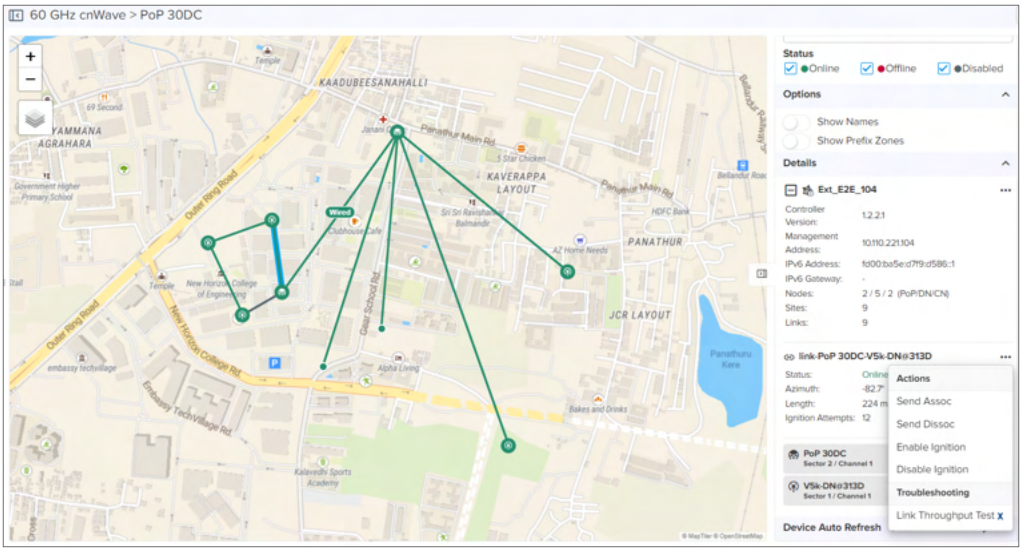
   When a device is selected from the map, the device details are displayed.

2. Click the ••• icon next to the device to view the device **Dashboard** and **Topology Scan.** For more details on how to troubleshoot a node using Topology Scan refer Topology Scan



Refer to Node Throughput Test and Current Best Routes in the Troubleshooting section.

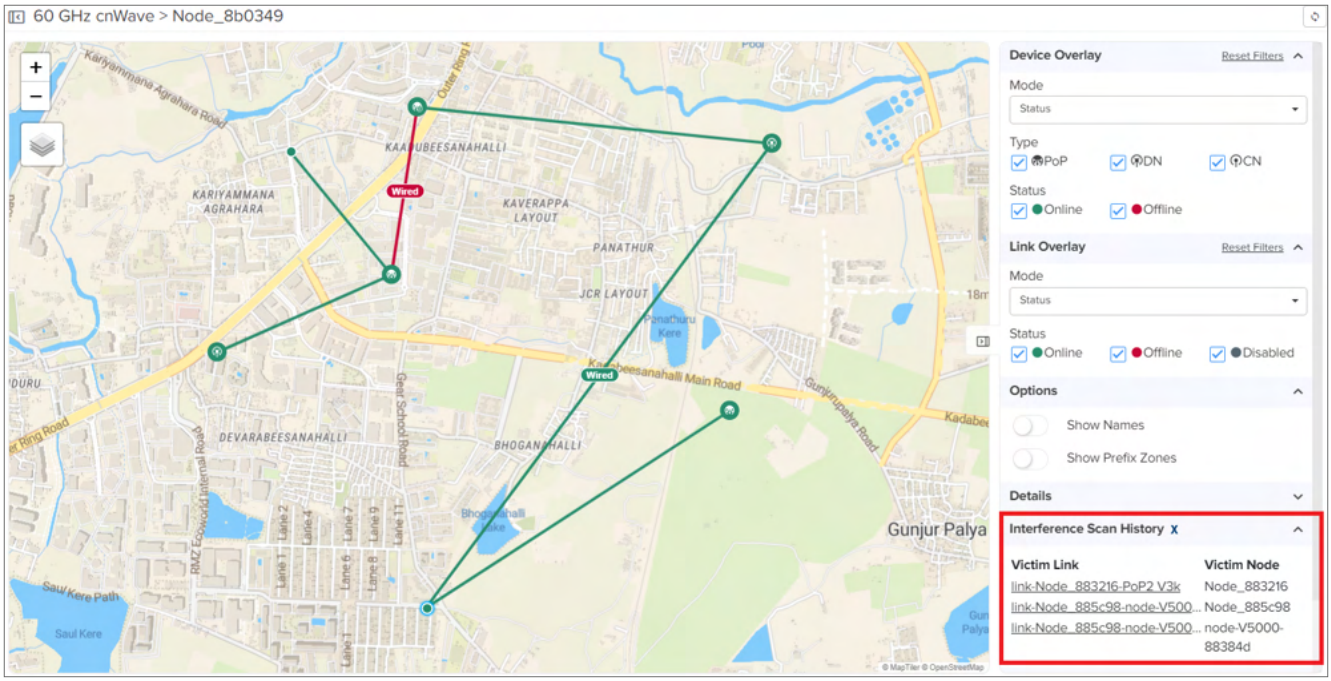
3. When a link is selected from the map, link details are displayed. Click ellipsis (•••) icon next to link to view the **Actions** details for the links.



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**.
3. Click the ⊖ icon to remove devices from **Auto Refresh**.

Note

- Channel and Polarity mode type are available for cnMaestro X users only.
- Airtime%, Golay, SNR, RSSI, MCS, Link Fade Margin, and Throughput (Mbps) are cnMaestro X features.

Using the **Details** section on the Map page, you can perform the following actions:

- Troubleshooting
- Changing channel or Golay for specific 60 GHz cnWave links
- Setting the Last Resort Metric (LRM) for a cnWave 60 GHz link

Troubleshooting

The **Troubleshooting** action allows you to run the following tests:

- Topology Scan
- Node Throughput Test
- Current Best Routes X

- Link Throughput Test X
- Interference Scan X

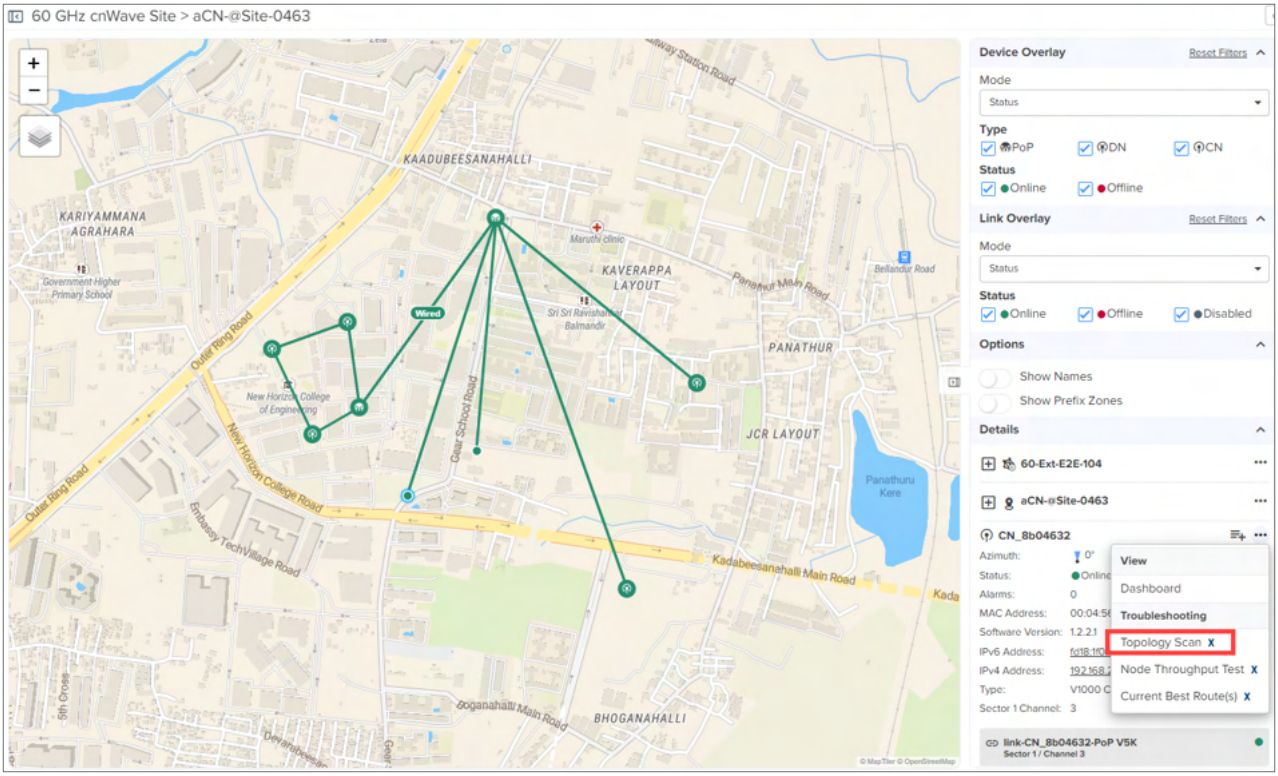
Topology Scan

Topology Scan X allows you to discover your entire network and create comprehensive, detailed network topology maps. This tool will only detect nodes operating in responder mode. It will not detect CNs with a wireless link already established. Offline nodes with a configured channel override will not be detected on a different channel.

Note

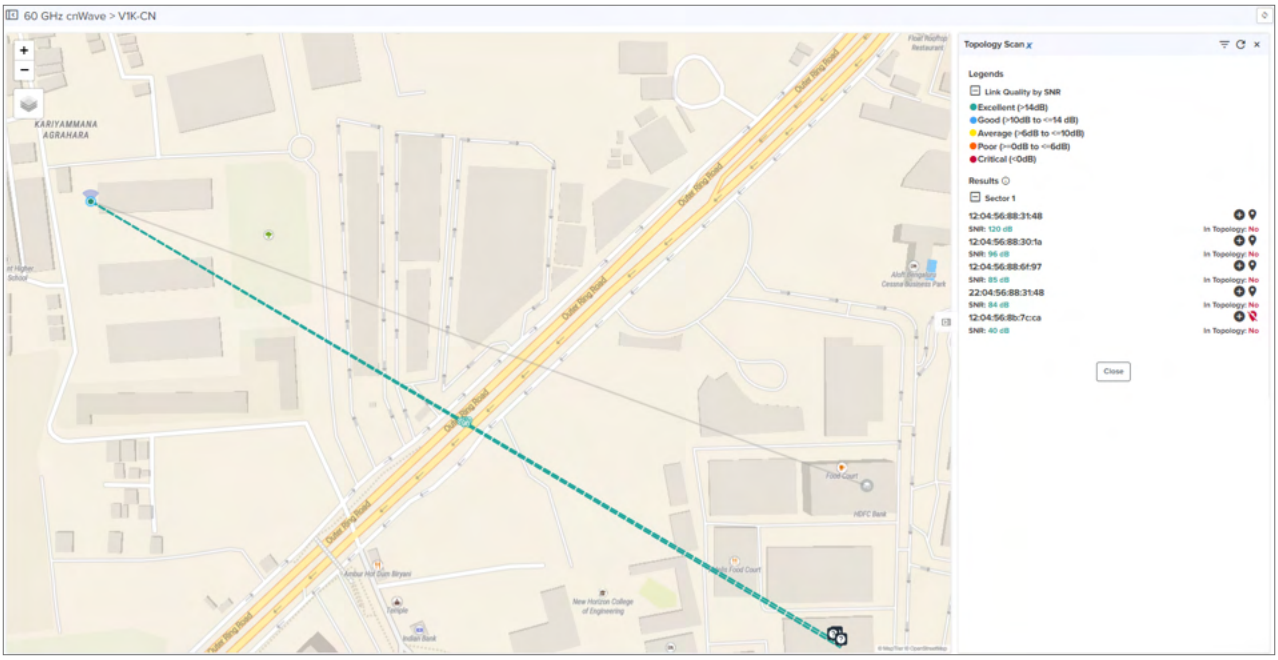
Topology Scan will cause a momentary throughput reduction in nearby links.

1. Select a node from the Map.
2. Click ellipsis (•••) icon next to the device to select the **Troubleshooting** > **Topology Scan.**



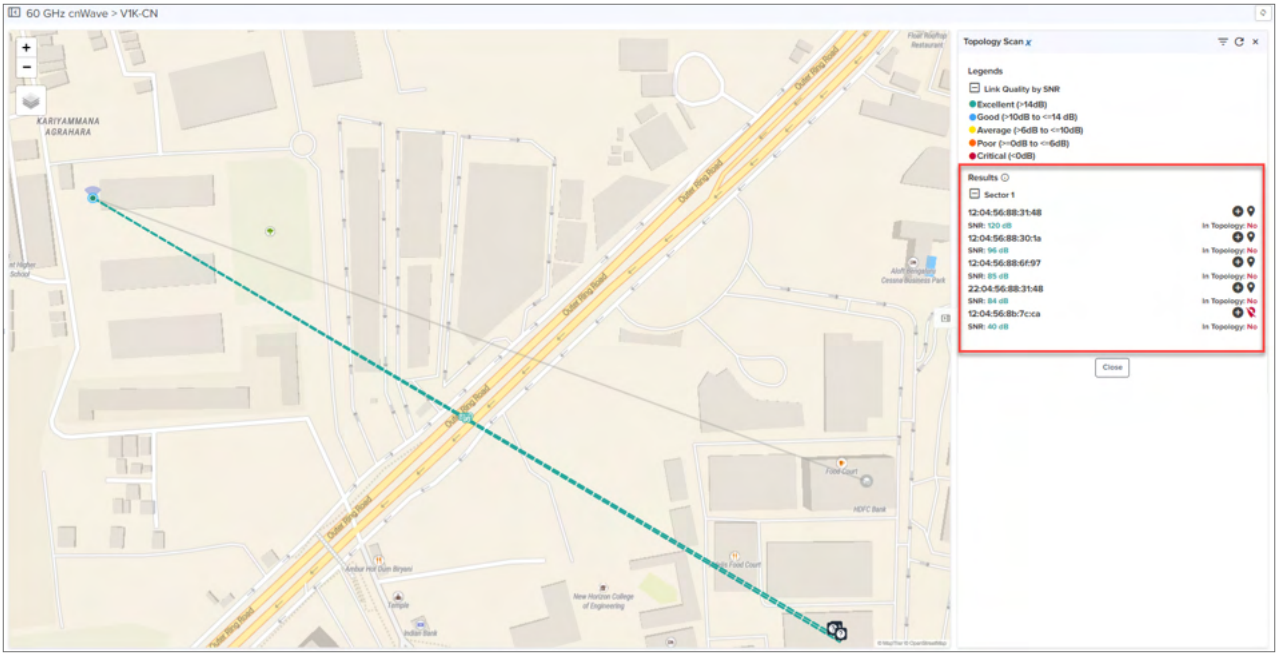
Topology Scan preview window is displayed towards the left pane.

3. Click **Start Topology Scan**. Topology Scan begins as shown in the following figure.



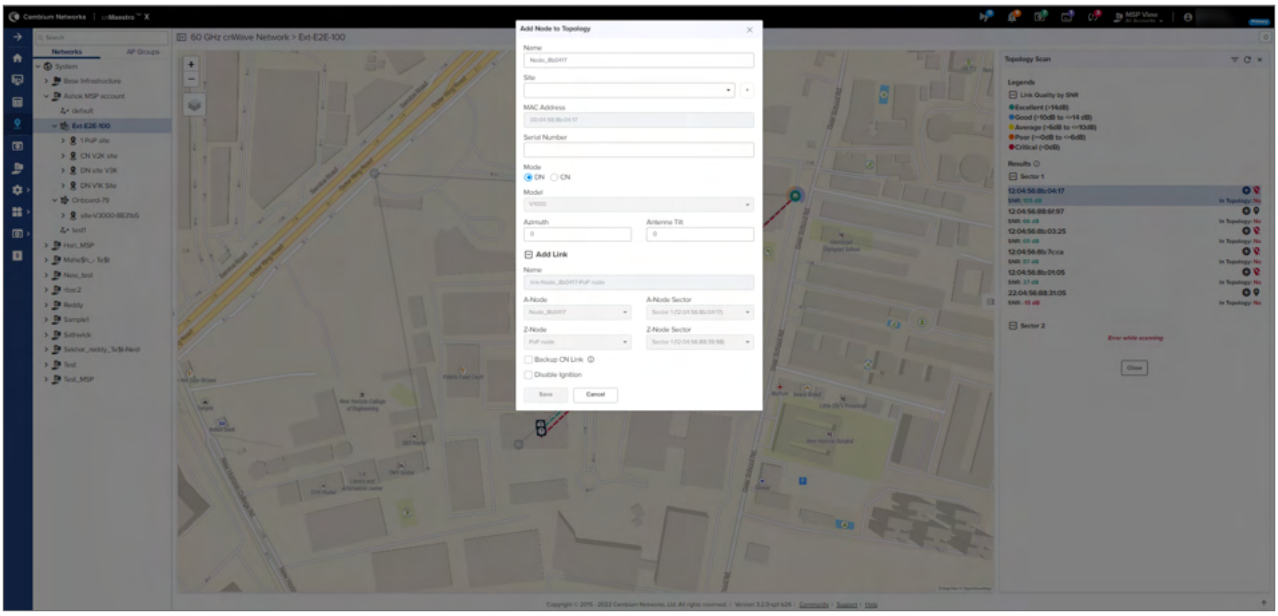
4. Click **Configure SNR Limit** ( ) next to **Topology Scan** header to add new value or reset the existing value. By default SNR value is 5 dB.
5. Click ( ) refresh icon to scan again.

   The results are based on **Link Quality by SNR** and the results are shown in the left pane. MAC Address of the links and the Link Quality is displayed.



   After topology scan, map displays available nodes and links in the network by Link Quality color codes. Only links available with GPS coordinates are shown in the map. You can add site, node, and link to the topology by clicking the plus sign **In Topology.**

6. **Add Node to Topology** window pops up.



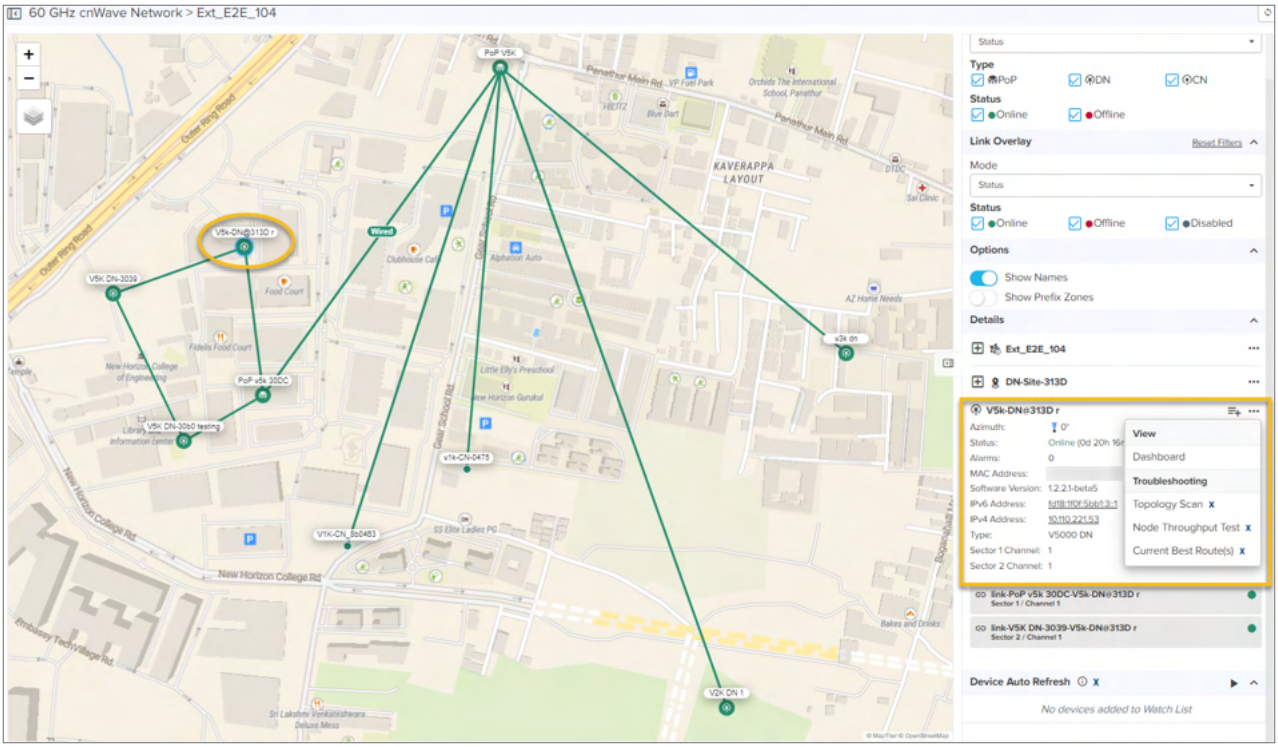
7. Enter the node and link details and click **Save**.

Node Throughput Test X

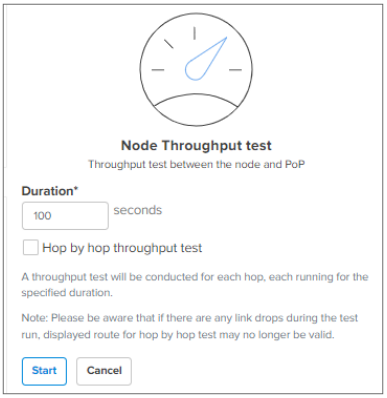
The **Node Throughput Test X** option allows you to test the throughput between a node and PoP. Using this option, you can conduct a throughput test for each hop seamlessly.

To run a node throughput test, complete the following steps:

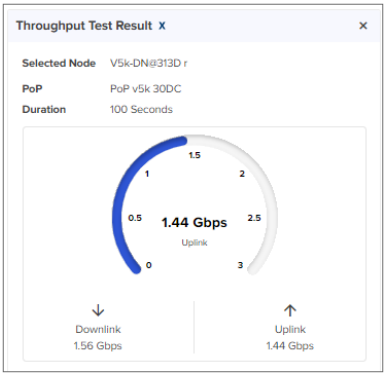
1. Select a device except the POP Node from the Map.

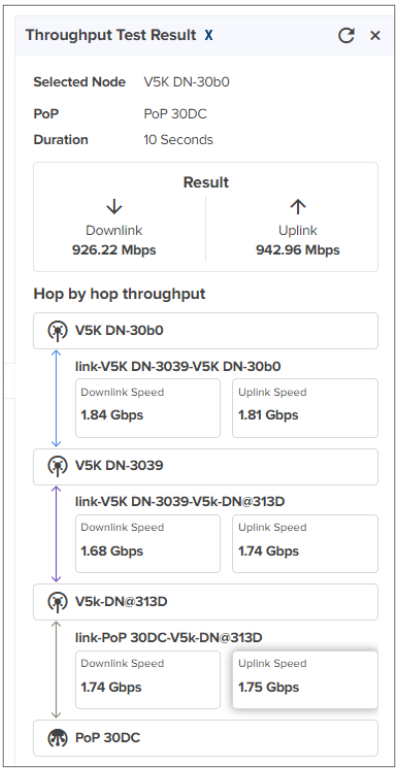


2. Click ellipsis (•••) icon next to the device name in the right pane, and select **Troubleshooting** >**Node Throughput Test X**



3. Enter the **Duration** between 5 to 300 seconds.
4. Select the **Hop by hop throughput test** checkbox to view the throughput for each hop separately.
5. Click **Start**.





Current Best Route(s) X

The Current Best Route(s) X feature is used to view the best route from a CN/DN to PoP. The **Current Best Route (s) X** map view displays statistics of the following parameters for uplink and downlink of wireless link of a node:

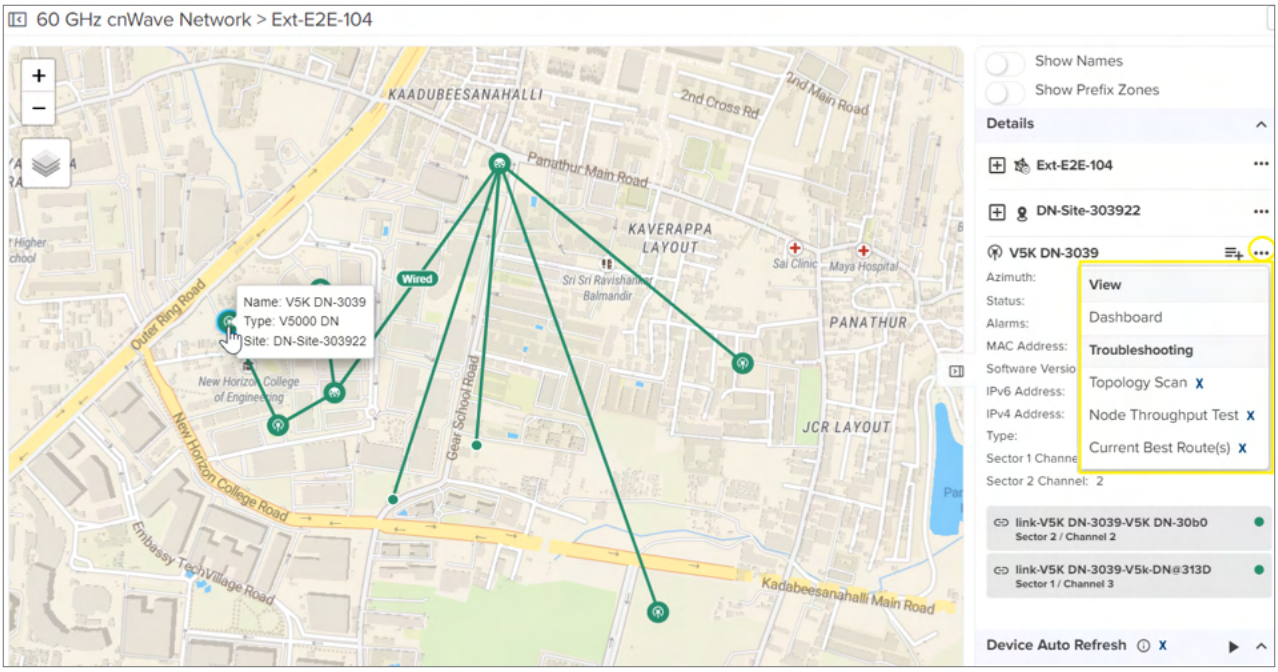
- Golay
- SNR
- MCS
- RSSI
- Throughput (Mbps)
- Airtime (%)
- Link Fade Margin (LFM)

Note

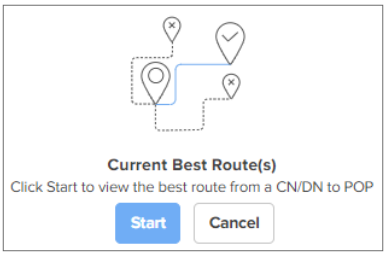
The **Current Best Route(s) X** feature is applicable only to X accounts. In addition, this feature is supported only on the E2E Controller (Onboard or external) running with software version 1.2.2.1 or later.

To view the current best routes, complete the following steps:

1. On the **Map** page, select a device node. The node details are displayed on the right side of the map.



2. Click the ••• icon next to the node name, and select **Troubleshooting** > **Current Best Route(s) X**. The **Current Best Route(s)** screen appears on the right side of the map.



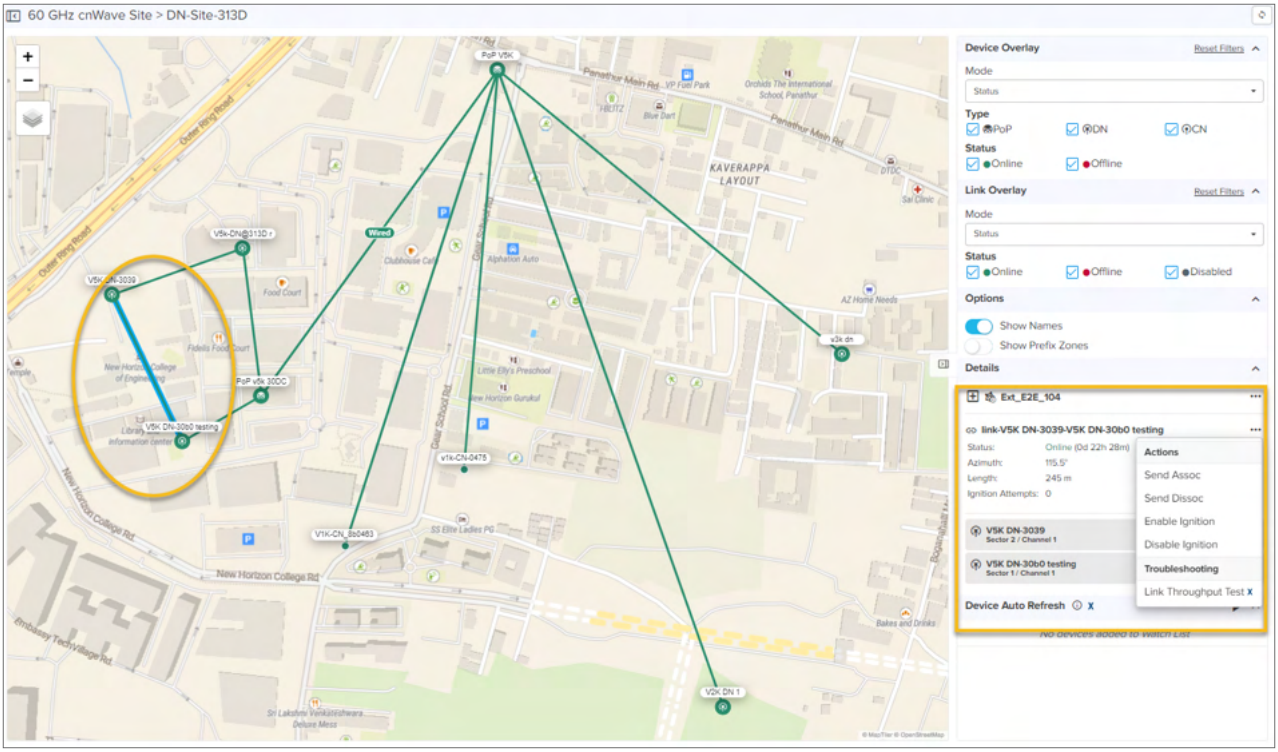
3. Click **Start**. The **Current Best Routes(s) X** section displays route details for the selected node.



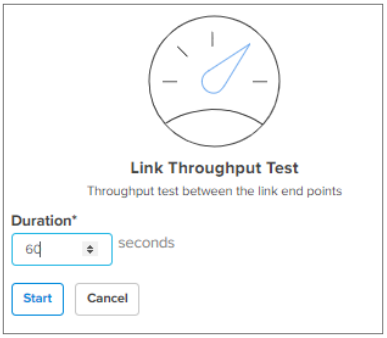
Link Throughput Test X

The **Link Throughput Test X** option allows you to test the throughput between the link end points. To run a link throughput test, complete the following steps:

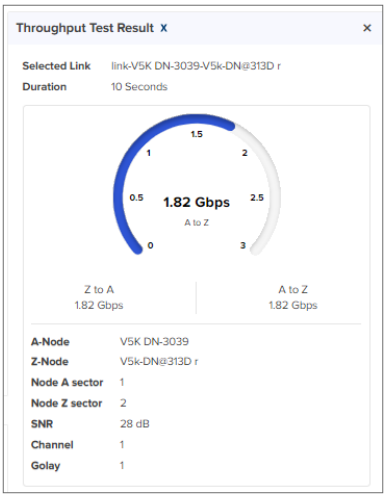
1. Select a Link from the Map.



2. Click ellipsis (•••) icon next to the link, and select the **Troubleshooting** >**Link Throughput Test X**



3. Enter the **Duration** between 5 to 300 seconds.
4. Click **Start**.



Interference Scan X

Interference Scan (also known as Interference Management (IM) Scan) is an end-to-end, Controller-coordinated scan that aims at performing real-time measurements of interference affecting a specific interfered link (referred to as the victim link). The Controller filters the network topology to identify potential interfering links (known as aggressor links).

The Controller then issues batches of scan requests to the filtered aggressor nodes or sectors. These requests are transmitted using the antenna beams and transmit power intended for their data links. Meanwhile, the victim receiver listens for these scan requests (transmissions). The extent to which the victim receiver detects these scan requests determines the level of interference exerted by the aggressor links on the victim receiver.

Note

The **Interference Scan X** feature is applies only to X accounts and is available for 60 GHz cnWave software version 1.5 and later.

Output of Interference Scan

Using the cnMaestro UI, you can run the Interference Scan tool. The scan results show the victim link and its corresponding receiver MAC address (which serves as a unique identifier for the network devices).

It also provides a list of aggressor links along with their corresponding Signal-to-Noise Ratio (SNR) values relative to the victim receiver. SNR indicates the measurement of a signal strength compared to background noise, with higher values indicating better signal quality.

Impact on link performance

The interference from aggressor links impacts the maximum data rate that the victim link can achieve, determined by the Modulation and Coding Scheme (MCS). For instance, achieving MCS9 requires an SNR of at least 10 dB. However, if interference from an aggressor link reduces the SNR to 6 dB, the victim link will be limited to MCS4 or lower, resulting in slower data rates.

If the SNR is less than 0 dB, the interference is minimal and the aggressor links are unlikely to impact the victim link's performance.

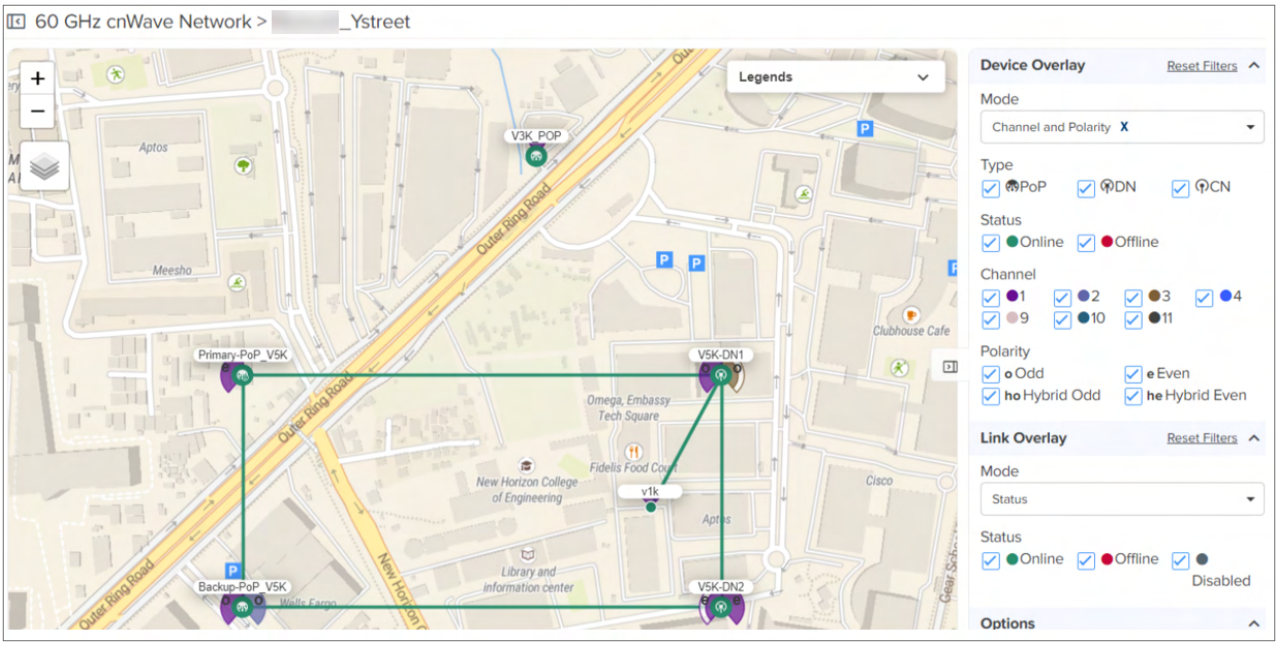
Running the Interference Scan tool

You can run the Interference Scan tool using the **Map** page in cnMaestro UI only. You can also view the last three scanned results for the cnWave network in the **Interference Scan History X** section in the **Map** page.

To run the Interference Scan tool, complete the following steps:

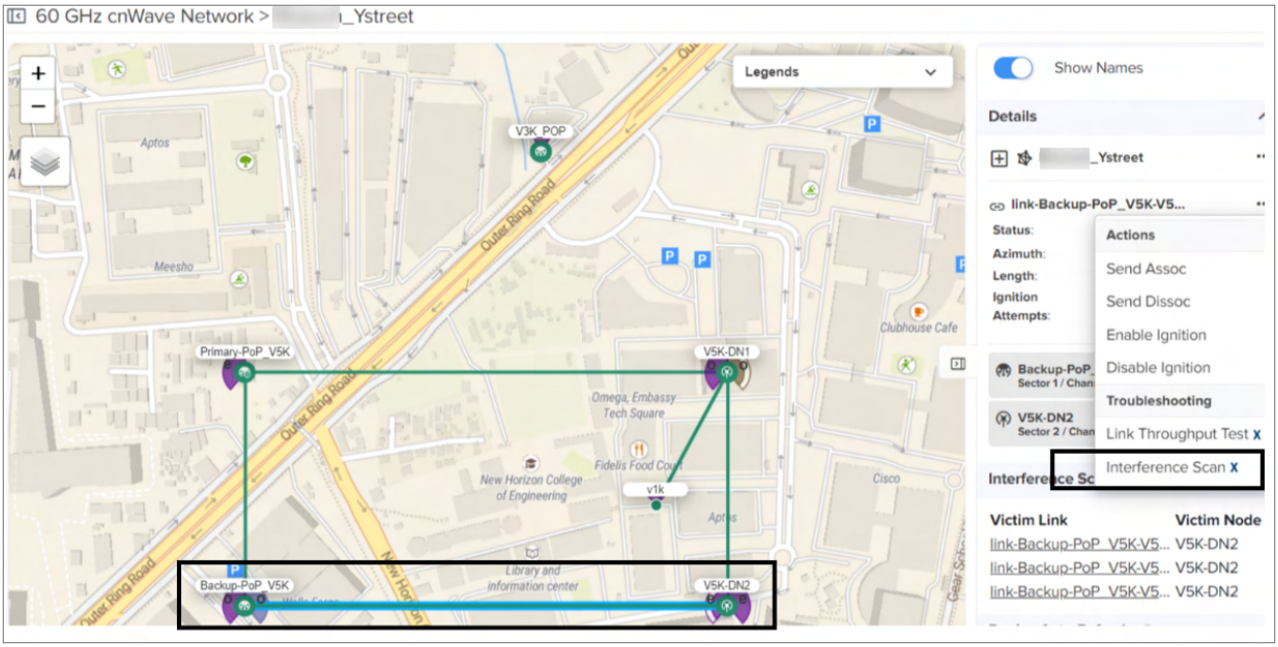
1. On the **Map** page, select a cnWave network and click on the link for which you want to run the interference Scan tool.

   The **Details** section on the right side of the **Map** page displays the selected link information. For example, there is a Backup-POP_V5K linked to V5K-DN2 in the figure shown below.

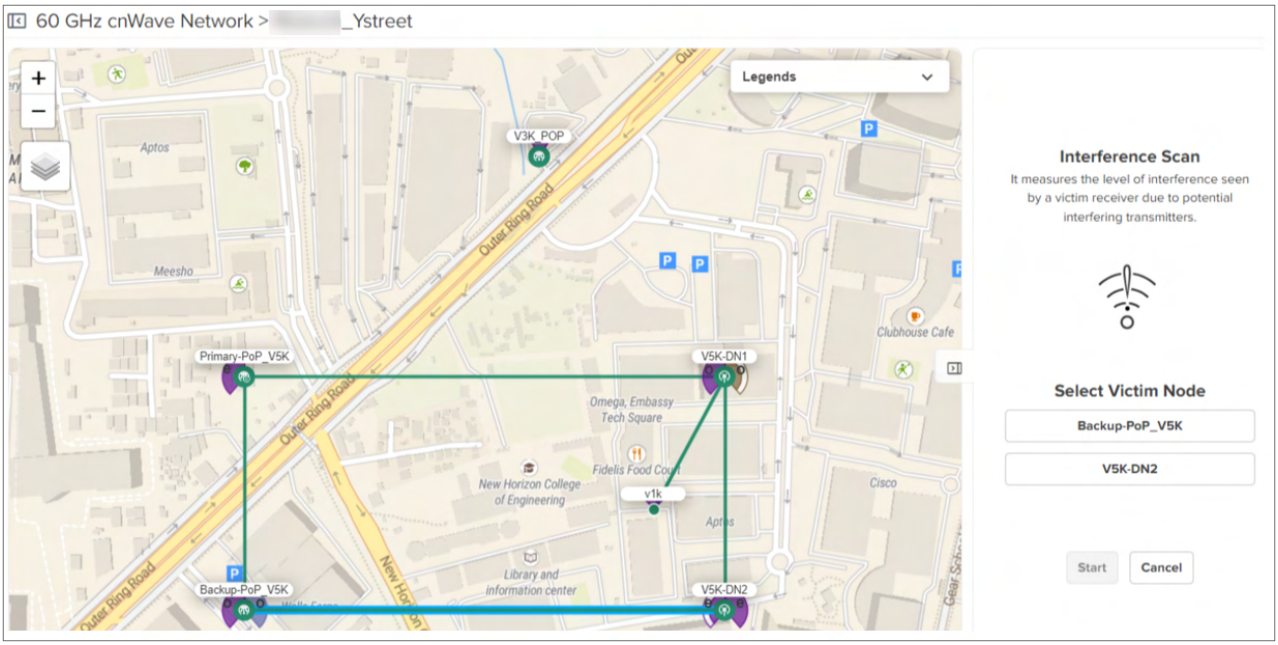


2. Click the ••• icon next to the link name and select **Interference Scan X** from the dropdown list.

   For example, Interference Scan is used for the link highlighted between Backup-POP_V5K linked to V5K-DN2 in the figure shown below.

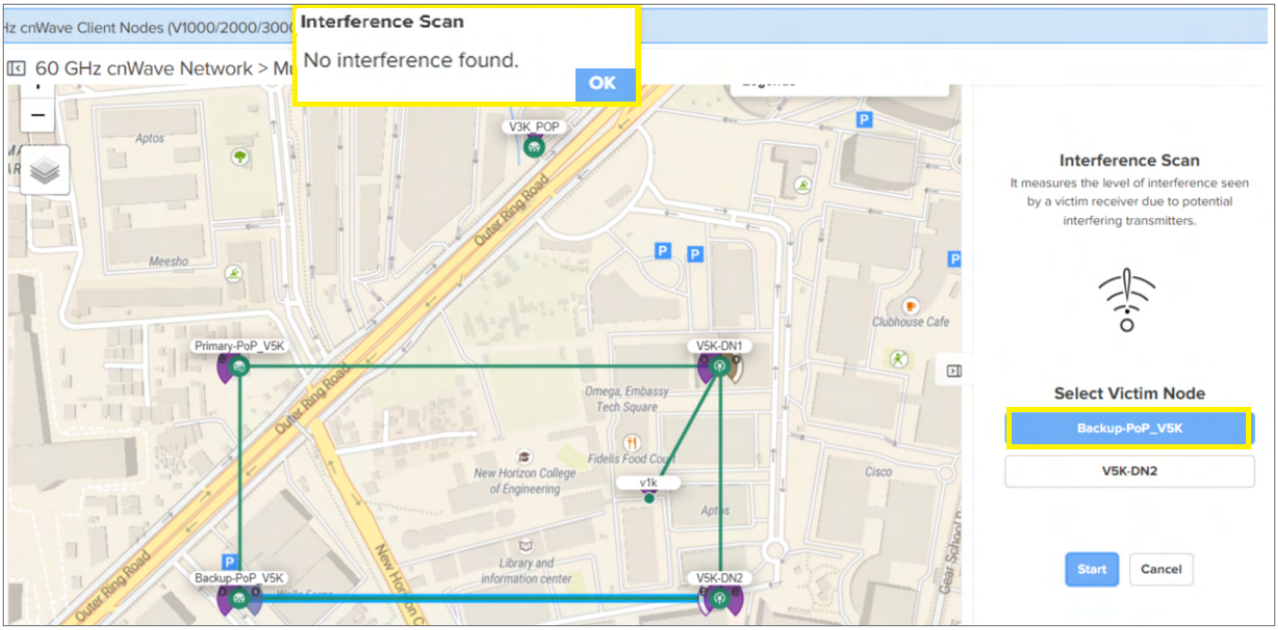


   When **Interference Scan X** is selected, the **Interference Scan** section appears with the victim node names on the right side of the Map page (as shown in the figure below).



3. Select the required victim node and click **Start**.

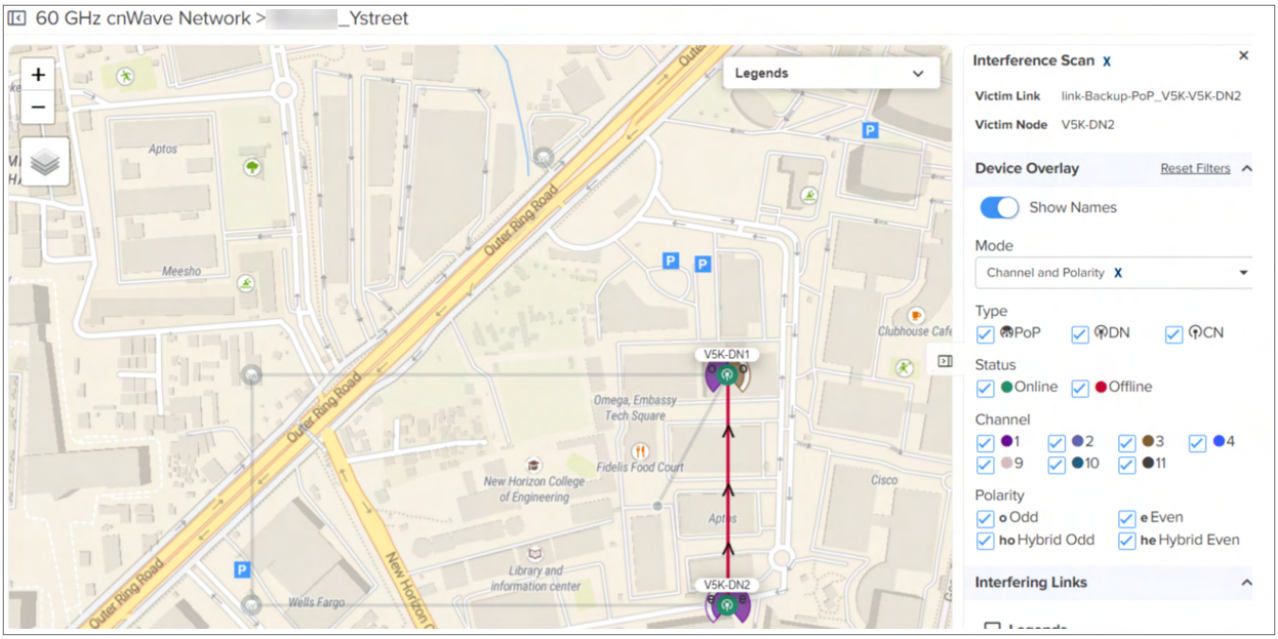
   The Interference Scan tool detects neighboring interfering links with wireless settings that may affect your network. The Interference Scan tool can be executed on any of the victim nodes. In the figure below, Interference Scan is executed on the first victim node Backup-POP_V5K. If no aggressor is found, a message appears stating that **no interference found**.



When you run the Interference Scan test on the second victim node (for example, V5K-DN2), the aggressor (if any) details are displayed as shown in the figure below. In this case, Backup-POP_V5K to V5K-DN2 uses channel 1 and V5K-DN2 to V5K-DN1 uses channel 1. The SNR values need to be analysed.

Note

The cnMaestro UI displays both a map view and a list view of the victim-aggressor relationship. The map is color-coded to show the severity of interference. The lower the SNR from aggressor links, the greater the interference on the victim link.



4. View the scan result for the selected victim node and take appropriate actions.

Changing channel or Golay for specific 60 GHz cnWave links

You have options on the **Maps** page in cnMaestro to perform the following operations:

- Change Channel for all links connected to a particular sector.
- Change Golay for a particular link connected between two nodes.

These operations help you to refrain from configuring the radio link for each node when there is any interference.

Change Channel

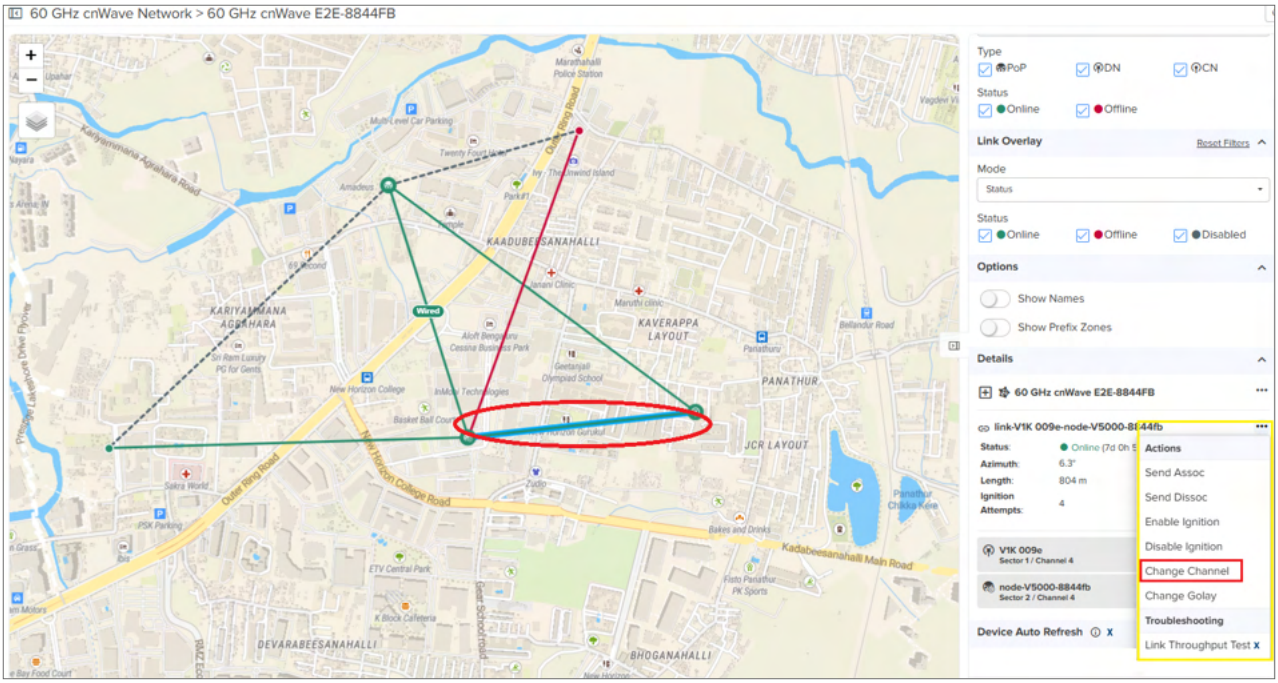
There may be an interference issue found when all the 60 GHz cnWave links in a **particular sector** have the same channel. In such a scenario, you can update or change the channel for all the links of a particular sector using the **Maps** page in cnMaestro UI.

Complete the following steps to change the channel:

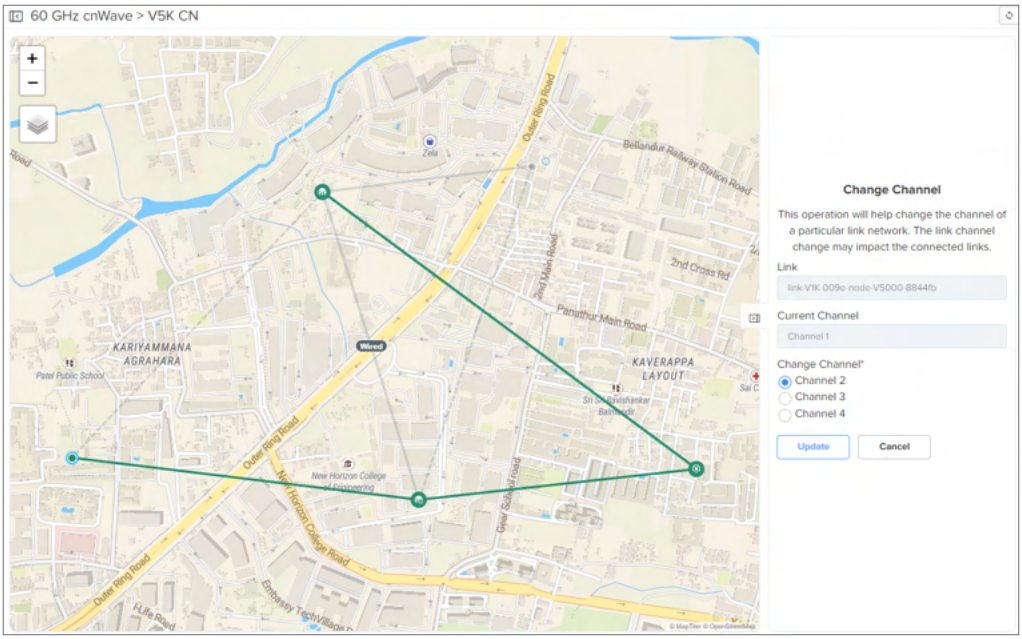
1. On the **Map** page, select a cnWave network and click on the link for which you want to change the channel.

   The **Details** section on the right side of the **Map** page displays information for the selected link.

2. Click the ••• icon next to the link name and select **Change Channel** from the **Actions** dropdown list.



When you select **Change Channel**, a screen appears on the right side of the **Maps** page displaying the current channel number used by the selected link. The Maps section highlights the other links that are using the current channel number in that particular sector.



3. Select the channel number and click **Update**.

   The **Confirm** message box appears, indicating that the channel change is applicable to the highlighted links.

4. Click **Continue**.

   A message appears, indicating the channel change is successful for the group of links in a sector.

Change Golay

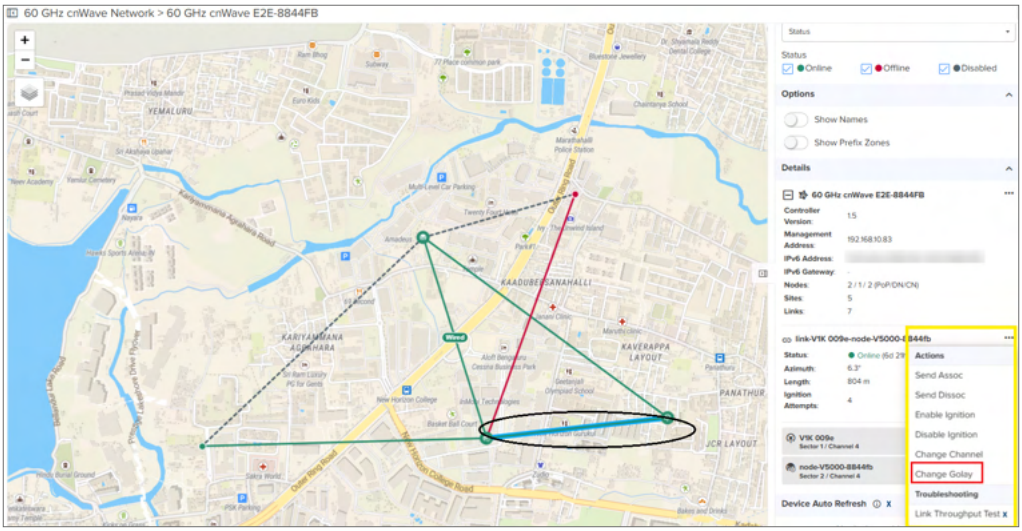
Using the **Maps** page in cnMaestro UI, you can change the Golay code for a **particular 60 GHz cnWave link** established between two nodes (not a sector) to avoid interference. Complete the following steps to change the

Golay:

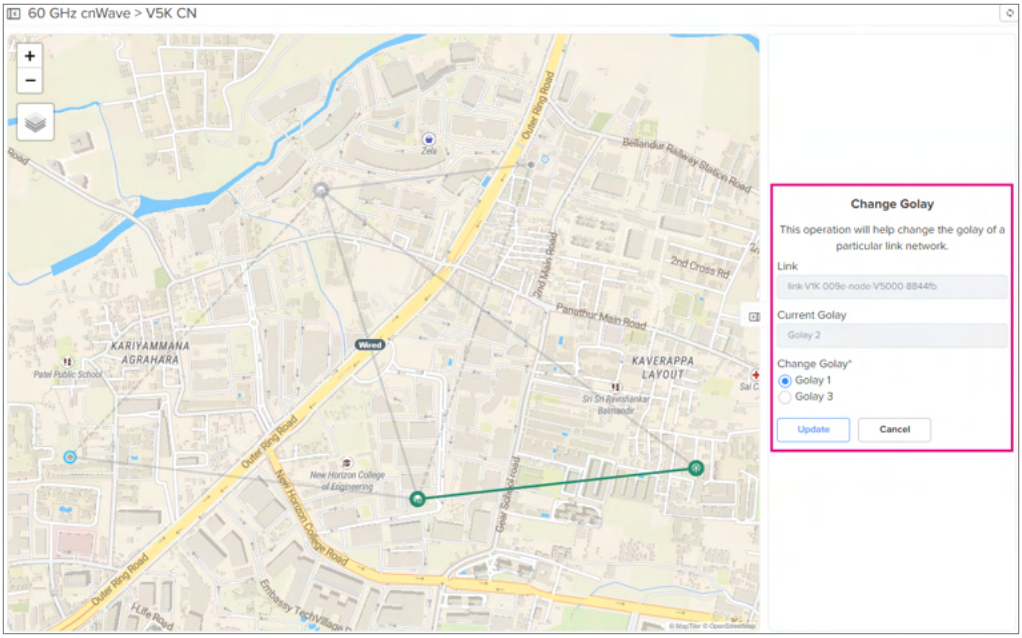
1. On the **Map** page, select a cnWave network and click on the link for which you want to change the Golay code.

   The **Details** section on the right side of the **Map** page displays information for the selected link.

2. Click the ••• icon next to the link name and select **Change Golay** from the **Actions** dropdown list.



When you select **Change Golay**, a screen appears on the right side of the **Maps** page displaying the current Golay code used by the selected link.



3. Select the required Golay code for the selected particular link.
4. Click **Update**.

   The **Confirm** message box appears, indicating that the Golay change is applicable to the particular link.

5. Click **Continue**.

   A message appears, indicating the Golay code change is successful for the particular link.

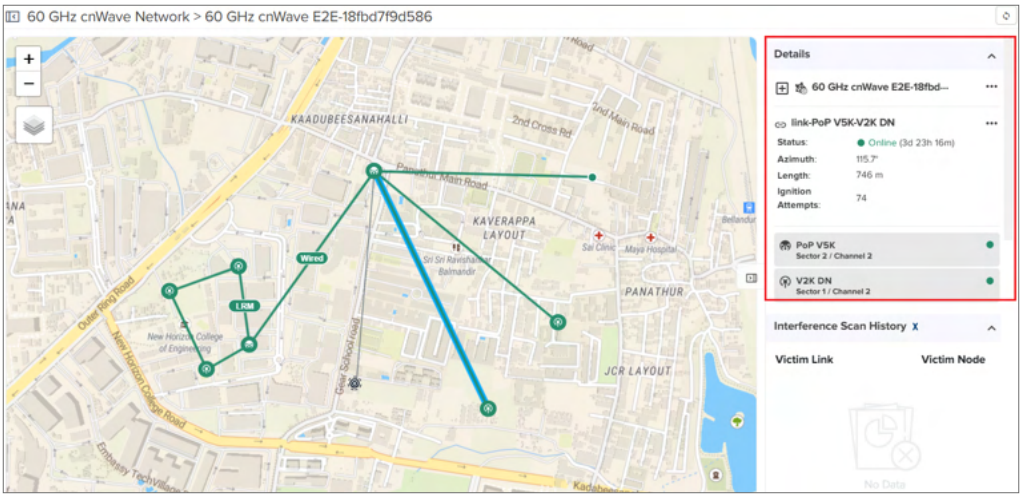
Setting the Last Resort Metric (LRM) for a cnWave 60 GHz link

You can set an extremely high Open/R metric for a wireless cnWave 60 GHz link using the **Maps** page in cnMaestro UI. This metric value is used as a last resort for routing traffic when all other paths are unavailable.

To set a last resort metric for a 60 GHz cnWave link, complete the following steps:

1. On the **Map** page, select a cnWave network and click on the link for which you want to set the last resort metric.

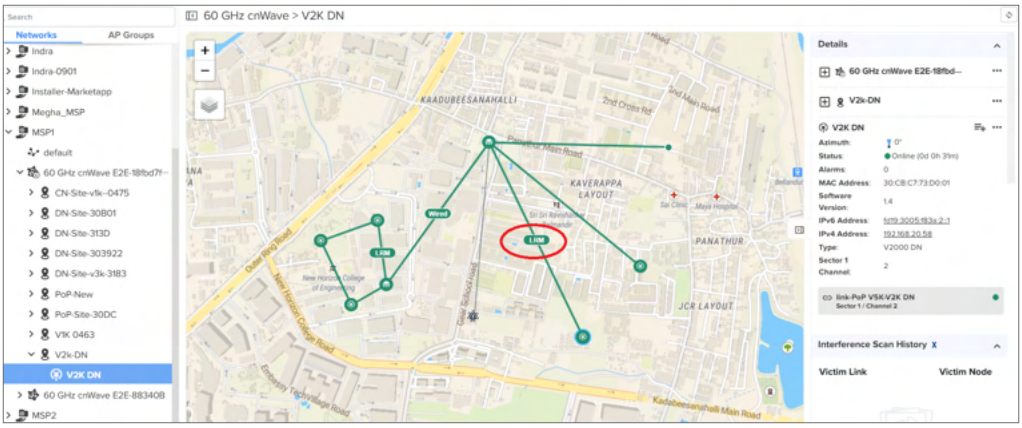
   The **Details** section on the right side of the **Map** page displays information for the selected link.



2. Click the ••• icon next to the link name and select **Set Last Resort Metric** from the **Actions** dropdown list.

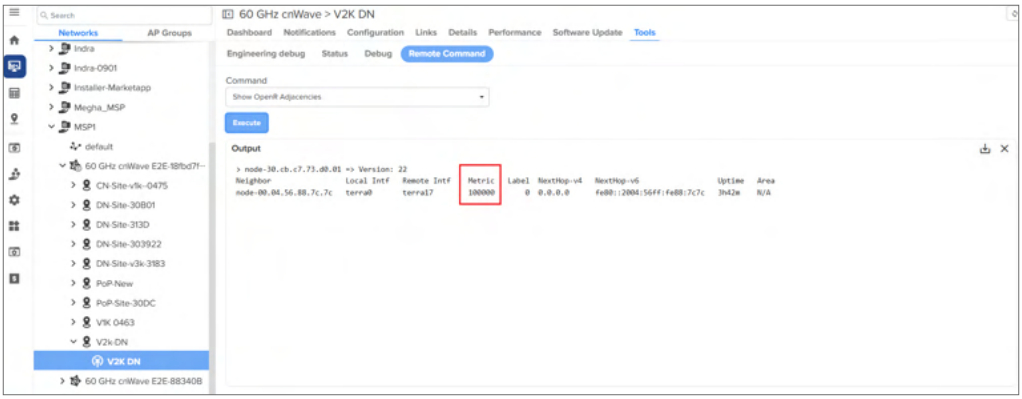


   When you select the **Set Last Resort Metric** option, a message appears indicating that the last resort metric is set successfully. You can see an **LRM** indicator on the selected link, as shown in the figure below.

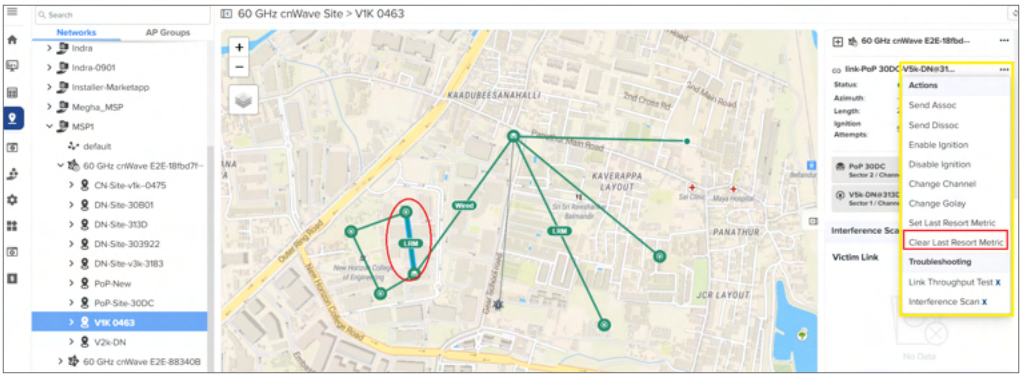


3. To verify the last resort metric that you set, navigate to the **Monitor and Manage** > **60 Ghz cnWave Network** > **Node** > **Tools** > **Remote Command**. The **Remote Command** page appears.
4. From the **Command** dropdown list, select **Show OpenR Adjacencies** and click **Execute**.

   The **Remote Command** page displays the output, indicating the last resort metric value (which is 100000). This mechanism also indicates that the link with the highest metric value is the last preferred link for routing traffic when other links are unavailable.



   For links that do not have the last resort metric set, the **Metric** field displays 1 as the value.
5. To **clear** the last resort metric for a link, select the required 60 GHz cnWave link on the **Maps** page.
6. Click the ... icon next to the link name and select **Clear Last Resort Metric** from the **Actions** dropdown list.



   When you select the **Clear Last Resort Metric** option, a message appears indicating that the last resort metric is cleared.

Tools

The Tools page allows the user to perform the following actions:

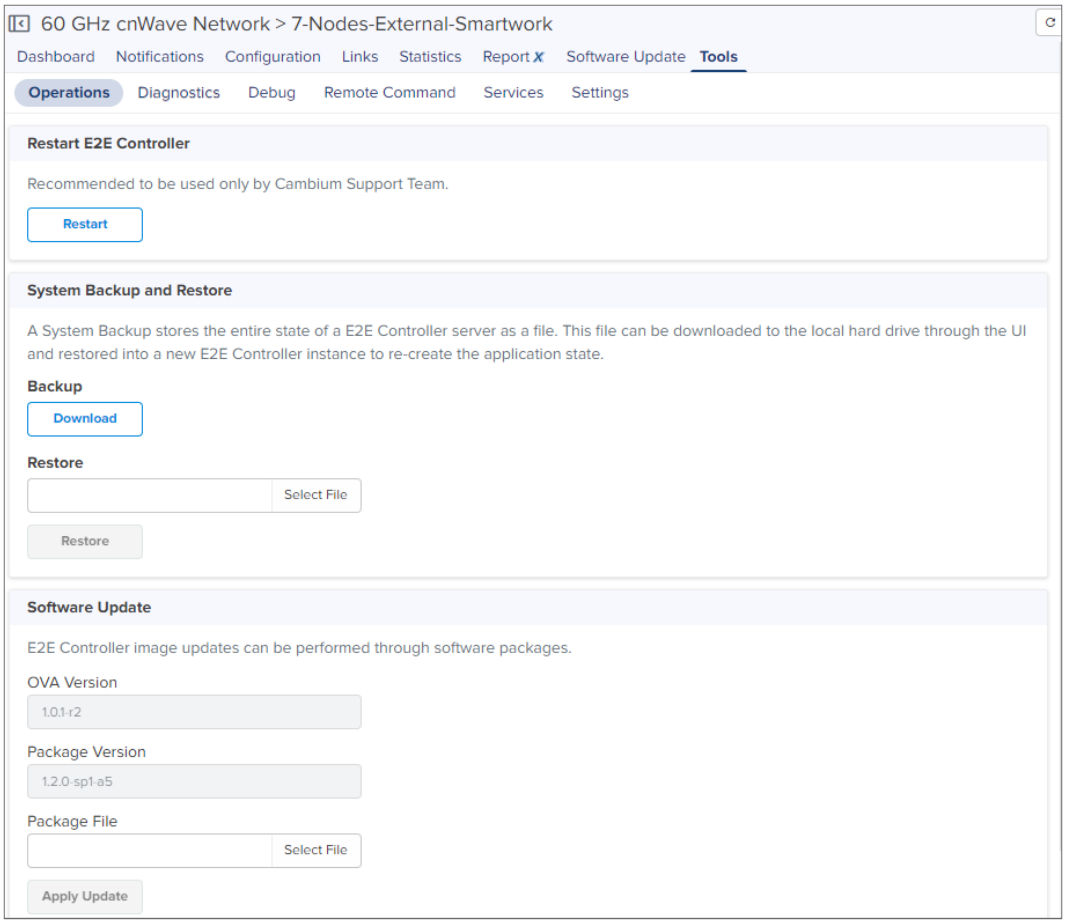
- Operations
- Diagnostics
- Debug
- Remote Command
- Services
- Settings

Operations

External E2E Controller deployment

If the device is deployed through **External E2E Controller** it displays the operations page as follows:

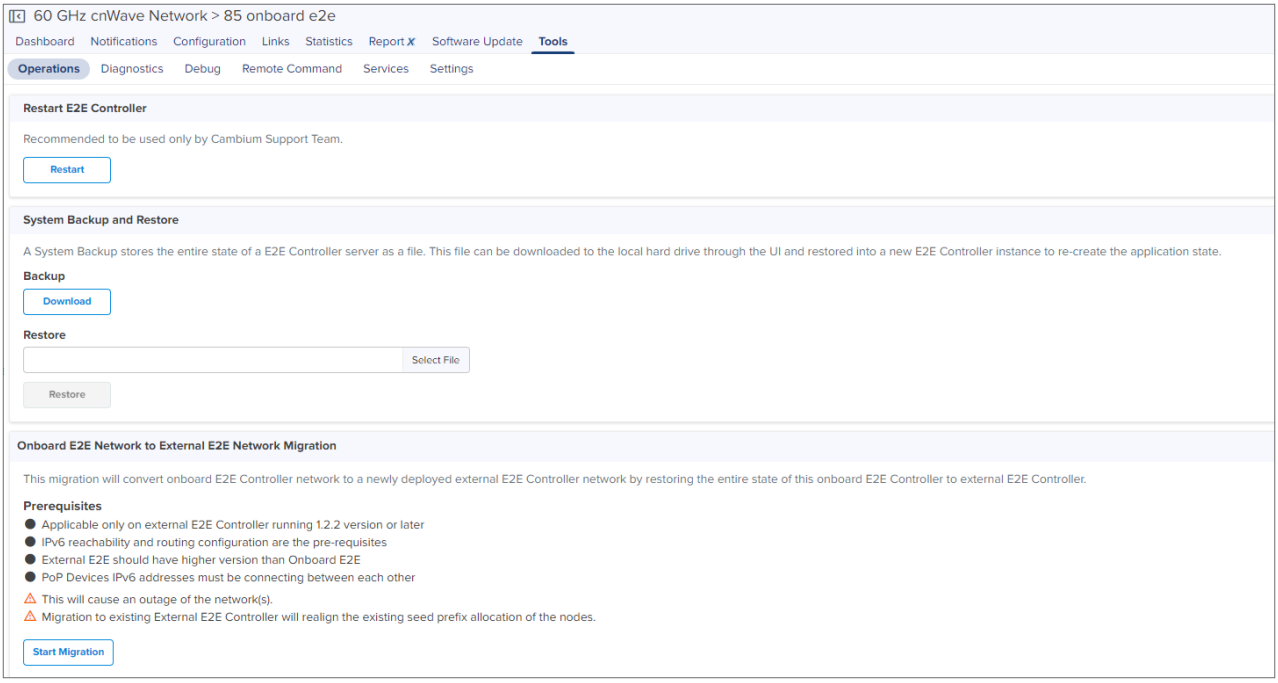
- **Restart E2E Controller** performs the **Restart.**
- A **System Backup and Restore** the entire state of a E2E Controller server as a file and file can be used to transfer data between two E2E Controller instances. It can be saved in local hard drive through the UI and restored into a new E2E Controller instance to re-create.
- The **Software Upgrade** is to upgrade E2E controller and can be done through E2E controller package.



Onboard E2E Controller deployment

If the device is running **Onboard E2E Controller** it displays the operations page as follows:

- **Operations** page allows the user to **Restart E2E Controller** and perform the **System Backup**. It also stores the entire state of a E2E Controller server as a file and file can be used to transfer data between two E2E Controller instances. It can be saved in local hard drive through the UI and restored into a new E2E Controller instance to re-create the application state.



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:

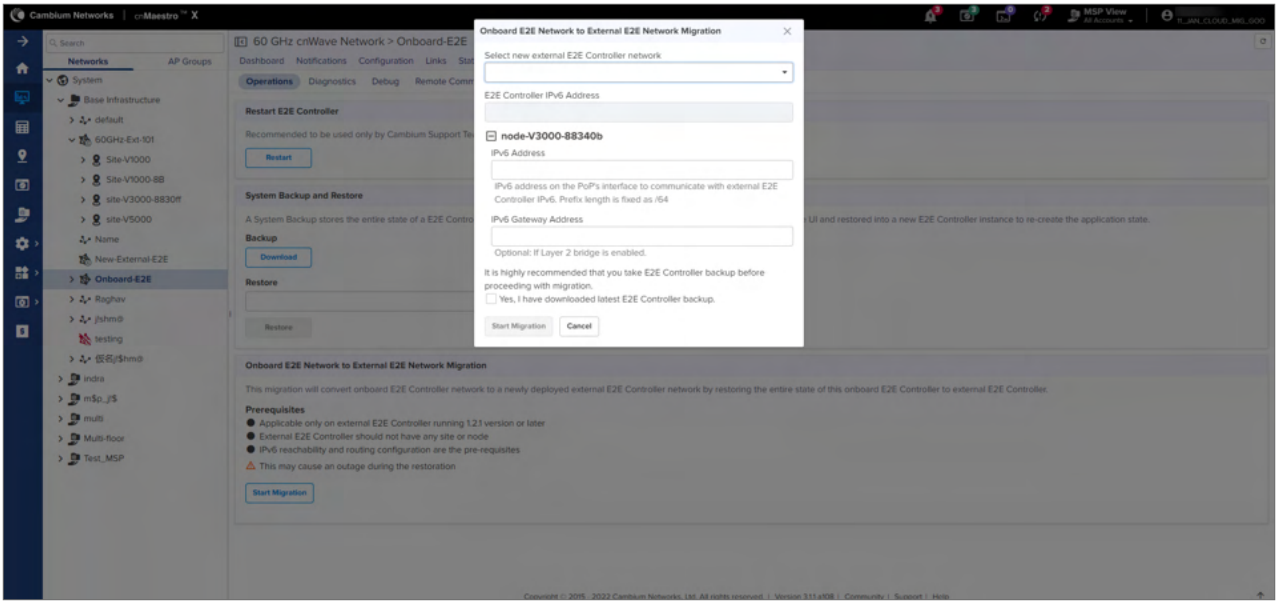
- Multi-PoP / Relay Port should be updated with the interface as in PoP interface configuration if not already done, to allow the connection between PoPs.
- If the existing E2E Network if configured with BGP, migrated PoP BGP Configuration must be updated in cnMaestro and then in POP GUI
- If the PoPs 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.

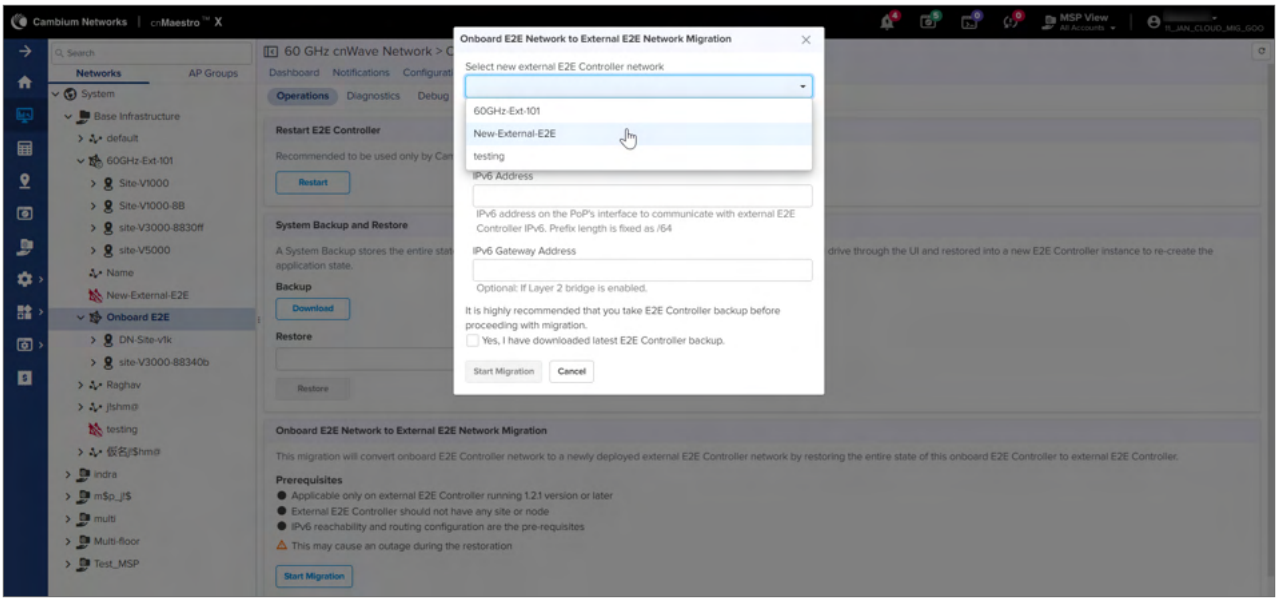
Perform the following steps to migrate Onboard E2E Controller to External E2E Controller:

1. Select Onboard E2E Network > **Tools** > **Operations.**
2. Click **Start Migration**.

   The **Onboard E2E Controller to External E2E Migration** window appears.



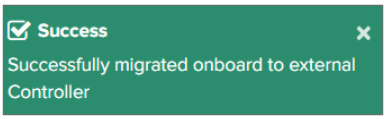
3. Select a new external E2E Controller network from the dropdown.



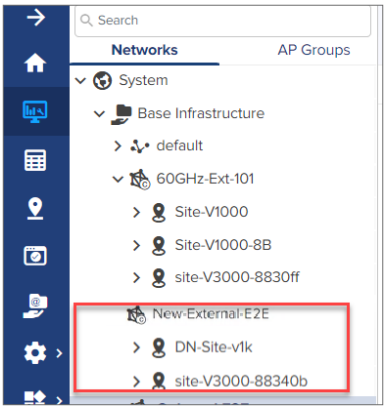
4. Enter **IPv6 Address**.
5. Enter **IPv6 Gateway Address** of PoP node, which is optional.

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.

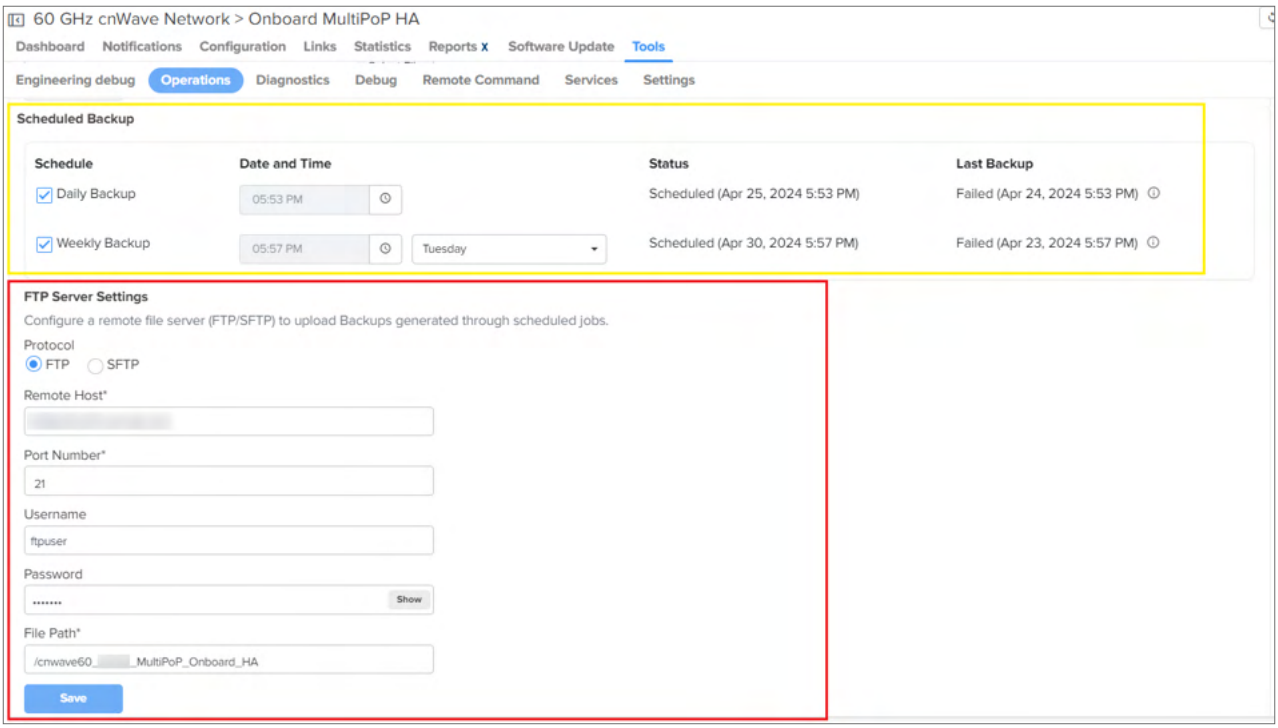


Table 88 lists the parameters required for configuring the remote FTP or sFTP server.

Table 88 *Parameters for FTP/sFTP server settings*

Parameter	Description
Protocol	File protocol (FTP or sFTP) required for uploading the backup of E2E Controller over the network. Select the required protocol.
Remote Host	The remote host name of the FTP or sFTP file server. Provide IP or DNS resolvable host name in the text box. This is a mandatory parameter.
Port Number	The port number used to allow in network firewall from a VM or device running E2E Controller service to the respective FTP or sFTP server. This is a mandatory parameter.
Username	Username to log in to the remote FTP or sFTP server.

Table 88 *Parameters for FTP/sFTP server settings*

Parameter	Description
Password	Password that is required to authenticate the remote FTP or sFTP server.
File Path	The remote file path of FTP or sFTP server where the backups are uploaded automatically on scheduling.

3. Click **Save**.

   The remote FTP or sFTP configuration is successfully updated.

4. To schedule the backup job, use the following options (either one or both) in the **Scheduled Backup** section:

   - **Daily Backup**: For the daily backup, set the time (in 24-hours format) using the **Date and Time** parameter.
   - **Weekly Backup**: For the weekly backup, set the time (in 24-hours format) and day.

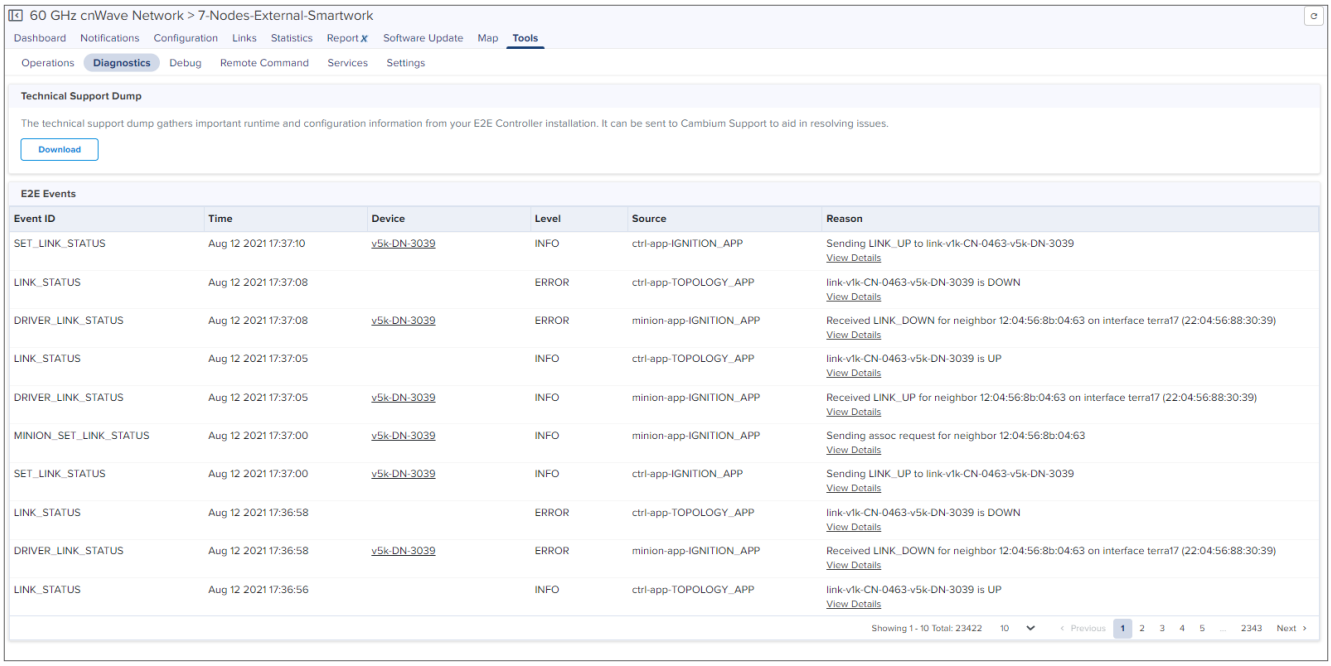
     The **Status** field in the **Scheduled Backup** section displays date and time of the scheduled job. Similarly, the **Last Backup** field displays date and time of the last failed job.

Diagnostics

Diagnostics page allows the user to gather Technical Support Dump and can be downloaded and sent to cambium support team.

All the events information of E2E controller can be viewed under E2E Events. In **E2E Events** tab user can view the **Event ID, Time, Device, Level, Source** and **Reason** of the E2E Network**.**

Figure 392 *Diagnostics*



Debug

In **Debug** tab, you can view and download the Node logs by executing the following log:

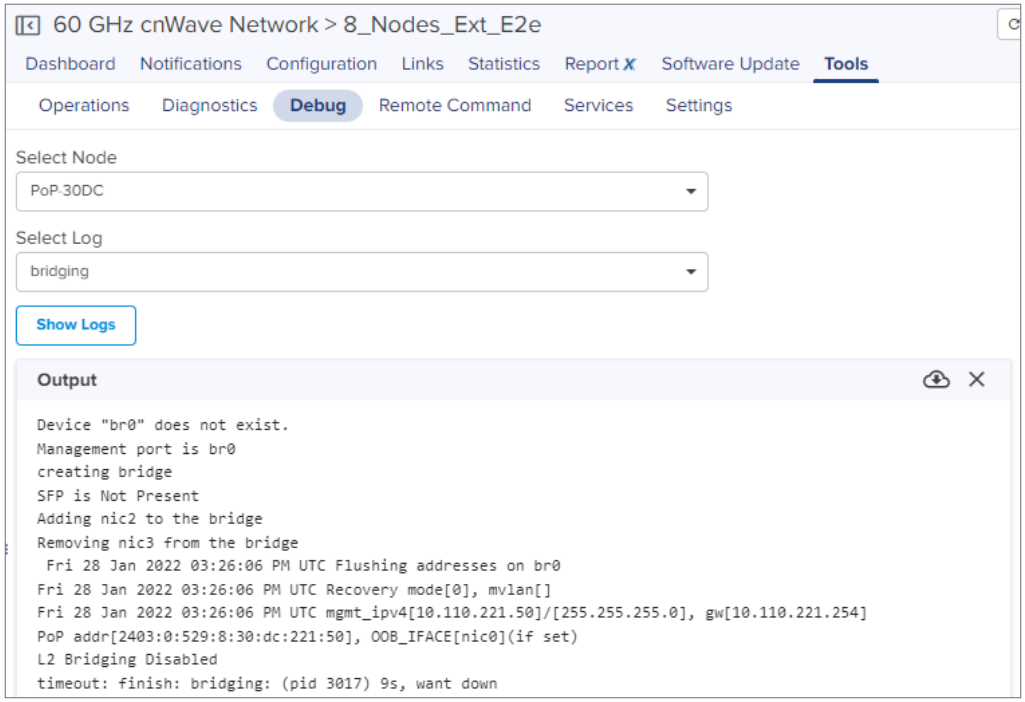
- bridging
- e2e_minion

- 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 (×) icon to clear the output.

Remote Command

In **Remote Command** tab, user can view or download command logs by executing the following command:

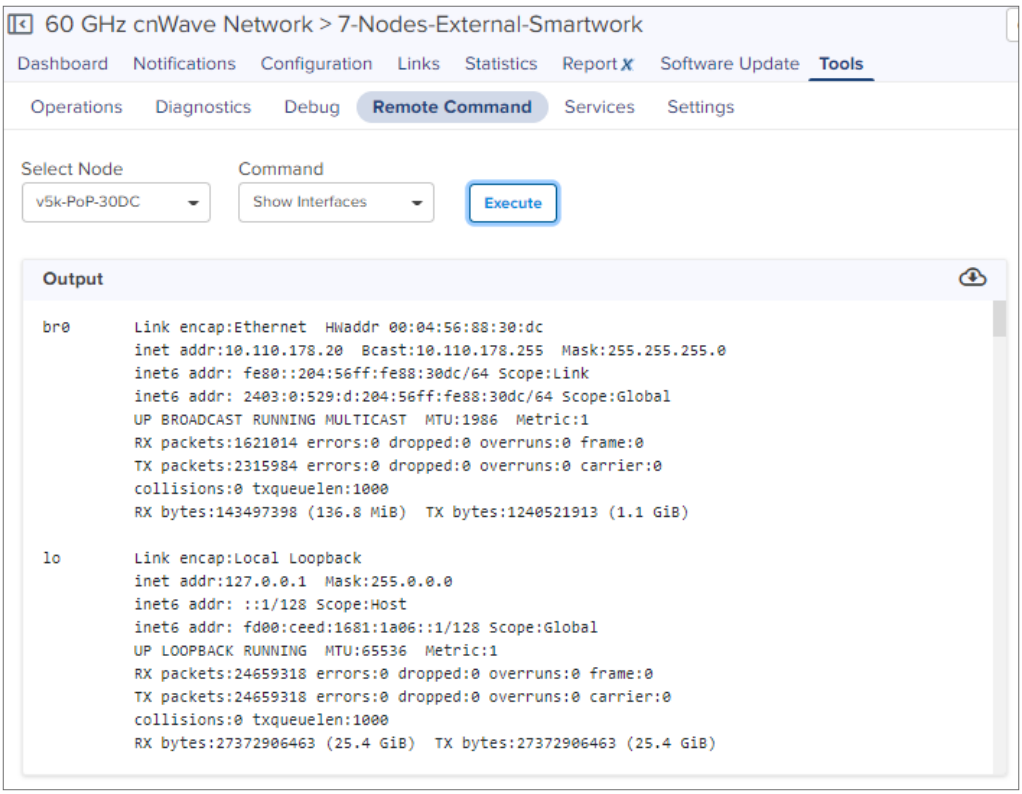
- Ping
- Show DHCP client lease (Applicable for only PoP node)
- Show IGMP Membership Table
- Show Interfaces
- Show IPv4 Neighbors
- Show IPv6 Neighbors

- 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:

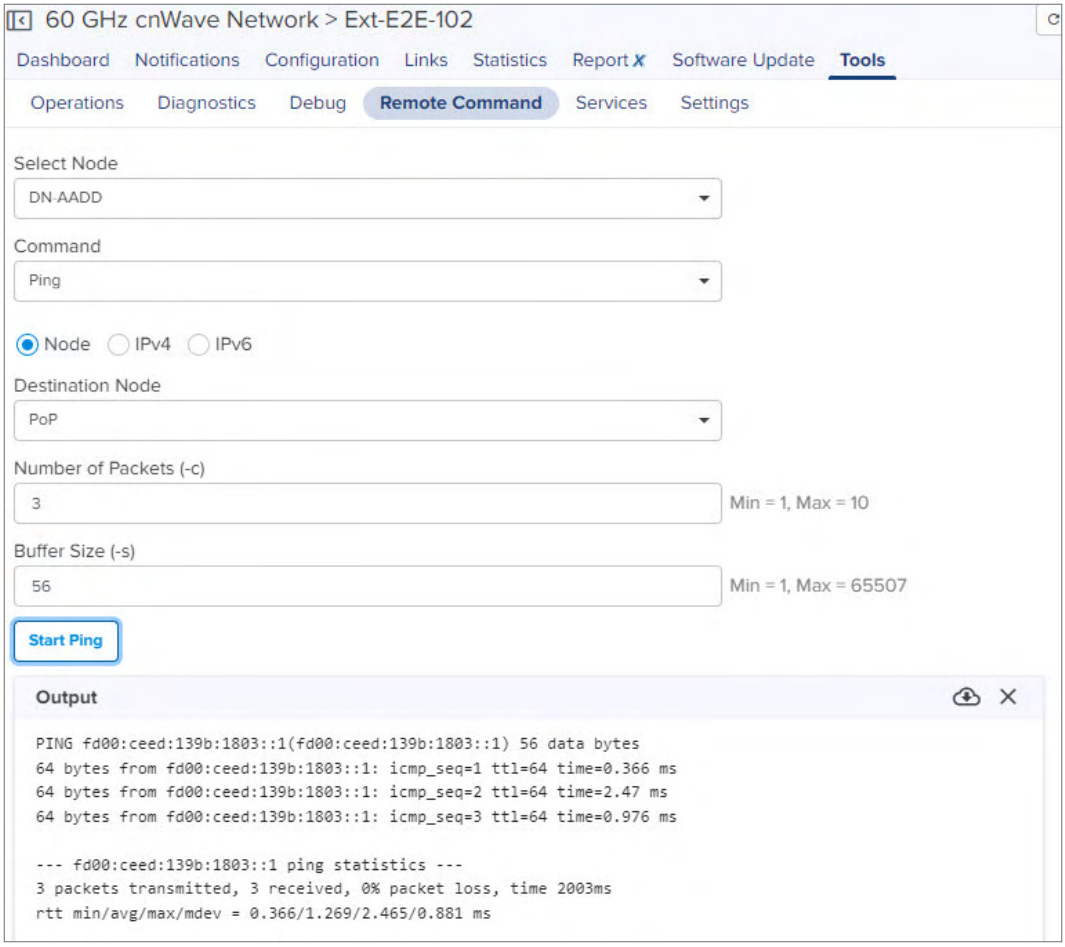
1. Select the **Ping** command from dropdown.
2. Select **Node** or type of **IP address** (IPv4 or IPv6).
3. Select the following options:

- 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 393.

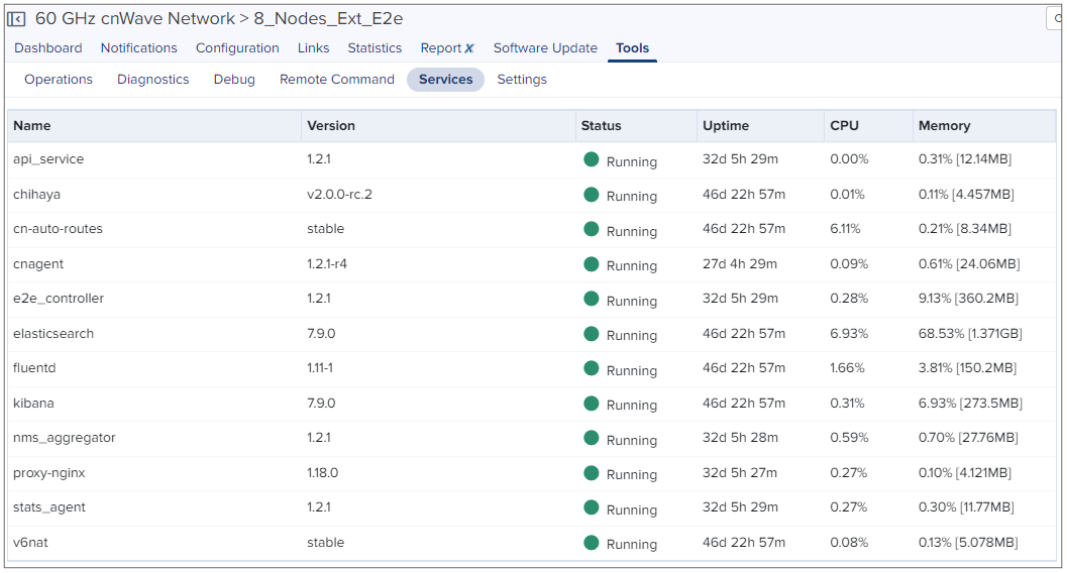
Figure 393 *Remote Command: Ping*



Services

In **Services** page user can view the services running in E2E Controller.

Figure 394 *Services*



Settings



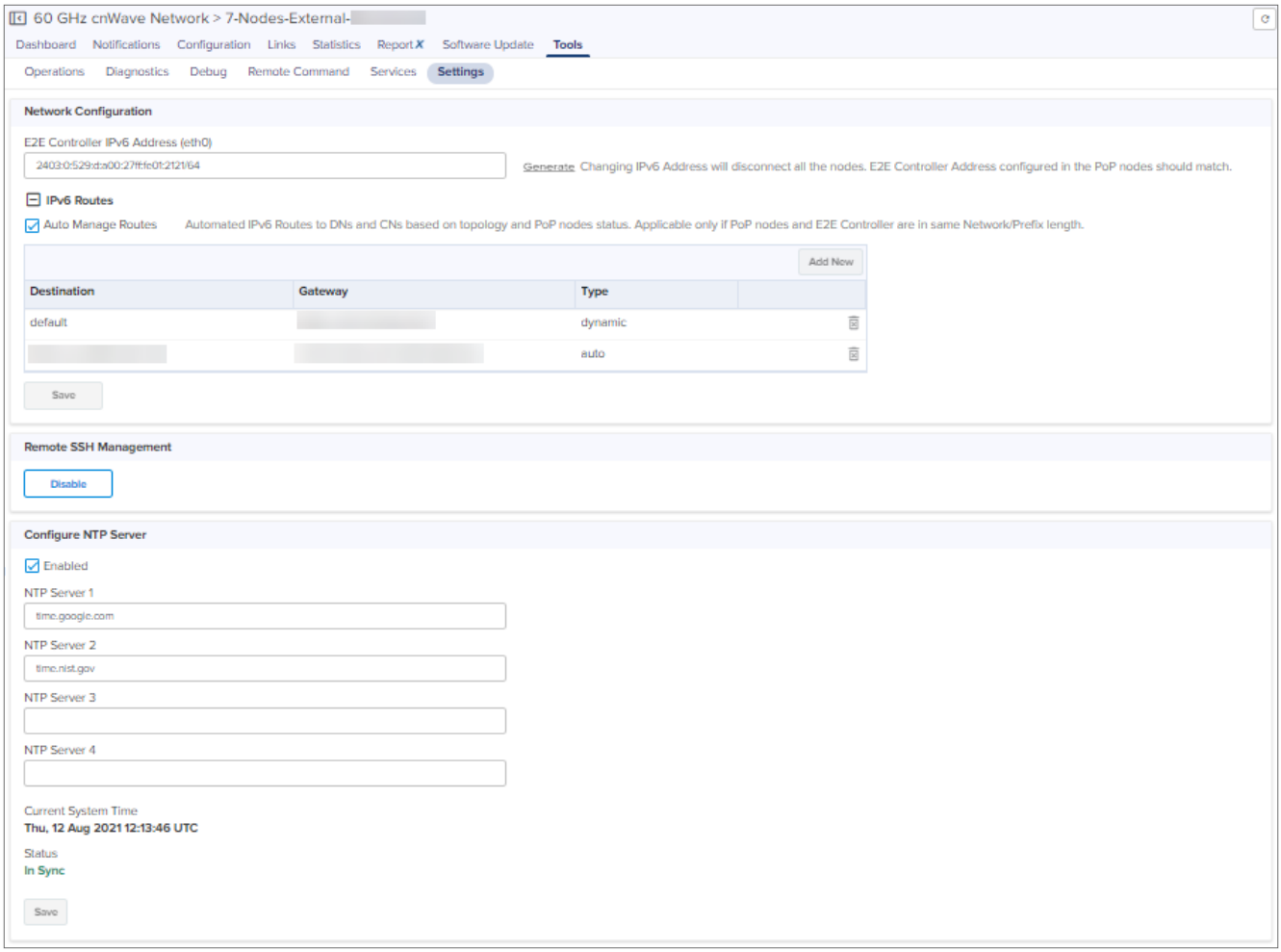
Note

E2E Settings are not applicable for Onboard E2E Controller deployment.

External E2E Controller deployment

External E2E Network displays the **Settings** page as follows:

Remote SSH Management allows the user to enable and disable **Remote SSH Management**.



In **Network Configuration** user can configure the **E2E Controller IPv6 Address** and **IPv6 Routes**.

To change **E2E Controller IPv6 Address**, perform the following:

1. Navigate to **Tools** > **Settings** > **Network Configuration** tab.
2. Click **Generate** to automatically generate IPv6 address or manually change the IPv6 Address of E2E Controller.
3. Click **Save**.

To configure **IPv6 Routes**, perform the following:

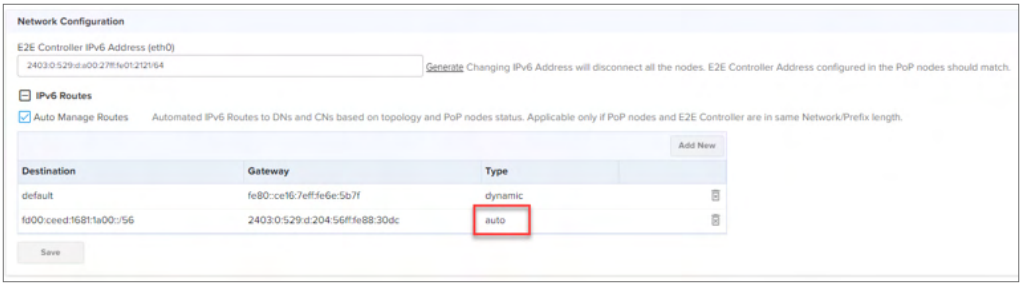
You can also enable the **Auto Manage Routes**. This automates IPv6 Routes to DNs and CNs based on the topology and PoP nodes status. It is applicable only if PoP nodes and E2E Controller are in same Network/Prefix length.

If IPv6 routes is enabled as **Auto Manage Routes**, **Type** field displays as **Auto**.

To Enable Auto Managed Routes:

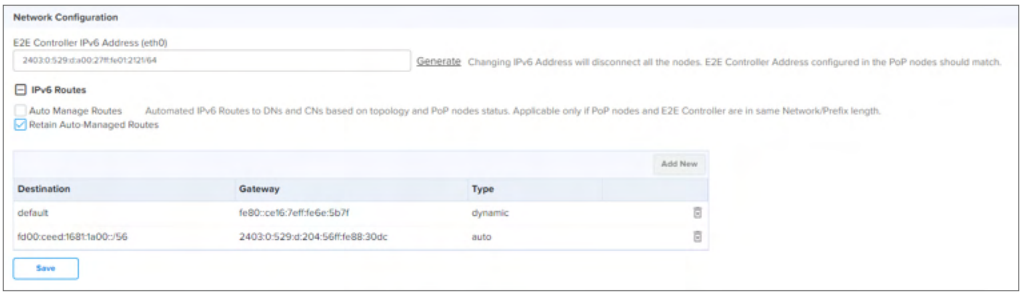
1. Navigate to **Tools** > **Settings** > **Network Configuration** tab.
2. Enable **Auto Manage Routes**.

3. Click **Save**.

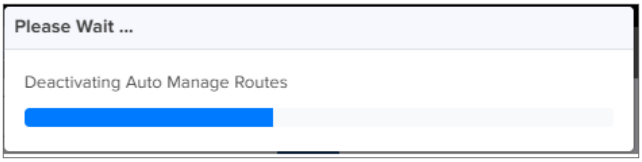


To retain auto-managed routes, even after auto-managed routes is disabled, complete the following steps:

1. Navigate to **Tools > Settings > Network Configuration** tab.



2. Enable **Retain Auto-Managed Routes.**
3. Click **Save.**



4. Please wait pops-up.

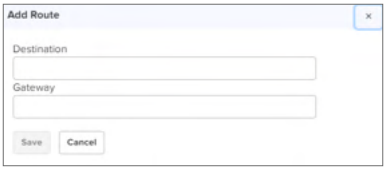
   Once the Auto Manage Routes is disabled, IPv6 routes can be managed through static routes and in type it displays as **Static**.



5. Click **Save**.

To add new static **IPv6 Routes**:

1. Click **Add New**.

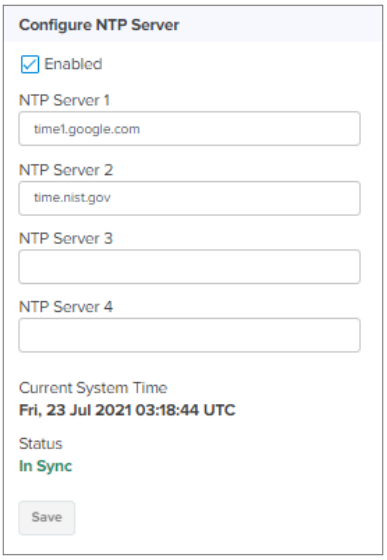


2. Enter **Destination** and **Gateway**.
3. Click **Save.**

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.

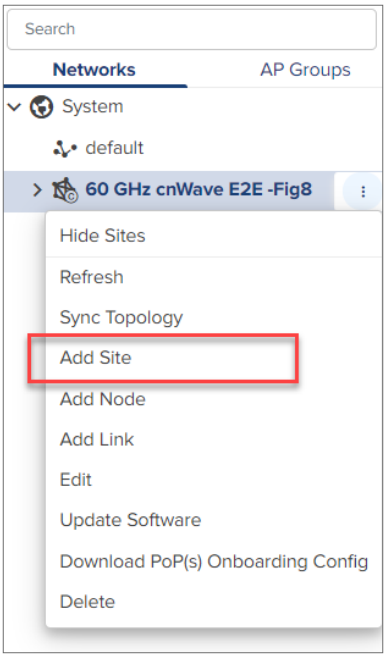


Site Configuration

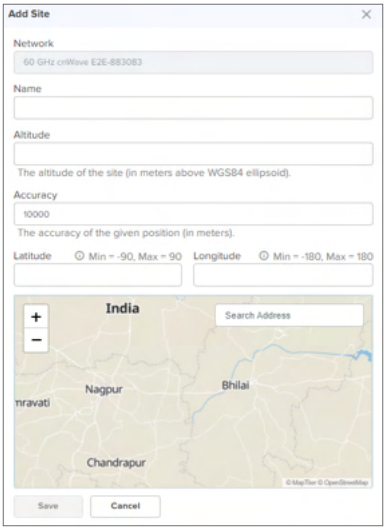
Sites are located within the networks and wireless access points attached to it.

To Add a Site

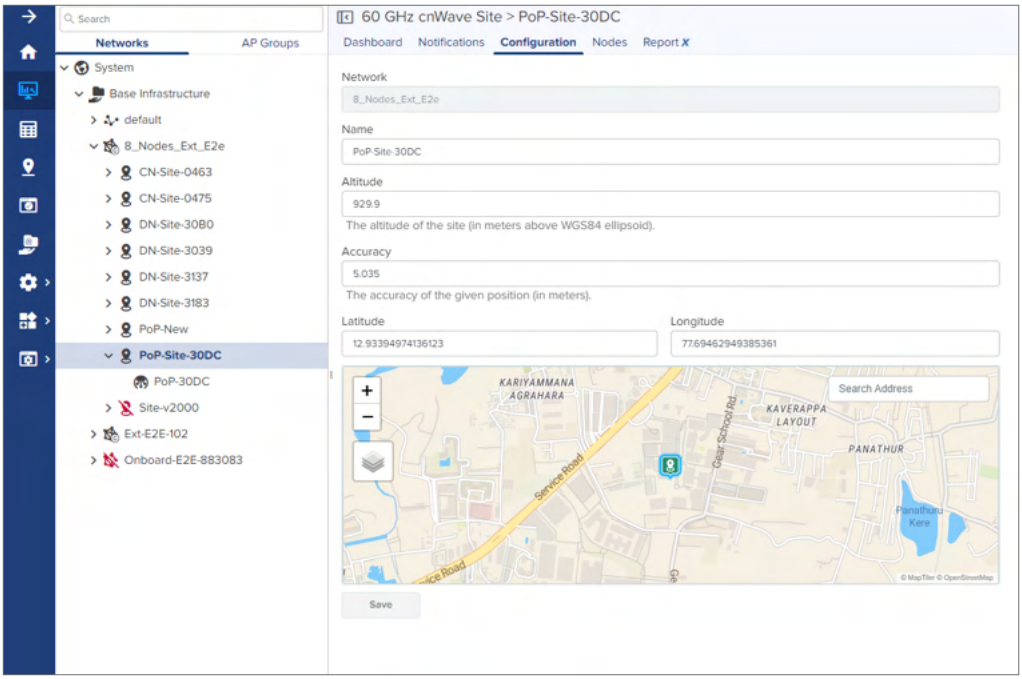
1. Navigate to **Network** and click ⋮ icon.
2. Select **Add Site** from the dropdown.



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.

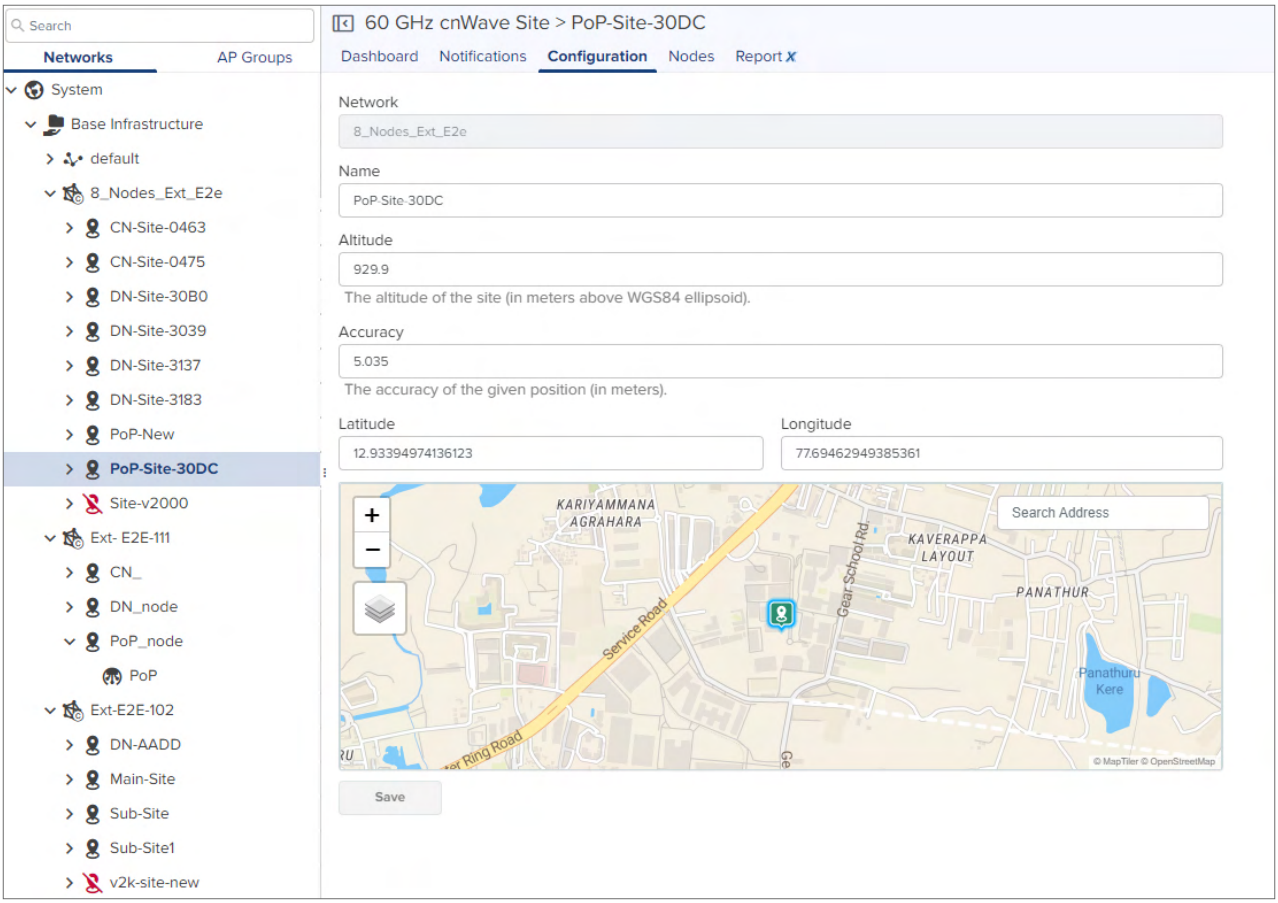


5. Click **Save**. When the Site is configured it gets added under the E2E Network.



To edit the **Site** perform the following:

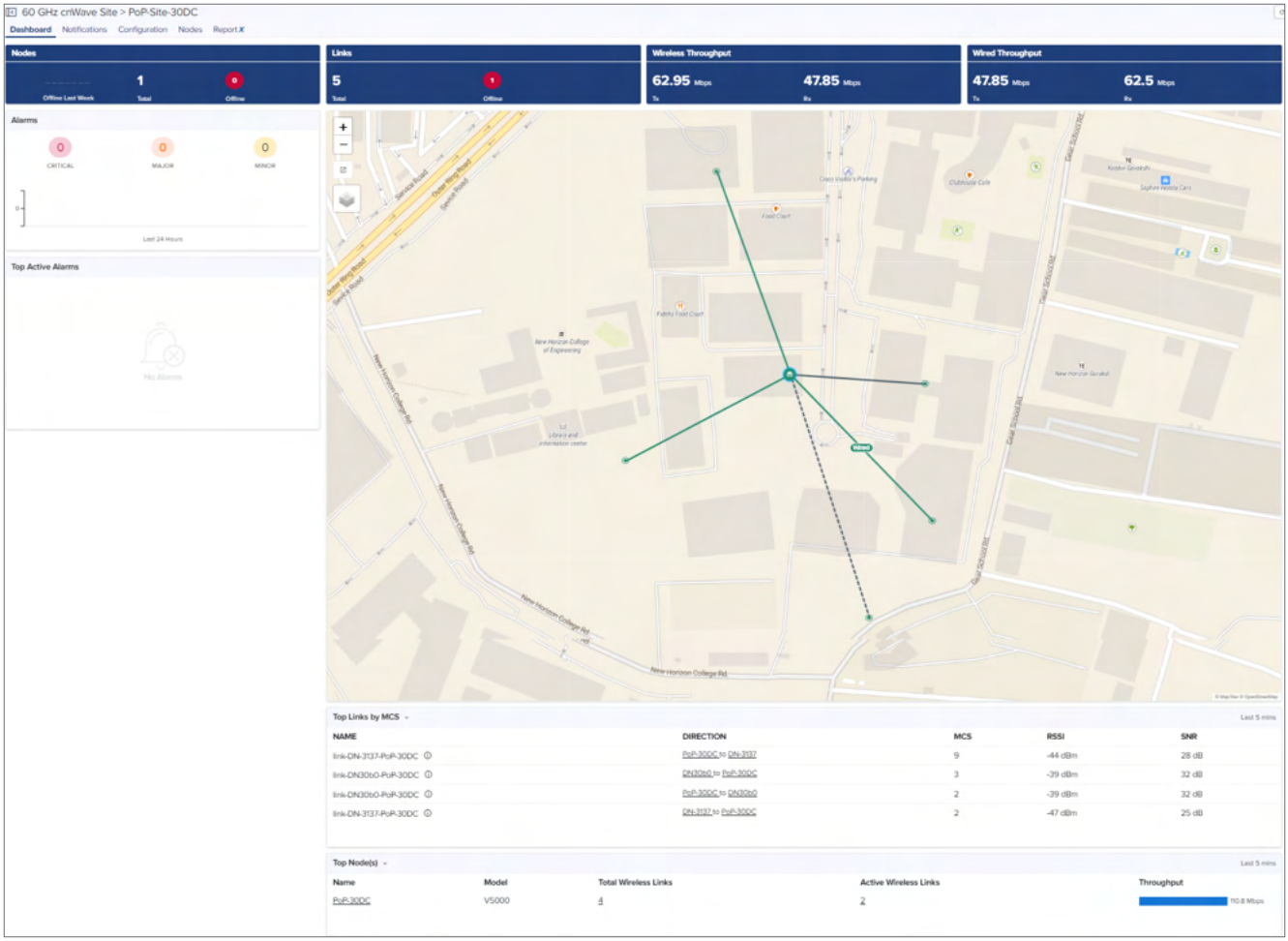
1. Navigate to **Network** > **Site** > **Configuration**.
2. Edit the details and click **Save.**



Site Dashboard

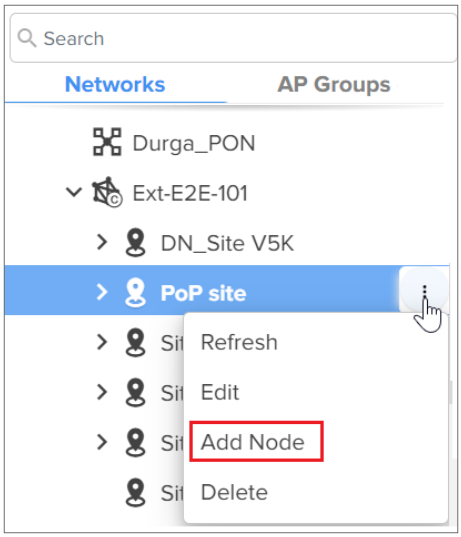
Dashboard pages are customized for each device type and aggregation level. The Site dashboard section displays the **Nodes, Links, Wireless Throughput, Wired Throughput, Alarms, Top Active Alarms, Top Links by MCS, Top Links by RSSI, Top Links by SNR, Top Node(s), Top PoP(s), Top DN(s), and Top CN(s).**

Figure 395 *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**.

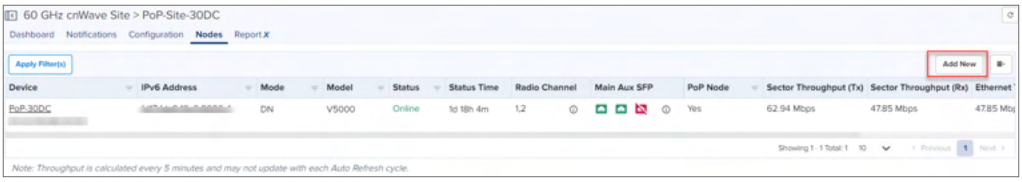


Note

From 3.1.1 release V2000 device (beta version) is supported.

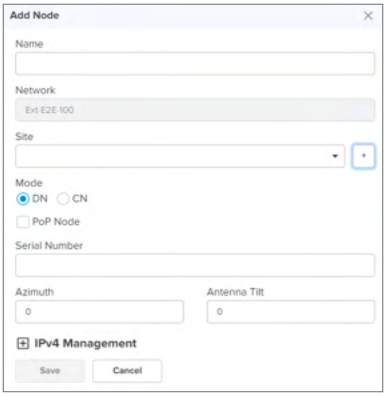
To Add a Node:

1. Navigate to the **Network** > **Site** > **Nodes.**



Add Node window pops-up.

2. Click **Add new.**



3. Click to add site.

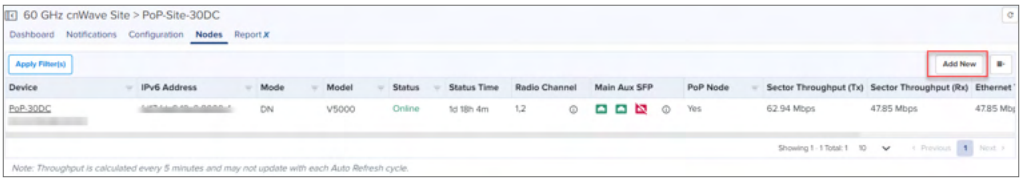
Adding the Node allows the user to create the different Nodes as shown below:

- PoP Node
- DN
- CN

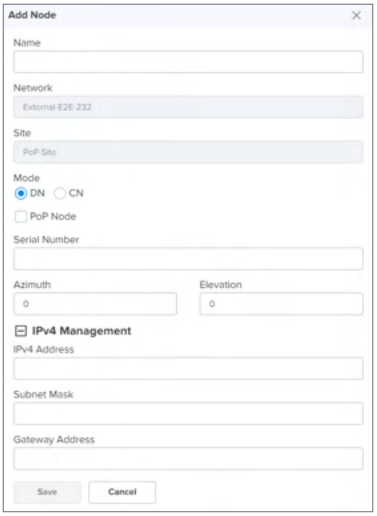
PoP Node configuration

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 **Serial Number** .
7. Enter the **Azimuth** and **Elevation**.
8. In the **PoP Configuration** select **BGP** or **Static Routing**.
9. In **Interface** select **Aux** or **Main** or **SFP** or **Disabled**.



10. Enter the **IPv6** and **Gateway Addresses.**

Note

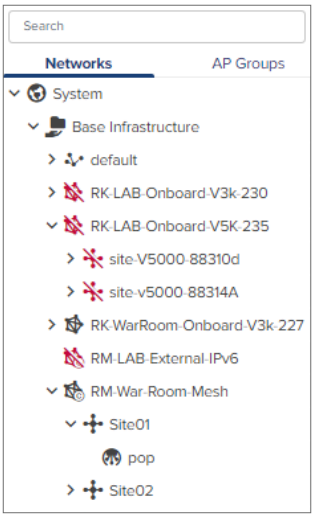
Generate IPv6 provides **Seed Prefix** in CIDR format from which subnet prefixes are allocated to all DNs and CNs (e.g. fdce:b00c:cafe:ba00::/56)

11. In IPv4 Management, enter the **IPv4 Address, Subnet Mask** and **Gateway Address**.
12. Click **Save.**

Note

Once the PoP Node is configured, **PoP(s) Onboarding Config.json** file gets downloaded automatically, which can be used to import and configure in the PoP Node UI.

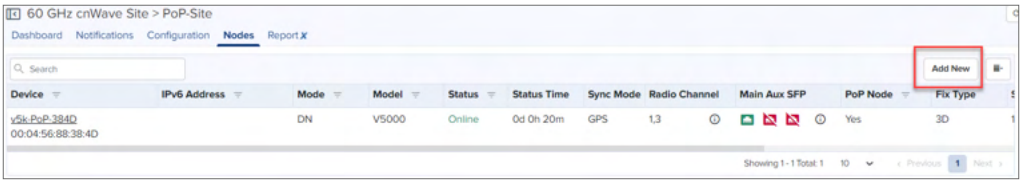
Once the **PoP** node is configured it gets listed under the **Site.**



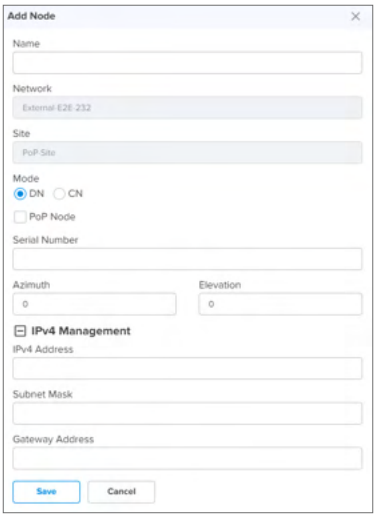
DN/CN Node configuration

To add DN/CN node:

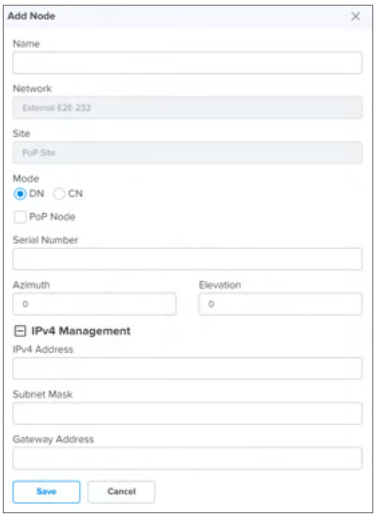
1. Navigate to the **Network** > **Site** > **Nodes.**
2. Click **Add New.**



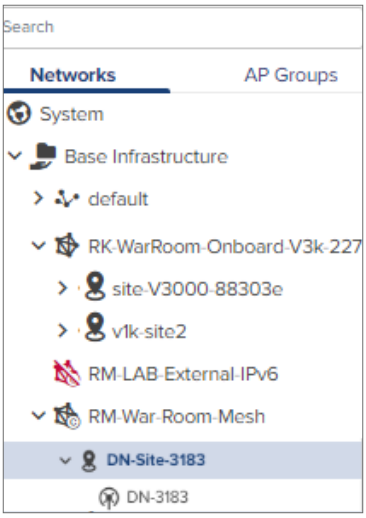
3. **Add Node** window pops-up.



4. Enter the **Node Name**, select the Mode **DN** or **CN.**
5. Enter the **Serial Number**.
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

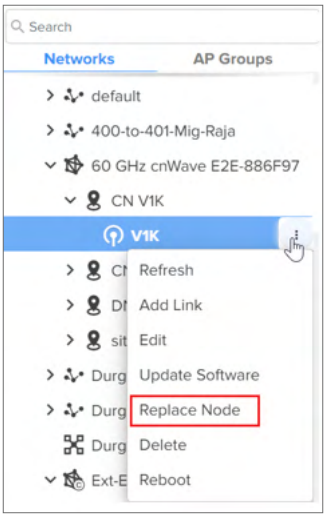
Replace Node allows to replace the existing faulty nodes with new nodes along with the configuration and links of existing faulty nodes.

Note

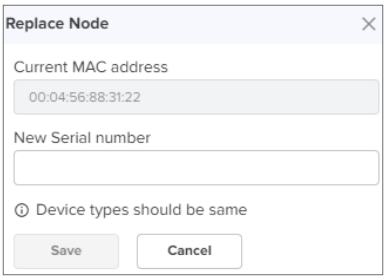
New node should be replaced with same model as existing node.

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 Serial number.**
5. Click **Save**.

PoP Node

Once the PoP node is configured it displays the monitoring panel of the PoP node.

Dashboard

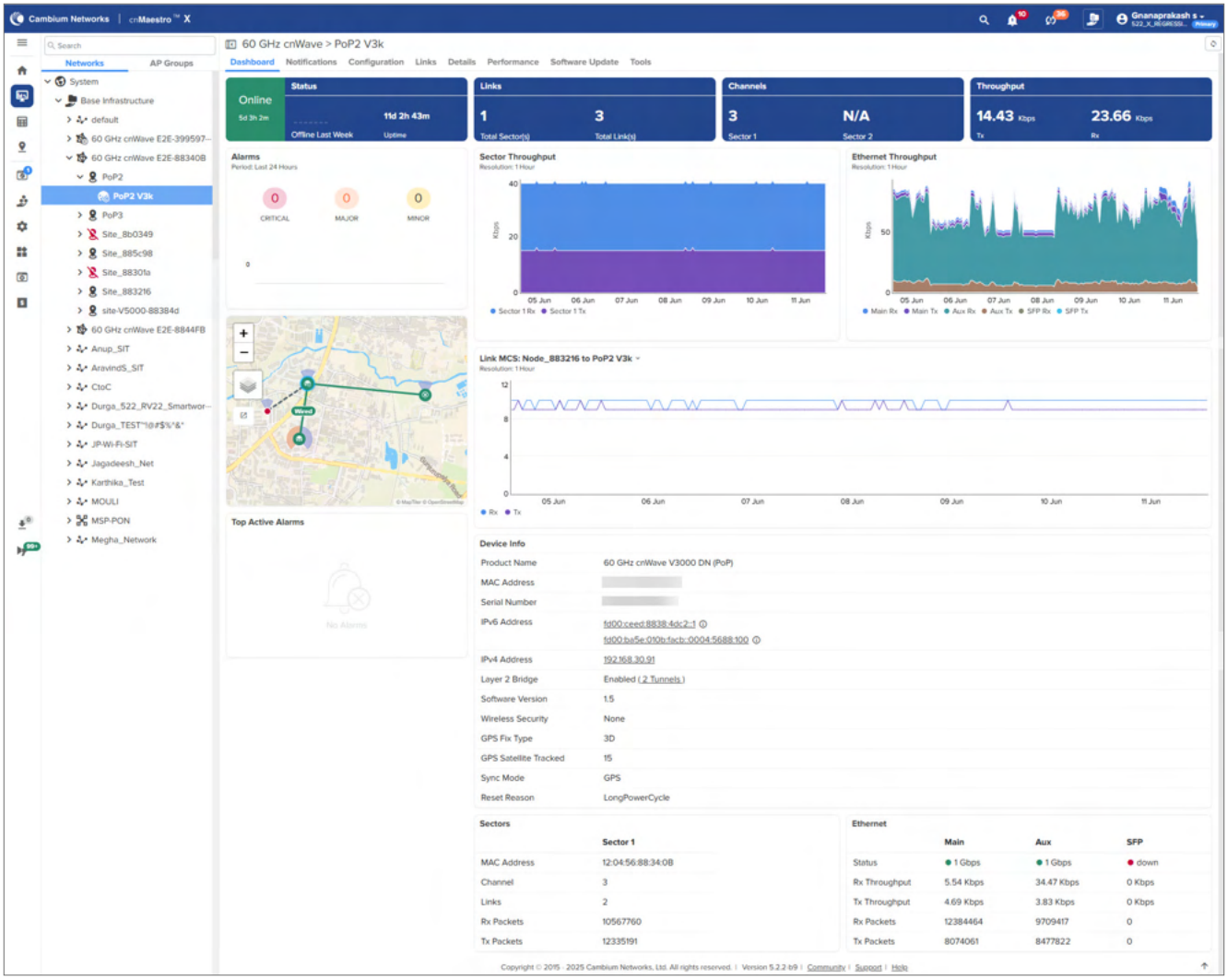
Dashboard pages can be customized for each device type and aggregation level. The PoP node dashboard section displays the **Status, Links, Channels, Throughput, Sector Throughput (Sector 1 and Sector 2), Ethernet Throughput (Main, Aux, SFP**), **Alarms, Top Active Alarms, Link MCS, Device Info, Sectors, and Ethernet**.

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 396 *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 397 *Basic*



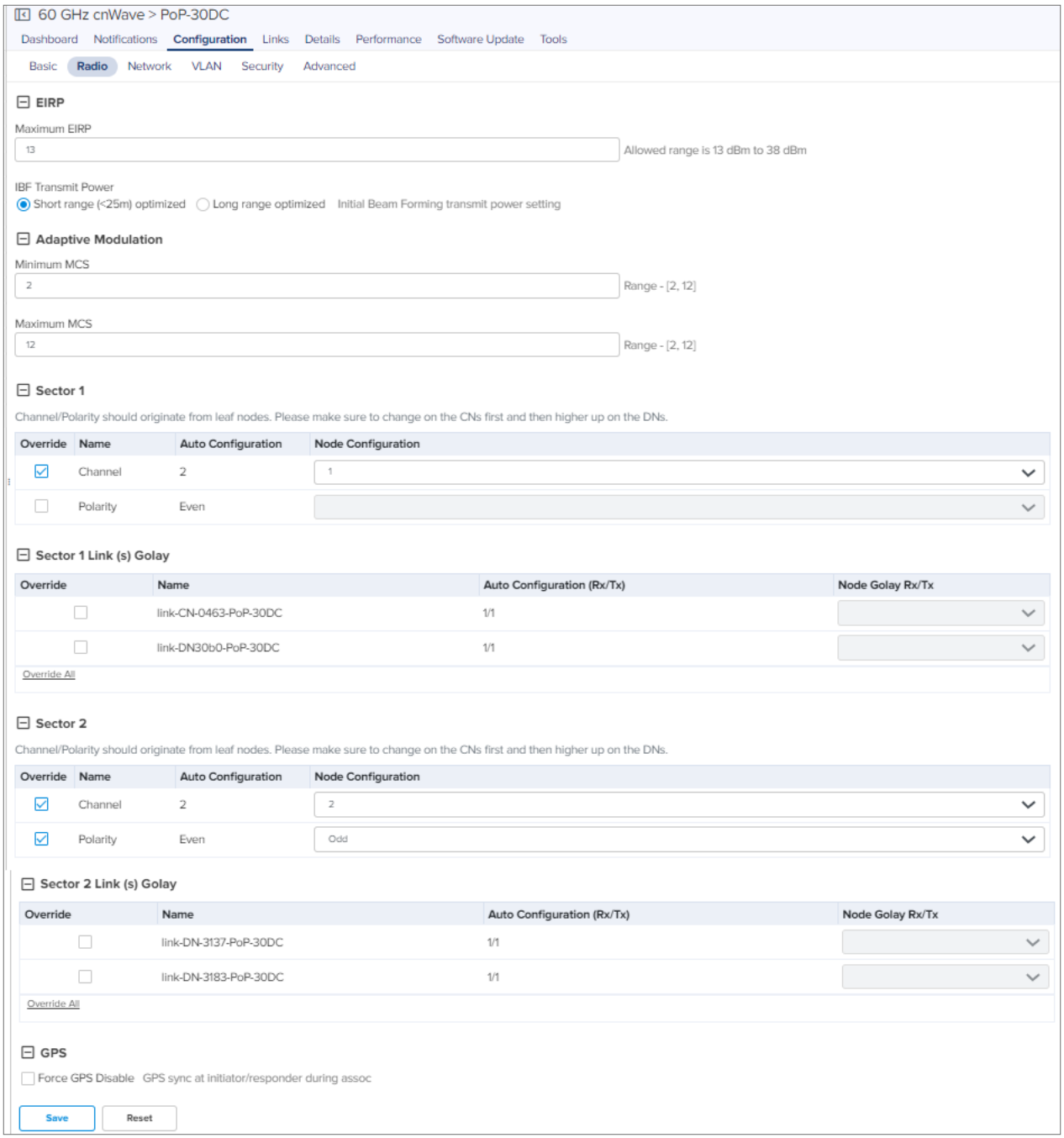
Radio

It allows the user to configure the **EIRP**, **Adaptive Modulation**, **Sectors (channels, Polarity and Link(s) Golay)**, and **GPS**.

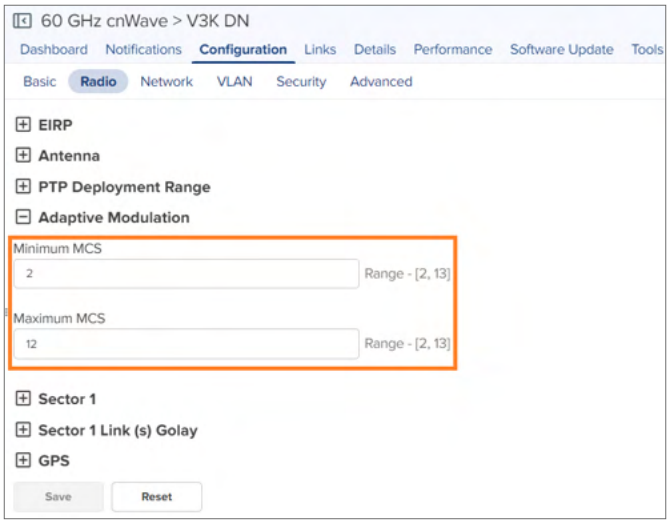
Note

Antenna and PTP deployment Range options is available only for v3000.

Figure 398 *Radio*



For V3000, MCS 13 is supported as seen the following UI:



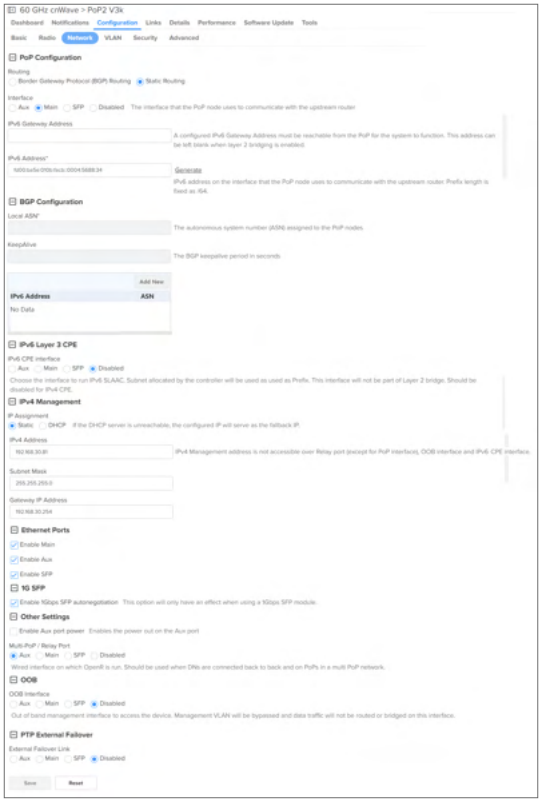
Network

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 399 *Network*



Configure the Network as shown below:

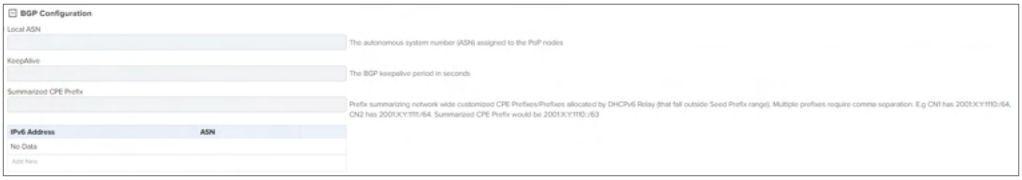
1. Navigate to the **Configuration** > **Network.**
2. In **PoP Configuration:**
    - Select the appropriate option in **Routing** and **Interface**.
    - Enter the **IPv6 Address.**
    - Enter **IPv6 Gateway Address** its optional.



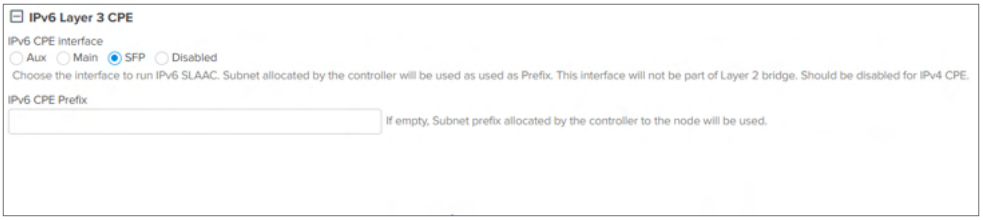
3. In **E2E Controller Configuration**, enter the **IPv6 Address.**



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.



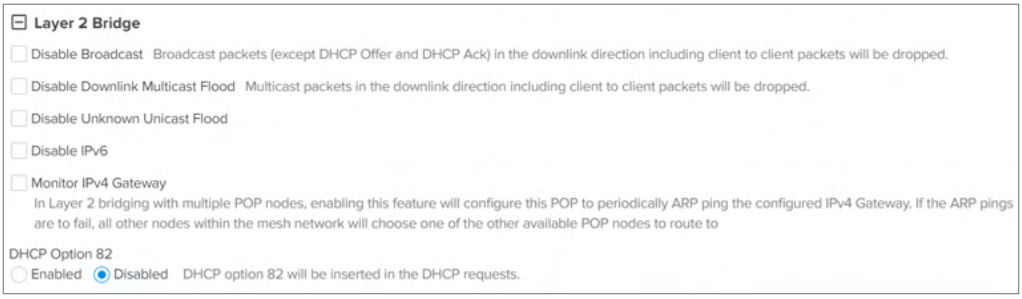
7. In **Ethernet Ports** enable the appropriate option **Main** or **Aux** or **SFP.**
8. In **Layer 2 bridge** enable the appropriate options such as:
   - Disable Broadcast Broadcast packets (except DHCP Offer and DHCP Ack) in the downlink direction including client to client packets will be dropped.
   - 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..

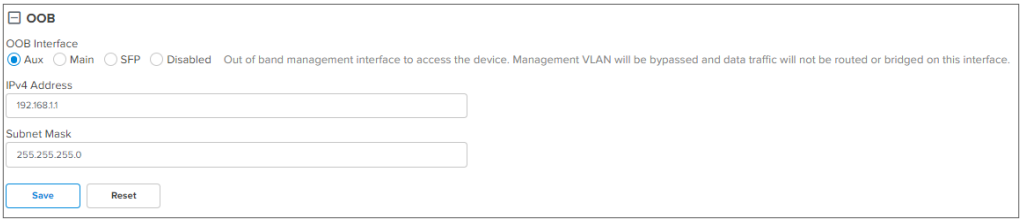
   - Insert DHCP Option 82



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:

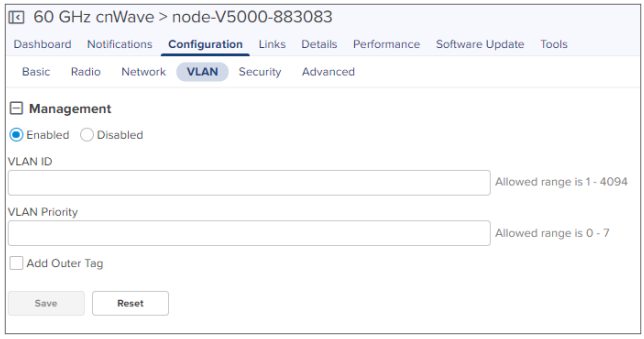
- When Layer2 bridge is disabled, Only PoP node Management VLAN ID can be configured.
- When Layer2 bridge is enabled, all nodes Management VLAN ID can be configured.

Node running version 1.1:

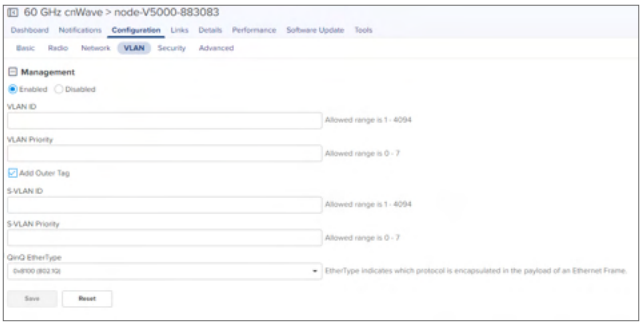
- When Layer2 bridge is disabled, Only PoP node Management VLAN ID, Priority with Outer Tag can be configured.
- When Layer2 bridge is enabled, all node management VLAN and ports can be configured.

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**.



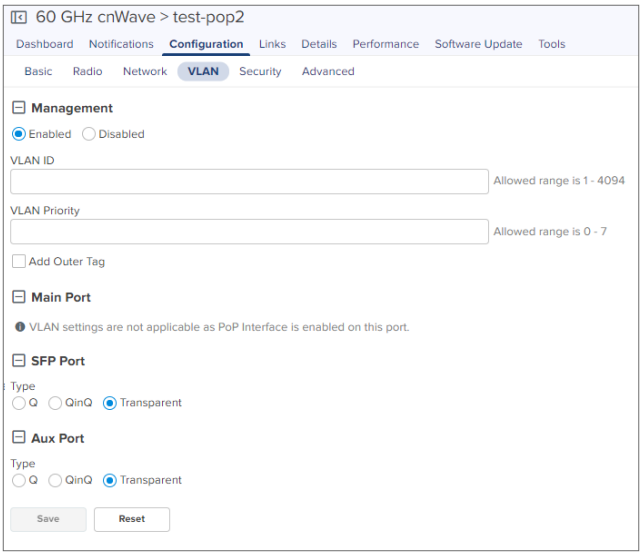
5. Enter **S-VLAN ID**.
6. Enter **S-VLAN Priority.**
7. Enter **QinQ EtherType.**
8. Click **Save.**

   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.



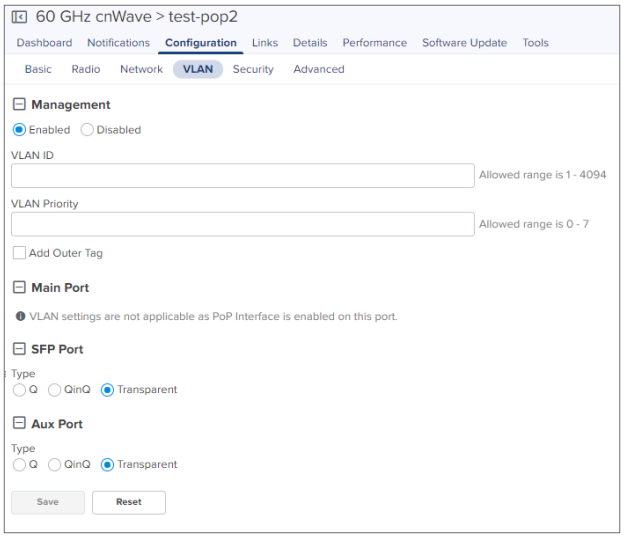
Note

VLAN settings are not applicable if Relay Port, SFP Port, or Aux Port is enabled on Network page.

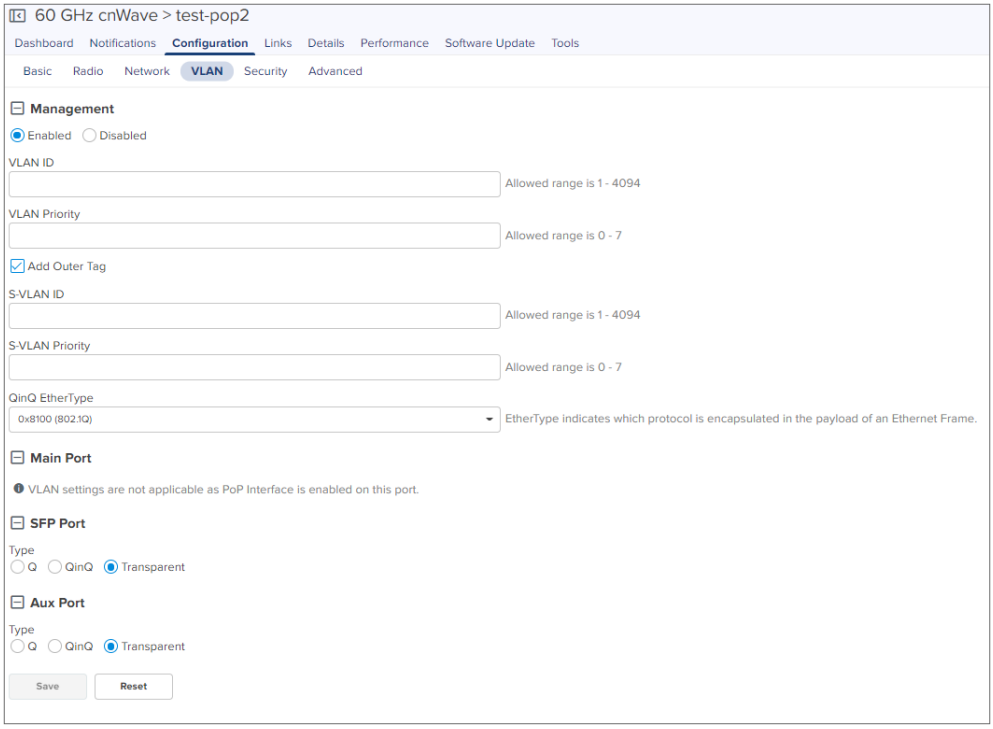


To add a VLAN:

1. Navigate to **Configuration > VLAN.**
2. Click Enabled.



3. Enter the **VLAN ID** and **VLAN Priority**.
4. Enable **Add Outer Tag**.

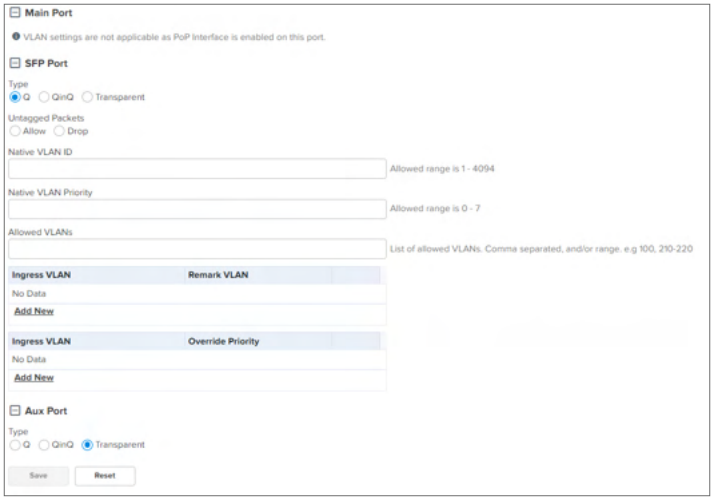


5. Enter **S-VLAN ID**.
6. Enter **S-VLAN Priority.**
7. Enter **QinQ EtherType.**

> **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.**



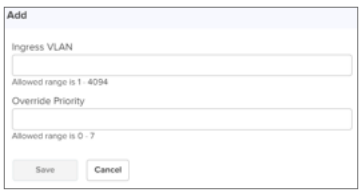
- Click Add New



  - Enter **Ingress VLAN** and **Remark VLAN**.
  - Click **Save**.
- To add new **VLAN Priority Override**.



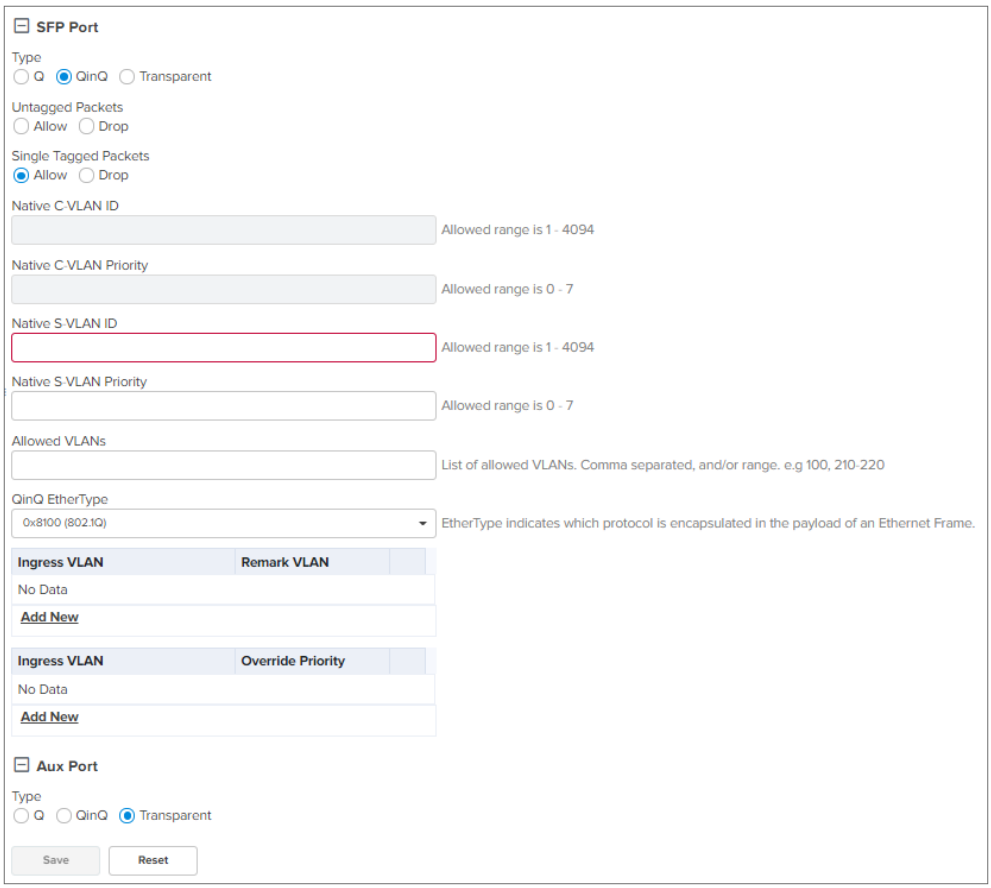
- Click **Add New**.



- 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 400 *Security*



Advanced

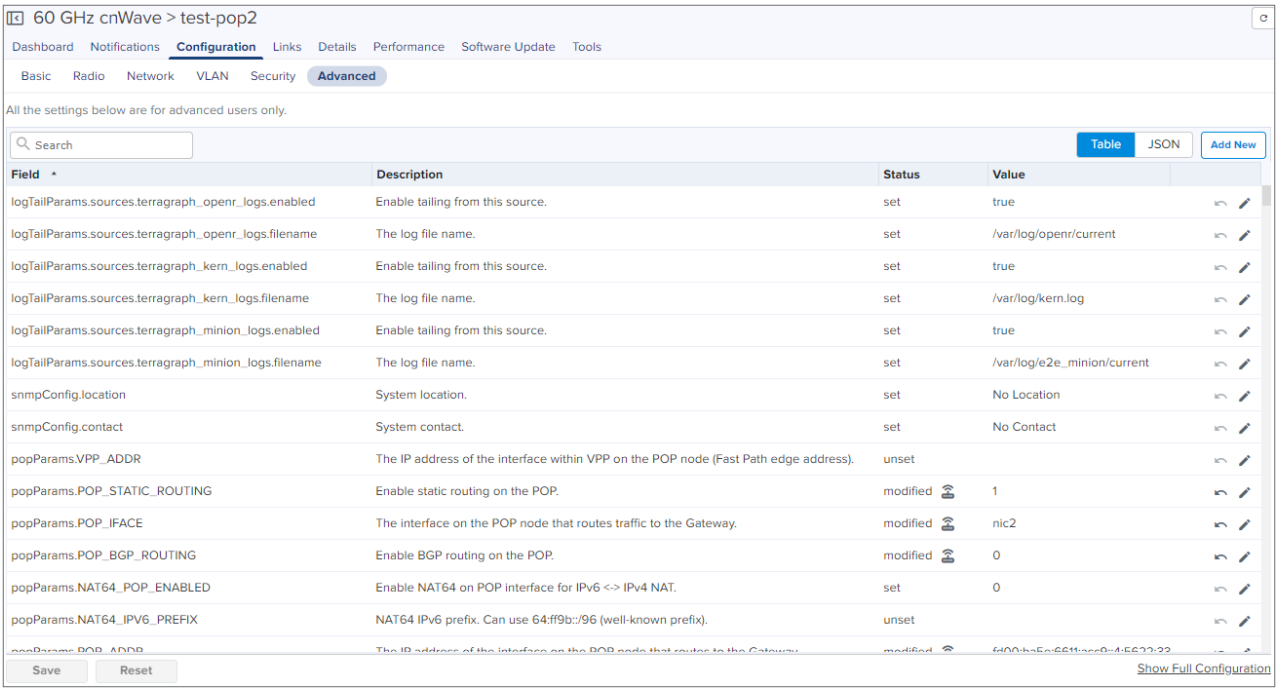
Advanced tab allows the advanced user to edit the settings of the Table and JSON format of the PoP Nodes.

Table

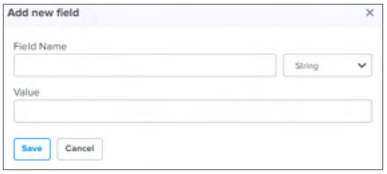
In the **Table** user can view and edit **Field Name** and **Value**. You can sort field name in alphabetical order.

To add a field:

1. Navigate to **Configuration** > **Advanced.**
2. Click **Add New.**



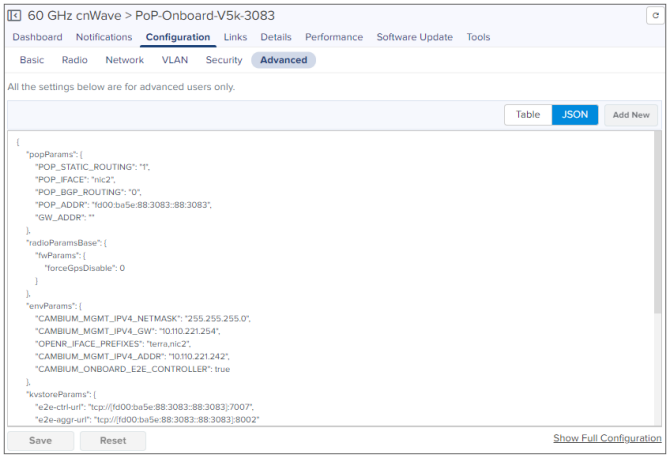
3. Enter the **Field Name** and **Value.**



4. Click **Save.**

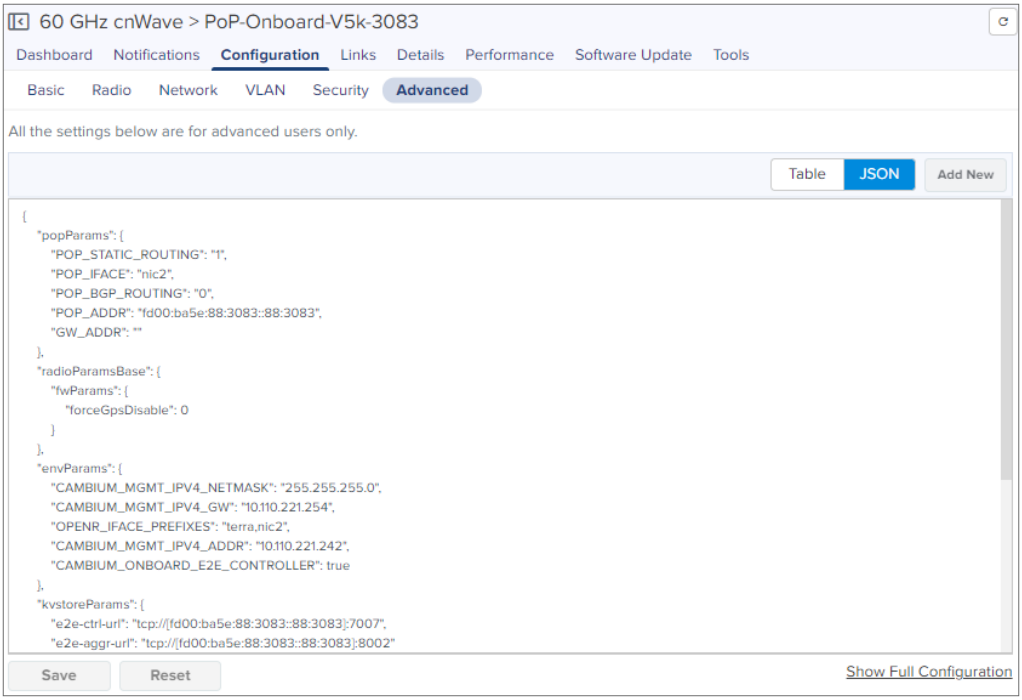
JSON

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**.

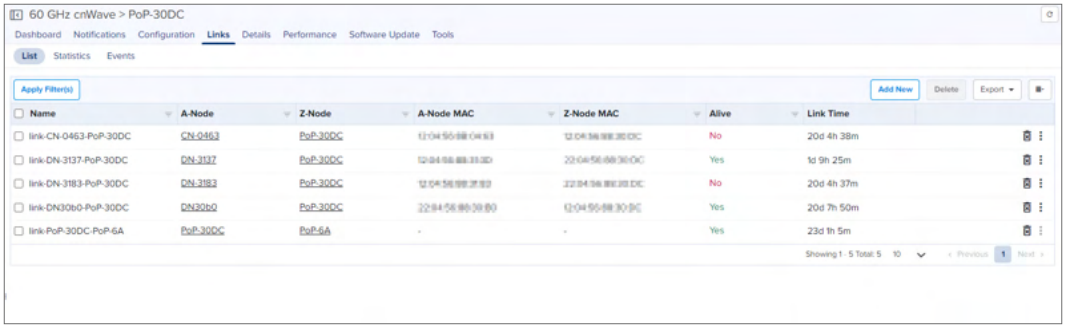
Links

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 401 *List*



For more details about adding a link and deleting a link in the network, refer the List section.

Note

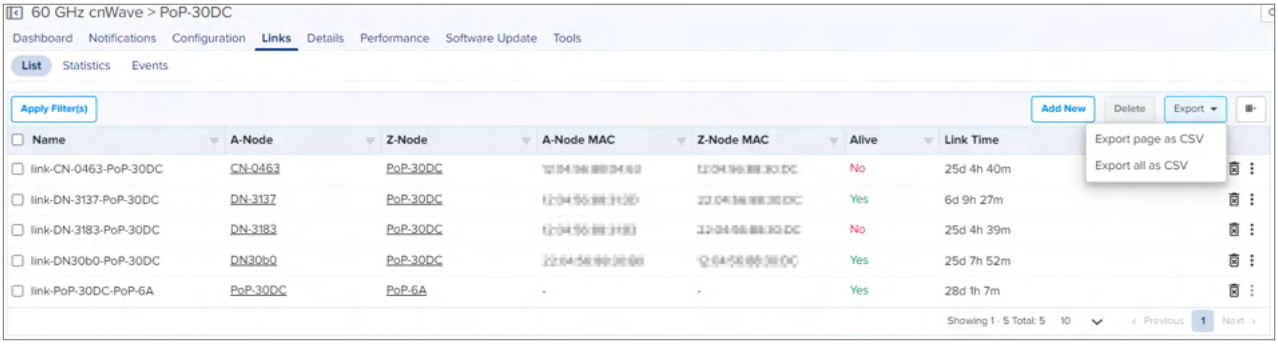
By default A Node is selected as node, when adding new link in the network.

Export List

Export list allow the user to export the PoP links list.

To export the links :

1. Navigate to **Links** > **List** > select **Export.**



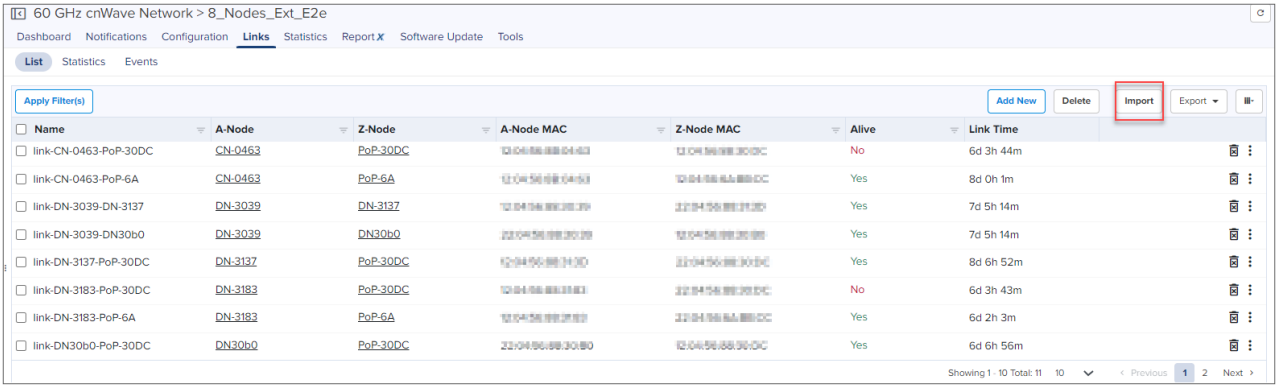
2. It exports .csv file format as shown below.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	LINK_NAME	A_NODE_I	A_NODE_I	Z_NODE_N	Z_NODE_N	LINK_TYPE	ALIVE	IGNITION_	DISTANCE	AZIMUTH	BACKUP_C	IGNITION_	TIMESTAMP		
2	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		
3	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		
4	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		
5	link-DN-D6-PoP-Onboard-V5k-3083	DN-D6	12:04:56:8	PoP-Onbo	12:04:56:8	Wireless	Yes	0	979	105.2	No	Enabled	2021-07-23T02:49:06.317Z		

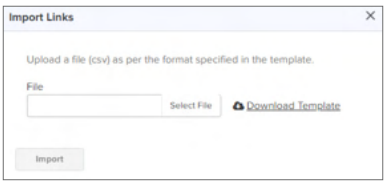
Import List

Import list allow the user to import the PoP links list.

1. Navigate to **Links**> **List** > select **Import.**



Import Links window appears.



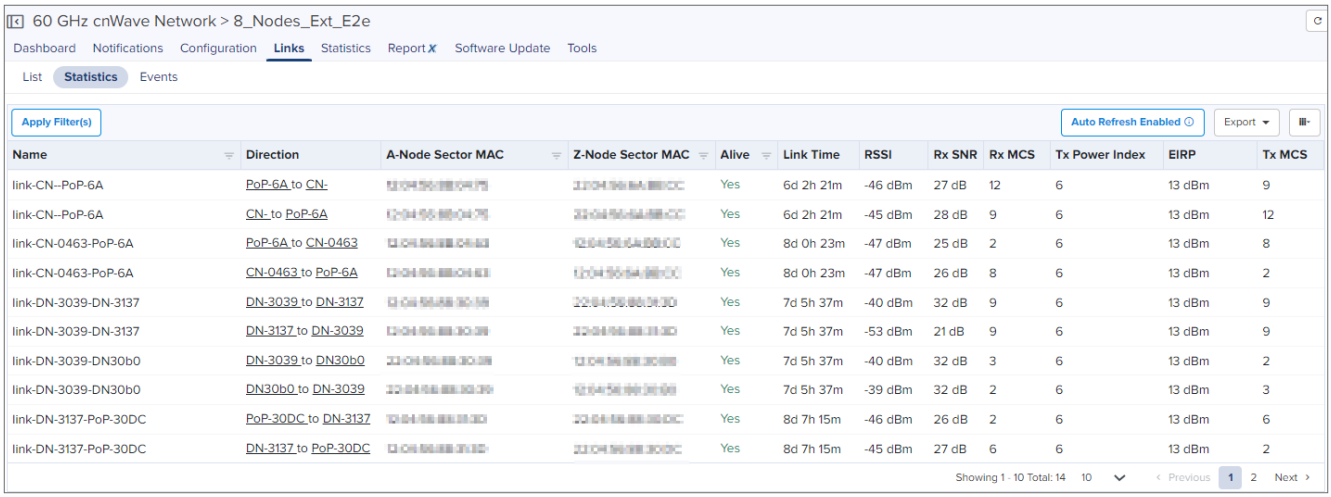
2. Click **Download Template** to download the .CSV format file.

	A	B	C	D	E
1	A_NODE_NAME	A_NODE_MAC	Z_NODE_NAME	Z_NODE_MAC	LINK_TYPE
2	A node name of the device	Sector 1/2 MAC Address	Z node name of the device	Sector 1/2 MAC Address	Wireless or Wired
3	POP		DN1		wireless
4	DN1		CN1		wireless
5	DN1		CN2		wired
6					
7					

3. Select the file and click **Import**.

Statistics

Links Statistics pages provides details of **Basic:** Name, Direction, A-Node, Z-Node Alive Link Time Type Distance Azimuth, Rx Golay, Tx Golay **Detailed Statistics**: A-Node Sector MAC, Z-Node Sector MAC, RSSI, Rx Airtime%, Rx Beam Azimuth Angle, Rx Beam Elevation Angle, Rx SNR, Rx MCS, Rx PER, Rx Scan Beams, Rx Throughput, Tx Airtime%, Tx Beam Azimuth Angle, Tx Beam Elevation Angle, Tx Power Index, EIRP, Tx MCS, Tx PER, Tx Scan Beams, Rx Errors, Rx Frames, Tx Errors, Tx Frames, Tx Throughput, Rx Time, Tx Time, and Link Fade Margin links created with PoP node, generally in a page format.

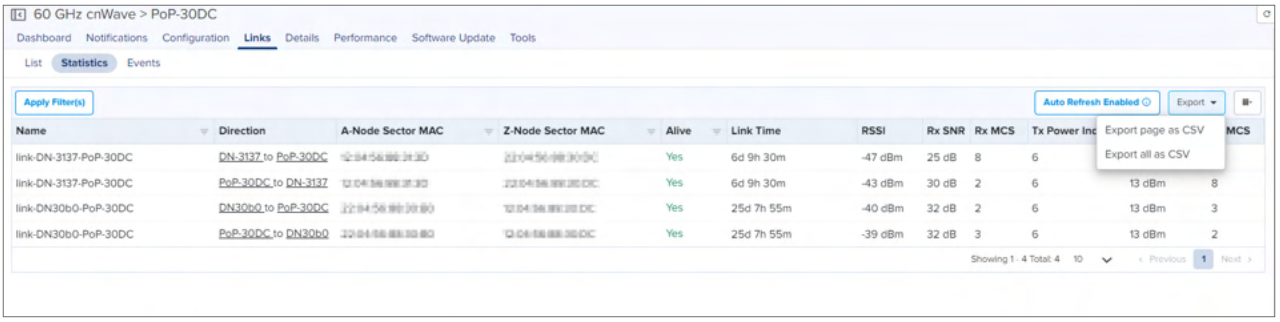


Export Statistics

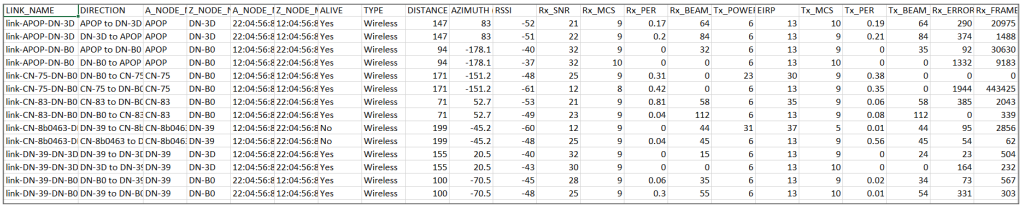
Export list allow the user to export the PoP links Statistics.

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_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 402 *Link Events*

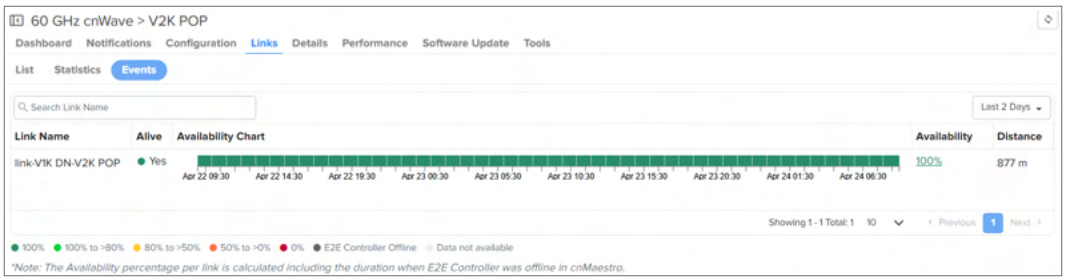


Table 89 *Link > Events fields*

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.

Table 89 *Link > Events fields*

Field	Description
	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 402.
Distance	Distance of the link in meters.

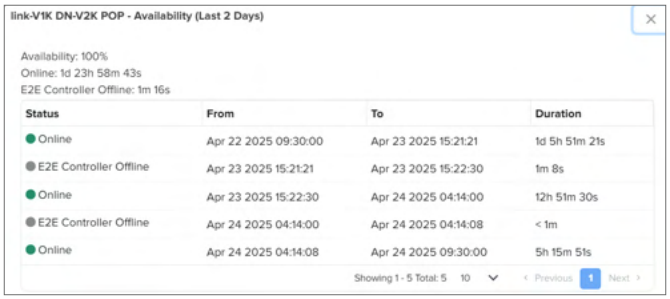
The **Availability Chart** field displays the ink availability in percentage and different colors, as shown below,

Figure 403 *Link Availability in Percentage*



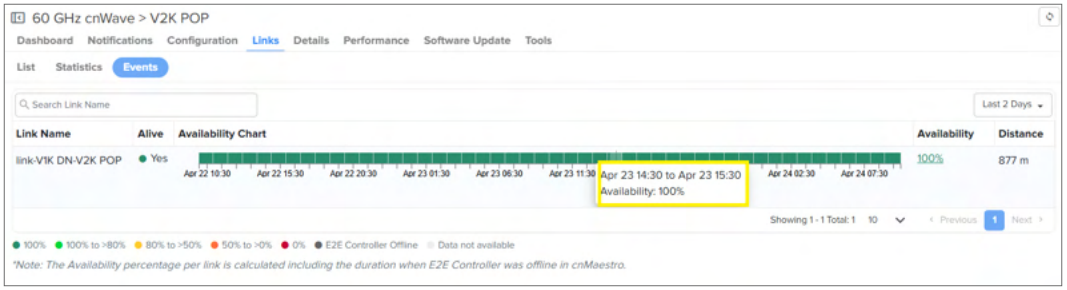
When you click on the percentage in the **Availability** column, you can view the detailed link availability information for the selected time range. Availability percentage per link is calculated, including the duration, when E2E Controller goes Offline in cnMaestro.

Figure 404 *Detailed link availability information*



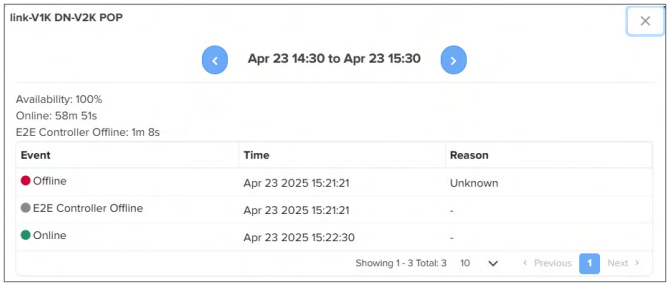
You can hover your mouse on the link to view the hourly availability of the link, as shown in the figure below.

Figure 405 *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 405), you can view the detailed link information for the selected one hour, including the link offline reason.

Figure 406 *Hourly details*



Details

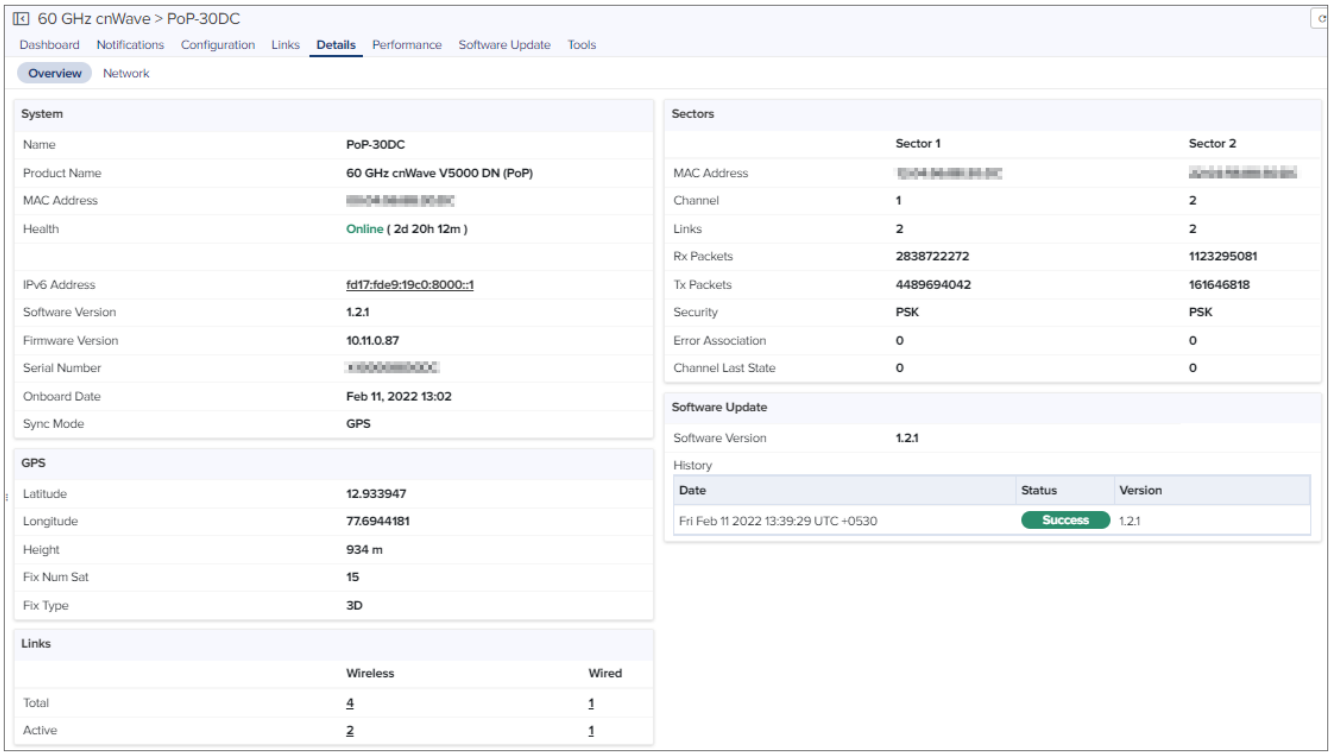
Details page provides the following device information:

- Overview
- Network

Overview

Overview page provides the device details and it also details of the last 3 software update history.

Figure 407 *Details Overview Page*

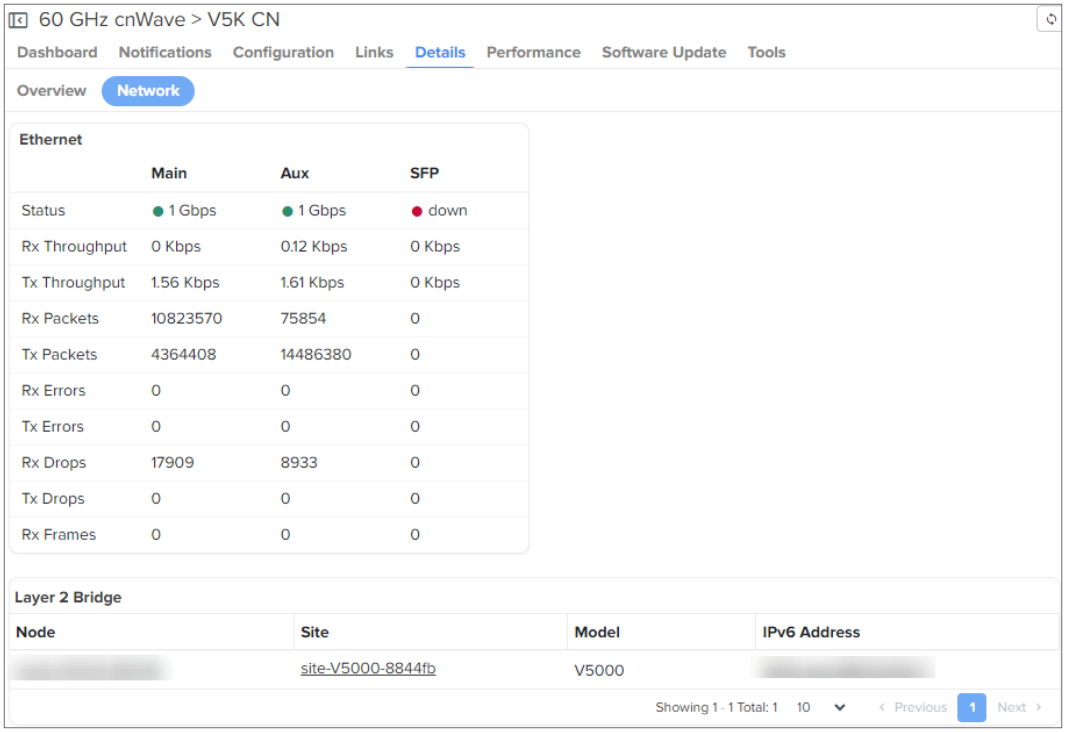


Network

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 408 *Details Network Page*



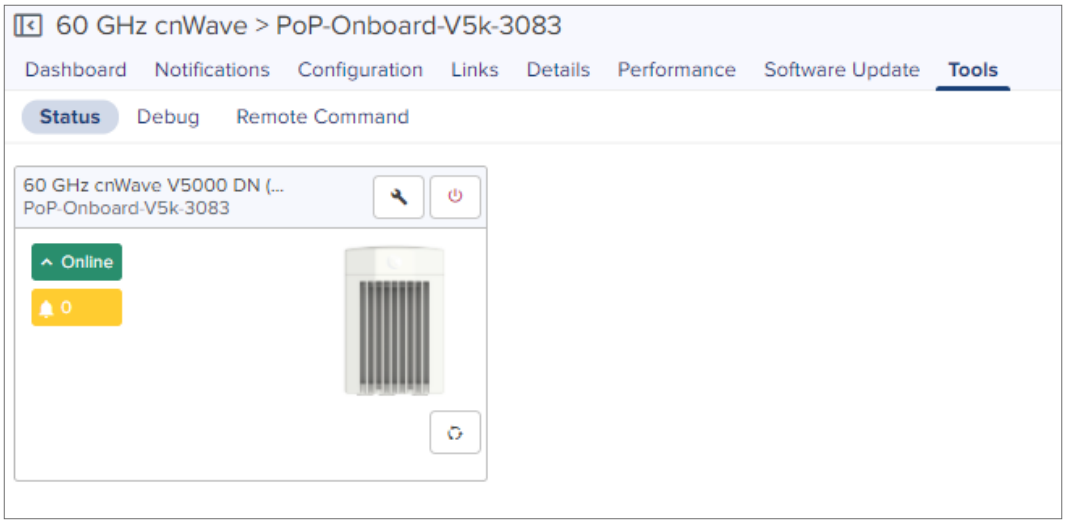
Tools

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.



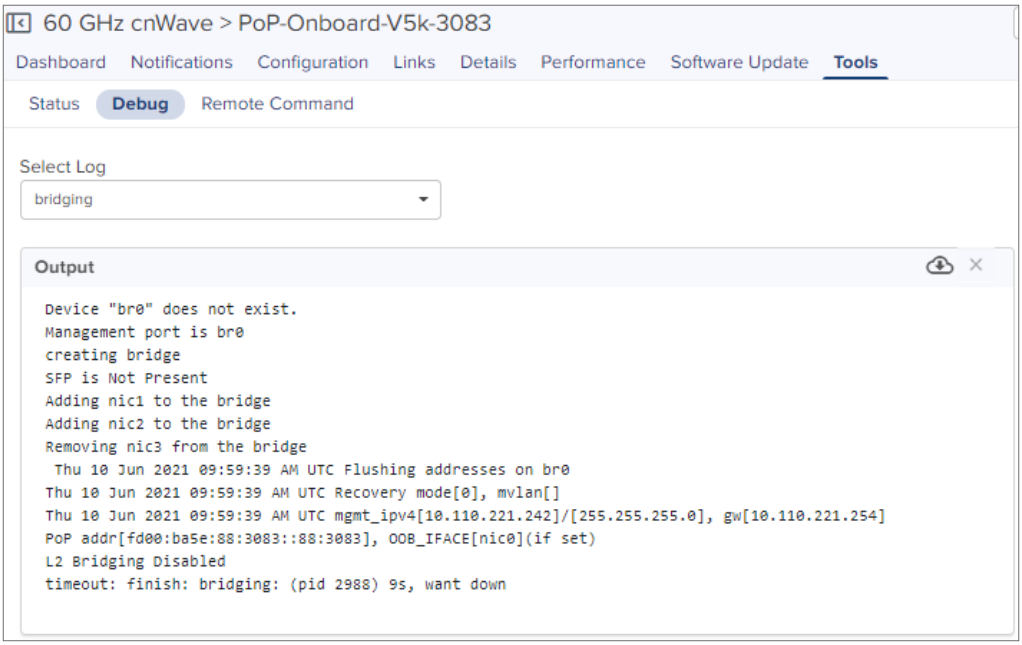
Debug

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)

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

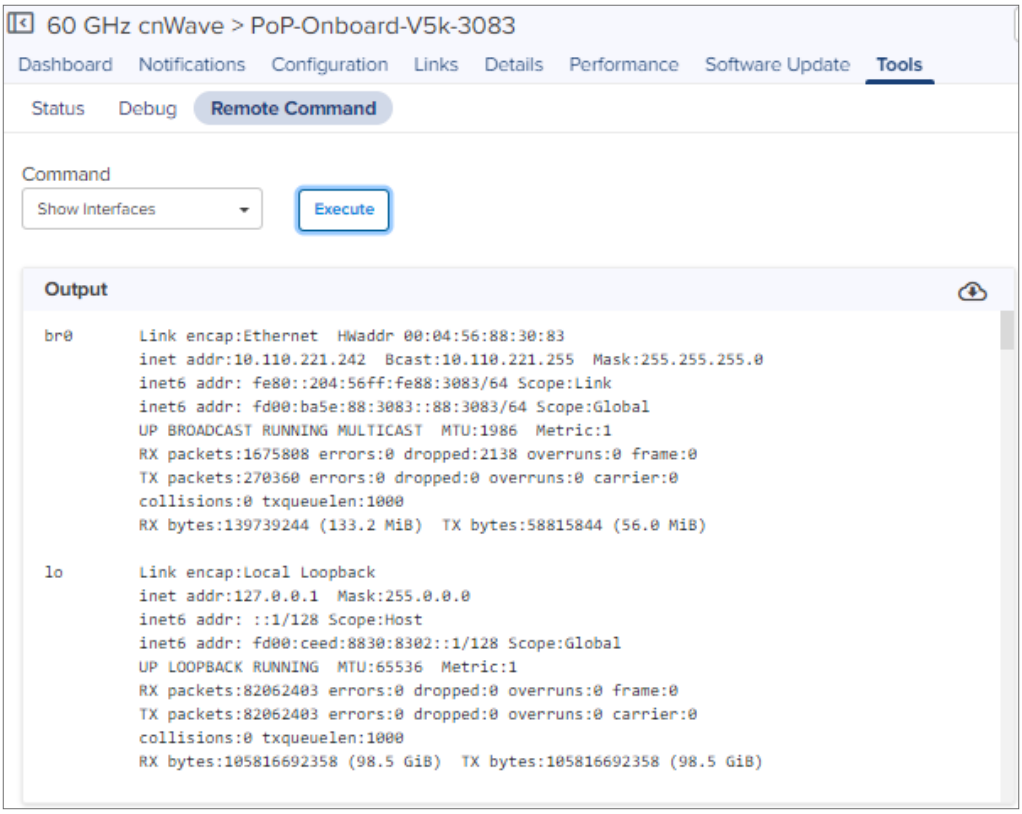
In **Remote command** tab, user can view or download Command logs by executing the following commands:

- 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

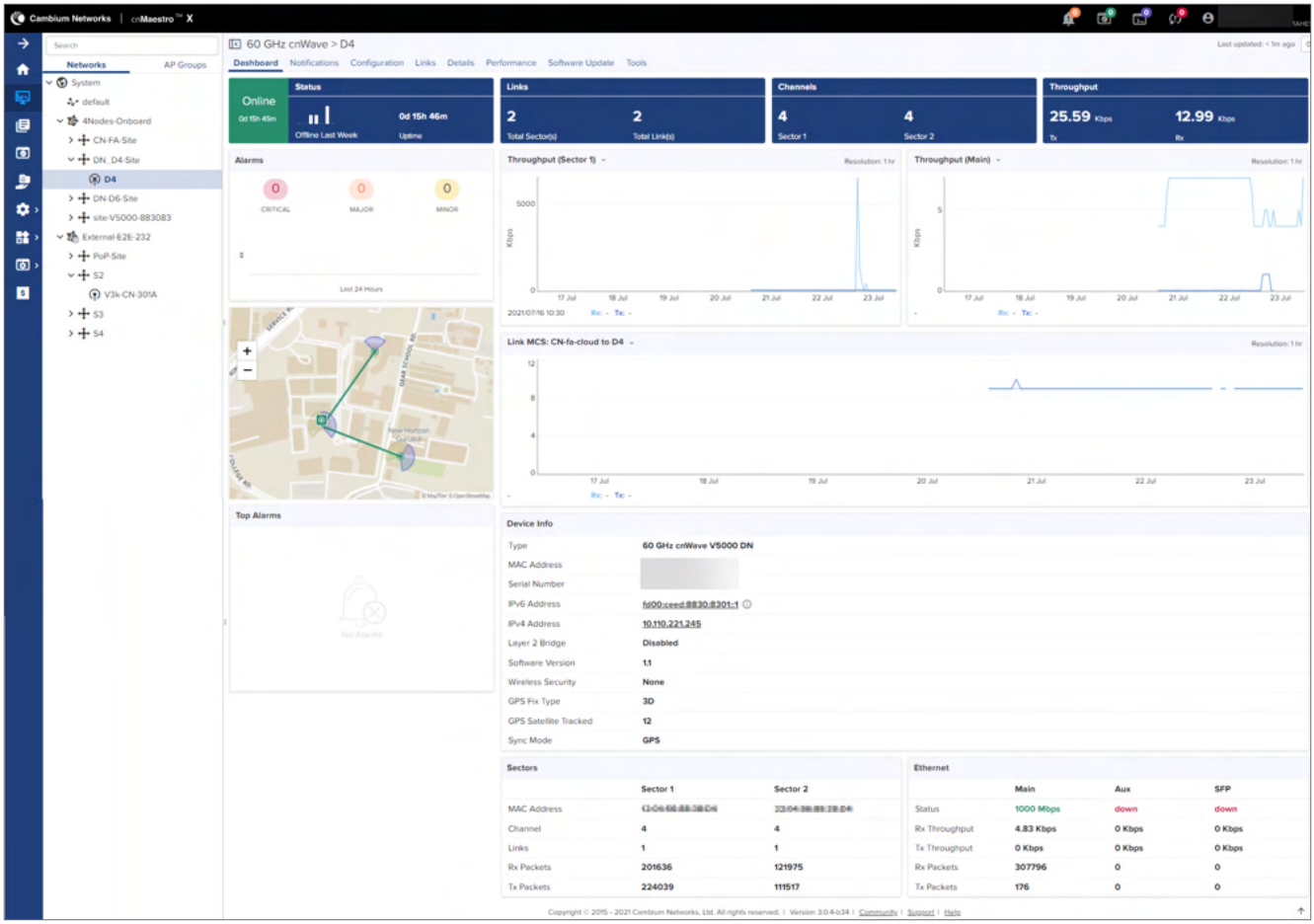
To create a new site, refer to Site.

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 409 *DN/CN Node Dashboard*



Configuration

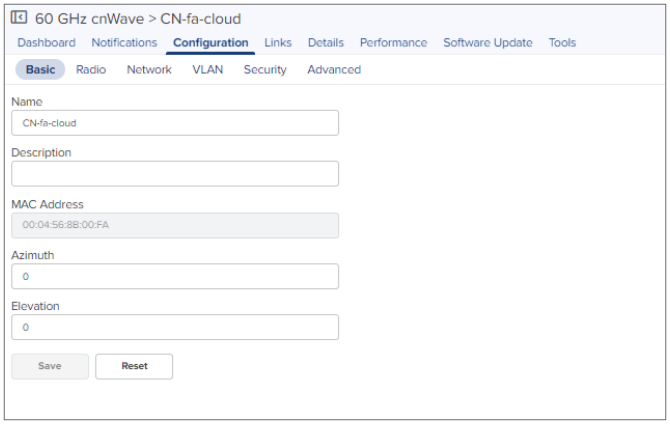
Configuration page allows the user to configure the following details of CN/DN:

- 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 410 *Basic*



Radio

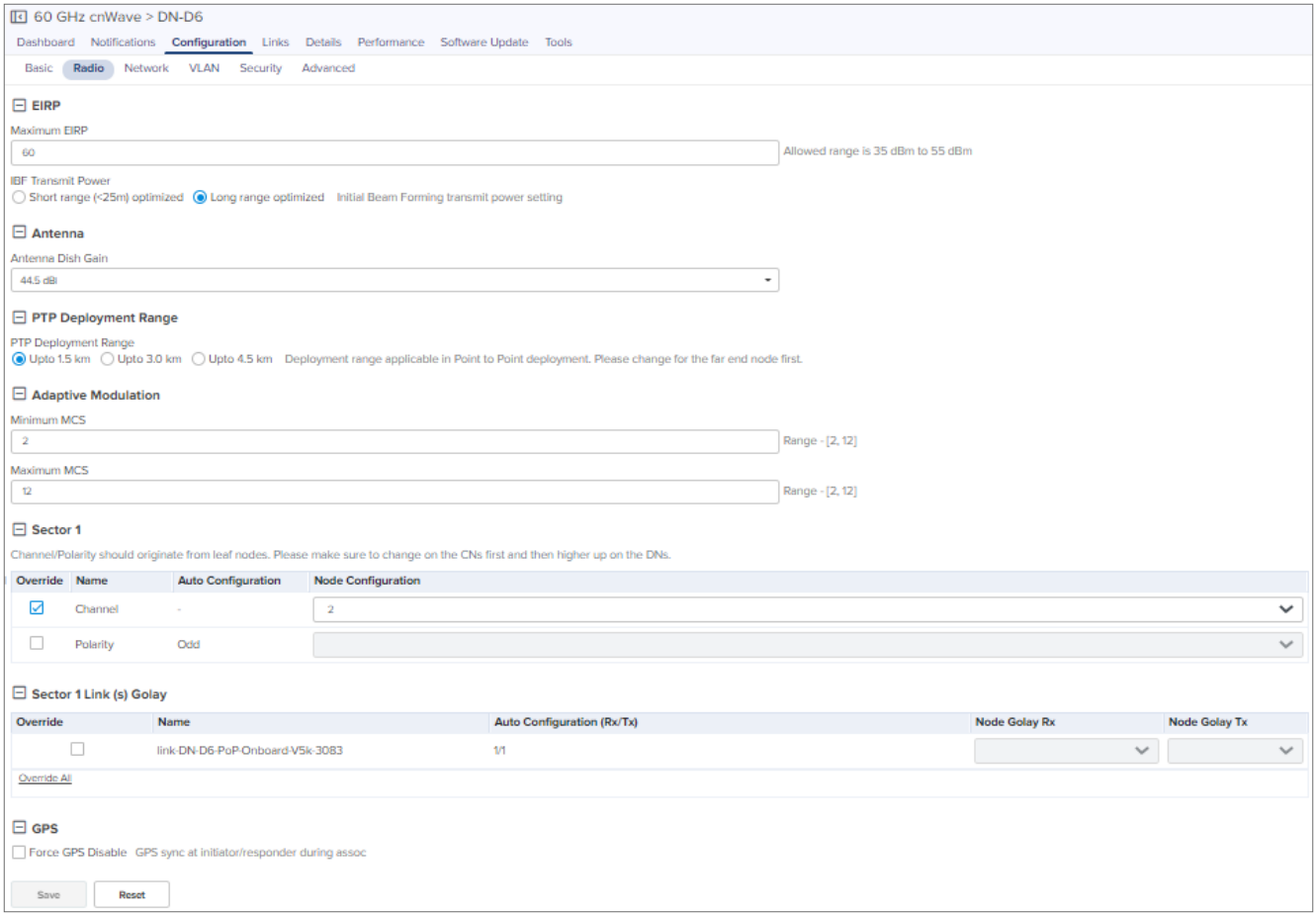


Note

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**.

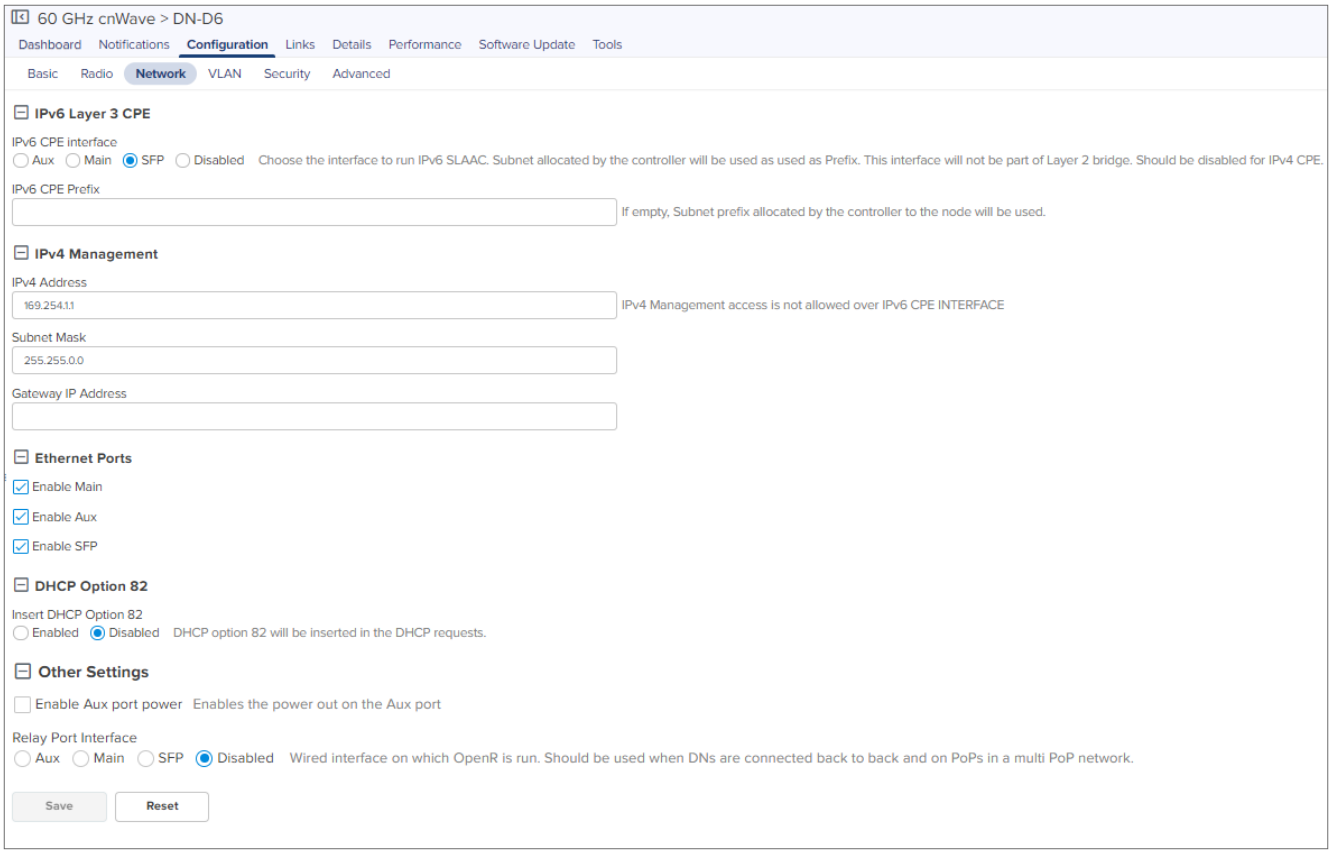
Figure 411 *Radio*



Network

Network tab allows the user to edit the **Layer 3 CPE, IPv4 Management**, **Ethernet Ports, PTP External Failover**, and **Other Settings.**

Figure 412 *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.

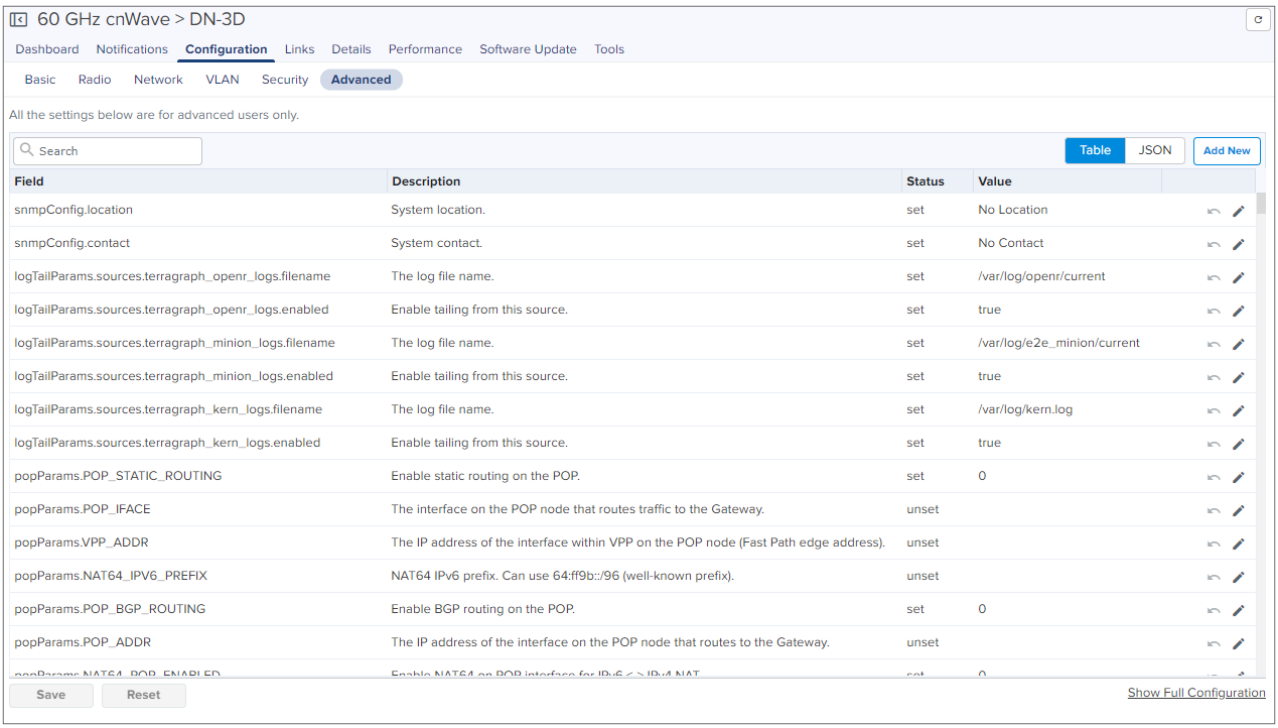
Figure 413 *Security*



Advanced

Advanced tab allows the advanced user to set Field Name and Value.

1. Navigate to **Configuration** > **Advanced.**
2. Click **Add New.**



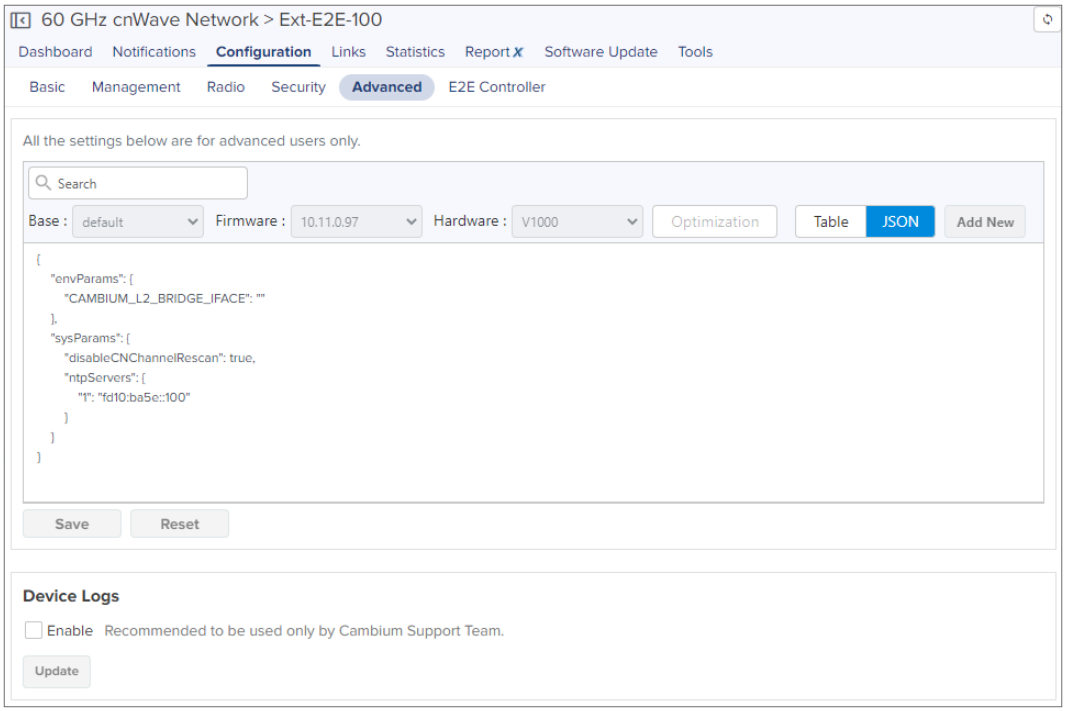
3. Enter the **Field Name** and **Value.**



4. Click **Save.**

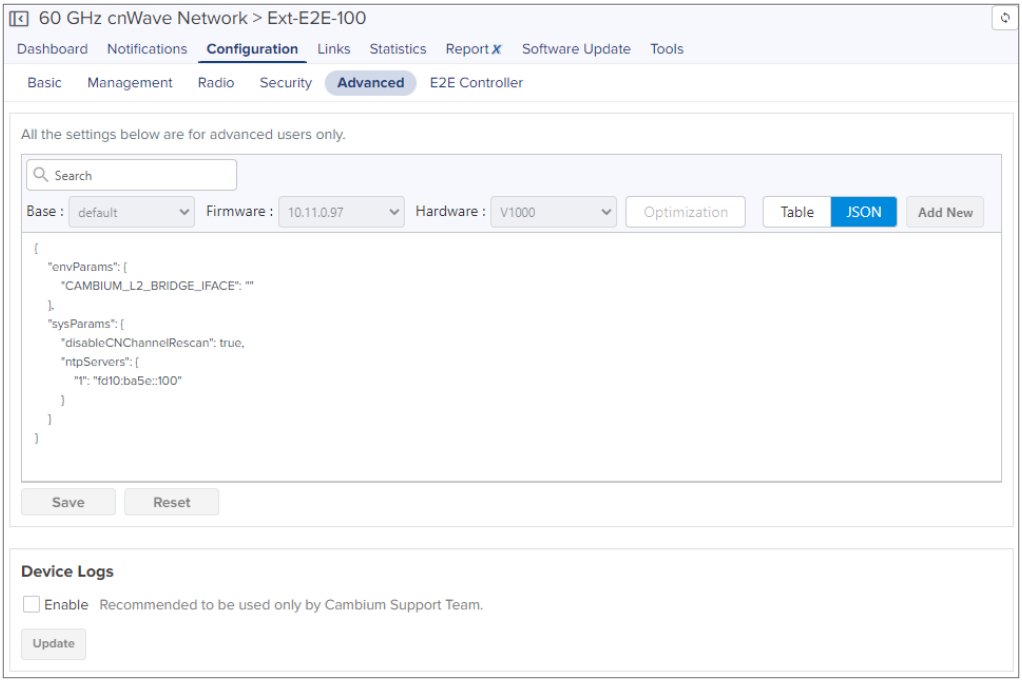
JSON

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**.

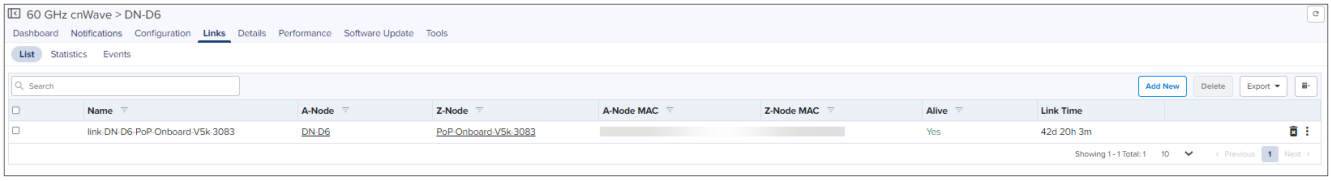
Links

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

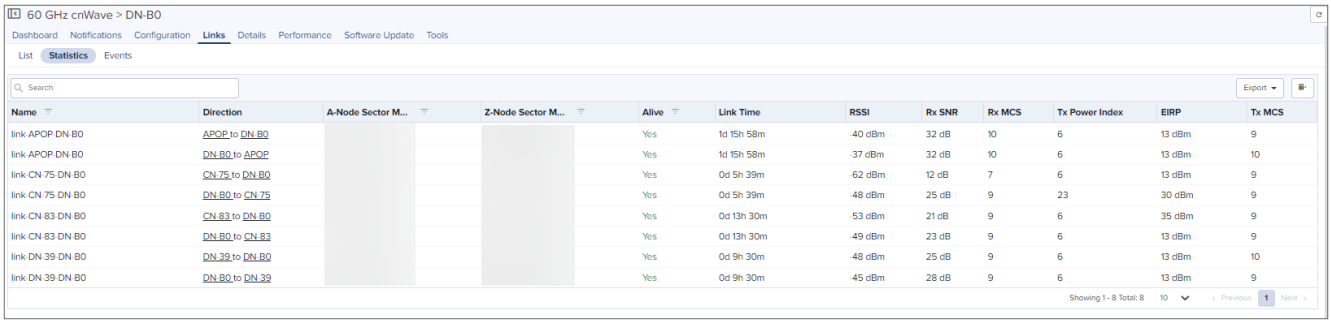
List provide the details about the links of the node and also provides the option to create a new link. User can delete the links in bulk by selecting the particular link.

Figure 414 *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 415 *Events*

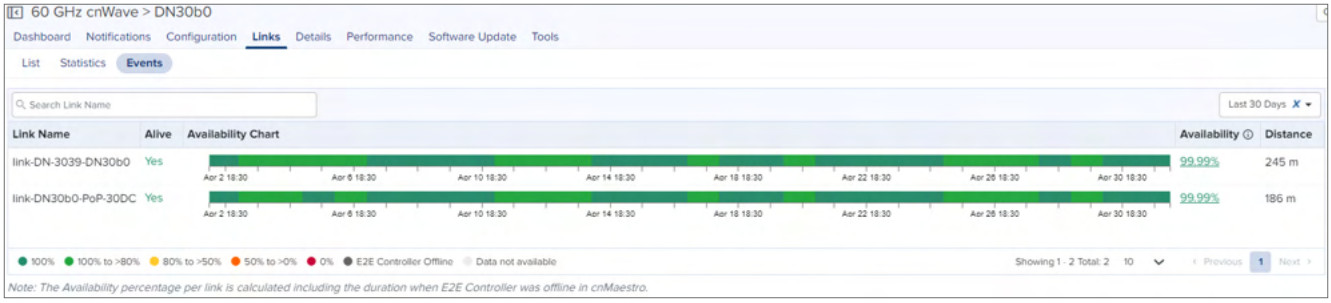


Table 90 *Events fields*

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 386. • Clicking on percentage link availability displays pop-up window as shown in Figure 387 • Link availability is presented in different colors in the chart as shown in Figure 385
Availability Percentage	• Clicking on percentage for the complete timeline link availability displays pop-up window as shown in Figure 417. • Availability of link is shown in percentage in the Availability column as shown in Figure 386.
Distance	Distance of the link in meters.

Figure 416 *Link Availability in Percentage*



Figure 417 *Link Availability details*



Availability percentage per link is calculated including the duration when E2E Controller was Offline in cnMaestro.

Figure 418 *Link Availability*

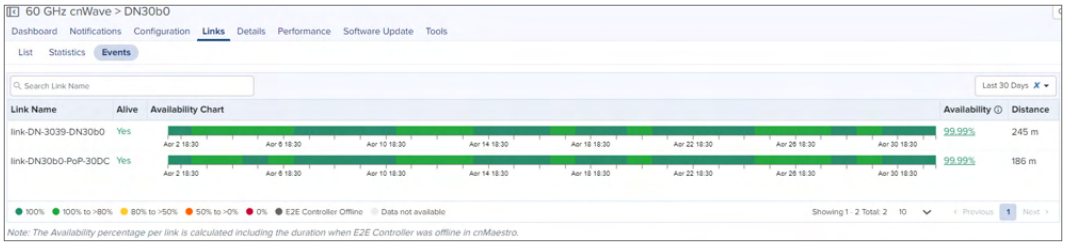
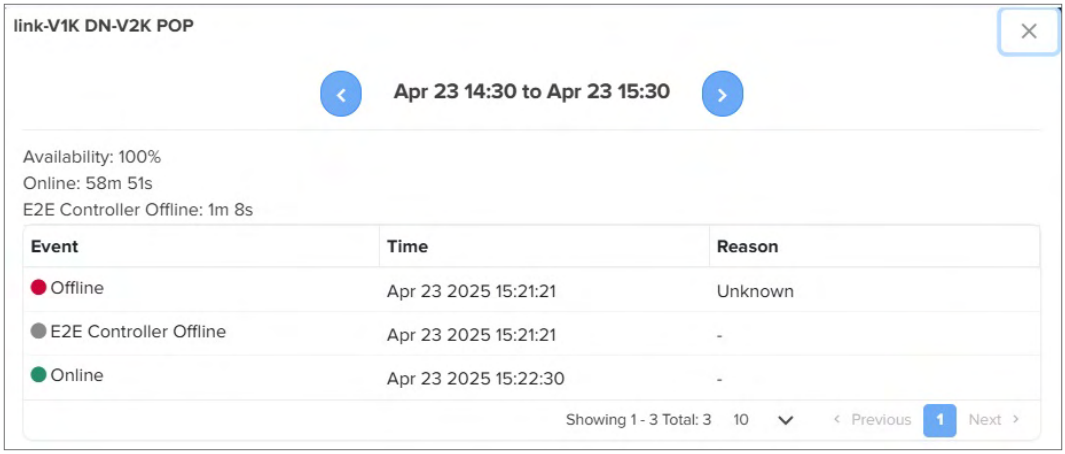


Figure 419 *Link Status*



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

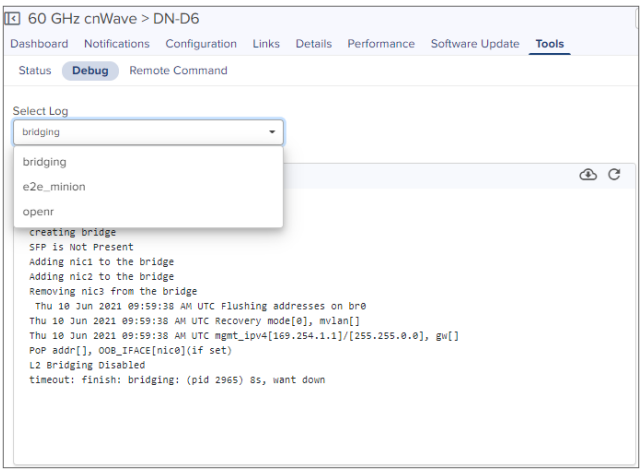
In **Debug** tab, you can view or download the DN or CN logs by executing the following log commands:

- 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:

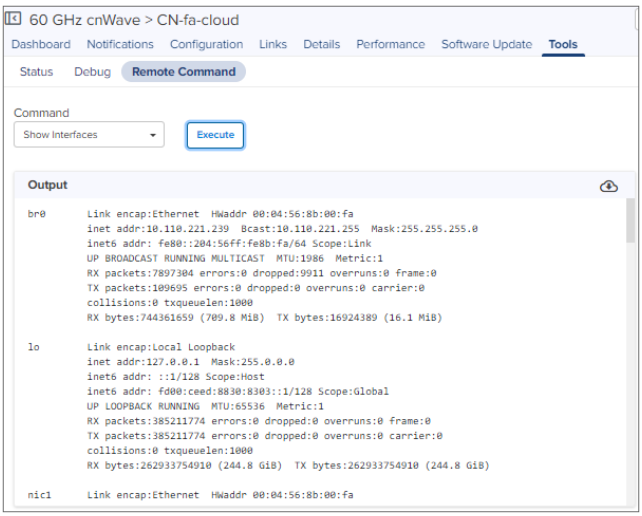
- Ping
- Show IGMP Membership Table
- Show Interfaces
- Show IPv4 Neighbors

- 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.

NSE Configuration

NSE devices are managed using the cloud-hosted cnMaestro (a management solution from Cambium Networks).

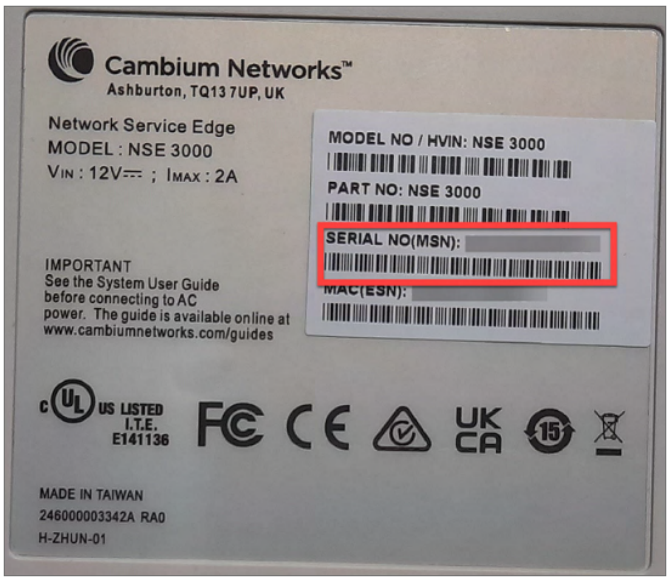
This section covers the following topics:

- Claiming an NSE device associated with a site
- High availability support for NSE
- Configuring NSE using cnMaestro Cloud
- Configuring WAN in the device UI
- Configuring Auto VPN
- Disabling or Enabling the Security Plus License Mode for NSE

Claiming an NSE device associated with a site

A device manufacturer serial number (MSN) is required to claim an NSE device. You can find the device MSN at the bottom of the device as shown in Figure 420.

Figure 420 *MSN of an NSE device*

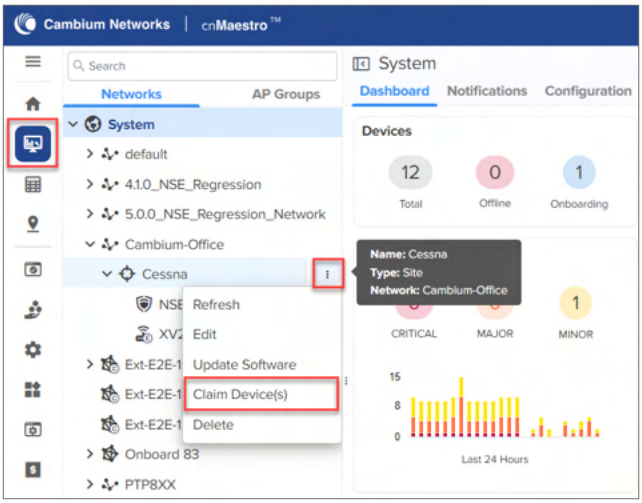


To claim an NSE device that is associated with a site, complete the following steps:

1. From the home page, navigate to **Monitor and Manage**.

   The **System** page appears, as shown in Figure 421.

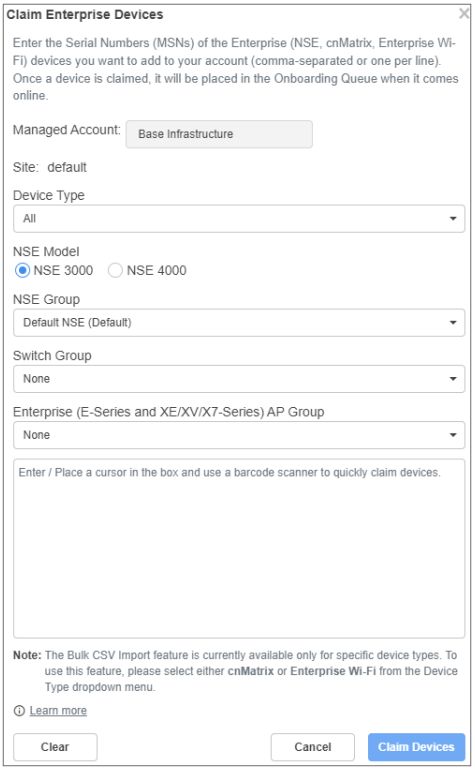
   Figure 421 *The System page*

2. On the left panel, in the **Networks** section, expand the site panel.
3. Click the actions (⋮) icon and select **Claim Device(s)**.

   The **Claim Enterprise Devices** window appears, as shown in Figure 422.

Figure 422 *The Claim Enterprise Devices window*



4. From the **NSE Group** dropdown list, select the required group.

Note

The selected NSE group is automatically pushed to the device while onboarding.

5. In the **Enter** field, enter the MSN of the NSE device.
6. Click **Claim Devices**.

   The NSE device that is associated with a site is claimed successfully.

High availability support for NSE

The high availability (HA) support allows two NSE devices to share health information when connected through a LAN port (Port-6). When the devices are connected as an HA pair, one is configured as **Primary** and the other as **Spare**. The **Spare** device serves as a backup in case of hardware failures.

If the **Primary** device goes down, the **Spare** device becomes active. When the **Primary** device is restored, it regains its active state and the **Spare** device reverts to a backup state.

Note

The HA support is available from NSE release version 1.7 and higher.

Licensing

An NSE3000 device requires a Tier-30 license to onboard to cnMaestro. An NSE4000 device requires a Tier-31 license to onboard to cnMaestro.

An HA pair (Primary - Spare) requires only one Tier-30 license. The **Spare** device does not require an additional license as it inherits the license from the **Primary** device.

On the expiry of the license, the device management is deactivated using cnMaestro. However, the devices are not deleted from the device list in cnMaestro.

Constraints on NSE devices

The following are the constraints on NSE devices in cnMaestro:

- A site can have either a single NSE device or a single NSE HA pair.
- An HA pair can only be created under a site. NSE group is mandatory for all NSE devices to onboard to the cnMaestro cloud 5.1.1 version.
- An NSE device must exist (with an NSE group attached) under the site to form an HA pair.
- If a device is in the **Onboarding** state under a site, you cannot claim another device under the same site.

Creating an HA pair in cnMaestro

You can create an HA pair using either of the following options:

- **Onboard as HA spare** (from the Onboarding queue)
- **Claim Device(s)** (at the site level)

The HA pair configuration involves the following tasks:

- Onboarding an NSE device as an HA spare
- Claiming an NSE device as an HA spare
- Moving the HA pair (in the tree)
- Deleting an NSE device from the HA pair
- Deprecation of device overrides
- Upgrading the firmware
- Viewing aggregated data of HA pair
- Creating Wireguard clients for NSE HA pair

Onboarding an NSE device as an HA spare

The primary device onboards as a standalone device to cnMaestro. An additional NSE device can be brought into the onboarding queue (without Tier-30 license) either by bulk claim (on the Onboard page) or using cambium-id and password. An HA pair is formed using the **Onboard as HA spare** option from the **Approve Device** window.



Note

- The primary device must have the firmware that supports HA functionality.
- The spare device must have the same firmware as the primary device. Otherwise, the system automatically upgrades the firmware of the spare device to match with the primary device.
- The spare device must have the same model as the primary device. For example, an

NSE3000 device can be paired only with another NSE3000 device model only. It cannot be paired with an NSE4000 device model.

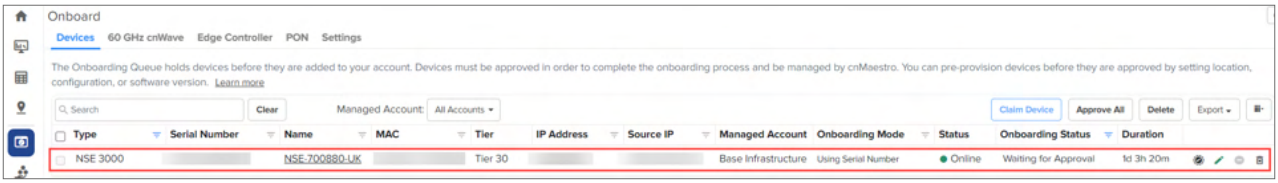
When onboarding an NSE device as a spare, the device automatically inherits the NSE group of the primary device. This holds good even if the devices are claimed at the site level. Additionally, any change in the NSE group of the primary device is automatically reflected in the spare device.

To onboard an NSE device as a spare device, complete the following steps:

1. From the home page, click the Onboard ( ) icon.

   The Onboard page appears.

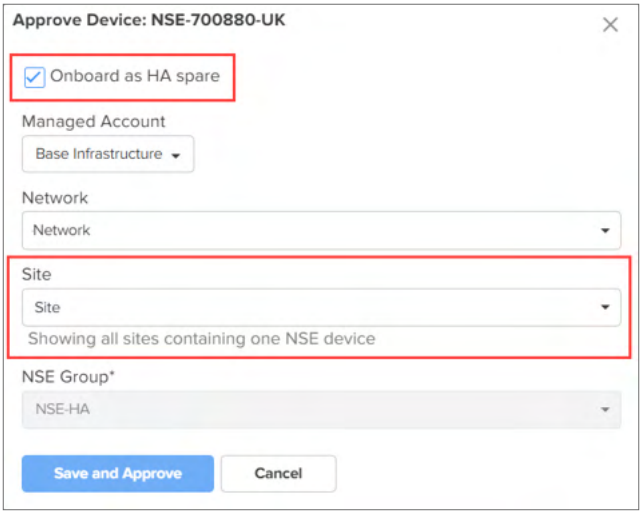
   Figure 423 *The Onboard page*



2. Click the approve device ( ) icon of the NSE device.

   The **Approve Device** window appears with the **Onboard as HA spare** option and shows all sites that have only one NSE device (as shown in Figure 424).

   Figure 424 *The Approve Device window*



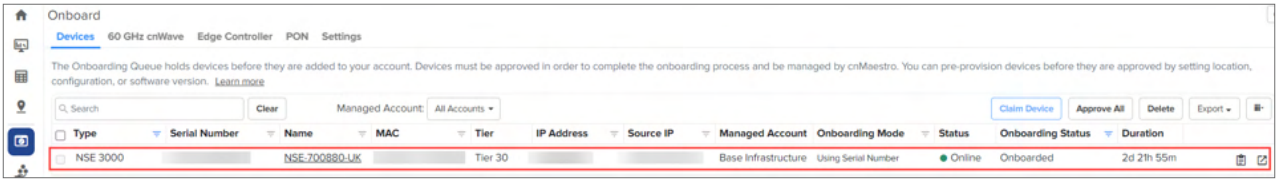
Note

The spare device has the same NSE group as that of the primary device.

3. Click **Save and Approve** from the **Approve Device** window (as shown in Figure 424).

   The spare device is onboarded (as shown in Figure 425) without an additional Tier-30 license.

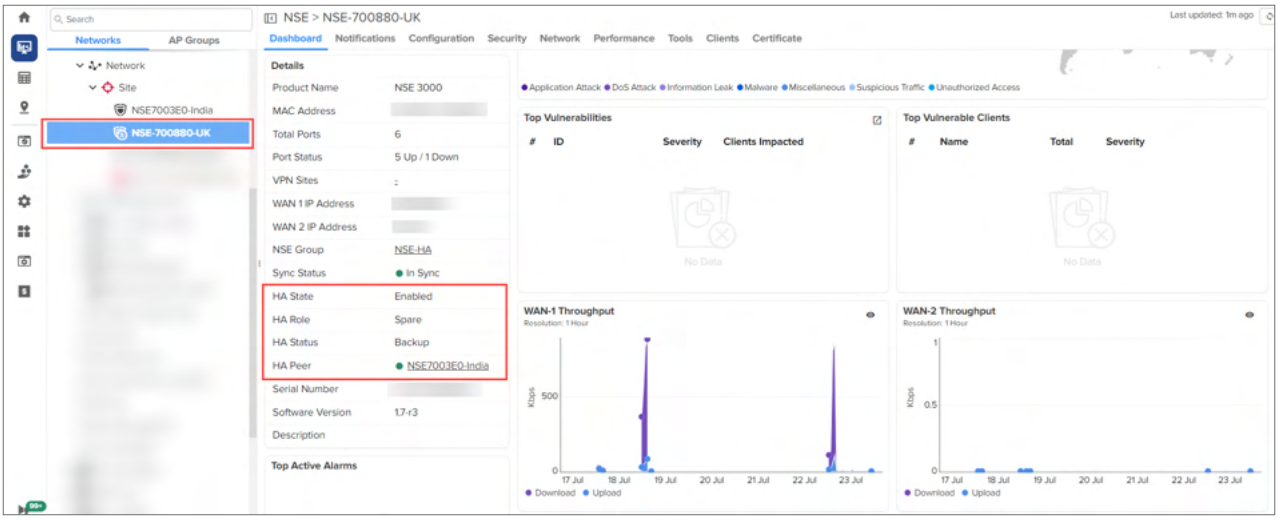
Figure 425 *Spare device onboarded*



4. Click on the spare device name.

   You can see the spare device under a site (as shown in Figure 426). You can view the HA details in the **Details** section of the dashboard (as shown in Figure 426).

Figure 426 *Details about HA for the Spare device*

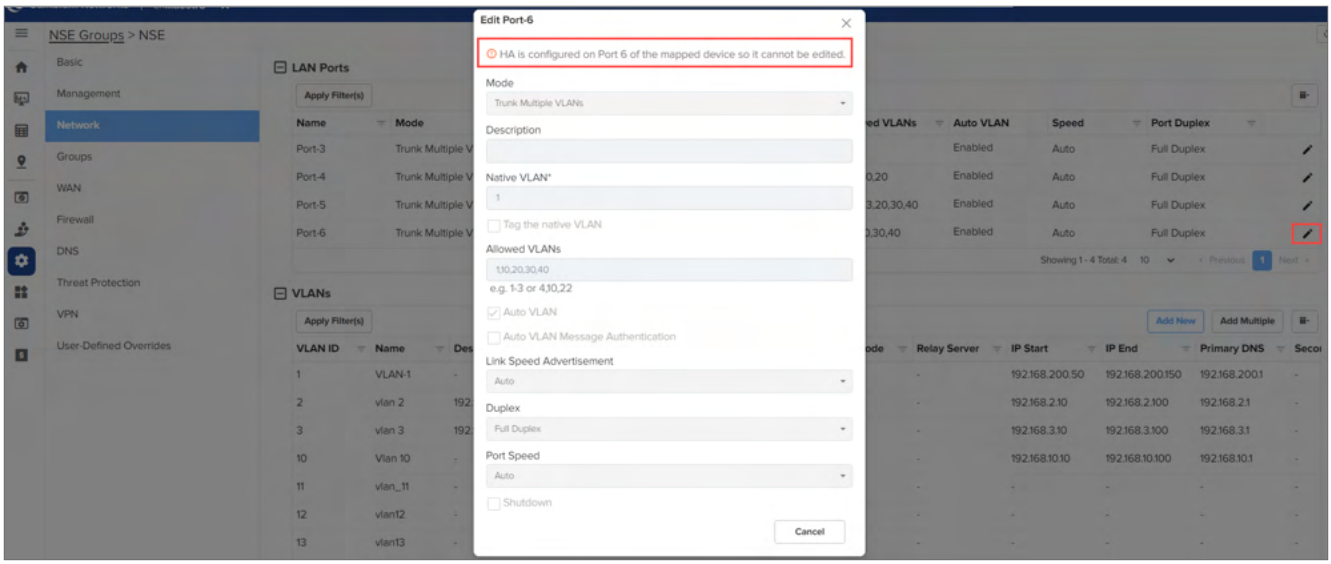




Note

When HA is configured on Port-6 of the mapped device, you cannot edit the Port-6 configuration. A message is displayed on the **Edit Port-6** window (as shown in Figure 427).

Figure 427 *The Edit Port-6 window*





Note

The fields in the **Approve Device** window (as shown in Figure 424) can also be configured using the

Edit Device ( ) icon from the **Onboard** page.

Claiming an NSE device as an HA spare

An NSE HA pair can be additionally formed using the **Claim Device(s)** option at the site level. When a second NSE device is claimed (assuming the primary already exists under the site), you have the option to claim it as a spare. However, claiming a second NSE device under the same site as a regular device is restricted.

To claim an NSE device as an HA spare, complete the following steps:

1. From the home page, click the Monitor and Manage ( ) icon.

   The **System** page appears.
2. On the left panel, in the **Networks** section, expand the site panel.
3. Click the actions ( ) icon and select **Claim Device(s)**.

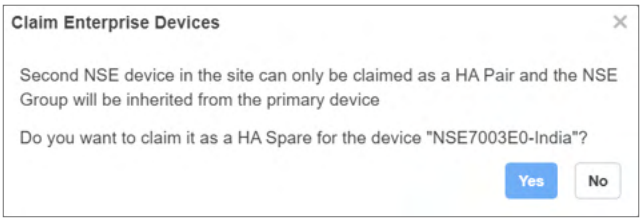
   The **Claim Enterprise Devices** window appears.
4. In the **Enter** field, enter the MSN of the NSE device.

   Note

   You can find the device MSN at the bottom of the NSE device.
5. Click **Claim Devices**.

   The **Claim Enterprise Devices** window appears.

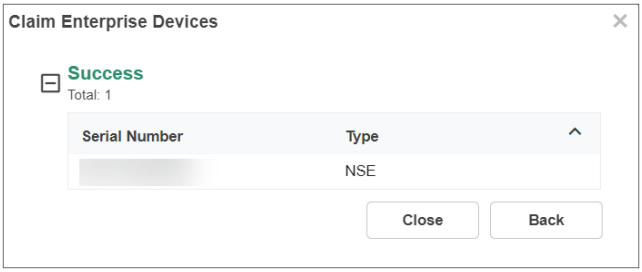
   Figure 428 *The Claim Enterprise Devices window*



6. Click **Yes**.

   The **Claim Enterprise Devices** window appears.

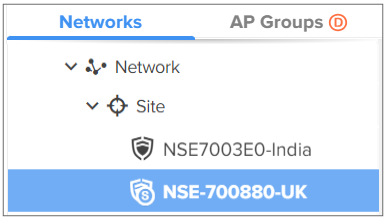
   Figure 429 *The Claim Enterprise Devices window*



7. Click **Close**.

   The device is claimed as an HA spare.

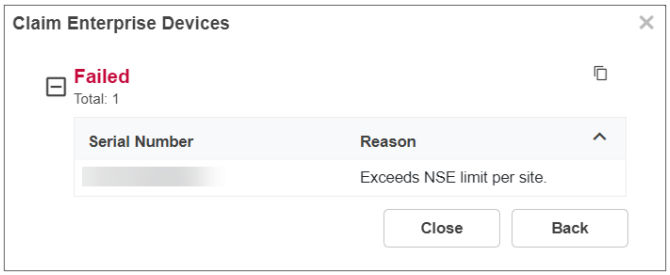
Figure 430 *Device claimed as an HA spare*



The ( ) icon indicates the primary NSE device. The ( ) icon indicates the spare NSE device.

When you click **No** in the **Claim Enterprise Devices** window (as shown in Figure 428), the **Claim Enterprise Devices** window appears (as shown in Figure 431). You cannot claim the device as an HA spare.

Figure 431 *The Claim Enterprise Devices window*



Moving the HA pair (in the tree)

The NSE HA pair can be moved as a single unit only. This can be done by changing the Network and Site for the primary device. The devices in the pair cannot be moved individually. Moreover, the NSE device or HA pair can only be moved to a site that has no NSE devices. Moving to a network is not allowed.

Note

An HA pair of NSE devices shares the same NSE group. Consequently, the NSE group selection for the spare device is disabled.

Deleting an NSE device from the HA pair

If one of the NSE devices in a pair is deleted, the other NSE device becomes standalone.

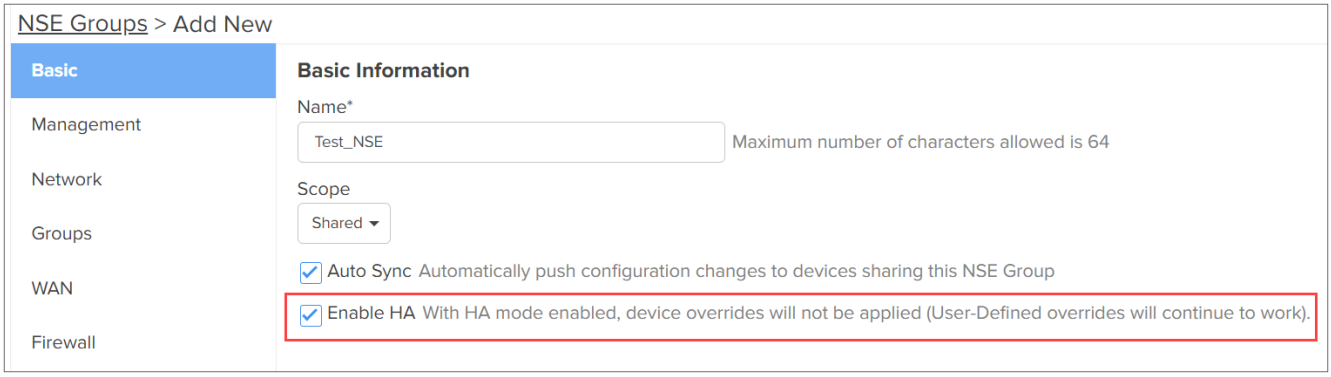
- When the primary device is deleted from the pair, the spare device becomes a standalone device and the pair's Tier-30 license is mapped to the spare device (instead of the primary device). Also, a configuration job for this standalone device with HA mode **Disable** is triggered.
- When the spare device is deleted from the pair, the primary device becomes a standalone device.
- When both primary and spare devices are deleted, a slot is released.

Deprecation of device overrides

The device overrides are removed from the Onboard page. The bulk overrides cannot be done for NSE devices.

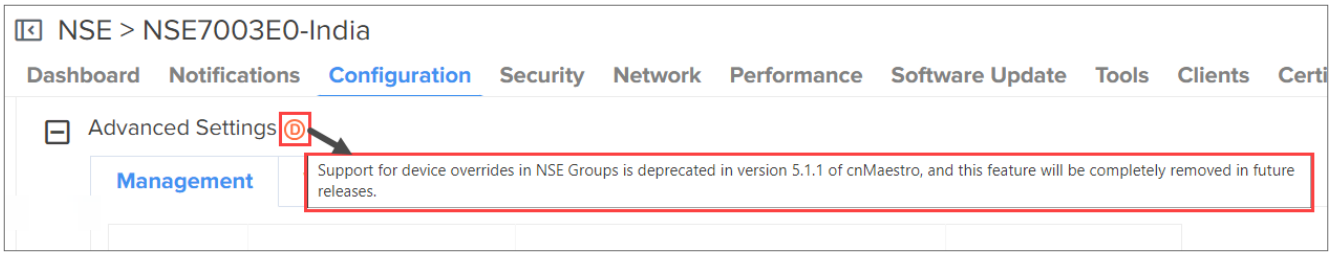
When HA is enabled in the NSE group, the device overrides in the device context are hidden.

Figure 432 *Device overrides are not applied when HA is enabled*



When HA is disabled in the NSE group, the deprecated icon ( ) is shown. Device overrides are being deprecated for NSE devices in the 5.1.1 version. When you hover the cursor over the deprecated ( ) icon, a message about the deprecation is displayed (as shown in Figure 433).

Figure 433 *A deprecation message*



Upgrading the firmware

When you upgrade the firmware on the primary device, the firmware on the spare device is automatically upgraded. This ensures that both primary and spare devices run the same version.

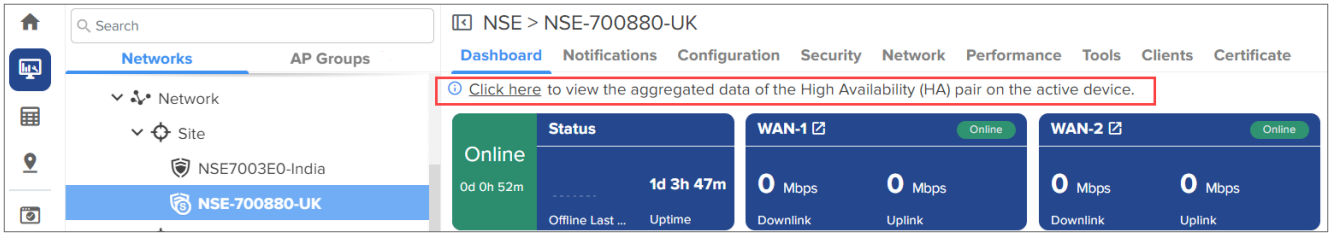
Note

The **Software Update** tab is available only for the primary device.

Viewing aggregated data of HA pair

In an HA pair, the active NSE device shows the aggregated data for the pair. In the spare NSE device, a banner provides a link to the active device's page (as shown in Figure 434) to view the aggregated data. The same banner is displayed under the **Security** > **Threats**, **Security** > **Vulnerabilities**, and **Clients** > **Local** tabs.

Figure 434 *Banner*



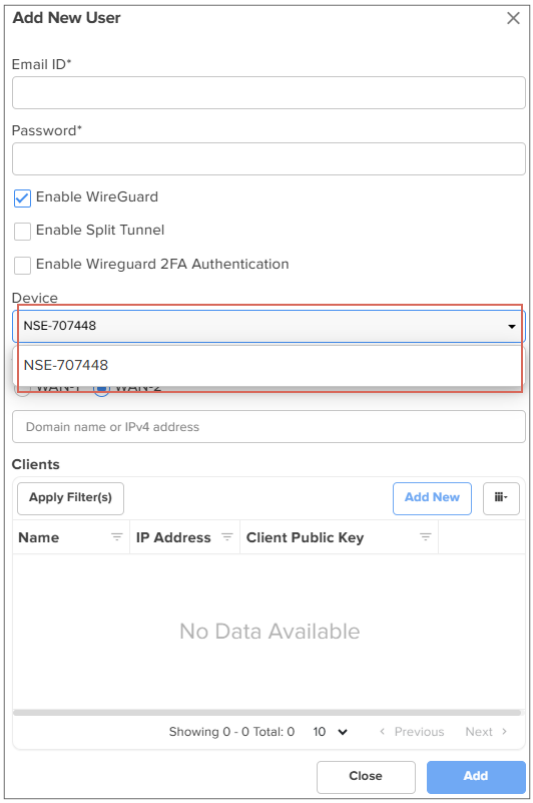
Note

- If the active device is offline, the aggregated data is not shown.

Creating Wireguard clients for NSE HA pair

When adding Wireguard clients from the **VPN** page, only the primary device is listed in the **Device** dropdown list (as shown in Figure 435).

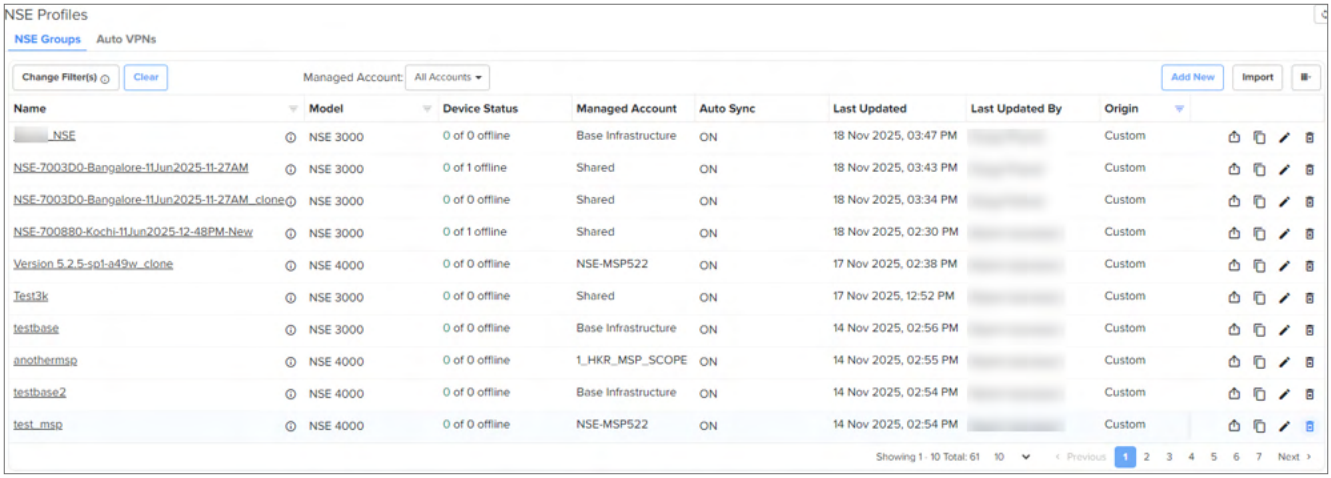
Figure 435 *The Add New User window -Wireguard*



Configuring NSE using cnMaestro Cloud

To configure NSE devices, create configuration profiles called NSE Groups. To create and configure a new NSE 3000 group, navigate to **Configuration** > **NSE Profiles**. Select the **NSE Groups** tab and click **Add New**.

Figure 436 *Creating NSE groups*



For a new NSE group, you must configure parameters using the following tabs:

- Basic
- Management
- Network
- Groups
- WAN
  - Adding a virtual WAN interface
  - Configuring rule precedence
- Firewall
  - Automatically assigning system-generated names to existing DNAT rules
- DNS
- Threat Protection
- VPN
- User-Defined Overrides

Basic

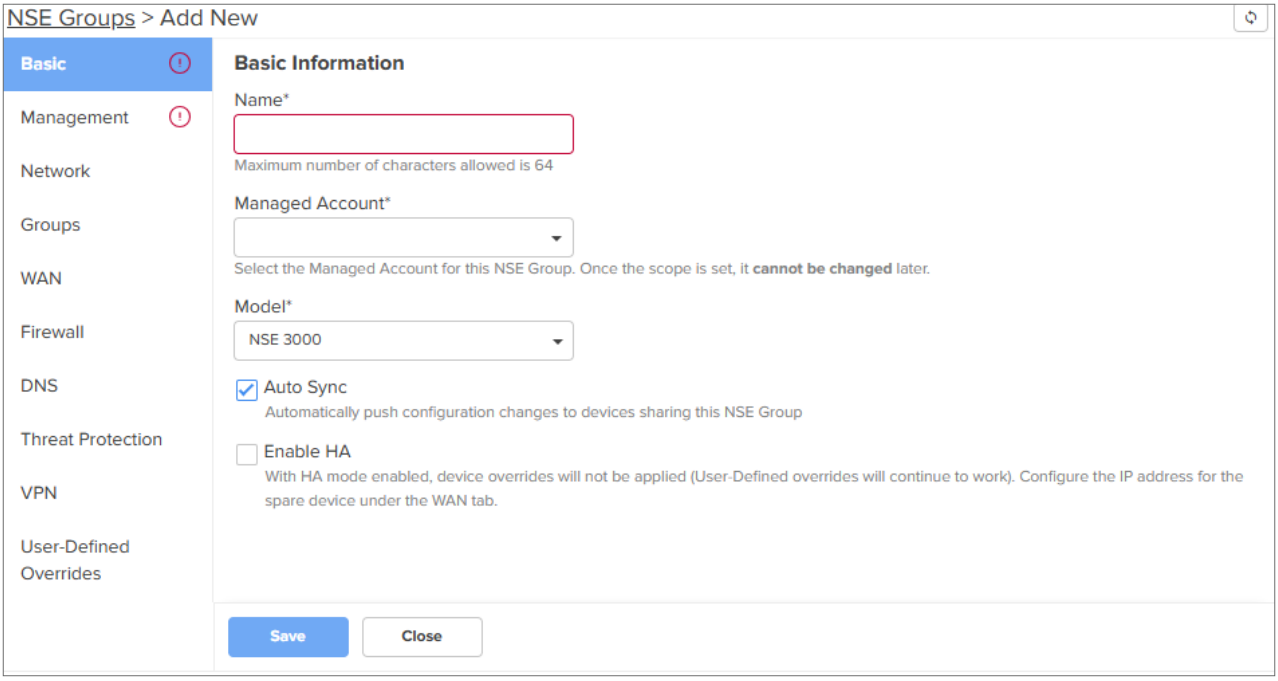
Using the **Basic** tab, you can configure basic group information, such as group name and group Managed Account. You have the option to enable automatic synchronization of the configuration changes for devices associated with the NSE group.

To configure parameters on the **Basic Information** page, complete the following steps:

1. Navigate to **Configuration** > **NSE Groups** and click **Add New**

   The **Basic Information** page appears, as shown in Figure 437.

Figure 437 *The Basic Information page*



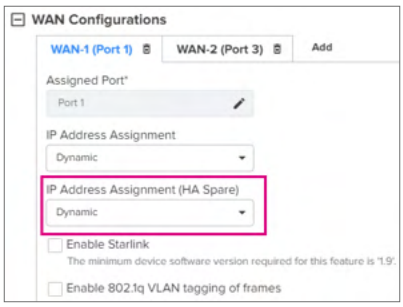
2. Configure the parameters, as described in Table 91.

Table 91 *Parameters on the Basic Information page*

Parameter	Description
Name	Name for the NSE group. This parameter allows a maximum of 64 characters. This is a mandatory parameter.
Managed Account	Determines the availability of the NSE group across different tenant accounts. By default, the following options are supported: • **Basic Infrastructure -** Configured NSE group will be available only to the Basic Infrastructure user. Other tenant accounts will not have access to the NSE group.
Model	NSE device platform for which the NSE group is configured. The following NSE platforms are supported: • NSE3000 • NSE4000
Auto Sync	Specifies whether the configuration changes made to the NSE group are automatically applied to all devices associated with the group. By default, auto sync is enabled.
Enable HA	Enables or disables the HA. By default, this parameter is disabled. **Note**: When this parameter is enabled, you must configure the **IP Address (HA Spare)** parameter by

Parameter	Description
	selecting the **Static** option from the **IP Address Assignment** dropdown list in the **WAN Configurations** section of the **WAN** screen (as shown in Figure 438).

Figure 438 *The WAN Configurations section*



3. Click **Save**.

Management

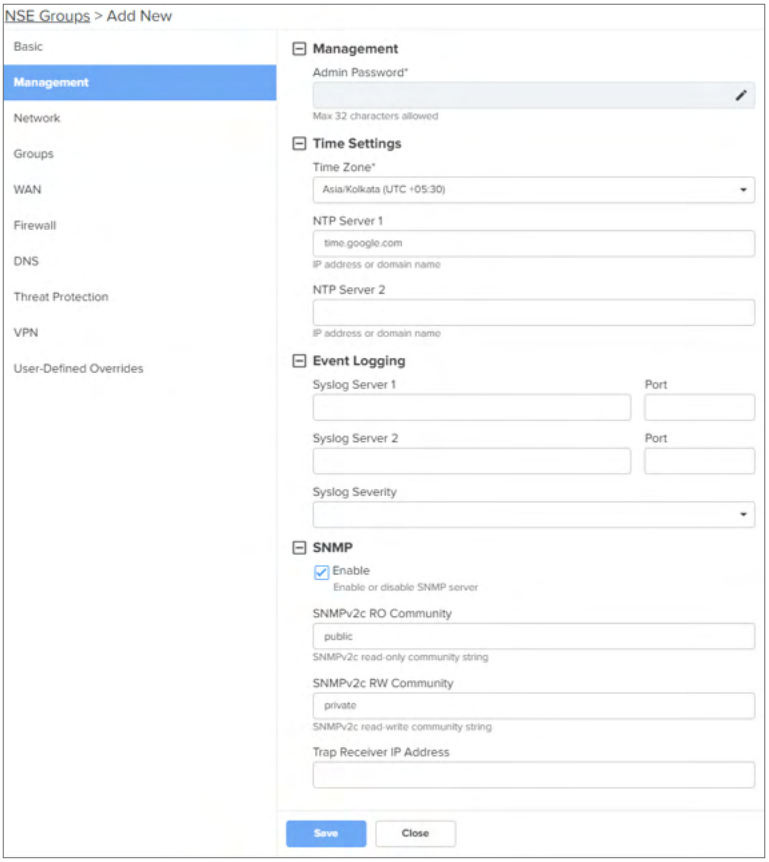
Using the **Management** tab, you can configure the profile-related parameters such as time settings and event logging.

To configure parameters on the **Management** page, complete the following steps:

1. On the **NSE Groups > Add New** page, select the **Management** tab.

   The **Management** page appears, as shown in Figure 439.

Figure 439 *The Management page*



2. Configure the parameters, as described in Table 92.

Table 92 *Parameters on the Management page*

Parameter	Description
On the Management page, there are **Management**, **Time Settings**, and **Event Logging** sections.	
Management	
Admin Password	The password used to authenticate the NSE users who access through SSH or web. This parameter allows a maximum of 32 characters. This is a mandatory parameter. **Note**: Click the edit icon to reset the password.
Time Settings	
Time Zone	The time zone based on the installation location of the device. Select an appropriate time zone from the dropdown list to ensure that the device clock is synchronized with the wall clock time.
NTP Server 1	The IPv4 address or domain name of the primary Network Time Protocol (NTP) server.
NTP Server 2	The IPv4 address or domain name of the secondary or a backup NTP server.
Event Logging	
Syslog Server 1	The IPv4 address or the domain name of the syslog server 1.
Port	The port number of the syslog server 1 to which the syslog messages are sent.

Parameter	Description
	Supported value: 1 to 65535.
Syslog Server 2	The IPv4 address or the domain name of the syslog server 2.
Port	The port number of the syslog server 2 to which the syslog messages are sent. Supported value: 1 to 65535.
Syslog Severity	The logs with the selected severity level that must be forwarded to the server. The following options are supported: • **Emergency (Level 0)** • **Alert (Level 1)** • **Critical (Level 2)** • **Error (Level 3)** • **Warning (Level 4)** • **Notice (Level 5)** • **Info (Level 6)** • **Debug (Level 7)**
SNMP By default, SNMP is disabled.	
Enable	Determines whether SNMPv2c support on the router is enabled. Select the checkbox to enable SNMPv2c support.
SNMPv2c RO Community	SNMP v2c read-only community string used as a password when obtaining information from the router.
SNMPv2c RW Community	SNMP v2c read-write community string used as a password when writing information to the router.
Trap Receiver IP Address	IPv4 address of the SNMP server to receive the SNMP traps.

3. Click **Save**.

Network

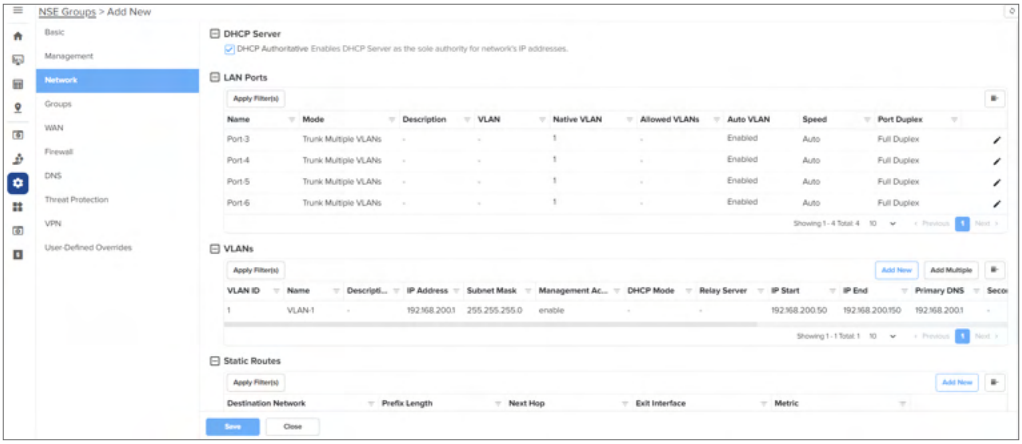
Using the **Network** tab, you can configure LAN ports, VLANs, and static routes.

To configure parameters on the **Network** page, complete the following steps:

1. On the **NSE Groups > Add New** page, select the **Network** tab.

   The **Network** page appears, as shown in Figure 440.

Figure 440 *The Network page*



2. Configure the parameters, as described in Table 93.

Table 93 *Parameters on the Network page*

Parameter	Description
On the Network page, there are **DHCP Server**, **LAN Ports**, **VLANs**, and **Static Routes** sections.	
DHCP Server	
DHCP Authoritative	Indicates that the DHCP server is the primary and trusted source for IP address assignments in the network. This parameter is enabled by default.
LAN Ports Click the edit icon to modify the configuration of the corresponding LAN port as shown in Figure 441, and click **Update** to apply the changes.	
Name	Name of the LAN port. This parameter cannot be modified.
Mode	The VLAN mode of the port. The following options are supported: • **Access Single VLAN**: An access port which places all traffic on its configured VLAN and only passes untagged traffic. • **Trunk Multiple VLANs**: A trunk port which allows the selected port to accept or pass 802.1Q tagged traffic.
Description	A brief description of the LAN port.
VLAN	This parameter is applicable only when the **Mode** parameter is set to **Access Single VLAN**. By default, VLAN value is 1. VLAN value can be in the range: 1 to 4094 This is a mandatory parameter.
Native VLAN	Indicates that the traffic on the native VLAN is untagged. This parameter is applicable only when the **Mode** parameter is set to **Trunk Multiple VLANs**.

Parameter	Description
	The Native VLAN value can be in the range: 1 to 4094 This is a mandatory parameter.
Tag the native VLAN	This parameter is applicable only when the **Mode** parameter is set to **Trunk Multiple VLANs**. When the **Tag the native VLAN** parameter is enabled, the native VLAN traffic is tagged with 802.1Q.
Allowed VLANs	This parameter is applicable only when the **Mode** parameter is set to **Trunk Multiple VLANs**. This parameter supports a range or comma-separated list of VLANs. Example: 1-3 or 4, 10, 22
Auto VLAN	This parameter is applicable only when the **Mode** parameter is set to **Trunk Multiple VLANs**. This parameter facilitates automatic assignment of VLANs in cnMatrix switches and access points (APs). When this parameter is enabled, the cnMatrix switches and APs use the Link Layer Discovery Protocol (LLDP) packets to obtain a list of VLANs for automatic assignment. **Note**: Auto VLAN works only with cnMatrix switches and access points (APs). It does not work with any third-party switches and APs. Auto VLAN allows cnMatrix switch to dynamically learn VLANs from an AP. The AP advertises the configured VLANs to the cnMatrix switch. The cnMatrix switch then advertises those VLANs to the uplink NSE device. This process ensures that VLANs are properly bridged. This parameter is enabled by default.
Auto VLAN Message Authentication	This parameter is applicable only when the **Mode** parameter is set to **Trunk Multiple VLANs**. This parameter enables authentication for the LLDP messages where the VLANs are advertised. This parameter is enabled by default.
Link Speed Advertisement	Indicates the port speed that must be configured for advertisement. Default: Auto The following options are supported: • **Auto** • **10 Mbps** • **100 Mbps** • **1000 Mbps** • **2500 Mbps** (Applicable only to NSE4000 devices)
Port Duplex	Specifies the mode of port communication. The following options are supported: • **Full Duplex** • **Half Duplex**
Port Speed	Specifies the port speed. Default: Auto

Parameter	Description
	The following options are supported: • **Auto** • **10 Mbps** • **100 Mbps** • **1000 Mbps** • **2500 Mbps** (Applicable only to NSE4000 devices)
Shutdown	Enables or disables the port. By default, this parameter is disabled.
VLANs **Note**: The recommended number of VLANs configurable is 250 on NSE3000 devices and 500 on NSE4000 devices. To add a new VLAN, click **Add New**. The **Add New VLAN** window appears, as shown in Figure 442. To edit an existing VLAN configuration, click the edit icon and modify the parameters in the **Edit VLAN** window. Finally, click **Update** to apply the changes.	
VLAN ID	Indicates the VLAN ID. The VLAN ID value can be in the range: 1 to 4094 This is a mandatory parameter.
Name	Name of the new VLAN. This is a mandatory parameter.
Description	Displays the user-configured description for the VLAN.
IP Address	IPv4 address that is assigned to the VLAN. This is a mandatory parameter.
Subnet Mask	Subnet mask that is assigned to the VLAN. This is a mandatory parameter.
Management Access	Indicates whether the management access is enabled or disabled. By default, this parameter is enabled.
Enable Rate Limit	Indicates whether the rate limit is enabled or disabled. By default, this parameter is disabled. When you select the **Enable Rate Limit** checkbox, the **Rate Limit** parameter appears**.**
Rate Limit	Specifies the rate of requests sent or received. This parameter appears only when you enable the **Enable Rate Limit** parameter. This parameter supports only integer values. This is a mandatory parameter.
Enable Port Scan	A scan identifies open ports within a network and helps in detecting potential vulnerabilities that can be exploited by attackers. By default, this parameter is enabled.
Enable Device	Enables device information (such as MAC, Manufacturer, Type, Model, and OS) of

Parameter	Description
Identification	clients connected to NSE devices to be displayed in the NSE **Clients** page. **Note** This option is available for the following subscribers: • Essentials subscribers in the Security Plus mode • cnMaestro X subscribers
Enable Inter-VLAN Routing	Enables routing of traffic between this VLAN and other VLANs. By default, this parameter is enabled.
DHCP mode	Specifies the DHCP mode. The following options are supported: • **None** • **DHCP Server—**When you select this option, the DHCP server-related parameters appear. • **DHCP Relay—**When you select this option, the **Relay Server IP address** parameter appears.
DHCP Server In addition to the below parameters, you must also configure the parameters in the **DHCP Options** and **MAC Binding List** sections, as shown in Figure 443.	
Start IP address	Starting IPv4 address in the range. This is a mandatory parameter.
End IP address	Ending IPv4 address in the range. This is a mandatory parameter.
Primary DNS	The primary DNS server for clients on the network. If the DNS server option is enabled on the NSE, the IPv4 address configured for the VLAN can be provided as the DNS server for the network.
Secondary DNS	The secondary DNS server for clients on the network.
Domain	The DNS search domain for the network.
Lease Time	The DHCP lease expiry time for the DHCP pool (in days, hours, and minutes). This is a mandatory parameter.
DHCP Options NSE allows configuration of standard and custom DHCP options. To add a new DHCP option, click **Add New**. The **Add New DHCP Option** window appears, as shown in Figure 444. To edit an existing DHCP option, click the edit icon and modify the parameters in the **Edit DHCP Option** window. Finally, click **Update** to apply the changes.	
Option	The following DHCP options are supported: • **Log server(7)** • **Domain name(15)**

Parameter	Description
	• **NTP server(42)** • **Vendor specific information(43)** • **Vendor class identifier(60)** • **TFTP server name(66)** • **Boot file name(67)** • **Proxy auto config(252)** • **Custom** This is a mandatory parameter.
Code	A value for the code. This parameter allows a maximum value of 254. This is a mandatory parameter.
Type	The following options are supported: • **Text** • **IP Address** • **Integer** This is a mandatory parameter.
Value	A value in ASCII. This is a mandatory parameter.
MAC Binding List For every DHCP pool configured, the user can bind the client MAC address with an IPv4 address from the network. This enables the client to obtain the same IPv4 address whenever they connect to the NSE device. Following parameters are required to create the binding list: • MAC address of the client • IPv4 address from the configured pool When you set **MAC** and **IP address** fields and click **Add**, the binding of MAC and IP address is added. **Note**: Upto 200 MAC to IP address bindings are supported per DHCP pool. **Note**: When you bind, the binding IP address should be outside the DHCP pool range. To add a new MAC binding, click **Add New**. The **Add New MAC Binding** window appears, as shown in Figure 445. To edit an existing MAC binding, click the edit icon and modify the parameters in the **Edit MAC Binding** window. Finally, click **Update** to apply the changes.	
MAC	The MAC address of the client. This is a mandatory parameter.
IP Address	The IPv4 address that must be assigned to the client. This is a mandatory parameter.
Description	Displays the user-configured description.

Parameter	Description
Import	Imports the MAC bindings. **Note**: The CSV file that you import must be in the three-column format, for example, MAC, IP address, and Description. To import MAC bindings, click **Import**. The **Import MAC Bindings** window appears, as shown in Figure 446.
Replace existing list	Indicates whether the imported bindings will overwrite the existing list or append to the list. • If enabled, the imported bindings will overwrite the existing list • If disabled, the imported bindings will append to the existing list. By default, this parameter is enabled.
Export	Exports the configured bindings list. The following options are supported: • **Export all as CSV** • **Export page as CSV** To export MAC bindings, click **Export**. The export options appear, as shown in Figure 447.
DHCP Relay	Indicates whether the DHCP relay unicasts the DHCP request to an external DHCP server. This is a mandatory parameter.
Relay Server IP address	IPv4 address of the external DHCP server. This is a mandatory parameter.
Static Routes To add a new route, click **Add New**. The **Add New Route** window appears, as shown in Figure 448. To edit an existing route, click the edit icon and modify the parameters in the **Edit Route** window. Finally, click **Update** to apply the changes.	
Destination Network	The IPv4 address of the destination network. This is a mandatory parameter.
Prefix Length	The prefix length for the network address. This parameter supports integer values and a maximum value of 32. This is a mandatory parameter.
Next Hop	The next hop IPv4 address for the route. This is a mandatory parameter.
Exit Interface	The exit interface through which the next hop is reachable. This is a mandatory parameter.
Metric	The metric for the route.
To add multiple VLANs, click the **Add Multiple** button. The **Add Multiple VLANs** window appears, as shown in Figure 449.	

Parameter	Description
To edit an existing VLAN configuration, click the edit icon and modify the parameters in the **Edit VLAN** window. Finally, click **Update** to apply the changes.	
Description	Displays the user-configured description for the VLAN.
First VLAN ID	Indicates the first VLAN ID. The supported VLAN ID value range is between 1 and 4094. This is a mandatory parameter.
Number of VLANs	Indicates the number of VLANs that you want to add. **Note**: You can configure up to 128 VLANs. This is a mandatory parameter.
Subnet The following options are supported: • **IP Address and Netmask** - When you select this option, the **IP address** and **Netmask** options appear. • **Hosts per subnet** - When you select this option, the **First IP Address** and **Hosts per subnet** options appear.	
IP address	The IPv4 address of the first VLAN. This is a mandatory parameter.
Netmask	The netmask of the subnet. This is a mandatory parameter.
First IP Address	The first IPv4 address of the subnet. This is a mandatory parameter.
Hosts per subnet	The number of hosts that you want for the subnet. This is a mandatory parameter.
Enable Rate Limit	Indicates whether the rate limit is enabled or disabled. By default, this parameter is disabled. When you select the **Enable Rate Limit** checkbox, the **Rate Limit** parameter appears**.**
Rate Limit	Specifies the rate of requests sent or received. This parameter appears only when you enable the **Enable Rate Limit** parameter. This parameter supports only integer values. This is a mandatory parameter when you enable rate limit.
DHCP mode	Specifies the DHCP mode. The following options are supported: • **None** • **DHCP Server -** When you select this option, the DHCP server-related parameters appear. • **DHCP Relay -** When you select this option, the **Relay Server IP address** parameter appears.
Lease Time	The DHCP lease expiry time for the DHCP pool (in days, hours, and minutes).

Parameter	Description
	This is a mandatory parameter.
DHCP Options NSE allows configuration of standard and custom DHCP options. To add a new DHCP option, click **Add New**. The **Add New DHCP Option** window appears, as shown in Figure 444. To edit an existing DHCP option, click the edit icon and modify the parameters in the **Edit DHCP Option** window. Finally, click **Update** to apply the changes.	
Option	The following DHCP options are supported: • **Log server(7)** • **Domain name(15)** • **NTP server(42)** • **Vendor specific information(43)** • **Vendor class identifier(60)** • **TFTP server name(66)** • **Boot file name(67)** • **Proxy auto config(252)** • **Custom** This is a mandatory parameter.
Code	A value for the code. This parameter allows a maximum value of 254. This is a mandatory parameter.
Type	The following options are supported: • **Text** • **IP Address** • **Integer** This is a mandatory parameter.
Value	A value in ASCII. This is a mandatory parameter.
DHCP Relay	Indicates whether the DHCP relay unicasts the DHCP request to an external DHCP server. This is a mandatory parameter.
Relay Server IP address	IPv4 address of the external DHCP server. This is a mandatory parameter.
ERSPAN The NSE ERSPAN feature allows users to monitor traffic on WAN, LAN, or VLANs and send the monitored traffic to destination ports.	

Parameter	Description
To add a new ERSPAN session, click **Add New**. The **Add New ERSPAN Session** window appears, as shown in Figure 450. To edit an existing ERSPAN session, click the edit icon and modify the parameters in the **Edit ERSPAN Session** window. Finally, click **Update** to apply the changes.	
Enable	Determines whether ERSPAN is enabled on the NSE device. Select the checkbox to enable ERSPAN.
Description	A short description for the ERSPAN session.
Local IP	Source IP address from where the mirrored traffic is sent.
Remote IP	IP address of the destination where the mirrored traffic is sent to.
Key	Password key to different between ERSPAN sessions. Supports integeter values in the range 1 to 1023.
Source Type	The type of interface whose traffic you want to monitor. Supported options are: • WAN • LAN • VLAN
Interface	WAN ID or the port number that you want to monitor. Applicable only when you select either **WAN** or **LAN** in the **Source Type** parameter.
VLAN ID	ID of the VLAN that you want to monitor. Applicable only when you select **VLAN** in the **Source Type** parameter.
Traffic capture direction	Traffic direction which you want to monitor the data. Supported options are: • Ingress • Egress • Both
Version	ERSPAN version that NSE supports. • Version 1 • Version 2

Figure 441 *The Edit Port window*

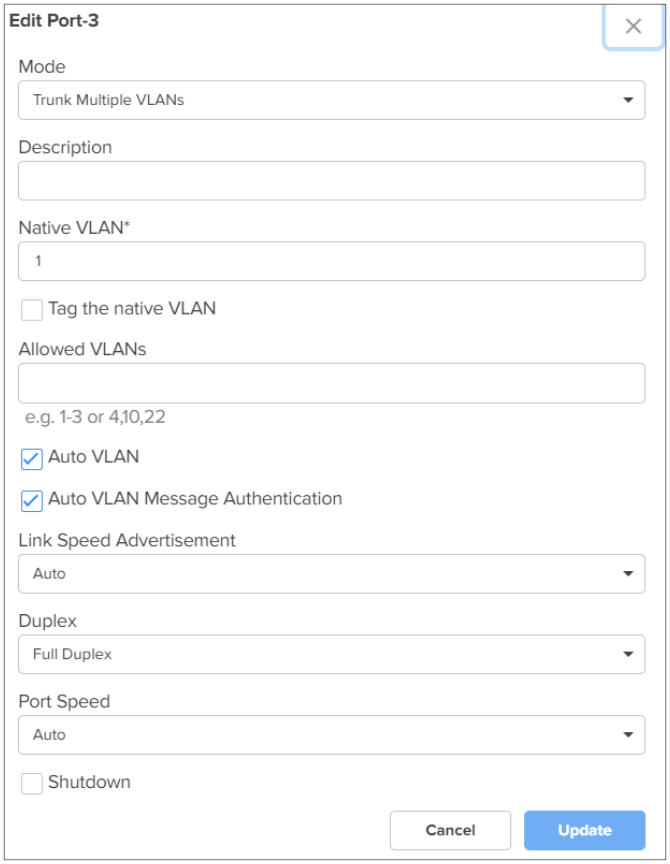


Figure 442 *The Add New VLAN window*

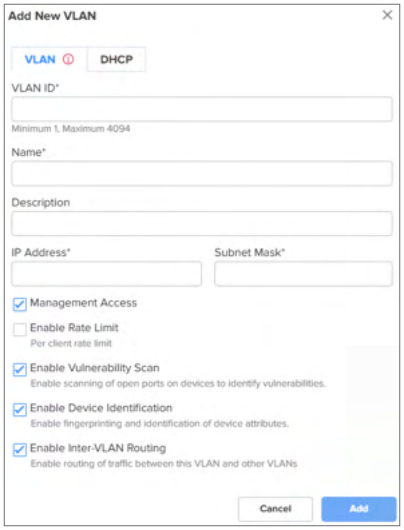


Figure 443 *DHCP Options and MAC Binding List*

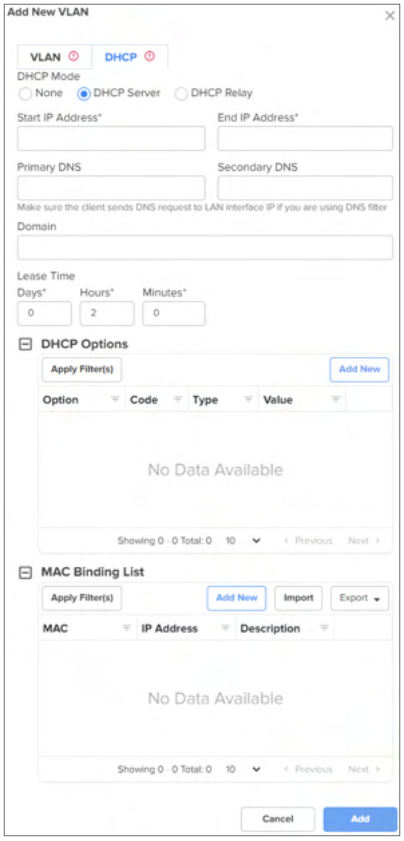


Figure 444 *The Add New DHCP Option window*

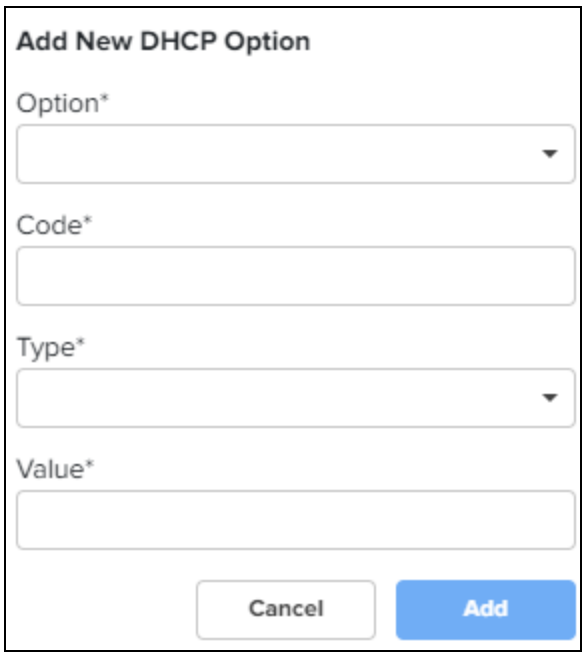


Figure 445 *The Add New MAC Binding window*

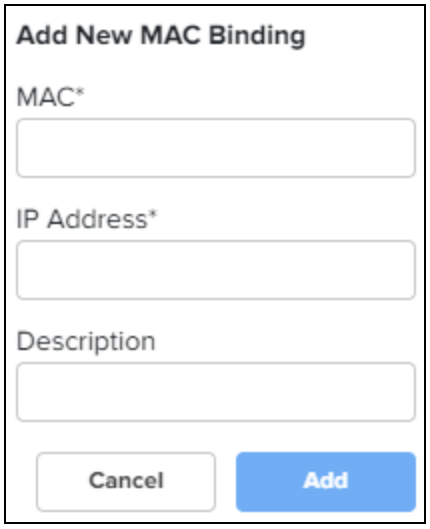


Figure 446 *The Import option in MAC Binding List*

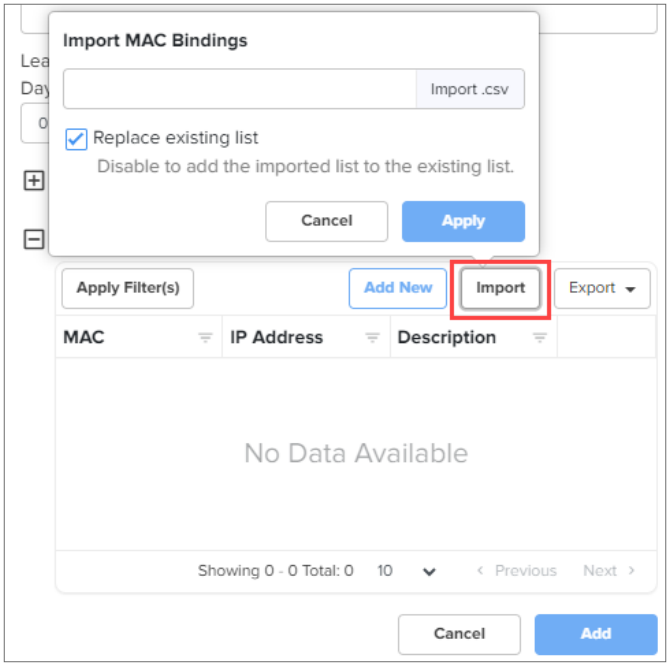


Figure 447 *The Export option in MAC Binding List*

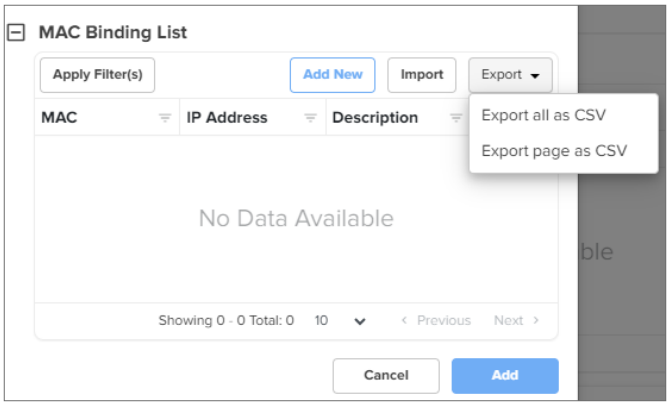


Figure 448 *The Add New Route window*

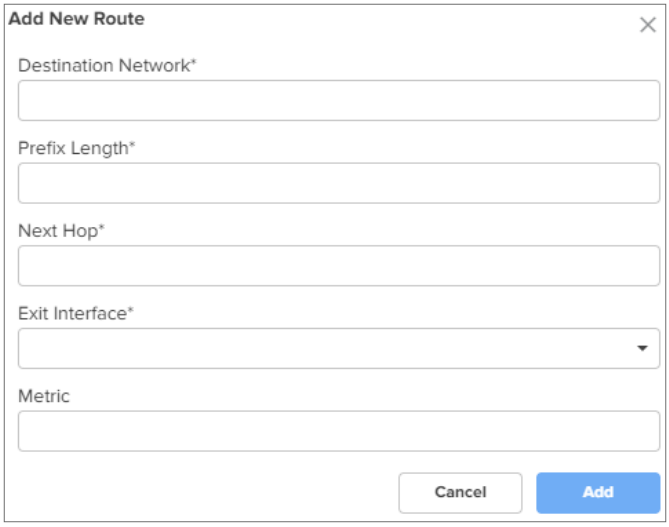


Figure 449 *The Add Multiple VLANs window*

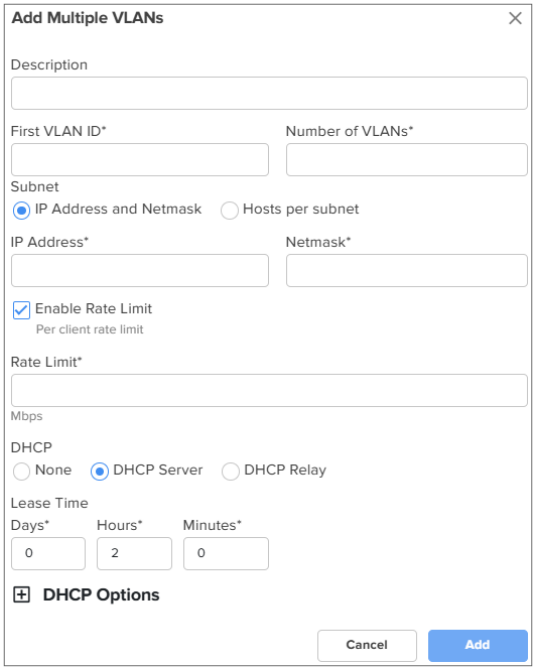


Figure 450 *ERSPAN Session parameters*



3. Click **Save**.

Groups

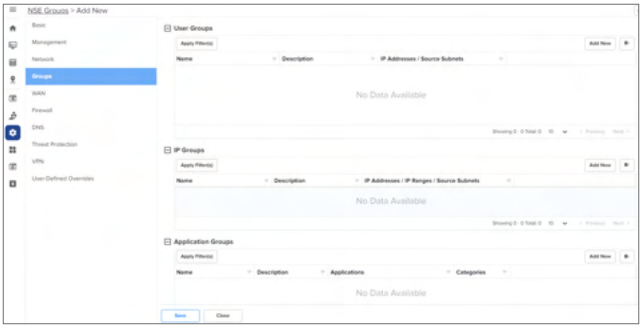
Using the **Groups** tab, you can configure user groups, IP groups, and application groups.

To view the **Groups** page, complete the following steps:

1. On the **NSE Groups > Add New** page, select the **Groups** tab.

   The **Groups** page appears, as shown in Figure 451.

   Figure 451 *The Groups page*

2. Configure the parameters, as described in Table 94.

   Table 94 *Parameters on the Groups page*

Parameter	Description
On the Groups page, there are **User Groups**, **IP Groups**, and **ApplicationGroups** sections.	
User Groups User groups are used to group locally configured networks and these groups can be used to associate with policies, especially application rules or DNS rules.	

Parameter	Description
To add a new user group, click **Add New**. The **Add User Group** window appears, as shown in Figure 452. To edit a user group, click the edit icon and modify the parameters in the **Edit User Group** window. Finally, click **Update** to apply the changes.	
Name	Name for the user group. This is a mandatory parameter.
Description	Description for the user group.
IP Addresses/Source Subnets	IPv4 addresses or source subnets for the user group. This is a mandatory parameter.
IP Groups IP groups are used to group networks originating from the WAN, and can be used to attach port forwarding rules. To add a new IP group, click **Add New**. The **Add IP Group** window appears, as shown in Figure 453. To edit an IP group, click the edit icon and modify the parameters in the **Edit IP Group** window. Finally, click **Update** to apply the changes.	
Name	Name for the IP group.
Description	Description for the IP group.
IP Addresses/IP Ranges/Source Subnets	IPv4 addresses, IP ranges, or source subnets for the IP group. This is a mandatory parameter.
Application Groups Application groups are used to group applications by using application names or categories, which can then be attached to a policy for permitting or denying access. To add a new application group, click **Add New**. The **Add New Application Group** window appears, as shown in Figure 454. To edit an application group, click the edit icon and modify the parameters in the **Edit Application Group** window. Finally, click **Update** to apply the changes.	
Name	Name for the application group.
Description	Description for the application group.
Applications To add applications to the application group, select the required application(s) from the dropdown list and click **Add New**. The selected applications are added in the **Name** list.	
Application Name	Applications for the new application group.
Categories To include categories for the new application group, select the required categories.	
Categories	Categories for the new application group.

Figure 452 *The Add User Group window*

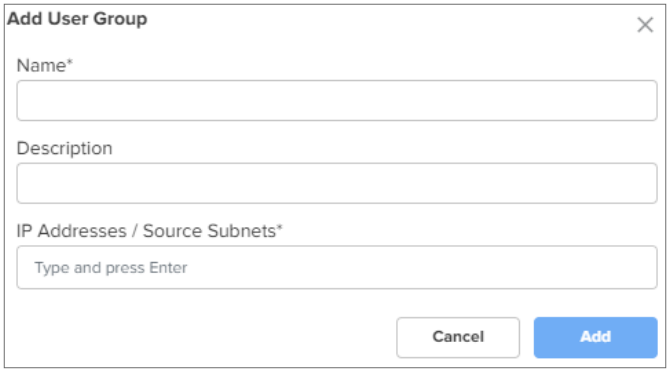


Figure 453 *The Add IP Group window*

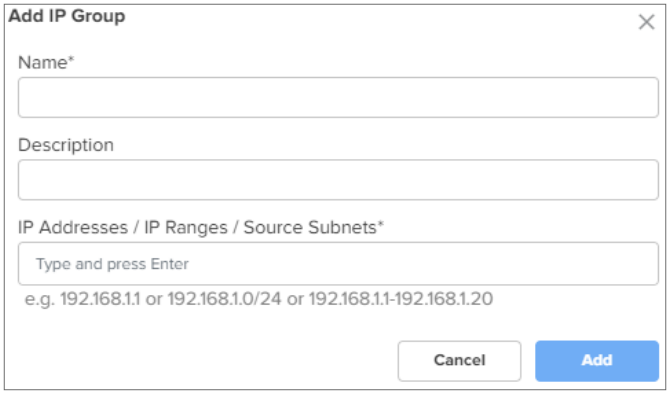
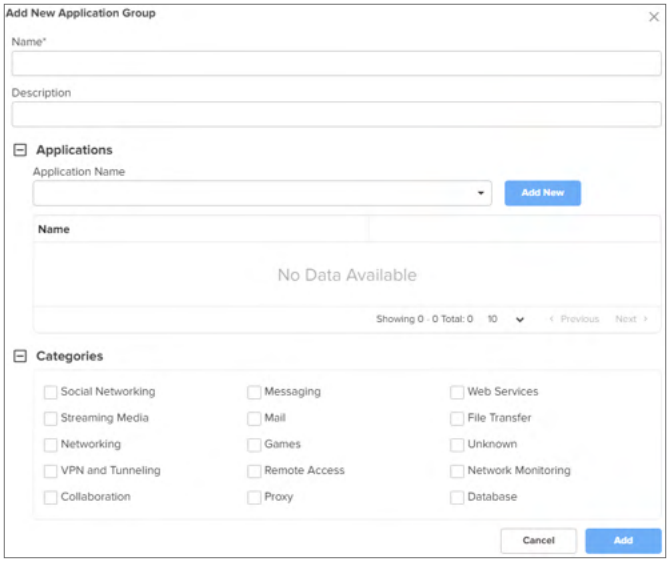


Figure 454 *The Add New Application Group window*



3. Click **Save**.

WAN

Using the **WAN** tab, you can configure the settings related to the WAN interface.

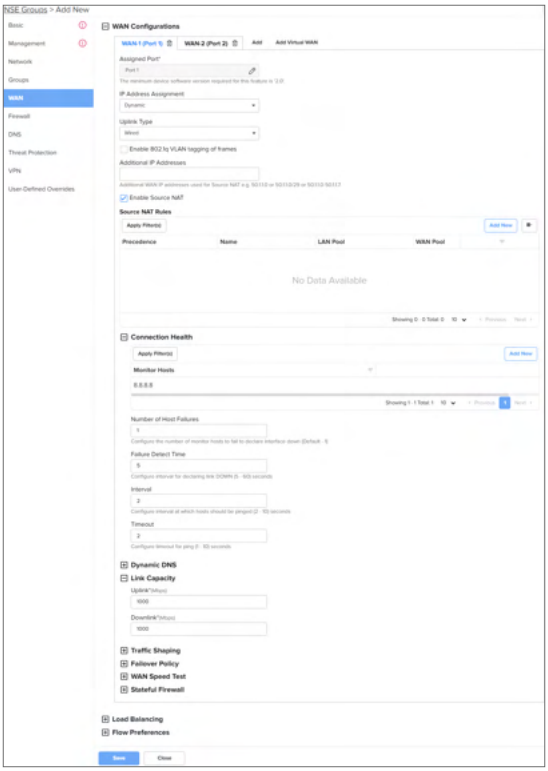
You can add up to four WANs for NSE3000 and five WANs for NSE4000 devices by converting LAN ports as WAN ports.

To configure parameters on the WAN page, complete the following steps:

1. On the **NSE Groups > Add New** page, select the **WAN** tab.

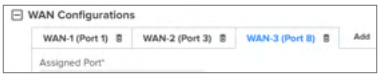
   The **WAN** page appears.

   Figure 455 *The WAN page*



2. Configure the parameters, as described in Table 95.

   Table 95 *Parameters on the WAN page*

Parameter	Description
On the WAN page, there are **WAN Configurations**, **LoadBalancing**, and **Flow Preferences** sections.	
WAN Configurations In this section, you can configure the parameters in **Connection Health**, **Dynamic DNS**, **Link Capacity**, **Traffic Shaping**, **Failover Policy**, **WAN Speed Test**, and **Stateful Firewall** subsections. The same parameters appear in all the WAN tabs. You can add up to four WANs for NSE3000 and five WANs for NSE4000 devices by converting LAN ports as WAN ports. To add additional WAN port configurations, click **Add** on the WAN tabs and select the port (LAN or WAN) (Figure 456 and Figure 457) you want to configure as WAN and click **Add**. Additional tabs are displayed as shown below:  **Note**: You must also configure the load balancing for the new WANs that are added.	

Parameter	Description
IP Address Assignment	Determines the mode of IP address assignment for the WAN interface. The following options are supported: • **Dynamic**: Dynamically learn the IP address and DNS from the DHCP server. • **Static**: Manually configure the IP address, gateway, and DNS server IP provided by the service provider. • **PPPoE**: When you configure PPPoE, you must provide the username and password of the service provider. While the account name and service name are not mandatory configurations, they may be required if the service provider enforces it. By default, the MTU is set to 1492 and the TCP MSS clamping is enabled. If required, you can also tag the packet on the WAN link to send.
Following parameters appear when you select **Static** from the **IP Address Assignment** dropdown list.	
IP Address	The IPv4 address of the WAN interface. This is a mandatory parameter.
IP Address (HA Spare)	This parameter appears only when **Enable HA** checkbox is selected from the **Basic** screen. The IPv4 address of the HA spare. This is a mandatory parameter.
Subnet Mask	The subnet mask for the IPv4 address of the WAN interface. This is a mandatory parameter.
Default Gateway	The IPv4 address of the default gateway for the WAN interface.
Primary DNS	The IPv4 address of primary upstream DNS server on this interface. This is a mandatory parameter.
Secondary DNS	The IPv4 address of secondary upstream DNS server on this interface.
Following parameters appear when you select **PPPoE** from the **IP Address Assignment** dropdown list.	
Account Controller Name	Name of the account controller. This parameter allows a maximum of 32 characters. This parameter is optional.
Service Name	Indicates the service name of the Account Controller. This parameter allows a maximum of 32 characters. The service name configuration is optional.
User	User name for PPPoE authentication. This is a mandatory parameter.
Password	Password for PPPoE authentication. This parameter is optional.
MTU	MTU for PPPoE interface. MTU ranges from 500 to 1492 bytes. Default: 1492 bytes.

Parameter	Description
TCP MSS Clamping	Indicates whether TCP MSS Clamping is enabled or disabled. By default, this parameter is enabled.
Uplink Type	Determines the uplink type that you want to configure. Following options are supported: • Wired • Starlink • Cellular Beta Additional parameters are displayed for Starlink and Cellular Beta uplink types. Refer to the below rows for more information.
Starlink-related parameters	Enables Starlink dish detection by the NSE device to collect and display performance and alignment data. Following are the additional parameters to be configured when this parameter is enabled: • **Starlink Dish IP**—IP address of the Starlink dish. Default—192.168.100.1 • **Starlink Dish Port**—Port number of the Starlink dish. Default—9200 • **Starlink Dish Operating Mode**—Mode in which the Starlink dish is configured to operate. ◦ **Bridge**—This option is selected by default. ◦ **Router**—The following additional parameters must be configured: ▪ **Starlink Gateway IP**—Gateway IP address of the Starlink dish. Default—192.168.100.1 ▪ **Starlink Gateway API Port**—Gateway port number of the Starlink dish. Default—9000
Cellular Beta - related parameters	**Note**: Cellular WAN is a Beta feature. Cellular WAN is supported only on NSE devices running version 2.2 and higher. Enables Cellular WAN detection by NSE device to collect and display statistics. Following are the additional parameters to be configured when this parameter is enabled: • **Cellular WAN Username**—Username of the cellular WAN interface • **Cellular WAN Password**—Password of the cellular WAN interface
Enable 802.1q VLAN tagging of frames	When this parameter is enabled, 802.1Q tag is inserted with configured VLAN ID for all the packets going out of the WAN interface. By default, this parameter is disabled.
VLAN ID	This parameter is applicable only when **Enable 802.1q VLAN tagging of frames** checkbox is selected. VLAN ID range: 1 and 4094. This is a mandatory parameter. When the 802.1Q header is configured, all transmitted frames are expected to include the 802.1Q header with the same VLAN ID.

Parameter	Description
Additional IP Addresses	WAN IP addresses that are available for source NAT. **Note**:The WAN interface supports up to 16 IP addresses.
Enable Source NAT	Indicates whether the source NAT is enabled or disabled. When enabled, NSE device will replace the source IP address of the traffic routed from LAN to WAN with the WAN interface IP address. By default, this parameter is enabled.
Source NAT Rules Allows user to configure source NAT rules. User can choose the WAN IP addresses from the Additional IP Address for source NAT. User can configure WAN IP address(es) of their choice for source NAT. By default, all the LAN users' traffic will be source NATed to the configured WAN IP address(es). When LAN pool is configured, the traffic from the specified LAN networks will be source NATed to the configured WAN IP address(es). **Note**: Source NAT Rules supports up to 16 rules per WAN. To add a new source NAT, click **Add New**. The **Add New Source NAT Rule** window appears, as shown in Figure 458.	
Name	Name of the Source NAT rule.
Precedence	The precedence value for the source NAT rule. The precedence value can be between 1 and 150. This is a mandatory parameter. For information about configuring precedence, refer to Configuring rule precedence.
LAN Pool	The following options are supported: • **All** • **IP Group** • **IP Address / Source Subnet**
IP Group	Select the IP group for the source NAT. IP groups are the ones that you configure in the **Groups** > **IP Groups** section. This parameter is applicable only when **IP Group** option is selected. This is a mandatory parameter.
IP Address / Source Subnet	This parameter is applicable only when **IP Address / Source Subnet** option is selected. This is a mandatory parameter.
WAN Pool	The following options are supported: • **Single IP Address** • **Multiple IP Addresses**
IP Address	IPv4 address for the WAN pool. Applicable only when **Single IP Address** option is selected.
Start IP	Starting IP address in the range. This parameter is applicable only when **Multiple IP Addresses** option is selected.

Parameter	Description
	This is a mandatory parameter.
End IP	Ending IP address in the range. This parameter is applicable only when **Multiple IP Addresses** option is selected. This is a mandatory parameter.
Connection Health This section is configured to monitor the WAN connection health. Click the edit icon to modify the **Monitor Host** configuration, as shown in Figure 459. Finally, click **Update** to apply the changes. To add a new monitor host, click **Add New**. The **Add New Monitor Host** window appears, as shown in Figure 460.	
Monitor Host	The hosts used to monitor and collect network traffic data. Default: 8.8.8.8 This is a mandatory parameter.
Number of Host Failures	The number of monitor hosts that fail to declare the link down. Default value: 1 The maximum number of monitor hosts that can be configured to fail is 5.
Failure Detect Time	The time period (in seconds) during which the device waits for the response from the monitored host before declaring the link down. Default: 5. Range: 5 to 60
Interval	The time interval (in seconds) used by the device to check and reach the monitor hosts. Default: 2. Range: 2 to 10
Timeout	The time period (in seconds) the device waits for a response from the monitor host after which the connection is timed out. Default: 2. Range: 1 to 10
Dynamic DNS	
Enable Dynamic DNS	Indicates whether the dynamic DNS for the interface is enabled or disabled. By default, this parameter is disabled.
Following parameters appear when **Enable Dynamic DNS** checkbox is selected**.**	
DNS Provider	The following options are supported: • **Cloudflare:** Requires secret/access token and zone configuration. In the Cloudflare account, navigate to **Profile** > **API Tokens** to create a token. Following is the recommended setting: ◦ Permissions: Zone, DNS, Edit ◦ ZoneResource: Include, Specific Zone, <zone name> • **Godaddy:** Requires API key, secret/access token, and zone configuration. In the Godaddy account, create an API key at https://developer.godaddy.com/keys

Parameter	Description
	• **Hetzner:** Requires secret/access token and zone configuration. In the Hetzner account, navigate to **Profile** > **API Tokens** and create an access token. • **Namecheap:** Requires password and zone configuration**.** 1. In the Namecheap account, navigate to **Domains** > **Free DNS** to manage external domains. 2. Before you update/create a record, a new record of type **A** must exist. To create a record, navigate to the dashboard, and then navigate to **Products** > **Advanced DNS**. Add a new record of type **A**. On the same page, enable Dynamic DNS and note the password. • **Noip:** Requires server name, username, and password configuration**.** • **Route53:** Requires API key, secret/access token, and zone configuration**.** 1. In the Route 53 account, navigate to **route53** > **Hosted Zones** > **Create Hosted Zone** to create a zone. Use type Public hosted zone. Note the name servers in hosted zone details and the hosted zone ID. 2. Navigate to **IAM** > **Users** > **Create user**. Select attach policies directly. Create a policy. The following is an example of a policy: { "Version": "2012-10-17", "Statement": [{ "Sid": "", "Effect": "Allow", "Action": ["route53:ListResourceRecordSets", "route53:GetChange", "route53:ChangeResourceRecordSets"], "Resource": ["arn:aws:route53:::hostedzone/<ZONE_ID>", "arn:aws:route53:::change/*"] }, { "Sid": "",

Parameter	Description

	<pre>"Effect": "Allow",
	"Action": [
	"route53:ListHostedZonesByName",
	"route53:ListHostedZones"
	],
	"Resource": "*"
	}
	]
	}</pre>
	3. Replace ZONE_ID in the policy with the previously noted zone id. Select the new policy for the previously created user.
	4. To create access key, navigate to users, select the user, **Security Credentials** > **Create Access Key**.
	• **Porkbun:** Requires API key, secret/access token, and zone configuration**.**
	In the Porkbun account, navigate to **Account** > **API Access** to create a token. Additionally, the domain configuration much be changed to enable API access.
	• **Dyn:** Oracle Dyn requires server name, username, and password configuration**.**
	• **DynDNS2 compliant:** Requires server name, username, and password configuration**.**
	By default, **Noip** option is selected.

DNS Hostname	Indicates the DNS host name.
Link Capacity	
Uplink	The WAN uplink capacity in Mbps. Default: 1000. Range: 1 to 1000 This is a mandatory parameter.
Downlink	The WAN downlink capacity in Mbps. Default: 1000. Range: 1 to 1000 This is a mandatory parameter.
Traffic Shaping **Note**: Traffic Shaping supports up to 16 rules per WAN. To add a new traffic shaping rule, click **Add New**, the **Add New Traffic Shaping Rule** window appears, as shown in Figure 461.	
Enable Traffic Shaping	Indicates whether traffic shaping is enabled or disabled. By default, this parameter is disabled.
Name	Name of the traffic shaping rule.
Precedence	The precedence value for the traffic shaping rule.

Parameter	Description
	The precedence value can be between 1 and 150. This is a mandatory parameter. For information about configuring precedence, refer to Configuring rule precedence.
Description	Displays a user-configured description for the traffic shaping rule.
Uplink Bandwidth	Indicates the uplink bandwidth in Mbps. Range: 1 to 1000 This is a mandatory parameter.
Downlink Bandwidth	Indicates the downlink bandwidth in Mbps Range: 1 to 1000 This is a mandatory parameter.
DSCP	Differentiated Services Code Point (DSCP) can range from 0 to 63, with 0 being the lowest priority and 63 being the highest priority.
Type	Indicates the type of filter rule. The following options are supported: • **IP Based** – Allows you to configure **Protocol** parameter as **TCP**, **UDP**, or **any**. • **Application Based** – Allows you to configure **Deep Packet Inspection (DPI) Type** parameter as **Application** or **Category**.
Deep Packet Inspection (DPI) Type	This parameter is applicable only when **Type** parameter is **Application Based**. The following options are supported: • **Application** – Specific type of application within a category. • **Category** – All applications belonging to a category (For example, Social Messaging). This is a mandatory parameter.
DPI Application	This parameter is applicable only when **Deep Packet Inspection (DPI) Type** parameter is set to **Application**. This is a mandatory parameter.
DPI Category	This parameter is applicable only when **Deep Packet Inspection (DPI) Type** parameter is set to **Category**. This is a mandatory parameter.
Protocol	This parameter is applicable only when **Type** parameter is **IP Based**. The following options are supported: • **TCP** – Match TCP traffic. • **UDP** – Match UDP traffic. • **any** – Match any of the above protocol traffic.
Source IP Address	The source IPv4 address for the shaping rule. This is a mandatory parameter.
Mask	The subnet mask for the shaping rule.

Parameter	Description
	This is a mandatory parameter.
Port	Displays the source port from which IPv4 address messaging is sent. This is a mandatory parameter.
Destination IP Address	The destination IPv4 address for the shaping rule. This is a mandatory parameter.
Mask	The subnet mask for the shaping rule. This is a mandatory parameter.
Port	Displays the destination port to which IPv4 address messaging is sent. This is a mandatory parameter.
Failover Policy **Note**: Failover Policy supports up to 32 rules per WAN. To add a new failover policy, click **Add New**. The **Add New Failover Policy** window appears, as shown in Figure 462.	
Enable Failover Policy	Indicates whether failover policy is enabled or disabled. By default, this parameter is disabled.
Name	Name of the failover policy.
Precedence	The precedence value for the failover policy. The precedence value can be between 1 and 150. This is a mandatory parameter. For information about configuring precedence, refer to Configuring rule precedence.
Description	A description for the policy.
Action	By default, this parameter is disabled.
Type	The type of failover rule. The following options are supported: • **IP Based** – Allows you to configure the **Protocol** parameter as **TCP**, **UDP**, or **any**. • **Application Based** – Allows you to configure **Deep Packet Inspection (DPI)Type** parameter as **Application**, **Category**, or **Application Group**.
Protocol	This parameter is applicable only when **Type** parameter is **IP Based**. The following options are supported: • **TCP** – Match TCP traffic. • **UDP** – Match UDP traffic. • **any** – Match any of the above protocol traffic.
Source IP Address	The source IPv4 address for the failover rule. This is a mandatory parameter.
Mask	The subnet mask for the failover rule. This is a mandatory parameter.

Parameter	Description
Port	The source port for the failover rule. This is a mandatory parameter.
Destination IP Address	The destination IPv4 address for the failover rule. This is a mandatory parameter.
Mask	The subnet mask for the failover rule. This is a mandatory parameter.
Port	Displays the destination port for the failover rule. This is a mandatory parameter.
Deep Packet Inspection (DPI) Type	This parameter is applicable only when **Type** parameter is **Application Based**. The following options are supported: • **Application** – Specific type of application within a category. • **Category** – All applications belonging to a category (For example, Social Messaging). • **Application Group -** All applications belonging to a group. This is a mandatory parameter.
Apply to	This parameter is applicable only when **Type** parameter is **Application Based**. The following options are supported: • **All** • **User Group** • **IP Address / Source Subnet**
User Group	This parameter is applicable when **User Group** option is selected. This is a mandatory parameter.
IP Address / Source Subnet	This parameter is applicable when **IP Address / Source Subnet** option is selected. This is a mandatory parameter.
WAN Speed Test	
Enable WAN Speed Test	Enable or disable the WAN speed test. By default, this parameter is disabled.
Stateful Firewall	
Allow traffic from WAN to LAN	Determines whether traffic from WAN to LAN is allowed or not. By default, this parameter is disabled. In special deployment cases, when NSE is positioned behind an MPLS uplink router, you can enable this behavior. To enable this behavior, select the **Allow traffic from WAN to LAN** checkbox. Additionally, you must disable source NAT on the WAN UI page to allow routing of traffic without NAT, originated on the LAN directed towards the WAN.

Figure 456 *Adding multiple WANs in NSE3000*



Figure 457 *Adding multiple WANs in NSE4000*



Figure 458 *The Add New Source NAT Rule window*

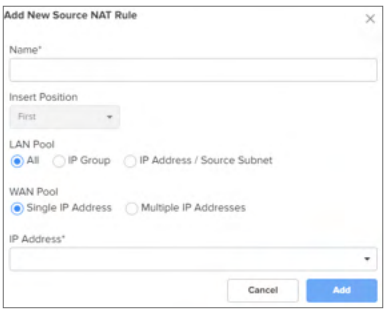


Figure 459 *The Edit Monitor Host window*

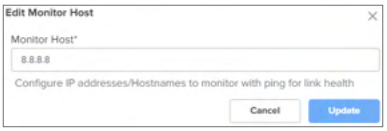


Figure 460 *The Add New Monitor Host window*



Figure 461 *The Add New Traffic Shaping Rule window*

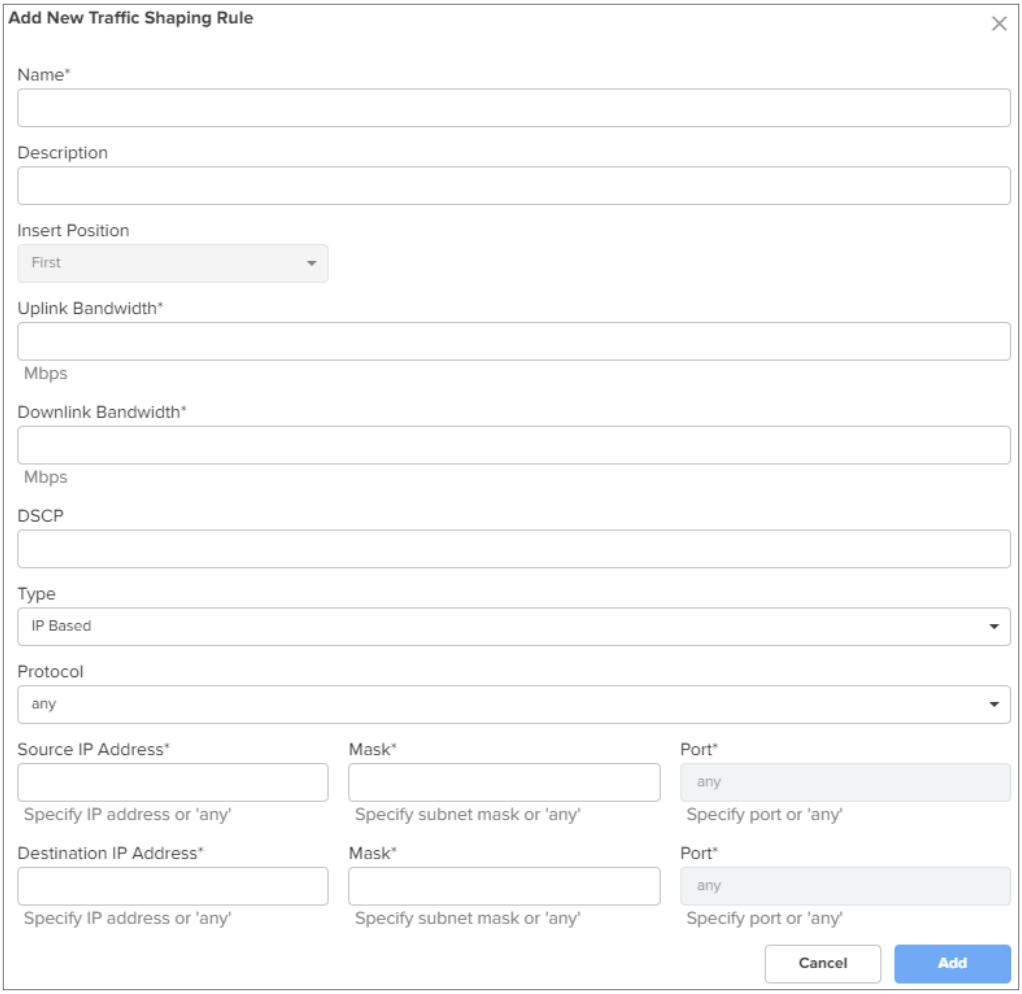
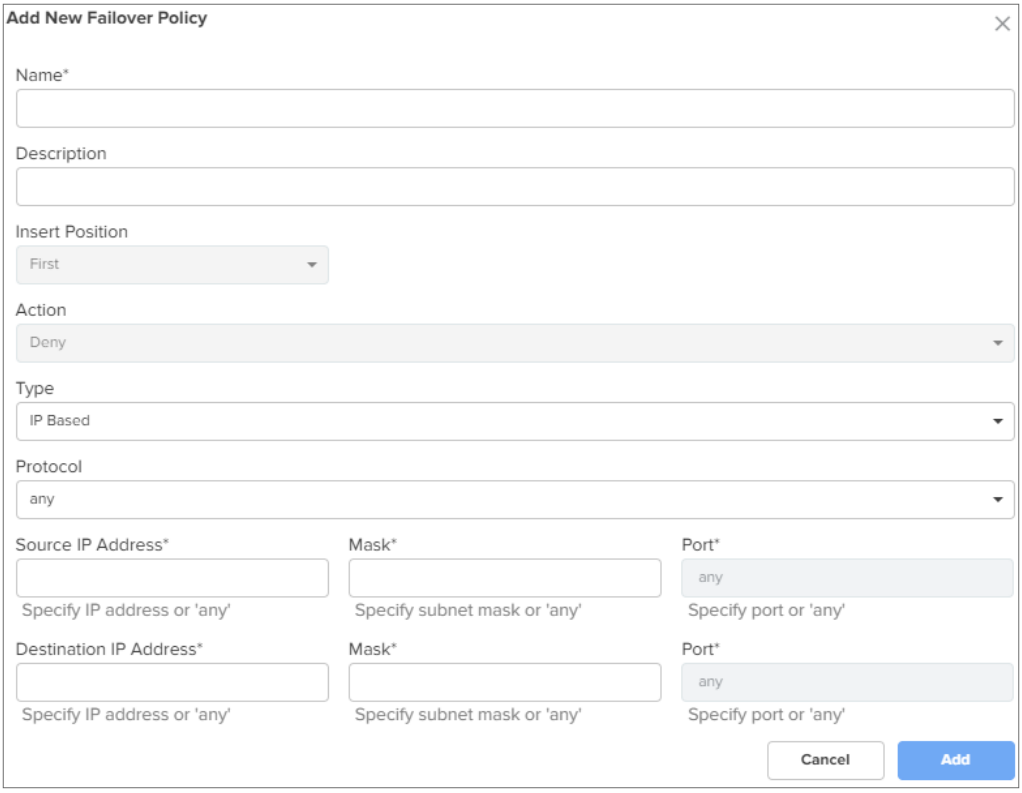


Figure 462 *The Add New Failover Policy window*



3. Expand the **Load Balancing** section and configure the parameters, as described in Table 96.

Table 96 *Parameters on the Load Balancing section*

Parameter	Description
Load Balancing	
WAN-1 Mode	Determines the load balancing mode of device. By default, the **WAN-1 Mode** parameter is set to **Shared**. The following options are supported: • **Shared** – Enables the WAN link to actively forward a percentage of user traffic. The percentage of user traffic on this link is set via the **Traffic Share Percentage** parameter. • **Backup** – The WAN link forwards user traffic only when all of the Shared WAN interfaces are down. • **Disabled** – Disables the WAN link from participating in WAN link load sharing, and failover procedures.
Traffic Share Percentage	For the **Shared** mode, the traffic share percentage must be between 5 and 100. This is a mandatory parameter.
WAN-2 Mode	Determines the load balancing adjust mode of device. By default, the **WAN-2 Mode** parameter is set to **Backup**. The following options are supported: • **Shared** – Enables the WAN link to actively forward a percentage of user traffic. The

Parameter	Description
	percentage of user traffic on this link is set via the **Traffic Share Percentage** parameter. • **Backup** – The WAN link forwards user traffic only when all of the Shared WAN interfaces are down. • **Disabled** – Disables the WAN link from participating in WAN link load sharing, and failover procedures.
Traffic Share Percentage	For the **Shared** mode, the traffic share percentage between 5 and 100. This is a mandatory parameter.
WAN-<3 to 5> Mode	Determines the load balancing mode of device on additional WANs added. The following options are supported: • **Shared** – Enables the WAN link to actively forward a percentage of user traffic. The percentage of user traffic on this link is set via the **Traffic Share Percentage** parameter. • **Backup** – The WAN link forwards user traffic only when all of the Shared WAN interfaces are down. • **Disabled** – Disables the WAN link from participating in WAN link load sharing, and failover procedures.
Traffic Share Percentage	For the **Shared** mode, the traffic share percentage must be between 5 and 100. This is a mandatory parameter.

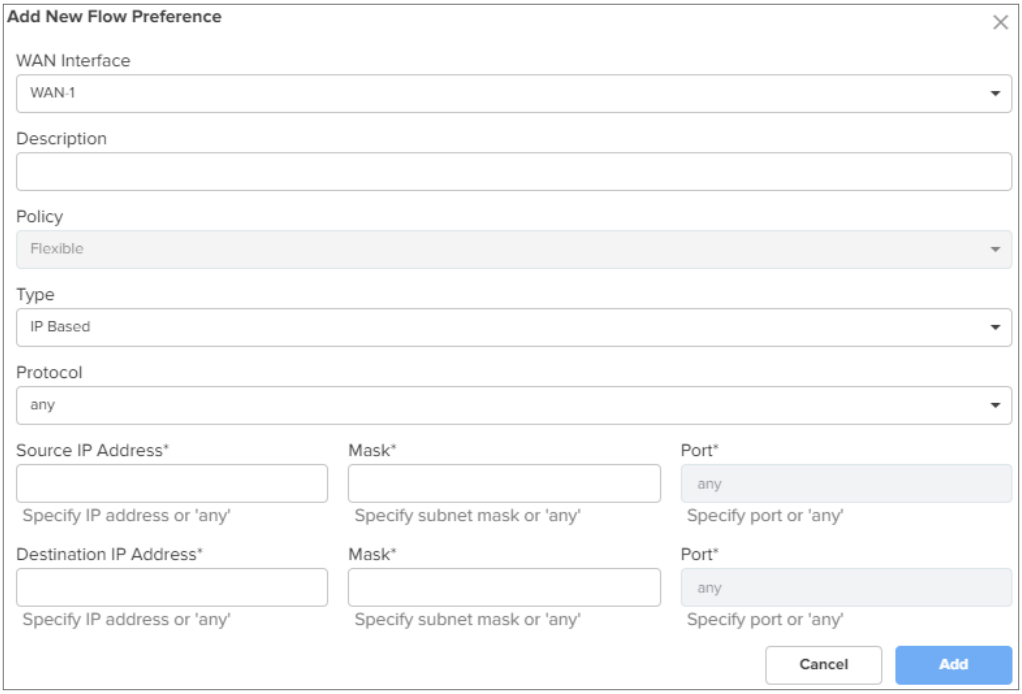
4. Expand the **Flow Preferences** section and configure the parameters, as described in Table 97.

Table 97 *Parameters on the Flow Preferences section*

Parameter	Description
Flow Preferences Flow preferences support up to 30 rules for both WANs combined. To add a new flow preference, click **Add New**. The **Add New Flow Preference** window appears, as shown in Figure 463.	
WAN Interface	The following options are supported: • **WAN-1** • **WAN-2**
Description	Provide a description for the flow preference.
Policy	The flow preference policy. The following options are supported: • **Flexible** – Allow traffic to failover if the preferred WAN link goes down. • **Strict** – Traffic is dropped in strict mode, if the preferred WAN link goes down.
Type	The flow preference type. The following options are supported: • **IP Based** – Allows you to configure **Protocol** parameter as **TCP**, **UDP**, or **any**. • **Application Based** – Allows you to configure **Deep Packet Inspection (DPI)**

Parameter	Description
	Type parameter as **Application** or **Category**.
Protocol	This parameter is applicable only when **Type** parameter is **IP Based**. The following options are supported: • **TCP** – Match TCP preference. • **UDP** – Match UDP preference. • **Any** – Match any of the above preferences.
Source IP Address	The source IPv4 address for the flow preference. This is a mandatory parameter.
Mask	The subnet mask for the flow preference. This is a mandatory parameter.
Port	The source port for the flow preference. This is a mandatory parameter.
Destination IP Address	The destination IPv4 address for the flow preference. This is a mandatory parameter.
Mask	The subnet mask for the flow preference. This is a mandatory parameter.
Port	The destination port for the flow preference. This is a mandatory parameter.
Deep Packet Inspection (DPI) Type	This parameter is applicable only when **Type** parameter is **Application Based**. The following options are supported: • **Application** – Specific type of application within a category. • **Category** – All applications belonging to a category (For example, Social Messaging). This is a mandatory parameter.
DPI Application	This parameter is applicable only when **Deep Packet Inspection (DPI) Type** parameter is set to **Application**. This is a mandatory parameter.
DPI Category	This parameter is applicable only when **Deep Packet Inspection (DPI) Type** parameter is set to **Category**. This is a mandatory parameter.

Figure 463 *The Add New Flow Preference window*



5. Click **Save**.

Adding a virtual WAN interface

Note

- Virtual WAN interface is applicable only to NSE devices running version 2.1 and higher.
- Virtual WAN interface is a NSE Security Plus feature.
- Virtual WAN that you add on this page will be available at the following locations:
  - **NSE Groups** > <NSE-Group-Name> > **Firewall** >:
    - **Port Forward Rules**
    - **NAT One-to-One**
    - **NAT One-to-Many**
  - **NSE Groups** > <NSE-Group-Name> > **VPN** >:
    - **VPN Server Interface**
    - **Users** (Only when WireGuard is enabled)

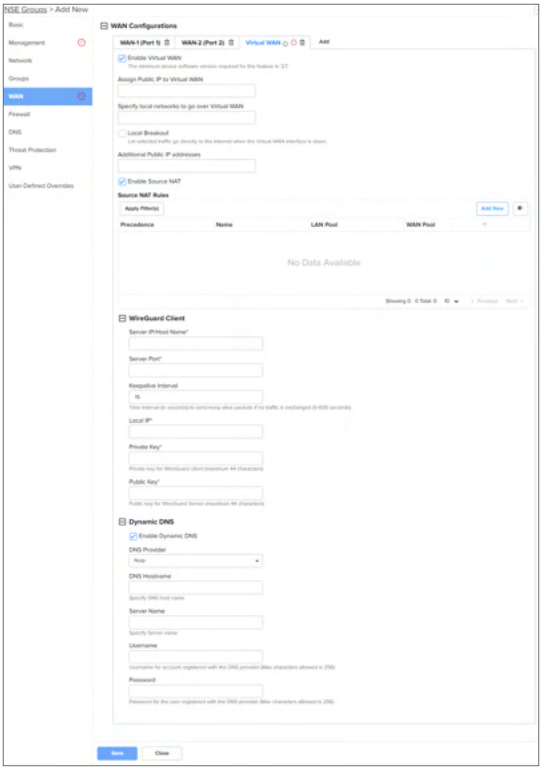
When a virtual WAN interface is enabled on a NSE group, the associated site receives a routable public IP address over a secure WireGuard tunnel—even if the WAN uses CGNAT (for example, Starlink or LTE). This WAN establishes an encrypted, performant L3 tunnel to extend networks across sites, branches, or cloud edges.

To add a virtual WAN interface, complete the following steps:

1. In the WAN configuration section, click **Add Virtual WAN**.

   The Virtual WAN window appears.

Figure 464 *NSE-Groups > Add New > WAN > Virtual WAN tab*



Parameter	Description
On the Virtual WAN page, the following sections are present: • Common parameters • **Source NAT Rules** • **WireGuard Client** • **Dynamic DNS**	
Enable Virtual WAN	Select this checkbox to enable Virtual WAN interface on the NSE device.
Assign Public IP to Virtual WAN	The public IPv4 address assigned for the Virtual WAN to be used for tunnel traffic.
Specify local networks to go over Virtual WAN	List of subnets that must be routed through the Virtual WAN tunnel.
Local Breakout	Specifies whether the traffic can directly access internet when the Virtual WAN is down.
Additional IP Addresses	WAN IP addresses that are available for source NAT. **Note**:The WAN interface supports up to 16 IP addresses.
Enable Source NAT	Indicates whether the source NAT is enabled or disabled. When enabled, the NSE device will replace the source IP address of the traffic routed from LAN to WAN with the WAN interface IP address. By default, this parameter is enabled.

Parameter	Description
Source NAT Rules Allows user to configure source NAT rules. User can choose the WAN IP addresses from the Additional IP Address for source NAT. User can configure WAN IP address(es) of their choice for source NAT. By default, all the LAN users' traffic will be source NATed to the configured WAN IP address(es). When LAN pool is configured, the traffic from the specified LAN networks will be source NATed to the configured WAN IP address(es). **Note**: Source NAT Rules supports up to 16 rules per WAN. To add a new source NAT, click **Add New**. The **Add New Source NAT Rule** window appears. When adding more than one rule, you can configure the precedence for the rules. For information, refer to Configuring rule precedence.	
Name	Name of the Source NAT rule.
LAN Pool	The following options are supported: • **All** • **IP Group** • **IP Address / Source Subnet**
IP Group	Select the IP group for the source NAT. IP groups are the ones that you configure in the **Groups** > **IP Groups** section. This parameter is applicable only when **IP Group** option is selected. This is a mandatory parameter.
IP Address / Source Subnet	This parameter is applicable only when **IP Address / Source Subnet** option is selected. This is a mandatory parameter.
WAN Pool	The following options are supported: • **Single IP Address** • **Multiple IP Addresses**
IP Address	IPv4 address for the WAN pool. Applicable only when **Single IP Address** option is selected.
Start IP	Starting IP address in the range. This parameter is applicable only when **Multiple IP Addresses** option is selected. This is a mandatory parameter.
End IP	Ending IP address in the range. This parameter is applicable only when **Multiple IP Addresses** option is selected. This is a mandatory parameter.
WireGuard Client This section is used to configure the WireGuard client for the WAN interface.	
Server IP/Host Name	IP address of the WireGuard server to which the Virtual WAN tunnel will connect.
Server Port	Port number on the WireGuard server that accepts client tunnel connections.
Keepalive	Frequency (in seconds) at which keepalive packets are sent to maintain NAT bindings.

Parameter	Description
Interval	Default: 15 seconds Range: 5-600 seconds
Local IP	Tunnel interface IP assigned to the WireGuard client on the device.
Private Key	WireGuard client's private key used for establishing a secure encrypted session with the WireGuard server.
Public Key	WireGuard server's public key associated with the private key.
Dynamic DNS	
Enable Dynamic DNS	Indicates whether the dynamic DNS for the interface is enabled or disabled. By default, this parameter is disabled.
Following parameters appear when **Enable Dynamic DNS** checkbox is selected**.**	

DNS Provider	The following options are supported:
	• **Cloudflare:** Requires secret/access token and zone configuration.
	In the Cloudflare account, navigate to **Profile** > **API Tokens** to create a token.
	Following is the recommended setting:
	◦ Permissions: Zone, DNS, Edit
	◦ ZoneResource: Include, Specific Zone, <zone name>
	• **Godaddy:** Requires API key, secret/access token, and zone configuration.
	In the Godaddy account, create an API key at https://developer.godaddy.com/keys
	• **Hetzner:** Requires secret/access token and zone configuration.
	In the Hetzner account, navigate to **Profile** > **API Tokens** and create an access token.
	• **Namecheap:** Requires password and zone configuration**.**
	1. In the Namecheap account, navigate to **Domains** > **Free DNS** to manage external domains.
	2. Before you update/create a record, a new record of type **A** must exist. To create a record, navigate to the dashboard, and then navigate to **Products** > **Advanced DNS**. Add a new record of type **A**. On the same page, enable Dynamic DNS and note the password.
	• **Noip:** Requires server name, username, and password configuration**.**
	• **Route53:** Requires API key, secret/access token, and zone configuration**.**
	1. In the Route 53 account, navigate to **route53** > **Hosted Zones** > **Create Hosted Zone** to create a zone. Use type Public hosted zone. Note the name servers in hosted zone details and the hosted zone ID.
	2. Navigate to **IAM** > **Users** > **Create user**. Select attach policies directly. Create a policy.
	The following is an example of a policy:
	`{`
	`"Version": "2012-10-17",`

Parameter	Description

	<pre>"Statement": [
	{
	"Sid": "",
	"Effect": "Allow",
	"Action": [
	"route53:ListResourceRecordSets",
	"route53:GetChange",
	"route53:ChangeResourceRecordSets"
	],
	"Resource": [
	"arn:aws:route53:::hostedzone/<ZONE_ID>",
	"arn:aws:route53:::change/*"
	]
	},
	{
	"Sid": "",
	"Effect": "Allow",
	"Action": [
	"route53:ListHostedZonesByName",
	"route53:ListHostedZones"
	],
	"Resource": "*"
	}
	]
	}</pre>
	3. Replace ZONE_ID in the policy with the previously noted zone id. Select the new policy for the previously created user.
	4. To create access key, navigate to users, select the user, **Security Credentials** > **Create Access Key**.
	• **Porkbun:** Requires API key, secret/access token, and zone configuration**.**
	In the Porkbun account, navigate to **Account** > **API Access** to create a token. Additionally, the domain configuration much be changed to enable API access.
	• **Dyn:** Oracle Dyn requires server name, username, and password configuration**.**

Parameter	Description
	• **DynDNS2 compliant:** Requires server name, username, and password configuration. By default, **Noip** option is selected.
DNS Hostname	Indicates the DNS host name.

Configuring rule precedence

You can configure precedence for rules in the following configurations:

- **WAN** tab > **WAN Configurations** > **Source NAT Rules**
- **WAN** tab > **WAN Configurations** > **Traffic Shaping**
- **WAN** tab > **WAN Configurations** > **Failover Policy**
- **Firewall** tab > **Outbound Filter Rules**

To configure rule precedence, complete the following steps:

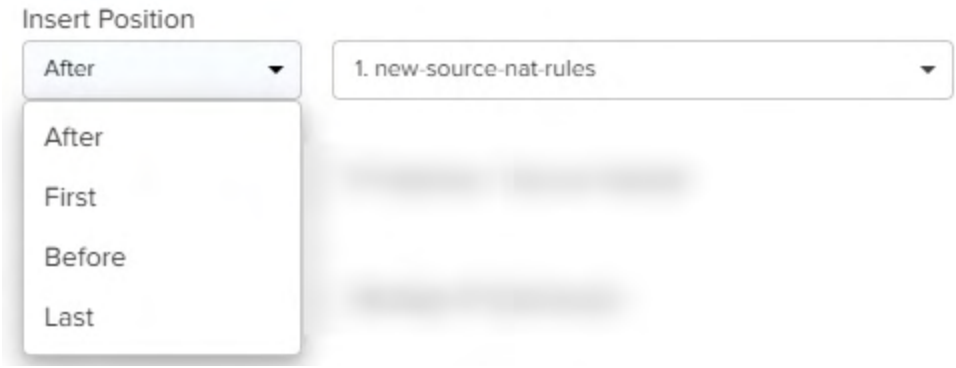
1. In the respective configuration sections, click **Add New**.

   The add new window appears.
2. Select the position of the rule from the **Insert Position** dropdown list. Supported values are **First**, **Last**, **After**, and **Before**.
   - For the first rule that is added, this field displays **First** and the dropdown is disabled.

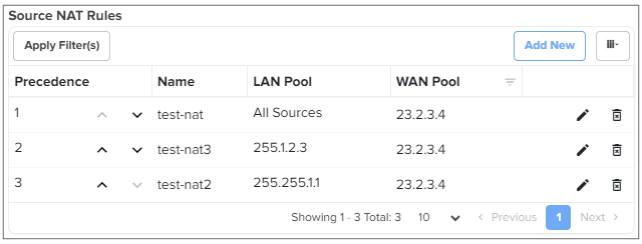
   - For subsequent rules that are added, you must select the position and also select the existing rule before or after which you want to place this rule from the adjacent rules dropdown list.

     If you select **First** or **Last** options (when more than one rule is already existing), then you are not required to select any existing rule.

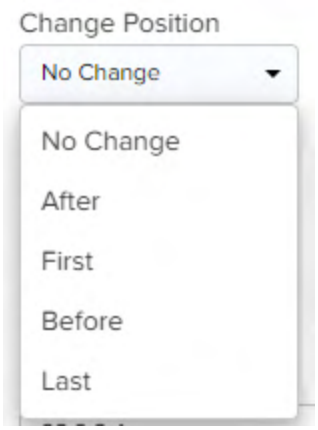
3. Click **Add**.

   The rules are listed in a table as shown in the image below (sample shown for Source NAT Rules).



4. To change the order of the rules, perform any of the following steps:
   - Click the move up (^) or move down (v) arrows corresponding to the rules you want to reorder.
   - Click the edit (✎) icon corresponding to the rule that you want to reorder.

     In the edit rule window, select the position from the **Change Position** dropdown list and the corresponding rule.



Firewall

NSE firewall allows the user to configure the IP-based and application-based outbound rules, GEO IP filters, port forward rules, one-to-one NAT mappings, and one-to-many NAT mappings. All inbound connections are denied by default. You can configure port forwarding or NAT rules to allow inbound traffic. Outbound traffic is allowed by default. Using application-based outbound rules, users can create rules to block websites without specifying IP addresses or port ranges. Application-based rules allow the user to block a specific type of application within a category or all applications belonging to a category (For example, social messaging).

Note

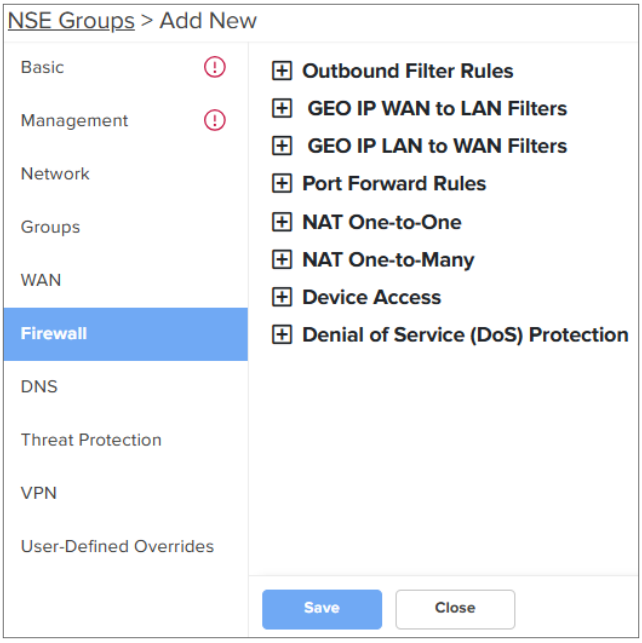
Up to 150 outbound firewall rules are supported for an NSE Group including combinations of IP-based and application-based rules.

To configure parameters on the **Firewall** page, complete the following steps:

1. On the **NSE Groups > Add New** page, select the **Firewall** tab.

   The **Firewall** page appears, as shown in Figure 465.

Figure 465 *The Firewall page*



2. Configure the parameters, as described in Table 98.

Table 98 *Parameters on the Firewall page*

Parameter	Description
On the Firewall page, there are **Outbound Filter Rules**, **GEO IP WAN to LAN Filters**, **GEO IP LAN to WAN Filters**, **Port Forward Rules**, **NAT One-to-One**, **NAT One-to-Many**, **Device Access**, **Inbound Filter Rules**, and **Denial of Service (DoS) Protection** sections.	
Outbound Filter Rules To add a new outbound filter rule, click **Add New**. The **Add New Filter Rule** window is displayed, as shown in Figure 466.	
Name	Name of the outbound filter rule.
Precedence	The precedence value for the filter rule. The precedence value can be between 1 and 150. This is a mandatory parameter. For information about configuring precedence, refer to Configuring rule precedence.
Description	Displays a user-configured description for the filter rule.
Action	Determines the action of filter. The following options are supported: • **Permit**—Allow traffic matching this filter rule. • **Deny**—Drop traffic matching this filter rule.
Type	The type of filter rule. The following options are supported:

Parameter	Description
	• **IP Based**—Configure **Protocol** parameter as **TCP**, **UDP**, **TCP & UDP, ICMP** or **any**. • **Application Based**—Configure **Deep Packet Inspection (DPI) Type** parameter as Application, Category, or Application Group
Protocol	This parameter is applicable only when **Type** parameter is **IP Based**. The following options are supported: • **TCP**—Match TCP traffic. • **UDP**—Match UDP traffic. • **TCP & UDP**—Match both TCP and UDP traffic. • **ICMP**—Match ICMP traffic. • **any**—Match any of the above protocol traffic.
Source IP Address	The source IP address for the filter rule. The following options are available: • All • User Group—This is applicable only to NSE devices that are running release version 2.3 and later. Select the user group from the **Source User Group** dropdown list. • IP Address / Subnet Mask—Configure the source IP address or subnet mask and the port number. Select the appropriate option. For **User Group** and **IP Address / Subnet Mask** options, there are additional parameters that you must configure.
Source IP Address	The source IPv4 address for the filter rule. This is a mandatory parameter.
Mask	The source subnet mask for the filter rule. This is a mandatory parameter.
Port	This parameter is applicable only when **Protocol** parameter is **TCP**, **UDP**, or **TCP & UDP**. Supported values: 1 to 65535 or any Supports the following value types: • a single port number • a port range. For example, 3-10. • comma-separated ports or port ranges. For example, 2,4,6-8 • any

Parameter	Description
	This is a mandatory parameter.
Destination IP Address	The destination IP address for the filter rule. The following options are available: • All • User Group—This is applicable only to NSE devices that are running release version 2.3 and later. Select the user group from the **Destination User Group** dropdown list. • IP Address / Subnet Mask—Configure the destination IP address or subnet mask and the port number. Select the appropriate option. For **User Group** and **IP Address / Subnet Mask** options, there are additional parameters that you must configure.
Destination IP Address	The destination IPv4 address for the filter rule. This is a mandatory parameter.
Mask	The destination subnet mask for the filter rule. This is a mandatory parameter.
Port	This parameter is applicable only when **Protocol** parameter is **TCP**, **UDP**, or **TCP & UDP**. Supported values: 1 to 65535 or any Supports the following value types: • a single port number • a port range. For example, 3-10. • comma-separated ports or port ranges. For example, 2,4,6-8 • any This is a mandatory parameter.
Deep Packet Inspection (DPI) Type	This parameter is applicable only when **Type** parameter is **Application Based**. The following options are supported: • **Application** – Specific type of application within a category. • **Category** – All applications belonging to a category (For example, Social Messaging). This is a mandatory parameter.
DPI Application	This parameter is applicable only when **DPI Type** parameter is set to **Application**. This is a mandatory parameter.
DPI Category	This parameter is applicable only when **DPI Type** parameter is set to **Category**.

Parameter	Description
	This is a mandatory parameter.
Apply to	This parameter is applicable only when **Type** parameter is **Application Based**. The following options are supported: • **All** • **User Group** • **IP Address / Source Subnet**
User Group	This parameter is applicable when **User Group** option is selected. This is a mandatory parameter.
IP Address / Source Subnet	This parameter is applicable when **IP Address / Source Subnet** option is selected. This is a mandatory parameter.
GEO IP WAN to LAN Filters GEO IP WAN to LAN filters allow users to configure rules to permit or deny traffic based on the source country of inbound traffic.	
Mode	Specifies the mode for GEO IP WAN to LAN filters. The following options are supported: • **Allow Only (Deny by default)** – Allow traffic coming from the countries that are configured. The traffic coming from the countries which are not part of the configured countries will be dropped. • **Deny Only (Allow by default)** – Block traffic coming from the countries that are configured. The traffic coming from countries that are not part of the configured countries will be allowed. • **None** – Disables the feature. Traffic is allowed from all the countries.
Countries	The source countries from which the traffic originates.
Exceptions for **GEO IP WAN to LAN Filters** Exceptions allow users to configure source IP address ranges that are allowed in the inbound traffic. To add a new exception, click **Add New**. The **Add New Exception** window appears, as shown in Figure 467.	
Start IP	Starting IPv4 address in the range. This is a mandatory parameter.
End IP	Ending IPv4 address in the range. This is a mandatory parameter.
GEO IP LAN to WAN Filters GEO IP LAN to WAN Filters allow users to configure rules to permit or deny traffic based on the destination country of outbound traffic.	

Parameter	Description
Mode	Specifies the mode for GEO IP LAN to WAN filters. The following options are supported: • **Allow Only (Deny by default)**: Allow traffic destined to the countries matching the configured countries. The traffic destined for the countries which are not part of the configured countries will be dropped. • **Deny Only (Allow by default)**: Block traffic destined to the countries matching the configured countries. The traffic destined for the countries which are not part of the configured countries will be allowed • **None**: Disables the feature. Traffic is allowed in all countries.
Countries	The destination countries to which the traffic is destined.
Exceptions for **GEO IP LAN to WAN Filters** Exceptions allow users to configure destination IPv4 address ranges that are allowed in the outbound traffic. To add a new exception, click **Add New**. The **Add New Exception** window appears, as shown in Figure 467.	
Start IP	Starting IPv4 address in the range. This is a mandatory parameter.
End IP	Ending IPv4 address in the range. This is a mandatory parameter.
Port Forward Rules Port Forward Rules allow users to forward traffic destined to the WAN Interface IP address of NSE on a specific TCP or UDP port to any of the LAN IP address. Port Forward Rules provides remote access to internal resources. To add a new port forward rule, click **Add New**. The **Add New Port Forward Rule** window appears, as shown in Figure 468.	
Name	Name of the port forwarding rule. The name must be unique across port forwarding, NAT one-to-one, and NAT one-to-many rules that you add. For rules created before this field was available, cnMaestro automatically generates a name during migration to the latest version. For more information, see Automatically assigning system-generated names to existing DNAT rules.
WAN	The interface to forward inbound traffic to the internal host. The following WANs are supported: • NSE3000: Maximum of four WANs + One Virtual WAN • NSE4000: Maximum of five WANs + One Virtual WAN. Only if the WAN is configured from NSE Group > WAN > WAN Configuration.

Parameter	Description
Description	Displays the user-configured description for the port forward rule.
LAN IP Address	The IPv4 address to which traffic will be forwarded. This is a mandatory parameter.
LAN Port	The LAN port to which the traffic will be forwarded. Supported values: 1 to 65535. This is a mandatory parameter.
Protocol	The protocol of forwarded traffic. The following options are supported: • **TCP** • **UDP**
Port	The destination port of the incoming traffic on the WAN interface. Supported values: 1 to 65535. This is a mandatory parameter.
Apply To	The following options are supported: • **All** • **IP Group** • **IP Address / Source Subnet**
IP Group	This parameter is applicable only when **IP Group** option is selected.
IP Address / Source Subnet	This parameter is applicable only when **IP Address / Source Subnet** option is selected. This is a mandatory parameter.
NAT One-to-One NAT One-to-One allows users to map a public IP address or an IP group on the WAN side to a single LAN IP address. The IP address on the WAN side should be different from any of the WAN interface IP addresses. NAT One-to-One mappings provide remote access to any of the LAN resources. You can apply this mapping to To add a new NAT one-to-one mapping, click **Add New**. The **Add New NAT One-to-One** window appears, as shown in Figure 469.	
Name	Name of the NAT one-to-one rule. The name must be unique across port forwarding, NAT one-to-one, and NAT one-to-many rules that you add. For rules created before this field was available, cnMaestro automatically generates a name during migration to the latest version. For more information, see Automatically assigning system-generated names to existing DNAT rules.
WAN	The WAN interface where the NAT one-to-one mapping is required.

Parameter	Description
	Select the required WAN interface from the dropdown list.
Public IP Address	The public IPv4 address on the WAN side that is used to access the LAN resource. The public IPv4 address is different from the IPv4 address of the WAN interfaces. This is a mandatory parameter.
LAN IP Address	The LAN IPv4 address of the server which is hosting the resource. This is a mandatory parameter.
Protocol	The protocol of the incoming traffic. The following options are supported: • **Any** • **TCP** • **UDP**
Apply to	Specifies whether this NAT one-to-one mapping must be applied to all IP address, specific IP addresses, or a group. The following options are supported: • **All** • **IP Group** Select the required IP group from the dropdown list. To add a new IP group, refer IP Groups. • **IP Address / Source Subnet** Specify the IP address or the source subnet in the box.
NAT One-to-Many NAT One-to-Many provides remote access to internal resources. It maps a public IP address or an IP group to multiple LAN IP addresses and ports. To add a new NAT one-to-many mapping, click **Add New**, the **Add New NAT One-to-Many** window appears, as shown in Figure 470.	
Name	Name of the NAT one-to-many rule. The name must be unique across port forwarding, NAT one-to-one, and NAT one-to-many rules that you add. For rules created before this field was available, cnMaestro automatically generates a name during migration to the latest version. For more information, see Automatically assigning system-generated names to existing DNAT rules.
WAN	The WAN interface where the NAT one-to-many mapping is required. Select the required WAN interface from the dropdown list.

Parameter	Description
Public IP Address	The public IPv4 address on the WAN side that is used to access the LAN resource. The public IPv4 address is different from the IPv4 address of the WAN interfaces. This is a mandatory parameter.
LAN IP Address	The LAN IPv4 address of the server that is hosting the resource. This is a mandatory parameter.
LAN Port	The LAN Port that is hosting the resource. Supports a single port number or a port range, for example, 3-10. This is a mandatory parameter.
Protocol	The protocol of the incoming traffic. The following options are supported: • **TCP** • **UDP**
Port	The destination port of the incoming traffic on the WAN interface. This is a mandatory parameter.
Apply to	Specifies whether this NAT one-to-many mapping must be applied to all IP addresses, specific IP address, or an IP group. The following options are supported: • **All** • **IP Group** Select the required IP group from the dropdown list. To add a new IP group, refer IP Groups. • **IP Address / Source Subnet** Specify the IP address or the source subnet in the box.
Device Access	
Respond to ICMP pings from WAN	This parameter is disabled by default. When enabled, this service is enabled for all the sources, unless specific IP addresses or IP groups are configured in the **IP Group** and **IP Address / Source Subnet** parameters.
IP Group	Specifies the IP group for this service.
IP Address / Source Subnet	Specifies the IPv4 address or source subnet for this service.
Denial of Service (DoS) Protection	
IP Spoof	Enable or disable the IP spoof attack protection. By default, this parameter is disabled.
Smurf Attack	Enable or disable the smurf attack protection. By default, this parameter is disabled.

Parameter	Description
IP Spoof Log	Enable or disable IP spoof log messages. By default, this parameter is disabled.
ICMP Fragment	Enable or disable the fragmented ping attack. By default, this parameter is disabled.

Figure 466 *The Add New Filter Rule window*

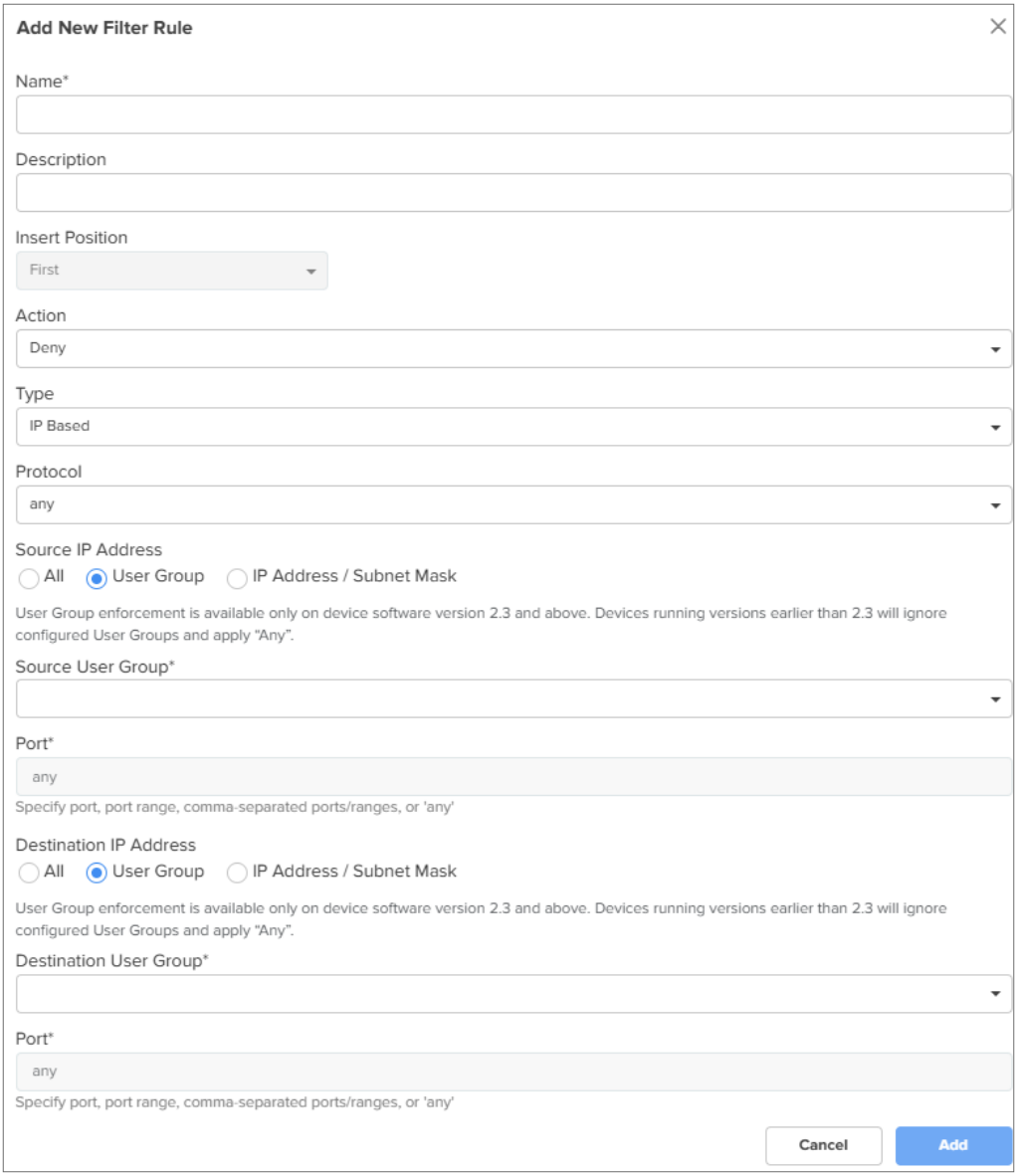


Figure 467 *The Add New Exception window*



Figure 468 *The Add New Port Forward Rule window*



Figure 469 *The Add New NAT One-to-One window*

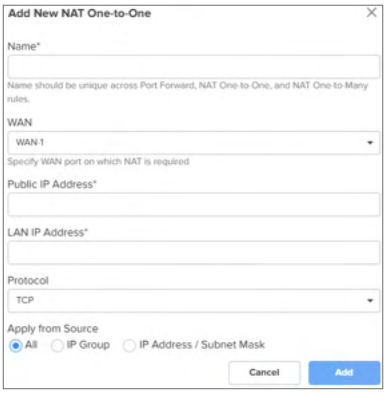


Figure 470 *The Add New NAT One-to-Many window*



3. Click **Save**.

Automatically assigning system-generated names to existing DNAT rules



Note

- This section is applicable only to **Port Forward**, **NAT One-to-One**, and **NAT One-to-Many** firewall rules configuration.
- The **Name** field in the above firewall rules is supported only from cnMaestro Cloud version 6.2.0 onwards.
- System-generated names are created only for existing rules that are migrated from earlier versions where the **Name** field was not available.

  Newly created rules must be assigned appropriate names to simplify identification and management.

When creating any of the following firewall rules, you can specify a unique name to identify and distinguish between rules:

- Port Forward Rule
- NAT One-to-One
- NAT One-to-Many

However, when upgrading to a version that introduces the **Name** field (Cloud version 6.2.0), existing firewall rules that do not already have a name are automatically assigned a unique system-generated name during migration. This ensures that every rule has a unique ID without requiring any manual changes.

The generated names are in the following format:

- Port Forward Rule: `dnat_wan<wan-id>_pf_rule_<index>`
- NAT One-to-One: `dnat_wan<wan-id>_1to1_rule_<index>`
- NAT One-to-Many: `dnat_wan<wan-id>_1ton_rule_<index>`

Where:

- *<wan-id>* represents the WAN interface (for example, wan1, wan2).
- *<index>* is a sequential number assigned per WAN interface and rule type, starting from 1.

For example,

- `dnat_wan2_pf_rule_1`
- `dnat_wan1_pf_rule_2`
- `dnat_wan1_1to1_rule_1`
- `dnat_wan1_1ton_rule_1`

DNS

NSE supports DNS-based filters. DNS-based filters allow users to block certain category of websites. From the blocked list, users can still allow certain websites by adding them to the exception list. For example, if user blocks social-media category then all the social websites will be blocked including linkedin.com since linkedin.com

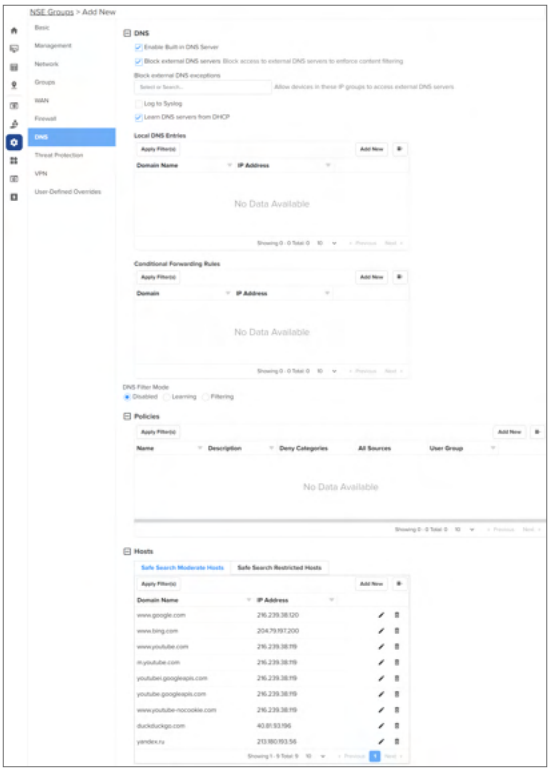
belongs to social-media category. Adding linkedin.com to the Exception to filters list will allow access to linkedin.com while blocking other social-media websites.

To configure parameters on the **DNS** page, complete the following steps:

1. On the **NSE Groups > Add New** page, select the **DNS** tab.

   The **DNS** page appears, as shown in Figure 471.

   Figure 471 *The DNS page*



2. Configure the parameters, as described in Table 99.

   Table 99 *Parameters on the DNS page*

Parameter	Description
On the DNS page, there are **DNS**, **Policies**, and **Hosts** sections.	
DNS	
Enable Built-in DNS Server	Indicates whether the on-board DNS server is enabled or disabled. By default, this parameter is enabled.
Block external DNS servers	Blocks the client to reach to any external DNS servers. By default, this parameter is enabled.
Block external DNS exceptions	Allows the clients added in the exceptions list to reach to any external DNS servers.
Log to Syslog	Specifies whether the DNS queries received from the client is logged to an external syslog server.
Learn DNS servers from DHCP	Dynamically learns the DNS server IP on WAN.

Parameter	Description
	By default, this parameter is enabled. When you disable this parameter, the **Primary DNS** and **Secondary DNS** parameters are displayed.
Primary DNS	The IPv4 address of the primary upstream DNS server.
Secondary DNS	The IPv4 address of the secondary upstream DNS server.
Local DNS Entries To add a new local host, click **Add New**. The **Add New Local Host** window appears, as shown in Figure 472.	
Domain	A domain name for the local host. This is a mandatory parameter.
IP address	The IPv4 address of the local host. This is a mandatory parameter.
Conditional Forwarding Rules To add a new forwarding rule, click **Add New**. The **Add New Forwarding Rule** window appears, as shown in Figure 473.	
Domain	A domain name for the forwarding rule. This is a mandatory parameter.
IP address	The IPv4 address of the server to which the DNS query is forwarded.
DNS Filter Mode	Specifies the mode for DNS filtering. The following options are supported: • **Disabled**: Disables DNS filter. By default, this option is selected. • **Learning**: Builds local cache for domain categories but does not filter requests. • **Filtering**: Filters requests based on configuration.
Policies To add a new policy, click **Add New**. The **Add New Policy** window appears, as shown in Figure 474.	
Name	Name for the policy. This is a mandatory parameter.
Description	Description about the policy.
Deny categories	Categories to deny in the following sections: • **Productivity** • **Privacy** • **Sensitive** • **Misc** • **IT Resources** • **Security**

Parameter	Description
	Expand the sections and select individual categories. To select all categories in a section, select the checkbox provided for the section.
Safe Search Mode	The following options are supported: • **Disabled:** Disables safe search mode. By default, this option is enabled. • **Moderate:** Enable moderate safe search mode. • **Restricted:** Enable restricted safe search mode.
Allow Exceptions (List of Domain Names)	Enter the exempted domain names separated by a comma (,).
Apply to	The following options are supported: • **All**: Apply to all user groups. By default, this option is selected. • **User Group**: Apply to selected user groups.
User Group	This parameter is applicable only when **User Group** option is selected for **Apply to** parameter. This is a mandatory parameter.
Hosts Hosts section contains two tabs - **Safe Search Moderate Hosts** and **Safe Search Restricted Hosts** The following parameters appear in both the tabs and can be configured as required. A list of hosts are already added by default. You can modify these hosts by clicking the edit icon or you can add new hosts by clicking **Add New** in the respective tabs as shown in Figure 475 and Figure 476.	
Domain Name	The domain name for the safe search host This is a mandatory parameter.
IP address	The IPv4 address of the safe search host. This is a mandatory parameter.

Figure 472 *The Add New Local Host window*



Figure 473 *The Add New Forwarding Rule window*



Figure 474 *The Add New Policy window*

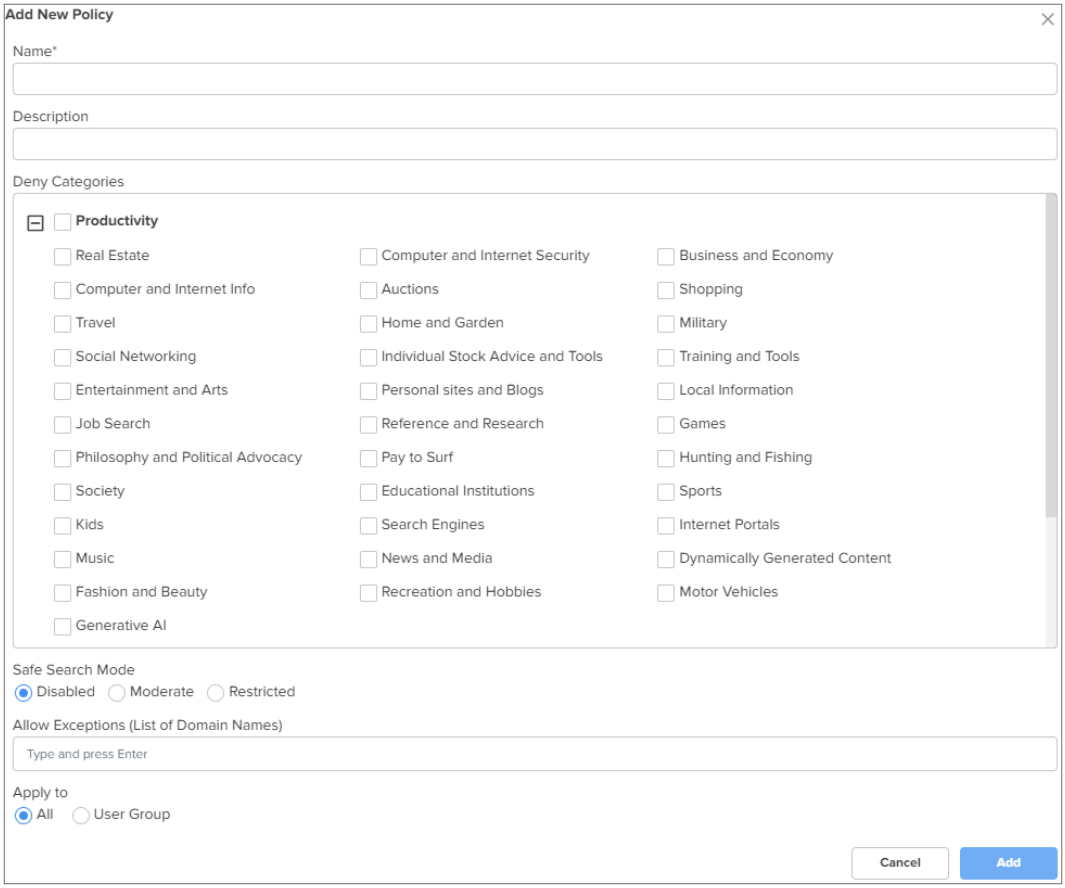


Figure 475 *The Add New Safe Search Moderate Host*



Figure 476 *The Add New Safe Search Restricted Host*



3. Click **Save.**

Threat Protection

Note

For NSE3000, release 6.2.0 introduces new categories for Snort vrt. The earlier categories (prior to release 6.2.0) are mapped to the corresponding newer categories.

Using the **Threat Protection** tab, you can configure the Intrusion Detection and Prevention system (IDS/IPS) parameters.

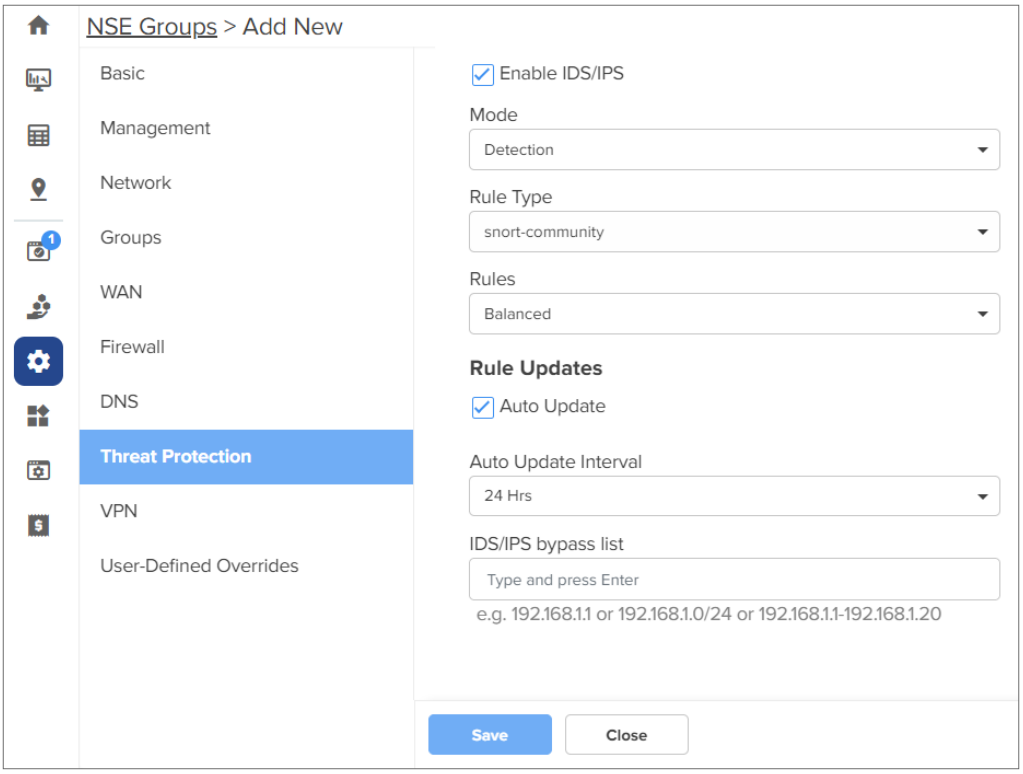
NSE supports IDS/IPS engine. IPS engine uses a series of rules that help define a malicious network activity. IPS engine supports rules from snort and emerging threats. The solution supports both community and licensed rules. The IPS engine uses these rules to find packets that match against them and generates alerts for users.

To configure parameters on the **Threat Protection** page, complete the following steps:

1. On the **NSE Groups > Add New** page, select the **Threat Protection** tab.

   The **Threat Protection** page appears, as shown in Figure 477.

   Figure 477 *The Threat Protection page*



2. Configure the parameters, as described in Table 100.

   Table 100 *Parameters on the Threat Protection page*

Parameter	Description
IDS/IPS	
Enable IDS/IPS	Indicates whether IDS/IPS is enabled or disabled. By default, this parameter is enabled *only in new NSE groups*. When this parameter is enabled, the following default settings apply: • **Mode**: Detection • **Rule Type**: snort-community • **Rules**: Balanced • **Auto Update**: Enabled • **Auto Update Interval**: 24 Hrs
Mode	Specifies the IDS/IPS mode.

Parameter	Description
	The following options are supported: • **Detection** – Detects malicious activity and generates alerts for users. • **Prevention** – Detects malicious activity, generates alerts for users, and takes action to prevent attacks.
Rule Type	Specifies the IDS/IPS rule type. The following options are supported: • **snort-community** – The community rule set is a GPLv2 Talos certified rule set that is distributed free of charge and without any license restrictions. The rules are updated every Tuesday and Thursday. • **snort-vrt** – The Snort Subscriber rule set is developed by Talos research team and is governed by license agreement. The rule set is updated on Tuesday and Thursday. The snort-vrt rule set requires an oinkcode to download and activate rules. • **emerging-threats open** – Consists of signatures contributed from the community. The emerging-threats open rule sets are distributed free of charge. • **emerging-threats pro** – Consists of signatures created as a result of Proofpoint research. The rule sets are governed by license agreement. The emerging-threats pro rule set requires an oinkcode to download and activate the rules.
Rules	Specifies the IDS/IPS rule policy. This parameter is applicable when **Rule Type** is **snort-vrt** or **snort-community**. The following options are supported: • **Connectivity** – Policy designed to favor device performance over the security controls in the policy. • **Balanced** – This policy is the default policy that is recommended for initial deployments. The policy attempts to balance security needs and performance characteristics. • **Security** – This policy is designed for customer base that is extremely concerned about organizational security. This policy is deployed in networks that have higher security requirements.
Oink Code	This parameter is applicable when **Rule Type** is **snort-vrt** or **emergency- threats pro**.
Category	Categories to select from the **Category** section. This parameter is applicable when **Rule Type** is **snort-vrt**, **emerging-threats open**, or **emerging-threats pro**. **Note**: The categories are same for **emerging-threats open** and **emerging-threats pro** rule types. You can select or clear all categories by using the **Category** checkbox.
Rule Updates	
Auto Update	Indicates whether the IDS/IPS rules must be automatically updated or not. By default, this parameter is enabled. When **Auto Update** is enabled, NSE will periodically download and activate the IDS/IPS rules.
Auto Update Interval	Time interval for the periodic updates of IDS/IPS rules. The following options are supported:

Parameter	Description
	• **12 Hrs** – Auto updates the rules every 12 hours. • **24 Hrs** – Auto updates the rules every 24 hours. By default, the **24 Hrs** option is selected.
IDS/IPS bypass list	List of allowed IPv4 addresses or range of allowed IPv4 addresses. IDS/IPS operating in prevention mode blocks traffic from a host on detecting malicious traffic from the host. When an IPv4 address is part of allowed IP addresses, IDS/IPS will not block traffic from the host even when malicious traffic is detected.

3. Click **Save**.

VPN

NSE provides an on-board VPN server that allows remote users to establish a connection using the native VPN client supported in most of the operating systems. The VPN server uses the L2TP/IPsec protocol with the IPsec encryption and hashing algorithms. The VPN server maintains a pool of IP addresses and leases the IP addresses from this pool for remote users.

NSE also provides an on-board RADIUS server that allows authentication and accounting of enterprise and remote users. The RADIUS server maintains user profiles in a central database.

The **VPN** page allows to set the following configurations:

- Site-to-Site VPN configuration
- Client VPN configuration
- User configuration for Client VPN protocols
- Tailscale configuration
- RADIUS Client configuration
- VPN Server interface configuration

Site-to-Site VPN configuration

IPsec tunnel is a VPN technology that provides a secure, encrypted connection between two devices or networks over the internet or another public network. It uses IPsec protocols to encrypt the traffic between two endpoints, making it difficult for anyone to intercept the communication.

IPsec site-to-site tunnel is used to connect two remote sites for secure communications. NSE allows setting up tunnels both in responder mode and initiator mode. Both, IKEv1 and IKEv2 are supported in the configuration. The default version is IKEv2.



Note

You can configure up to 100 IPsec site-to-site tunnels.

Pre-shared key is the authentication method supported by the NSE device. Each site can have its own pre-shared key. The site is identified by an identifier (string or the IP address of the site). Each site has to be configured with a local and remote site for the tunnel to establish.

Note

NSE supports VPN translation for a Site-to-Site configuration. The local subnets that are advertised to peers are configured to translate to a different equally sized subnet. This is useful in deployments where the same local subnet is used in multiple locations. For example, the 192.168.200.0/24 network can be found in multiple locations as it is the default network configuration. If 192.168.200.0/24 is available in multiple locations, this can be configured to be translated to 10.10.10.0/24. to prevent address conflicts, The translation can also be 1 to M. In case of 1 to M, 192.168.200.0/24 can be configured to be translated to 10.10.10.10/32.

You can perform the following configurations:

- Enabling a Site-to-site VPN configuration
- Switching to Auto VPN from Site-to-Site VPN

Enabling a Site-to-site VPN configuration

To enable a site-to-Site VPN and configure the settings, complete the following steps:

1. On the **NSE Groups**>**Add New** page, select the **VPN** tab.
2. In the **Site-to-Site VPN** section, select the **Enable Site-to-Site VPN** checkbox to enable the site-to-site VPN configuration. By default, it is disabled. When you enable site-to-site VPN, you are allowed to add a new site-to-site VPN and configure parameters.
3. To add a new site-to-site VPN, click **Add New**. The **Add New Site-to-Site VPN** window appears, as shown in Figure 478.

   Figure 478 *The Add New Site-to-Site VPN window*

4. Configure the parameters, as described in Table 101.

   Table 101 *Parameters for the Site-to-Site VPN configuration*

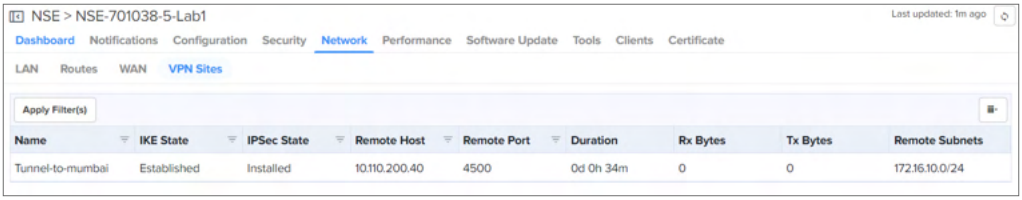
Parameter	Description
Name	A name for the new site-to-site VPN. This is a mandatory parameter.
IKE version	The Internet Key Exchange (IKE) version for the site-to-site VPN. The following options

Parameter	Description
	are supported: • **IKE v1** • **IKE v2**
Role	Specifies the role for the tunnels. The following options are supported: • **Initiator** • **Responder** Default role: Responder
Dead peer detection interval	The interval (in seconds) for detecting dead peers. Range: 30 - 600 seconds. Default: 120 seconds This is a mandatory parameter.
Remote ID	The remote ID. The value of 192.168.50.10 is pre-configured and is not modifiable. This is a mandatory parameter.
Local ID	The local ID. This is a mandatory parameter.
Local Subnets	This is a mandatory parameter. This parameter allows you to add multiple local subnets. To add new local subnets, complete the following steps: a. Click **Add New**. The **Add New Local Subnet** window appears. b. Select the required local subnet address from the **Local Subnets** dropdown list. The **VPN subnet** field is optional. If the Local subnets have a VPN translation, then provide a VPN network address in the **VPN subnet** field or it can be left blank (empty). NSE supports the VPN translation feature. c. Click **Add** on the Add New Local Subnet window.
Remote Subnets	The comma-separated list of remote subnets. This is a mandatory parameter.
Remote PSK	The remote PSK. This is a mandatory parameter.
Local PSK	The local PSK. This is a mandatory parameter.
The following parameters are common for both **IKE Phase 1** and **IKE Phase 2**.	
Encryption	The following options are supported: • **aes128** • **aes192** • **aes256** • **aes128-gcm16** • **aes192-gcm16**

Parameter	Description
	• **aes256-gcm16** • **3des**
Integrity	The following options are supported: • **md5** • **sha1** • **sha256**
DH Group	The following options are supported: • **1** • **2** • **5** • **14** • **15**
Key Lifetime	The duration (in hours) for the pre-shared key. Range: 1 to 24

5. Click **Add**. The new site-to-site VPN is added.
6. Click **Save** on the Add New page to apply the changes.
7. To view the IPsec tunnel statistics, navigate to the **NSE Group > Network > VPN Sites** tab, as shown in Figure 479.

Figure 479 *The VPN Sites page*



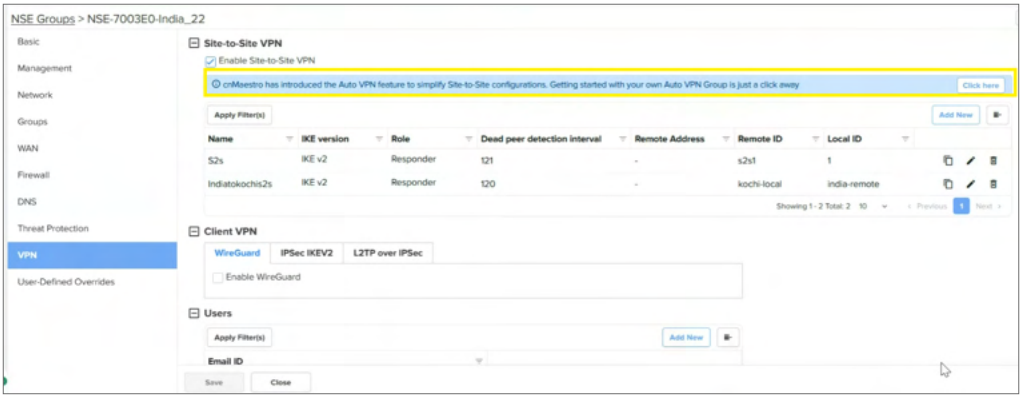
Switching to Auto VPN from site-to-site VPN

Currently, NSE supports 100 site-to-site VPN tunnels, However, cnMaestro allows the Auto VPN configuration to simplify Site-to-Site configuration. The Auto VPN configuration is useful for device-level configuration, device-level monitoring, and debugging.

Consider the following key points:

- If there is an NSE device for which the Auto VPN is not configured, the **Site-to-Site VPN** section on the VPN page displays a message (as shown in Figure 480). This message indicates that you can add the Auto VPN configuration for this NSE device. When you configure an auto VPN group using the **Configuration** > **NSE Profiles** > **Auto VPN** page, the Site-to-Site VPN configuration changes are disabled for the NSE device.

Figure 480 *The site-to-site VPN configuration before switching to Auto VPN*

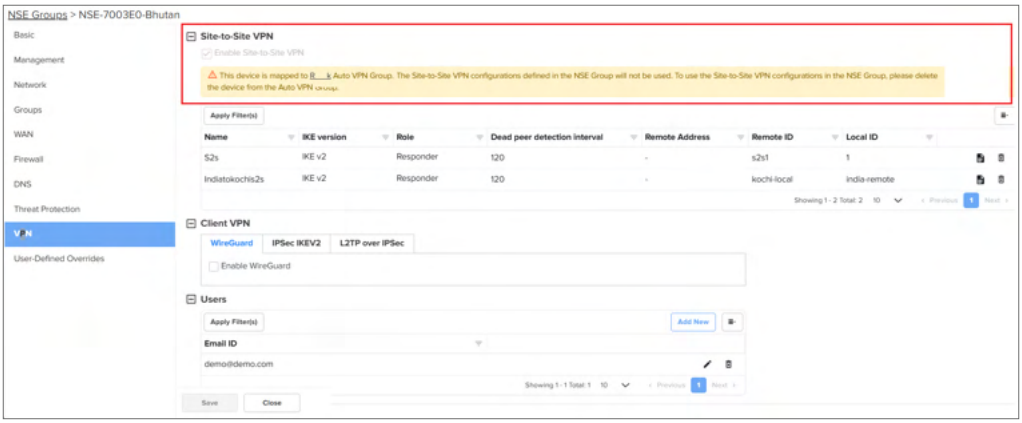


- If the sites are already added to an Auto VPN group, then you cannot use the Site-to-Site VPN configuration. A message is displayed in the **Site-to-Site VPN** section on the VPN page. You must delete the NSE device from the Auto VPN group on the **Auto VPN** page to use the Site-to-Site VPN configuration.

Note

You CANNOT configure a site-to-site VPN for the NSE device on which auto VPN is configured. You must delink the devices from Auto VPN group and then configure the Site-to-Site VPN feature.

Figure 481 *The site-to-site VPN configuration after switching to Auto VPN*



Client VPN configuration

To configure Client VPN specific parameters on the **VPN** page, complete the following steps:

1. On the **VPN** page (as shown in), go to the **Client VPN** section.

   The **Client VPN** section contains the following tabs:

   - WireGuard: A VPN protocol that is highly secure.It is simpler and more efficient than traditional IPSec. It is simpler and more efficient than traditional IPSec.
   - IPSec IKEV2
   - L2TP over IPSec

2. Configure the parameters, as described in Table 102.

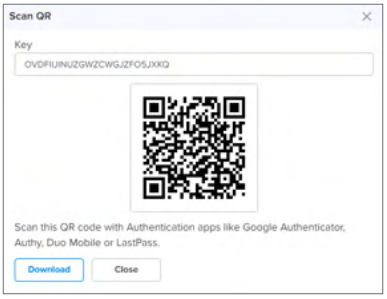
Table 102 *Parameters for the Client VPN configuration*

Parameter	Description
WireGuard	
Enable WireGuard	Indicates whether WireGuard is enabled or disabled. By default, this parameter is disabled.
Following parameters appear when you select **Enable WireGuard** checkbox.	
Port	Indicates the WireGuard listen port number. Default: 51820 This is a mandatory parameter.
Client Pool	Indicates the WireGuard interface IP for the device and the client IPs to be assigned for the WireGuard clients. This is a mandatory parameter.
Offline Interval	Duration (in minutes) after which a WireGuard peer is marked offline. Default: 5 minutes This is a mandatory parameter.
Enable Split Tunnel	Indicates whether the split tunnel is enabled or disabled. By default, this parameter is disabled. **Note**: When you enable split tunnel, only the traffic destined to tunnelled subnets is allowed. You can override the **Enable Split Tunnel** parameter at the user level.
Tunnelled Subnets	Specifies the list of local subnets in NSE that should be allowed access from the WireGuard clients. **Note**: The same **Tunnelled Subnets** field is auto-populated in the **Add New User** window. You can edit this field at the user level.
Two Factor Authentication Session TTL	Duration (in hours) for which a user's session is valid. Default: 8 hours, Range: 1-24 This is a mandatory parameter.
Two Factor Authentication Idle Timeout	Duration (in minutes) after which a user's session is marked idle. Default: 30 minutes, Range: 1-60 This is a mandatory parameter.
Two Factor Authentication Customization parameters	
Title	Specifies the portal title Default: Sign In
Subtitle	Displays a message for completing authentication. Default: Authenticate to access the network
Username Label	Specifies the label for the username field. Default: Username
Password Label	Specifies the label for the password field. Default: Password

Parameter	Description
Sign In Button	Specifies the label for the sign in button. Default: Sign In
Save Link Text	Specifies the text for saving this authentication link. Default: Save this link
Copy Button	Specifies the label for the copy button. Default: Copy
Username Password Required Message	Message displayed when any of the fields are empty. Default: Username and password are required.
Network Error	Error message displayed when authentication is unable to proceed because of connectivity or network issues. Default: Network error.
Link Copied	Confirmation message displayed when you copy the link. Default: Link Copied
Status Title	Title displayed on the status page Default: Status
Status Message	Message displayed indicating the current authentication or session state. Default: You are authenticated and can use the network.
Status Logout Button	Specifies the label for the logout button. Default: Logout
Exempt Title	Title displayed when a device is exempt from Two Factor Authentication. Default: Not Required
Exempt Heading	Message displayed when a device is exempt from Two Factor Authentication. Default: No login required
Exempt Message	Description message displayed informing the device's Two Factor Authentication is not required. Default: This device is not configured for portal authentication.
IPSec IKEV2	
Enable IPSec IKEV2	Indicates whether IPSec IKEV2 is enabled or disabled. By default, this parameter is disabled.
Following parameters appear when you select **Enable IPSec IKEV2** checkbox.	
Client IP Pool Range Start	Starting IPv4 address in the range. This is a mandatory parameter.
Client IP Pool Range End	Ending IPv4 address in the range. This is a mandatory parameter.
L2TP over IPSec	
Enable L2TP over IPSec	Indicates whether L2TP over IPSec is enabled or disabled. By default, this parameter is disabled.

Parameter	Description
Following parameters appear when you select **Enable L2TP over IPSec** checkbox.	
Client IP Pool Range Start	Starting IPv4 address in the range. This is a mandatory parameter.
Client IP Pool Range End	Ending IPv4 address in the range. This is a mandatory parameter.
IPsec Shared Secret	Enter a pre-shared key string for the IPsec protocol. The shared secret is used between the VPN Client and Server for device authentication. This is a mandatory parameter.
Enable 2FA	Indicates whether two-factor authentication (2FA) is enabled or disabled. By default, this parameter is disabled.

3. When you enable **two-factor authentication (2FA)**, scan the QR code to add a 16-digit key to a particular user's Google Authenticator app.



An email is also sent to the configured email address with the QR code and the 16-digit key. The two-factor authentication gets enabled for the user when the user tries to connect to the NSE device using the remote VPN client from the WAN side. Users on the LAN side do not require two-factor authentication (2FA).

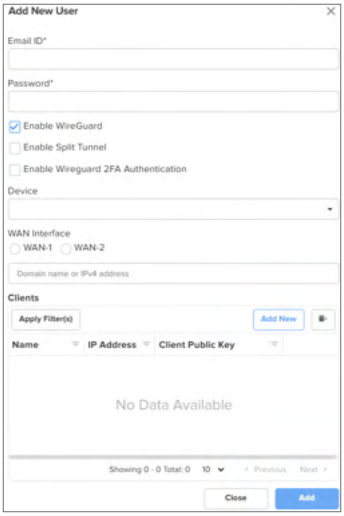
4. Click **Save** on the Add New page to add the changes.

User configuration for Client VPN protocols

The **Users** section on the VPN page is common for all the three protocols - WireGuard, IPSec IKEV2, and L2TP over IPSec. To configure user specific parameters on the **VPN** page, complete the following steps:

1. On the **VPN** page (as shown in), go to the **Users** section.
2. To add a new user, click **Add New**. The **Add New User** window appears, as shown in Figure 482.

Figure 482 *The Add New User window*



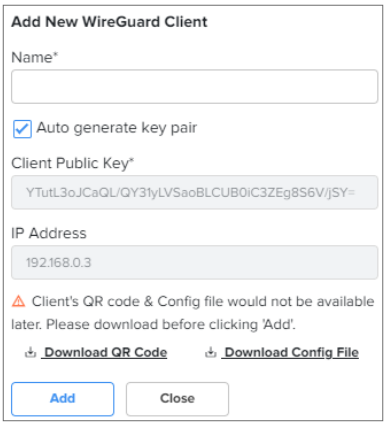
3. Configure the parameters, as described in Table 103.

Table 103 *Parameters for the user configuration*

Parameter	Description
Users	
Email ID	Email ID of the user. User is either an enterprise user or a remote user. This is a mandatory parameter.
Password	Password for the user. This is a mandatory parameter.
Enable WireGuard	Indicates whether WireGuard is enabled or disabled. This parameter is visible on the **Add New User** window only if you have selected the **Enable WireGuard** checkbox in the Client VPN section. By default, this parameter is disabled.
Following parameters appear when **Enable WireGuard** checkbox is selected in the **Add New User** window.	
Enable Split Tunnel	Indicates whether split tunnel is enabled or disabled. By default, this parameter is disabled. When enabled, you must also configure the allowed subnets in the **Tunnelled Subnets** parameter.
Tunnelled Subnets	Specifies the list of local subnets in NSE that should be allowed access from the WireGuard clients.
Enable Wireguard 2FA Authentication	Indicates whether WireGuard 2FA authentication is enabled or disabled. By default, this parameter is disabled.
Device	Indicates the NSE device. When you select an NSE device, the device's public key is populated in the **[Peer]** section of the WireGuard client configuration file. This is a mandatory parameter.
WAN Interface	WAN Interface of the NSE device.

Parameter	Description
	When you select a WAN interface, the NSE device's WAN IP is populated as the endpoint IP in the [Peer] section of the WireGuard client configuration file. The following WAN Interface options are supported: • WAN-1 • WAN-2
Clients: In this section, you have an option to add a new WireGuard client. To add a new WireGuard client, click **Add New**. The **Add New WireGuard Client** window appears, as shown in Figure 483.	
Name	Name for the new WireGuard client. This is a mandatory parameter.
Auto generate key pair	Generates a public and private key pair for the client. By default, this parameter is enabled. When this option is enabled, the **Client Public Key** field is auto-populated with the public key generated for that client. When this option is disabled, you need to provide the WireGuard client public key generated on the WireGuard client device.
Client Public Key	Public key of the client. This is a mandatory parameter.
IP Address	Auto-generated IP address of the WireGuard client.
Note: You have options to download QR code and configuration file in the **Add New WireGuard Client** window, as shown in Figure 483.	

Figure 483 *The Add New WireGuard client window*



4. Click **Add**. The user configuration is added.
5. Click **Save** on the Add New page to apply the changes.

Tailscale configuration

Note

Tailnet page and the corresponding Tailscale configuration are supported only when NSE **Security Plus** mode is enabled.

To view the Tailnet information on **NSE** > **Network** page, you must enable the Tailscale option and configure the parameters accordingly.

To enable and configure Tailscale parameters, complete the following steps:

1. On the **VPN** page, go to the **Tailscale** section.
2. Select the **Enable Tailscale** checkbox.
3. Configure the parameters as described in the following table.

Figure 484 *Tailscale section*



Table 104 *Parameters for the Tailscale configuration*

Parameter	Description
Authentication Key	Tailscale pre-shared authentication key.
Enable Accept Routes	Select this checkbox if you want NSE to approve subnet routes advertised by other Tailscale nodes.
Advertise Routes	Comma-separated list of subnets to advertise to Tailnet.

Note

The user must approve the routes in the Tailscale admin console.

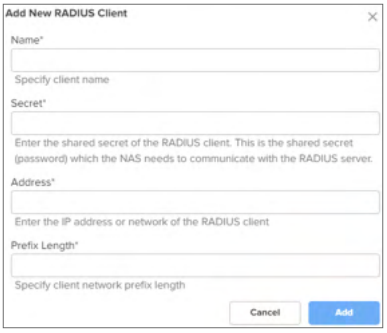
4. Click **Save**.

RADIUS Client configuration

To set the RADIUS client configuration on the VPN page, complete the following steps:

1. On the **VPN** page, go to the **RADIUS Clients** section.
2. To add a new RADIUS client, click **Add New**. The **Add New RADIUS Client** window appears, as shown in Figure 484.

Figure 485 *The Add New RADIUS Client window*



3. Configure the parameters, as described in Table 14.

   Table 105 *Parameters for the RADIUS Client configuration*

Parameter	Description
Name	Name of the RADIUS client. This is a mandatory parameter.
Secret	The shared secret of the RADIUS client. This is the shared secret (password) that the NAS needs to communicate with the RADIUS server. This is a mandatory parameter.
Address	The IPv4 address or network address of the RADIUS client. This is a mandatory parameter.
Prefix Length	The client network prefix length. This is a mandatory parameter.

4. Click **Add** on the Add New RADIUS Client window.
5. Click **Save** onthe Add New page to add the changes.

VPN Server interface configuration

To configure the VPN Server interface, complete the following steps:

1. On the **VPN** page (as shown in), go to the **VPN** section.

   The **VPN Server Interface** dropdown list is visible. This parameter displays the following options:

   - **WAN-1 -** The first WAN interface on your server.
   - **WAN-2 -** The second WAN interface on your server.
   - **All -** Applies to all WAN interfaces.
2. Select the required option from the dropdown list.
3. Click **Save** on the Add New page to add the changes.

User-Defined Overrides

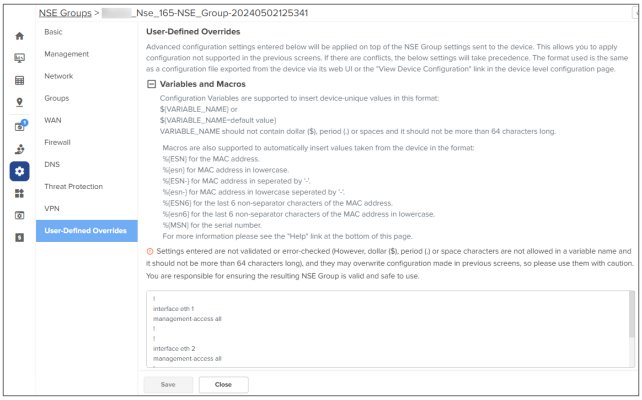
Using the **User-Defined Overrides** tab, you can configure the user-defined overrides.

To configure parameters on the **User-Defined Overrides** page, complete the following steps:

1. On the **NSE Groups > Add New** page, select the **User-Defined Overrides** tab.

   The **User-Defined Overrides** page appears, as shown in Figure 486.

Figure 486 *The User-Defined Overrides page*



2. In the text box, enter the configuration that you want to apply to the device.
3. Click **Save**.

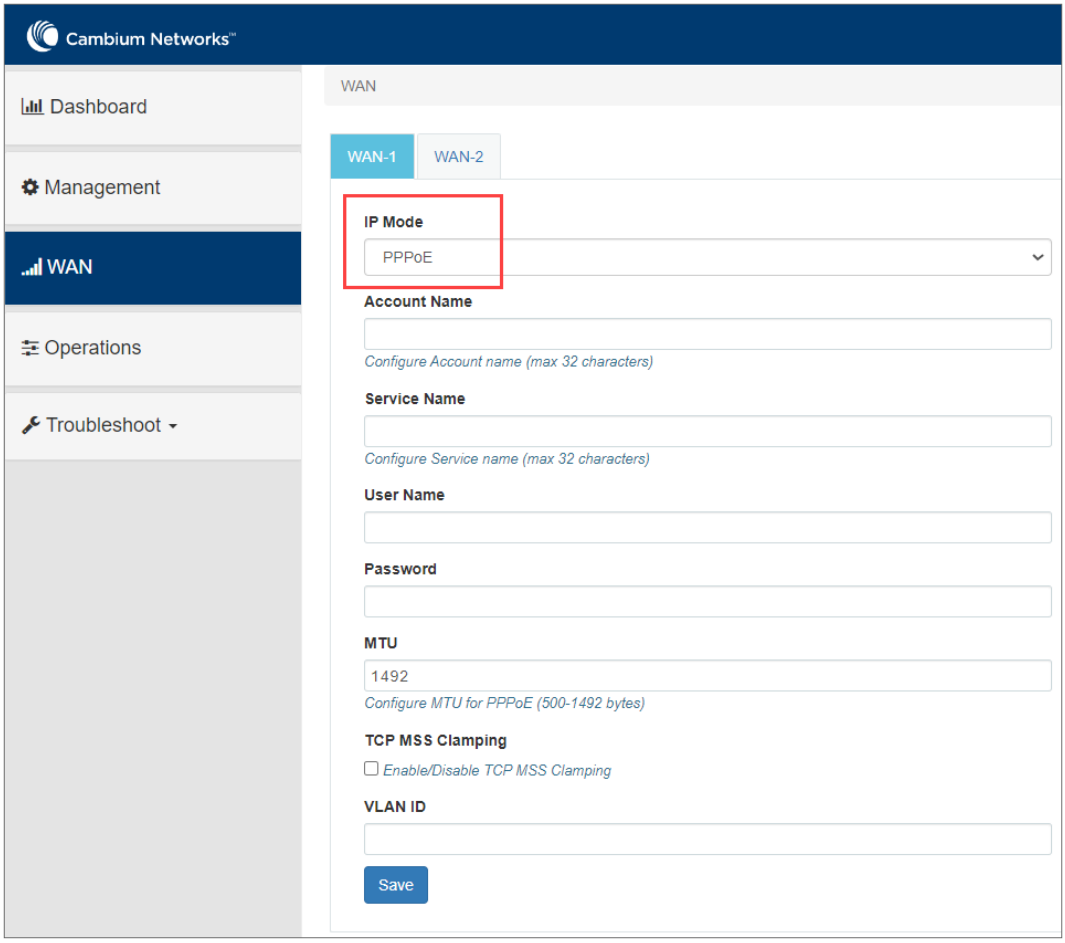
Configuring WAN in the device UI

In the **WAN** page, you can configure the device's IPv4 address based on the IP mode.

Note

If **PPPoE** is used as the WAN connection mode as shown in Figure 487, make sure to configure the PPPoE username and password. Once you have configured the PPPoE user name and password, you can proceed to configure the NSE group by providing the same username and password and then attaching the default NSE group to the device.

Figure 487 *PPPoE as WAN connection mode*



To view and configure the WAN settings, complete the following steps in the device UI:

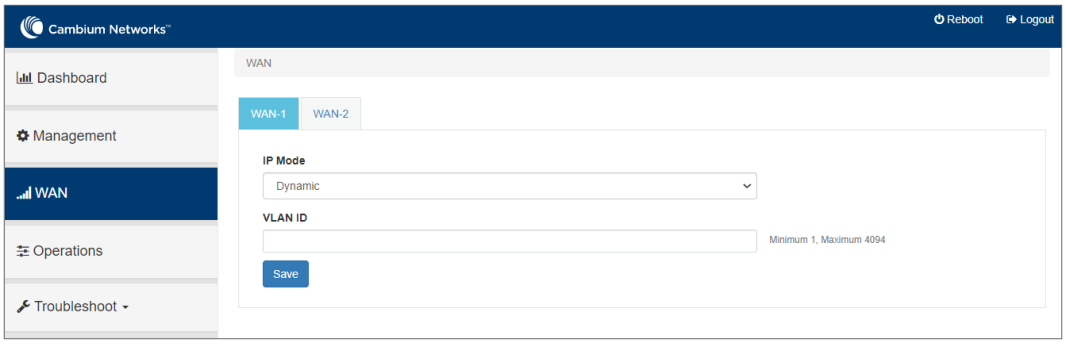
1. From the main NSE dashboard page, click **WAN** tab from the left panel.

   The **WAN** page appears, as shown in Figure 488.

Note

By default, WAN-1 page appears. You can configure WAN on WAN-1 or WAN-2.

Figure 488 *The WAN page*



2. Configure the parameters, as described in Table 106.

Table 106 *Parameters on the WAN page*

Parameter	Description
IP Mode	Determines the network that must be configured to use IPv4 addresses. The following options are supported: • **Dynamic** • **Static** • **PPPoE** By default, the **Dynamic** mode is selected.
VLAN ID	The VLAN ID can range from 1 to 4094. The VLAN configuration is optional. When the 802.1Q header is configured, all transmitted frames are expected to include the 802.1Q header with the same VLAN ID.
Following parameters appear only when you select the mode as **Static** from the **IP Mode** dropdown list, as shown in Figure 489.	
IP Address	The 32-bit binary number that identifies a network element by both network and host.
Subnet Mask	The subnet mask for the destination IP/network for the route.
Gateway	The gateway for the destination IP/network for the route.
DNS	
Primary DNS	The IPv4 address of primary upstream DNS server.
Secondary DNS	The IPv4 address of secondary upstream DNS server.
Following parameters appear only when you select the mode parameter as **PPPoE** from the **IP Mode** dropdown list, as shown in Figure 490.	
Account Name	The name of Access Controller. This parameter allows a maximum of 32 characters. This parameter is optional.
Service Name	Service name of Access Controller. This parameter allows a maximum of 32 characters. This parameter is optional.
User Name	A user name for PPPoE authentication. This parameter is mandatory.
Password	A password for PPPoE authentication. This parameter is optional.
MTU	MTU for PPPoE interface in bytes. Default: 1492. Range: 500 to 1492
TCP MSS Clamping	Indicates whether TCP MSS Clamping is enabled or disabled. By default, this parameter is disabled.

Figure 489 *Static mode*

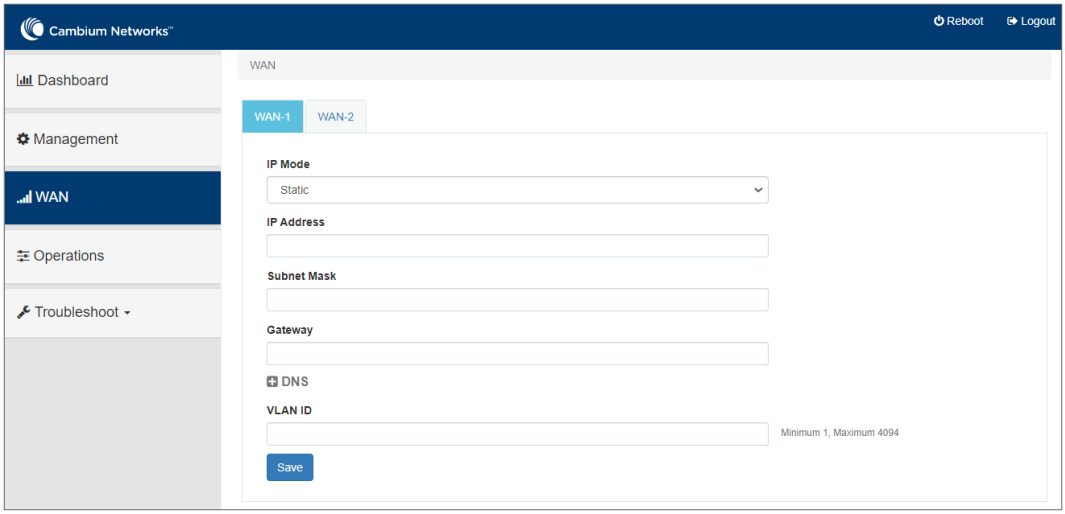
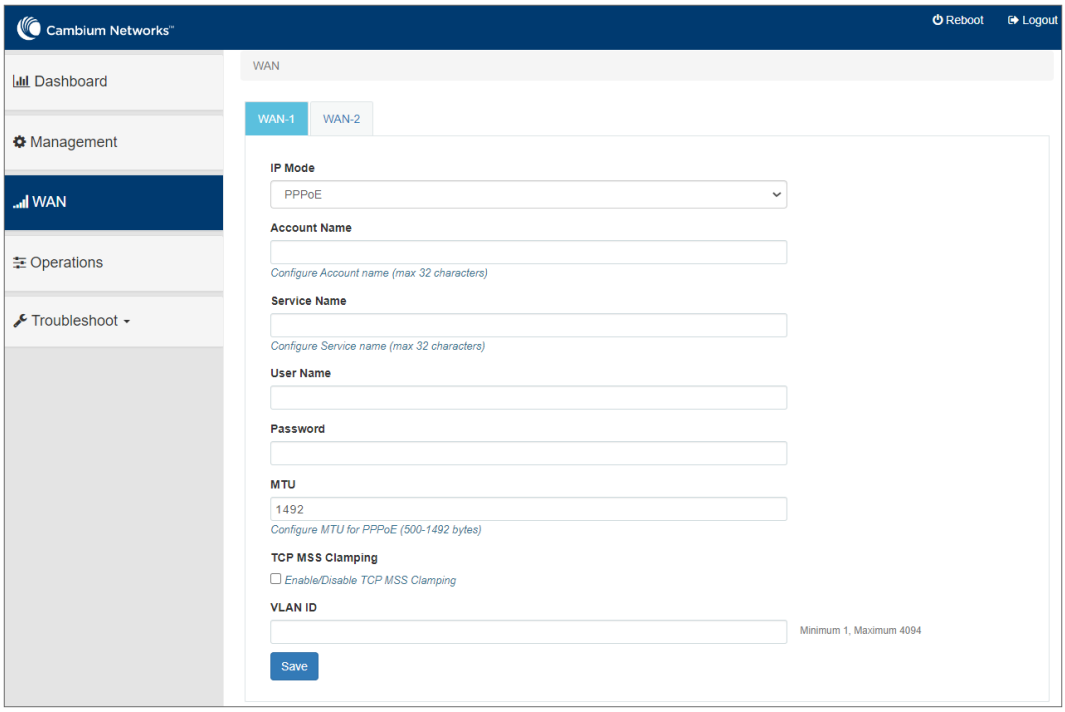


Figure 490 *PPPoE mode*



3. Click **Save**.

Configuring Auto VPN

Site-to-site VPN is a secure way of connecting multiple networks across sites. Currently, NSE supports 100 site-to-site VPN tunnels, However, this site-to-site VPN has some problems specific to device-level configuration, device-level monitoring, and debugging.

As a solution, the **Auto VPN** feature of NSE offers simplified configuration, monitoring, and debugging of site-to-site tunnels. With this feature, NSE devices can be networked in either of the following modes: Hub and Spoke, Mesh, or Hybrid. For example, there is one NSE device (two in HA mode) present in one site. With Auto VPN

configured, the NSE device connects multiple sites in either one of the modes (Hub and Spoke mode or Mesh' mode).

When Auto VPN is configured using cnMaestro, NSE automates the setting up of site-to-site tunnels for the VPN groups between Cambium NSE devices. Site-to-site tunnels can be deployed either in a Hub and Spoke mode or in full mesh mode.

Hub and Spoke mode

In the Hub and Spoke mode, 100+ NSE devices can be accommodated in the network, which are connected to a single hub node. There is no need to edit 100 NSE groups to connect all these devices.

The hub can be a non-Cambium device, allowing for greater flexibility in deployment scenarios.

Example: In current deployments of NSE devices, third-party firewalls are used as hubs and NSE devices as spokes. If the Hub and Spoke mode is configured, only a single hub (non-Cambium) is used and all the sites are connected to this single hub. In this mode, the spoke devices (NSE) establish secure connections with the hub.

Mesh mode

Full mesh deployments require configuring of the networks on each NSE device. When Auto VPN is configured, the devices in the group establish connectivity with the every other member in the group in a full mesh mode.

The Mesh mode is applicable only when the cambium hubs are used.



Note

You CANNOT configure a site-to-site VPN for the NSE device on which Auto VPN is configured. You must delink the devices from the Auto VPN group to configure the Site-to-Site VPN feature. The device cannot have both site-to-site VPN and auto VPN at the same time.

Using the cnMaestro UI, you can configure the Auto VPN feature of NSE. The Auto VPN configuration involves the following tasks:

- Creating Auto VPN groups
- Adding hubs and spokes for sites

Creating Auto VPN groups

With the flexibility of configuring modes for NSE devices, you can create an Auto VPN group for:

- **All Cambium hubs**: Create an Auto VPN group by disabling the **Use non-Cambium Hub** option. For details, see Auto VPN group for all Cambium hubs.
- **A non-Cambium hub**: Create an Auto VPN group by enabling the **Use non-Cambium Hub** option. For details, see Auto VPN group for a non-Cambium hub.

Auto VPN group for all Cambium hubs

For a traditional Cambium-only setup, you can create auto VPN groups by disabling the **Use non-Cambium Hub** option. Complete the following steps to configure the Auto VPN group for all Cambium hubs:

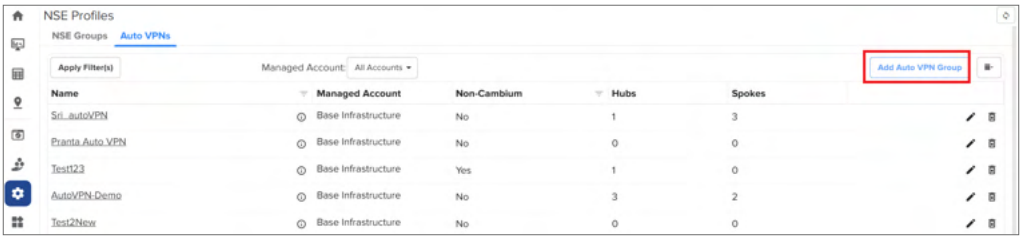
1. From the home page, navigate to **Configuration** > **NSE Profiles**.

   The **NSE Profiles** page appears.

2. On the **NSE Profiles** page, click the **Auto VPNs** tab.

   The **Auto VPNs** page appears.

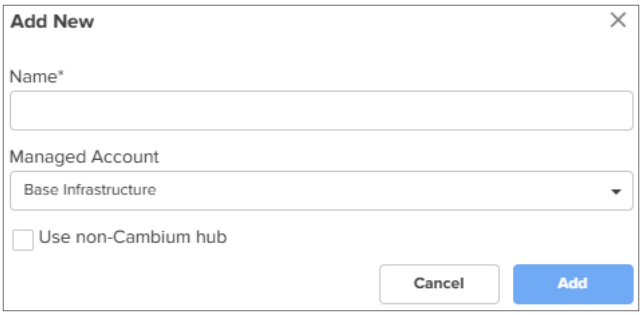
   Figure 491 *The Auto VPN page*



3. To create a new auto VPN group, click **Add Auto VPN Group**.

   The **Add Auto VPN Group** window appears.

   Figure 492 *The Add Auto VPN Group window*



4. On the **Add Auto VPN Group** window, provide the values as described:

   a. In the **Name** field, enter a valid name for the VPN group.

   b. From the **Managed Account** dropdown list, select a name of the managed account.

   c. To create the auto VPN goup for all Cambium hubs, ensure that the **Use non-Cambium hub** checkbox is not selected.

5. Click **Add**.

   The Auto VPN group for all Cambium hubs is created.

Auto VPN group for a non-Cambium hub

For a hybrid setup where a non-Cambium device serves as the hub, you must enable the **Use non-Cambium hub** option.

Complete the following steps to configure the Auto VPN group for a non-Cambium hub:

1. From the home page, navigate to **Configuration** > **NSE Profiles**.

   The **NSE Profiles** page appears.

2. On the **NSE Profiles** page, click the **Auto VPNs** tab.

   The **Auto VPNs** page appears.

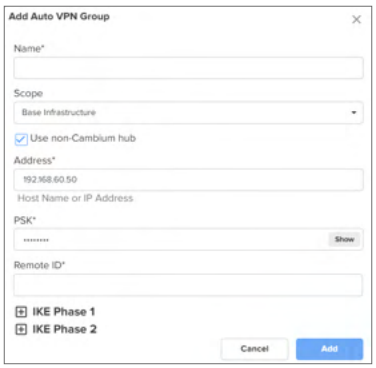
3. To create a new auto VPN group, click **Add Auto VPN Group**.

The **Add Auto VPN Group** window appears.

4. On the **Add Auto VPN Group** window, perform the following steps:
   a. In the **Name** field, enter a valid name for the group.
   b. Select the required option from the **Managed Account** dropdown list.
   c. To create an auto VPN group for a non-Cambium hub, select the **Use non-Cambium hub** checkbox.

      Additional fields are displayed as shown in the figure below.

      Figure 493 *Additional fields specific to non-Cambium hub settings*

      Note

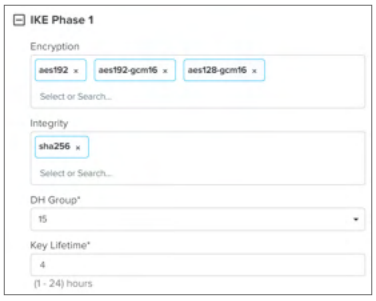
      The **Address** and **PSK** fields are auto-populated.

      PSK, a 12-character key, is auto-generated by cnMaestro for Cambium hubs only. This key is used as the local PSK and remote PSK for all the sites in the Auto VPN group.

   d. In the **Remote ID** field, enter an appropriate value. This is a mandatory parameter. The remote ID is the local ID of the non-cambium hub device. On creation of a hub or spoke, the local ID (generated sequentially) is assigned as local ID.
   e. Expand the **IKE Phase 1** panel.

      The default configuration is displayed, as shown in Figure 494.

      Figure 494 *Default configuration of the IKE Phase 1*

   f. Using the **IKE Phase 1** panel, complete the following steps:
      i. In the **Encryption** field, select the required encryption method. By default, **aes192**, **aes192-gcm16**, **aes128-gcm16** are selected.
      ii. In the **Integrity** field, select the required integrity method. By default, **sha256** is selected.

iii. In the **DH Group** field, select the required DH group option. Default value: 15.

iv. In the **Key Lifetime** field, enter a value. Default value: 4.

g. Similarly, expand the **IKE Phase 2** panel and set the configuration.

The default configuration is shown in Figure 495.

Figure 495 *Default configuration of the IKE Phase 2*



5. Click **Add**.

The Auto VPN group is created for a non-Cambium hub.

Adding hubs and spokes for sites

You must add hubs and spokes as part of the Auto VPN configuration. A site has to be linked at the time of creating a hub or a spoke. You must select a site from the list of sites and this site must have met the following criteria:

- The site should have an NSE device.
- An NSE group should be mapped to the NSE device.
- The site should not be part of any other Auto VPN group.

Note

- You must first add a hub before adding a spoke.
- You can add multiple hubs and spokes for all Cambium-hub Auto VPN groups.
- You can add multiple spokes for a non-Cambium hub Auto VPN groups.
- You can add only spokes for a non-Cambium hub Auto VPN group. Hubs cannot be added but their configuration can be updated.

This topic covers the following sections:

- Adding a hub and a spoke for a Cambium-hub Auto VPN group
- Adding a spoke for a non-Cambium hub Auto VPN group

Adding a hub and a spoke for a Cambium-hub Auto VPN group

You can add a single or multiple hubs and spokes for a Cambium-hub Auto VPN group.

Adding a hub

Complete the following steps to add a hub:

1. On the **NSE Profiles** page, click the **Auto VPNs** tab.

   The Auto VPNs page appears with a list of auto VPN groups created.

   Figure 496 *The Auto VPNs page*

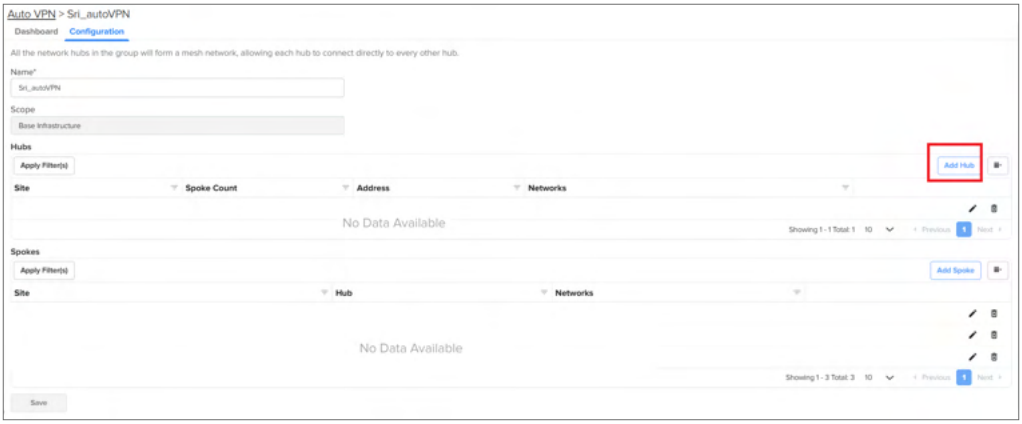


   If the value of **Non-Cambium** field on the Auto VPN page is No, then it is a Cambium-hub Auto VPN group. Otherwise, it is a non-Cambium hub Auto VPN group (if the value of Non-Cambium is Yes).

2. Click on the required Cambium-hub Auto VPN group name.

   The **Configuration** page appears for the selected auto VPN group.

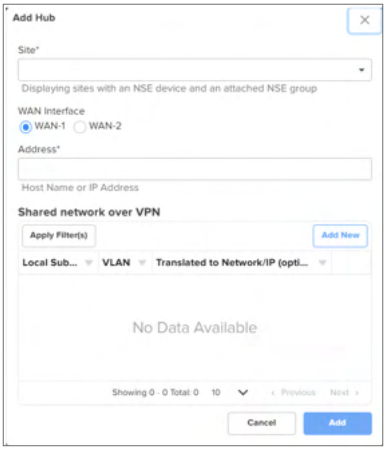
   Figure 497 *The Configuration page*



3. Click **Add Hub**.

   The **Add Hub** window appears.

   Figure 498 *The Add Hub window*



4. To add a hub, provide the values as described:

a. From the **Site** dropdown list, select a site name. This is a mandatory field.

   The Site dropdown list displays sites that have an NSE device and an attached NSE group.

b. In the **WAN Interface** field, select the required WAN option.

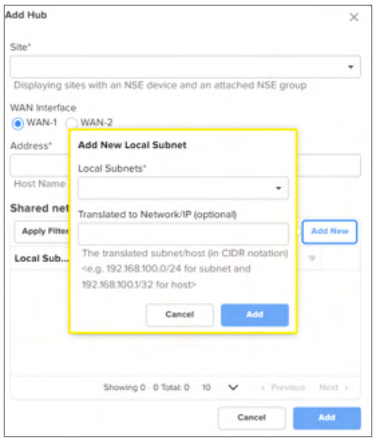
c. In the **Address** field, enter the host name or the WAN IP address of the NSE device. This is a mandatory field.

   This field auto-populates the value with the configured WAN IPs if the static IPs are configured.

d. In the **Shared network over VPN** section, Click **Add New** to add VLAN IDs of required networks.

   The **Add New Local Subnet** window appears. Using this window, you can add networks that the hub will advertise. You can add multiple networks.

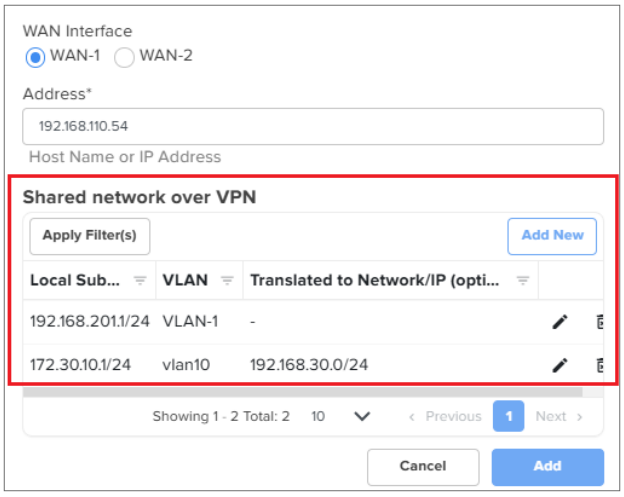
Figure 499 *The Add New Local Subnet window*



e. In the Add New Local Subnet window, enter a valid address in the **Local Subnets** field. The **Translated to Network/IP (optional)** field is optional. If the Local subnets have a VPN translation, then provide a VPN network address in the **Translated to Network/IP (optional)** field or it can be left blank (empty).

f. Click **Add** on the Add New Local Subnet window.

   The shared network details are added to the **Add Hub** window.



The NSE device communicates over the specified VLAN.

Note

NSE supports VPN translation. The local subnets that are advertised to peers are configured to translate into a different, equally sized subnet. This is useful in deployments where the same local subnet is used in multiple locations.

For example, the 192.168.200.0/24 network can be found in multiple locations as it is the default network configuration. If 192.168.200.0/24 is available in multiple locations, this can be configured to be translated to 10.10.10.0/24. to prevent address conflicts, The translation can also be 1 to M. In case of 1 to M, 192.168.200.0/24 can be configured to be translated to 10.10.10.10/32.

g. Click **Add** on the Add Hub window.

A hub is added to the **Hubs** section on the **Configuration** page.

Figure 500 *The Hubs section*



Adding a spoke

Complete the following steps to add a spoke:

1. On the **NSE Profiles** page, click the **Auto VPN** tab.

   The Auto VPN page appears with a list of auto VPN group created.

2. Click on the required auto VPN group name.

   The **Configuration** page appears for the selected auto VPN group.

   Figure 501 *The Configuration page - Add Spoke*



3. Click **Add Spoke**.

   The **Add Spoke** window appears.

Figure 502 *The Add Spoke window*

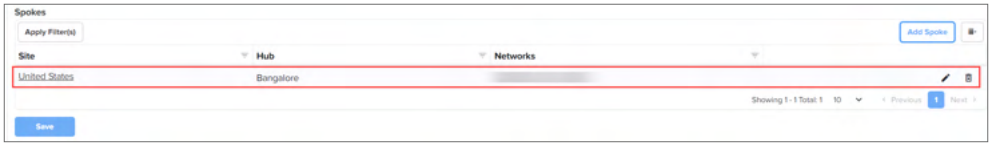


4. Complete the following steps to add a spoke:
   a. Select a site from the **Site** dropdown list. This is a mandatory field.
   b. Select a hub from the **Hub** dropdown list. This is a mandatory field. You must select a hub to connect from the list of hubs, which are already created in the Auto VPN group.
   c. In the **Shared network over VPN** section, Click **Add New**. The **Add New Local Subnet** window appears.

      Using this window, you can add networks that are local to the spoke. You can add multiple networks. If there are multiple hubs, these networks will be advertised by the hub they are connected to.
   d. In the **Add New Local Subnet** window, enter a valid address in the **Local Subnets** field. The **Translated to Network/IP (optional)** field is optional. If the Local subnets have a VPN translation, then provide a VPN network address in the **Translated to Network/IP (optional)** field or it can be left blank (empty).
   e. Click **Add** on the Add New Local Subnet window. The shared network details are added to the **Add Spoke** window. The NSE device communicates over the specified VLAN.
   f. Click **Add** on the Add Spoke window.

      A spoke is added to the **Spokes** section.

      Figure 503 *The Spokes section*

5. Click **Save** on the Configuration page.

   The figure below is an example of the **Configuration** page for a Cambium-hub Auto VPN group (after adding a hub and a spoke). You can add multiple hubs and spokes for a Cambium-hub Auto VPN group.

Figure 504 *The Configuration page for a Cambium-hub Auto VPN group*



6. Click **Save** on the Configuration page to apply the changes.
7. To view the dashboard page for the configured Auto VPN group, click on the **Dashboard** tab (located before the **Configuration** tab).

   You can view the status of connection and tunnel type used by the NSE device for communication.

   Figure 505 *The Dashboard page of an Auto VPN group*



8. On the **Dashboard** page, click on the ⓘ icon (next to **Tx Range**) to view the network details.

   Figure 506 *The Networks page*



Adding a spoke for a non-Cambium hub Auto VPN group

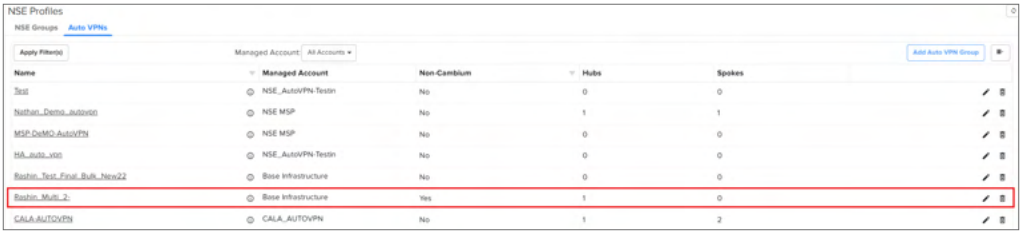
You can add a single or multiple spokes for a non-Cambium hub Auto VPN group. You cannot add a hub but you can update or modify its configuration for a non-Cambium hub Auto VPN group.

Complete the following steps to add a spoke:

1. On the **NSE Profiles** > **Auto VPNs** page, select a non-Cambium hub Auto VPN group from the available list.

   If the value of **Non-Cambium** field on the Auto VPNs page is Yes, then it is a non-Cambium hub Auto VPN group.

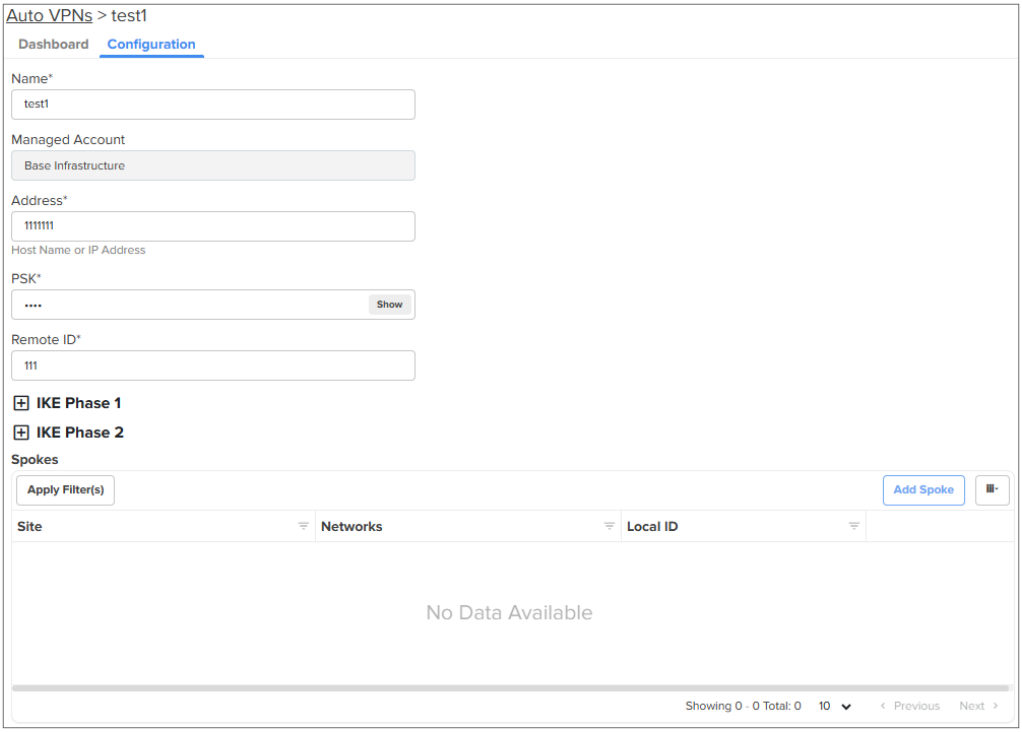
Figure 507 *The Auto VPNs page - Non-Cambium hub*



2. Click on the required non-Cambium hub Auto VPN group name.

   The **Configuration** page appears for the selected auto VPN group.

Figure 508 *The Configuration page - Non-Cambium hub*



   The following parameters are already set at the time of creating a non-Cambium hub Auto VPN group:

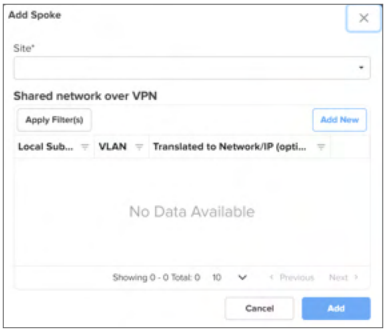
   - Name
   - Managed Account
   - Address
   - PSK
   - Remote ID
   - IKE Phase 1 and IKE Phase 2

   You can update or modify the hub-specific parameters except for Managed Account (disabled). For more information about these parameters, check Auto VPN group for a non-Cambium hub.

3. To add a spoke for a non-Cambium hub Auto VPN group, click **Add Spoke** on the Configuration page.

   The **Add Spoke** window appears.

Figure 509 *The Add Spoke window - Non-Cambium hub*



4. Complete the following steps to add a spoke:
   a. Select a site from the **Site** dropdown list. This is a mandatory field.
   b. In the **Shared network over VPN** section, Click **Add New**. The **Add New Local Subnet** window appears.

      Using this window, you can add networks that are local to the spoke. You can add multiple networks. These networks will be advertised by the hub they are connected to.

      Note

      NSE supports VPN translation. For more information, check the note described here.

   c. In the **Add New Local Subnet** window, enter a valid address in the **Local Subnets** field. The **Translated to Network/IP (optional)** field is optional. If the Local subnets have a VPN translation, then provide a VPN network address in the **Translated to Network/IP (optional)** field or it can be left blank (empty).
   d. Click **Add** on the Add New Local Subnet window. The shared network details are added to the **Add Spoke** window. The NSE device communicates over the specified VLAN.
   e. Click **Add** on the Add Spoke window.

      A spoke is added to the **Spokes** section.
5. Click **Save** on the Configuration page to apply the changes.
6. To view the dashboard page for the configured Auto VPN group, click on the **Dashboard** tab (located before the **Configuration** tab).

   On the **Dashboard** page, you can use the ⓘ icon (next to **Tx Range**) to view the network details.

Disabling or Enabling the Security Plus License Mode for NSE

Currently, a subscription is required to onboard and manage NSE using cnMaestro (both Essentials and X). This paid subscription license mode (with all features available) is referred to as **Security Plus**.

However, Cambium Networks also offers a flexibility to onboard and manage NSE devices using cnMaestro **without a subscription**. This subscription-free license mode is referred to as **Security**. The Security mode allows you to onboard and operate an NSE device with limited features.

Note

The Security Plus license mode is available for both cnMaestro Essentials and X. But the **Security** mode is available only for cnMaestro Essentials.

The table below lists some of the features available in the Security Plus license mode and the Security mode.

Table 107 *List of feature sets available for NSE in different license modes*

Feature sets available in the Security Plus license mode (Paid subscription)	Feature sets available in the Security mode (Subscription-free)

• Geo-IP Firewall
• DNS Content Filtering
  ◦ 80+ categories
  ◦ Fast with data caches around the world
• LAN Vulnerability Assessment
• High Availability
  ◦ 1 + 1 in Active-Backup mode
• Auto VPN
  ◦ One-click setup of VPN tunnels
• IoT Device Identification
• cnMaestro reports and analytics for DNS filtering, Geo-IP, LAN Vulnerability Assessment, and Device Identification
	• SD-WAN
	  ◦ WAN Active-Active and Active-Backup
	  ◦ Layer-3 and Layer-7 flow preferences
	• Site to Site VPNs
	  ◦ IKEv1
	  ◦ IKEv2
	• Remote VPN
	  ◦ L2TP-IPSec
	  ◦ IKEv2
	  ◦ WireGuard
	• Next-Gen Firewall
	  ◦ Layer-3 and Layer-7 (Application based)
	• Intrusion Detection and Prevention
	  ◦ Choice of free and commercial rule sets
	• Application Visibility and Control
	• LAN services (DHCP, DNS (Local Hosts), RADIUS)
	• cnMaestro Analytics (Dashboard, WAN performance, Client and VPN session, Application statistics, Threats, CPU, Available memory, Alarms, Alarms History, Events)

With the introduction of the new feature sets, the following three different account states are observed for NSE in cnMaestro:

1. **cnMaestro Essentials with Security**: Free subscriptions (1000 free slots) are granted for NSE devices.
2. **cnMaestro Essentials with Security Plus**: Users must activate Tier 30 licenses for NSE3000 devices and Tier 31 licenses for NSE4000 devices.
3. **cnMaestro X with Security Plus**: Users must activate Tier 30 licenses for NSE3000 devices and Tier 31 licenses for NSE4000 devices.

How does the Security Plus license mode work?

By default, the Security Plus license mode is enabled for NSE and all the features are available for existing and new user accounts. In this default license state, all the security features, such as Geo-IP firewall, DNS content filtering, high availability, LAN vulnerability assessment, device identification, device fingerprinting, and cnMaestro reports are enabled.

Using cnMaestro Essentials, you can disable the Security Plus mode and switch to the Security mode (subscription-free). You can also switch back (enable) to the Security Plus mode. For details, refer to Disabling the Security Plus mode and Enabling the Security Plus mode.

How does the Security (subscription-free) mode work?

The subscription model for NSE devices remains unchanged but cnMaestro grants a free subscription if the user chooses to use only the Security mode in cnMaestro Essentials.

To switch to the Security mode, an account-level setting is required in the cnMaestro UI. When you select between Security and Security Plus modes, cnMaestro verifies before changing the mode and throws an error if any of the criteria fails.

On changing to the Security mode, cnMaestro activates 1000 (configurable) Tier 30 free slots with a rotating validity period (after which cnMaestro resets to a future date before a slot reaches its expiry). These free slots cannot be transferred to X unlike the regular Tier 30 slots.

When the Security mode is enabled, cnMaestro automatically disables all features that are supported in the Security Plus mode. For information on how to enable the Security mode, refer to Disabling the Security Plus mode.



Note

If an account running in the Security mode (earlier) is upgraded to X, then cnMaestro automatically toggles it to the Security Plus mode.

How to switch back to Security Plus mode?

To switch back to (enable) the Security Plus mode, an account-level setting is required in the cnMaestro UI. However, the users must have activated sufficient number of Tier 30 and 31 licenses to meet their NSE device count (as a prerequisite task). On changing to the Security Plus mode, cnMaestro deactivates the grant (free subscription) and all features are available in this mode (by default). For information on how to switch back to the Security Plus mode in cnMaestro, refer to Enabling the Security Plus mode.



Note

Fresh accounts are initialized with Essentials and Security Plus. That is, the user must activate Tier 30 and Tier 31 licenses to manage the NSE3000 and NSE4000 devices respectively.

How do license modes work during a manual or automatic downgrade from X?

Automatic downgrade happens when all activated subscriptions (licenses) expire for the X account.

When automatically downgraded from X, the Security Plus mode is continued in Essentials and any devices without valid licenses are marked as expired. If you want to use the Security license mode, you must disable the Security Plus mode using the **Administration** > **Settings** > **General** page in cnMaestro UI. For details, refer to Disabling the Security Plus mode.



Note

Switching to Security mode will automatically reactivate the expired devices.

A manual downgrade from X is possible under the following three conditions for NSE:

- If all required Tier 30 and/or Tier 31 subscriptions are available, then the Security Plus mode can be continued in Essentials.
- If partial Tier 30 and/or Tier 31 subscriptions are available, then cnMaestro continues in the Security Plus mode and devices without valid Tier 30 or and Tier 31 licenses are marked as expired.
- If no Tier 30 and/or Tier 31 subscriptions are available, then cnMaestro follows the automatic downgrade path.

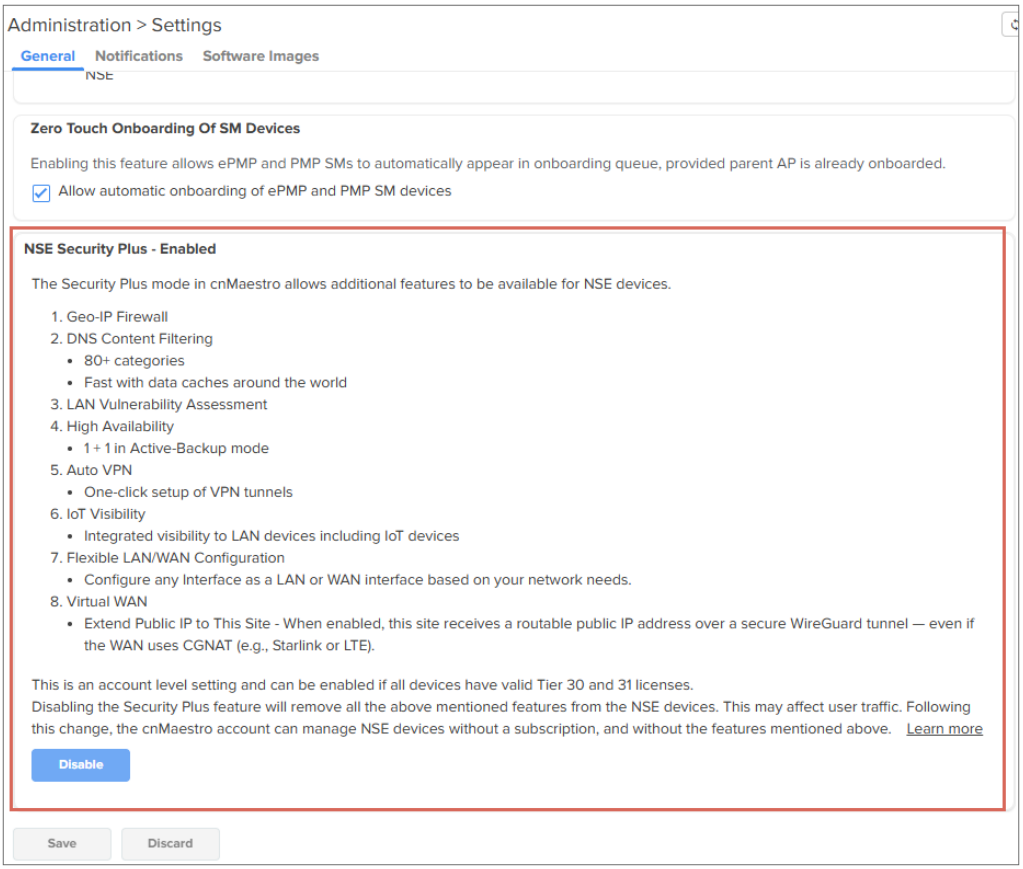
Disabling the Security Plus mode

When you disable the Security Plus mode for NSE using cnMaestro Essentials, the Security mode (subscription-free) is enabled. Complete the following steps to disable the Security Plus mode:

1. Log in to cnMaestro Essentials using appropriate username and password.
2. From the home page, navigate to **Administration** > **Settings**. The **Settings** page appears with the following tabs: General, Notifications, and Software Images. By default, the **General** tab is selected.

   The General page displays Time zone, Account view, Zero Touch Onboarding, and NSE Security Plus settings (default state).
3. On the **General** page, go to the **NSE Security Plus** section.

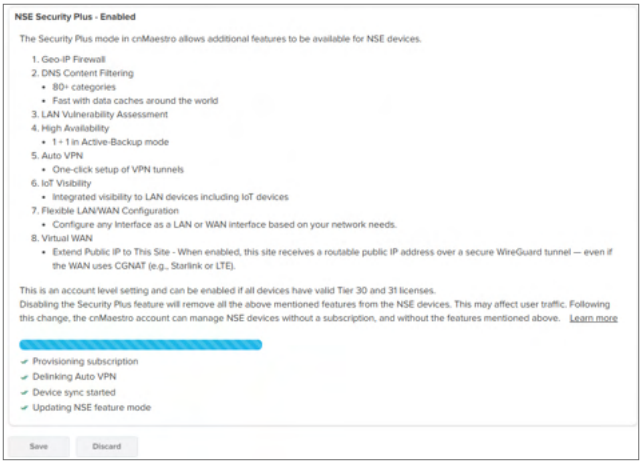
   Figure 510 *NSE Security Plus section*



   By default, the Security Plus mode is enabled for the NSE devices. In the NSE Security Plus section (as shown in Figure 1), you can view the details of features enabled.
4. To disable the Security Plus mode, click **Disable**.

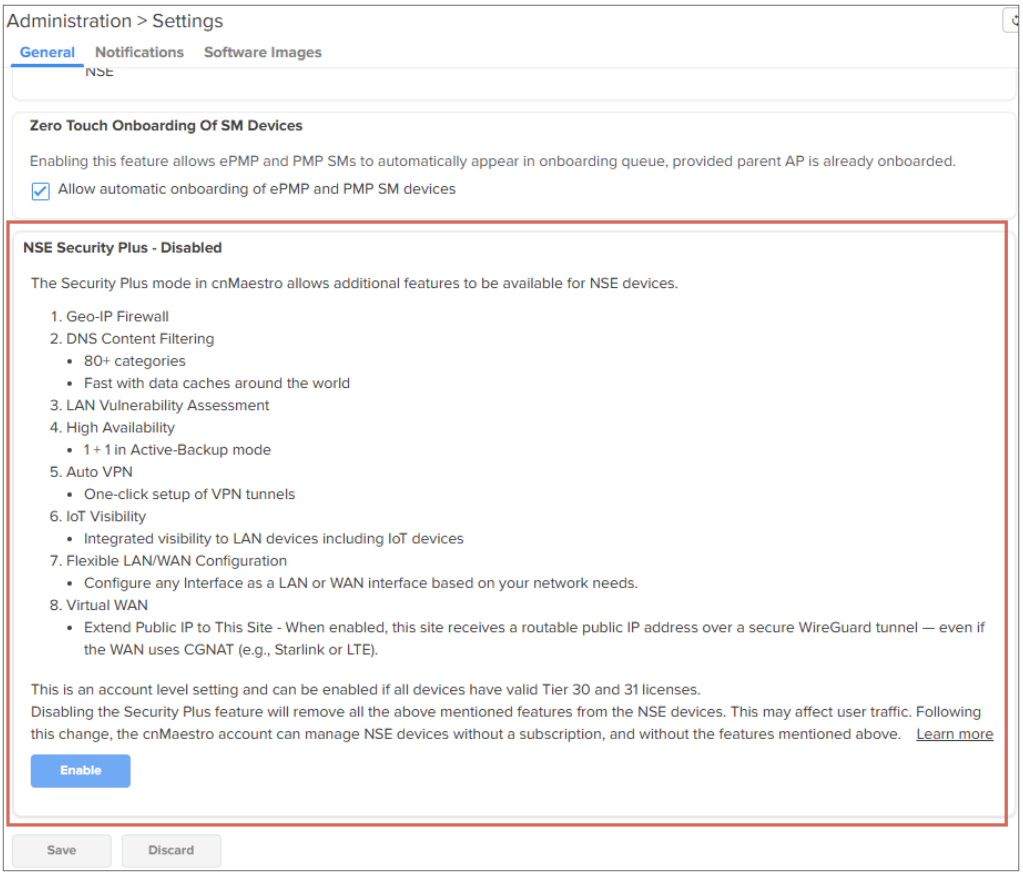
   The process begins, indicating the subscription provisioning and device sync as shown in Figure 2.

Figure 511 *Process of disabling the Security Plus mode*



The **Security** license mode is enabled now. You can proceed with configuration of the related features on the **NSE Groups** page. For example, WAN and LAN services. Check Table 107 for the list of feature sets available in the Security mode (subscription-free).

Figure 512 *NSE Security Plus mode disabled*

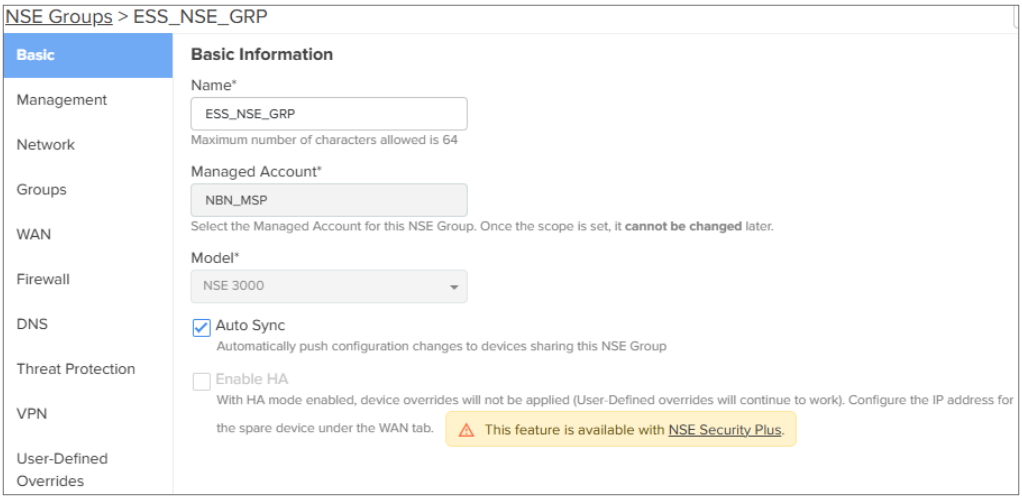


When the Security mode is enabled, the unsupported features are disabled in the cnMaestro UI. Feature-level messages are displayed on the UI as part of the configuration for the NSE device.

Based on the account level mode selection, the cnMaestro UI turns off (disable) and turns on (enable) the related features. For example, if you select the **Basic** tab on the NSE Groups page, a feature level message is

visible, indicating that the high availability (HA) configuration is available only with the Security Plus mode. In addition, the HA configuration checkbox is disabled and provides an option (link) to enable the Security Plus mode (as shown in Figure 3).

Figure 513 *Example of a feature-level message*

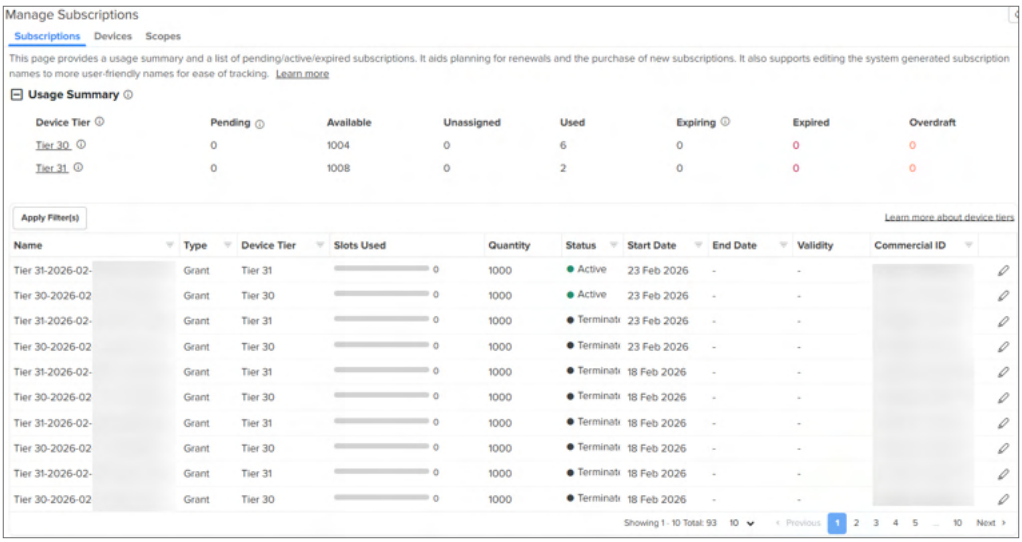


Similarly, you can find such feature-level messages for specific configurations on **Firewall** and **DNS** pages for the Security mode. In addition, Vulnerabilities is not available at all levels, and Auto VPN, GEO IP Firewall, and DNS Content Filtering are also unavailable.

5. Configure the required features available in the Security mode.

   cnMaestro grants 1000 free slots, which you can use to onboard and manage the NSE devices. To view the summary of grant, check the **Manage Subscriptions** page. Figure 4 is an example of a grant summary, showing that one slot is used, and 1099 free slots are available for NSE devices. These free slots can be used to onboard and manage the NSE devices in cnMaestro.

Figure 514 *Viewing the grant summary on the Manage Subscriptions page*



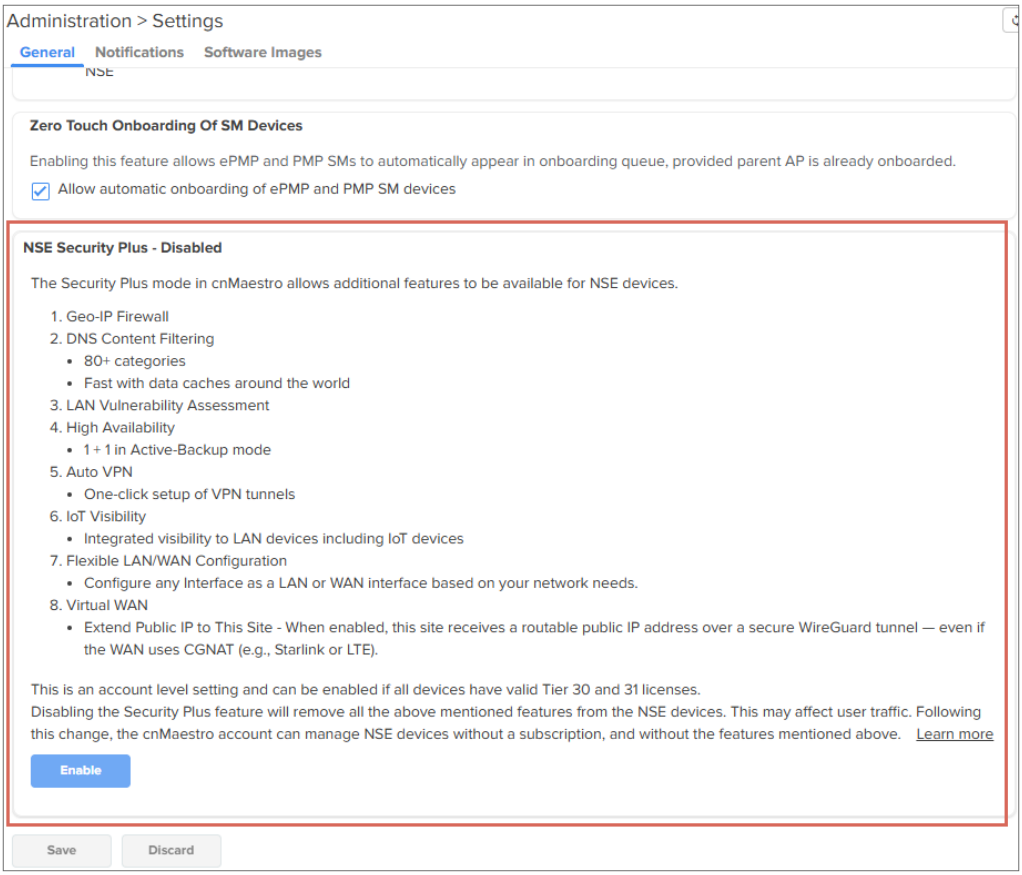
Enabling the Security Plus mode

You have an option to enable or switch back to the Security Plus mode in cnMaestro. With this action, the Security mode is disabled and all features (available in the Security Plus mode) are enabled automatically.

To switch back to or enable the Security Plus mode, complete the following steps:

1. From the home page of cnMaestro Essentials, navigate to **Administration** > **Settings**. By default, the General tab is selected.
2. On the **General** page, go to the NSE Security Plus section.

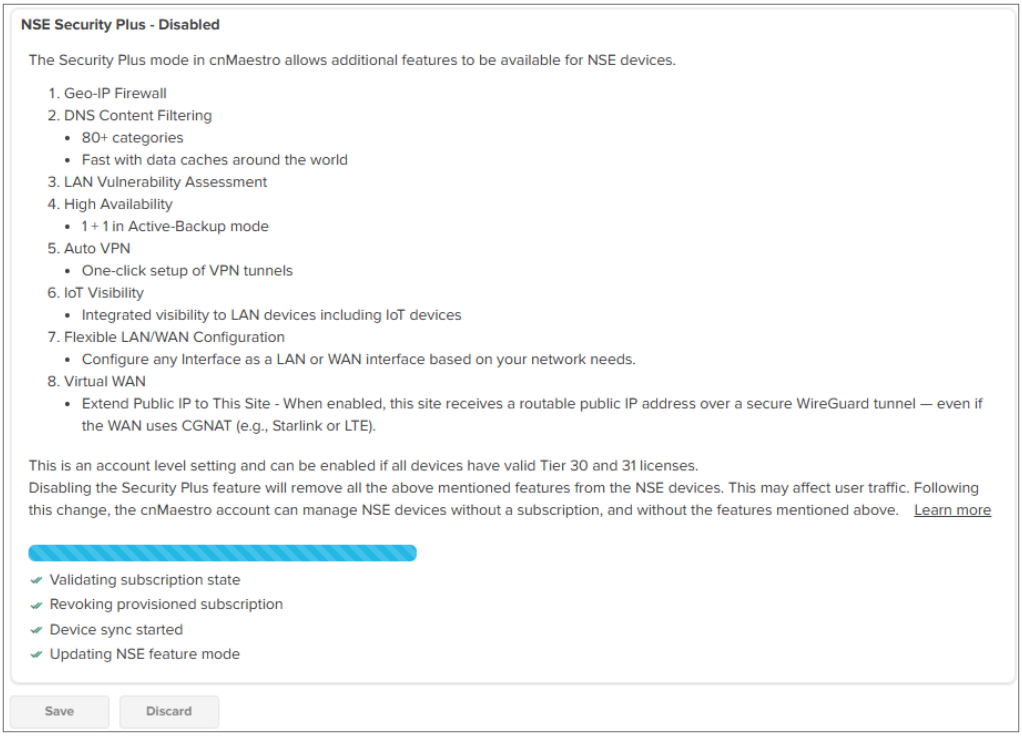
   Figure 515 *The NSE Security Plus section with the Enable button*



3. To enable the Security Plus mode, click **Enable** in the NSE Security Plus section.

   The process of enabling the Security Plus mode begins, as shown in Figure 6.

Figure 516 *Enabling the Security Plus mode - cnMaestro Essentials*

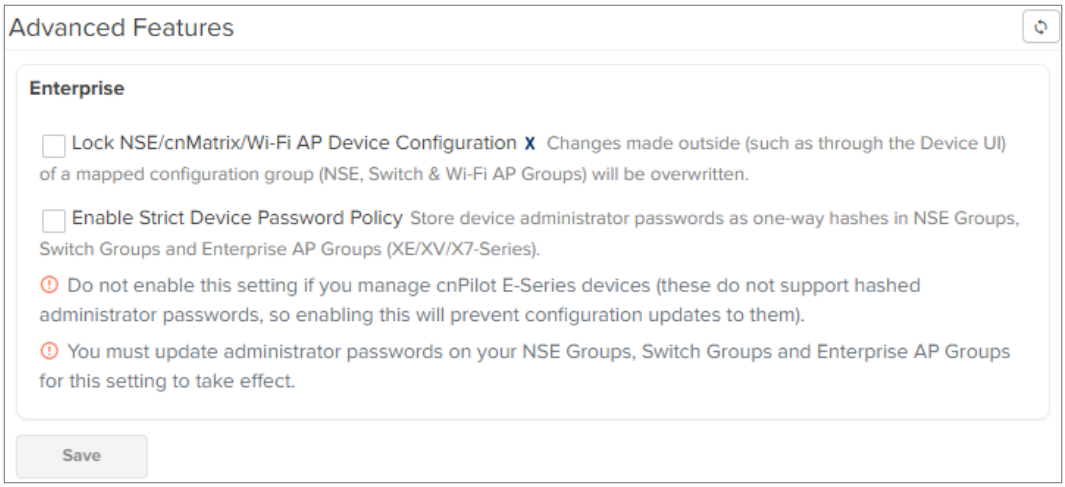


4. Click **Save** to apply the change when the process is complete.

   You have now enabled the Security Plus mode for the NSE devices. With this action, all features, such as high availability, firewall settings, vulnerabilities, and Auto VPN, are enabled in the cnMaestro UI.

Configuring Advanced Features

To configure advanced features, navigate to **Configuration > Advanced Features** page.



Lock Device Configuration

To lock NSE, cnMatrix, and Wi-Fi device configuration, select the checkbox. Once you enable this checkbox, you cannot update the device-level configuration using the device UI or any other method. Only the configuration pushed from cnMaestro for NSE, switch, and Wi-Fi AP groups will be retained on the device.

Strict Device Password Policy

To enable strict password policy for Switch Groups or Enterprise AP Groups, select the **Enable Strict Device Password Policy** checkbox.

If you enable this option:

- The device administrator passwords are stored as one-way hashes for all NSE Groups, Switch Groups, and Enterprise AP Groups (XE/XV/X7-series).
- The administrator password has to be updated for all NSE Groups, Switch Groups, and Enterprise AP Groups under **Configuration > NSE Group > Management** page, **Configuration > Switch 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 1.3 for NSE, 4.6.1 for cnMatrix, and 6.5.3 for Enterprise Wi-Fi XE/XV/X7-Series to support the strict password policy. cnMaestro will not push any configuration to devices not meeting these requirements, including all cnPilot E-Series devices when the strict policy is enabled.

If you disable this option:

- The password must be updated for all NSE Groups, Switch Groups, and Enterprise AP Groups under the respective **Management** pages for this setting to take effect.

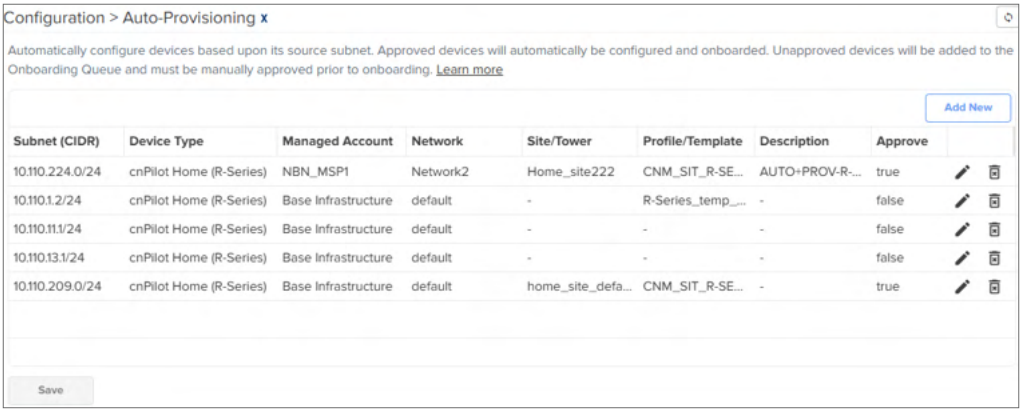
Auto-Provisioning

cnMaestro supports Auto-Provisioning for cnVision, Wireless LAN devices (Enterprise Wi-Fi, cnPilot R-Series, and Xirrus) and fixed devices (PMP and ePMP). It allows the user to automatically configure and approve devices based upon IP address.

Creating Auto-Provisioning Rule

To create a rule for Auto-Provisioning, perform the following steps:

1. Navigate to **Configuration** > **Auto-Provisioning** page.



2. Click **Add New** and following window appears.

Figure 517 *Auto-Provisioning for cnPilot Home (R-Series) devices*

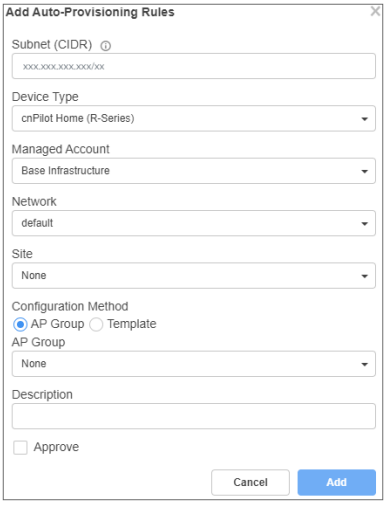
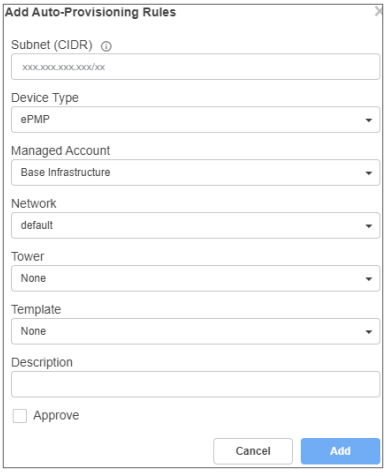


Figure 518 *Auto-Provisioning for all other devices*



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**.

Managing Home Mesh Router

The Home Mesh Router is engineered to provide superior Wi-Fi performance and mesh networking capabilities. It incorporates the advanced 802.11ax technology, ensuring it is fully compatible with a wide range of consumer devices while offering low latency and high throughput. These routers are specifically designed for comprehensive home coverage, supporting simultaneous operation on both 2.4 GHz and 5 GHz bands. This enables extended range, enhanced efficiency, and reduced interference compared to previous generations of Wi-Fi technology. Additionally, the routers are configured to work in tandem, creating a seamless mesh network that covers the entire home, effectively eliminating areas with weak or no Wi-Fi signal.

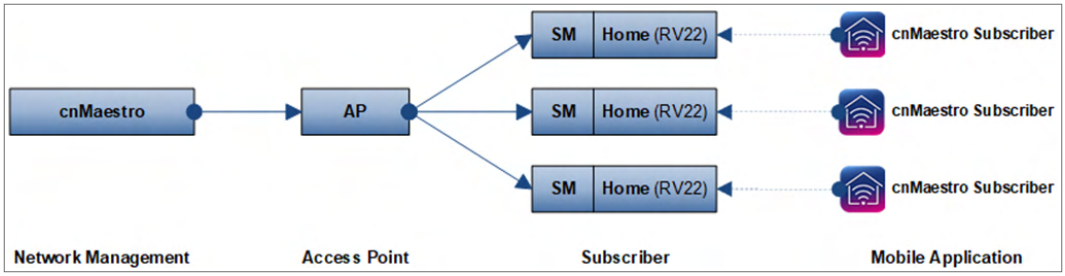
The Home Mesh Routers can be configured using cnMaestro Cloud and the cnMaestro Subscriber application.

For information on supported platforms and hardware overview, see *Home Mesh Router User Guide*.

Warning

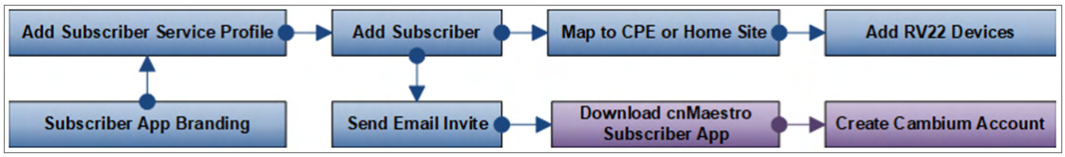
The WAN port of the Home Mesh Router may be damaged if a 48 VDC passive power (passive POE) is connected to the WAN port.

The basic architecture of the Home Mesh Router is as shown below.



The cnMaestro Subscriber application allows home customers to manage RV22 devices using their mobile phones. In the graphic above, the Subscriber is demarcated by the SM CPE. Alternatively, it could be mapped to a PON ONU, or to no explicit backhaul at all. In the latter case, the Subscriber would be attached to a new cnMaestro Home Site.

The workflow for creating and onboarding Subscribers, so customers can use the mobile application, has a cnMaestro (blue) and a customer (purple) component, as shown below.



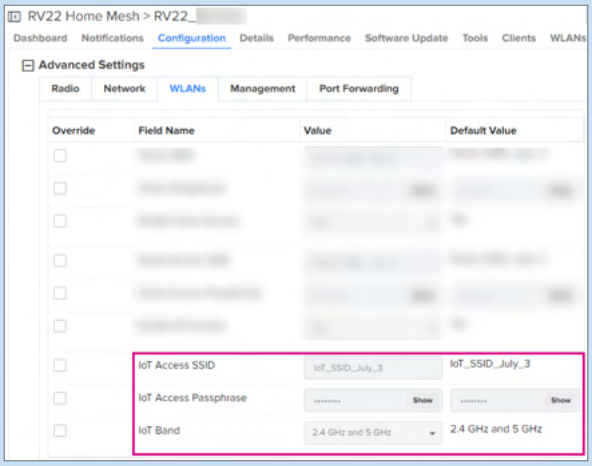
A Subscriber is configured in cnMaestro Cloud, and an invite is sent to the customer's email address, which will enable home Wi-Fi management using the mobile application. The customer must download the cnMaestro Subscriber application from the Apple App store or Google Play Store. The "Site" in the application, which maps to the Subscriber, can be customized and branded.

Feature	Details
Onboarding	Supported using Cambium ID or Serial Number (MSN).
Dashboard	Dashboards tailored for Home Site and RV22 Home Mesh.
Configuration	Available through RV22 Home Mesh AP Groups.
Details	Overview and network information display.
Notifications	Alarms, AP Events, and Wi-Fi Events aggregated at System, Managed Account, Network, Site, and Device levels.
Performance	WAN Throughput, Wireless Throughput (downlink/uplink), Clients by Band, Noise Floor, Interference, and Airtime (2.4/5 GHz) performance graphs.
Statistics	System, Managed Service, and Network statistics available.
Software Update	Software update provided at System, Managed Account, Network, Site, and Device levels.
Maps	Location of Home Sites and Devices.
Clients	Both Wired and Wireless Clients supported at Site and Device levels.
Tools	Status, Debug, Network Connectivity, Wi-Fi Analyzer, Speed Test, and Packet Capture tools available.
Reports	Data Reports downloaded from the System, Managed Service, Network, and Site levels.

Feature	Details
Port Forwarding	Allows external devices to access services hosted on internal network devices (for example, web servers and game servers) by routing traffic through the router to the configured internal IP and port. **Note** • The port forwarding rule can also be added by the subscribers through the cnMaestro Subscriber application. • In a mesh configuration, this rule is applied only to the Mesh Base router. • Port forwarding is available on RV22 Home Mesh Routers running version 1.2.0 or later. • A maximum of 16 port forwarding rules are supported.
IoT Access SSID	Dedicated third SSID for IoT devices, typically fixed-location devices, such as smart bulbs, thermostats, and TVs. It ensures stable connectivity and isolates IoT traffic from other network traffic. **Note** IoT access SSID is available on RV22 Home Mesh Routers running version 1.2.0 or later. This can be configured in one of the following places: • Under the **WLANs** page • Under the **AP Gropus** page, when adding a new WLAN under the **Basic** section. • Under device **Device** > **Configuration** tab > **Device Configuration** > **Advanced Settings** > **WLANs** tab. • Under **Subscribers** > **Service Configuration** > **Home Wi-Fi Devices Setting Override** section.

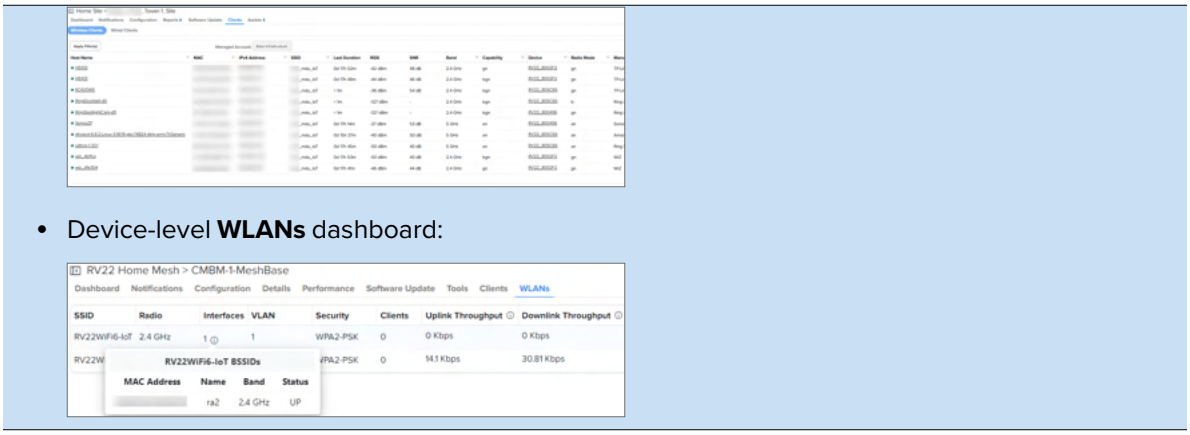
Note

If enabled and configured through the cnMaestro Subscriber application, the IoT SSID parameters are displayed under **Device > Configuration tab > Device Configuration > Advanced Settings > WLANs** tab in cnMaestro Cloud UI.



The IoT clients are displayed under the following pages:

- Device-level **Clients** dashboard:



- Device-level **WLANs** dashboard:

This topic contains the following sections:

- Configuring Home Mesh Router
- Viewing router system information and network traffic status
- Viewing, editing, and blocking connected clients
- Monitoring and troubleshooting the Home Mesh Router

Configuring Home Mesh Router

Before shipping the Home Mesh Routers to the subscribers, they must be configured with AP groups, Wi-Fi profiles, and associated with the corresponding subscriber.

Configuring the routers involves the following steps:

1. Configuring WLAN profiles (SSIDs)
2. Configuring AP Groups
3. Onboarding the Home Mesh Router to cnMaestro
   a. cnMaestro Subscriber application branding
   b. Adding a Subscriber Service Profile
   c. Adding a subscriber
   d. Claiming the Home Mesh Router

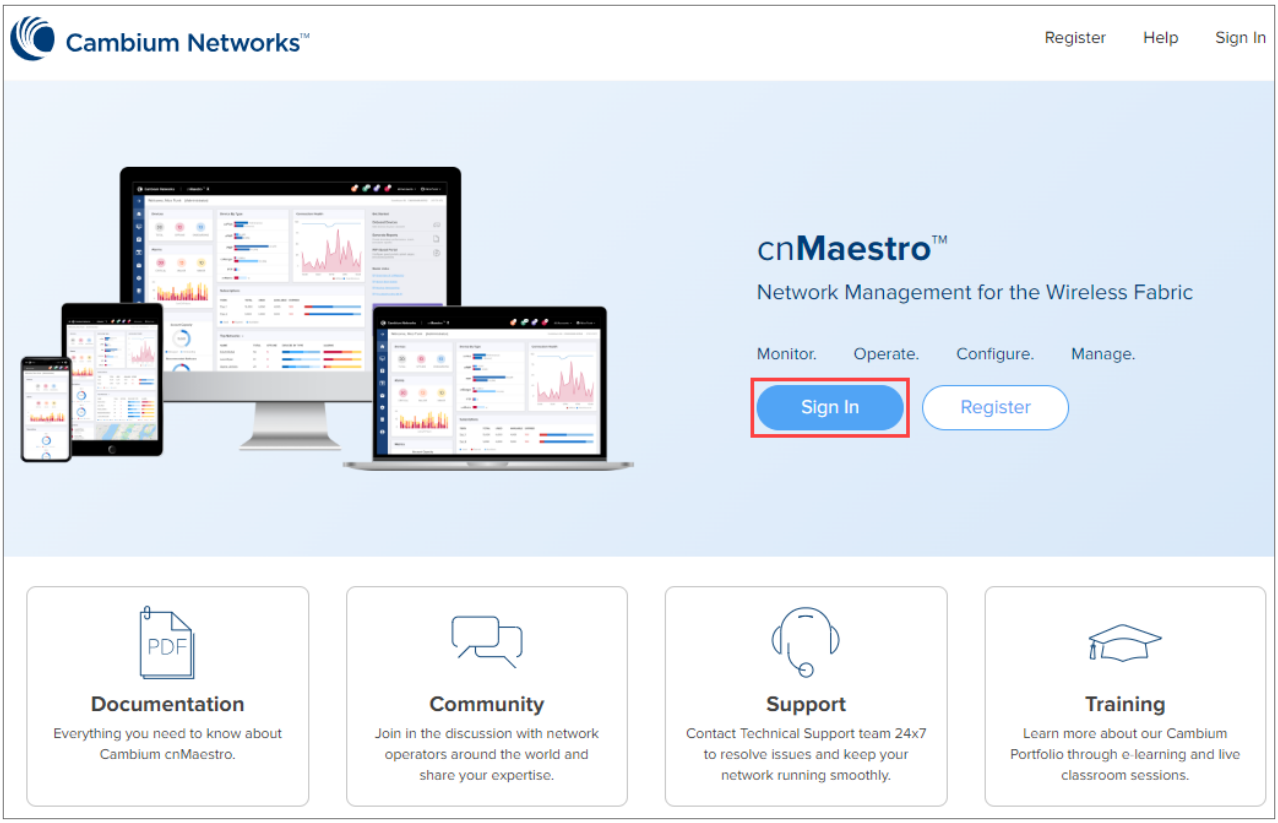
Configuring WLAN Profiles (SSIDs) for Home Mesh Routers

WLANs allow you to configure home and guest access SSIDs for the Home Mesh Router. This WLAN profile is associated with an AP group that contains configuration applied on the Home Mesh Routers. These SSIDs act as default SSIDs on all routers associated with the AP group.

To configure a WLAN profile, complete the following steps:

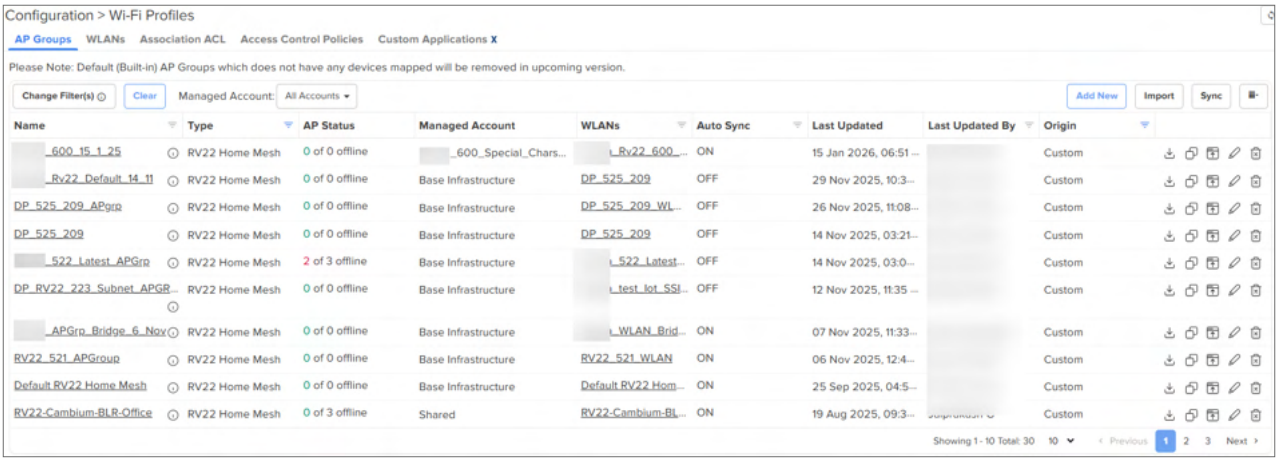
1. Sign in to cnMaestro.

   The home page appears.



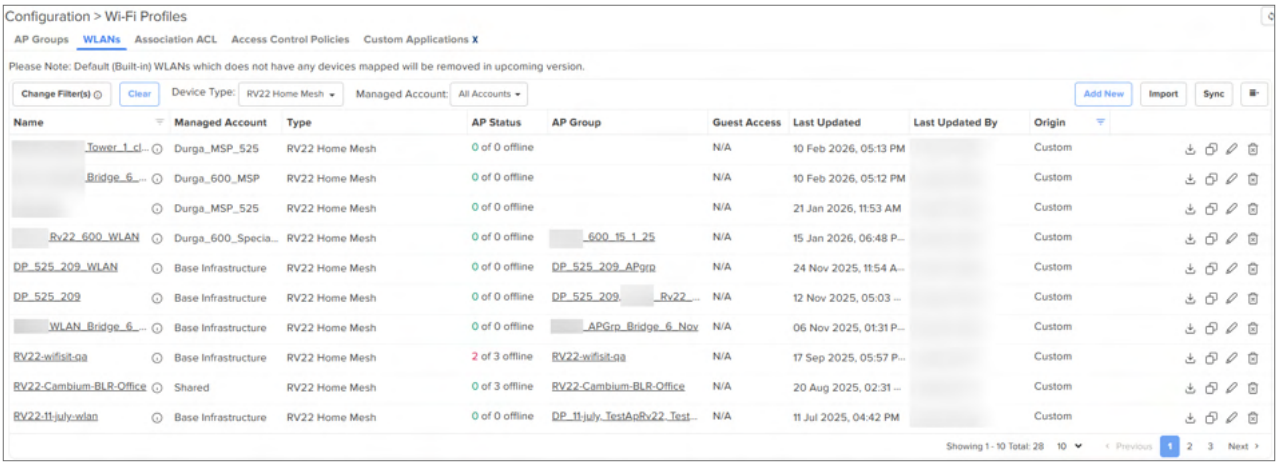
2. Navigate to **Configuration** > **Wi-Fi Profiles**.

   The **AP Groups** page under **Wi-Fi Profiles** appears, by default.



3. Click the **WLANs** tab.

   The **WLANs** page appears.



4. Click **Add**.

   The **WLANs** > **Add New** window appears.

   In the **WLANs** > **Add New** window, configure the WLAN parameters as described in Table 108.

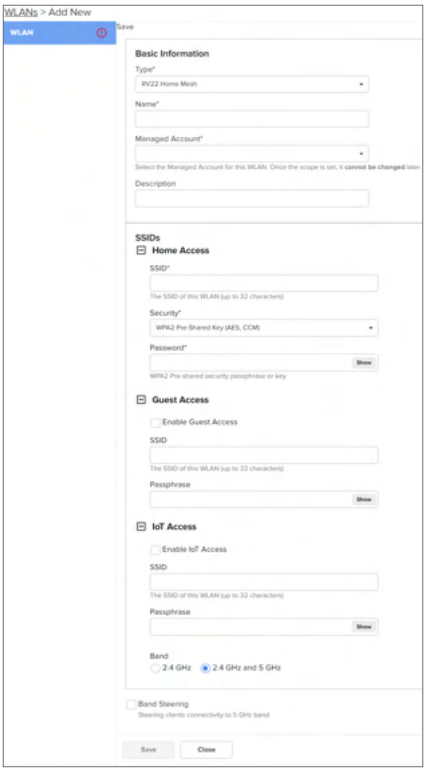


Table 108 *WLAN parameters*

Parameter	Description
Basic Information	
Type	Type of device for which the WLAN profile is configured. Select **RV22 Home Mesh** from the dropdown list.
Name	Name of the WLAN profile.
Managed	Specifies the availability of the WLAN profile across managed accounts.

Parameter	Description
Account	The following values are supported: • Base Infrastructure—The WLAN profile is available only for the global account. It is not shared with other managed accounts. • Managed Account—The WLAN profile is available only for that specific managed account.  **Note** Once the Managed Account is configured for a WLAN profile, it cannot be modified.
Description	Brief description for the WLAN profile.
SSIDs—Home Access Configure the default SSID for connecting devices wirelessly. Only one home SSID can be configured.	
SSID	Unique name of the SSID for this WLAN. Supports a maximum of 32 characters. You must either configure the default SSID or enter a customized SSID. The default SSID: `RV22_<last 6 digits of device MAC>`. For example, `RV22_123456`.
Security	Security method used for encryption. The following security methods are supported: • **Open** • **WPA Pre-Shared Key (AES, CCM)** • **WPA2 Pre-Shared Keys (AES, CCM)** • **WPA/WPA2 Pre-Shared Keys (TKIP, AES)** • **WPA Pre-Shared Key (TKIP, AES)** Default: **WPA2 Pre-Shared Keys (AES, CCM)**  **Note** If you select **Open**, you must disable 802.11r roaming under **AP Groups** > **Radio** configuration.
Password	Security passphrase or key used to connect to this SSID. You must either configure the default password or enter a customized password. Default password: `password`
SSIDs—Guest Access Configure the guest SSID to allow any guest devices to access the wireless network.	
Enable Guest Access	Determines whether the guest access is enabled. Select the checkbox to enable guest access.
SSID	Unique name of the guest SSID for this WLAN. Supports a maximum of 32 characters.

Parameter	Description
Passphrase	Security passphrase or key used to connect to this guest SSID.
IoT Access Configure a SSID specific to IoT devices. **Note** IoT access SSID is available on RV22 Home Mesh Routers running version 1.2.0 or later.	
Enable IoT Access	Determines whether the IoT device access is enabled. Select the checkbox to enable IoT device access.
SSID	Unique name of the IoT device SSID for this WLAN. Supports a maximum of 32 characters.
Passphrase	Security passphrase or key used to connect to this IoT Access SSID.
Band	The radio band in which the devices must connect with the AP. Following are the supported values: • 2.4 GHz • 2.4 GHz and 5 GHz
Band Steering	Determines whether the band steering is enabled for the wireless clients. When enabled, APs steer wireless clients to connect to the 5 GHz band.

5. Click **Save**.

Configuring AP Groups for Home Mesh Routers

AP groups apply the same configuration to multiple Home Mesh Routers. AP groups contain configuration, such as administrator password, event logging, radio settings, WAN mappings, and DNS mode.

The following are part of the AP group configuration for Home Mesh Routers:

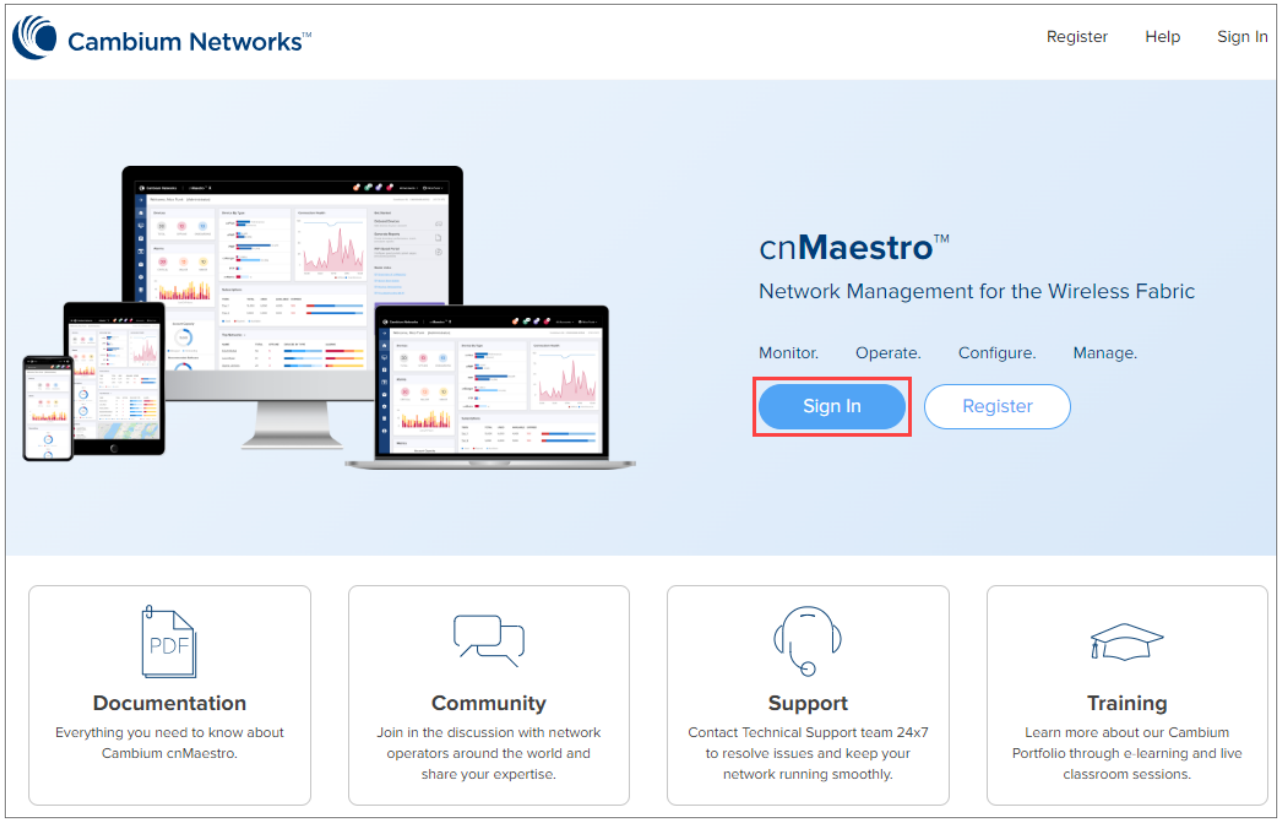
- **Basic**
- **Management**
  - Administrator Access
  - Time Settings
  - Event Logging
  - SNMP
- **Radio**
- **Network**
  - WAN Configuration
  - LAN Configuration
- **Security**

- DoS Protection
- Access Control List (ACL)

To configure an AP group, complete the following steps:

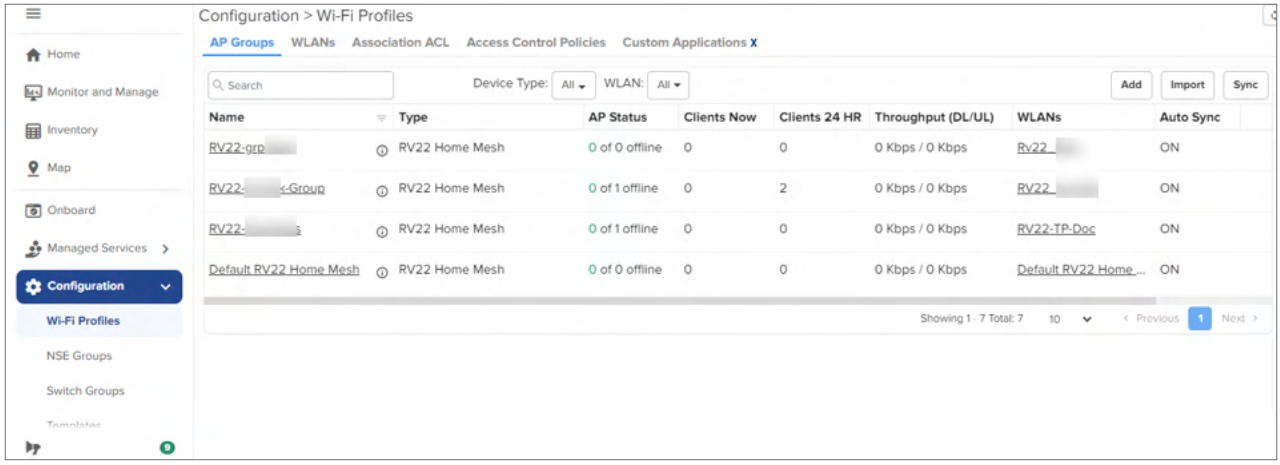
1. Sign in to cnMaestro.

   The home page appears.



2. Navigate to **Configuration** > **Wi-Fi Profiles**.

   The **AP Groups** page under **Wi-Fi Profiles** appears, by default.



3. Click **Add**.

   The **Add New** window appears with multiple tabs. By default, the **Basic** tab is selected.

4. In the **Add New** window > **Basic** tab, select **RV22 Home Mesh** in the **Type** dropdown list and configure the parameters described in Table 109.

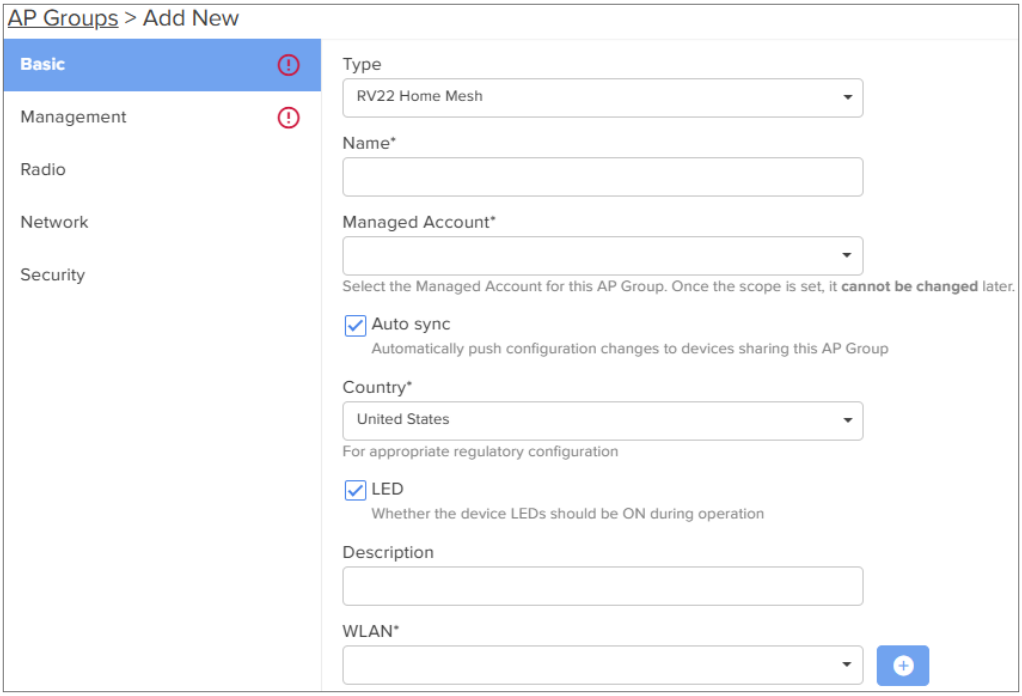


Table 109 *Basic parameters*

Parameter	Description
Type	Type of device for which the AP group is configured. Select **RV22 Home Mesh** from the dropdown list.
Name	Hostname of the device. Supports a maximum of 64 characters.
Managed Account	Specifies the availability of the AP group across managed accounts. The following values are supported: • Base Infrastructure—AP group is available only for the global account. It is not shared with other managed accounts. • Managed Account—AP group is available only for that specific managed account. **Note** Once the Managed Account is configured for an AP group, it cannot be modified.
Auto sync	Specifies whether configuration is applied to the router automatically after saving. Select the checkbox to enable auto sync of configuration.
Country	Country from where the device is operated. This parameter must be configured only by the administrator. The allowed operating channels and the respective transmit power levels depend on the country of operation. The list of countries supported depends on the SKU of the device

Parameter	Description
	(FCC and ROW). **Note** Radios remain disabled unless this parameter is configured.
LED	When enabled, turns on the device LEDs during operation.
Description	Brief description for the AP group.
WLAN	WLAN profile to be associated with this AP group. WLAN profile contains SSID details of the wireless network. Select the WLAN from the dropdown list. If no WLAN is configured, create one by clicking the add ( ) icon. For more information, See Configuring WLAN profiles (SSIDs).

5. Click the **Management** tab on the left pane and configure the parameters described in Table 110.

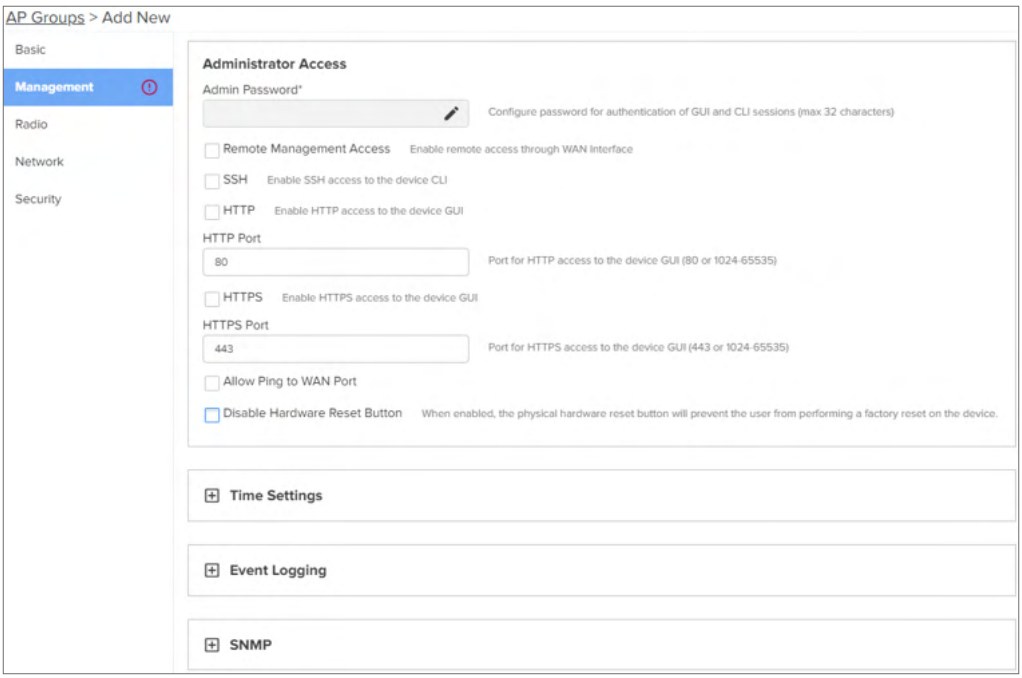


Table 110 *Management parameters*

Parameter	Description
Administrator Access	
Admin Password	Password required for authentication of the router.
Remote Management Access	Specifies whether remote management access to the device WAN interface is enabled or disabled.
SSH	Specifies whether access to the device CLI through SSH is enabled or disabled.
Disable Hardware Reset Button	Determines whether the reset button on the router is required to prevent a factory reset operation of the router.

Parameter	Description
	Select the checkbox to prevent the user from performing the factory reset operation.
Allow Ping to WAN Port	Enables or disables ICMP (ping) responses on the WAN interface.  **Note** This feature is available on RV22 Home Mesh Routers running version 1.2.0 or later.
Time Settings	
Time Zone	Time zone of the location where the router is installed. Select an appropriate time zone from the dropdown list.
NTP Server 1	Hostname or IPv4 address of the Network Time Protocol (NTP) server.
NTP Server 2	Hostname or IPv4 address of a second NTP server.
Event Logging	
Syslog Server	Hostname, IPv4, or IPv6 address of the Syslog server and the respective port number. Default port number: 514
Syslog Severity	The severity level of event that must be forwarded to the server. The supported severity levels (0-7) are based on RFC standards.
SNMP	
Enable	Determines whether SNMPv2c or SNMPv3 support on the router is enabled. Select the checkbox to enable SNMP support. By default, SNMP is disabled. **Note**: Remote access management is required for SNMP. Enable the **Remote Management Access** parameter under the **Administrator Access** section.
Trap Receiver IP	IPv4 address of the SNMP server to receive the SNMP traps. This parameter is applicable to both SNMP v2c and v3 versions.
Version	Specifies the SNMP version configured for the router. The following options are available: • v2c • v3
SNMPv2c-related parameters	
SNMPv2c RO community	The SNMP v2c read-only community string used as a password when obtaining information from the router.
SNMPv2c RW community	The SNMP v2c read-write community string used as a password when writing information to the router.
SNMPv3-related parameters	
SNMPv3 Username	Username for the SNMPv3 server. Supports a maximum of 32 characters.
Enable Authentication	Indicates whether authentication is enabled for SNMP communication. Select the checkbox to enable authentication.
Authentication	Specifies the authentication protocol.

Parameter	Description
Protocol	The following options are available: • MD5 • SHA **Note**: Cambium uses SHA-1 authentication protocol. By default, the **SHA** option is selected.
Authentication Password	Password used for authentication. Supports 8 to 32 characters.
Enable Encryption	Indicates whether encryption is enabled for SNMP communication. Select the checkbox to enable encryption.
Encryption Type	Specifies the encryption type. The following options are available: • AES • DES By default, the **AES** option is selected.
Encryption Password	Password used for encryption. Supports 8 to 32 characters.

6. Click the **Radio** tab on the left pane and configure the preferred radios (2.4 GHz or 5 GHz or both).

   By default, both the radios are enabled. You can disable only the 2.4 GHz radio.

   Configure the parameters (described in Table 111), which are similar across 2.4 and 5 GHz radios.

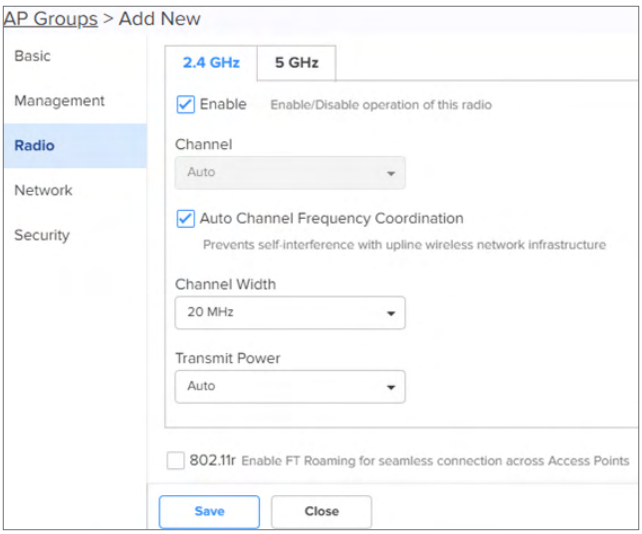
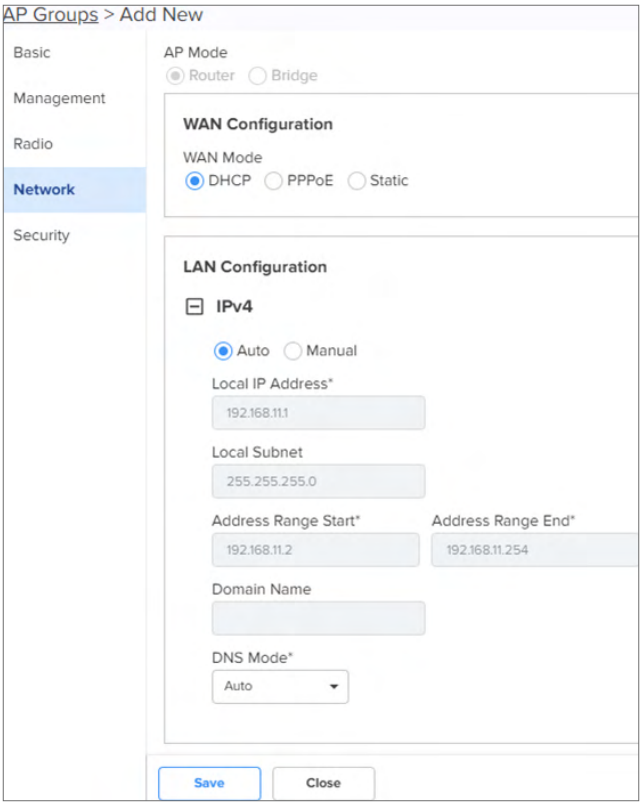


Table 111 *Radio parameters*

Parameter	Description
Enable	Enables the operation of radio.
Channel	This parameter cannot be modified.

Parameter	Description
	Specifies the 2.4 GHz channel that is used. Default: **Auto**
Auto Channel Frequency Coordination	Enable to prevent router from self-interference with upline wireless network infrastructure.
Channel Width	Operating channel width of the selected radio. Following channel widths are supported: • For 2.4 GHz—20 MHz and 40 MHz. Default: **20 MHz** • For 5 GHz—20 MHz, 40 MHz, 80 MHz, and 160 MHz. Default: **80 MHz**
Transmit Power	Transmit power of the router in percentage (%). The following options are available: • Auto • 20 • 40 • 60 • 80 • 100
802.11r	Enables the 802.11r Fast Transition (FT) mechanism for faster roaming between Home Mesh routers in a network. **Note** Disable 802.11r roaming when the WLAN security is configured as **Open** under **WLANs** > **Home Access** > **SSID**.
Candidate Channels	This parameter is applicable only to 5 GHz radio. Configures whether all channels in the 5 GHz band are used or not. Following are the supported values: • **All**—Includes all channels supported in the 5 GHz band. • **Prefer Non-DFS**—Excludes the DFS channels (radar channels) and includes only the non-DFS channels.

7. Click the **Network** tab on the left pane and configure the WAN mode and IP address assignment parameters.



a. The **AP Mode** is pre-configured as **Router** and cannot be modified.

b. In the **WAN Configuration** section, select the required WAN mode and configure the corresponding parameters.

   This mode selects the mode of IP address assignment for the WAN interface. The following WAN modes are supported:

   - **DHCP**—This mode is selected by default.

     No additional parameter configuration is required.

   - **PPPoE**—Configure the PPPoE parameters as described in Table 112.

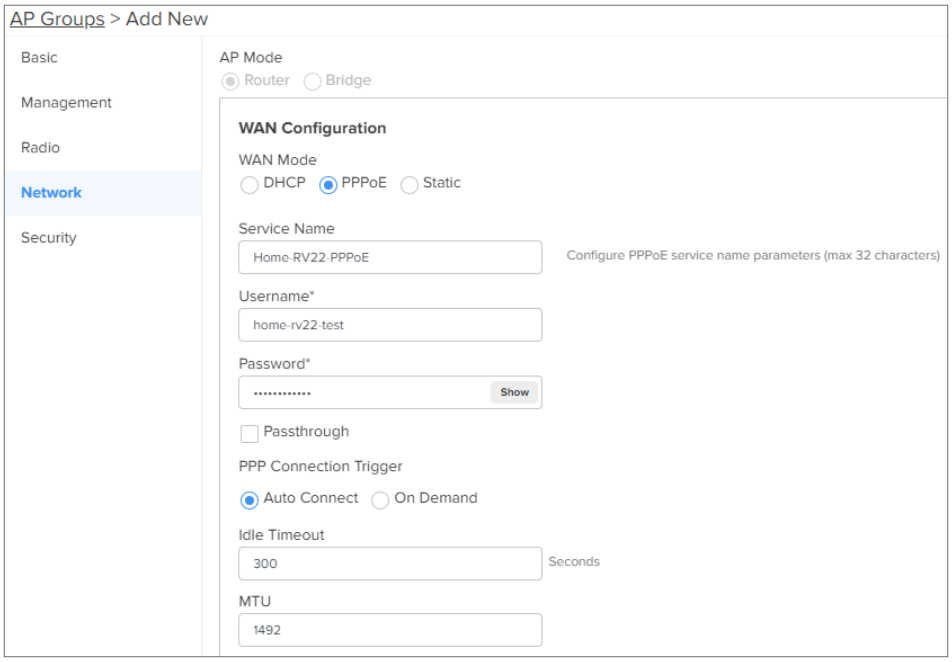


Table 112 *WAN Mode: PPPoE parameters*

Parameter	Description
PPPoE-related parameters	
Service Name	Name of the PPPoE service name. Supports a maximum of 32 characters.
Username	Username of the PPPoE service required for authentication.
Password	Password of the PPPoE service required for authentication.
Passthrough	Indicates whether the clients must directly establish connection with the service provider. Select the checkbox to enable passthrough.
PPP Connection Trigger	Indicates the connection method for the router for keeping the connection intact. The following options are supported: • Auto Connect • On Demand
Idle Timeout	This parameter is mandatory when you select **On Demand** type of **PPP Connection Trigger**. Specifies the duration (in seconds) after which PPPoE keep-alive packets must be sent to keep the connection intact. Default: 300
MTU	Maximum size (in bytes) of each packet sent in a single transmission between connected devices. Default: 1492

- **Static**—Configure the Static parameters as described in Table 113.

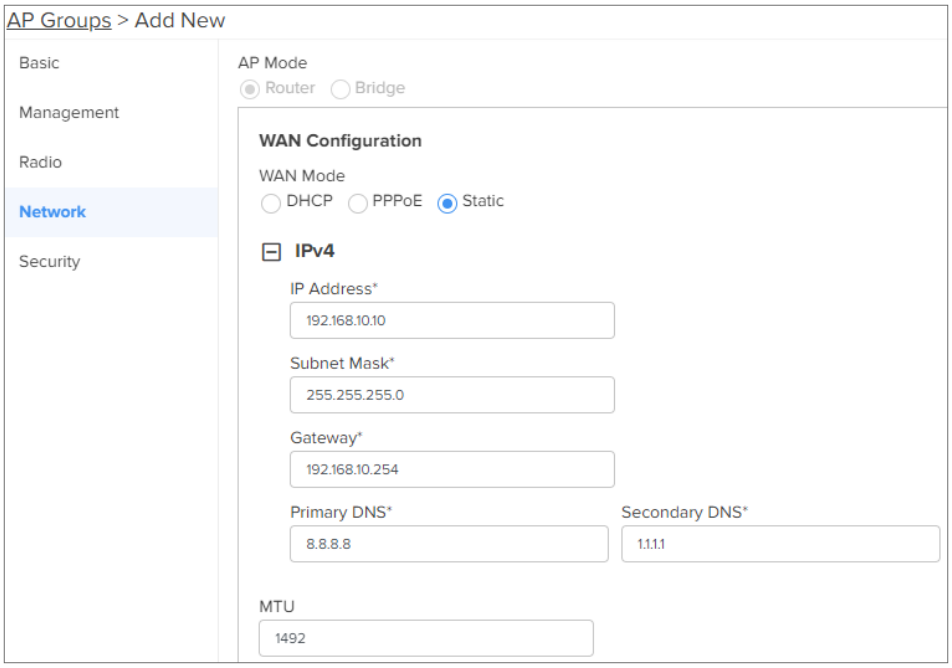


Table 113 *WAN Mode: Static parameters*

Parameter	Description
Static-related parameters	
IP Address	IPv4 address assigned to the router.
Subnet Mask	Subnet mask assigned to the router's IPv4 address.
Gateway	IPv4 address of the gateway used for communication.
Primary DNS	IPv4 address of the primary DNS server.
Secondary DNS	IPv4 address of the secondary DNS server.
MTU	Maximum size (in bytes) of each packet sent in a single transmission between connected devices. Default: 1492

Note

If you select **PPPoE** or **Static** mode, you must preconfigure the settings in the router before shipping the routers to customers. Complete the following steps before shipping the Home Mesh Router to the customers:

1. Onboard the Home Mesh Router using the standard WAN mode as **DHCP**.
2. After the Home Mesh Router is onboarded, set the WAN mode to **PPPoE** or **Static**.
3. Configure the username and password credentials.

   The configuration and the credentials are applied on the Home Mesh Router.
4. Disconnect the Home Mesh Router and ship it to the customer.

   When the customer connects the router to the PPPoE authenticated network, the Home Mesh Router uses the PPPoE credentials to authenticate.

c. In the **LAN Configuration** section, configure the mode of IP address assignment for connecting devices to **Auto** or **Manual**.

If you select Manual mode of assignment, configure the following parameters:

Table 114 *LAN Configuration parameters for Manual mode*

Parameter	Description
IPv4-related parameters	
Local IP Address	Local IPv4 address assigned to the router.
Local Subnet	Subnet mask assigned to the router's IPv4 address.
Address Range Start	Starting IPv4 address in the address pool.
Address Range End	Ending IPv4 address in the address pool.
Domain Name	The domain name.
DNS Mode	DNS mode used for IP address resolution. Following are the supported options: • Auto • Manual • Proxy

8. Click the **Security** tab on the left pane and configure protection against different types of attacks, such as Smurf attack and ICMP fragment.

Select the checkbox corresponding to the DoS protection options.

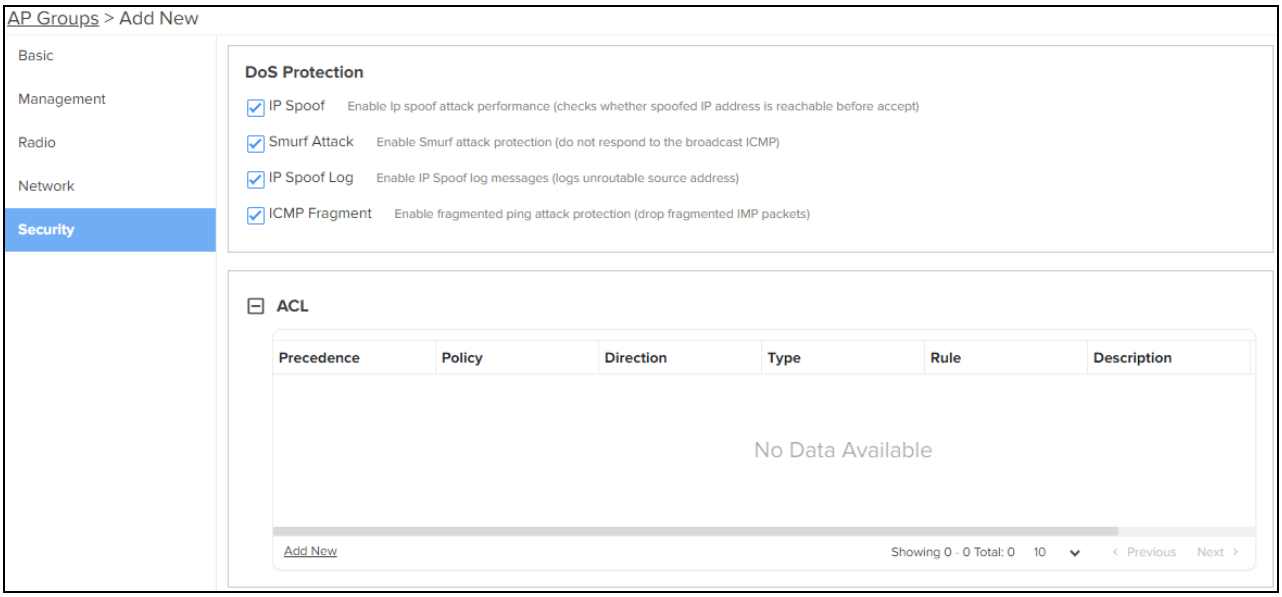


Table 115 *Security parameters: DoS Protection*

Parameter	Description
IP Spoof	Enable protection agains IP spoof attacks. When enabled, the router checks whether the spoofed IP address is reachable before accepting.

Table 115 *Security parameters: DoS Protection*

Parameter	Description
Smurf Attack	Enable protection agains Smurf attacks. When enabled, the router does not respond to the broadcast ICMP.
IP Spoof Log	Enable logging of IP spoof addresses. When enabled, the router logs the unroutable source IP address.
ICMP Fragment	Enable protection against ICMP fragmented ping attack. When enabled, the router drops the fragmented ICMP packets.

9. Click **Add New** in the **ACL** section and configure the parameters as described in Table 115.

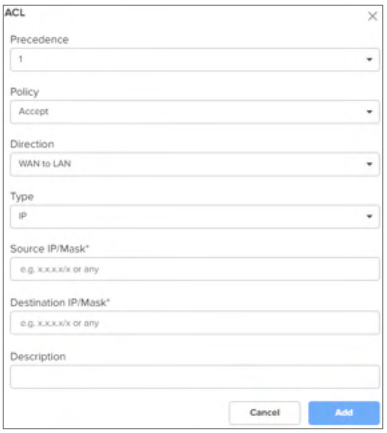


Table 116 *Security parameters: Access Control List (ACL)*

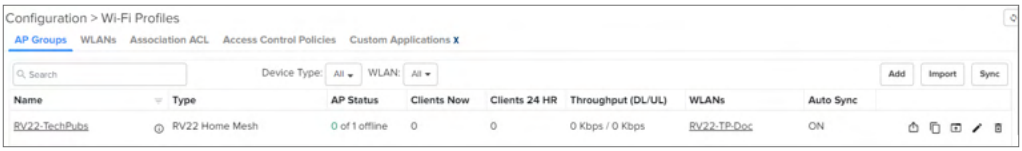
Parameter	Description
Precedence	Specifies the priority of the rule configured. Select the precedence from the dropdown list.
Policy	Indicates the action to be taken for the policy. The following are the supported actions: • Accept • Drop • Reject
Direction	Direction to which the policy must be applied. The following are the supported options: • WAN to LAN • LAN to WAN • WAN to Router • Router to WAN
Type	Type of traffic to which the policy must be applied. The following are the supported options: • IP

Table 116 *Security parameters: Access Control List (ACL)*

Parameter	Description
	• IPv6 • MAC • Protocol • Protocolv6 Additional parameters are enabled when you selct the type.
Source IP/Mask Destination IP/Mask	This field is applicable when you select the **Type** as **IP**, **IPv6**, **Protocol**, or **Protocolv6**. Specifies the source IPv4 or IPv6 address and the destination IPv4 or IPv6 address for the policy. You can configure **Any** if there is no specific IP address to apply the policy to any source IP address.
Source MAC/Mask Destination MAC/Mask	This field is applicable when you select the **Type** as **MAC**. Specifies the source MAC address and the destination MAC address for the policy. You can configure **Any** if there is no specific MAC address to apply the policy to any source IP address.
Protocol	Type of protocol for which the policy must be applied. The following are the supported options: • TCP • UDP • ICMP • Any Additional parameters are enabled when you selct the protocol.
Source Port	This field is applicable when you select the **Protocol** as **TCP**, **UDP**, or **Any**. Specifies the source port number for the policy.
Destination Port	This field is applicable when you select the **Protocol** as **TCP**, **UDP**, or **Any**. Specifies the source port number for the policy.
Description	Description for the rule.

10. Click **Save**.

    The AP group is successfully created with the configured parameters.



Onboarding the Home Mesh Router to cnMaestro

After creating a WLAN profile and an AP group, you must now create a subscriber profile and associate it with the subscriber. Finally, you must onboard the router(s) to the corresponding subscriber.

Adding a subscriber and onboarding the router involves the following steps:

1. cnMaestro Subscriber application branding
2. Adding a Home Site
3. Adding a Subscriber Service Profile
4. Adding a subscriber
5. Claiming the Home Mesh Router

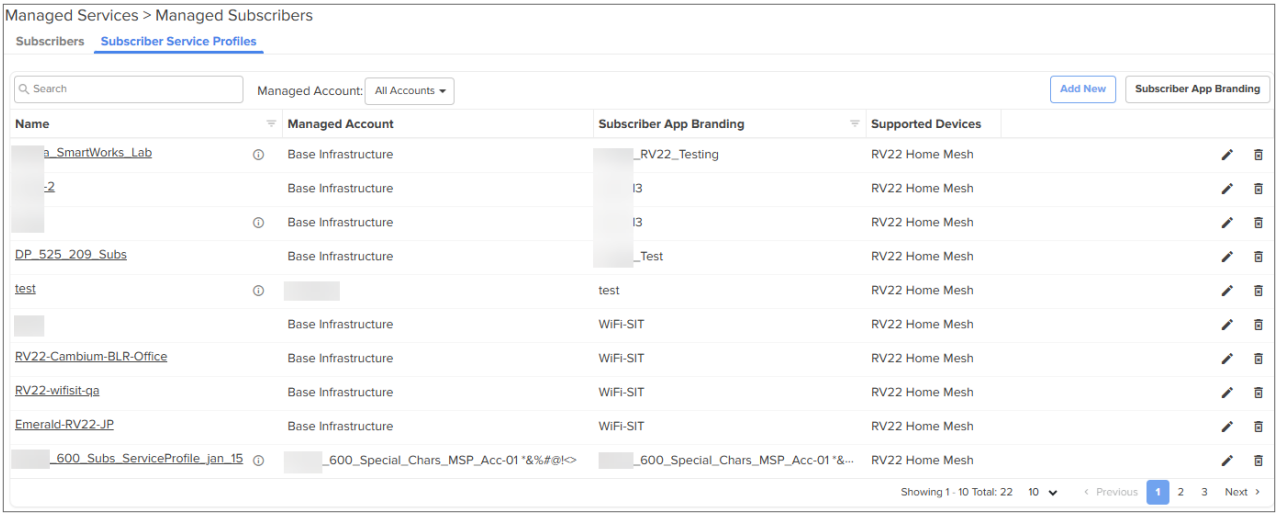
cnMaestro Subscriber application branding

Customize the cnMaestro Subscriber mobile application with your company name, brand logo, and other details, such as support contact information and hours. This branding can be associated with individual subscriber service profiles.

To add brand details to the cnMaestro Subscriber application, complete the following steps:

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

   The **Subscriber Service Profiles** page appears.



2. Click **Subscriber App Branding**.
3. Click the add (+) icon.

   The **Subscriber App Branding** window appears. Configure the following parameters as described in Table 117.

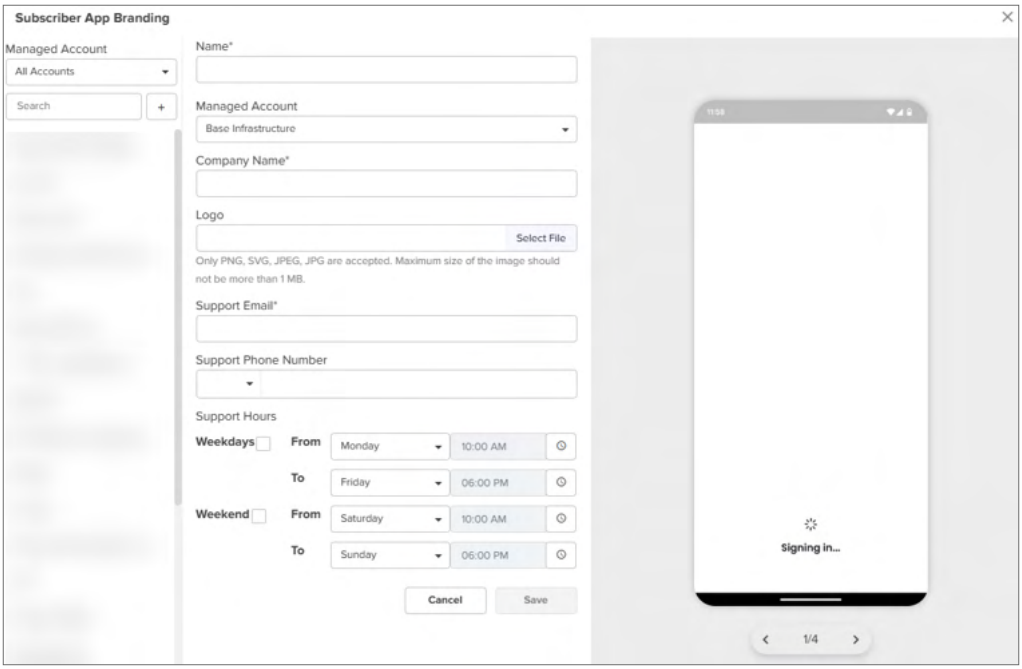


Table 117 *Subscriber App Branding parameters*

Parameter	Description
Name	Name of the application branding.
Managed Account	Specifies the availability of the subscriber across managed accounts. The following values are supported: • Base Infrastructure—Subscriber is available only for the global account. It is not shared with other managed accounts. • Managed Account—Subscriber is available only for that specific managed account. **Note** Once the Managed Account is configured for a Subscriber App Branding, it cannot be modified.
Logo	Brand logo displayed in the cnMaestro Subscriber application. Maximum size of the image supported is 1 MB. Only JPEG, JPG, PNG, and SVG file formats are supported.
Support Email	Email address for customer support team displayed in the application.
Support Phone Number	Phone number for customer support team displayed in the application.
Support Hours	Contact hours for the customer support team. • Select the **Weekdays** checkbox and configure the week days on when the customer support team is available. You can also configure the time using the time picker tool. • Select the **Weekends** checkbox and configure the weekend days on when the customer support team is available. You can also configure the time using the time picker tool.

You can preview your branding updates by scrolling through the images in the preview window on the right.

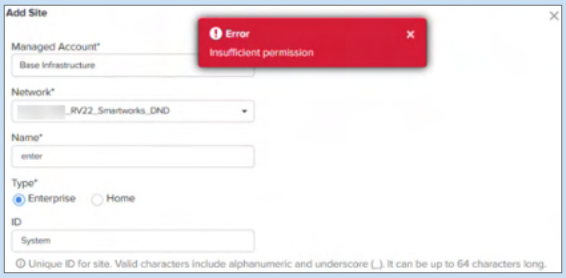
4. Click **Save**.

Adding a Home Site

Note

- Operator users can add or delete a home site for the RV22 Home Mesh Routers.

  However, they are not allowed to create Enterprise sites while creating subscribers. The following error message appears in case they try to create an Enterprise site:

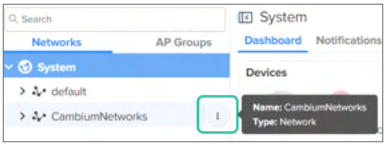


- Operator users can also modify the details, such as latitude, longitude, and network, under the **Configuration** tab at the home site-level.

A home site is required to associate the subscriber's device with the device configuration.

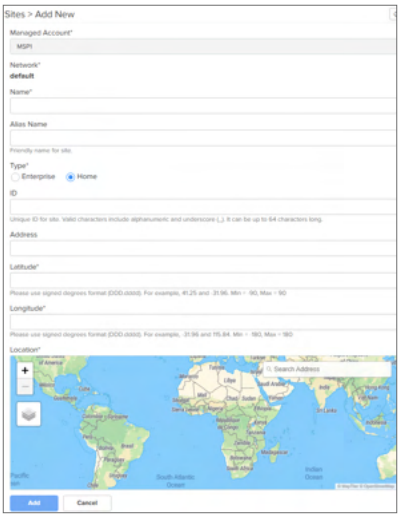
To create a home site, complete the following steps:

1. Click **Monitor and Manage** ( ).
2. In the **Networks** tab, search for the network and hover over the network name.



3. Click the actions ( ) icon and select **Add Site**.

   The **Sites > Add New** page appears.



4. Enter the required name for the site and a friendly name for the site in the **Name** and **Alias Name** fields.
5. Select the **Home** option in the **Type** field.
6. Enter the location details in the **Longitude** and **Latitude** fields.

   You can also search for the location in the map to fill in the details.
7. Click **Add**.

Managing subscribers (end-customer)

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

This pocess involves the following actions:

1. Adding a Subscriber Service Profile
2. Adding a subscriber
   a. Modifying the owner details for the Subscriber App
3. Claiming the Home Mesh Router

Note

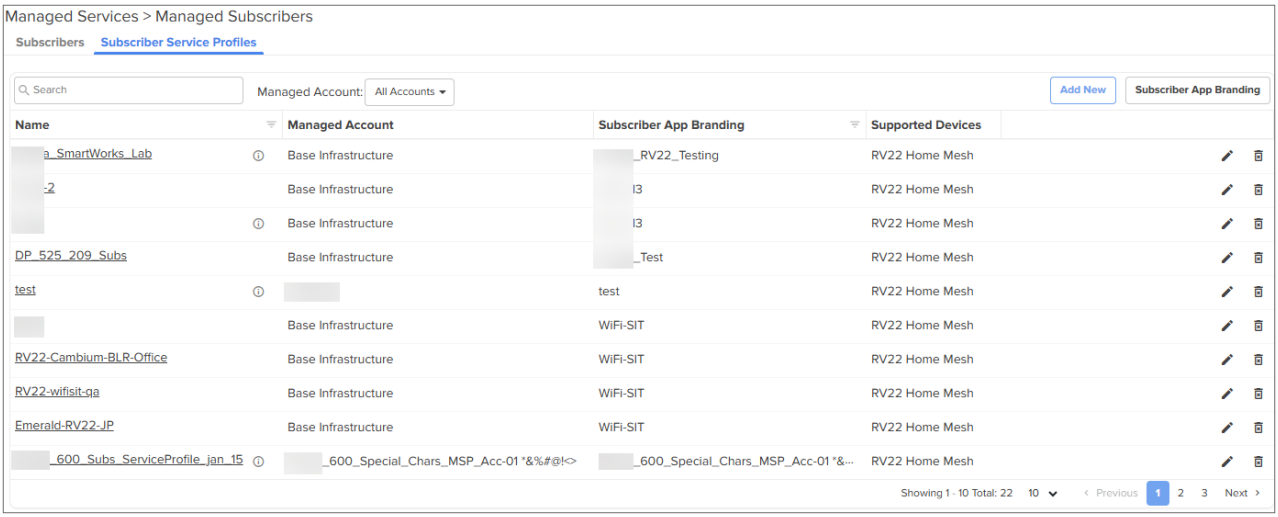
- Operator users can add new subscribers only.
- Operator users are not allowed to add or configure Subscriber Service Profiles or the Subscriber application branding.

Adding a Subscriber Service Profile

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

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

   The **Subscriber Service Profiles** page appears.



2. Click **Add New**.

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



3. Select the Home Mesh Router configuration to which you want to associate with the subscriber service profile and configure the parameters as described in Table 118.

Table 118 *Subscriber Service Profile parameters*

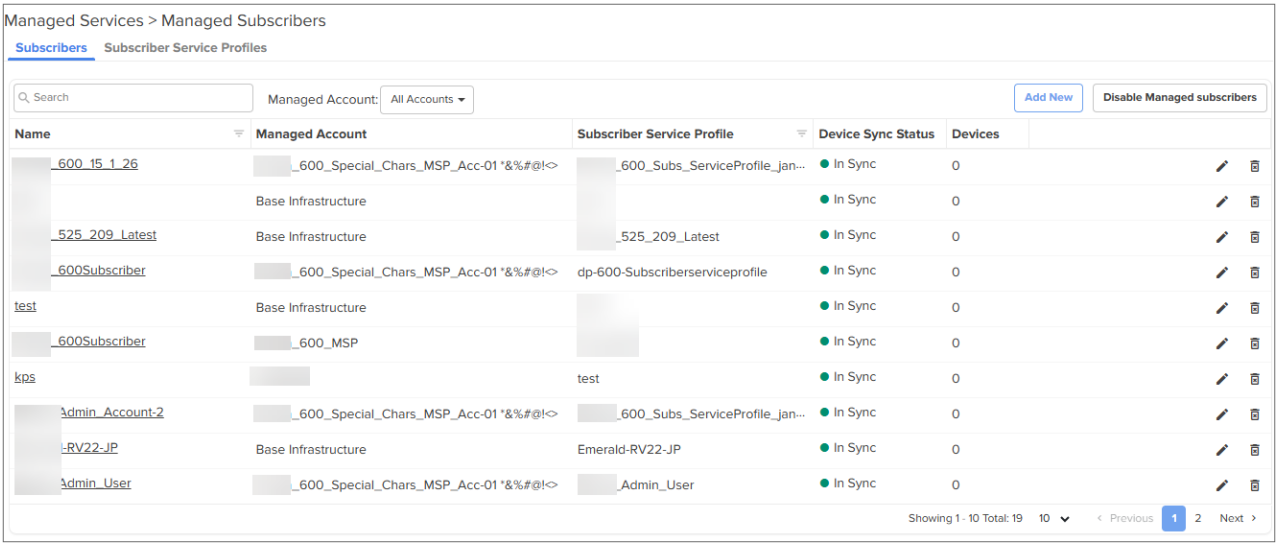
Parameter	Description
Name	Name of the subscriber service profile.
Managed Account	Specifies the availability of the subscriber service profile across managed accounts. The following values are supported: • Base Infrastructure—Subscriber service profile is available only for the global account. It is not shared with other managed accounts. • Managed Account—Subscriber service profile is available only for that specific managed account. **Note** Once the Managed Account is configured for a Subscriber Service Profile, it cannot be modified.

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

4. Click **Save**.

Adding a subscriber

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



6. Click **Add New**.

   The **Add Subscriber** window appears.



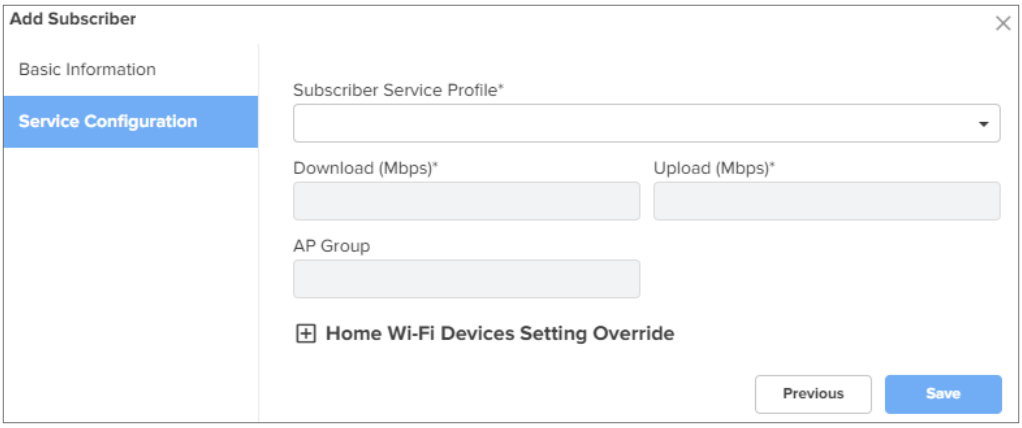
7. In the **Add Subscriber** window, configure the details of the subscriber in the **Basic Information** section, as described in Table 119.

Table 119 *Subscriber > Basic tab parameters*

Parameter	Description
Full Name	Name of the subscriber.
Managed Account	Specifies the availability of the subscriber across managed accounts. The following values are supported: • Base Infrastructure—Subscriber is available only for the global account. It is not shared with other managed accounts. • Managed Account—Subscriber is available only for that specific managed account. **Note** Once the Managed Account is configured for a Subscriber, it cannot be modified.
Email ID	Email address of the subscriber. This email address receives the invitation to join the Home Mesh Router (RV22) site. Through this email address the user will be able to access and manage the router as a primary user and invite other users (secondary users), through the mobile application, to manage the routers. **Note** You can edit this email address at anytime. However, editing this email address will remove all existing users, both primary and secondary. For information about how to modify the email ID, refer to Modifying the owner details for the Subscriber App.
Phone Number	Phone number of the subscriber.
Customer ID	Unique ID for the subscriber.
Address	Address of the subscriber where the routers will be installed.

8. Click **Next**.

The **Service Configuration** tab is displayed.

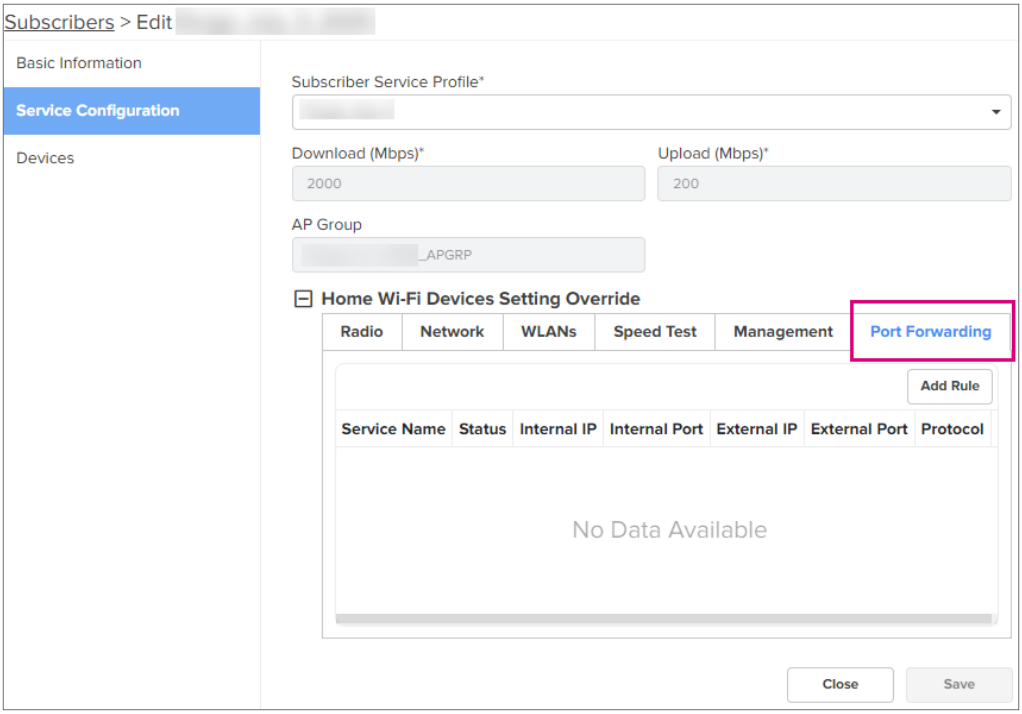


9. Select the subscriber service profile to be associated with this subscriber from the **Service Profile** dropdown list.
10. To configure port forwarding rules, expand the **Home Wi-Fi Devices Setting Override** section and click the **Port Forwarding** tab.

    Port forwarding allows external devices to access services hosted on internal network devices (for example, web servers and game servers) by routing traffic through the router to the configured internal IP and port.

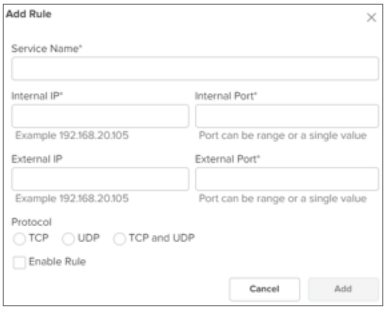
Note

- The port forwarding rule can also be added by the subscribers through the cnMaestro Subscriber application.
- In a mesh configuration, this rule is applied only to the Mesh Base router.
- Port forwarding is available on RV22 Home Mesh Routers running version 1.2.0 or later.
- A maximum of 16 port forwarding rules are supported.



11. Click Add Rule.

The **Add Rule** window is displayed.



12. Configure the following parameters:

Table 120 *Subscriber > Service Configuration > Port Forwarding rule parameters*

Parameter	Description
Service Name	Name of the service.
Internal IP	IP address of the device on the local network that will receive the forwarded traffic. For example, 192.168.20.105
Internal Port	Port number of the device on the local network that will receive the forwarded traffic. The field supports a single port number or a port range. For example: 80, 22, 3000-3010
External IP (Optional)	IP address from which incoming traffic is allowed. For example, 203.0.113.25
External Port	Port number of the router's public IP that listens for incoming connections. For example, 8080
Protocol	Type of protocol to be used for providing access. The following protocols are supported: • TCP • UDP • TCP and UDP
Enable Rule	Indicates whether the port forwarding rule must be enabled or disabled. Select the checkbox to enable the rule.

13. Click **Add**.

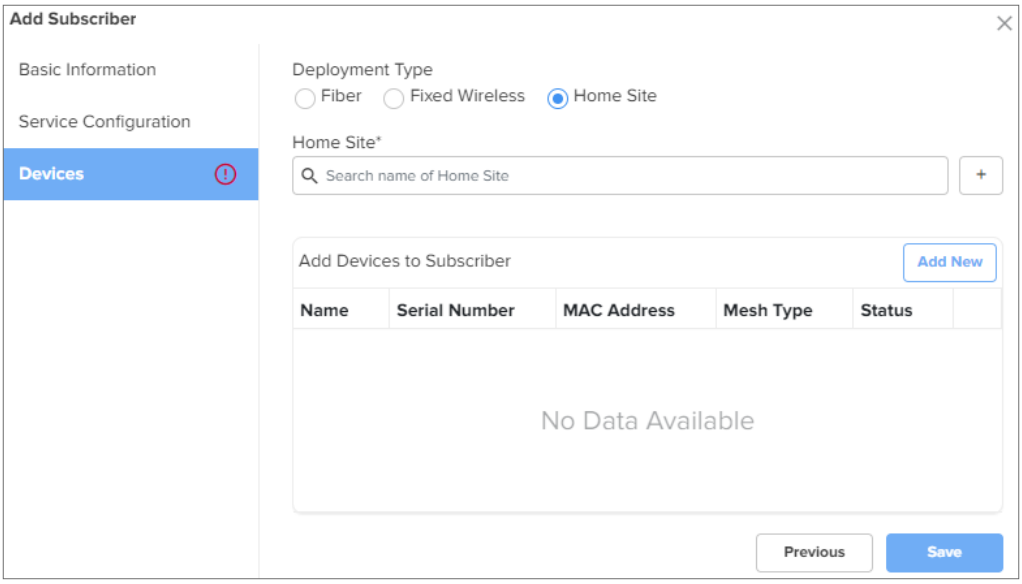
    The rule is listed in the **Port Forwarding** tab.

14. Click **Save**.

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

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

15. Click **Devices**.

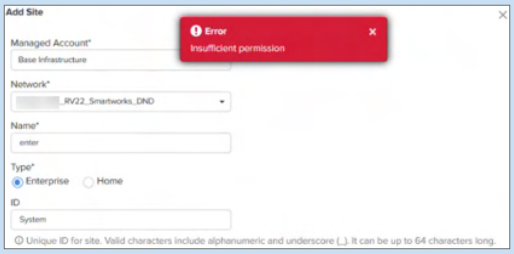


16. Select one of the following options in the **Deployment Type** field to filter the available deployment types:
    - **Fiber**—Select the Optical Network Unit (ONU) device that you want to associate with the subscriber's router by searching in the **ONU** search box.
    - **Fixed Wireless**—Select the Subscriber Module (SM) device that you want to associate with the subscriber's router by searching in the **SM** search box.
    - **Home Site**—Select the home site you want to associate with the subscriber's router by searching in the **Home Site** search box. To add a home site, see Adding a Home Site.

Note

- Operator users can add or delete a home site for the RV22 Home Mesh Routers.

  However, they are not allowed to create Enterprise sites while creating subscribers. The following error message appears in case they try to create an Enterprise site:



- Operator users can also modify the details, such as latitude, longitude, and network, under the **Configuration** tab at the home site-level.

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

Modifying the owner details for the Subscriber App

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

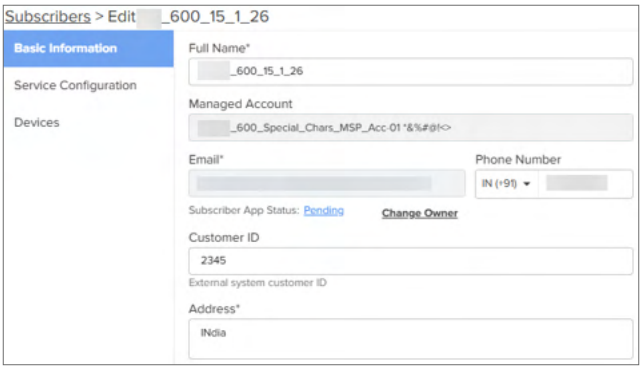
Warning

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

To modify the email address, complete the following steps:

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

   The corresponding subscriber details are displayed.



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

   The Change Owner window is displayed.



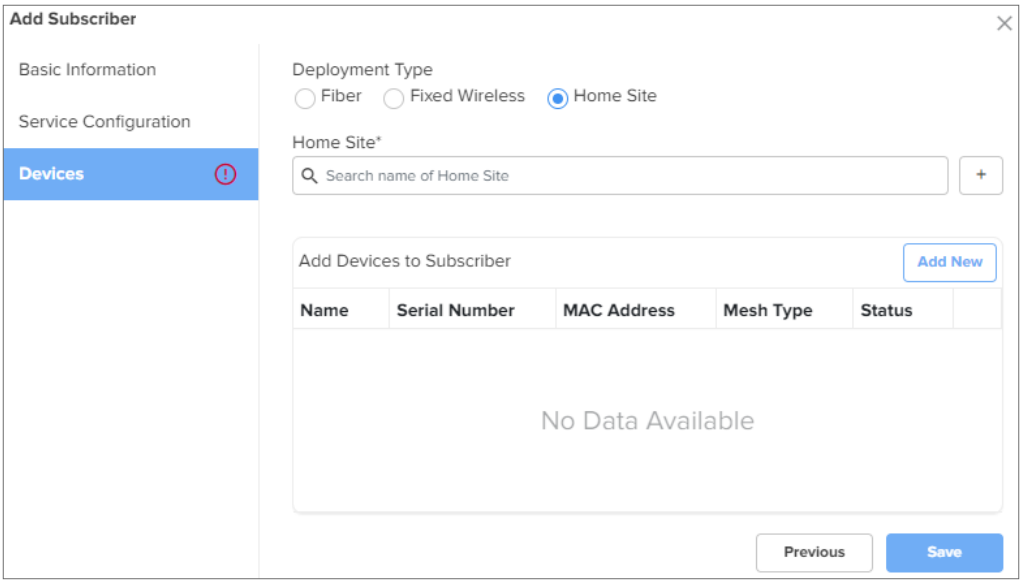
4. Enter the new email ID for the subscriber.
5. Click **Update**.

Claiming the Home Mesh Router

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

To claim the router, complete the following steps:

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

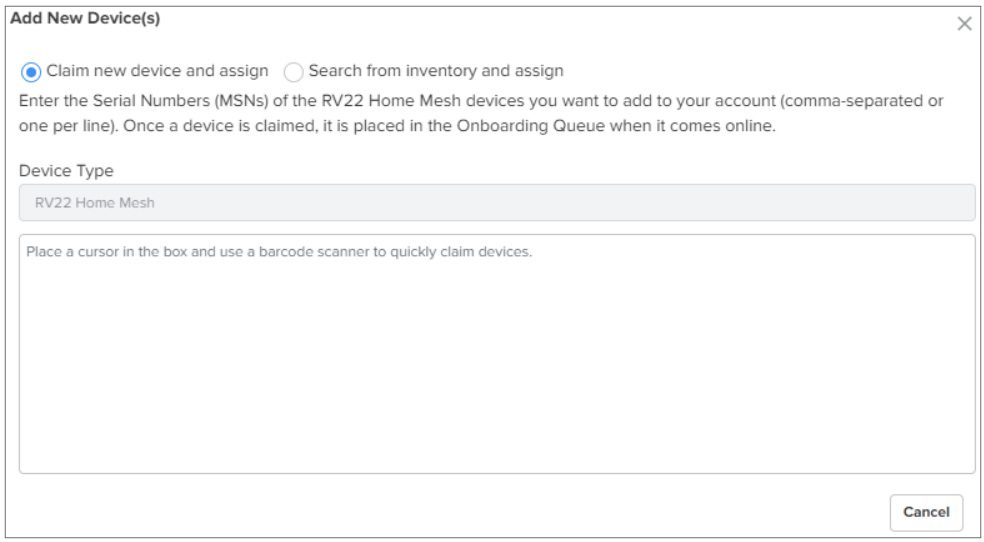


The **Link Subscriber** window appears.

5. In the **Link Subscriber** window, link the Home Mesh Router to the subscriber by using any of the following methods:

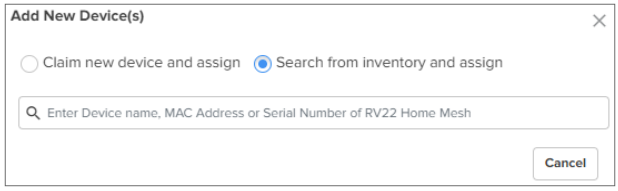
   - To claim a new router that is not onboarded to cnMaestro, select the **Claim new and assign** option and enter the serial number of the device to be claimed.

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



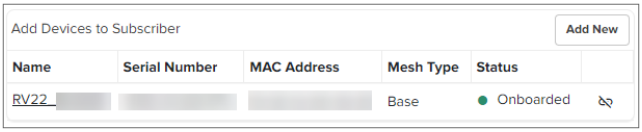
   - To claim a router that is already onboarded to cnMaestro, select the **Search for inventory and assign** option.

     Enter the details of the router you want to claim.



6. Click **Assign**.

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



Note

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

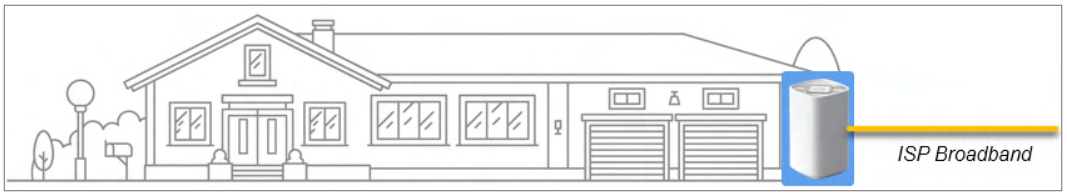
Setting up the Home Mesh Router

Home Mesh Routers can be deployed in one of the following modes:

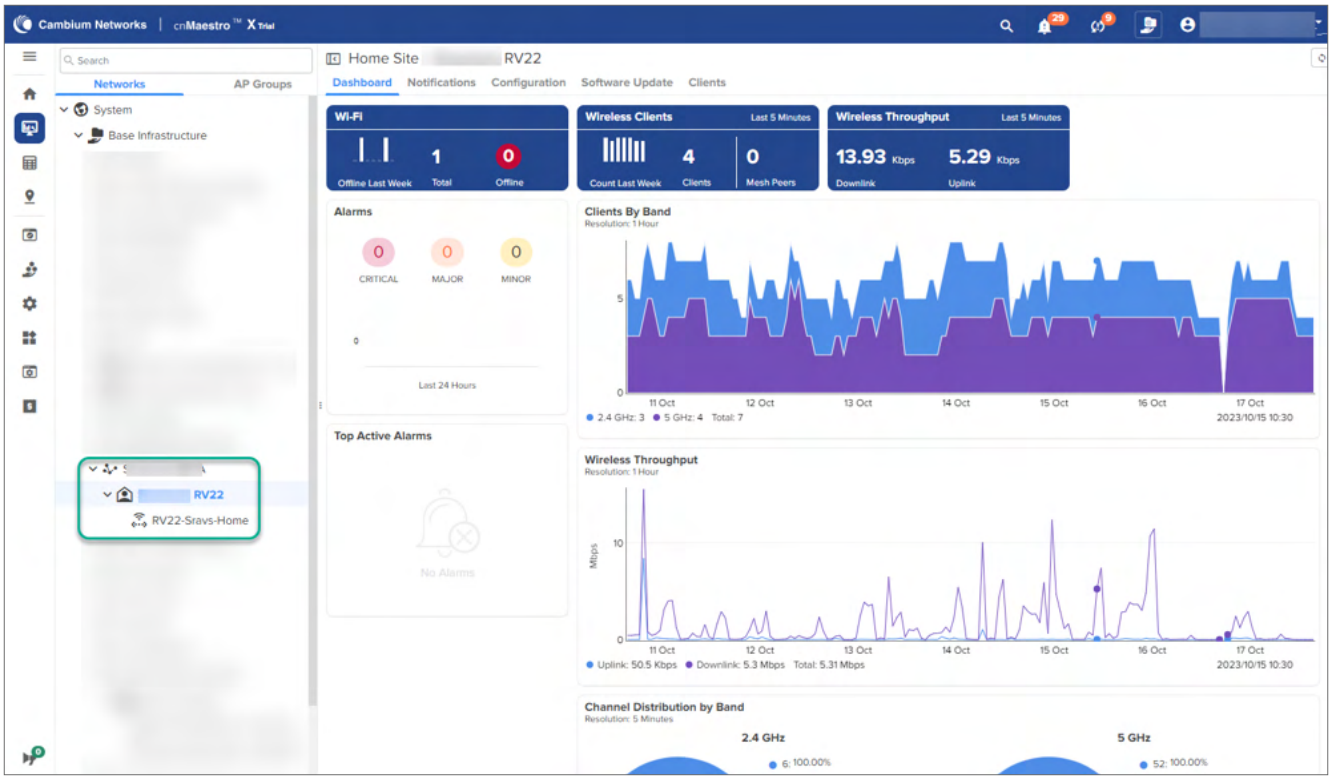
- Setting up the Home Mesh Router—Standalone mode
- Setting up the Home Mesh Router—Wireless Mesh Mode
- Setting up the Home Mesh Router—Wired Mesh Mode

Setting up the Home Mesh Router—Standalone mode

In standalone mode of deployment, there is only one Home Mesh Router deployed. A sample scenario is shown in the following figure:



A sample cnMaestro dashboard for the standalone mode of deployment is shown in the following figure:



Setting up the Home Mesh Router—Wireless Mesh Mode

To configure a wireless mesh, onboard the routers to a site—Claim all the routers, which you want to be part of the mesh, on cnMaestro in the subscriber workflow. See Claiming the Home Mesh Router. Connect the mesh base router to the internet and wirelessly connect the node routers. The AP group mapped to the subscriber is applied to all the routers to sync the configuration.

Following are some of the wireless mesh configuration scenarios and the corresponding dashboards and hierarchy in cnMaestro:

- Wireless mesh: 1-1 deployment
- Wireless mesh: 1-1-1 deployment
- Wireless mesh: 1-2 deployment
- Wireless and wired mixed mesh 1-2 deployment

Wireless mesh: 1-1 deployment

In this deployment, the base router is connected to one node router, thereby creating a wireless 1-1 mesh deployment.

Figure 519 *Wireless mesh: 1-1 deployment*

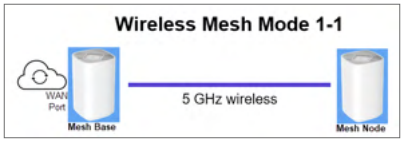


Figure 520 displays a sample cnMaestro dashboard for the wireless mesh 1-1 deployment.

Figure 520 *Sample dashboard for wireless mesh: 1-1 deployment*

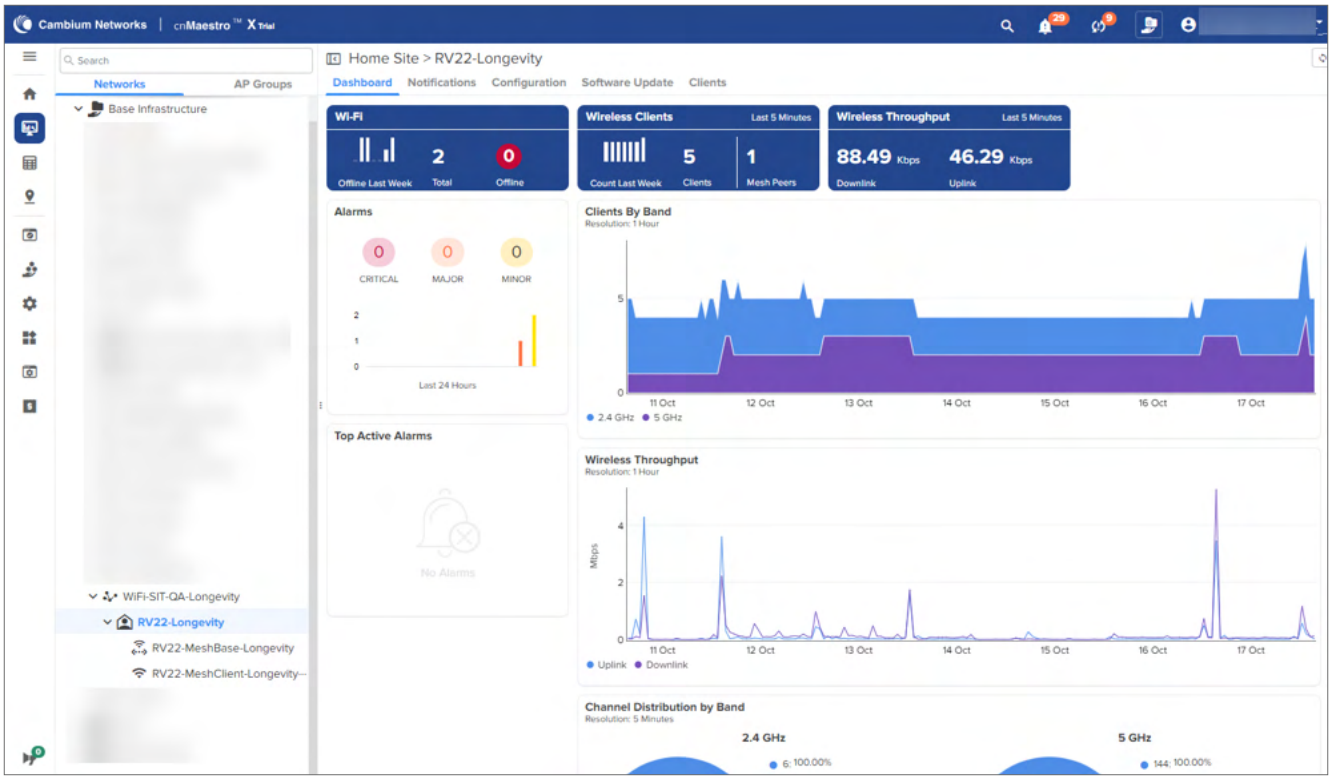
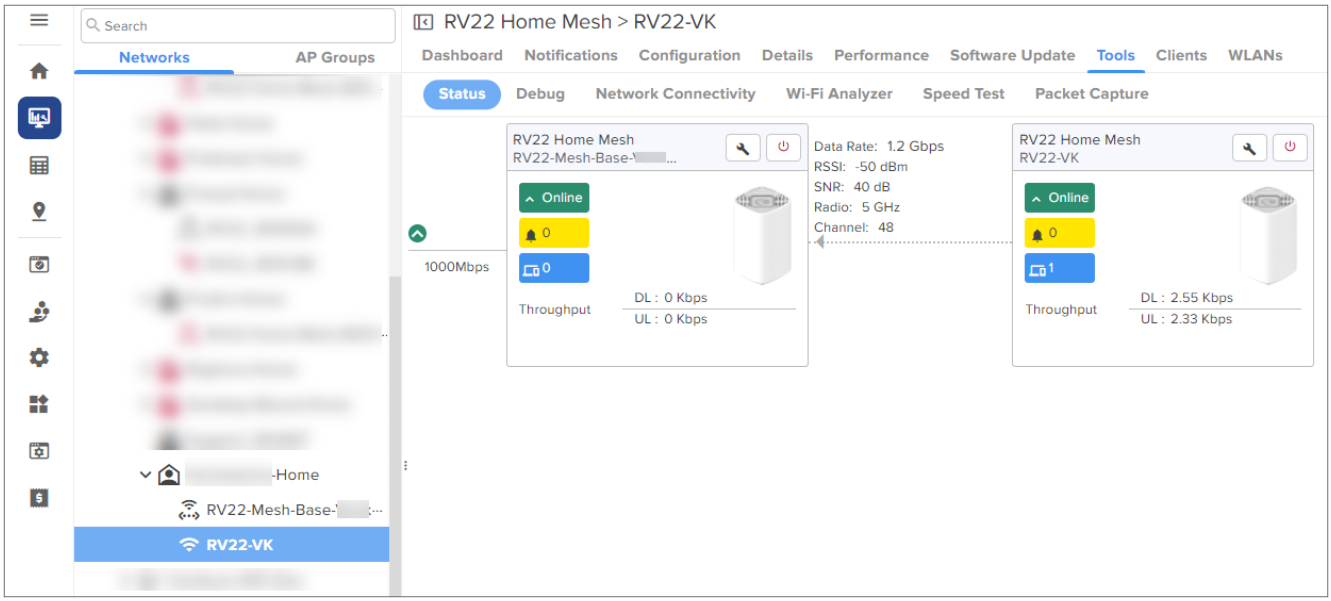


Figure 521 displays a sample cnMaestro status page for the wireless mesh 1-1 deployment.

Figure 521 *Sample status page for wireless mesh: 1-1 deployment*



Wireless mesh: 1-1-1 deployment

In this deployment, the base router is connected wirelessly to only one of the node routers, which is in turn connected to another node router, thereby creating a wireless 1-1-1 mesh deployment.

Figure 522 *Wireless mesh: 1-1-1 deployment*

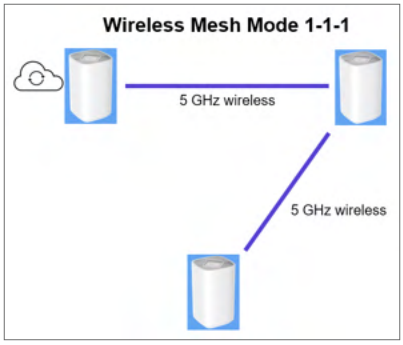


Figure 523 displays a sample cnMaestro dashboard for the wireless mesh 1-1-1 deployment.

Figure 523 *Sample dashboard for wireless mesh: 1-1-1 deployment*

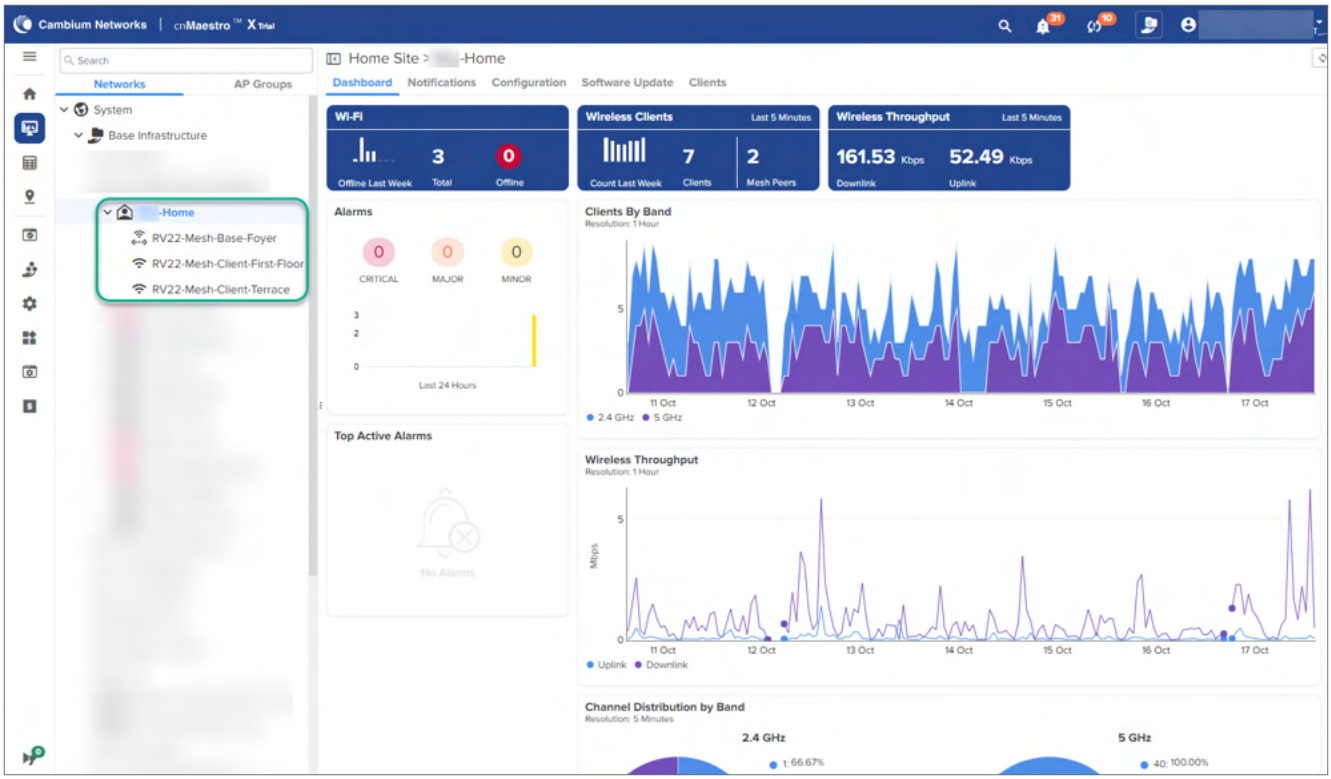
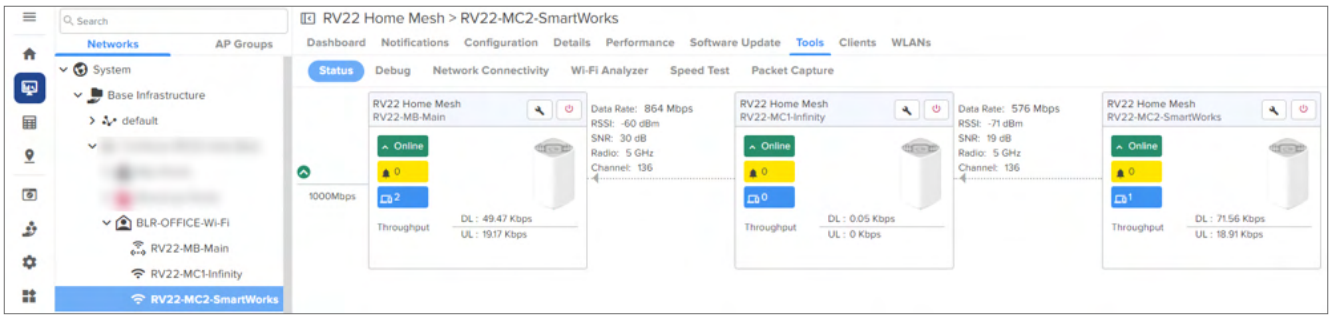


Figure 524 displays a sample cnMaestro status page for the wireless mesh 1-1-1 deployment.

Figure 524 *Sample status page for wireless mesh: 1-1-1 deployment*



Wireless mesh: 1-2 deployment

In this deployment, the base router is connected to two node routers simultaneously, thereby creating a wireless 1-2 mesh deployment.

Figure 525 *Wireless mesh: 1-2 deployment*

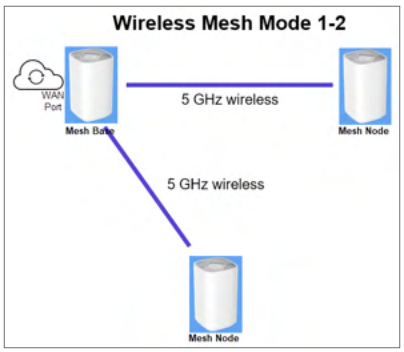


Figure 526 displays a sample cnMaestro dashboard for the wireless mesh 1-2 deployment.

Figure 526 *Sample dashboard for wireless mesh: 1-2 deployment*

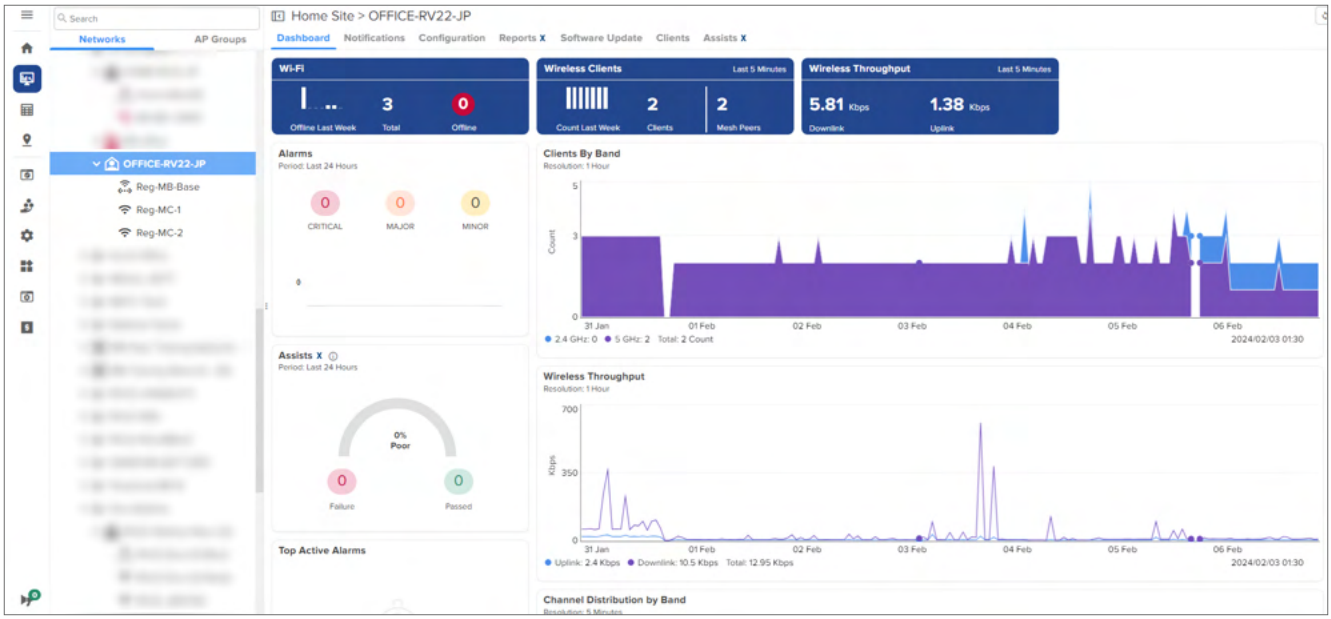
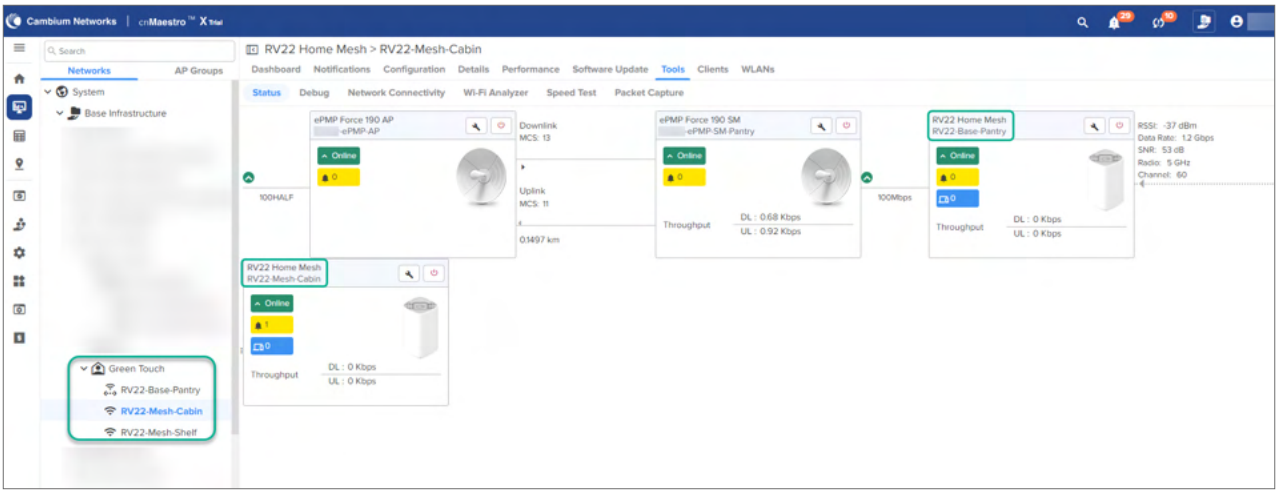


Figure 527 and Figure 528 display sample status pages for the node routers in a wireless mesh 1-2 deployment.

In the following status samples, the **RV22-Base-Pantry** router is connected to both **RV22-Mesh-Shelf** and **RV22-Mesh-Cabin** routers, forming a 1-2 multi-mesh topology.

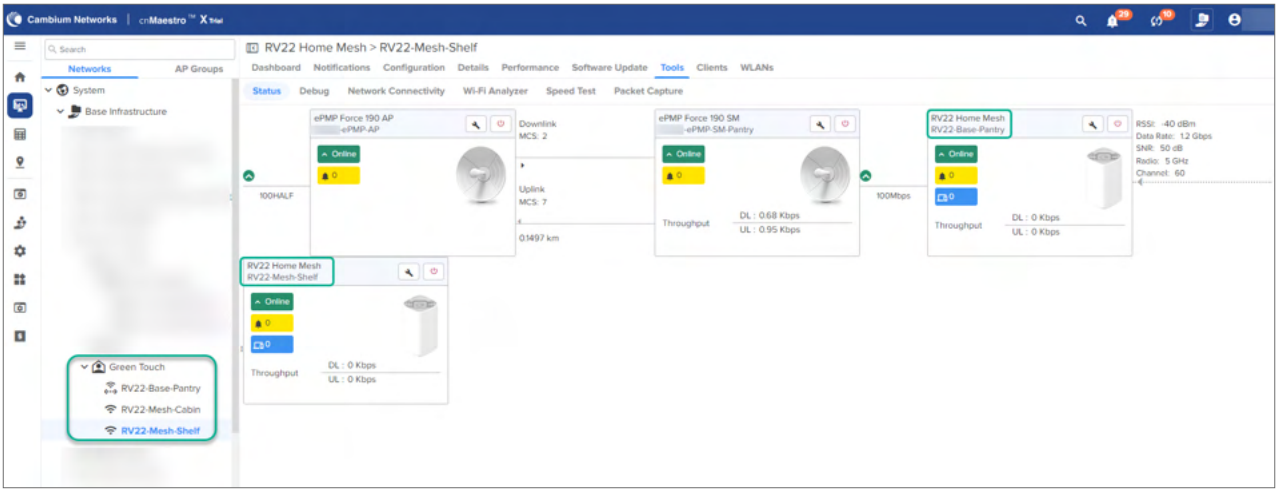
- Network toplogy for the **RV22-Mesh-Cabin** router

Figure 527 *Sample status page for RV22-Mesh-Cabin node router in a wireless mesh: 1-2 deployment*



- Network toplogy for the **RV22-Mesh-Shelf** router

Figure 528 *Sample status page for RV22-Mesh-Shelf node router in a wireless mesh: 1-2 deployment*



Wireless and wired mixed mesh 1-2 deployment

In this deployment, the base router is connected to one node router wirelessly and simultaneously to another by a wired connection, thereby creating a mixed 1-2 mesh deployment.

Figure 529 *Wireless and wired mixed mesh: 1-2 deployment*

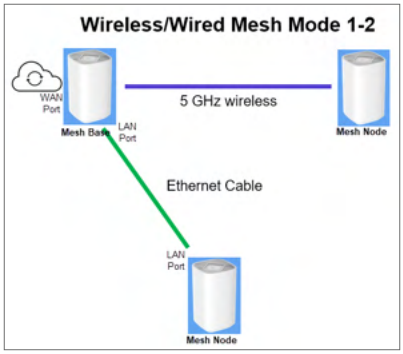
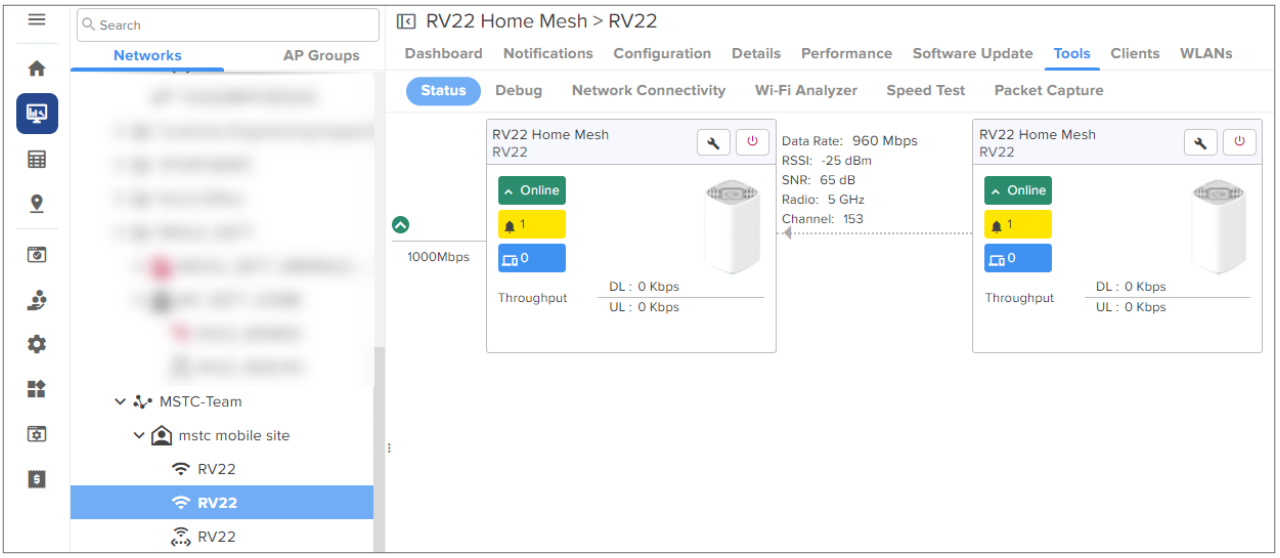


Figure 527 and Figure 528 display sample status pages for the node routers in a mixed mesh 1-2 deployment.

In the following status samples, one RV22 base router is connected to one RV22 node router wirelessly and simultaneously to another RV22 node router by a wired connection.

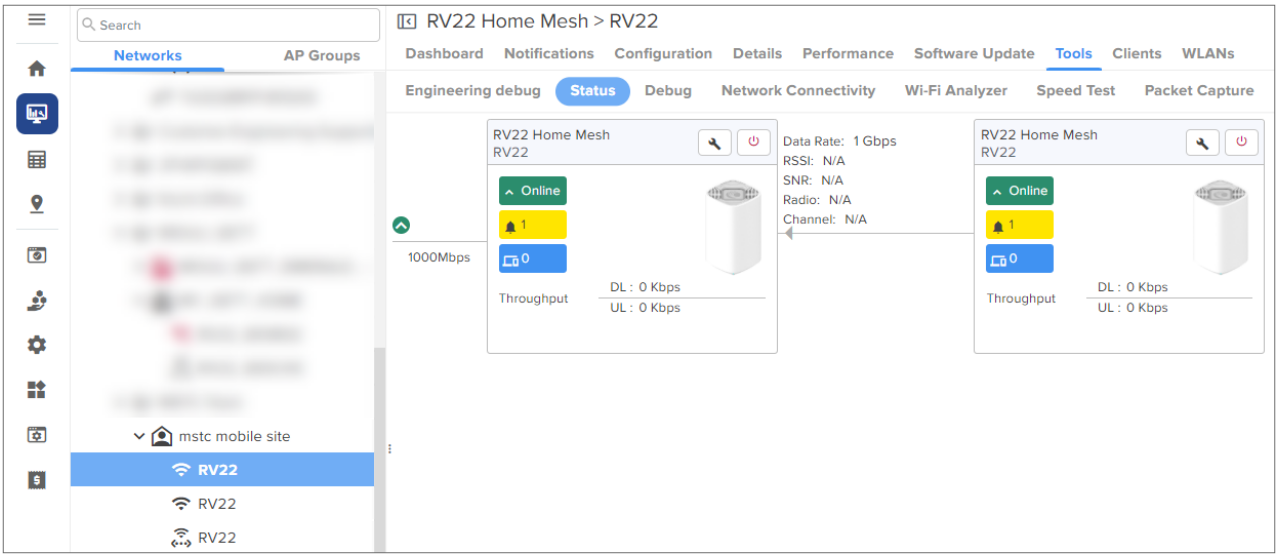
- Network toplogy for the wireless RV22 node router

Figure 530 *Sample status page for the wireless RV22 node router in a mixed mesh: 1-2 deployment*



- Network toplogy for the wired RV22 node router

Figure 531 *Sample status page for the wired RV22 node router in a mixed mesh: 1-2 deployment*



Setting up the Home Mesh Router—Wired Mesh Mode

To configure a wired mesh, onboard the routers to a site—Claim the routers, which you want to be part of the mesh, on cnMaestro in the subscriber workflow. See Claiming the Home Mesh Router. Connect the mesh base router to

the internet and connect the node routers to the base router using Ethernet cables. The AP group mapped to the subscriber is applied to all the routers to sync the configuration.

No configuration changes are required for RV22 routers to work in both wired and wireless mesh modes. Use any LAN port on the mesh base and any LAN port on the mesh node routers to establish a wired mesh connection. When a mesh node router detects an RV22 neighbor on its LAN port, it automatically establishes a wired mesh link using the LAN ports.

Note

You must not use the WAN port on the mesh node router to establish a wired mesh.

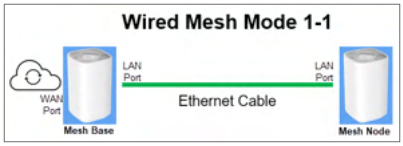
Following are some of the wired mesh configurations supported:

- Wired mesh: 1-1 deployment
- Wired mesh: 1-1-1 deployment
- Wired mesh: 1-2 deployment

Wired mesh: 1-1 deployment

In this deployment, the base router is connected to one node router using an Ethernet cable (between any LAN ports on both routers), thereby creating a wired 1-1 mesh deployment.

Figure 532 *Wired mesh: 1-1 deployment*



Wired mesh: 1-1-1 deployment

In this deployment, the base router is connected to only one of the node routers, which is in turn connected to another node router, by a wired connection (between any LAN ports on the routers), thereby creating a wired 1-1-1 mesh deployment.

Figure 533 *Wired mesh: 1-1-1 deployment*

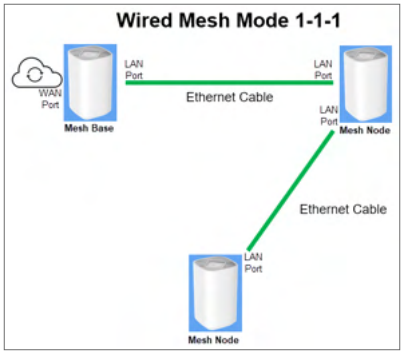
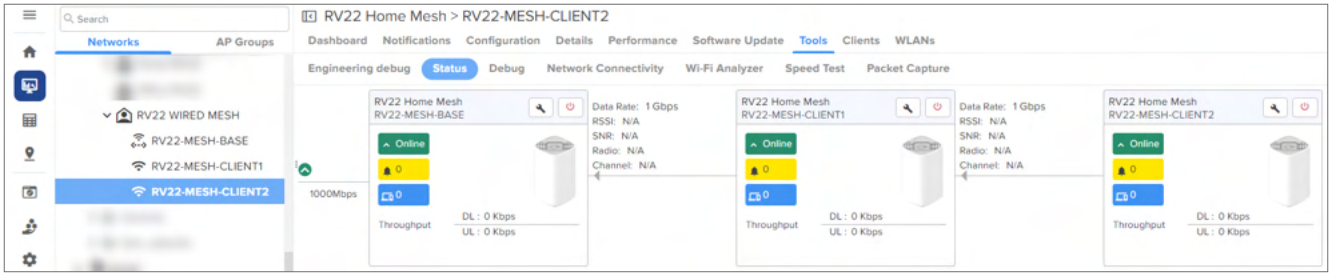


Figure 534 displays a sample cnMaestro status page for the wired mesh 1-1-1 deployment.

Figure 534 *Sample status page for wired mesh: 1-1-1 deployment*



Wired mesh: 1-2 deployment

In this deployment, the base router is connected to two node routers simultaneously by a wired connection, thereby creating a wired 1-2 mesh deployment.

Figure 535 *Wired mesh: 1-2 deployment*

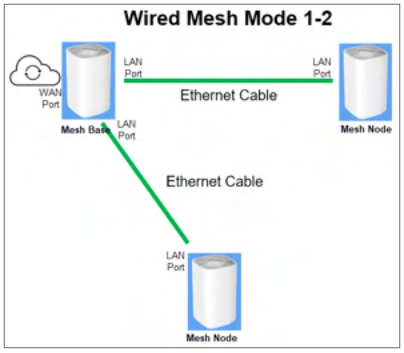
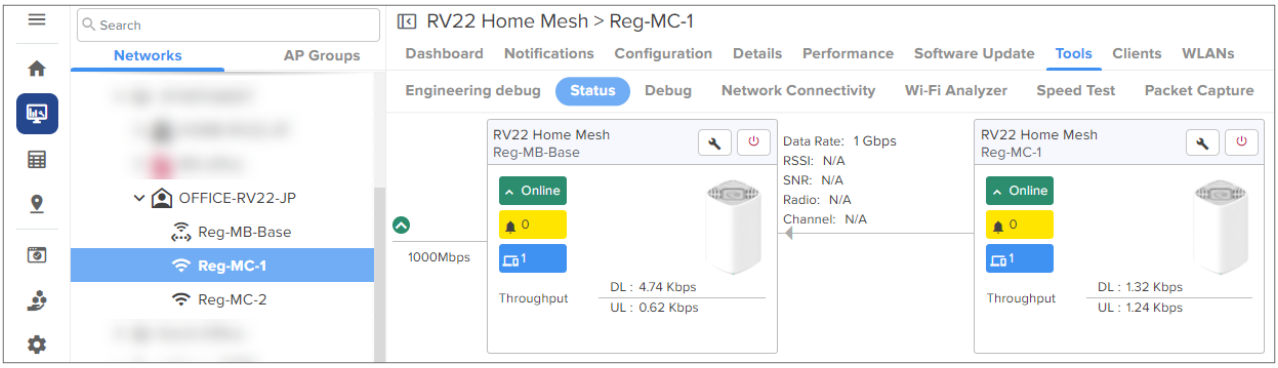


Figure 536 and Figure 537 display sample status pages for the node routers in a wired mesh 1-2 deployment.

In the following status samples, the **Reg-MB-Base** router is connected to both **Reg-MC-1** and **Reg-MC-2** routers using Ethernet cables, forming a wired 1-2 multi-mesh topology.

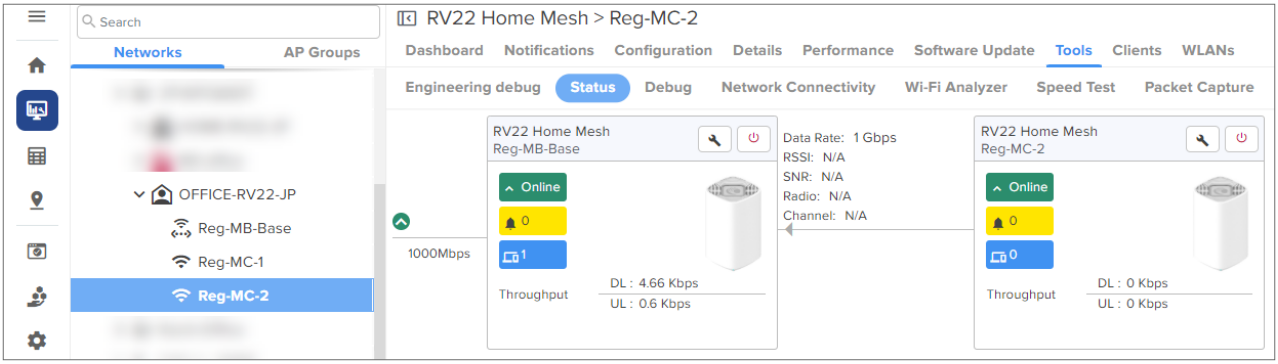
- Network toplogy for the **Reg-MC-1** router

  Figure 536 *Sample status page for Reg-MC-1 node router in a wired mesh: 1-2 deployment*



- Network toplogy for the **Reg-MC-2** router

Figure 537 *Sample status page for Reg-MC-2 node router in a wired mesh: 1-2 deployment*



Viewing router system information and network traffic status

When the customer configures the Home Mesh Router and connects to the internet, you can check the connection of the router in cnMaestro. You can also check the details of the clients that are connected.

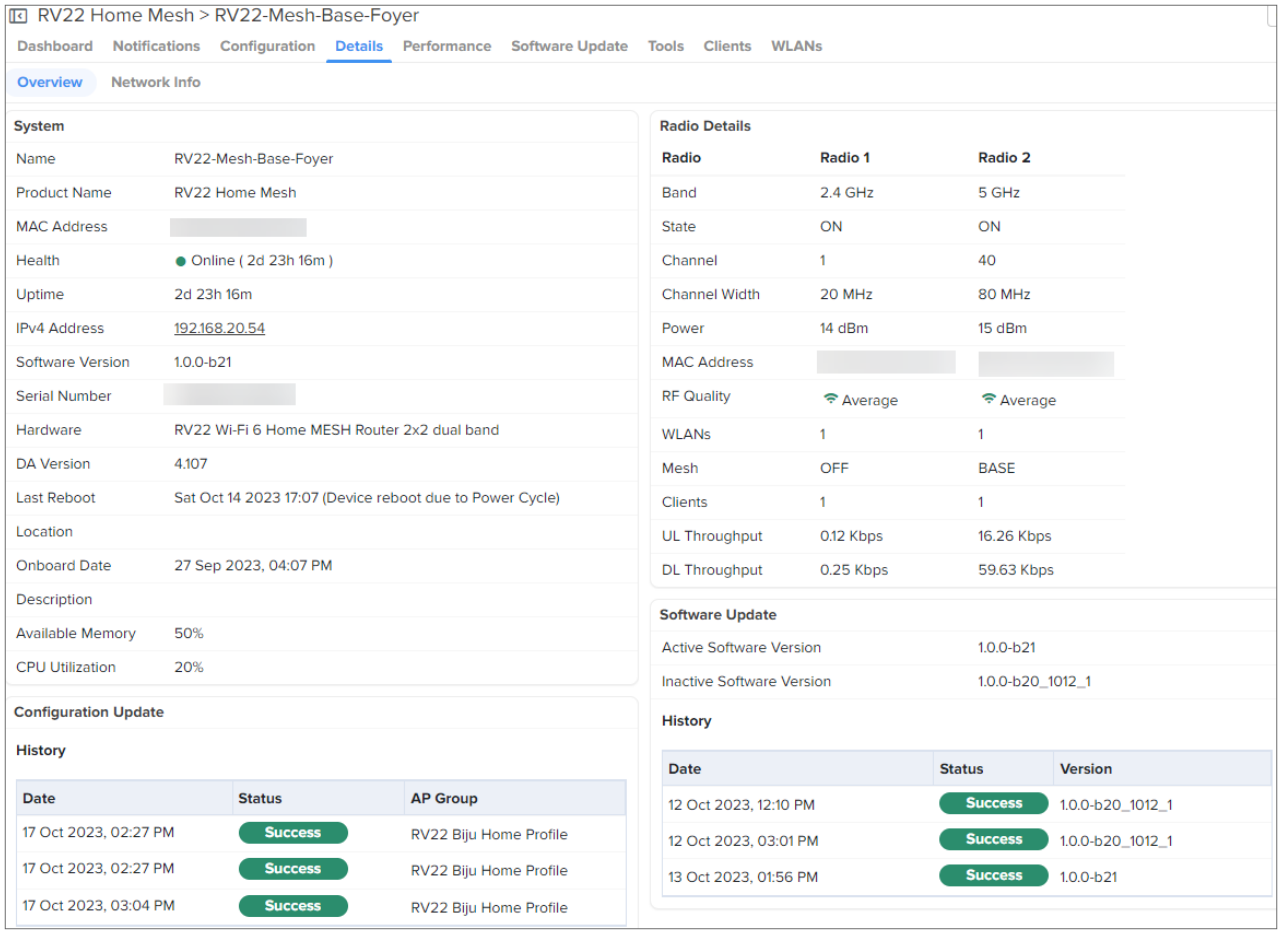
To view router system information and the connection status, navigate to **Monitor and Manage** > *<Home-Mesh-Router-name>* > **Details** tab.

The **Details** page displays information in the following tabs:

- **Overview**

  This page displays information in the following sections:

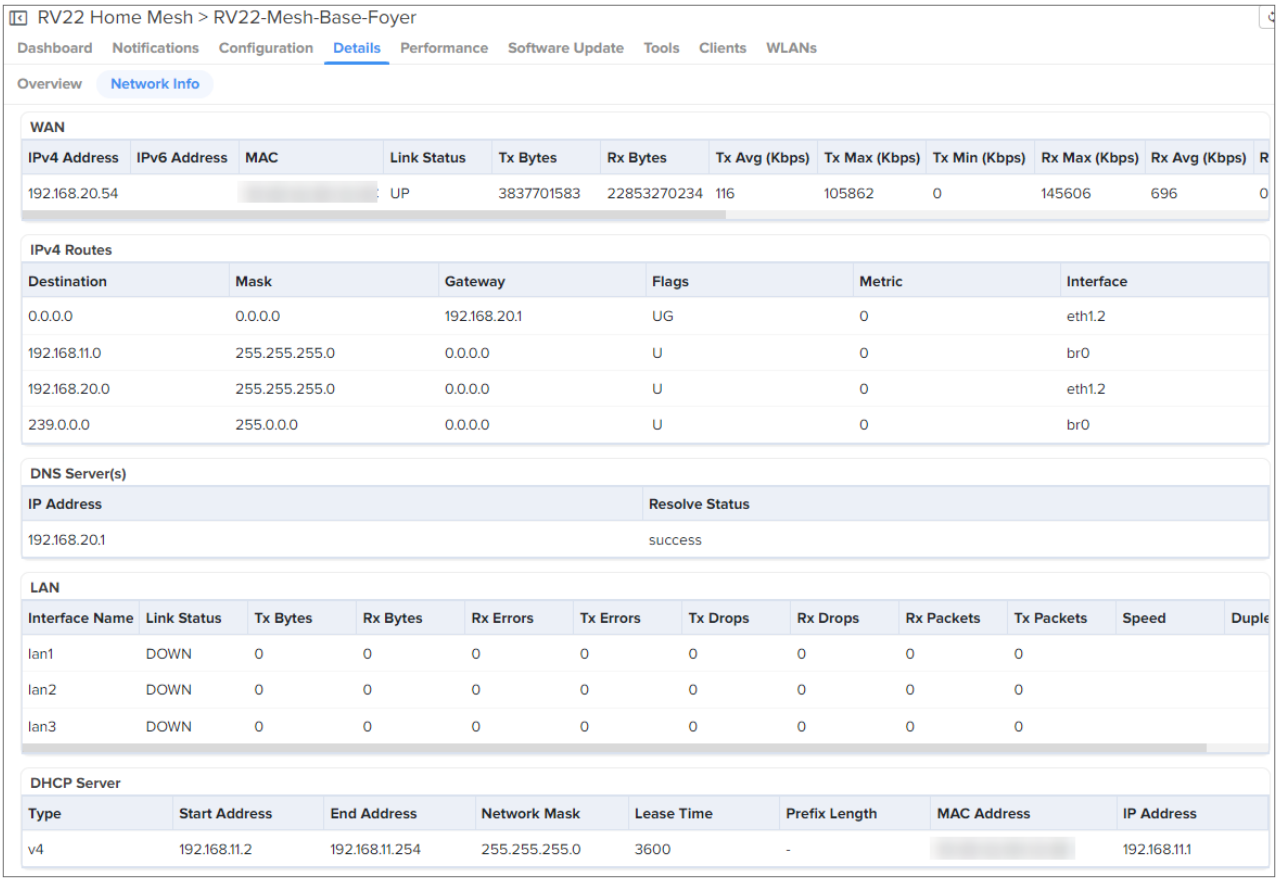
  - **System**—Displays information, such as router name, MAC address, health of the router (online, offline), software version, and location.
  - **Radio**—Displays radio details, such as the running bands, RF quality, count of clients connected to each radio, and the average throughput.
  - **Configuration Update**—Displays the history of configuration updates to the router.
  - **Software Update**—Displays the currently running software version and a history of software updates that were performed and the status.



- **Network Info**

  This page displays information in the following sections:

  - **WAN**—Displays collective statistics about total number of transmitted and received data packets, data bytes, packets dropped, maximum and average speeds
  - **IPv4 Routes**—Displays the IPv4 routes configured for the router.
  - **DNS Server(s)**—Displays the details of the DNS servers.
  - **LAN**—Displays details of the LAN interfaces, their status, total number of transmitted and received data packets and size (in bytes), packet errors and drops.
  - **DHCP Server**—Displays details of the DHCP servers, start and end IP address in the range used for allocation, and the lease time.



Viewing, editing, and blocking connected clients

cnMaestro allows you to view details of clients (both wired and wireless) connected to the router and edit the name of clients. You can also block certain clients that you do not want to be connected to your wireless networks.

This topic contains the following sections:

- Viewing connected clients
- Editing client host name
- Blocking clients

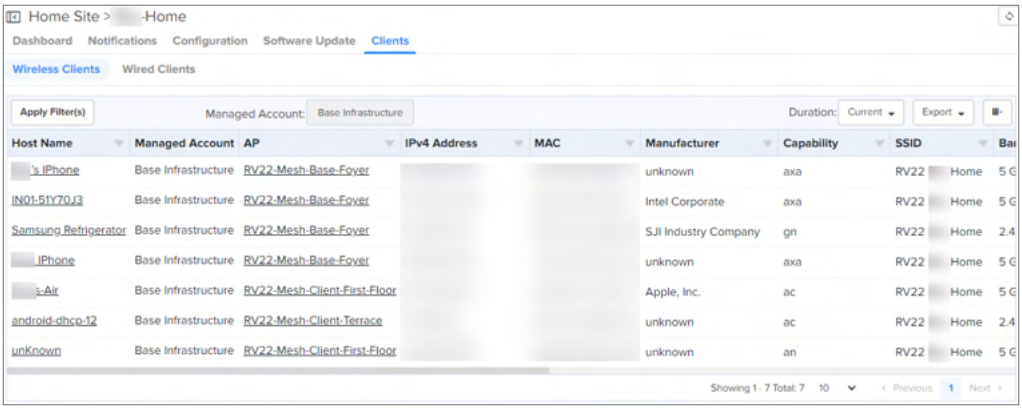
Viewing connected clients

To view the list of connected clients, both wired and wireless, navigate to **Monitor and Manage** > *<Home-Mesh-Router-name>* > **Clients** tab.

The **Details** page displays information in the following tabs:

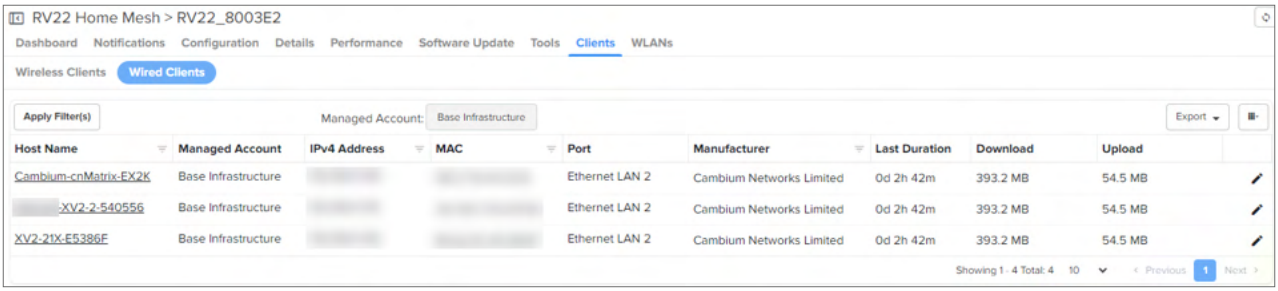
- **Wireless Clients**

  This page displays information about the wireless clients connected to the router, such as the host name, MAC address, IPv4 addess assigned, the router it is connected to, and the status of connection with the router (online, offline).



- **Wired Clients**

  This page displays information about the wired clients connected to the router, such as the host name, MAC address, IPv4 addess assigned, port number to which it is connected, the manufacturer of device connected, last connected duration, and the download and upload data size (in MB).



Editing a client's host name

To edit the host name of a connected client, click the edit client name ( ) icon corresponding to the client.

Enter the name in the **Host Name** field and click **Save**.



Blocking clients

To block a connected client, click the block ( ) icon corresponding to the client.

Monitoring and troubleshooting the Home Mesh Router

You can monitor and perform troubleshooting tasks on the Home Mesh Router using cnMaestro. This topic covers the following sections

- Monitoring the Home Mesh Router
- Troubleshooting the Home Mesh Router
- Upgrading the Home Mesh Router firmware

Monitoring the Home Mesh Router

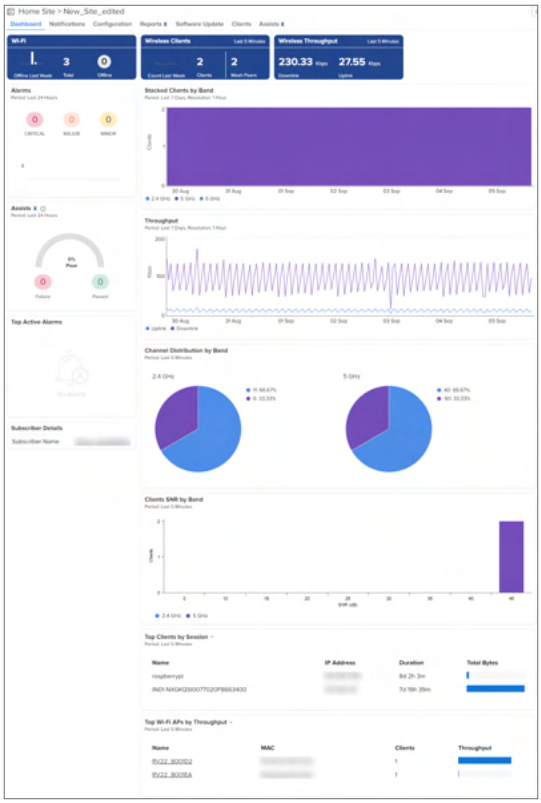
When the device is onboarded to cnMaestro, based on the deploymnet type, the router is displayed under the site that it is configured.

Using the following pages in cnMaestro, monitor and view details of the router and the deployment.

- Home Site Dashboard
- Notifications
- Software Update
- Performance

Home Site Dashboard

To view the site dashboard, access the **Dashboard** page under **Monitor and Manage >** <Home-site-name> **> Dashboard.**



Notifications

The Notifications page displays current alarms, previous alarms, Wi-Fi-related events, and other device-related events.

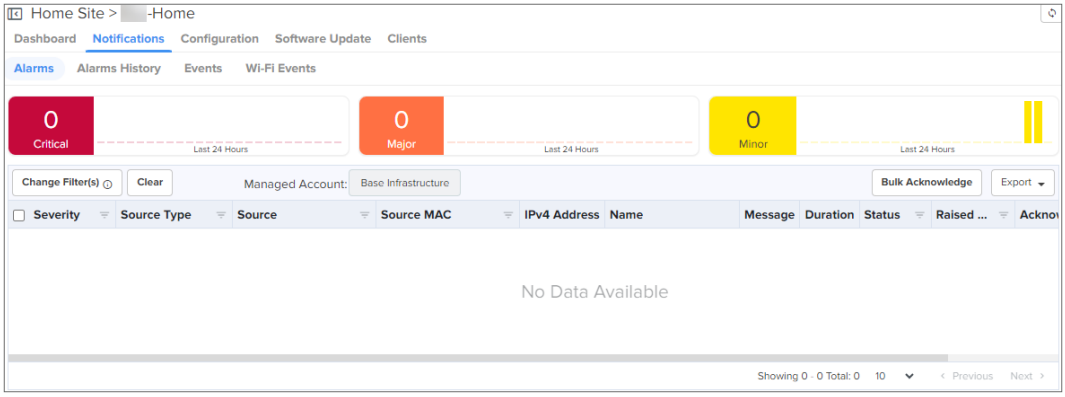
cnMaestro displays the following types of notifications:

- Alarms
- Alarms History
- Events
- Wi-Fi Events

Alarms

The Alarms page displays the number of critical, major, and minor events observed for the Home Mesh Router.You can also view the details of the events, such as severity level, name of the event, time and action taken.

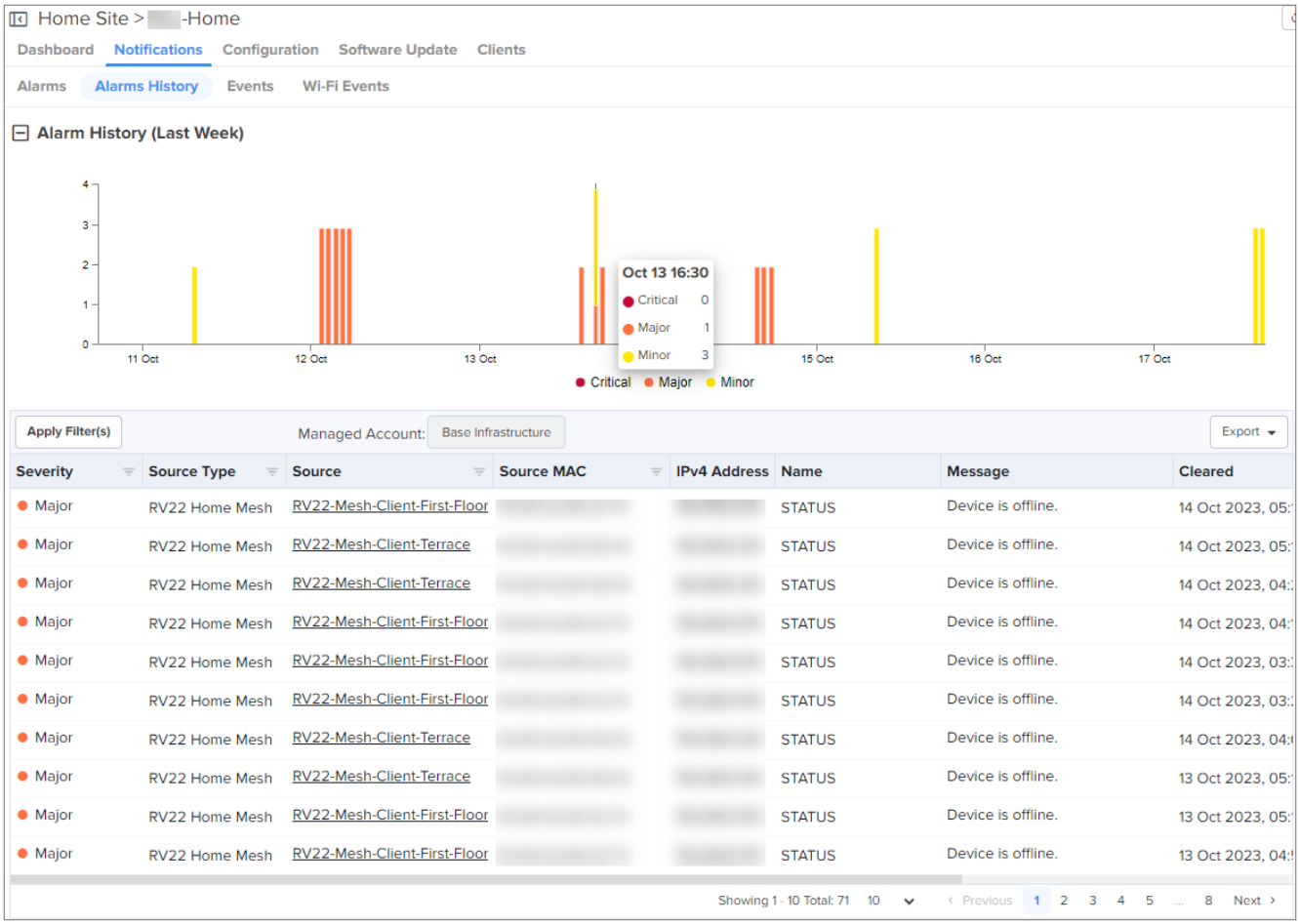
To view the alarms raised, access the **Alarms** page under **Monitor and Manage >** <Home-site-name> **> Notifications > Alarms.**



Alarms History

The Alarms History page displays the number of critical, major, and minor events observed in the previous week.

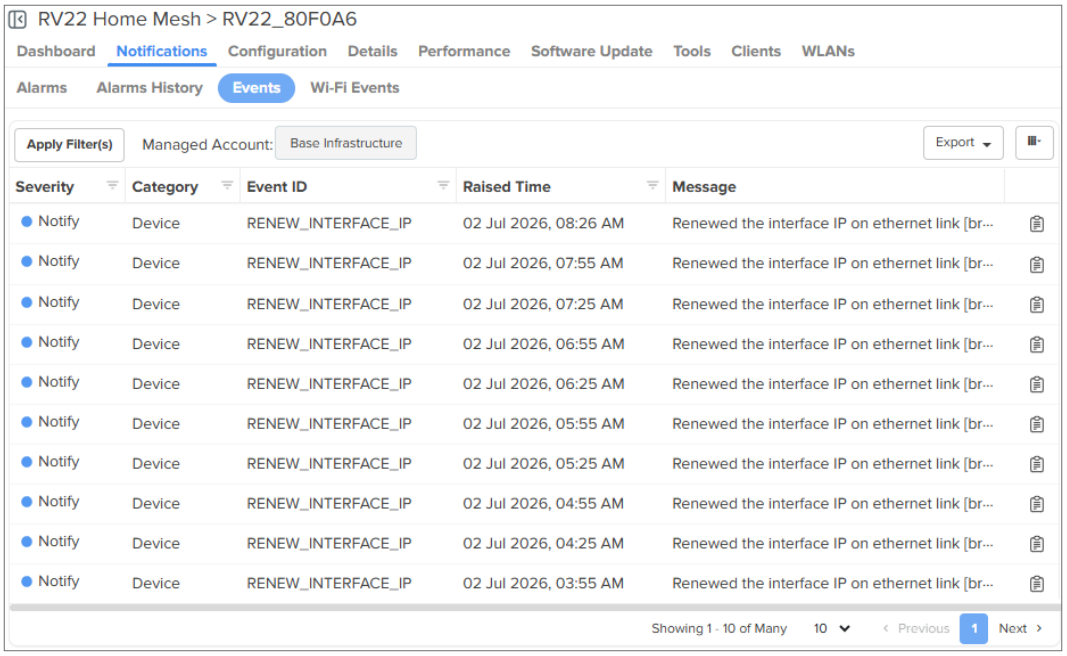
To view the alarms history displayed as a graphical representation, access the **Alarms History** page under **Monitor and Manage >** <Home-site-name> **> Notifications > Alarms History**.



Events

The Events page displays Home Mesh Router-related events, such as its status, if there were any changes in bandwidth, and when the DHCP server IP was assigned to the connected clients.

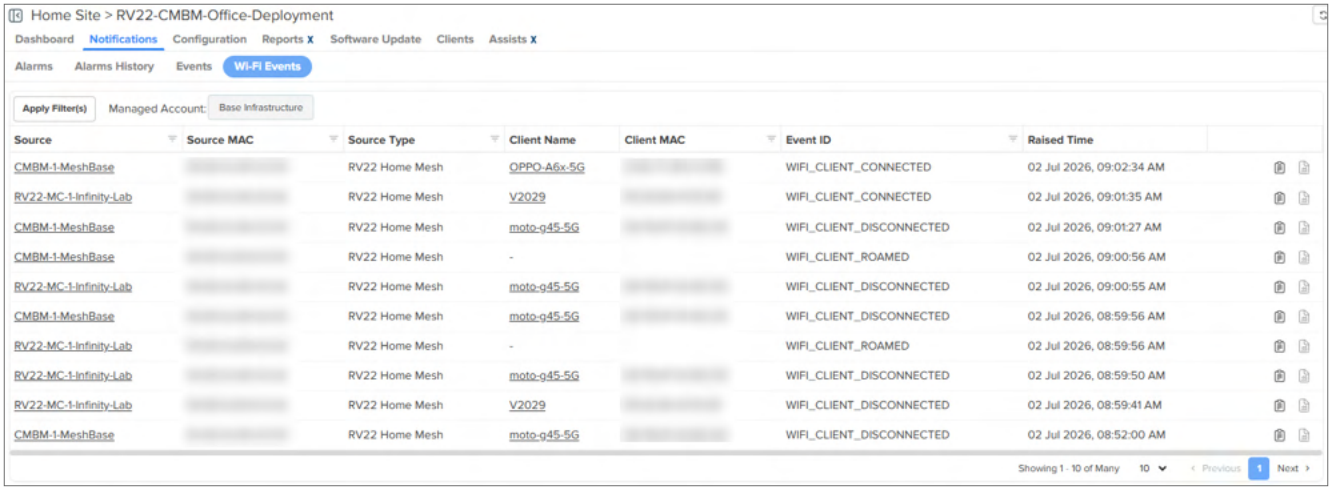
To view the events, access the **Events** page under **Monitor and Manage >** <Home-site-name> **> Notifications > Events**.



Wi-Fi Events

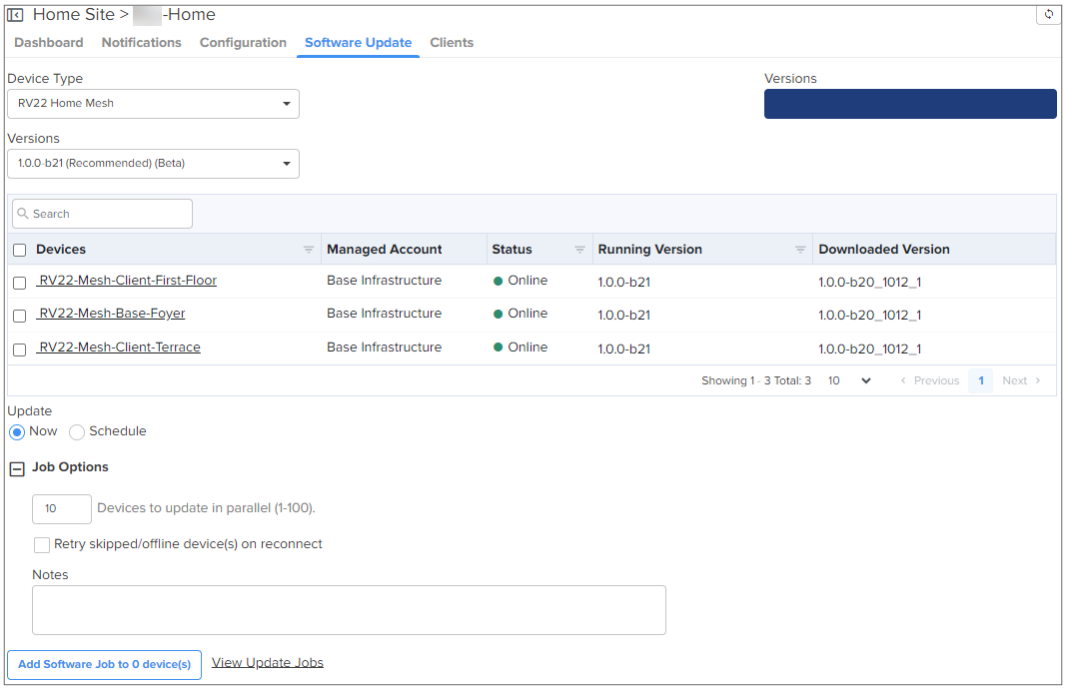
The Wi-Fi Events page displays client-related events, such as when the client connected to the network, when it was disconnected, and authentication events.

To view the Wi-Fi events, access the **Wi-Fi Events** page under **Monitor and Manage >** <Home-site-name> **> Notifications > Wi-Fi Events**.



Software Update

To upgrade the router firmware, go to the **Software Update** page. See Upgrading the Home Mesh Router firmware for more information.



Performance

To view the performace of the router, access the **Wi-Fi Events** page under **Monitor and Manage >** <Home-Mesh-Router-name> **> Performance**.

The page displays the following graphical information:

Table 121 *Performance page graphs—Base and Node routers*

Parameter	Description	Router (Base / Node / Both)
Stacked WAN Throughput	Hourly throughput for both downlink and uplink in the WAN interface for each band of the mesh base router.	Base only
Stacked Throughput by Band (Downlink)	Downlink speed in each band.	Both
Stacked Throughput by Band (Uplink)	Uplink speed in each band.	Both
Stacked Clients by Band	Count of number of clients connected in each band.	Both
Noise Floor	Amount of background noise (in dBm) or interference created by devices in the same frequency.	Both
Interference	Interefence (in dBm) caused by other wireless signals and devices interrupting the router's Wi-Fi signal.	Both
Airtime 2.4 GHz	Capacity utilization (in %) of the 2.4 GHz band for effective transmission.	Both
Airtime 5 GHz	Capacity utilization (in %) of the 5 GHz band for effective transmission.	Both
Available Memory	Amount of router memory (in %) available for use.	Both
CPU	Router CPU utilization in percentage (%).	Both

Parameter	Description	Router (Base / Node / Both)
SNR *	Minimum, average, and maximum SNR values (in dB) for the mesh node router.	Node only
RSSI *	Received Signal Strength Indicator (RSSI) value (in dBm) for the mesh node router.	Node only
Data Rate *	Minimum, average, and maximum data rates (in Mbps or Gbps) provided by the mesh node router to the client devices.	Node only

Note

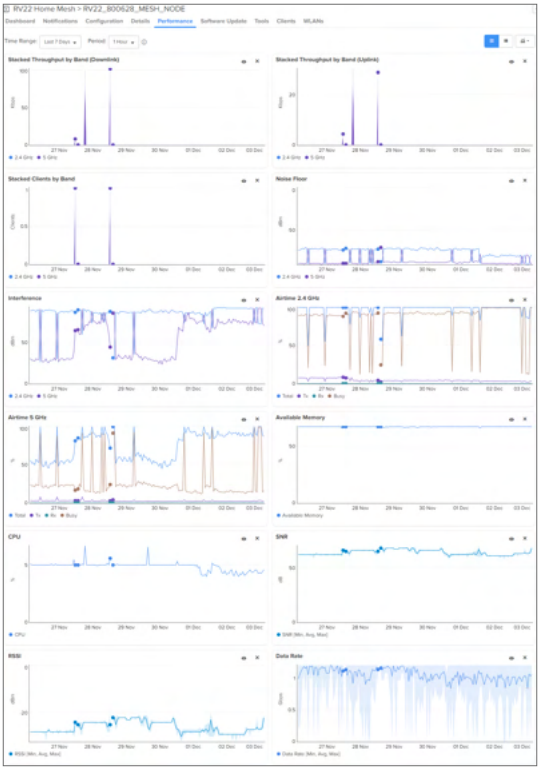
* The SNR, RSSI, and Data Rate performance graphs are displayed only for those nodes that are connected through a wireless mesh link.

Following are sample performance graphs for base and node routers:

- Performance of the base router in a mesh deployment



- Performance of the node router in a mesh deployment



Troubleshooting the Home Mesh Router

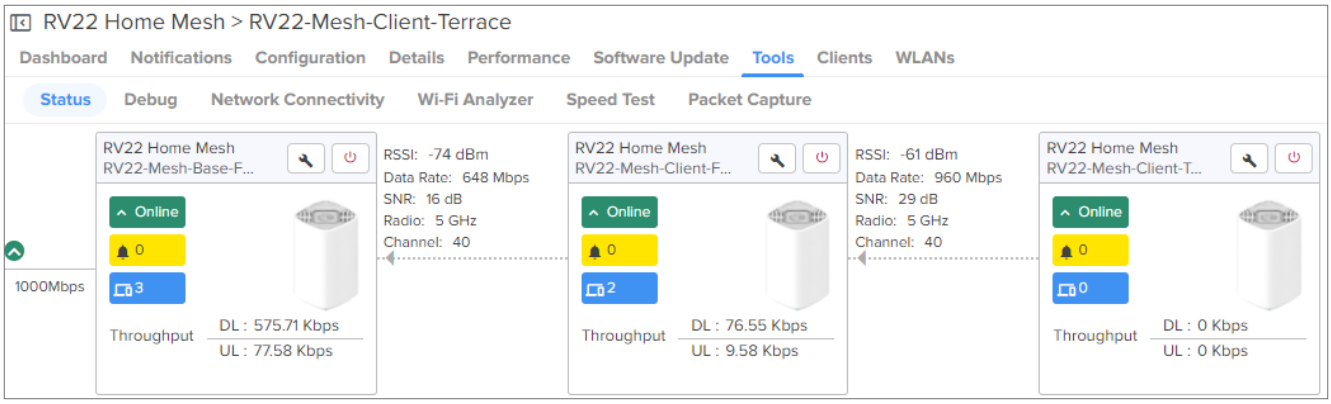
cnMaestro provides the following troubleshooting options for the router:

- Status
  - Downloading tech support file
- Debug
- Network Connectivity
- Wi-Fi Analyzer
- Speed Test
- Packet Capture

Status

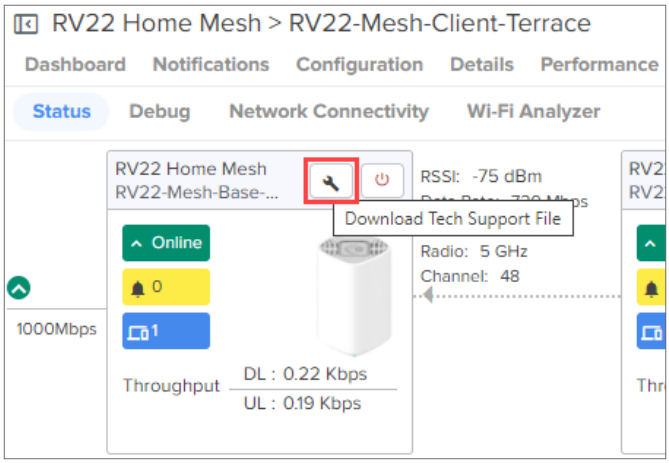
The Status page displays the status of link between the Home Mesh Router base and client devices.

To view the status of the link between the Home Mesh base and client devices, access the **Status** page under **Monitor and Manage** > <Home-Mesh-Router-name> > **Tools.**



Downloading tech support file

To download the tech support file, click the Download Tech Support File ( ) icon on the **Status** page.

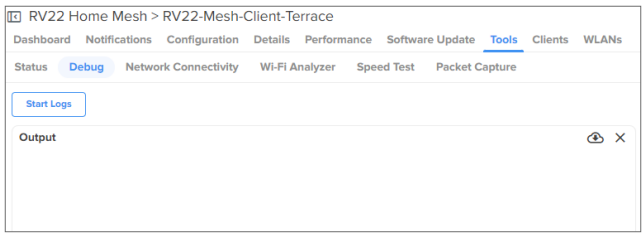


Debug

The Debug page displays log information of the Home Mesh Router. To view the debug information, complete the following steps:

1. Navigate to the **Monitor and Manage >** <Home-Mesh-Router-name> **> Tools** > **Debug** tab.
2. Click **Start Logs**.

   The log information is displayed in the **Output** window.



Network Connectivity

The Network Connectivity page provides network connectivity information of the Home Mesh Routers.

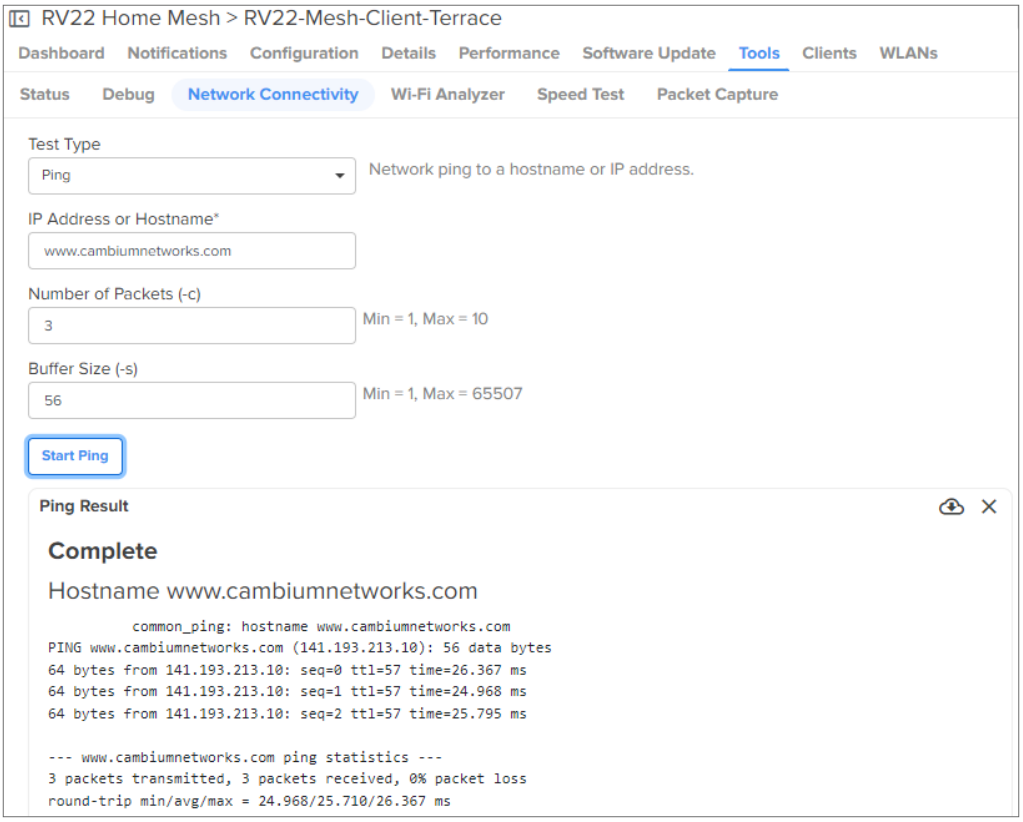
cnMaestro supports the following tests to provide connectivity information for the Home Mesh Routers:

- Ping
- DNS Lookup
- Traceroute

To test network connectivity of the router, complete the following steps:

1. Navigate to the **Monitor and Manage >** <Home-Mesh-Router-name> **> Tools** > **Network Connectivity** tab.
2. Select the required test type from the **Test Type** dropdown list and configure the corresponding parameters required for the test.
3. Click **Start Test**.

   cnMaestro initiates the test and displays the result in the **<Test Type> Result** window.



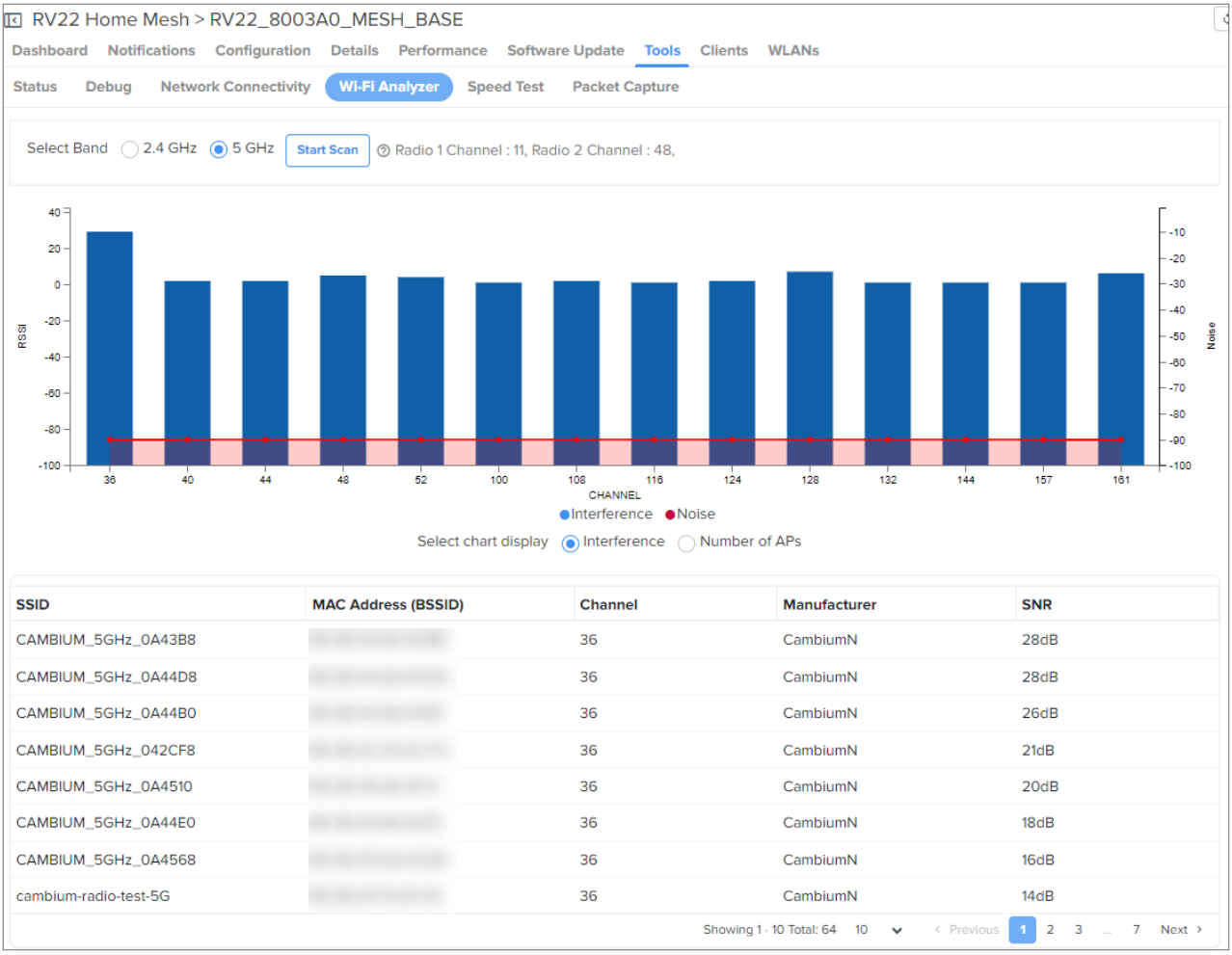
Wi-Fi Analyzer

The Wi-Fi Analyzer page displays radio traffic and signal information for the selected band. It displays the interference and noise measured for the selected band.

To view the Wi-Fi Analyzer details, complete the following steps:

1. Navigate to the **Monitor and Manage >** <Home-Mesh-Router-name> **> Tools** > **Wi-Fi Analyzer** tab.
2. Select the required band (2.4 or 5 GHz).
3. Click **Start Scan**.

cnMaestro analyzes the band and displays the result in a table.



Speed Test

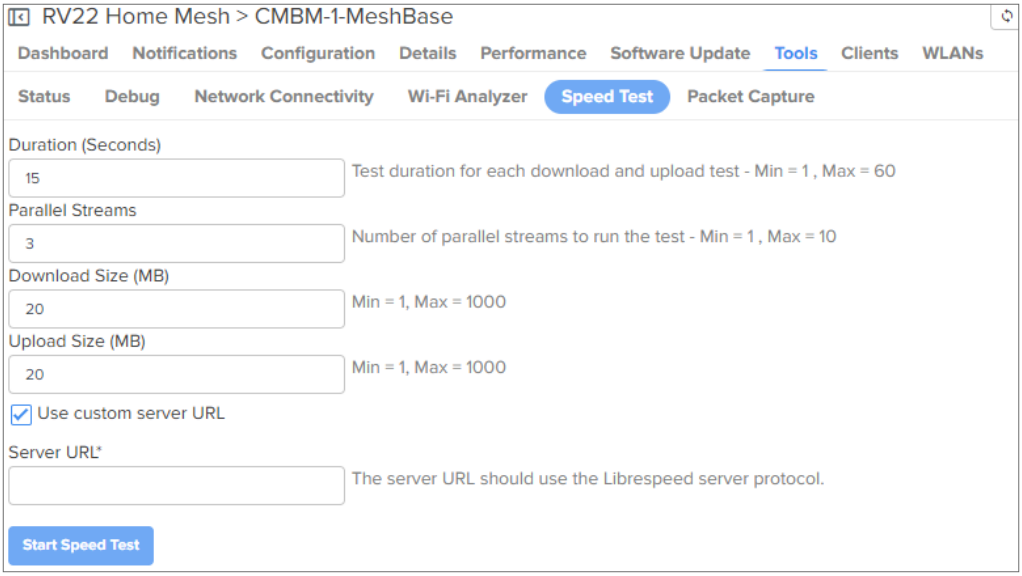
The Speed Test page displays the internet speed provided by the Home Mesh Router.

To know the speed of the router, complete the following steps:

1. Navigate to the **Monitor and Manage >** <Home-Mesh-Router-name> **> Tools** > **Speed Test** tab.
2. Configure the required values for testing the speed.

   To use a custom server URL, select the **Use custom server URL** checkbox and provide the server URL that uses a LibreSpeed server protocol.
3. Click **Start Speed Test**.

cnMaestro checks the speed and displays both download and upload speeds in megabits per second (Mbps).

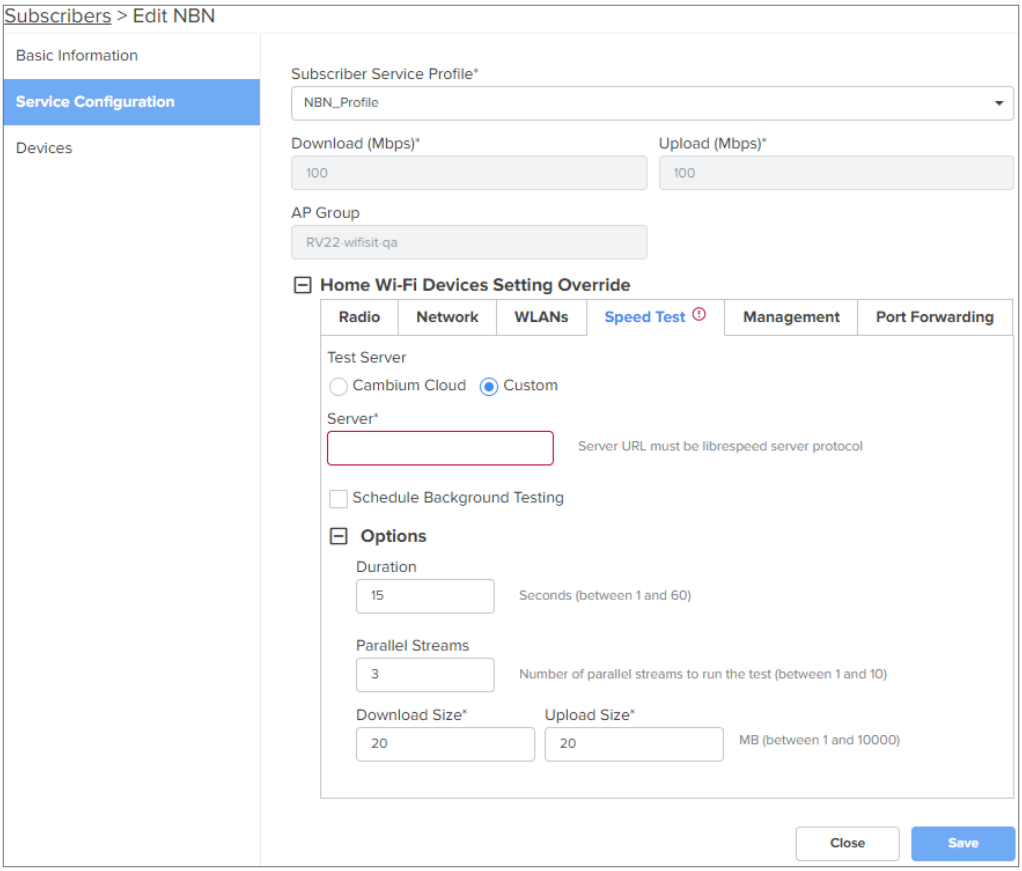


The speed test option is also available on the **Subscriber** page in the **Home Wi-Fi Devices Setting Override** section.

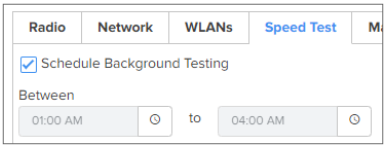
To avail this speed test option, complete the following steps:

1. Navigate to the **Manage Service Providers** > **Managed Subscribers** > **Subscribers** tab.
2. From the list of subscribers, click the subscriber name for which you want to configure the speed test.

   The **Edit <Susbcriber-name>** window is displayed.
3. Click the **Service Configuration** tab.
4. In the **Home Wi-Fi Devices Setting Override** section, click the **Speed Test** tab.



5. Select the test server from the following:
   - Cambium Cloud
   - Custom—Provide a custom server URL, which must use the LibreSpeed server protocol.
6. To schedule the speed test at a particular duration, select the **Schedule Background Testing** checkbox.
7. Select the start and end time for performing the speed test on the router.



Packet Capture

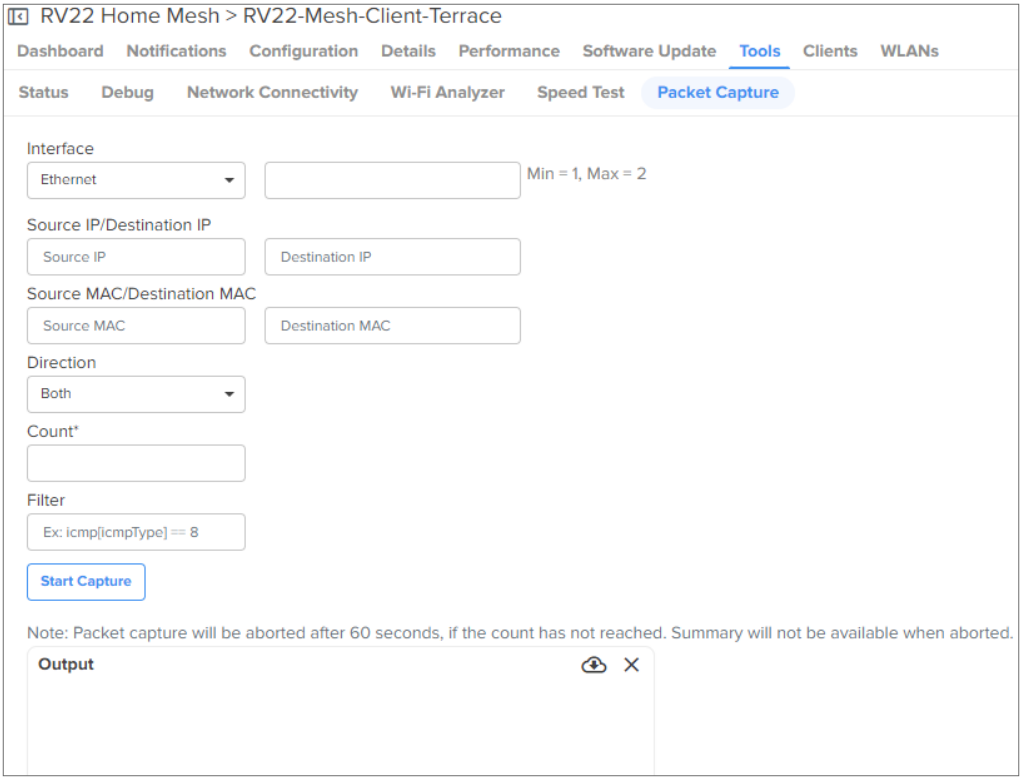
The Packet Capture page allows the user to capture all packets on a specified interface.

To capture packet data, complete the following steps:

1. Navigate to the **Monitor and Manage >** <Home-Mesh-Router-name> **> Tools** > **Packet Capture** tab.
2. Select the required interface, and provide the source and destination IP address or MAC address.
3. Provide the number of packets that must be captured.
4. Click **Start Capture**.

   cnMaestro displays the information in the **Ouput** window.

5. To download the PCAP file, click the download ( ) icon.



Upgrading the Home Mesh Router firmware

To upgrade the firmware of Home Mesh routers present in a home site, complete the following steps:

1. Navigate to **Monitor and Manage >** <Home-site-name> **> Software Update**.

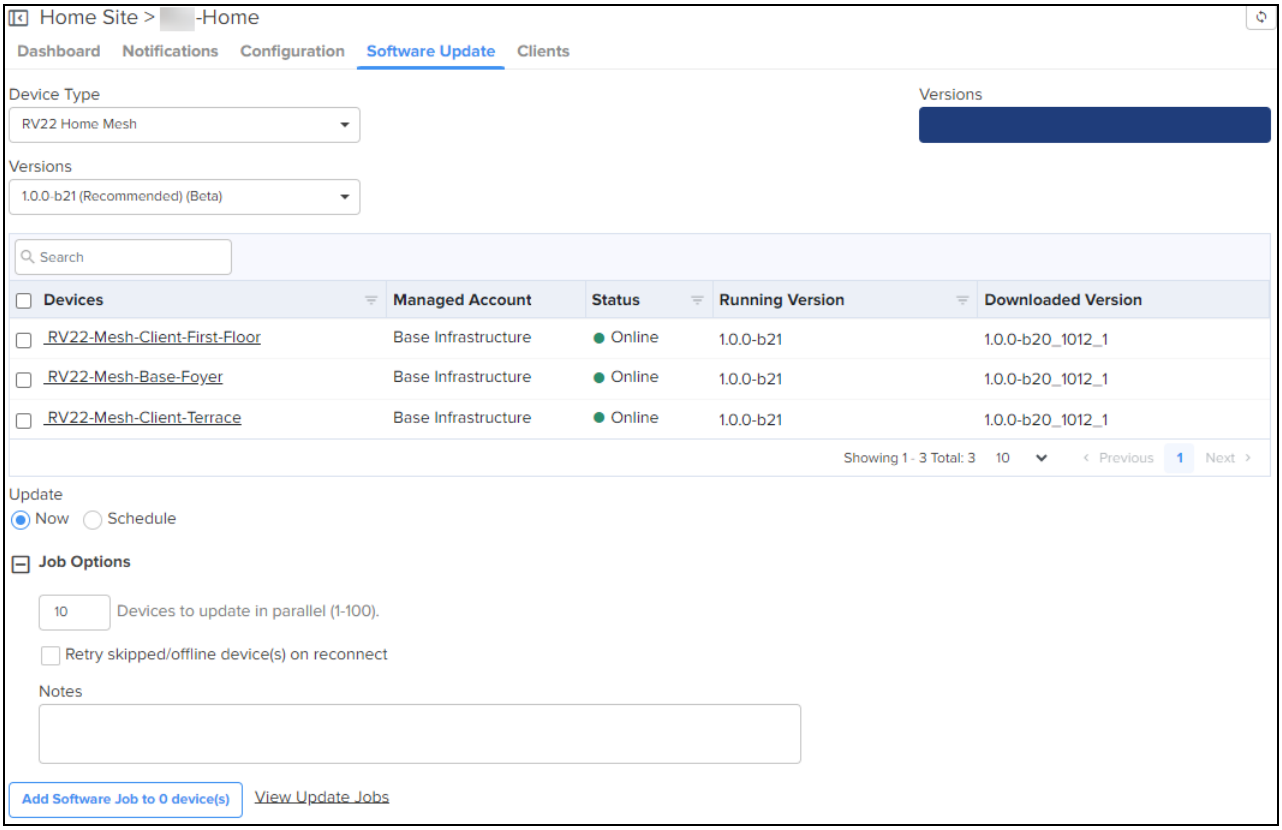
   The Software Update page appears.
2. Select **RV22 Home Mesh** from the **Device Type** dropdown list.
3. Select the software version from the **Versions** dropdown list.
4. In the list of devices table, select the checkboxes corresponding to the devices for which you want to upgrade the firmware.

   You can also select one router to upgrade the firmware of only that router.
5. Select the **Now** option in the **Update** field to upgrade the firmware immediately.

   To schedule the upgrade job, select the **Schedule** option and configure the required date and time.
6. Click **Add Software Job to** <number of devices> **device(s)**.

   The upgrade is scheduled to run at the specified date and time.

To view the status of the update jobs, click **View Update Jobs**.



Assurance X

This chapter covers the following topics:

- Assurance X
- Overview
- Use cases
  - Resolve connectivity issues
  - Analyzing Connection Failures of Wi-Fi Clients and Poor Performance of Wi-Fi Networks
  - Analyzing Connection Failures of Wi-Fi Clients and Poor Performance of Wi-Fi Networks
  - Address poor performance of applications
  - Analyzing Connection Failures of Wi-Fi Clients and Poor Performance of Wi-Fi Networks
  - Identify OS, SSID, and AP-specific issues
- Accessing the Assurance X page
- Accessing Site-level consolidated details at the System- and MSP-levels
- Setting filters to view the connection data
  - Suppressed clients
    - Classifying clients as suppressed
    - Viewing suppressed clients and events
    - Removing a manually suppressed client from the Suppressed Clients list
- Viewing the connection events
  - Dashboard page
  - Assurance X page
    - Connection tab
    - Disconnection tab
    - Viewing hourly data and corresponding events
    - Viewing a client or host-specific connection or disconnection event
    - Viewing an event-based connection or disconnection event
    - Viewing AP-specific information

Analyzing Connection Failures of Wi-Fi Clients and Poor Performance of Wi-Fi Networks

The Wi-Fi Assurance X feature provides deep visibility into the health of Wi-Fi client connections, including root cause analysis of failures and possible remediations. It also provides analytics on aggregated data that can help to improve client connectivity in the Wi-Fi network.

Overview

The Assurance X feature analyzes the Wi-Fi client connection events and helps to troubleshoot common network connectivity and performance issues such as the following:

- **Connectivity**—Association, authentication, and network connectivity failures.
- **Poor Performance**—Low RSSI, low data rate, high retry rate, and high latency in AAA, DHCP, DNS, and applications.

You can use this feature to detect and analyze common network problems that occur in your wireless networks.



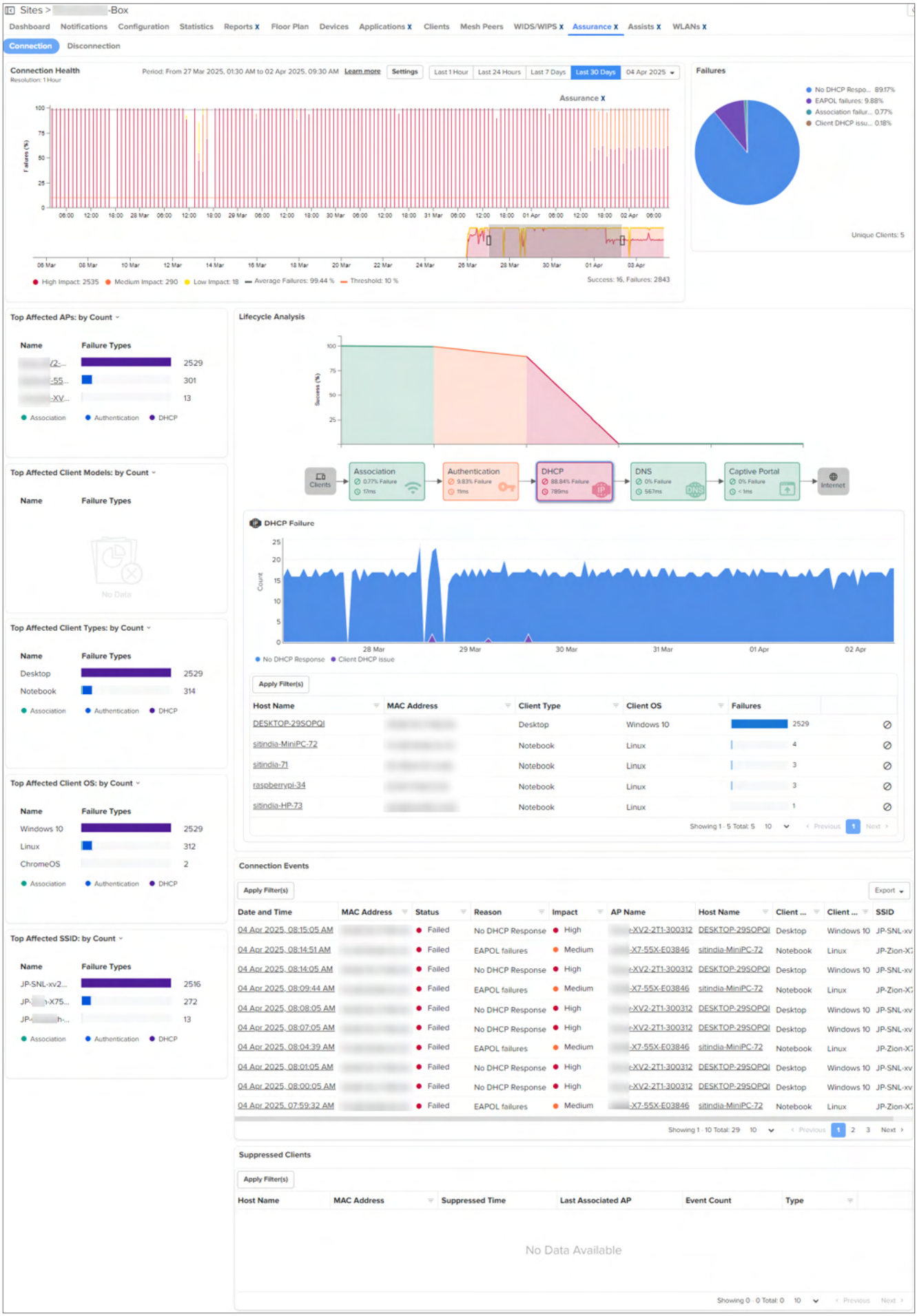
Note

Assurance X is supported only for XV and XE devices.

The **Assurance X** page reports the following data for the Wi-Fi clients:

- Statistics of successful connections per connection type such as new, reconnection, and roaming.
- Statistics of failed connections and disconnections, such as reason codes for association, EAP/EAPOL handshake, DHCP, DNS, and Captive Portal failures.

Figure 538 *The Assurance X page*


Sites > -Box
Dashboard
Notifications
Configuration
Statistics
Reports X
Floor Plan
Devices
Applications X
Clients
Mesh Peers
WIDS/WIPS X
Assurance X
Assists X
WLANs X
Connection
Disconnection
Connection Health
Resolution: 1 Hour
Period: From 27 Mar 2025, 01:30 AM to 02 Apr 2025, 09:30 AM
Learn more
Settings
Last 1 Hour
Last 24 Hours
Last 7 Days
Last 30 Days
04 Apr 2025
Assurance X
Failures (%)
High Impact: 2535
Medium Impact: 290
Low Impact: 18
Average Failures: 99.44 %
Threshold: 10 %
Success: 16, Failures: 2843
Failures
No DHCP Respo... 89.17%
EAPOL failures: 9.88%
Association failur... 0.77%
Client DHCP issu... 0.18%
Unique Clients: 5
Top Affected APs: by Count
Name
Failure Types
2529
301
13
Association
Authentication
DHCP
Top Affected Client Models: by Count
No Data
Top Affected Client Types: by Count
Desktop
Notebook
314
Top Affected Client OS: by Count
Windows 10
Linux
312
ChromeOS
2
Top Affected SSID: by Count
JP-SNL-xv2...
2516
272
13
Lifecycle Analysis
Success (%)
Clients
Association
0.77% Failure
17ms
Authentication
9.83% Failure
11ms
DHCP
88.84% Failure
789ms
DNS
0% Failure
567ms
Captive Portal
0% Failure
< 1ms
Internet
DHCP Failure
Count
28 Mar
29 Mar
30 Mar
31 Mar
01 Apr
02 Apr
No DHCP Response
Client DHCP issue
Apply Filter(s)
Host Name
MAC Address
Client Type
Client OS
Failures
DESKTOP-29SOPQI
Desktop
Windows 10
2529
sitindia-MiniPC-72
Notebook
Linux
4
sitindia-71
3
raspberrypi-34
sitindia-HP-73
1
Showing 1 - 5 Total: 5
Previous
Next
Connection Events
Export
Date and Time
Status
Reason
Impact
AP Name
Host Name
Client ...
SSID
04 Apr 2025, 08:15:05 AM
Failed
No DHCP Response
High
DESKTOP-29SOPQI
Windows 10
JP-SNL-xv
04 Apr 2025, 08:14:51 AM
EAPOL failures
Medium
sitindia-MiniPC-72
Linux
04 Apr 2025, 08:14:05 AM
04 Apr 2025, 08:09:44 AM
04 Apr 2025, 08:08:05 AM
04 Apr 2025, 08:07:05 AM
04 Apr 2025, 08:04:39 AM
04 Apr 2025, 08:01:05 AM
04 Apr 2025, 08:00:05 AM
04 Apr 2025, 07:59:32 AM
Showing 1 - 10 Total: 29
Suppressed Clients
Host Name
MAC Address
Suppressed Time
Last Associated AP
Event Count
Type
No Data Available
Showing 0 - 0 Total: 0

Use cases

Following are some of the **use cases**, to identify the connectivity issue and analyze the root cause:

Resolve connectivity issues

The **Assurance X** page provides visual analytics of client connection failures in each phase such as baseline performance and key metrics in the form of graphs and tables with multiple data filters. You can easily identify the root cause based upon the phase of the Wi-Fi connection lifecycle.

- **Association**—Accessing the AP may fail if the client has low RSSI; if the request for capabilities is not supported by the AP; or if the AP is already handling the maximum number of clients.
- In such cases, you can use the **Lifecycle Analysis** widget on the **Assurance X** page. This widget displays the statistics of 802.11 authentication and association failures in percentage. In addition, you can use the **Events** page to analyze the reason, cause, impact, and the recommended action.
- **Authentication**—Authentication may fail when 802.1X or EAP key is incorrect; the RADIUS server cannot be reached; or the WPA2-PSK or WPA3-SAE key derivation is invalid.
- In such cases, the **Lifecycle Analysis** widget displays the RADIUS authentication failure count in percentage.
- **Network connection**—When a client is successfully authenticated, it must be assigned an IP address by the DHCP server and provided networking information such as for DNS and Gateway. When the DHCP server fails, connectivity to the network cannot be established.
- In such cases, the **Lifecycle Analysis** widget can help identify that the DHCP server failure, and the **Events** page can analyze the reason and cause.
- **Aggressive roaming**—Time sensitive applications such as voice and video require uninterrupted connectivity. To ensure this, Wi-Fi clients monitor the RSSI from local APs and probe better APs when the connection degrades. The RSSI threshold at which a client moves from the current AP to another AP may be different for each client and is vendor specific. Some clients may have aggressive roaming where they move frequently across APs. This can result in increased contention in the network and longer delay for other clients connecting or transmitting data. The client drill down presents the association, authentication, and network connectivity events generated due to aggressive roaming.
- You can use the **Lifecycle** page to analyze the RSSI ranges, roam quality, and lifecycle events.
- **DHCP, AAA, or DNS latency**—Each of the association, authentication, and network connectivity stages might add latency to the total connection time.
- The **Lifecycle Analysis** widget and the **Events** page display statistics for the DHCP, AAA, and DNS latencies.

Address poor performance of applications

Wi-Fi clients may use a wide range of advanced video coding (AVC) applications such as Google Meet, Microsoft Teams, Zoom, Skype, YouTube, and multiple e-commerce applications such as Flipkart and Amazon. In such scenarios, clients may experience poor network performance or network disconnection due to low RSSI or bad roam quality.

You can view the **Session Timeline** section in the **Lifecycle** page to analyze the RSSI ranges, and events such as success, failed, connected, disconnected, and roam quality. This analysis helps you to understand the cause and take recommended actions.

Identify OS, SSID, and AP-specific issues

Apart from run-time metrics, the **Connection Health** widget provides filters to identify performance issues with a specific vendor, operating system, and associated AP and SSID.

Accessing the Assurance X page

To access the Assurance X page:

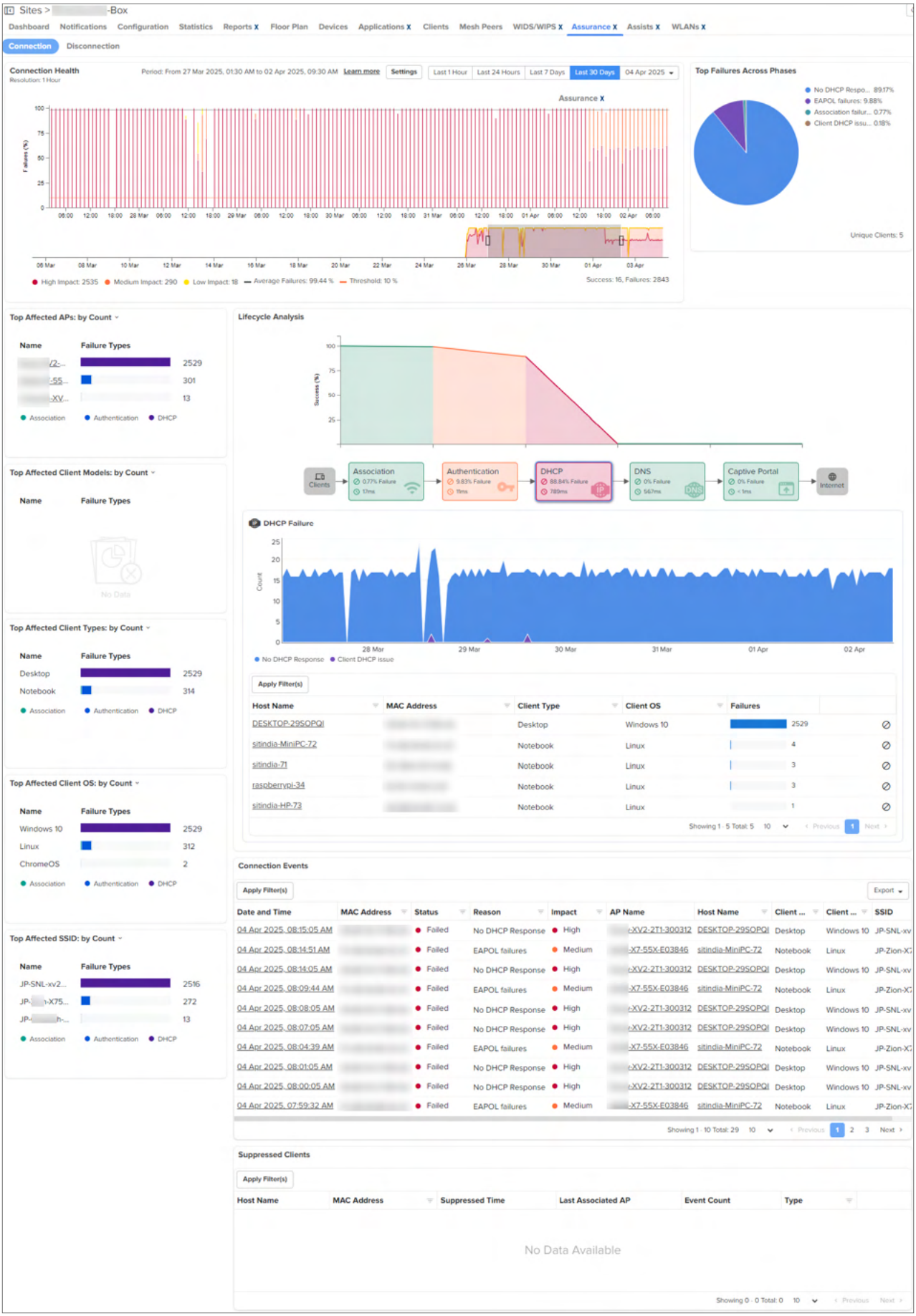
1. On the left navigation pane, click the **Monitor and Manage** () icon.
2. In the **Networks** tab, select either a **System, MSP,** or **Network,** and then a **Site** node in the tree.

   Note

   The **Assurance X** page is available only at the site and client levels.

   The **Dashboard** tab displays the default Wi-Fi connection statistics.
3. Click the **Assurance X** tab.

The **Assurance X** > **Connection** page is displayed.


Sites > -Box
Dashboard
Notifications
Configuration
Statistics
Reports X
Floor Plan
Devices
Applications X
Clients
Mesh Peers
WIDS/WIPS X
Assurance X
Assists X
WLANs X
Connection
Disconnection
Connection Health
Resolution: 1 Hour
Period: From 27 Mar 2025, 01:30 AM to 02 Apr 2025, 09:30 AM
Learn more
Settings
Last 1 Hour
Last 24 Hours
Last 7 Days
Last 30 Days
04 Apr 2025
Assurance X
Failures (%)
High Impact: 2535
Medium Impact: 290
Low Impact: 18
Average Failures: 99.44 %
Threshold: 10 %
Success: 16, Failures: 2843
Top Failures Across Phases
No DHCP Respo... 89.17%
EAPOL failures: 9.88%
Association failur... 0.77%
Client DHCP issu... 0.18%
Unique Clients: 5
Top Affected APs: by Count
Name
Failure Types
2529
301
13
Association
Authentication
DHCP
Top Affected Client Models: by Count
No Data
Top Affected Client Types: by Count
Desktop
Notebook
314
Top Affected Client OS: by Count
Windows 10
Linux
312
ChromeOS
2
Top Affected SSID: by Count
JP-SNL-xv2...
2516
272
13
Lifecycle Analysis
Success (%)
Clients
Association
0.77% Failure
17ms
Authentication
9.83% Failure
19ms
DHCP
88.84% Failure
789ms
DNS
0% Failure
567ms
Captive Portal
0% Failure
< 1ms
Internet
DHCP Failure
Count
28 Mar
29 Mar
30 Mar
31 Mar
01 Apr
02 Apr
No DHCP Response
Client DHCP issue
Apply Filter(s)
Host Name
MAC Address
Client Type
Client OS
Failures
DESKTOP-29SOPQI
Desktop
Windows 10
2529
sitindia-MiniPC-72
Notebook
Linux
4
sitindia-71
3
raspberrypi-34
sitindia-HP-73
1
Showing 1 - 5 Total: 5
Previous
Next
Connection Events
Export
Date and Time
Status
Reason
Impact
AP Name
Host Name
Client ...
SSID
04 Apr 2025, 08:15:05 AM
Failed
No DHCP Response
High
DESKTOP-29SOPQI
Windows 10
JP-SNL-xv
04 Apr 2025, 08:14:51 AM
EAPOL failures
Medium
sitindia-MiniPC-72
JP-Zion-X
04 Apr 2025, 08:14:05 AM
04 Apr 2025, 08:09:44 AM
04 Apr 2025, 08:08:05 AM
04 Apr 2025, 08:07:05 AM
04 Apr 2025, 08:04:39 AM
04 Apr 2025, 08:01:05 AM
04 Apr 2025, 08:00:05 AM
04 Apr 2025, 07:59:32 AM
Showing 1 - 10 Total: 29
Suppressed Clients
Host Name
MAC Address
Suppressed Time
Last Associated AP
Event Count
Type
No Data Available
Showing 0 - 0 Total: 0

Accessing Site-level consolidated details at the System- and MSP-levels

cnMaestro allows you to access consolidated information from all sites located in an account- or at the MSP-level. The information is displayed in a tabular format including details, such as the Managed Account name, the network to which the site belongs, failure threshold and what percentage of events have crossed this threshold, and the high, medium, and low impact events.

Note

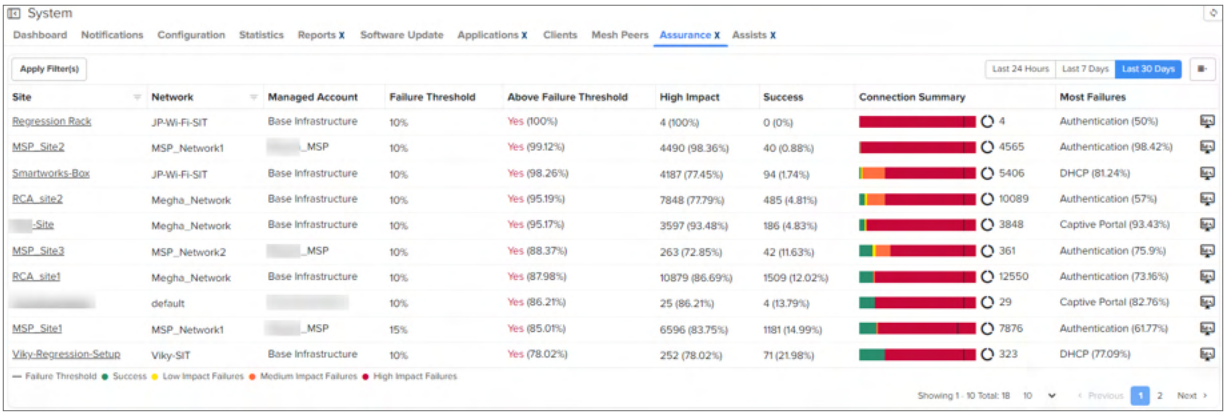
Consolidated information from all sites at the System- and MSP-levels are available only for those sites where devices are onboarded and clients are connected.

To view consolidated site-level information, complete the following steps:

1. Navigate to **Monitor and Manage**.
2. In the **Networks** tab, select one of the following options:
   - To view account-level information, click **System** > **Assurance X**.

     The **Assurance X** page is displayed with consolidated information from all the sites in that account. At the system-level, data is aggregated from all sites including sites under MSP accounts. However, at the MSP-level, data is aggregated from only those sites under the MSP account.

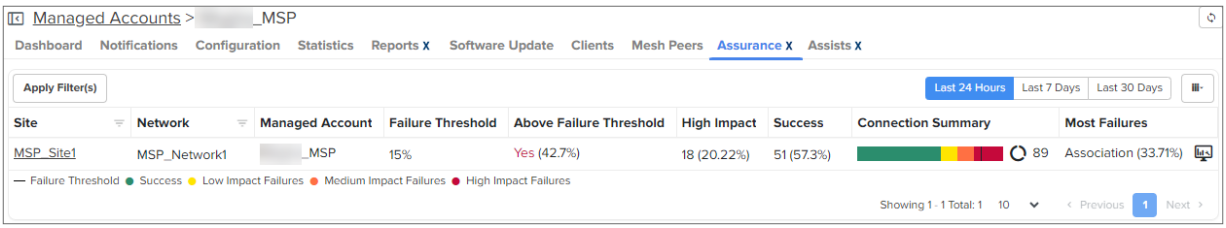
     Figure 539 *System-level information from all sites and MSP accounts*



   - To view MSP-level information, click ***<MSP-Name>*** > **Assurance X**.

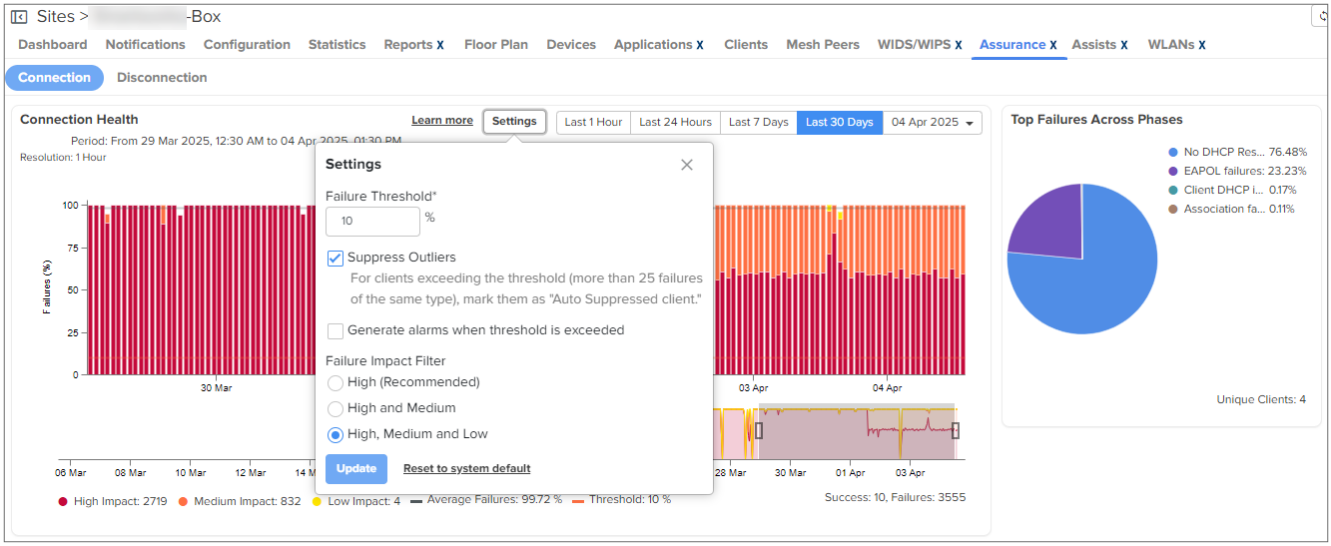
     The **Assurance X** page is displayed with consolidated information about from all the sites in that account.

     Figure 540 *MSP-level information from all sites in that MSP*



Setting filters to view the connection data

After accessing the **Assurance X** page, you may change the default threshold for failed connections and set the period to view the connection events such as 1 hour, 24 hours, 7 days, or 30 days.



To set failure threshold and period:

1. Navigate to the **Connection** tab
2. Click **Settings** located inside the **Connection Health** widget.
3. Enter the **Failure Threshold**.

   The default value is 10% and higher. To reset the threshold, click **Reset to system default**.
4. Select or clear the **Suppress Outliers** checkbox to exclude or include, respectively, the suppressed clients from the **Connection Health** dashboard.

   When enabled (by default), cnMaestro suppresses or excludes those clients that are repeatedly generating the same type of failures from the **Connection Health** dashboard.

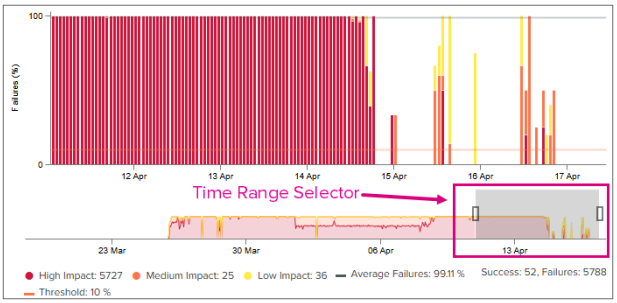
   For more information about suppressed clients, see Suppressed clients.
5. Select the **Generate alarms when threshold is exceeded** checkbox to generate a System Alarm whenever the threshold is surpassed.
6. Select the **Failure Impact Filter** as one of the following options:
   - High (Recommended)
   - High and Medium
   - High, Medium and Low

   Default value: **High (Recommended)**
7. To apply the configuration changes, click **Update**.
8. To view the connection or disconnection events for a specific period, click one of the following options:
   - Last 1 Hour
   - Last 24 hours (Resolution 1 Hour)
   - Last 7 days (Resolution 1 Hour)

- Last 30 days (Resolution 1 Hour)—Data is available for the last 30 days. However, at any instance the data displayed in the **Connection Health** graph is for a maximum of seven days only.

  The smaller graph below the main graph displays data for the last 30 days. Set the duration by dragging the time range selector as shown in the following figure.

  Minimum days to be selected in the selector is one. Maximum is seven days.

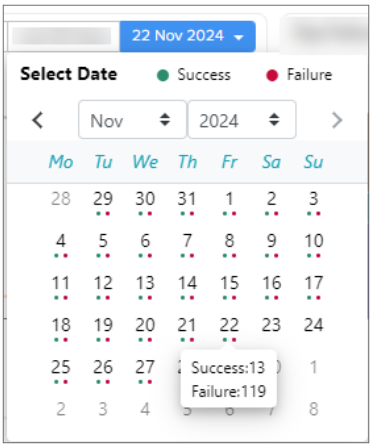


- **Date**—To view the connection or disconnection data for a specific date, select the required date from the date picker.

  You can select a date upto last 30 days.

  In the date picker dropdown, hover over a date to view the success and failure counts on that date.

Figure 541 *Date picker*



Based on the failure threshold, failure Impact filter, and the period, the **Dashboard** and **Assurance X** pages display the Wi-Fi client's connection data. Whenever the failure percentage exceeds the configured failure threshold, the Assurance X page automatically generates alerts.

Note

Consider the following key points specific to impact level failures:

- **High impact failure**—Occurs when a client is unable to establish a connection with an access point or transmit data over a connection. These failures are typically permanent until the underlying problem is resolved. High impact failures include incorrect pre-shared key (PSK); the VLAN not being configured or present on the switch; and AP software issues.
- **Medium impact failure**—Occurs when a client is intermittently unable to connect to a network, and the time to connect is relatively short (sub-seconds). These failures may not be noticed by end users. They are caused by transient issues such as the moving client or when an access point locks the necessary information during the initial connection attempt. Medium impact failure events include fast transition (FT); authentication failure; missed packets during the four-way handshake; DHCP request process; or momentary interference from other wireless devices.

- **Low impact failure**—Occurs when a client is unable to connect to a network, without causing any noticeable impact for end users. These failures may arise due to specific wireless LAN features or configurations, such as band steering. These failures are expected, based upon the Wireless LAN protocols, and do not impact the user experience. In some cases, adjusting WLAN configuration can resolve such failure issues.

Suppressed clients

When a client attempts to connect to an AP, failures may occur. If a few clients repeatedly experience the same failure, they can disproportionately increase the overall failure percentage in site-level analytics, leading to misleading data. To address this, cnMaestro classifies such clients as suppressed clients and exclude their failure events from the site-level analytics data.

This section describes the following topics:

- Classifying clients as suppressed
- Viewing suppressed clients and events
- Removing a manually suppressed client from the Suppressed Clients list

Classifying clients as suppressed

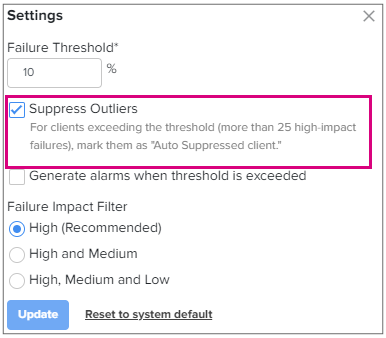
Clients can be classified as suppressed clients in one of the following ways:

- Automatically suppressed clients—When a client generates 25 high-impact failure events within one hour (regardless of other failure events that may occur in that duration), cnMaestro automatically classifies the client as Auto Suppressed client and adds it to the Suppressed Clients list.

  To enable automatic suppressing of clients, select the **Suppress Outliers** checkbox in the **Connection Health** dashboard > **Settings** window.

  Note

  This setting is enabled, by default, for all sites in an account.

  An auto suppressed client remains in the Suppressed Clients list as long as it generates any failure event—high, medium, or low impact. The auto suppressed client cannot be manually removed from the Suppressed Clients list. An auto suppressed client is automatically removed from the Suppressed Clients list when the client:

  - generates a success event, or
  - does not generate any high-impact failure event for an hour

- Manually suppressed clients—A user manually classifies a client that generates a failure event multiple times, as suppressed.

  To manually classify a client as suppressed, click the **Mark as suppressed** (⊘) icon, available for clients listed in the site **Assurance X** page > **Lifecycle Analysis** widget.



Note

- Only successful events generated by manually suppressed clients are included in the site-level analytics data. However, a successful event does not remove the client from the Suppressed Clients list.

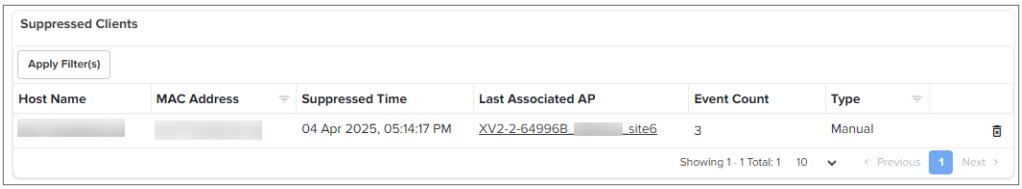
  For removing the manually suppressed clients from the Suppressed Clients list, see Removing a manually suppressed client from the Suppressed Clients list.

- All failure events generated by manually suppressed clients are discarded from the site-level analytics data.

Viewing suppressed clients and events

Suppressed clients and the corresponding failure events are displayed in the following pages in cnMaestro:

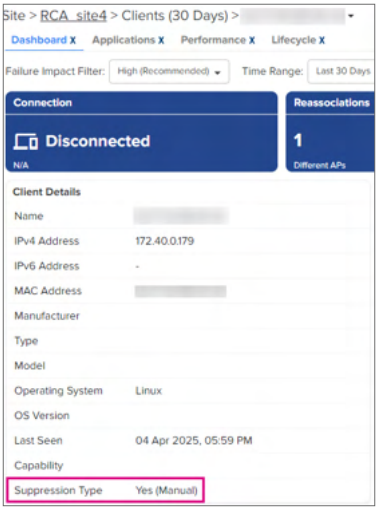
- Site > **Assurance X** > **Connection** dashboard—under the **Suppressed Clients** table—Lists all clients that are suppressed either automatically or manually.



The details of the list are described in the following table:

Filter name	Description
Host Name	Host name of the suppressed client.
MAC Address	MAC address of the suppressed client.
Suppressed Time	Timestamp when the client was suppressed.
Last Associated AP	Host name of the AP to which the suppressed client was last associated with.
Event Count	Number of failure events that were suppressed.
Type	Specifies the type of suppression of the client. The following values are displayed: • Auto—Client is suppressed automatically • Manual—Client is suppressed manually
	Allows to remove the manually suppressed clients from this list.

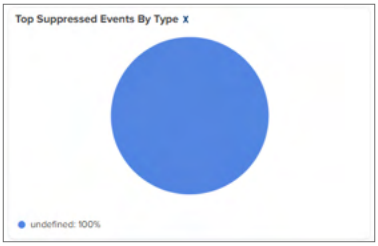
- Client's **Dashboard X** tab
  - **Client Details** section—Displays if the client is suppressed or not in the selected site. If suppressed, it also displays if it suppressed automatically or manually.



  - **Suppressed Failure Events** widget—Displays the percentage of suppressed failure events for each of the sites that the client is associated with.

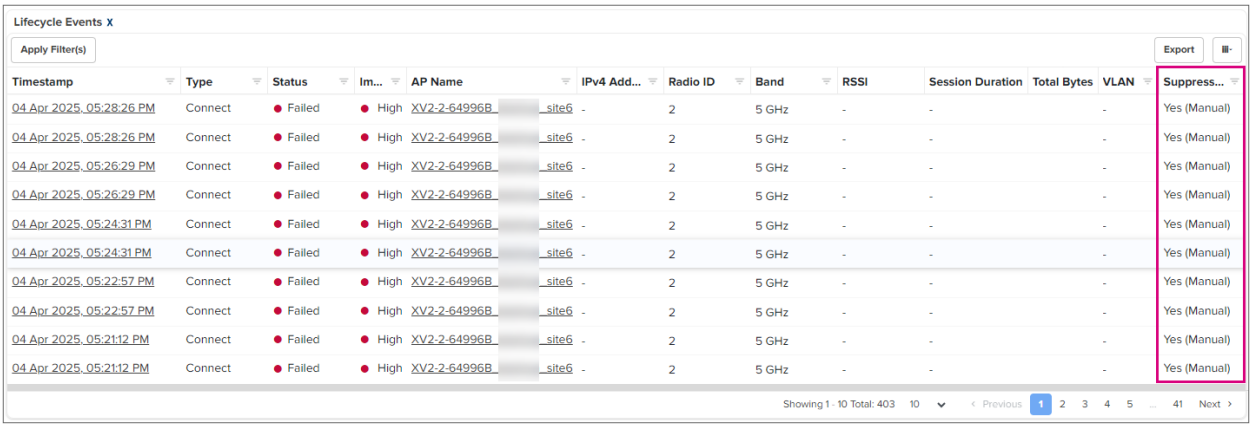


- **Top Suppressed Events By Type X** widget—Displays the top events that were suppressed categorized by the event type.



- **Lifecycle Events X** section > **Suppressed** column—This column displays if the failure event is a suppressed event or not. If yes, then it also displays if it is an event generated by an automatically suppressed client or a manually suppressed client.

  The same information is also displayed in the Client's **Lifecycle X** tab.



Removing a manually suppressed client from the Suppressed Clients list

Note

An auto suppressed client is automatically removed from the Suppressed Clients list when the client:

- generates a success event, or
- generates a different failure event, or
- does not generate any event for one hour

To remove a manually suppressed client from the Suppressed Clients list, complete the following steps:

1. Navigate to **Manage and Monitor** > Site > **Assurance X** > **Connection** dashboard.
2. Under the **Suppressed Clients** table, click the **Remove Suppressed Client** ( ) icon corresponding to the client you want to remove from this list.
3. Click **Yes** in the confirmation box.

Viewing the connection events

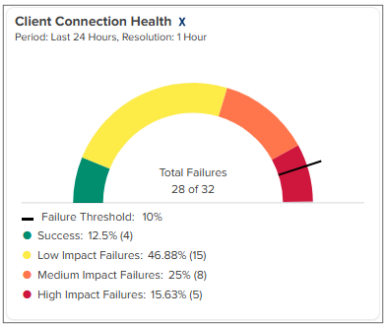
You can view and analyze the Wi-Fi connection events using the following UI pages:

- Dashboard page
- Assurance X page

Dashboard page

The site **Dashboard** page displays the following widgets:

- **Client Connection Health**—Displays overall statistics for connection events through a gauge or a dial chart. Based on the impact level filter set on the **Assurance X > Settings** page, this widget displays the statistics for failed connections.



Note

The default impact filter for a Site is **High**.

The resolution of this chart is 1 hour, which means every 1 hour this chart is updated. This chart displays the data based on the threshold and the impact level filter you set.

  - Number and percentage of successful connections.
  - Number and percentage of impact level failures for failed connections.

Note

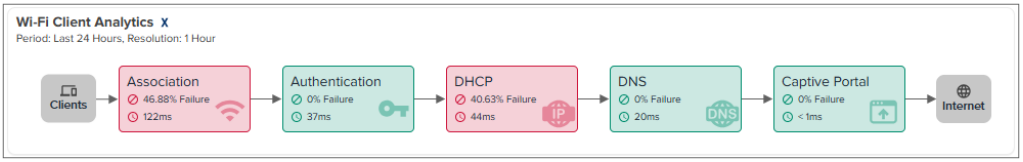
The **Client Connection Health** widget score is calculated, as follows.

Score = (Failures * 100)/(Failures+Success) %

Depending on the selection of the impact level filter on the **Assurance X > Settings** page, the failure count is calculated as follows:

- **High Impact**—Includes high impact failures only.
- **High and Medium Impact**—Includes medium and high impact failures.
- **High, Medium, and Low Impact**—Includes all failures: high, medium, and low impact.

- **Wi-Fi Client Analytics X**—Indicates the percentage of failed connections at each step in the client lifecycle.



The phase-wise chart displays the current status by highlighting the phase in:

  - **Red**—If the failure percentage exceeds the configured failure threshold configured in **Assurance X> Settings** page,

- **Orange**—If the failure percentage falls within the range of 80-100% of the configured failure threshold,
- **Green** —If the failure percentage is below 80% of the configured failure threshold.

The **Wi-Fi Client Analytics X** widget displays the connection state of clients to the Internet in the following phases:

- Duration in each phase indicates the average time taken by the clients in the respective phase.
- **Association**—Indicates the percentage of failed connections during the association phase.
- **Authentication**—Indicates the percentage of failed client authentications such as EAP, RADIUS, and authentication key derivation (EAPOL) failures.
- **DHCP**—Indicates the percentage of failed DHCP request or responses from or to the client.
- **DNS**—Indicates the percentage of failed DNS request or responses from or to the client.



Note

This is applicable only to captive portal clients.

- **Captive Portal**—Indicates the percentage of failed captive portal accesses.



Note

A captive portal is a web page launched in a browser that enables access to a public network. For example, business centers, airports, hotel lobbies, coffee shops, and other public venues use captive portals to offer free Wi-Fi hotspots for internet users.

Assurance X page

After accessing the **Assurance X** page and setting the failure threshold percentage, failure impact filter, and duration, you can analyze the connection events using the following tabs:

- Connection—Provides statistics for the connection events.
- Disconnection—Provides statistics for the disconnection events.

In addition to the data presented in the above tabs, more detailed information about the connection and disconnection events are available when you click an hour bar in the **Connection Health** or the **Disconnection** graphs. For information, refer Viewing hourly data and corresponding events.



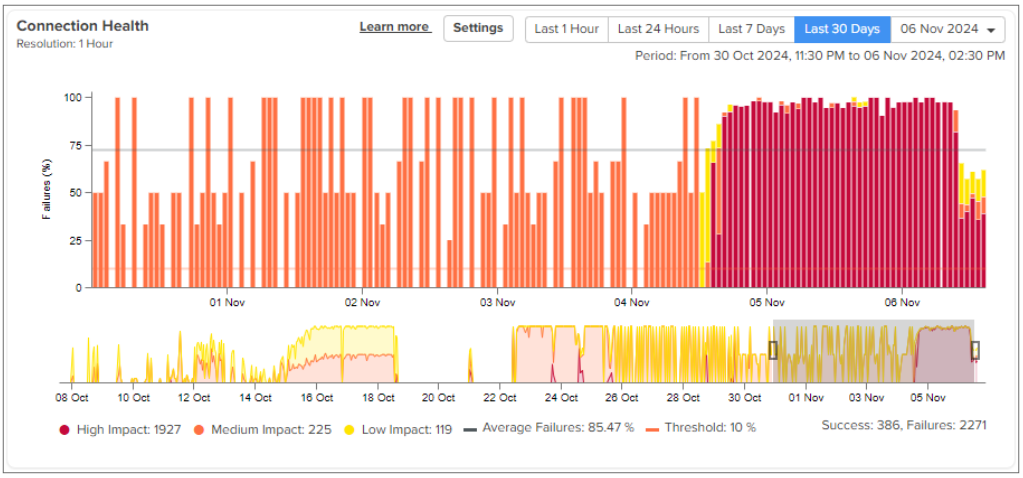
Note

The Assurance X page retains the connection and disconnection data for a maximum of 30 days.

Connection tab

Following widgets on the **Connection** tab show connection failure events for the configured duration:

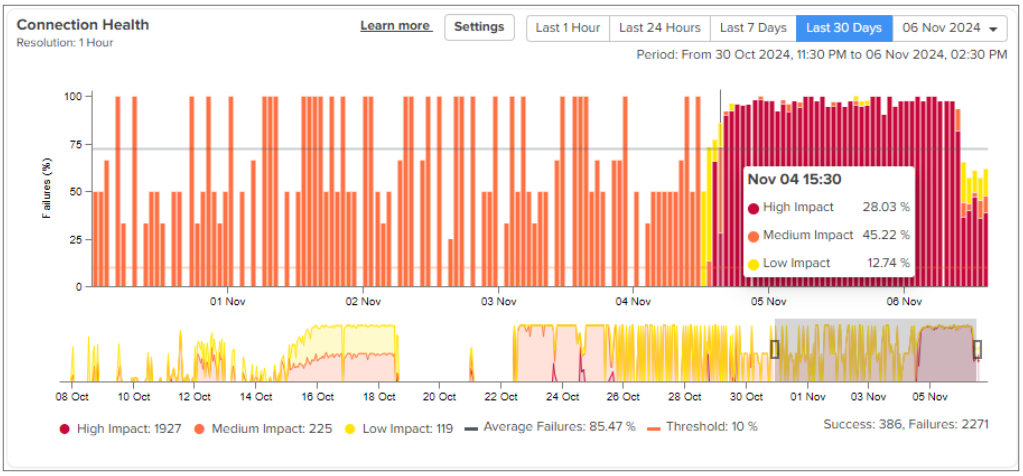
- **Connection Health**—Displays statistics of the failed connections in a bar chart, based on the threshold you set and the impact level failures in percentage.



The **Connection Health** bar chart represents the following data:

- Percentage of failed connections in a specific period for each failure impact—High, Medium, and Low.
- Percentage of average failures highlighted by a grey line.
- Percentage of high, medium, and low impacted connections in different colors.
- Failure threshold percentage configured indicated by an orange line.

To view the connection statistics for a particular date and time (at a particular hour), click on a bar in the chart, the chart displays the connection statistics for the selected date and hour.



When you click an hour bar on the **Connection Health** chart, the following widgets display failure data for that hour:

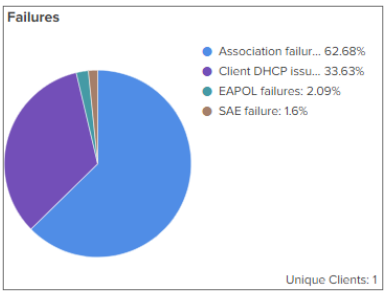
- Failures
- Lifecycle Analysis
- Top Affected APs
- Top Affected Client Models
- Top Affected Client Types
- Top Affected Client OS
- Top Affected SSID
- Connection Events

To view the events that have occurred in an hour's duration, refer Viewing hourly data and corresponding events.

Note

Click the refresh ( ) icon, located on the top right corner of the **Assurance X** page, to refresh the page.

- **Failures**—Displays statistics of top failures in a pie chart, indicating failure reasons in percentage.



When you select any top failure slice on the pie chart, the following widgets display data for the selected top failure:

  - Lifecycle Analysis
  - Top Affected APs
  - Top Affected Client Models
  - Top Affected Client Types
  - Top Affected Client OS
  - Top Affected SSID

- **Lifecycle Analysis**—Displays statistics for failed connections that help you analyze the life cycle of an event. By default, the phase with highest failure percentage is selected and highlighted.



This **Lifecycle Analysis** widget displays data through the following formats:

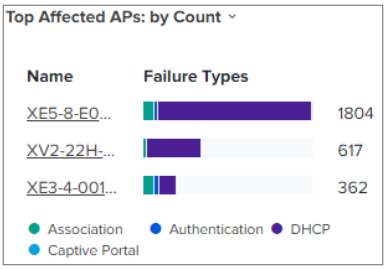
- **Phase-wise chart**—Displays the phase-wise chart that indicates the percentage of failed Wi-Fi client connections. When you click on a phase, the line graph below the phase-wise chart displays the corresponding data.
- **Line graph**—Displays the count of failed connections based on the date and time.
- Table with data corresponding to the failure selected.

  The following details are displayed in the table:

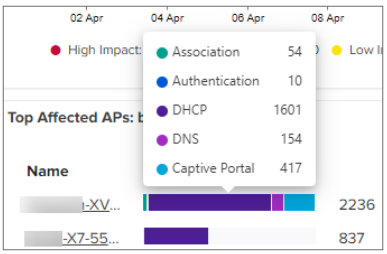
Filter name	Description
Host Name	The name of the host. Click the host name link to view the site-specific **Clients** page that displays the connection data for the selected host.
MAC Address	The MAC address of the client.
Client	Type of device used for the connection.

Filter name	Description
Type	
Client OS	The operating system (OS) running on the client.

- **Top Affected APs**—Displays the name of top affected APs and the statistics for the failed connection.



To view the statistics of top affected APs in percentage or count, click the collapse (⌄) icon next to the widget title. Hover over on any color bar to view the failure type and the corresponding count of disconnection events. Click the link in the **Name** column to view the site-specific **Wi-Fi** dashboard with the AP information.



- **Top Affected Client Models**—Displays details of the most affected client models with the failure type.

  To view the statistics of top affected client models in percentage or count, click the collapse (⌄) icon next to the widget title. Hover over on any color bar to view the failure type and the corresponding count of disconnection events.

- **Top Affected Client Types**—Displays the name of top affected client types and the statistics for the failed connection.

  To view the statistics of top affected client types in percentage or count, click the collapse (⌄) icon next to the widget title. Hover over on any color bar to view the failure type and the corresponding count of disconnection events.

- **Top Affected Client OS—**Displays the name of top affected OS and the statistics for the failed connection.

  To view the statistics of top affected client OS in percentage or count, click the collapse (⌄) icon next to the widget title. Hover over on any color bar to view the failure type and the corresponding count of disconnection events.

- **Top Affected SSID**—Displays details of the most affected SSIDs with the failure type.

  To view the statistics of top affected SSIDs in percentage or count, click the collapse (⌄) icon next to the widget title. Hover over on any color bar to view the failure type and the corresponding count of disconnection events.

- **Connection Events : Last 1 Hour**—A table with filters displays the details of successful or failed connection events that occurred in the last one hour.

Note

Failure events per AP, Client type, and Client OS are displayed only when you click an hour bar in the **Connection Health** graph.

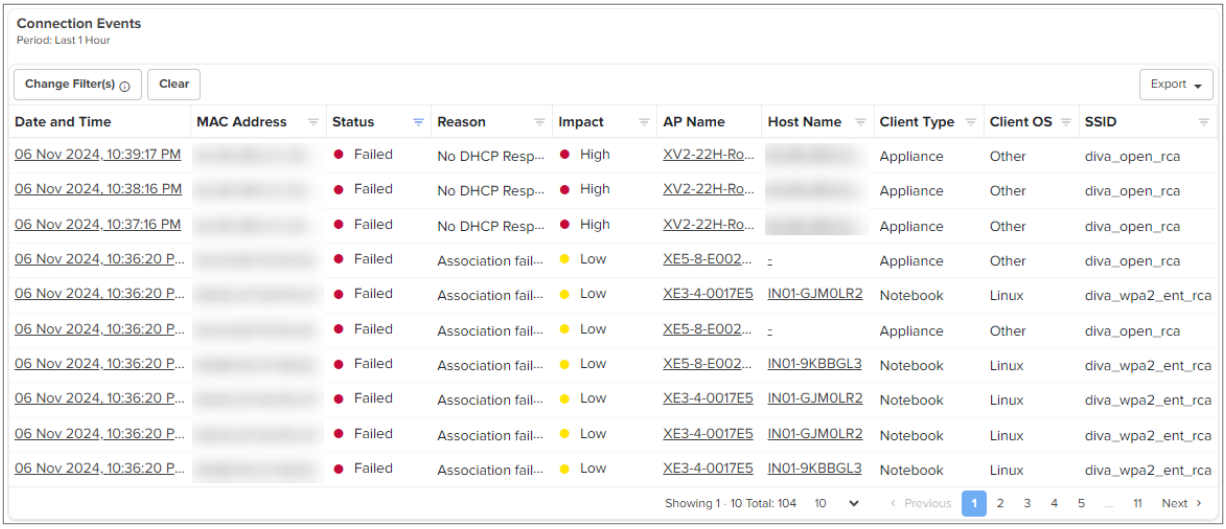
To use filters and view the connection details for the last one hour, perform the following steps:

1. Inside the **Connection Events : Last 1 Hour** widget, click **Apply Filters**.
2. To search and view data for the last one hour, enter one or more of the following details:

Filter name	Description
MAC Address	The MAC address of the device with connection events.
Success	Select whether you want to view successful or failed connection events. • Success • Failed
Reason	Select the required reason type from the dropdown list such as MAC-ACL, MAC-AUTH, QoS failure, Passpoint failure, Capability mismatch, L2 Auth failure, Association failure, Roaming failure, SAE failure, Cipher failure, or TDLS failure.
Impact	Select the required impact type from the list: • Low • Medium • High
Host Name	The name of the host for which you want to view the connection state.
Client Type	The type of device used for the connection.
Client OS	The operating system (OS) running on the client.

3. Click **Apply Filter(s)** to apply the changes.

   The table displays the connection event details with date, time, and AP names for the searched criteria.



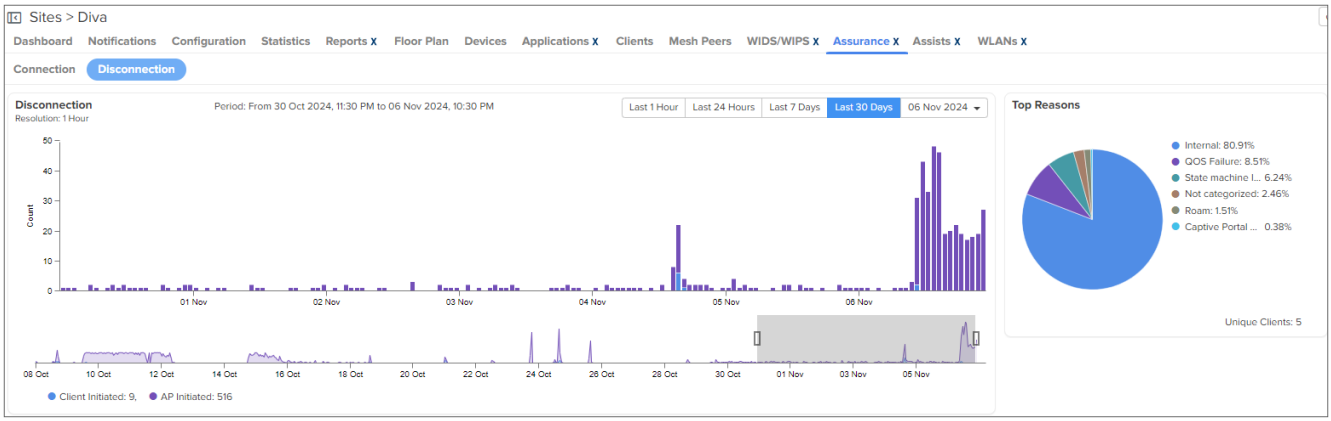
Note

You can also click the icon in the table to quickly search for status, reason, impact level, AP name, host name, client type, and client OS.

- When you click on any date and time, the **Events** page displays connection state data for the selected date and time. Refer Viewing an event-based connection or disconnection event.
- When you click on any AP name, the site-specific **Wi-Fi** dashboard displays the AP or device information.
- When you click on a host name, the site-specific **Clients** page displays the connection data for the selected host.

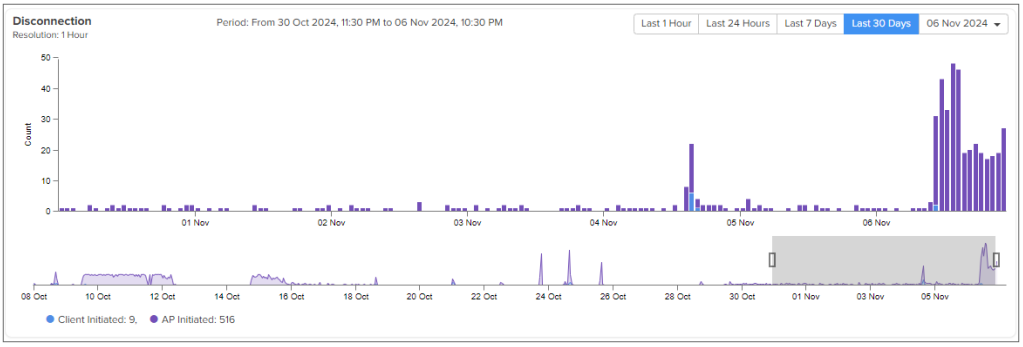
Disconnection tab

On accessing the **Assurance X** page, click on the **Disconnection** tab and set the time filter by choosing the required time period as last 1 hour, last 24 hours, last 7 days, last 30 days or select a custom date from the date picker. The **Disconnection** tab displays the data for the selected time period.



The following widgets on the **Disconnection** page support root cause analysis:

- **Disconnection**—Displays the count of client disconnections initiated by either the clients or the APs.



When you click on a bar in the chart, the chart displays the count of disconnection events initiated by the clients and the APs at the specific date and time.

Click any hour bar on the **Disconnection** chart to view the corresponding data in the following widgets:

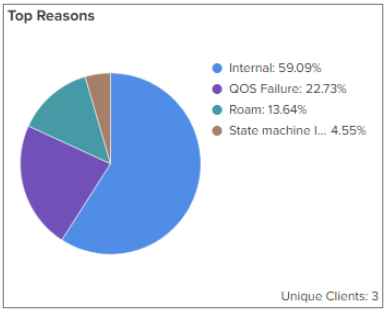
- Analytics
- Top Reasons
- Top Reporting APs by Count

- Top Reporting Client Models by Count
- Top Reporting Client Types by Count
- Top Reporting Client OS by Count
- Top Affected SSID by Count

Note

Click the refresh ( ) icon, located on the top right corner of the **Assurance X** page, to refresh the page.

- **Top Reasons**—Displays statistics of top failure reasons such as state machine issues, roam, QoS failures, and timeout failures.



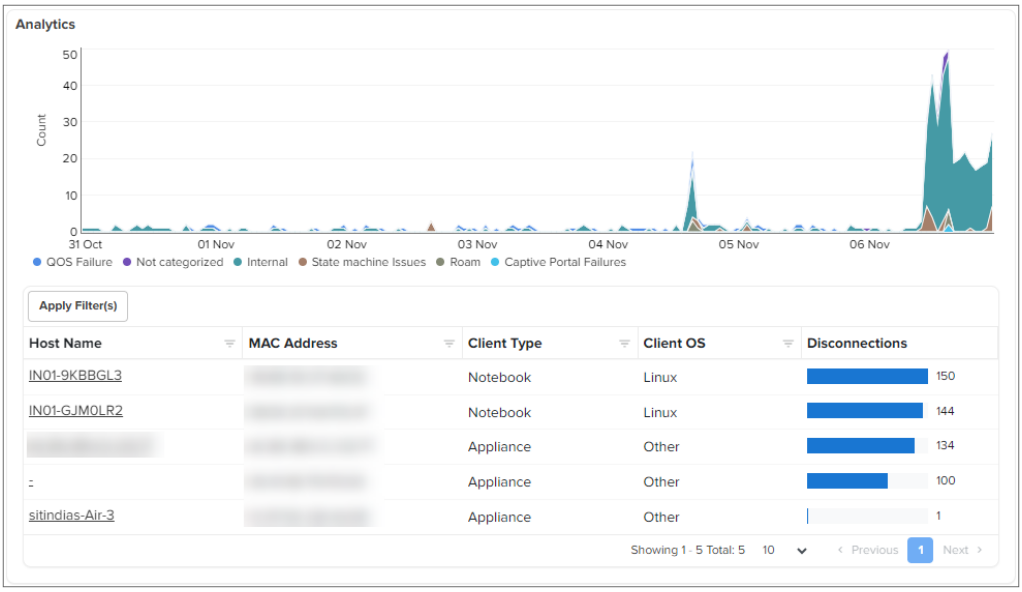
When you select any top failure slice on the pie chart, the following widgets display data for the selected top failure:

- Top Reporting APs by Count
- Analytics
- Top Reporting Client Models by Count
- Top Reporting Client Types by Count
- Top Reporting Client OS by Count
- Top Affected SSID by Count

Note

Click the refresh ( ) icon, located on the top right corner of the **Assurance X** page, to refresh the page.

- **Analytics**—Displays statistics for disconnections to help analyze failure events in detail.



This widget displays data in the following formats:

- **Line graph**: Displays the count of disconnections, including the date, time, and failure reasons in different colors.
- **Filters to view the required disconnection in detail**: A table with filters displays detailed information of a disconnection event.

  To use filters and view the details of a disconnection event, perform the following steps:

  1. Inside the **Analysis** widget, click **Apply Filters** located below the line graph section.
  2. To search for and view data of the required client's disconnection state, enter one or more of the following:

Filter name	Description
Host Name	The name of the host for which you want to view the disconnection details.
MAC Address	The MAC address of the device for which you want to view the disconnection details.
Client Type	Type of device used for the connection.
Client OS	The operating system (OS) running on the client.

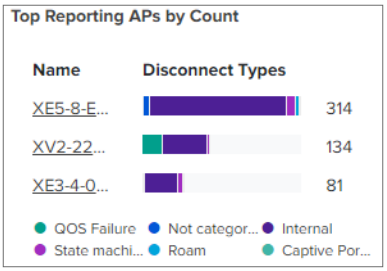
  3. Click **Apply Filter(s)** to apply the changes.

  Note

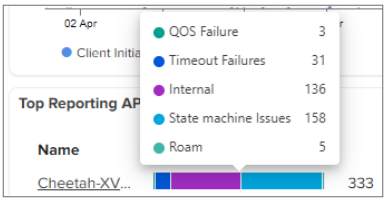
  You can also click the icon in the table to quickly search for MAC address, client type, client OS, and disconnection count.

  When you click on a host name, the site-specific **Clients** page displays the disconnection state data for the selected host.

- **Top Reporting APs by Count**—Displays the names of top APs and the count of disconnections in different colors based on the disconnection types.



Hover over on any color bar to view the failure type and the corresponding counts of disconnection events.



- **Top Reporting Client Models by Count**—Displays the names of the top device model names and the count of disconnections in different colors based on the disconnection reasons. Hover over on any color bar to view the failure type and the corresponding counts of disconnection events.
- **Top Reporting Client Types by Count**—Displays the names of the top device types and the count of disconnections in different colors based on the disconnection reasons. Hover over on any color bar to view the failure type and the corresponding counts of disconnection events.
- **Top Reporting Client OS by Count**—Displays the names of top OS and the count of disconnections. Different colors are used to highlight the disconnection reasons. Hover over on any color bar to view the failure type and the corresponding counts of disconnection events.
- **Top Affected SSID by Count**—Displays the top SSIDs and the count of disconnections in different colors based on the disconnection reasons. Hover over on any color bar to view the failure type and the corresponding counts of disconnection events.
- **Disconnect Events: Last 1 Hour**—A table with filters displays the data of disconnection events that occurred in the last one hour.

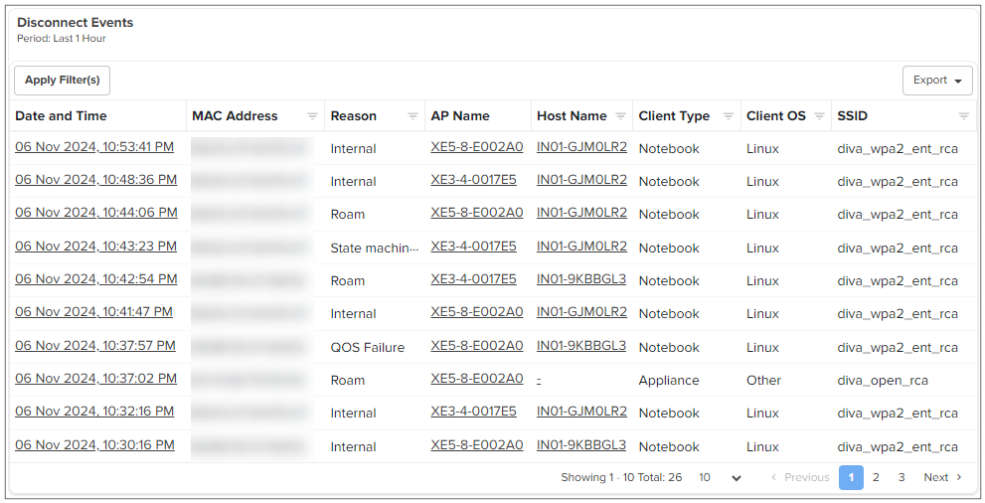
  To use filters and view the disconnection state details for the last one hour, perform the following steps:

  1. Inside the **Disconnection Events : Last 1 Hour** widget, click **Apply Filters**.
  2. To search for and view data of the disconnection events, enter one or more of the following:

Filter name	Description
MAC Address	The MAC address of the client for which you want to view the disconnection events.
Reason	Select the type of reason from dropdown list such as Unknown-disc-O, QoS failure, Radius failures, TDLS failures, timeout failures, state machine issues, AP Resource failures, AP assisted roaming, and roam.
Host Name	The name of the host for which you want to view the disconnection state.
Client Type	Type of device used for the connection.
Client OS	The operating system (OS) running on the client.

3. Click **Apply Filter(s)** to apply the changes.

   The table displays the disconnection state with date, time, and AP names for the searched criteria.



Date and Time	MAC Address	Reason	AP Name	Host Name	Client Type	Client OS	SSID
06 Nov 2024, 10:53:41 PM		Internal	XE5-8-E002A0	IN01-GJM0LR2	Notebook	Linux	diva_wpa2_ent_rca
06 Nov 2024, 10:48:36 PM		Internal	XE3-4-0017E5	IN01-GJM0LR2	Notebook	Linux	diva_wpa2_ent_rca
06 Nov 2024, 10:44:06 PM		Roam	XE5-8-E002A0	IN01-GJM0LR2	Notebook	Linux	diva_wpa2_ent_rca
06 Nov 2024, 10:43:23 PM		State machin...	XE3-4-0017E5	IN01-GJM0LR2	Notebook	Linux	diva_wpa2_ent_rca
06 Nov 2024, 10:42:54 PM		Roam	XE3-4-0017E5	IN01-9KBBGL3	Notebook	Linux	diva_wpa2_ent_rca
06 Nov 2024, 10:41:47 PM		Internal	XE5-8-E002A0	IN01-GJM0LR2	Notebook	Linux	diva_wpa2_ent_rca
06 Nov 2024, 10:37:57 PM		QOS Failure	XE5-8-E002A0	IN01-9KBBGL3	Notebook	Linux	diva_wpa2_ent_rca
06 Nov 2024, 10:37:02 PM		Roam	XE5-8-E002A0	-	Appliance	Other	diva_open_rca
06 Nov 2024, 10:32:16 PM		Internal	XE3-4-0017E5	IN01-GJM0LR2	Notebook	Linux	diva_wpa2_ent_rca
06 Nov 2024, 10:30:16 PM		Internal	XE5-8-E002A0	IN01-9KBBGL3	Notebook	Linux	diva_wpa2_ent_rca

Showing 1 - 10 Total: 26 10 Previous 1 2 3 Next

Note

You can also click the icon in the table to quickly search for MAC address, reason, AP name, client type, client OS, and disconnection count.

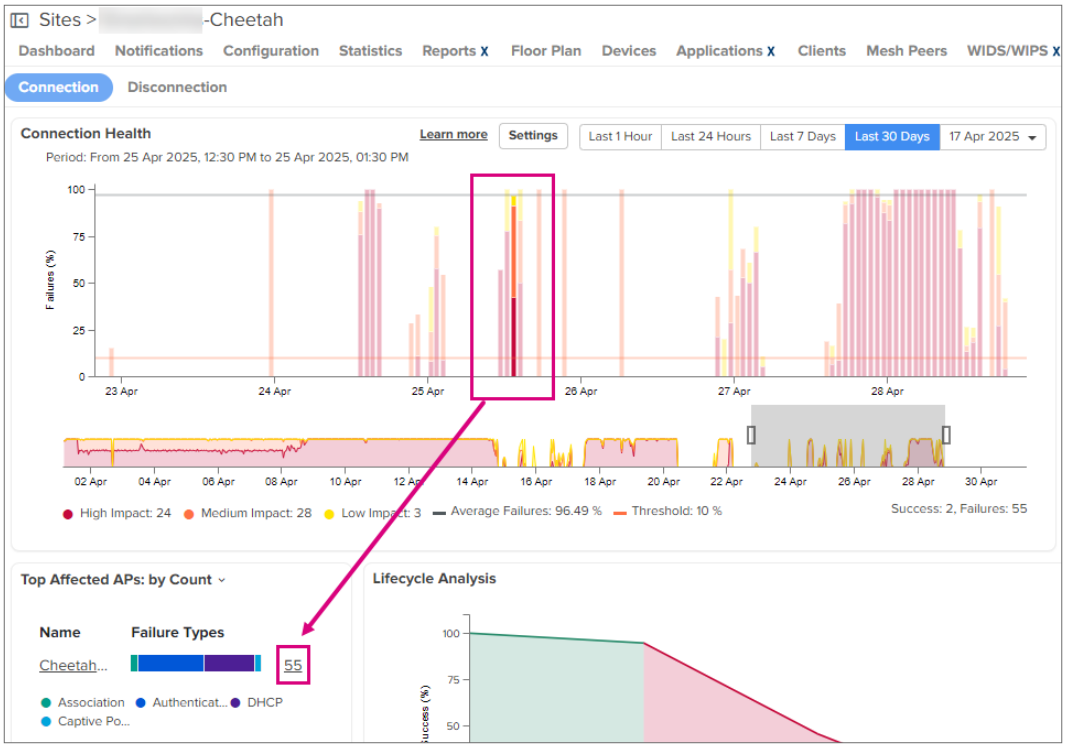
- When you click on any date and time, the **Events** page displays the disconnection state data for the selected date and time.
- When you click on any AP name, the site-specific **Wi-Fi** dashboard displays the AP or device information.
- When you click on a host name, the site-specific **Clients** page displays the disconnection state data for the selected host.

Viewing hourly data and corresponding events

When you click an hour bar in the **Connection Health** or the **Disconnection** graphs on the **Connection** and **Disconnection** tabs respectively, the following widgets display a link corresponding to the count of failures:

- **Connection** tab
  - Top Affected APs
  - Top Affected Client Models
  - Top Affected Client Types
  - Top Affected Client OS
  - Top Affected SSID
- **Disconnection** tab
  - Top Reporting APs by Count
  - Top Reporting Client Models by Count
  - Top Reporting Client Types by Count
  - Top Reporting Client OS by Count
  - Top Affected SSID by Count

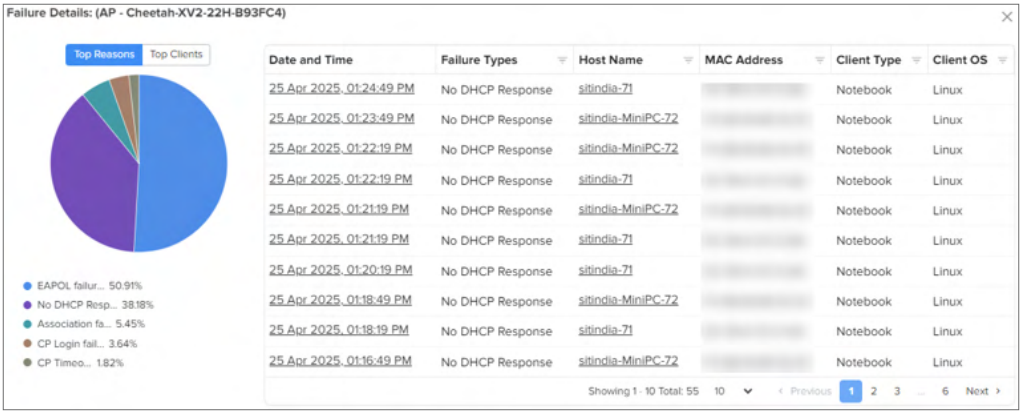
For example,



To view failure details for the corresponding entity depending on the widget you click the link, perform the following steps:

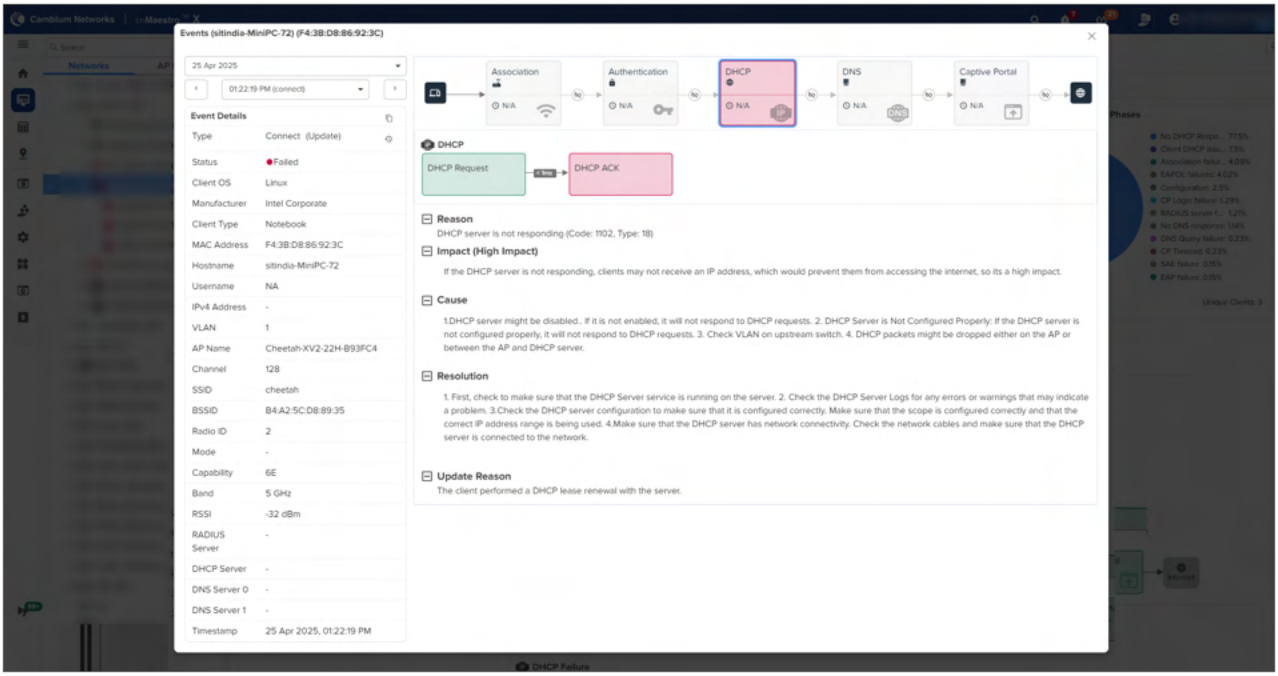
1. Navigate to **Site** > **Assurance X** > **Connection** or **Disconnection** tab.
2. In the **Connection Health** or the **Disconnection** widget, select the time duration for which you want to view the data.
3. In the bar graph, click an hour bar.
4. In the widgets listed above, click the link corresponding to the failure count or percentage.

   The **Failure Details** page is displayed.



5. From the **Date and Time** column, click any timestamp link to view the event details.

For more information, refer Viewing an event-based connection or disconnection event.



Viewing a client or host-specific connection or disconnection event

You can analyze client or host-specific connection or disconnection events in detail and take appropriate actions.

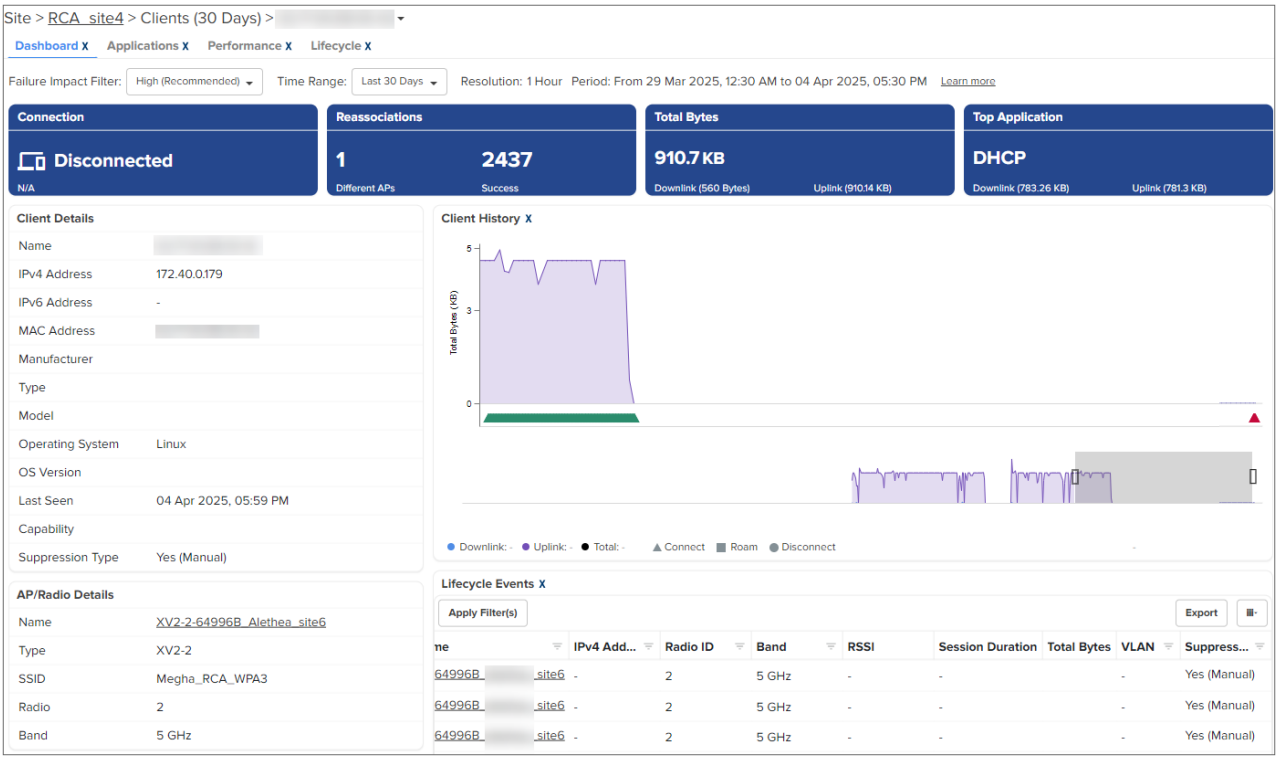
To view client or host-specific information, perform the following steps:

1. Click on a host name to view the connection or disconnection state in detail.

   You can locate the host names in the following widgets:

   - **Lifecycle Analysis** on the Connection page—host names are available in a table below the line graph section.
   - **Connection Events: Last 1 Hour** on the Connection page.
   - **Analytics** on the Disconnection page.
   - **Disconnect Events: Last 1 Hour** on the Disconnection page.

   When you click the required host name, the site-specific **Clients** page displays detailed information for the selected host. The following figure is an example of the site-specific **Clients** page:

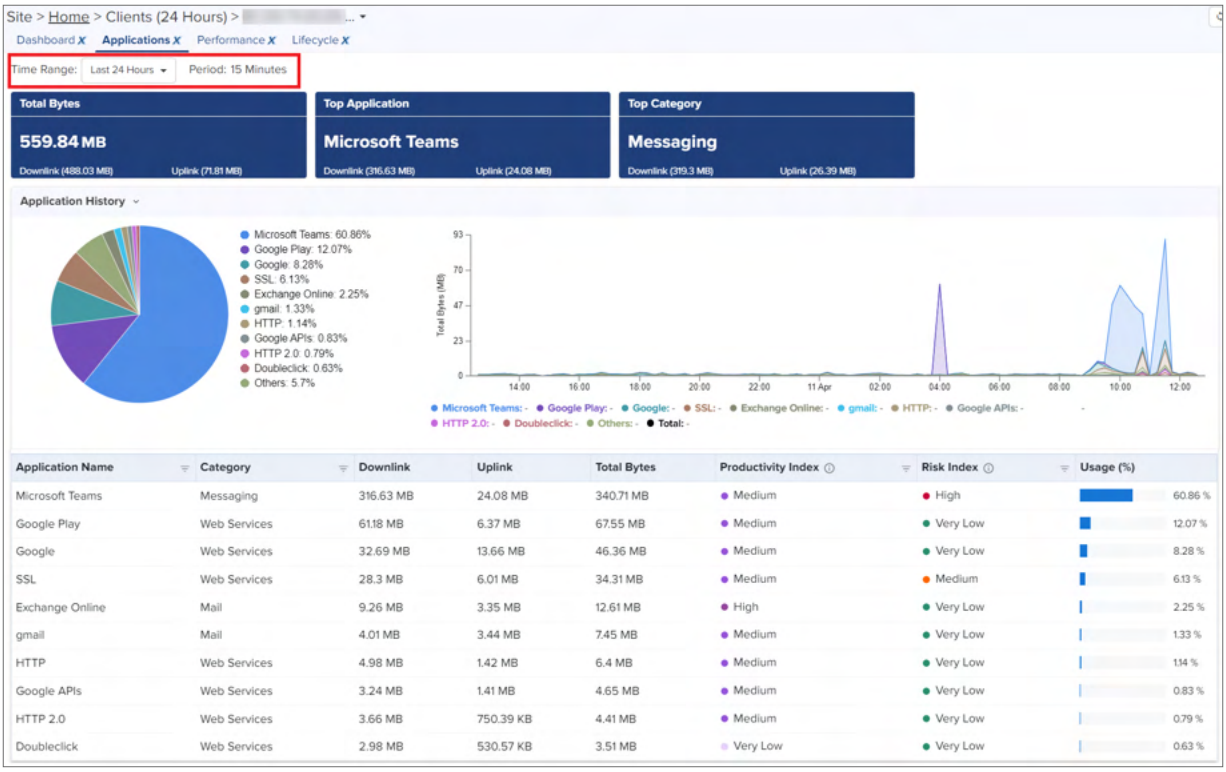


This site-specific **Clients** page contains the following tabs:

- **Dashboard X**—Provides a summary of the client connection or disconnection events such as Client history or lifecycle events.

  By default, the **Dashboard** tab is visible when the site-specific **Clients** page appears. Based on the time period (Last 24 Hours, Last 7 Days, or Last 30 days) you select from the **Time Range** filter, the site-specific client **Dashboard** page displays the Wi-Fi client information in the following widgets:

  - Connection
  - Reassociations
  - Total Bytes
  - Top Application
  - Client Details
  - Client History X
  - AP/Radio Details
  - Lifecycle Events X
  - Suppressed Failure Events
  - Connection Success Rate X
  - Failures X
  - Top Suppressed Events By Type X
  - Top Applications
  - Top Categories
- **Applications X**—Provides detailed information of top applications used for the connection.

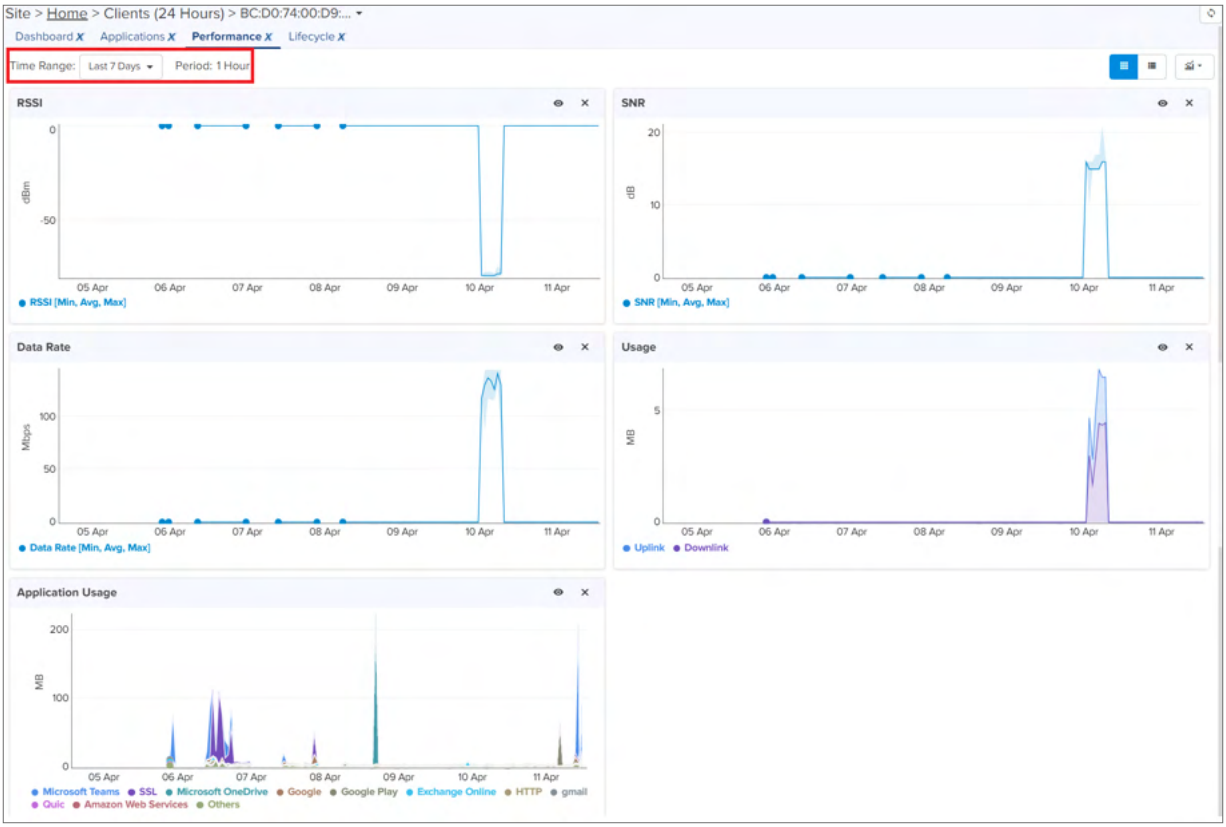


Based on the time period (Last 24 Hours, Last 7 Days, or Last 30 days) you select from the **Time Range** filter, the site-specific client **Applications** page displays the application information for the Wi-Fi client in the following widgets:

- Total Bytes
- Top Application
- Top Category
- Application / Category History

  Click the ⌄ icon next to the **Application History** title to view the details category-wise.

- **Performance X**—Provides detailed information of RSSI, SNR, date rate, usage in uplink and downlink, and the application usage.

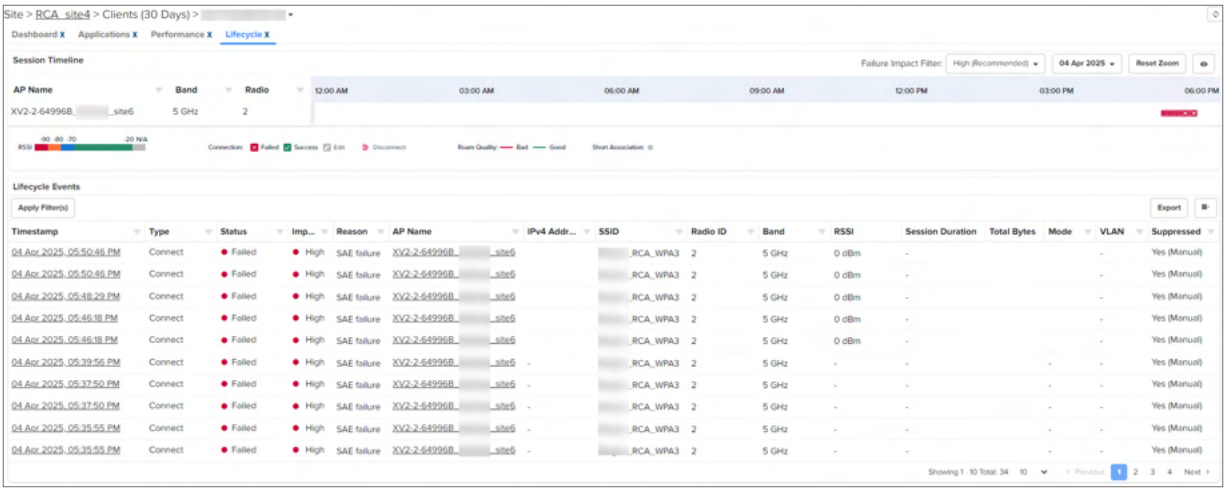


Based on the time period (Last 24 Hours, Last 7 Days, or Last 30 days) you select from the **Time Range** filter, the site-specific client **Performance** page displays the network performance for the Wi-Fi client in the following widgets:

- RSSI
- SNR
- Data Rate
- Usage
- Application Usage

You can click the icon (Data point selector) to filter and view the required options specific to performance in the widgets.

- **Lifecycle X**—Provides detailed information of the client's connection or disconnection events.



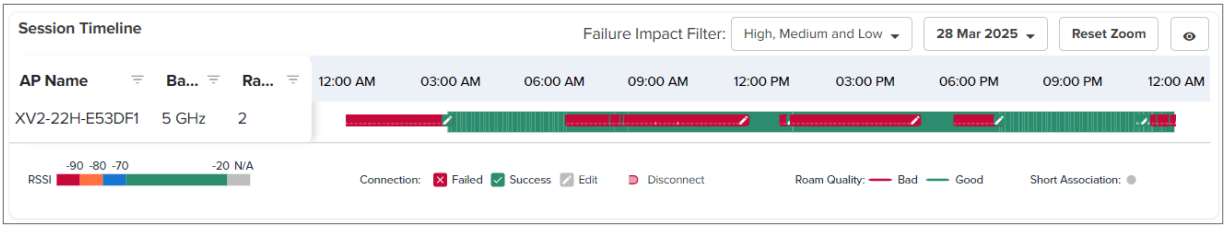
Based on the date and impact levels you select from the date picker and **Failure Impact Filter** dropdown list, the site-specific client **Lifecycle** page displays the session timeline and the lifecycle events of the Wi-Fi client for the selected date.

Note

Lifecycle data is available for a maximum of up to 30 days.

In the **Session Timeline** section, you can find the AP names, band used, and the radio index. In addition, different indicators mark RSSI, the connection event as failed or success, the disconnection event, the roam quality as bad or good, and short association.

For example, in the following UI page, the RSSI ranges and the roam quality are highlighted using different colors.



- Placing the cursor on the ✅ icon, displays date and time of the succeeded event.
- Placing the cursor on the ❌ icon, displays the reason and cause for the failed event.
- Clicking ✅ or ❌ icon in the **Session Timeline** section, displays the **Events** page with detailed information for the selected event.
- Clicking the disconnect (🔌) icon, displays details about the event and disconnection reason.
- The short association (⚪) icon denotes that the client connected and disconnected within a minute.
- The edit (✏️) icon denotes that the client connection failed in DHCP, DNS or Captive portal phase in the first connection attempt but succeeded later.

Note

A client connection is considered failed in DHCP, DNS, or CP, if the client fails to complete the phase within 45-60 secs.

The **Lifecycle Events** section provides detailed information of the client's connection and disconnection events such as timestamp, connection type, connection status, AP name, IPv4 address, radio ID, impact of the event, band used, RSSI, session duration, total bytes, wireless mode used, VLAN used, and WLAN details.

You can also use the filters to view and analyze the required event information. To view the required lifecycle event using filters, perform the following steps:

a. In the **Lifecycle Events** section, click **Apply Filter(s)**.

b. Enter one or more of the following details:

Filter name	Description
Timestamp	Time period for which you want to view the data: • Between • After • Before
Type	Type of event for which you want to view the data: • Roam • Connect • Disconnect
Status	State of the event: • Success • Failed
AP Name	Name of the AP that is used in the event.
IPv4 Address	The IPv4 address used for the connection.
Radio ID	ID of the radio used in the event.
Impact	Impact level of the event. • Low • Medium • High
Band	The bandwidth used for the connection.
Mode	The standard wireless mode used for the connection. For example, 802.1ac
VLAN	The VLAN ID used for the connection.
WLAN	The WLAN ID used for the connection.



Note

You can also click the icon in the **Lifecycle Events** table to quickly search for type, status, AP name, IPv4 address, radio ID, impact, band, RSSI, VLAN, and WLAN.

c. Click **Apply Filter(s)**.

The table in the **Lifecycle Events** section is updated with the required information for the client or host.

You can also drill down an event to view what went wrong during the connection or the reason for the disconnection event. Refer Viewing an event-based connection or disconnection event.

2. Analyze the data for the required client or host and take actions.

Viewing an event-based connection or disconnection event

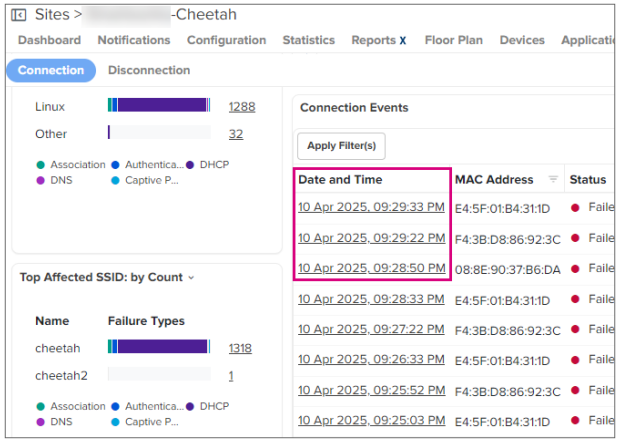
After viewing the lifecycle events for a specific client or host, you can drill down an event to analyze what caused a failed connection or a disconnection.

To view an event-based connection or disconnection state, perform the following steps:

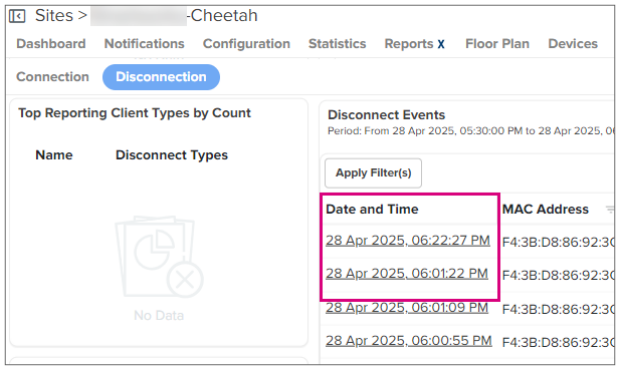
1. Click the timestamp present in either the **Date and Time** or **Timestamp** columns to view the connection or disconnection event in detail.

   You can locate a date or timestamp in the following widgets:

   - **Date and Time** column in the **Connection Events: Last 1 hour** on the **Connection** page (data is available only when you click any of the hour bars in the **Connection Health** graph)

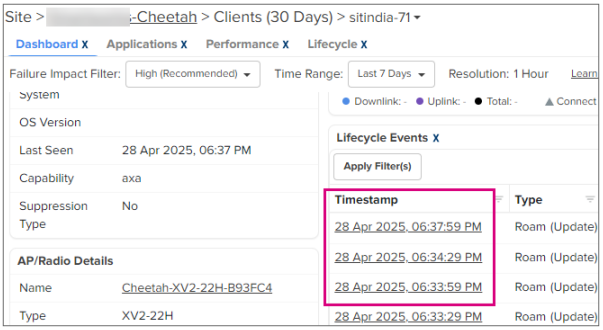


   - **Date and Time** column in the **Disconnect Events: Last 1 hour** widget on the **Disconnection** page (data is available only when you click any of the hour bars in the **Disconnection** graph)

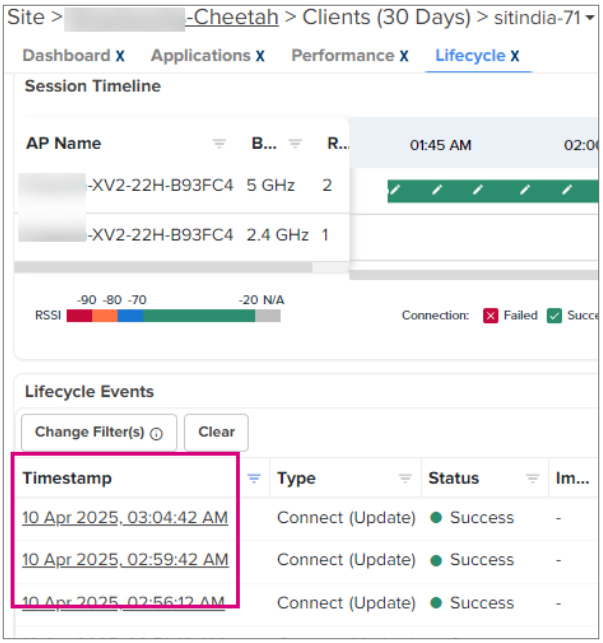


   - **Timestamp** column in the **Lifecycle Events** widget available on both the client > **Dashboard** page and the client > **Lifecycle** page.

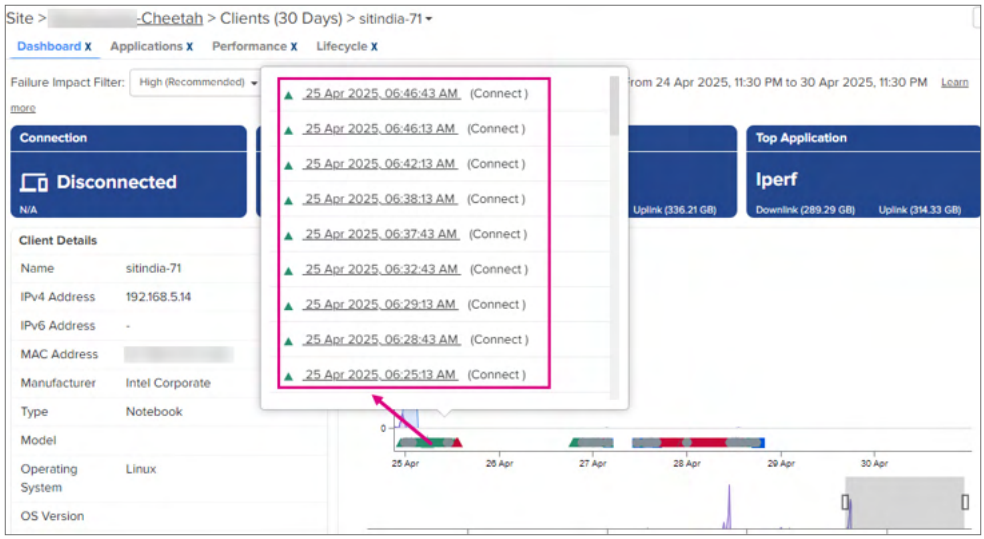
- client > **Dashboard** page



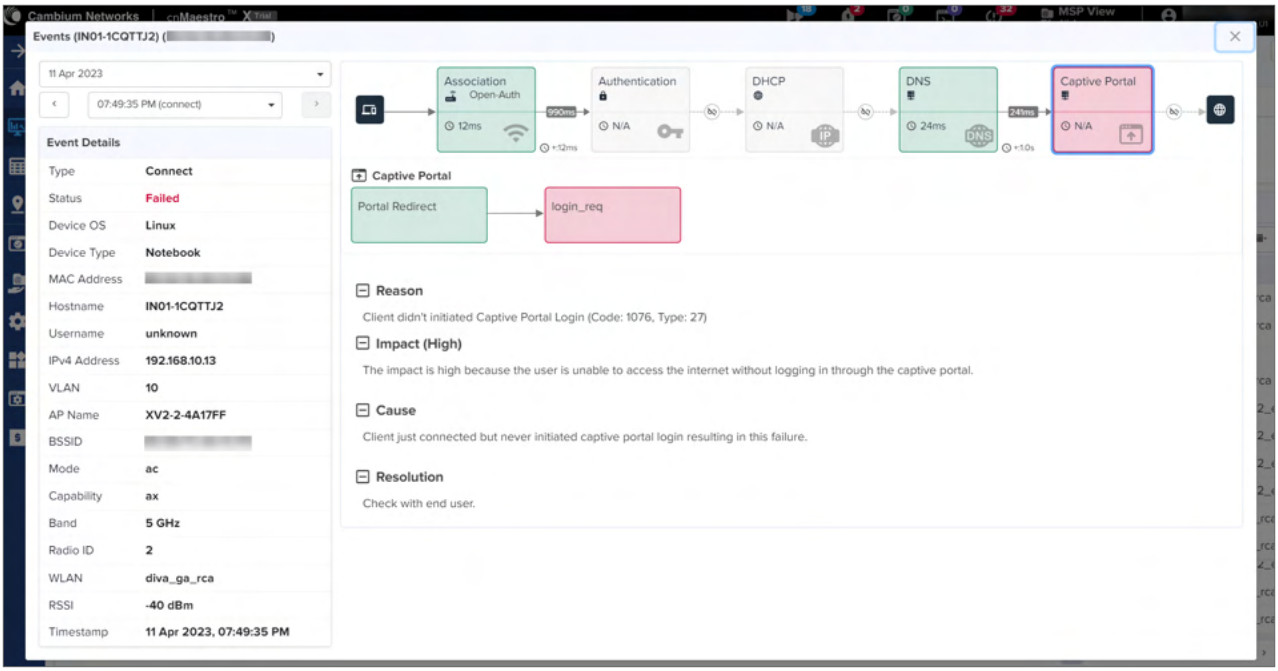
- client > **Lifecycle** page



- Timestamp listed in the pop-up window when you click a point in the **Client History X** graph in the client > **Dashboard** page.



When you click on **Timestamp** or **Date and Time**, the **Events** screen displays the detailed event information.



The **Events** page provides phase-wise information with complete event details such as reason, impact, cause, and resolution. These event-based details help with troubleshooting any issues.

2. To view an event for a specific date, you can select the required date from the date dropdown list.



Similarly, you can use **<** or **>** to view time-based events for a client. You can also select the time-based events from the dropdown list.

3. Click the ✕ icon to close the **Events** page.

Viewing AP-specific information

You can view an AP-specific information for the required client or event and analyze the connection or disconnection data. This analysis helps identify device details used for the connection.

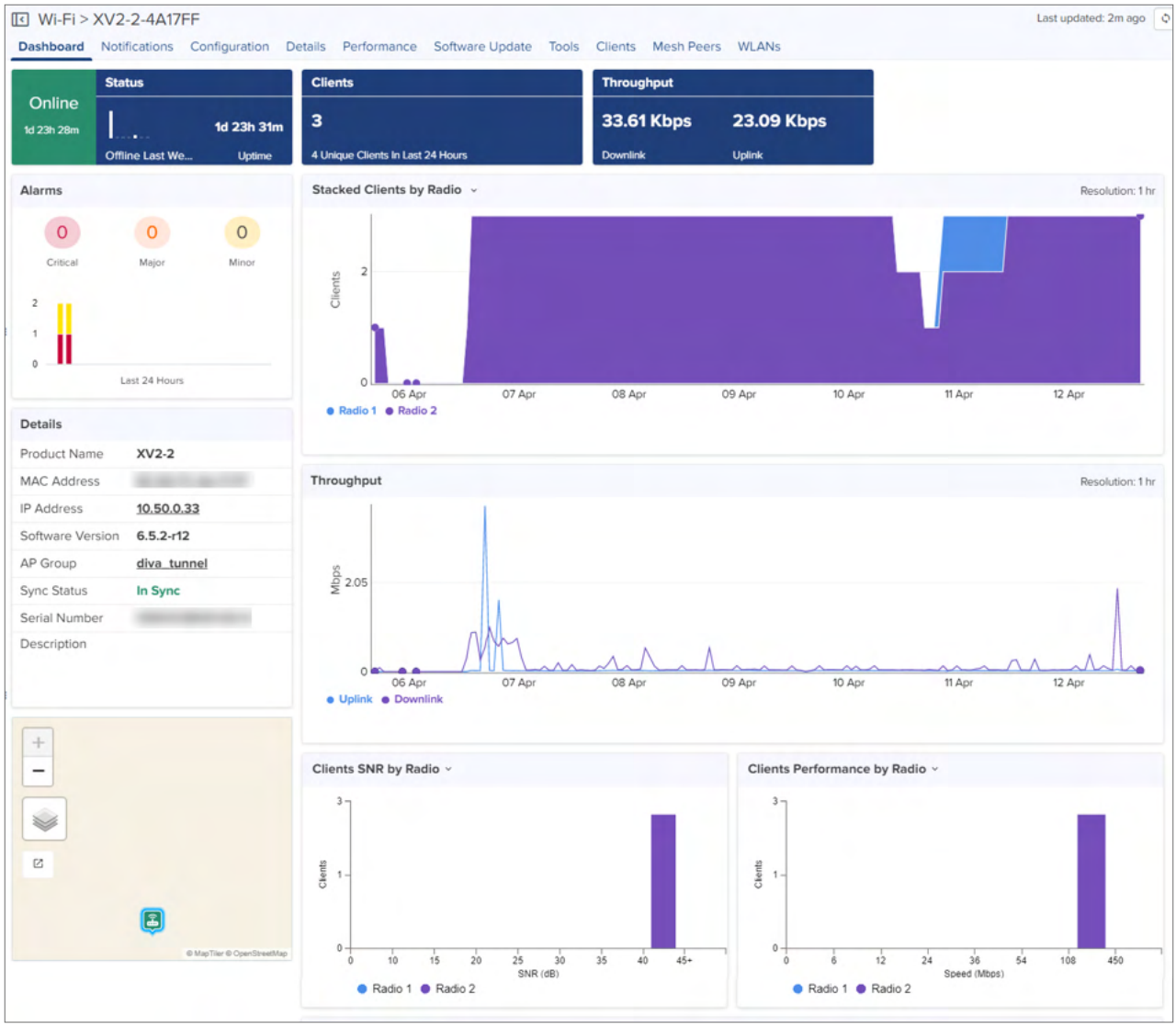
To view AP-specific information, perform the following steps:

1. Click the **AP Name** to view the data.

   You can locate an AP name in the following widgets:

   - Top Affected APs on the **Connection** page
   - Connection Events—Last 1 Hour on the **Connection** page
   - Top Reporting APs on the **Disconnection** page
   - Disconnect Events—Last 1 Hour on the **Disconnection** page
   - Lifecycle Events on both the **Connection** and **Disconnection** pages

   When you click on the required AP name, the site-specific **Wi-Fi** dashboard displays the AP or device information.



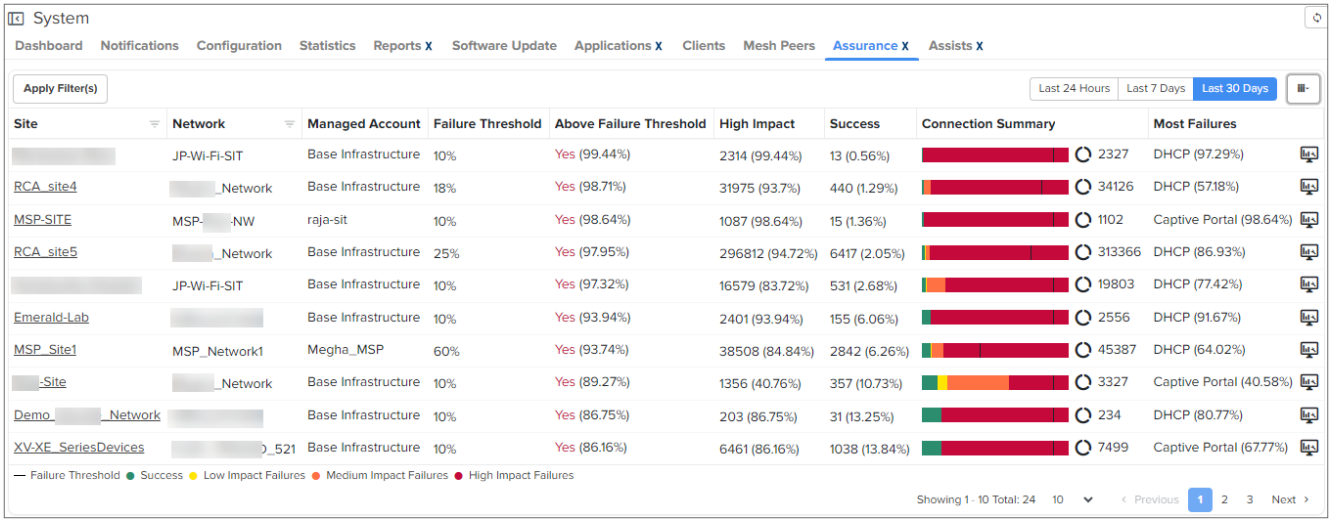
   For more information on the AP (or device) specific dashboard, refer to the Wireless LAN Dashboards section of cnMaestro Cloud User Guide.

2. Analyze the AP data and take appropriate actions.

System-level Assurance

The System-level **Assurance X** page provides the consolidated data of all the site analytics. For more information, refer to Assurance X page.

Figure 542 *System Assurance*



Managed Services

This section includes the following topics:

- Managed Accounts
- Managing subscribers (end-customer)

Managed Accounts

This section includes the following topics:

- Overview
  - Managed Accounts
  - Accounts
  - Managed Account Service
  - Account Service Users (Administrators)
- Configuring Managed Account Services
  - Enable Managed Accounts
  - Creating Managed Account Services
  - Creating Account
  - Validating Account Users
- Managed Account Administration
  - Overview
  - System Dashboard
  - Account Administration
  - Device Management
  - Swap 60 GHz cnWave Accounts
  - Disabling the Managed Accounts feature

Overview

Managed Accounts allow the cnMaestro owner to partition their installation into independent accounts with their own administrators and configuration. This feature is for MSPs who want to provision a full cnMaestro account for their customers, while still maintaining control over the global deployment.

Managed Accounts

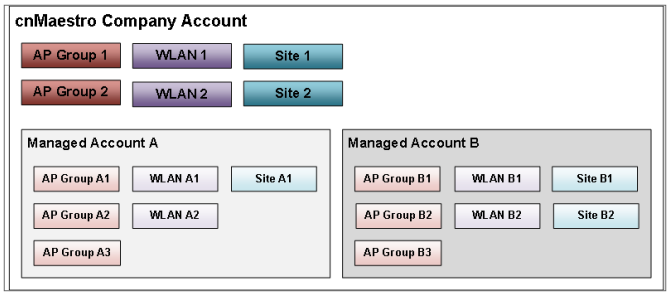
The Managed Accounts feature combines Accounts with Account Services.



Accounts

Managed Accounts group cnMaestro devices and configuration objects (such as AP Groups, WLANs, and Sites) into administration domains within a single cnMaestro deployment . Accounts are independent, and the devices added to them are configured using the objects in the Account.

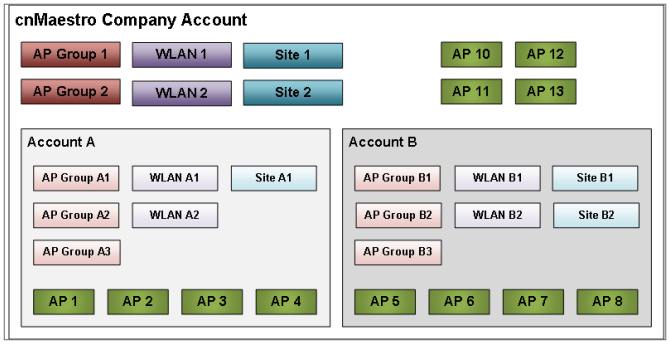
Figure 543 *Accounts*



Access Points

Access Points exist in the global Company Account, or they can be added to a single Managed Account. Access Points in a Managed Account are configured using the Wi-Fi Profiles in that Managed Account.

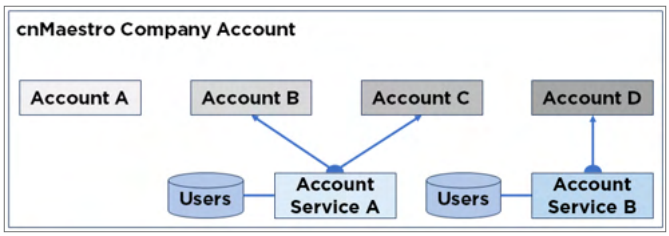
Figure 544 *Access Points*



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 545 *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 546 *Account UI - Sample 1*

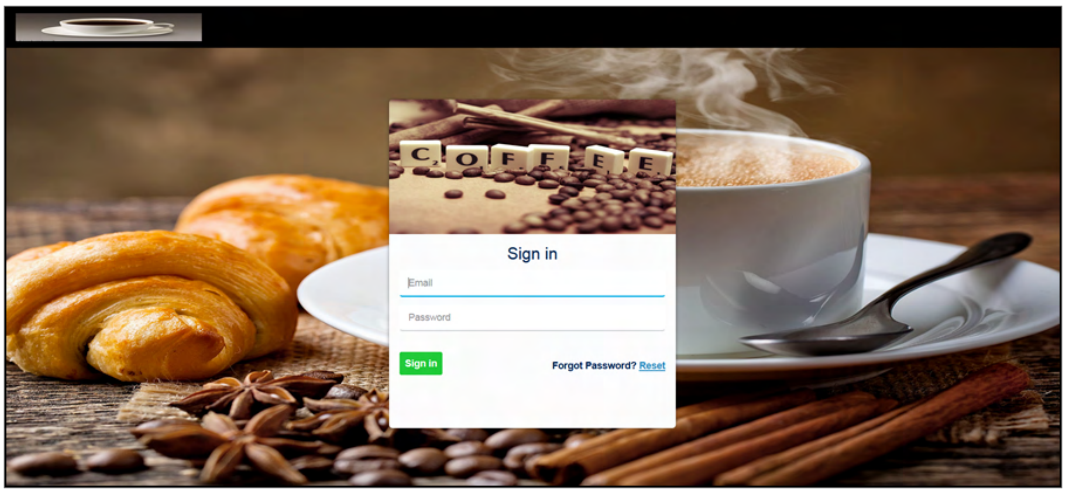
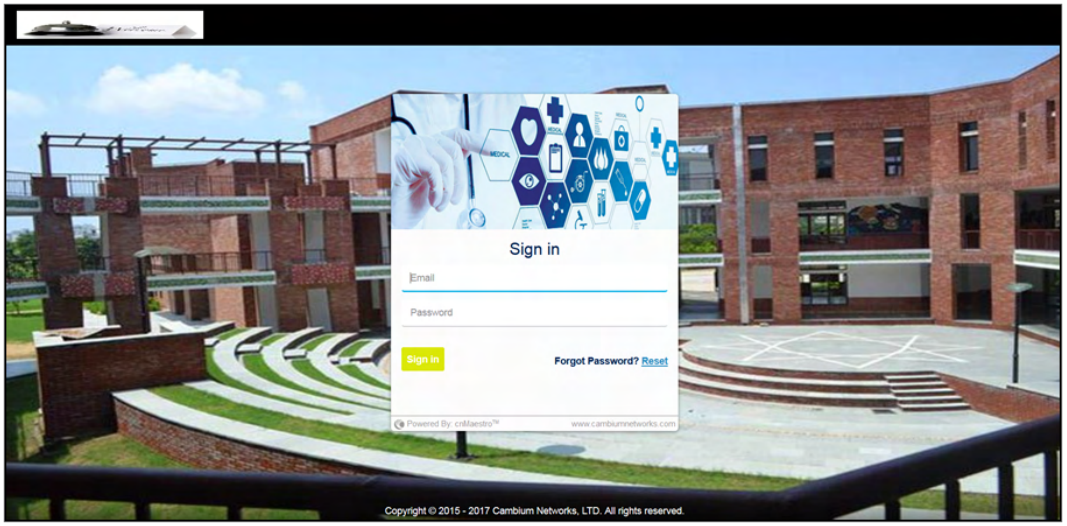


Figure 547 *Account UI - Sample 2*



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 122 *Tenant Administrator Roles*

Feature	Description	Administrator	Operator	Monitor
AAA Services (Global cnMaestro administrator only)	Add AAA services	None	None	None
Administration Settings (Global cnMaestro administrator only)	Change global application configuration, Onboarding settings like password change	None	None	None
API Management (Global cnMaestro administrator only)	Create API clients	None	None	None
Application Operations 1	Create Networks, Towers, and Sites	All	View	View
Application Operations 2	Tech Dump, import/export server data, change Account Type (Enterprise or Access and Backhaul)	None	None	None
Association ACL	Configure MAC list on the controller	All	View	None
Auto-provisioning (Global cnMaestro administrator only)	Support for global auto-provisioning rules	All	View	None

Table 122 *Tenant Administrator Roles*

Feature	Description	Administrator	Operator	Monitor
Audit logs	Logs user action of different features	All	All	All
Device Operations	Reboot device, link test, connectivity test	All	All	None
Device Override	Per-device configuration changes	All	All	View
Global Configuration	Apply configuration through Templates and AP 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 Monitoring)	None (Except System Monitoring)	None (Except System Monitoring)
User Management	Manage users, roles, and sessions	All	None	None

Configuring Managed Account Services

This section provides the following details on configuration of Account Services in cnMaestro:

- Enable Managed Accounts
- Creating Managed Account Services
- Creating Account
- Validating Account Users

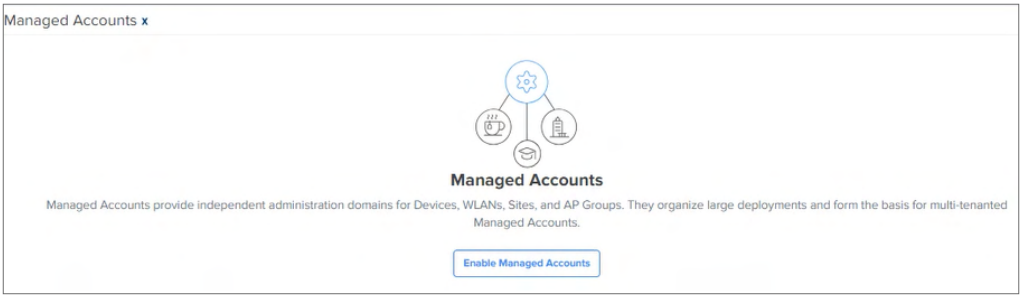
Enable Managed Accounts

By default, Account Services is disabled in the cnMaestro UI.

To enable Account Services:

1. Navigate to **Managed Services > Managed Accounts**.
2. Click the **Enable Managed Accounts.**

Figure 548 *Enabling Managed Accounts*



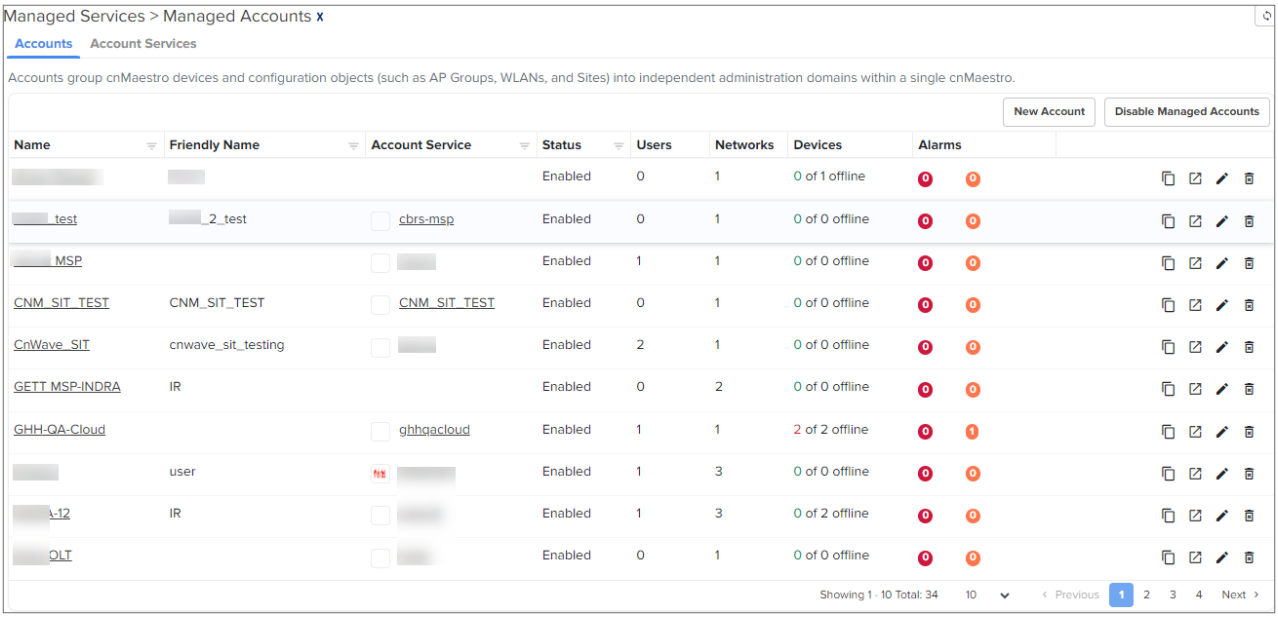
Note

Account Services provide independent administration domains for Devices, WLANs, Sites, and AP Groups. They organize large deployments and form the basis for multi-tenanted Account Services.

Additions in the cnMaestro UI when Managed Accounts is Enabled

- Once Managed Accounts is enabled, **Accounts** and **Account Services** tabs appear in the cnMaestro UI.

Figure 549 *Accounts and Account Services tabs*



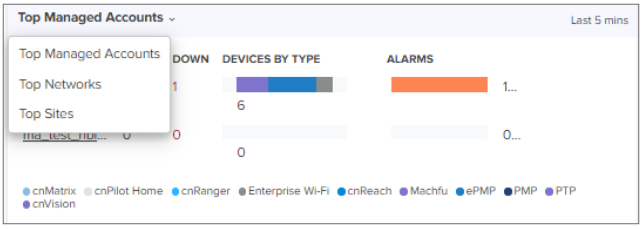
- The Header adds a select box that allows the Global Administrator to enter the context of Account selected.

Figure 550 *Managed Accounts Component in Header*



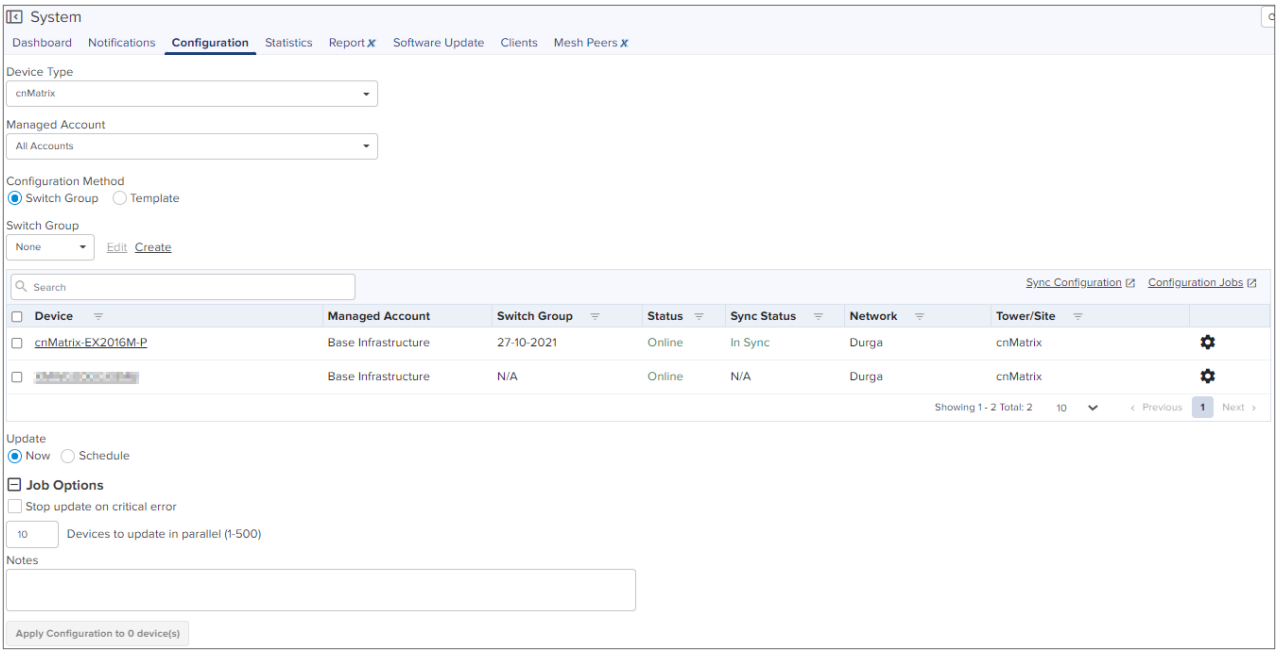
- The System Dashboard adds a Health component for Top Managed Accounts.

Figure 551 *Dashboard > Top Managed Accounts*



- Global tabs in the UI are updated with a Managed Account column.

Figure 552 *Managed Account Column*



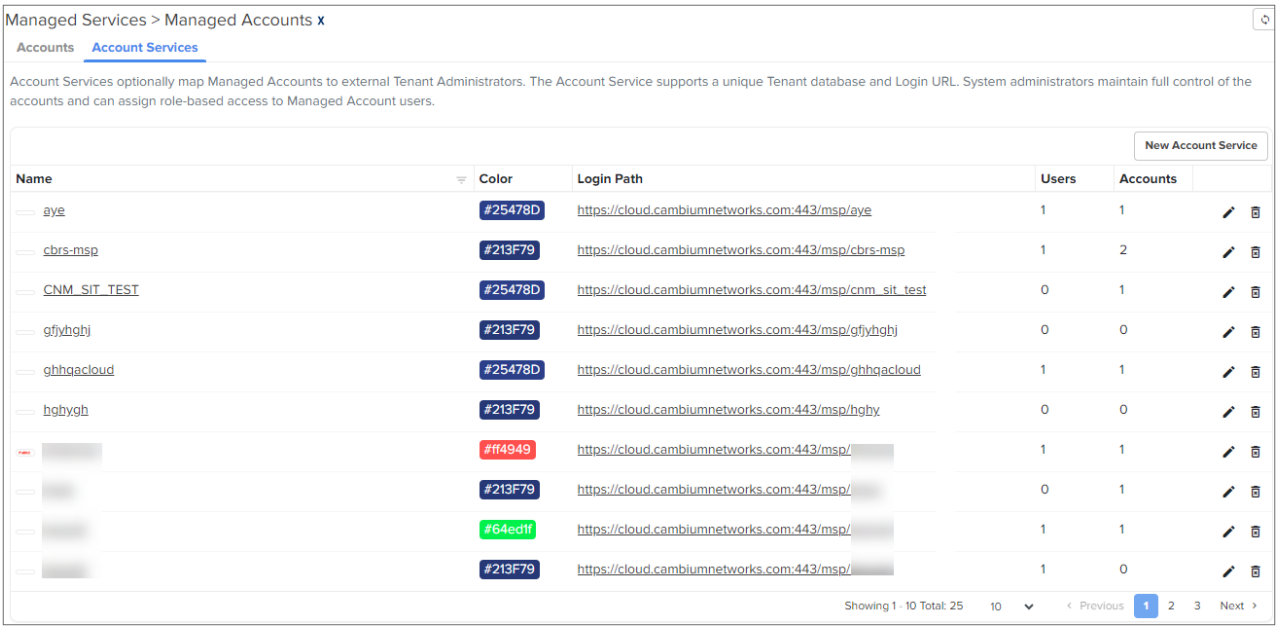
Creating Managed Account Services

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.

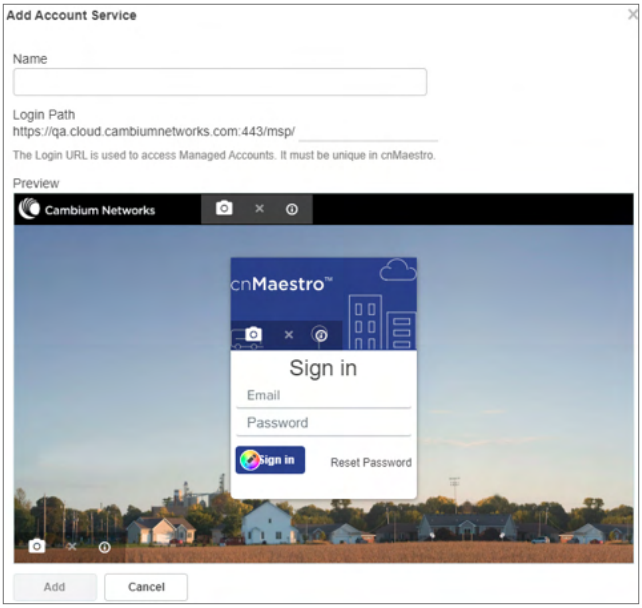
   Account Services Tab



2. Click **New Account Service.**

   The **Add Account Service** window is displayed.

   Add Account Service Window



3. Enter the following details:

Table 123 *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.

Table 123 *Parameters in the Add Account Service Window*

Parameter	Description
	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.

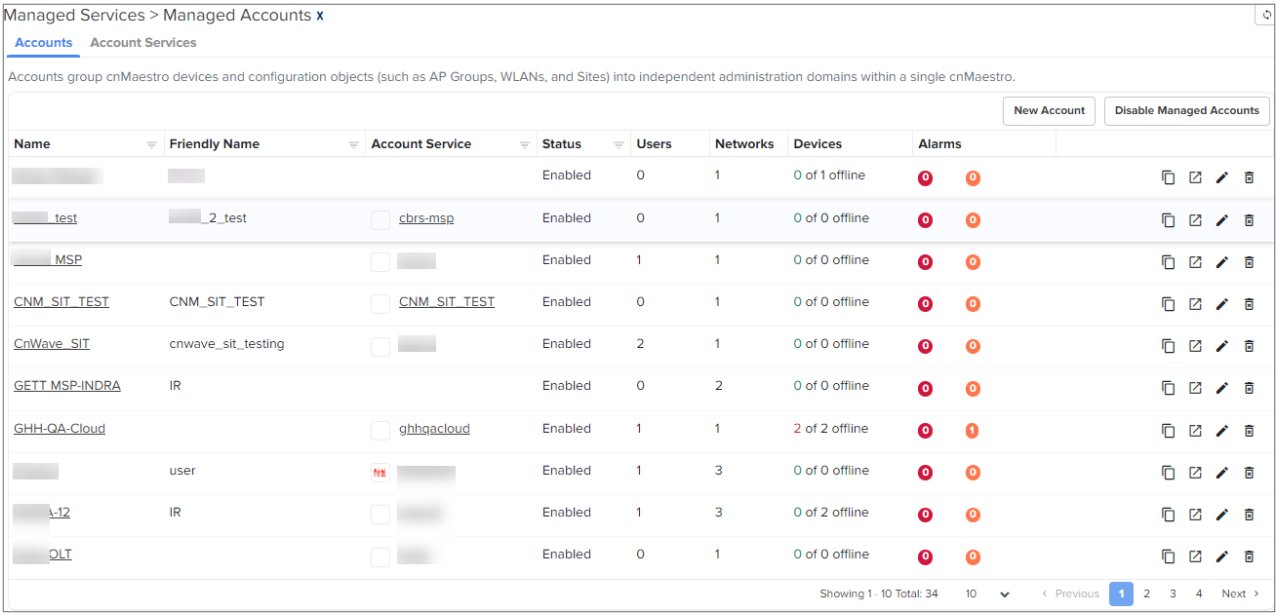
4. Click **Add**.

Creating Account

To create an Account:

1. Navigate to **Managed Accounts** > **Accounts** tab.

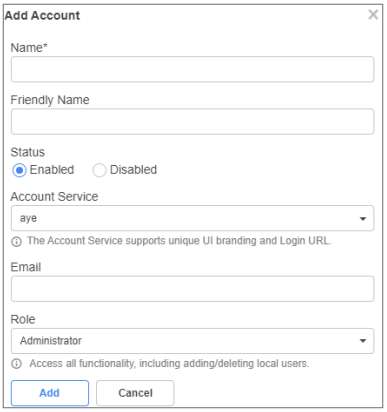
   Figure 553 *Accounts Tab*



2. Click **New Account**.

   The **Add Account** window is displayed.

Figure 554 *Add Account window*



3. Enter the following details:

Table 124 *Parameters in the Add Account Window*

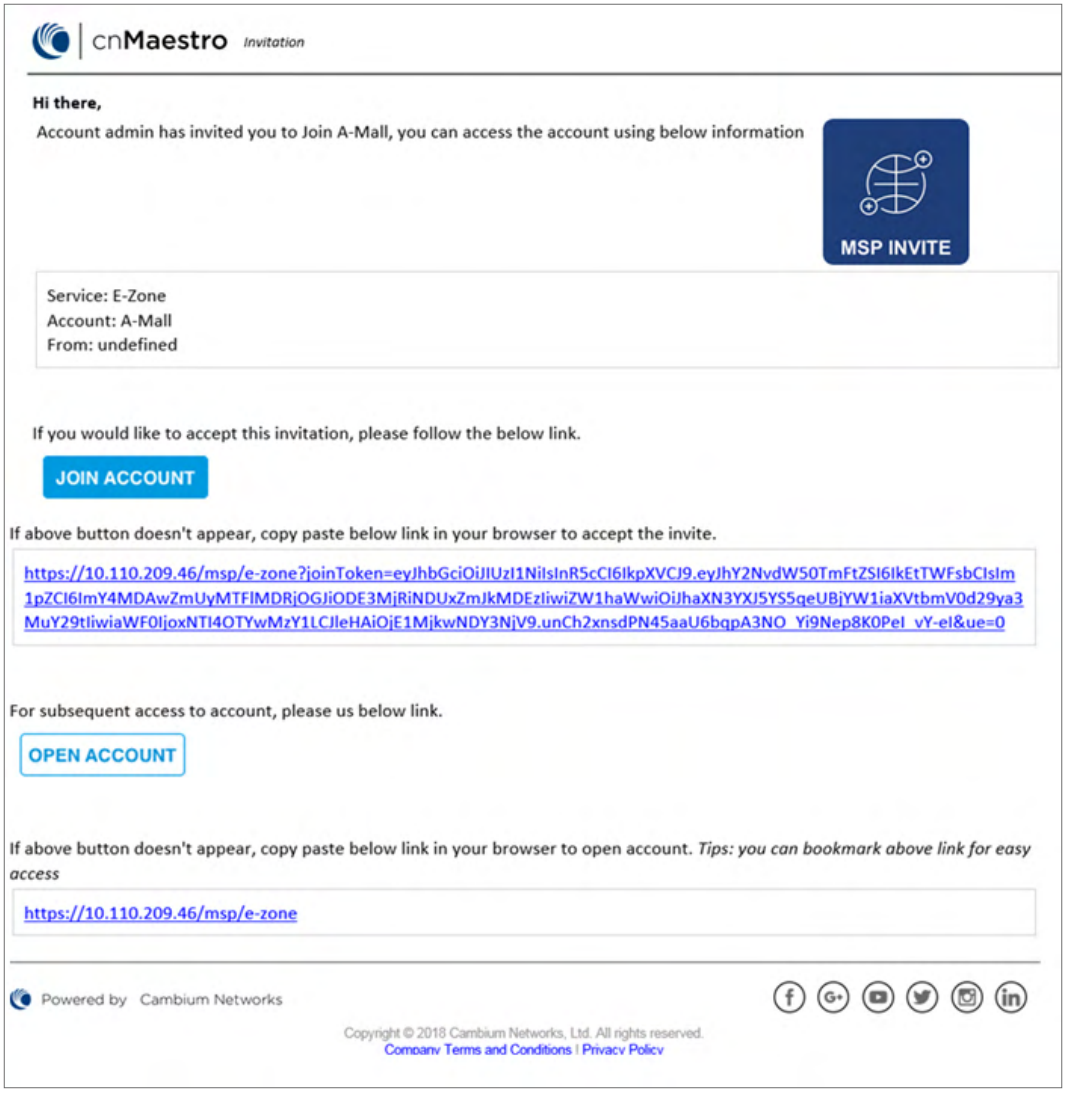
Parameter	Description
Name	Name of the Account. This is sent in the invitation email when users are invited to the account.
Friendly Name	The Friendly Name will be sent in the invitation email.
Status	Determines whether the account is enabled or disabled. When an account is disabled, all Account Users (users) are logged out.
Account Service	The Account Service used for branding and authentication.
Email	The email address of the first Account User. You can add more users after the account has been created.

4. Click **Add**.

Validating Account Users

Once an Account is created, the Account User is sent an email invitation. The email provides directions on how to access the Account UI and set their password.

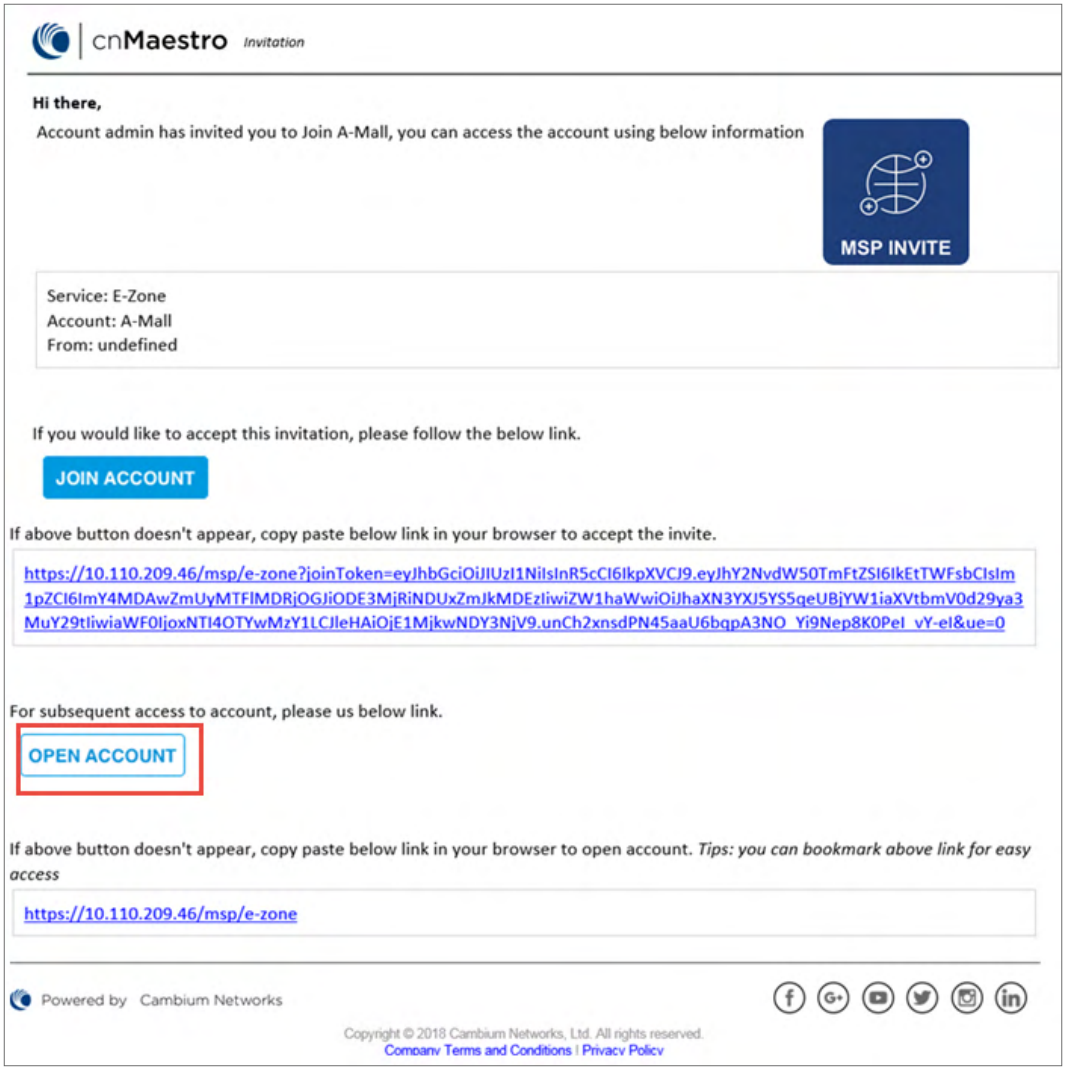
Figure 555 *Sample Email Invitation*



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 556 *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.

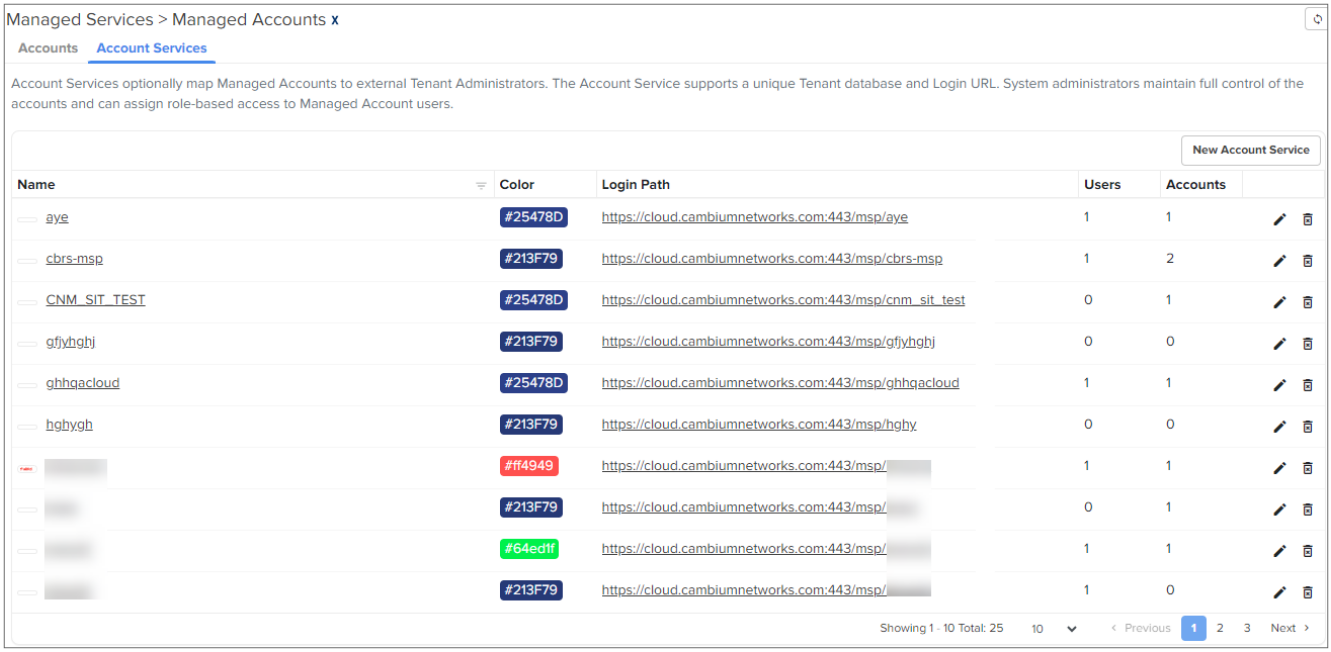
Note

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 557 *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 558 *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.

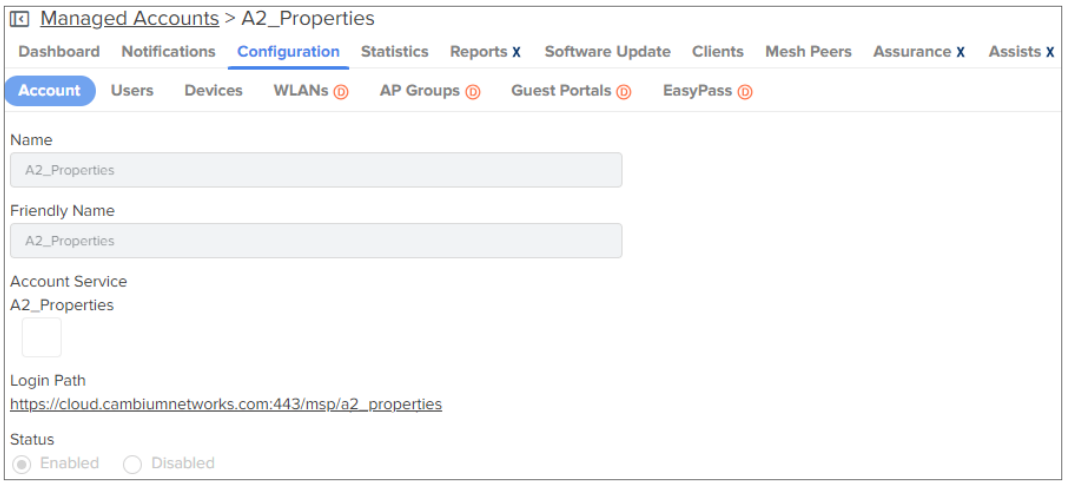
Note

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.

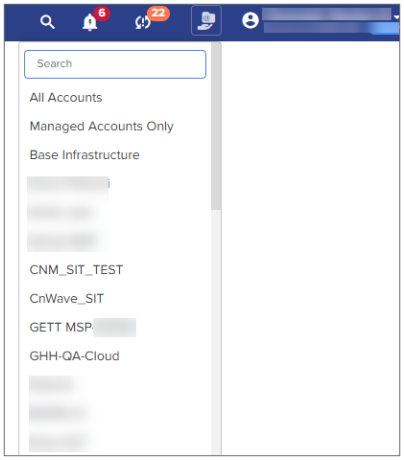
Figure 559 *Account View*



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 560 *Managed Account Administrator (User) View*



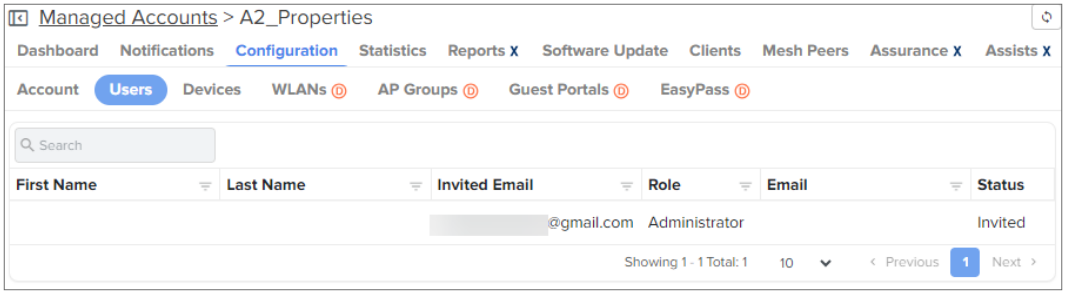
Users View

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.

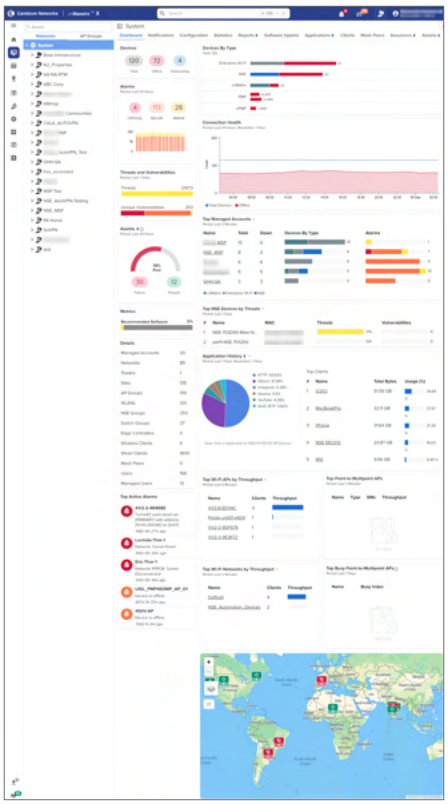
Figure 561 *Users*



System Dashboard

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

Figure 562 *System Dashboard*



Account Administration

AP Groups, WLANs, and Switch Groups have the following types of accessibility as shown below:

Table 125 *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.

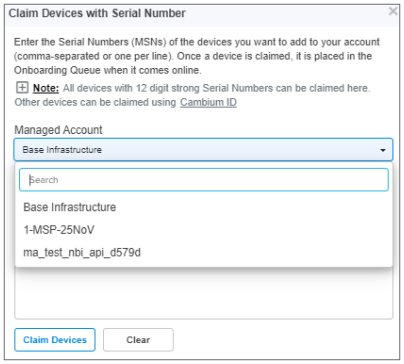
Device Management

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 563 *System Onboarding*



Device Onboarding

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

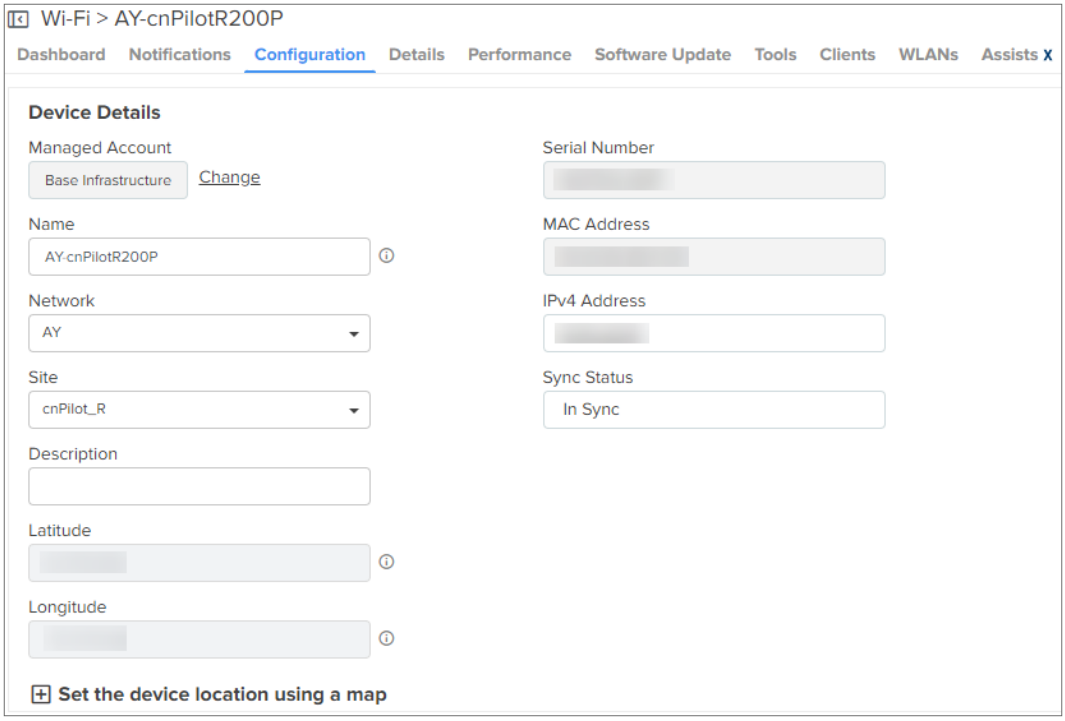
Note

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 564 *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 565 *Moving a device between Accounts in Enterprise View*



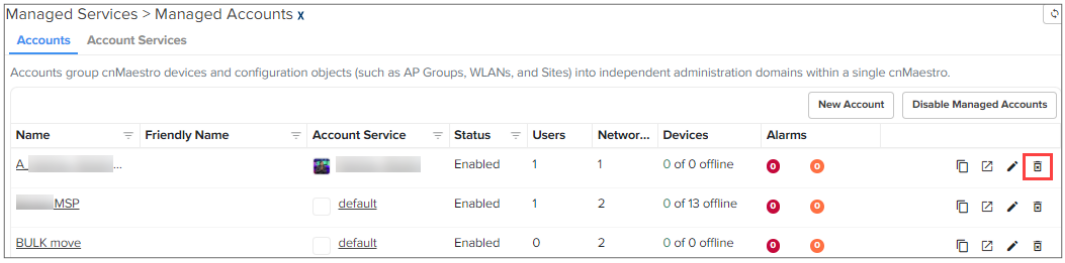
Account Deletion

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 566 *Account Deletion*



Disabling the Managed Accounts feature

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

Managing subscribers (end-customer)

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

This pocess involves the following actions:

1. Adding a Subscriber Service Profile
2. Adding a subscriber
   a. Modifying the owner details for the Subscriber App
3. Claiming the Home Mesh Router

Note

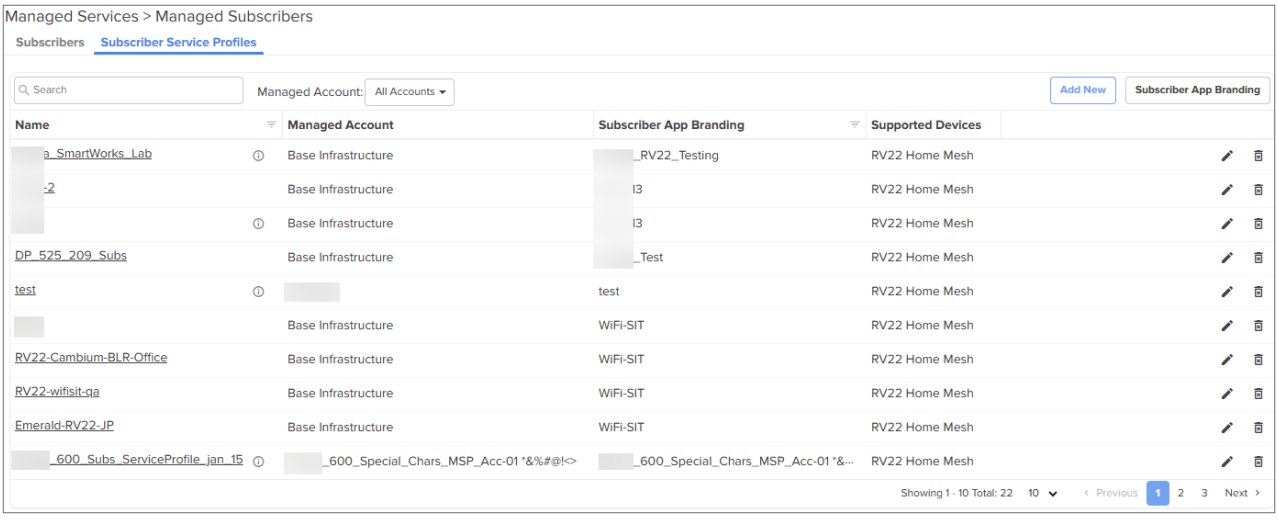
- Operator users can add new subscribers only.
- Operator users are not allowed to add or configure Subscriber Service Profiles or the Subscriber application branding.

Adding a Subscriber Service Profile

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

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

   The **Subscriber Service Profiles** page appears.



2. Click **Add New**.

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



3. Select the Home Mesh Router configuration to which you want to associate with the subscriber service profile and configure the parameters as described in Table 126.

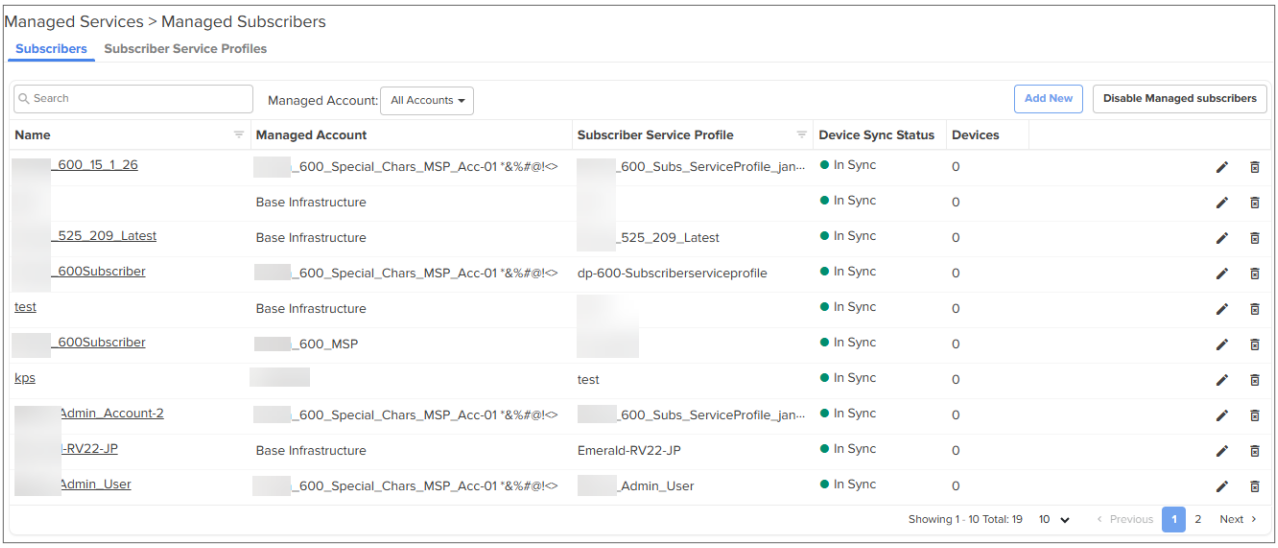
Table 126 *Subscriber Service Profile parameters*

Parameter	Description
Name	Name of the subscriber service profile.
Managed Account	Specifies the availability of the subscriber service profile across managed accounts. The following values are supported: • Base Infrastructure—Subscriber service profile is available only for the global account. It is not shared with other managed accounts. • Managed Account—Subscriber service profile is available only for that specific managed account. **Note** Once the Managed Account is configured for a Subscriber Service Profile, it cannot be modified.
Description	Brief description for the subscriber service profile.
Download (Mbps)	Download speed (in Mbps) configured for the profile.
Upload (Mbps)	Upload speed (in Mbps) configured for the profile.
Type	Displays the device type as **RV22 Home Mesh**. This field cannot be modified.
Device Configuration	Specifies the Wi-Fi AP group (created for the Home Mesh Router device type) that must be associated with the service profile. Select the group from the dropdown list.
Subscriber App Branding	Specifies the cnMaestro Subscriber application branding that must be used in this profile. All routers sent to subscribers in this service profile contain the selected branding logo and information. Select the required branding from the dropdown list. If no branding is present, create one by clicking the add (+) icon. See cnMaestro Subscriber application branding for more information.

4. Click **Save**.

Adding a subscriber

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



6. Click **Add New**.

   The **Add Subscriber** window appears.



7. In the **Add Subscriber** window, configure the details of the subscriber in the **Basic Information** section, as described in Table 127.

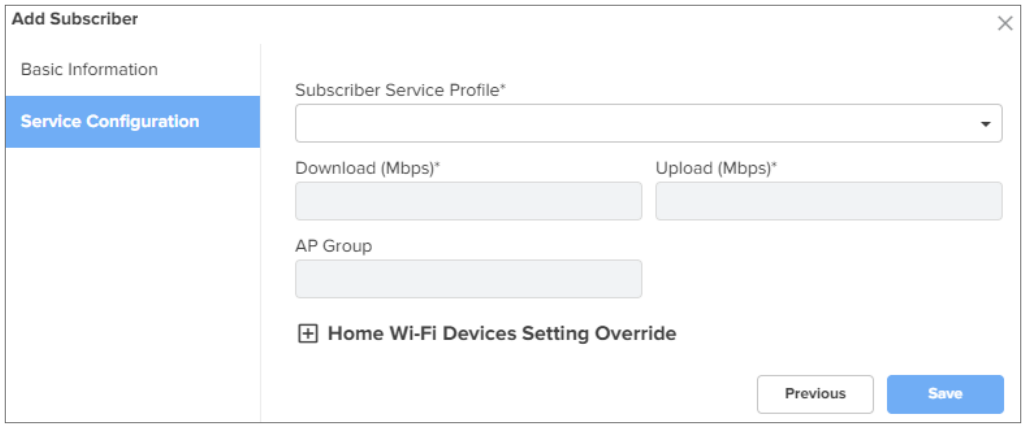
Table 127 *Subscriber > Basic tab parameters*

Parameter	Description
Full Name	Name of the subscriber.
Managed Account	Specifies the availability of the subscriber across managed accounts. The following values are supported: • Base Infrastructure—Subscriber is available only for the global account. It is not shared with other managed accounts. • Managed Account—Subscriber is available only for that specific managed account.

Parameter	Description
	Note Once the Managed Account is configured for a Subscriber, it cannot be modified.
Email ID	Email address of the subscriber. This email address receives the invitation to join the Home Mesh Router (RV22) site. Through this email address the user will be able to access and manage the router as a primary user and invite other users (secondary users), through the mobile application, to manage the routers. **Note** You can edit this email address at anytime. However, editing this email address will remove all existing users, both primary and secondary. For information about how to modify the email ID, refer to Modifying the owner details for the Subscriber App.
Phone Number	Phone number of the subscriber.
Customer ID	Unique ID for the subscriber.
Address	Address of the subscriber where the routers will be installed.

8. Click **Next**.

   The **Service Configuration** tab is displayed.



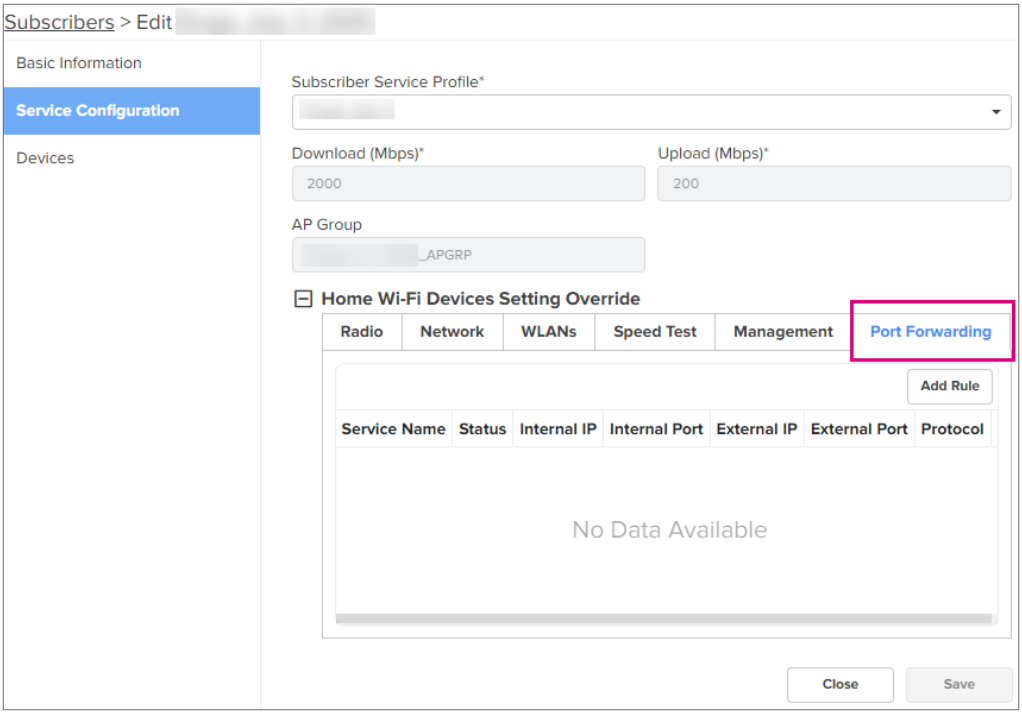
9. Select the subscriber service profile to be associated with this subscriber from the **Service Profile** dropdown list.
10. To configure port forwarding rules, expand the **Home Wi-Fi Devices Setting Override** section and click the **Port Forwarding** tab.

    Port forwarding allows external devices to access services hosted on internal network devices (for example, web servers and game servers) by routing traffic through the router to the configured internal IP and port.

Note

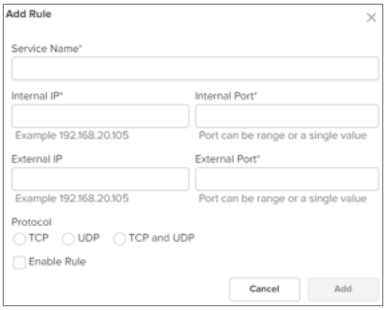
- The port forwarding rule can also be added by the subscribers through the cnMaestro Subscriber application.
- In a mesh configuration, this rule is applied only to the Mesh Base router.
- Port forwarding is available on RV22 Home Mesh Routers running version 1.2.0 or later.

- A maximum of 16 port forwarding rules are supported.



11. Click Add Rule.

    The **Add Rule** window is displayed.



12. Configure the following parameters:

Table 128 *Subscriber > Service Configuration > Port Forwarding rule parameters*

Parameter	Description
Service Name	Name of the service.
Internal IP	IP address of the device on the local network that will receive the forwarded traffic. For example, 192.168.20.105
Internal Port	Port number of the device on the local network that will receive the forwarded traffic. The field supports a single port number or a port range. For example: 80, 22, 3000-3010
External IP (Optional)	IP address from which incoming traffic is allowed. For example, 203.0.113.25

Parameter	Description
External Port	Port number of the router's public IP that listens for incoming connections. For example, 8080
Protocol	Type of protocol to be used for providing access. The following protocols are supported: • TCP • UDP • TCP and UDP
Enable Rule	Indicates whether the port forwarding rule must be enabled or disabled. Select the checkbox to enable the rule.

13. Click **Add**.

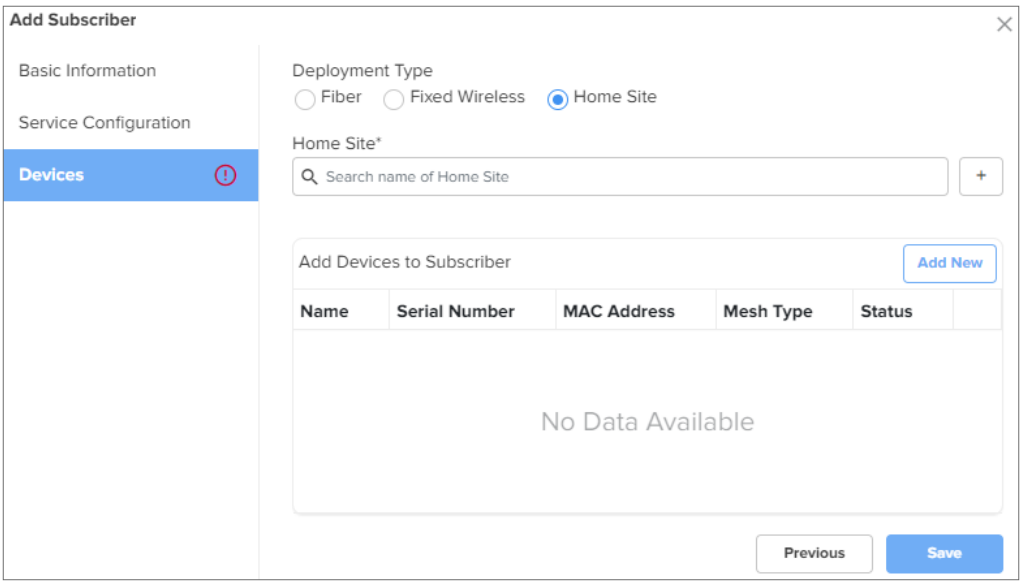
    The rule is listed in the **Port Forwarding** tab.

14. Click **Save**.

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

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

15. Click **Devices**.



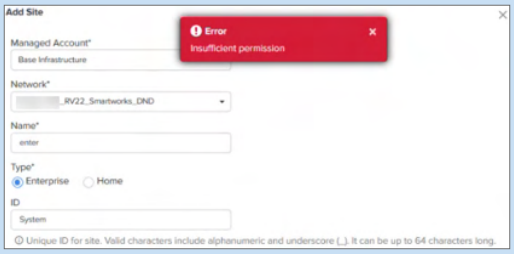
16. Select one of the following options in the **Deployment Type** field to filter the available deployment types:

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

Note

- Operator users can add or delete a home site for the RV22 Home Mesh Routers.

  However, they are not allowed to create Enterprise sites while creating subscribers. The following error message appears in case they try to create an Enterprise site:



- Operator users can also modify the details, such as latitude, longitude, and network, under the **Configuration** tab at the home site-level.

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

Modifying the owner details for the Subscriber App

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

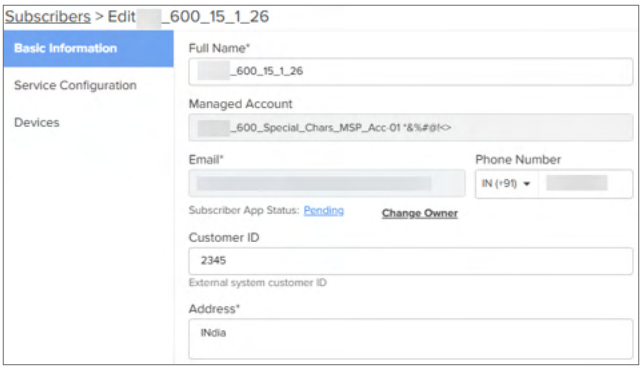
Warning

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

To modify the email address, complete the following steps:

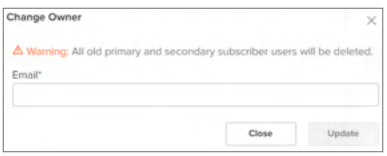
1. Navigate to the **Manage Services** > **Managed Subscribers** > **Subscribers** tab.
2. In the list of subscribers, click the subscriber name for which you want to modify the email ID.

   The corresponding subscriber details are displayed.



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

   The Change Owner window is displayed.



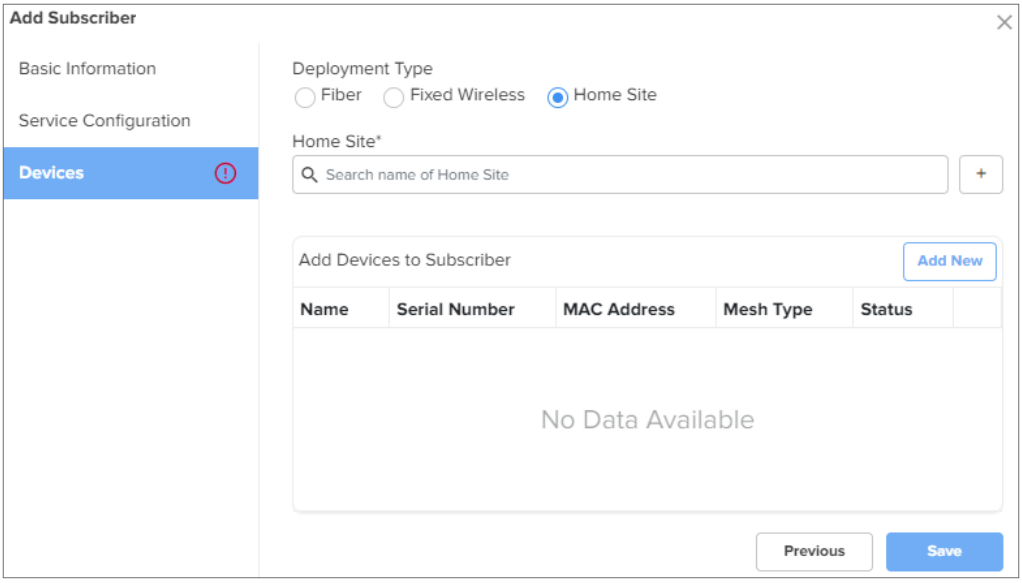
4. Enter the new email ID for the subscriber.
5. Click **Update**.

Claiming the Home Mesh Router

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

To claim the router, complete the following steps:

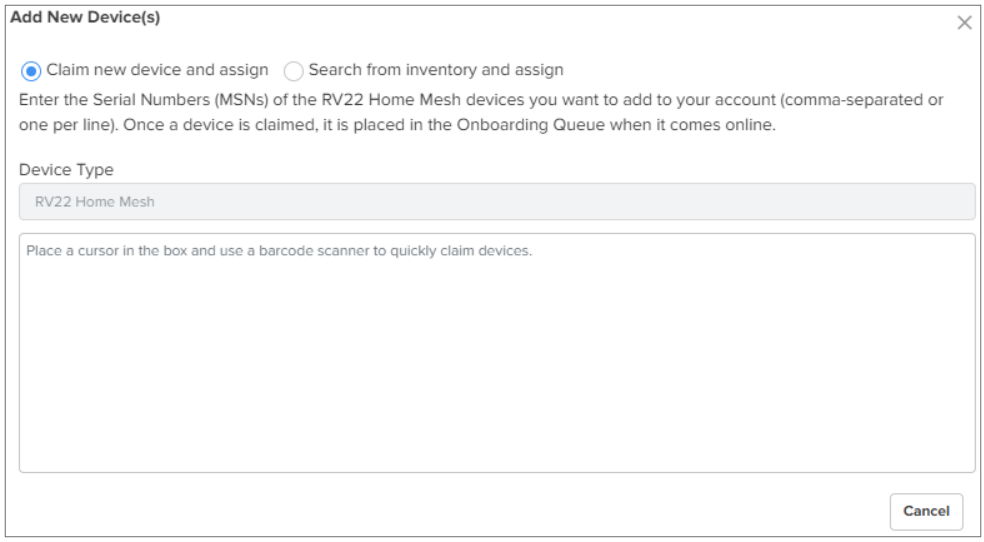
1. Navigate to the **Manage Services** > **Managed Subscribers** > **Subscribers** tab.
2. In the list of subscribers, select the subscriber name for which you want to associate the Home Mesh Router.
3. Click the **Devices** tab.
4. In the **Add Devices to Subscriber** section, click **Add New**.



The **Link Subscriber** window appears.

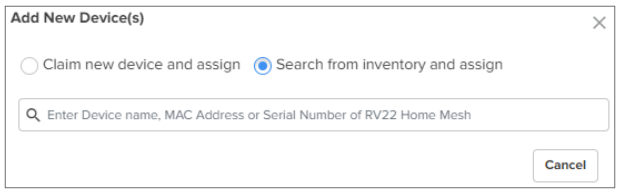
5. In the **Link Subscriber** window, link the Home Mesh Router to the subscriber by using any of the following methods:
   - To claim a new router that is not onboarded to cnMaestro, select the **Claim new and assign** option and enter the serial number of the device to be claimed.

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



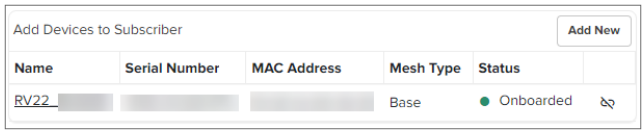
- To claim a router that is already onboarded to cnMaestro, select the **Search for inventory and assign** option.

  Enter the details of the router you want to claim.



6. Click **Assign**.

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



Note

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

Network Services

This section includes the following topics:

- API Client
- RESTful API
- EasyPass
- MarketApps
- CBRS
- Organization
- LTE
- Managing Edge Controller
- Installation Summary
- Spectrum Analyzer

API Client

Overview

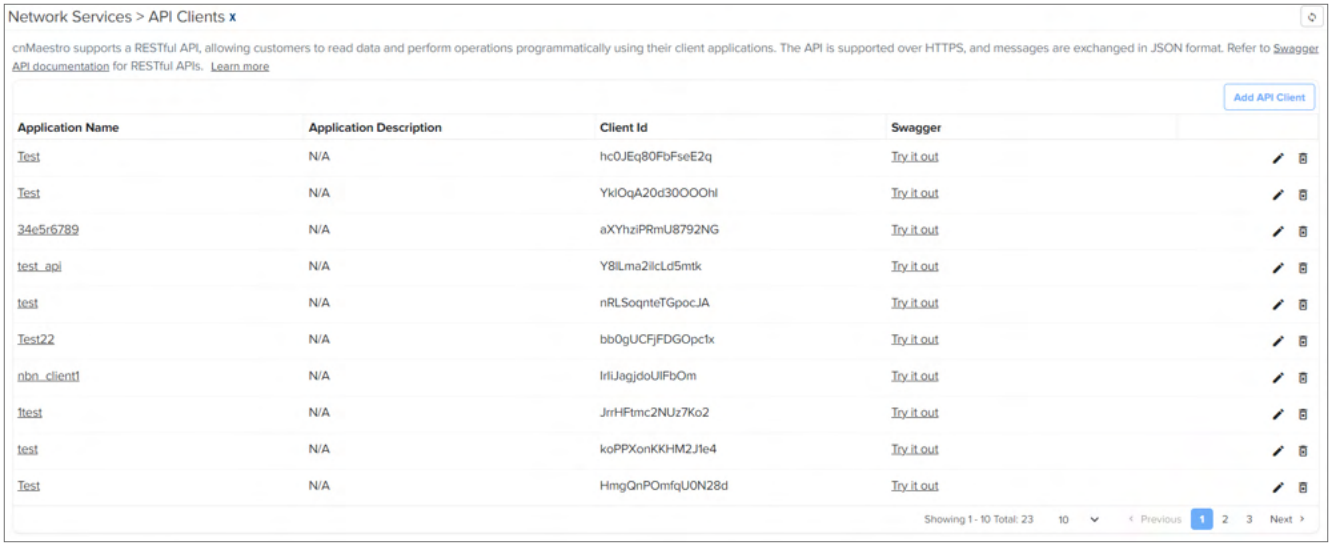
The cnMaestro RESTful API allows customers to manage their deployment programmatically using their own client applications. The API is supported over HTTPS, and messages are exchanged in JSON format. Modern programming languages have rich support for RESTful interfaces.

Note

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

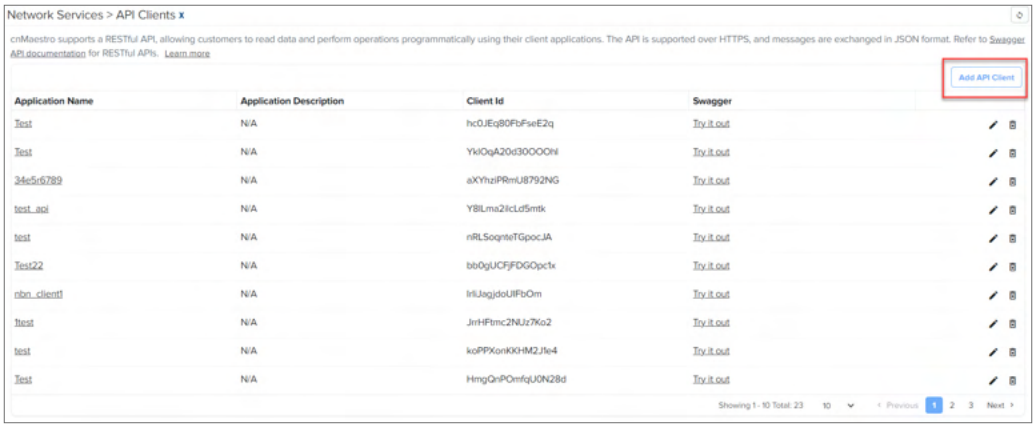
API Clients

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



To add an **API Client**:

1. Navigate to **Network Services** > **API Clients**.
2. Click **Add API Client**.



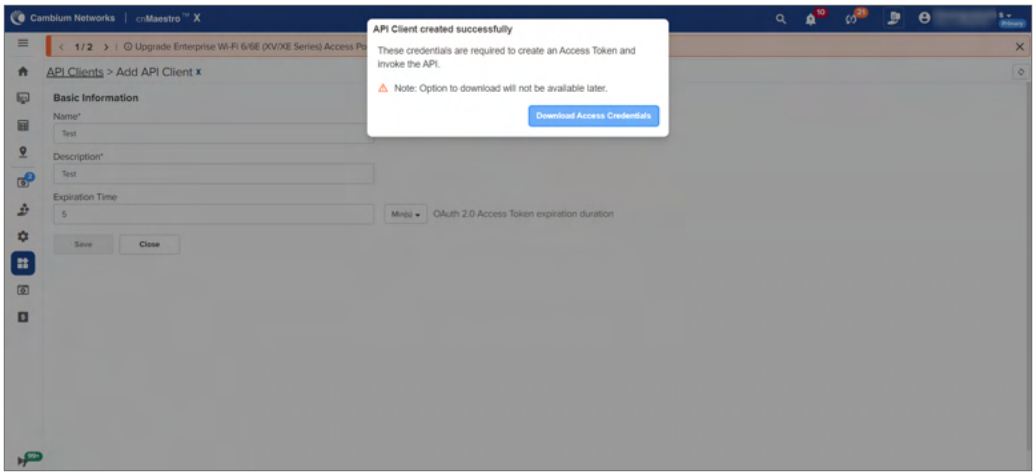
3. **Add API Client** window appears.



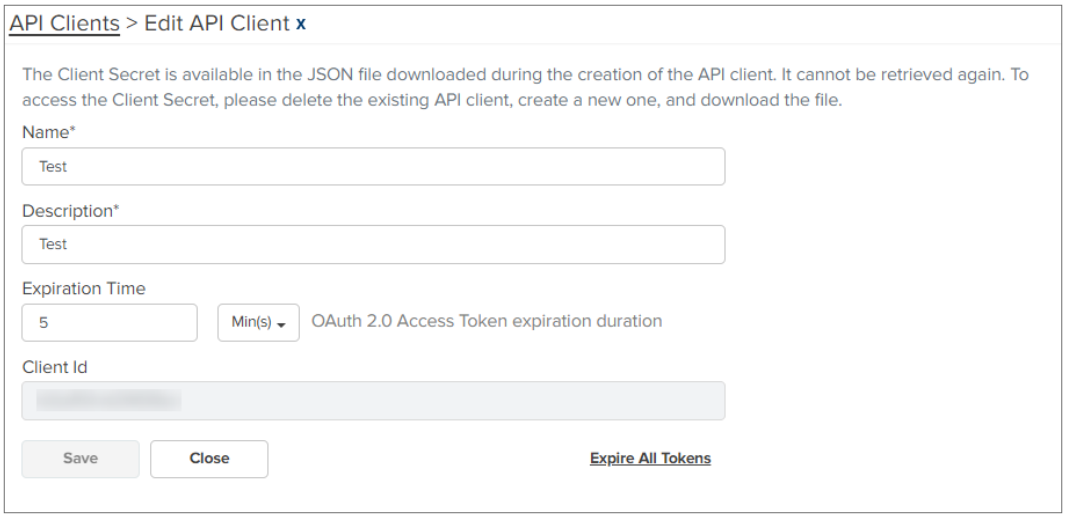
4. Enter **Name**.
5. Enter **Description**.
6. Select **Day(s)**, **Hour(s)**, and **Min(s)** from the dropdown list and enter the **Expiration Time**.
7. Click **Save**.

API Client created successfully window pops up.

8. Click **Download Access Credentials**.



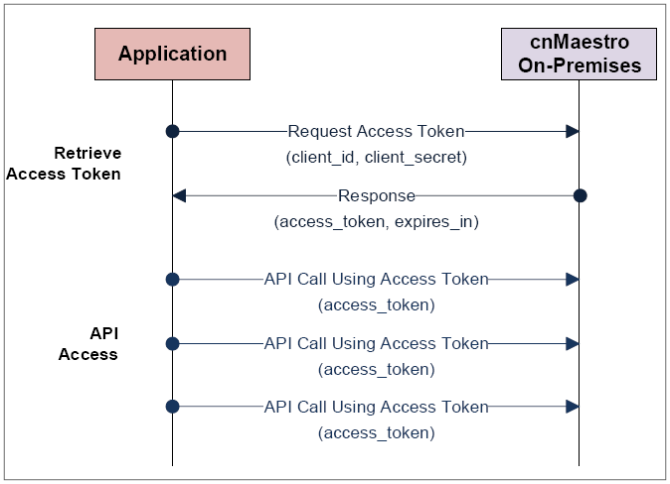
Once the API Clients is added, you can edit, view client Id, or expire all tokens from the **Edit API Client** page.



RESTful API Specification

Authentication

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



Establish a Session

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

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

API Access

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

Session Expiration

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

Rate Limiter

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

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

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

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

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

Devices	**GET**	**POST/Others**
101	10	3
501	24	3
1001	47	5

Devices	GET	POST/Others
2001	92	10
4001	163	17

Example of a Python client:

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

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

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

def call_api(method, host, path, access_token):
    """
    Makes HTTP call to an API with given method.
    Parameters:
        `method` -
 method for the new Request object: GET, OPTIONS, HEAD, POST, PUT, PATCH, or DELETE\n
        `host` - host for the url\n
        `path` - path for the url\n
        `access_token` - a valid access token for header
    Returns:
        `(response_status_code, headers, body)`
    """
    api_url = "https://%s%s" % (host, path)
    headers = {
      "Authorization":"Bearer %s" % access_token,
    }
    response = requests.request(method=method, url=api_
url, headers=headers, verify=False)
    headers = response.headers
    body = response.json()
```

```
    response_status_code = int(response.status_code)
    return response_status_code, headers, body

def main():

    try:
        # Getting the access token using client id and client secret
        access_token, expires_in = get_access_parameters(TOKEN_URL, CLIENT_
ID, CLIENT_SECRET)

        # For the purpose of the example, let's send 100 requests back to back
        for i in range(100):
            # Calling the endpoint with GET method
            status_code, header, body = call_api
('GET', HOST, '/api/v2/devices/statistics', access_token)
            # identifying any client or server side error codes
            client_errors = (status_code - status_code%100) == 400
            server_errors = (status_code - status_code%100) == 500

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

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

                if (status_code == 503):
                    sleep_time = 10 # default wait time
                    # try block prevents any dict value exception
                    try:
                        # Reading the header
                        sleep_time = int(header["Retry-After"])
                    except: pass
                    # if sleep_time is not greater than 0, defaulting to 10 seconds
                    sleep_time = sleep_time if sleep_time > 0 else 10
                    print("Sleeping for %d seconds" % sleep_time)
                    # sleeping the main thread
                    time.sleep(sleep_time)
            else:
                # process response
                print("Success: [%s]" %(json.dumps(body, indent=2)))

    except Exception as E:
        print("Failure: [%s]"%E)
        sys.exit()

if __name__ == "__main__":
    main()
```

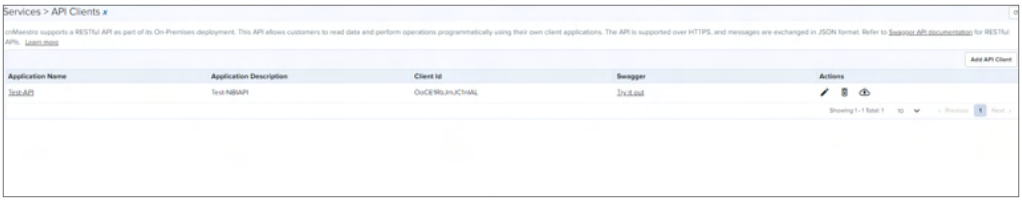
Swagger API

Introduction

Swagger API is a tool set that simplifies the process of RESTful web service documentation. It contains a standardized framework that allows visualization and interaction with API resources.

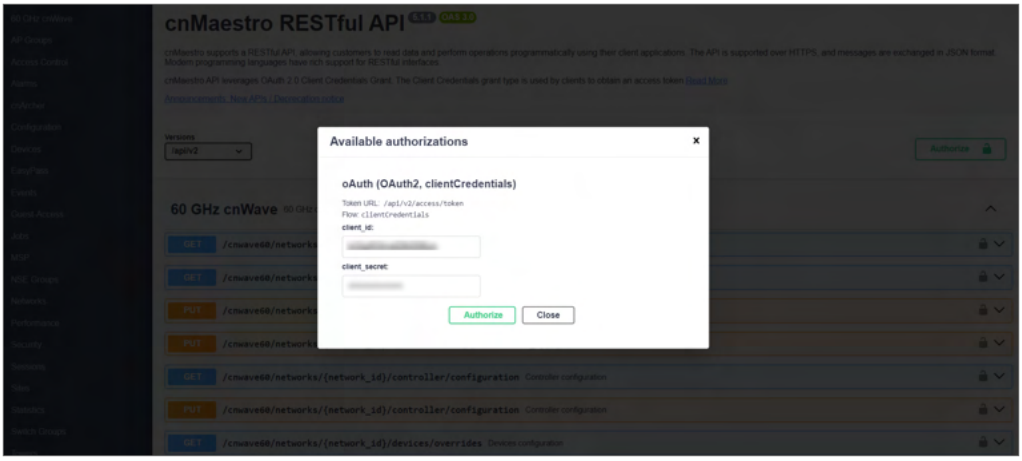
To access Swagger API, perform the following steps:

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



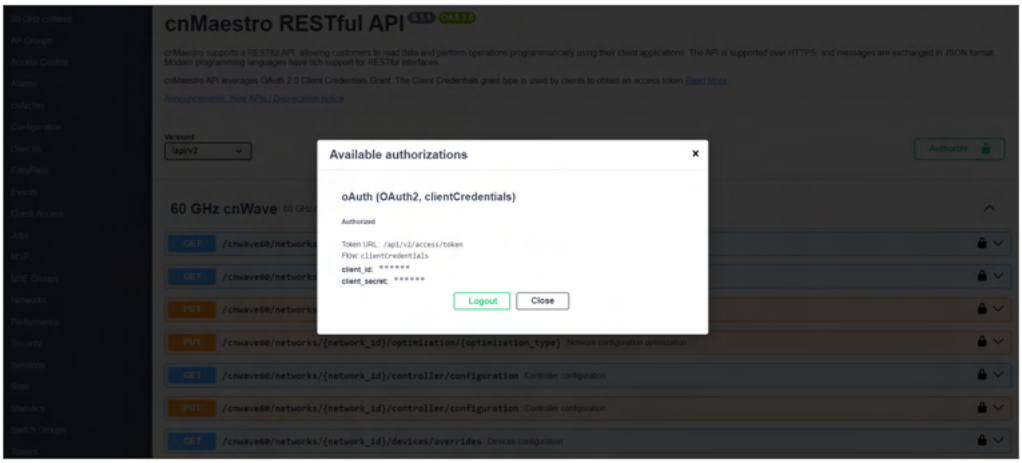
2. Click **Try it out**to open the Swagger UI.

   The **Available authorizations** window appears.



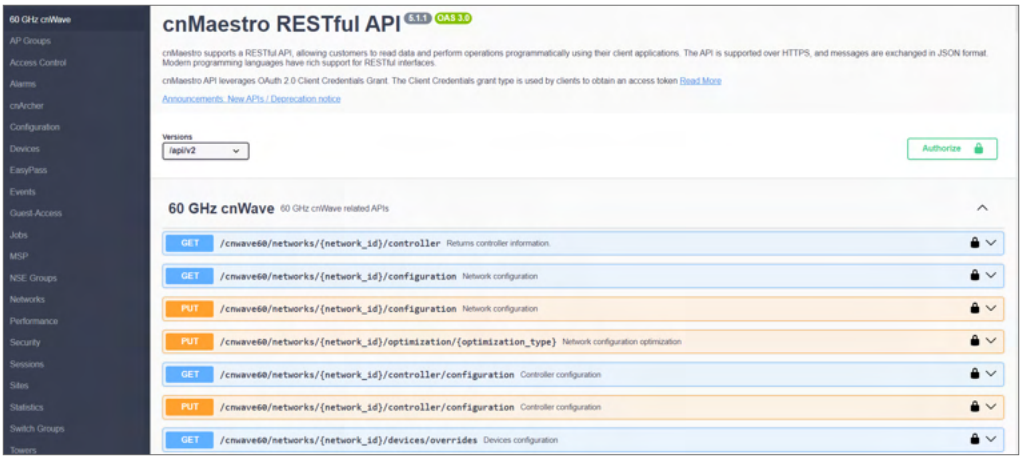
3. Enter **client_secret**.
4. Click **Authorize**.

   On successful authorization, an **Authorized** message appears in the **Available Authorization** window.



5. Click **Close**.

   The authorized **cnMaestro RESTful API** page appears.



API Session

Introduction

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

Retrieve Access Token

Access Token Request (RFC 6749, section 4.4.2)

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

Note

The fields are separated by a colon (:).

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

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

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

grant_type=client_credentials
```

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

```
POST /api/v2/access/token HTTP/1.1
```

```
Host: server.example.com
Content-Type: application/x-www-form-urlencoded

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

Access Token Response (RFC 6749, section 4.4.3)

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

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache
{
  "access_token":"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 129 *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"
}
```

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 130 lists the response codes that are supported in cnMaestro and may be returned through the HTTP protocol.

Table 130 *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 131 lists the HTTP request codes supported in cnMaestro.

Table 131 *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 132 *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.

Context	Details
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 133 *Sub-Resources*

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

Responses

Successful Response

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

The request URL is:

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

Response:

```
{
 "paging": {
   "offset": 0,
   "limit": 5,
   "total": 540
 },
 "data": [
   {
     "mac": "C1:00:0C:00:00:21",
     "type": "wifi-home"
   },
   {
     "mac": "C1:00:0C:00:00:18",
     "type": "wifi-home"
   },
   {
     "mac": "C1:00:0C:00:00:12",
     "type": "wifi-home"
   },
```

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

Error Response

Error Responses return a message and an error cause.

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

Parameters

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

Field selection

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

Table 134 *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 135 describes the standard filtering parameters as shown below:

Table 135 *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 136 are not specified, then the start or stop times will be open-ended.

Table 136 *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 137 *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 138 *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 139 *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 140 describes about the header and its values as shown below:

Table 140 ***Headers***

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

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

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

Body

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

```
grant_type=client_credentials
```

Response

The response returns credentials for API access.

Body

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

```
{
   "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.
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

This topic lists the changes made to the cnMaestro APIs.

- Sunsetted APIs/Fields
- Deprecated APIs/Fields

Sunsetted APIs/Fields

The following API fields have been removed from their respective APIs.

Request Method	Path	Details
GET	`/api/v2/devices`	The deprecated field `ap_group` has been removed in cnMaestro release 5.2.0. Use the `profile_attached` key as the replacement.
GET	`/api/v2/devices/{mac}/performance`	The deprecated fields `rx`, `tx`, `max_rx`, `min_rx`, `max_tx`, `min_tx` have been removed in cnMaestro release 5.2.0. Use the fields `rx_bps`, `tx_bps`, `max_rx_bps`, `min_rx_bps`, `max_tx_bps`, `min_tx_bps` as the replacement
GET	`/api/v2/devices`	The deprecated field `Location.type` has been removed in cnMaestro release version 5.2.0.
GET	`/api/v2/devices`	The deprecated field `status` has been removed in cnMaestro release version 5.2.0. Use the `online` field as the replacement.

Deprecated APIs/Fields

The following API fields have been deprecated and are scheduled for removal in future releases.

Request Method	Path	Details
GET	`/devices/clients`	The `ap_mac` field is deprecated and replaced with a new generic field, `device_mac`, to accommodate other non-Wi-Fi device types, such as NSE. For a similar reason, `rx_bytes` and `tx_bytes` fields have also been taken out of the radio property of an AP device. These deprecations will be removed in cnMaestro release 5.3.0.
GET	`/devices/wired_clients`	The `ap_mac` field is deprecated and replaced with a new generic field, `device_mac`, to accommodate other non-Wi-Fi device types, such as NSE. This deprecation will be removed in cnMaestro release version 5.3.0.

For a detailed overview of all new API changes, updates to existing APIs, and deprecations, see cnMaestro 5.2.1 API Swagger Announcements.

Devices, Statistics, and Performance APIs

Overview

cnMaestro APIs are defined within the Swagger tool, accessed here https://docs.cloud.cambiumnetworks.com/api/5.2.0/index.html. This section only presents additional details for the Device, Statistics and Performance APIs, which have unique responses based upon device type, and are not present within Swagger.

cnMaestro v2 API

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

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

There are unique API responses such as:

- Devices API Response (v2 Format)
- Statistics API Response (v2 Format)
- Performance API Response (v2 Format)

Devices API Response (v2 Format)

Name	Details	ePMP	PMP	Wi-Fi	cnReach	cnVision	PTP	PTP 8xx	cnMatrix	60 GHz cnWave	cnWave 5G Fixed	NSE
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	NSE
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	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Name	Details	ePMP	PMP	Wi-Fi	cnReach	cnVision	PTP	PTP 8xx	cnMatrix	60 GHz cnWave	cnWave 5G Fixed	NSE
	state.											
online	Offline or online	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
product	Product name	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
profile_attached	Profile attached to the device			✓								✓
registration_date	Registration date	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
role	Role of the device [PTP Slave, PTP Master]						✓					
site	Site			✓					✓	✓		✓
site_id	Site unique identifier			✓					✓	✓		
software_version	Active Software version	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
status_time	Uptime/downtime interval (seconds)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
temperature	Temperature							✓				
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.

Onboarding State	Details
UPDATING	Device software is being updated prior to getting onboarded.
ONBOARDED	Device is onboarded successfully.
ONBOARDED_WITH_ERRORS	Device is onboarded to cnMaestro but with errors.
WAITING_FOR_CLOUD_SYNC	Device is waiting for cnMaestro cloud sync process to acquire a subscription slot.
CLOUD_SYNC_ERROR	Device onboarding failed due to cloud sync error. For error details, see Device onboarding failure error codes.

Supported values for device type

- epmp
- pmp
- wifi-home
- wifi-enterprise
- cnreach
- ptp
- cnmatrix
- 60ghz-cnwave
- nse
- wifi-xirrus
- ptp 820/850
- cnWave 5G Fixed
- cnvision

Device onboarding failure error codes

Error Codes	Details
ERR_UNSUPPORTED_DEVICE	Claiming {{type}} devices is not currently supported.
ERR_NON_ENTERPRISE_WIFI_TYPE	Only cnPilot Enterprise (ePMP Hotspot), Enterprise Wi-Fi (E-Series and XE/XV-Series) and cnMatrix devices are allowed into Enterprise account.
ERR_NON_WIFI_TYPE	Cannot claim non Wi-Fi device under a Site.
ERR_UNSUPPORTED_TYPE	Unsupported device type in current account view - {{view}}.
ERR_UNKNOWN_DEVICE	Unknown Device.
ALREADY_CLAIMED	Device already claimed.
LTE_CLAIMED	cnRanger devices are not supported in production accounts.
ERR_INVALID_MSN	Invalid Serial Number.
ERR_OWNER_DIFFERENT	Device is claimed into another account.
ERR_INTERNAL	System encountered an internal error; please try again later. If the

Error Codes	Details
	problem persists, contact support.
ERR_INVALID_MAC	Invalid MAC.
ERR_DUPLICATE_KEY	The device is already claimed.
UNPROCESSABLE	Device state does not allow to cloud sync.
CBRS_ERROR_DEVICES	MAC is already claimed. It cannot be claimed on CBRS.
SUBSCRIPTION_FAIL	Device could not acquire slot.
SUBSCRIPTION_FAIL_FEATURE_MISMATCH	Device is mapped to another On-Premises instance.
SUBSCRIPTION_FAIL_TOO_MANY_ASSOCS	Device is mapped to another On-Premises instance.

Statistics API Response (v2 Format)

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

- 60 GHz cnWave
- cnMatrix
- cnReach
- Fixed Wireless (cnVision, ePMP and PMP)
- PTP 650/670/700
- PTP 820/850
- Wi-Fi
- cnWave 5G Fixed

60 GHz cnWave

General

Name	Details	Mode
cpu	CPU utilization	All
last_sync	Last synchronization (UTC Unix time milliseconds)	All
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

Name	Details	Mode
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

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

Networks

Name	Details
ip	IP address

cnReach

General

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

Networks

Name	Details	Mode
ip	IP address	All

Radios (Array format)

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

Fixed Wireless (cnVision, ePMP and PMP)

General

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

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

Networks

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

Radios

Name	Details	cnVision	ePMP	PMP
radio.auth_mode	Authentication mode	SM	SM	
radio.auth_type	Authentication type ePMP [open, wpa1, eap- 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

Name	Details	cnVision	ePMP	PMP
radio.frame_period	Frame period			AP
radio.dl_frame_utilization	Downlink frame utilization			AP
radio.dl_lqi	Downlink Link Quality Indicator			SM
radio.dl_mcs	Downlink MCS	SM	SM	
radio.dl_modulation	Downlink Modulation			SM
radio.dl_pkts	Downlink packet count	AP/SM	AP/SM	AP/SM
radio.dl_pkts_loss	Downlink packet loss			AP/SM
radio.dl_retransmits	Downlink Retransmission	AP/SM	AP/SM	
radio.dl_retransmits_pct	Downlink Retransmission percentage	AP/SM	AP/SM	
radio.dl_rssi	Downlink RSSI	SM	SM	SM
radio.dl_rssi_imbalance	Downlink RSSI imbalance			AP
radio.dl_snr	Downlink SNR (dB)	SM	SM	
radio.dl_snr_h	Downlink SNR (dB) horizontal			SM
radio.dl_snr_v	Downlink SNR (dB) vertical			SM
radio.dl_throughput	Downlink throughput	AP/SM	AP/SM	AP/SM
radio.mac	Wireless MAC	AP/SM	AP/SM	
radio.mode	Radio mode [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

Name	Details	cnVision	ePMP	PMP
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
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	Details	Mode
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

Name	Details	Mode
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
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

Name	Details	Mode
managed_account	Managed account name	All
ip	IP Address	All
mode	Device mode	All
name	Device name	All
network	Network	All
tower	Tower name	All
status	Status [online, offline, claimed, waiting, onboarding]	All
status_time	Uptime/downtime interval (seconds)	All
config_version	Current config version	All
type	Device type	All
connected_cpe	Number of CPEs connected to the BTS	BTS
registered_cpe	Number of CPEs registered with the BTS	BTS
cpe_registration_state	CPEs Registration State	CPE
cpe_registration_count	CPEs Registration Count	CPE
cpe_imsi	CPE Device Identity	CPE

Boot

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

Shutdown (Array format)

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

Interface Config

Name	Details	Mode
sfp1_speed	SFP1 Speed	BTS
sfp2_speed	SFP2 Speed	BTS

Interfaces (Array format)

Name	Details	Mode
interfaces[].port_name	Port name	BTS
interfaces[].in_octets	Received octets	BTS

Name	Details	Mode
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

Name	Details	Mode
ul_rx_power	Uplink Received Power	CPE
dl_rx_power	Downlink Received Power	CPE
ul_spatial_freq	Uplink Spatial Frequency	CPE
dl_spatial_freq	Downlink Spatial Frequency	CPE

Wireless and Ethernet interfaces

Name	Details	Mode
in_octets	Received octets	CPE
out_octets	Transmitted octets	CPE
in_ucast_pkts	Received unicast packets	CPE
out_ucast_pkts	Transmitted unicast packets	CPE
in_mcast_pkts	Received multicast packets	CPE
out_mcast_pkts	Transmitted multicast packets	CPE
in_bcast_pkts	Received broadcast packets	CPE
out_bcast_pkts	Transmitted broadcast packets	CPE
in_discards	Received discarded packets	CPE
out_discards	Transmitted discarded packets	CPE
in_errors	Received errored packets	CPE
out_errors	Transmitted errored packets	CPE

Performance API Response (v2 Format)

Performance API response v2 format is shown for the following devices:

- 60 GHz cnWave
- cnMatrix
- cnReach
- Fixed Wireless (cnVision, ePMP and PMP)
- PTP 650/670/700
- PTP 820/850
- Wi-Fi
- cnWave 5G Fixed

60 GHz cnWave

General

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

Radios (Array format)

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

Ethernet Ports (Array format)

Name	Details	Mode
ethports[].port	Port name	All
ethports[].rx_bps	Ports receive bits per second	All
ethports[].tx_bps	Ports receive bits per second	All
ethports[].min_rx_bps	Ports minimum receive bits per second	All
ethports[].min_tx_bps	Ports minimum transmit bits per second	All
ethports[].max_rx_bps	Ports maximum receive bits per second	All
ethports[].max_tx_bps	Ports maximum transmit bits per second	All

cnMatrix

General

Name	Details
mac	MAC address
managed_account	Managed account name
mode	Device mode

Name	Details
name	Device name
network	Network
site	Site
timestamp	Timestamp
tower	Tower
type	Device type

Switch

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

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

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

Ethernet Ports (Array format)

Name	Details	Mode
ethports[].pkt_error	Ports packet error	All
ethports[].port	Port name	All
ethports[].rx_bps	Ports receive bits per second	All
ethports[].tx_bps	Ports receive bits per second	All
ethports[].min_rx_bps	Ports minimum receive bits per second	All
ethports[].min_tx_bps	Ports minimum transmit bits per second	All
ethports[].max_rx_bps	Ports maximum receive bits per second	All
ethports[].max_tx_bps	Ports maximum transmit bits per second	All

Ethernet

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

PTP 820/850

General

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

Radio

Name	Details	Mode
radios[].id	Radio ID	All
radios[].max_rsl	Radio Maximum Receiver Signal Level	All
radios[].max_tsl	Radio Maximum Transmission Signal Level	All
radios[].min_rsl	Radio Minimum Receiver Signal Level	All
radios[].min_tsl	Radio Minimum Transmission Signal Level	All
radios[].peak_throughput	Radio Peak Throughput	All
radios[].radio_location	Radio Location	All
radios[].throughput	Radio Throughput	All
radios[].modem_max_mse	Modem maximum MSE in dB	All
radios[].modem_min_mse	Modem minimum MSE in dB	All
radios[].modem_max_xpi	Modem maximum XPI in dB	All
radios[].modem_min_xpi	Modem minimum XPI in dB	All
radios[].modem_max_mrmc_profile	Modem maximum MMRC	All
radios[].modem_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
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[].interference	Wi-Fi interference	All
radios[].noise_floor	Noise floor	All
radios[].non_wifi_interference	Non-Wi-Fi interference	All
Radios[].packet_error_rate	Packet error rate	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

Name	Details	Mode
timestamp	Timestamp	All
type	Device type	All
uptime	Duration (seconds) that the device has been online	All
cpe_registered	Count of CPEs registered with the BTS	BTS
cpe_connected	Count of CPEs connected with the BTS	BTS
cpe_registrationCnt	Number of times the CPE has registered with the BTS	CPE

Radio

Name	Details	Mode
ul_throughput	Uplink throughput of BTS	BTS
dl_throughput	Downlink throughput of BTS	BTS
cpe_ul_throughput	Uplink throughput of CPE	CPE
cpe_dl_throughput	Downlink throughput of CPE	CPE
cpe_ul_evm	Uplink Error Vector Magnitude (EVM) of CPE	CPE
cpe_dl_evm	Downlink EVM of CPE	CPE
cpe_ul_mcs	Uplink Modulation Coding Scheme (MCS) of CPE	CPE
cpe_dl_mcs	Downlink MCS of CPE	CPE
cpe_ul_rxPower	Uplink receive power of CPE	CPE
cpe_dl_rxPower	Downlink receive power of CPE	CPE

Client API Response (v2 Format)

Client details API Response v2 format are shown below:

Name	Details
address_type	IP address type (DHCP/Static)
ap_mac	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

Name	Details
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  **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.

Name	Details
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

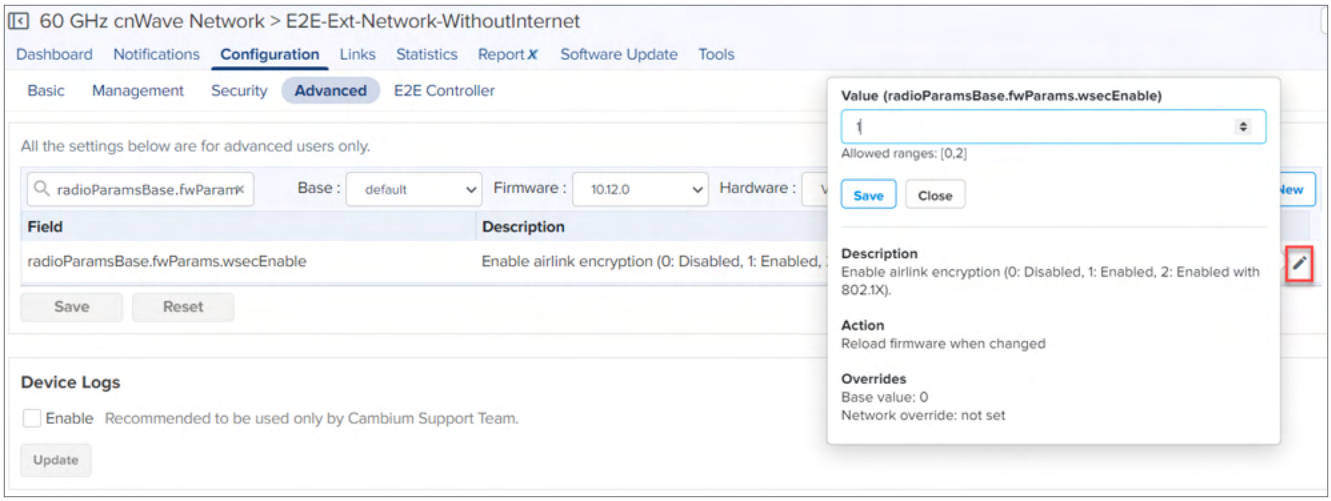
cnMaestro supports configuration overrides for 60 GHz cnWave E2E Network, E2E Controller, and Node(s) using the RESTful API.

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}`

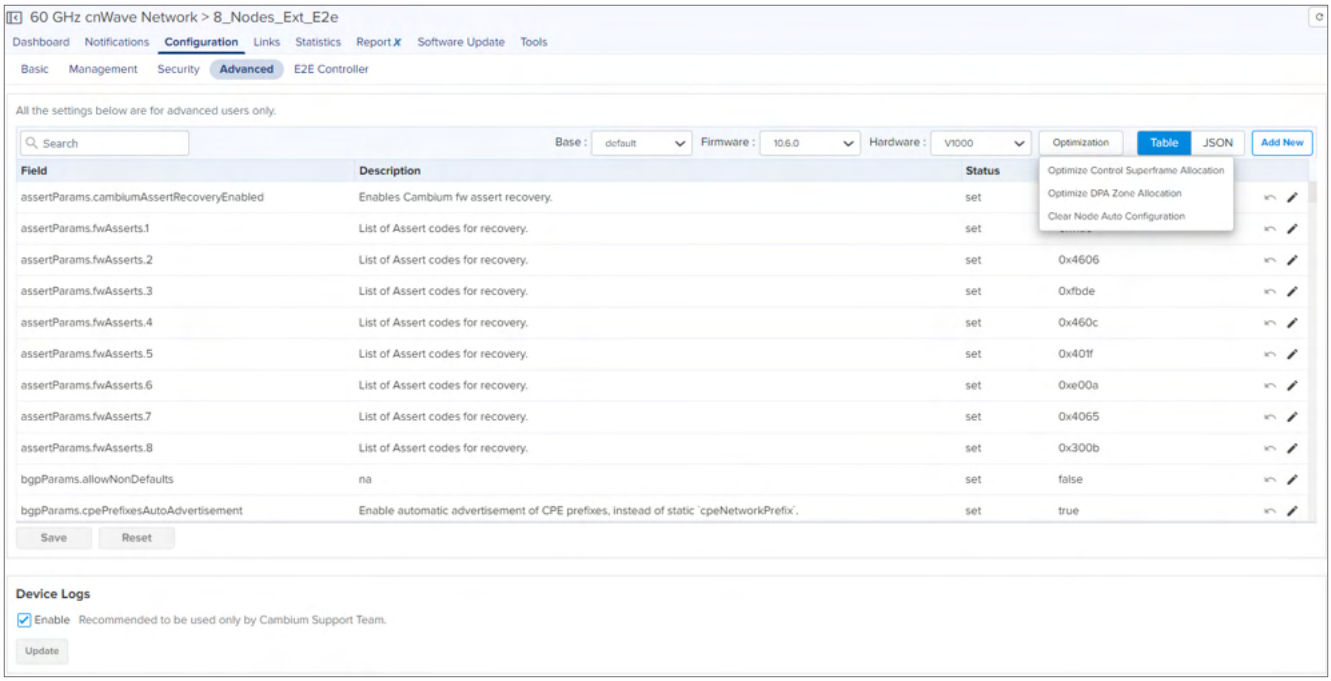
PUT `/api/v2/cnwave60/networks/{network_id}/optimization/{optimization_type}`

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

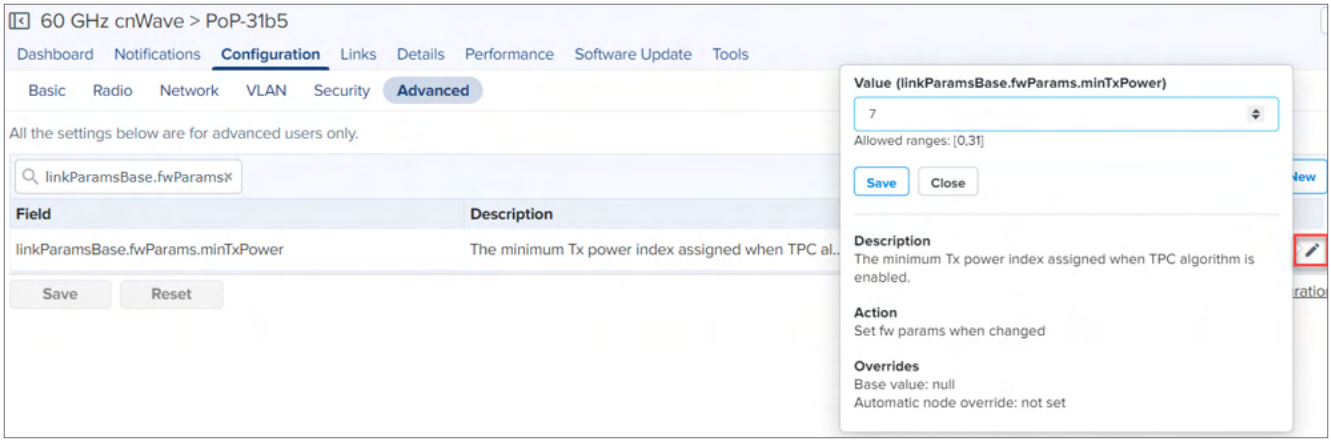
In case of field name `linkParamsBase.fwParams.minTxPower`, object to send in the API payload will be:

```
{
    "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`

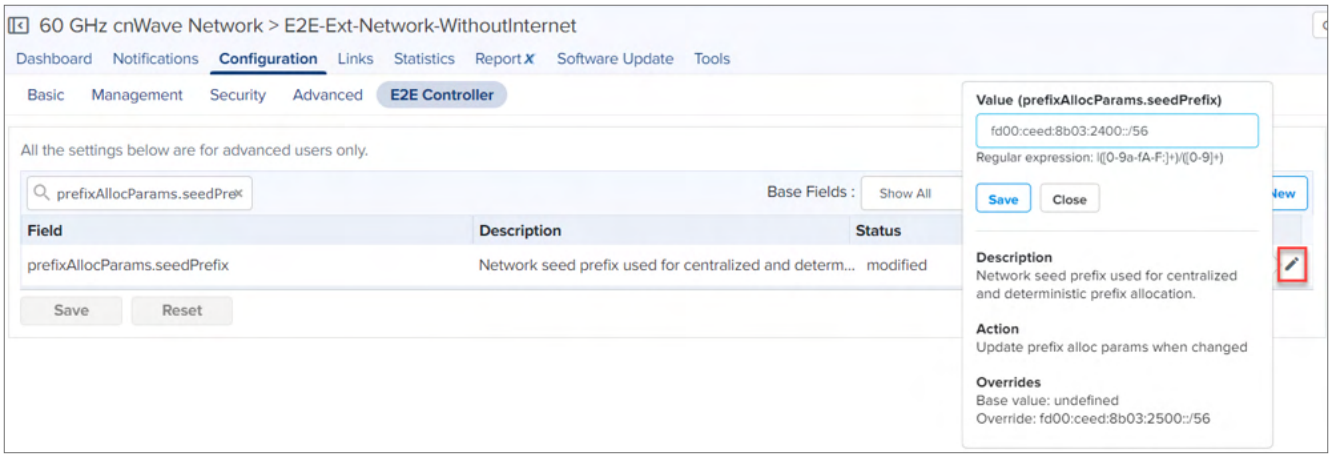
PUT `/api/v2/cnwave60/networks/{network_id}/controller/configuration`

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.

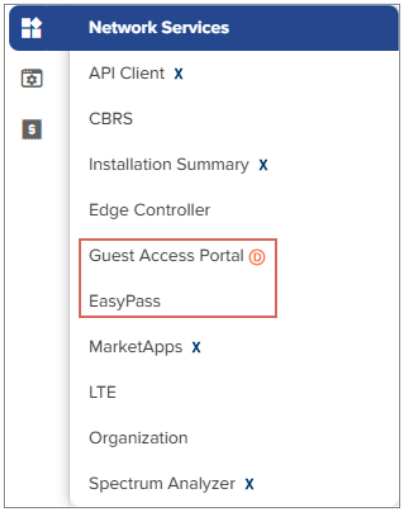
EasyPass

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

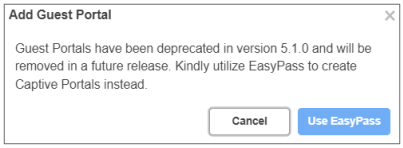
From cnMaestro 5.1.0 release onwards, the **Guest Access Portal** configuration wizard is deprecated and a new wizard, **EasyPass**, is introduced (as shown in Figure 567).

Figure 567 *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 568).

Figure 568 *The Add Guest Portal window*



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

Table 141 lists the supported devices and their compatibility with EasyPass.

Table 141 *List of supported devices - EasyPass*

Device	EasyPass support
Wi-Fi 5	Yes **Note**: Microsoft Entra ID and GSuite are not supported.
Wi-Fi 6	Yes

Table 141 *List of supported devices - EasyPass*

Device	EasyPass support
Wi-Fi 7	Yes
Xirrus APs	No

EasyPass portal types are grouped into the following categories:

- Guest/Public Access
- Employee/Student Access
- Combined

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

Guest/Public Access

This category includes the following portal types:

- One Click—All guests have access after agreeing to terms of use without needing to create an account. The **Social Login** options are integrated with One Click.



Note

The **Social Login** option is available only in cnMaestro Cloud accounts.

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

Management Systems (PMS) applications.

This is a Beta feature.



Note

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

Employee/Student Access



Note

The portal types listed under the **Employee/Student Access** category are available only in cnMaestro Cloud accounts.

This category includes the following portal types:

- Microsoft Entra ID **X**—A single sign-on process allows seamless access to Microsoft Entra ID X by integrating Wi-Fi and authentication.
- Google Login **X**—A single sign-on process allows seamless access to Google Login X by integrating Wi-Fi and authentication.
- Onboarding **X**— Clients can register on an open SSID with their email, Google Workspace, or Microsoft Entra ID (Office 365) credentials to receive a enhanced pre-shared key (ePSK), which can be used to connect to a secure network SSID.



Note

- Microsoft Entra ID **X** and Google Login **X** are supported on APs running firmware version 6.x or later.
- Onboarding **X** is supported only on Wi-Fi 6 and 6E APs running firmware version 6.6.2 or later.

Combined

This category includes the following portal types:

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



Note

- cnMaestro Essentials supports a maximum of four EasyPass portals.
- cnMaestro X supports a maximum of 500 EasyPass portals.

The following table lists the support of EasyPass portal types across Cloud and On-Premises accounts.

Table 142 *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**	✔	✔

EasyPass portal type	cnMaestro Cloud	cnMaestro On-Premises
Voucher	✔	✔
One Click	✔	✔
Social Login (Google and Facebook) Available on the **Design** page in the following portals: • One Click • One Click + Voucher • One Click + Paid **X**	✔	
Paid **X**	✔	✔
WiFi4EU	✔	✔
Third-party Integration	✔	
Hospitality PMS **Beta**	✔	
Employee/Student Access		
Microsoft Entra ID **X**	✔	
Google Login **X**	✔	
Onboarding **X**	✔	
Combined		
One Click + Voucher	✔	✔
One Click + Paid **X**	✔	✔
Voucher + Paid **X**	✔	✔

Implementation of EasyPass portals for various types of users

Table 143 lists the various types of users for whom the EasyPass portals can be implemented or be best suited:

Table 143 *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 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
Microsoft Entra ID **X**	✔				✔						
Google Login **X**	✔				✔	✔					
Onboarding **X**	✔			✔	✔			✔			✔

EasyPass configuration

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

- Creating a portal
  - Creating One Click portal
  - Creating Self Registration X portal
  - Creating Sponsored Guest X portal
  - Creating Voucher portal
  - Creating Paid X portal
  - Creating WiFi4EU portal
  - Creating Microsoft Entra ID X portal
  - Creating Google Login X portal
  - Creating Onboarding X portal
    - Adding a new user
  - Creating One Click + Voucher portal
  - Creating One Click + Paid X portal
  - Creating Voucher + Paid X portal
  - Creating a Third-Party Integration portal
  - Creating a Hospitality PMS Beta portal
- Configuring common parameters
  - The Basic screen parameters
  - The Limits screen parameters
  - The Design screen parameters
  - The Voucher screen parameters

- The One Click screen parameters
- The Plans screen parameters
- Accessing the common tabs
  - Sessions
  - Guests
    - Adding a new guest user
  - Vouchers
  - Paid Transactions X
  - Users X

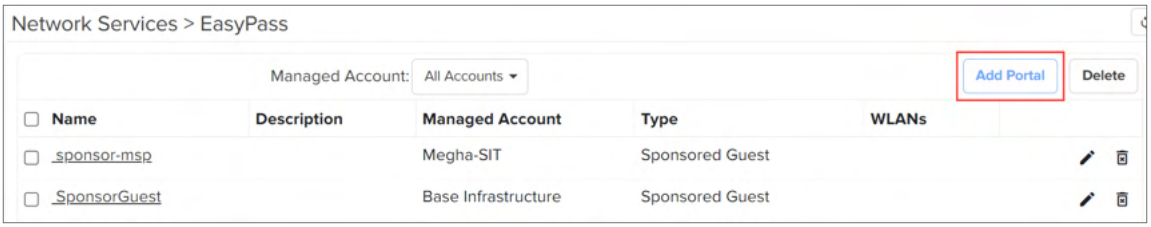
Creating a portal

Complete the following steps to create a portal:

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

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

   Figure 569 *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 570 displays the options available for cnMaestro Essentials.

   Figure 570 *The Select Portal Type window—cnMaestro Essentials*

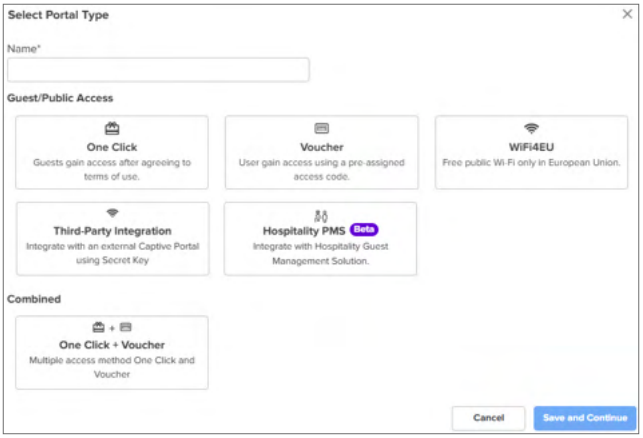
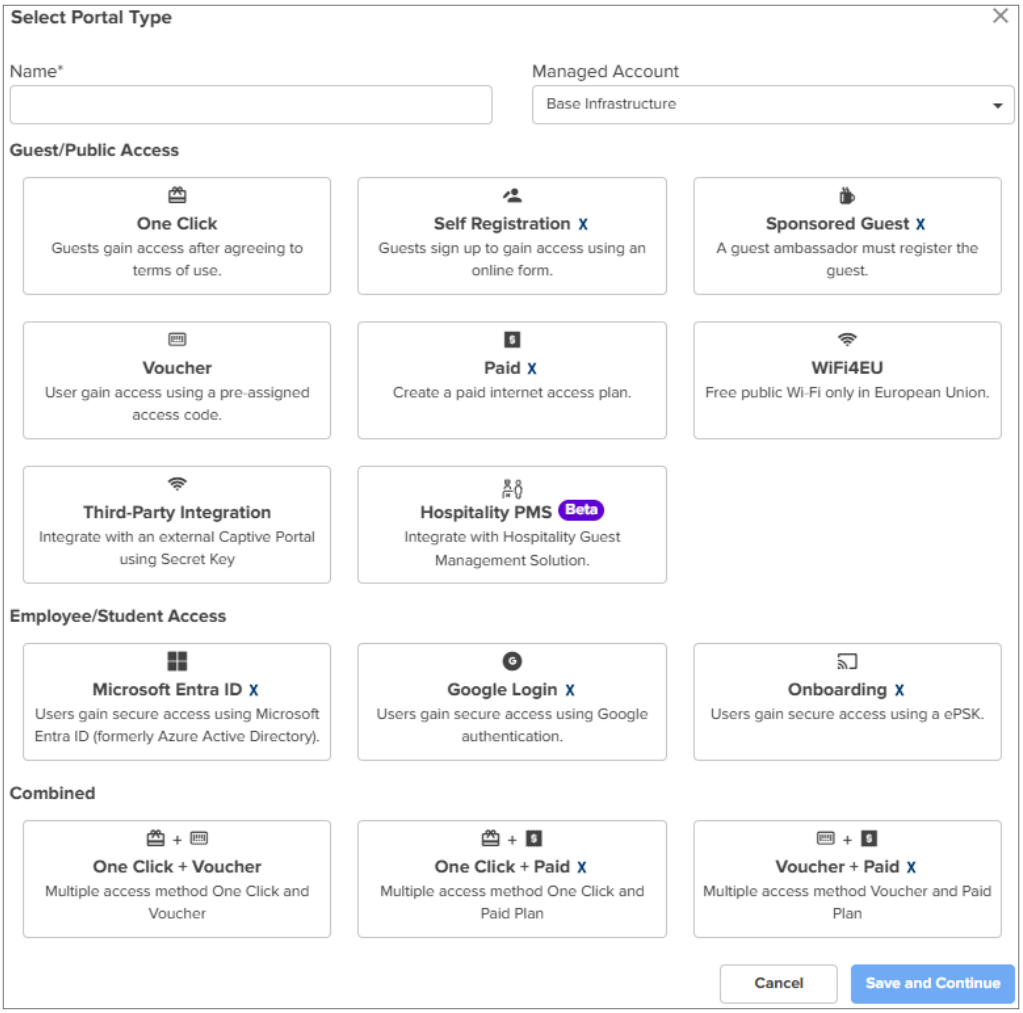


Figure 571 displays the options available for cnMaestro X.

Figure 571 *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 a 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.

<Available in Essentials and X>The **Managed Account** option is available only on cnMaestro X

accounts.

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

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

   For information on parameters of the **Basic** screen, see The Basic screen parameters.
7. Click the next tab.



Note

- For **One Click** portal, go to step 8 and configure the parameters on the **Limits** screen.
- The **Voucher**, **One Click + Voucher**, and **Voucher + Paid X** portal types have a few common parameters that you must configure on their respective **Voucher** screens. For information on parameters of the **Voucher** screen, see The Voucher screen parameters.
- The **Paid X**, **One Click + Paid X**, and **Voucher + Paid X** portal types have a few common parameters that you must configure on their respective **Plans** screens. For information on parameters of the **Plans** screen, see The Plans screen parameters.
- The **One Click + Voucher**, and **One Click + Paid X** portal types have a few common parameters that you must configure on their respective **One Click** screens. For information on parameters of the **One Click** screen, see The One Click screen parameters.

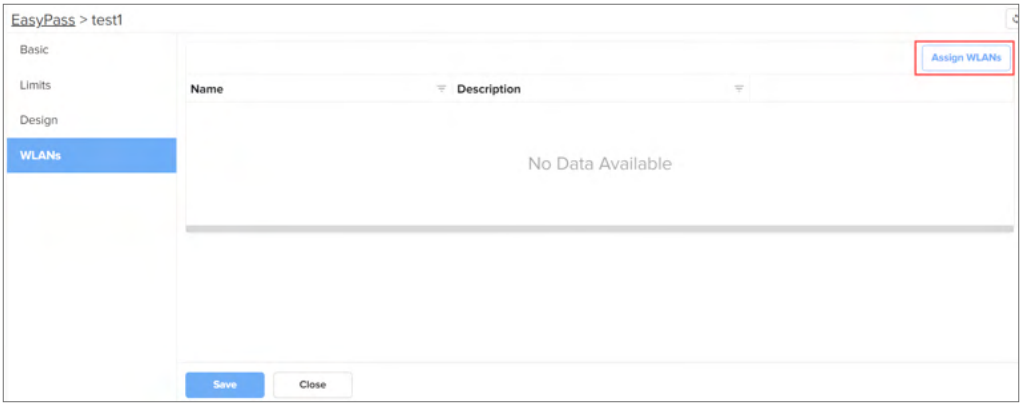
   Depending on the portal type you selected, you will either see a **Limits** screen or portal-specific screen.

   - For the **Self Registration X** portal type, follow the additional steps described in Creating Self Registration X portal.
   - For the **Sponsored Guest X** portal type, follow the additional steps described in Creating Sponsored Guest X portal.
   - For the **Voucher** portal type, follow the additional steps described in Creating Voucher portal.
   - For the **Paid X** portal type, follow the additional steps described in Creating Paid X portal.
   - For the **WiFi4EU** portal type, follow the additional steps described in Creating WiFi4EU portal.
   - For the **Microsoft Entra ID X** portal type, follow the additional steps described in Creating Microsoft Entra ID X portal.
   - For the **Google Login X** portal type, follow the additional steps described in Creating Google Login X portal.
   - For the **Onboarding X** portal type, follow the additional steps described in Creating Onboarding X portal.
   - For the **One Click + Voucher** portal type, follow the additional steps described in Creating One Click + Voucher portal.
   - For the **One Click + Paid X** portal type, follow the additional steps described in Creating One Click + Paid X portal.
   - For the **Voucher + Paid X** portal type, follow the additional steps described in Creating Voucher + Paid X portal.
   - For the Hospitality PMS **Beta** portal type, follow the additional steps described in Creating a Hospitality PMS Beta 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 572 *The WLANs screen*

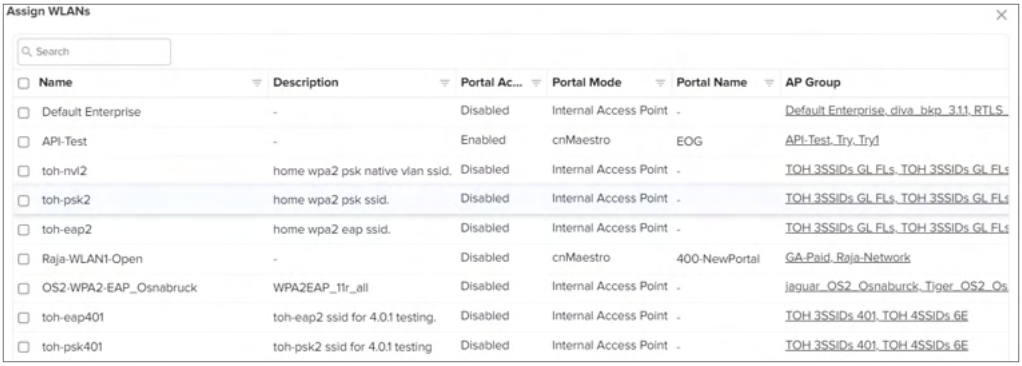


> **Note**
>
> - The **WLANs** screen is different for the **Onboarding X** portal type. When the **Enable Self-Onboarding** checkbox is selected from the **Onboarding** screen, the **WLANs** screen displays the **Network SSID** and **Registration SSID** sections.

11. Click **Assign WLANs**.

    The **Assign WLANs** window appears.

    Figure 573 *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 574 *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 575 displays the **Basic** screen parameters.

Figure 575 *The Basic screen*

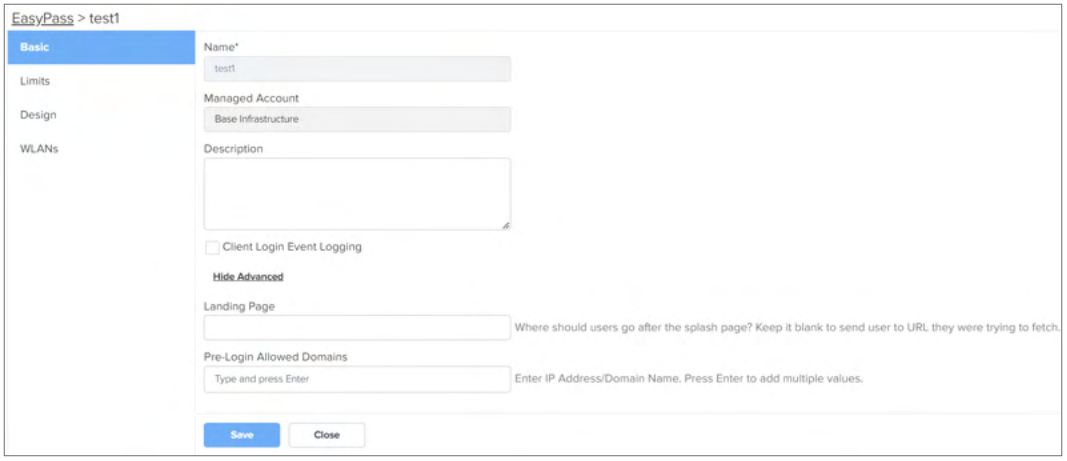


Table 144 describes the **Basic** screen parameters that appear across all portal types on their respective **Basic** screens.

Table 144 *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 144 *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 576 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 576 *The Limits screen*

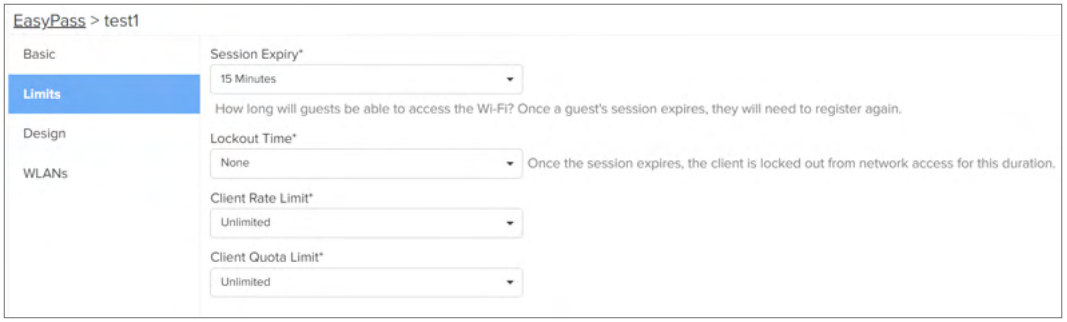


Table 145 describes the **Limits** screen parameters that appear across all portal types on their respective **Limits** screens.

Table 145 *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 145 *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, Paid X, Microsoft Entra ID X, Google Login X, and Onboarding 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 145 *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 • Microsoft Entra ID X • Google Login 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 577 displays the **Design** screen parameters.

Note

The layout of the preview window differs based on the portal type you select.

Figure 577 *The Design screen*

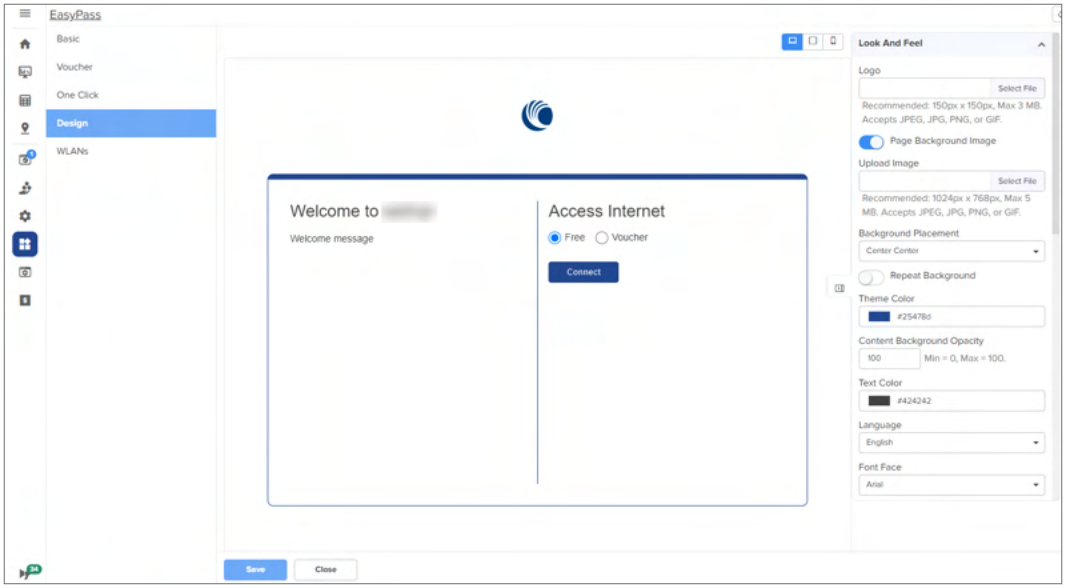


Table 146 describes the common **Design** screen parameters that appear across all portal types on their respective **Design** screens.

Table 146 *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

Table 146 *The Design screen parameters*

Parameter	Description
	• Left Bottom • Right Top • Right Center • Right Bottom • 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

Table 146 *The Design screen parameters*

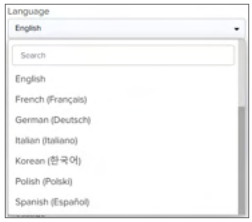
Parameter	Description
	 Default is English. When you change the language to a value other than English, the design page parameters are updated in the selected language, except the Title, message, and any terms and conditions that you might have added. You must manually enter these contents in the selected 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.
Social Login	Enable or disable the social login option to log in to the EasyPass portal.

Table 146 *The Design screen parameters*

Parameter	Description
	This option is available only in cnMaestro Cloud accounts. The following social login options are supported: • Google • Facebook When the social login option is enabled, the portal page contains **Sign in with Facebook** and/or **Sign in with Google** options.  **Note**: When the social login option is enabled, **Sign in with Facebook** and/or **Sign in with Google** buttons replace the **Connect** button.
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 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.	

Table 146 *The Design screen parameters*

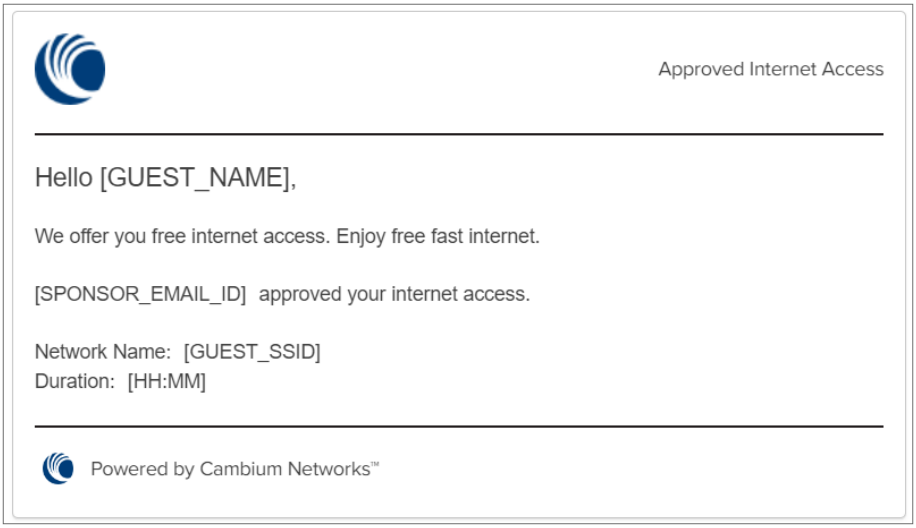
Parameter	Description
Preview tab The **Preview** tab is selected, by default. The following fields appear on the design page.	
Email	Enter the email ID. This field is mandatory.
Password	Enter the password. This field is mandatory.
Email Template tab When you click the **Email Template** tab, the following email template appears:  	
Note: For the **Sponsored Guest X** portal type, configuration of additional parameters is required to identify users, create personalized accounts, verify email ownership, and send targeted notifications to guests. Additionally, these fields are necessary to notify users of important updates, promotions, or account-related changes. Configure the following additional parameters:	
Guest Name	Enter the guest name.
Guest Email	Enter the guest email ID.
Sponsor Email	Enter the sponsor email ID.
Note: For the **Voucher** portal type, configure the following additional parameter:	
Voucher Code	Indicates a voucher code. Enter a voucher code. This is a mandatory field.
Note: For the **Paid X** portal type, configure either of the following options:	
Select a Plan	Select the required plan from the dropdown list.
Payment Code	The payment code of the plan. Enter the payment code.
Note: For the **Microsoft Entra ID X** portal type, the following option is available:	
Sign in with Microsoft	Use this option to sign in with Microsoft.
Note: For the **Google Login X** portal type, the following option is available:	
Sign in with Google	Use this option to sign in with Google.
Note: For the **Onboarding X** portal type, the following option is available:	

Table 146 *The Design screen parameters*

Parameter	Description
Connect	You must enter the email ID and name before you click the **Connect** button.
Note: For the **One click + Voucher** portal type, configure either of the following options:	
Free	You can select this option to provide free access to the internet.
Voucher	You must enter a voucher code when you select this option.
Note: For the **One click + Paid X** portal type, configure either of the following options:	
Free	You can select this option to provide free access to the internet.
Paid	When you select this option, you can either use **Select a Plan** or **Payment Code** option.
Note: For the **Voucher + Paid X** portal type, configure either of the following options:	
Voucher	When you select this option, you must enter a voucher code.
Paid	When you select this option, you can either use **Select a Plan** or **Payment Code** option.



Note

After configuring the **Design screen** parameters, proceed to step 10 described in the Creating a portal process.

The Voucher screen parameters

Table 147 displays the **Voucher** screen parameters that appear across **Voucher**, **One Click + Voucher**, and **Voucher + Paid X** portal types on their respective **Voucher** screens.

Table 147 *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.
Session Expiry	For information on this parameter, see Table 145.
Voucher Expiry	The expiry time of the voucher. The following options are supported: • 15 Minutes • 1 Hour

Table 147 *The Voucher screen parameters*

Parameter	Description
	• 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 145.
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 578 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 578 *The One Click screen*

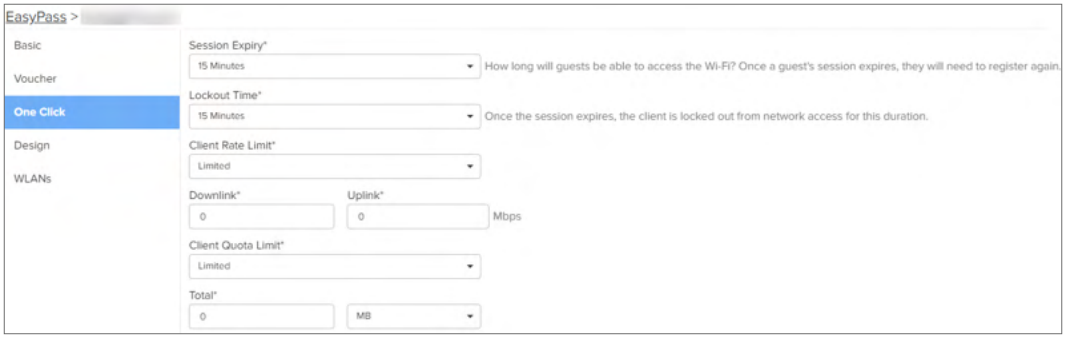


Table 145 describes the parameters that appear only for **One Click + Voucher** or **One Click + Paid X** portal types on the respective **One Click** screens.

Table 148 *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.
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.

Table 148 *The Limits screen parameters*

Parameter	Description
	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.

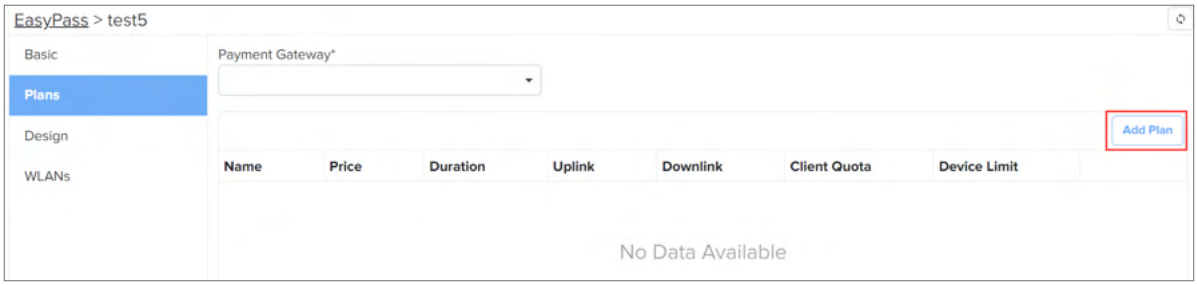
Note

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 579 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 579 *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 579).

   The **Add New Plan** window appears.

Figure 580 *The Add New Plan window*

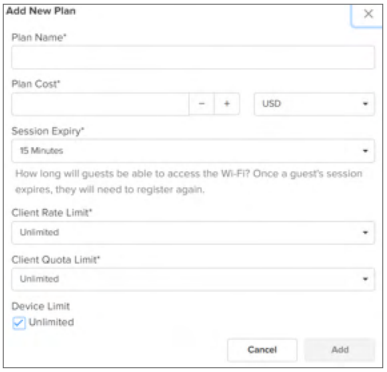


Table 149 describes the common **Plans** screen parameters that appear across **Paid X**, **One Click + Paid X**, and **Voucher + Paid X** portal types on their respective **Plans** screens.

Table 149 *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 145.
Client Rate Limit	
Downlink	
Uplink	
Client Quota Limit	
Total	
Device Limit	
Unlimited	Enable or disable the parameter. 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 580).

   The plan is added.

Figure 581 *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 582) and configure corresponding parameters as described in the following sections..

Figure 582 *Payment gateway options*



The following options are supported:

- IP Pay
- Quickpay
- PayPal

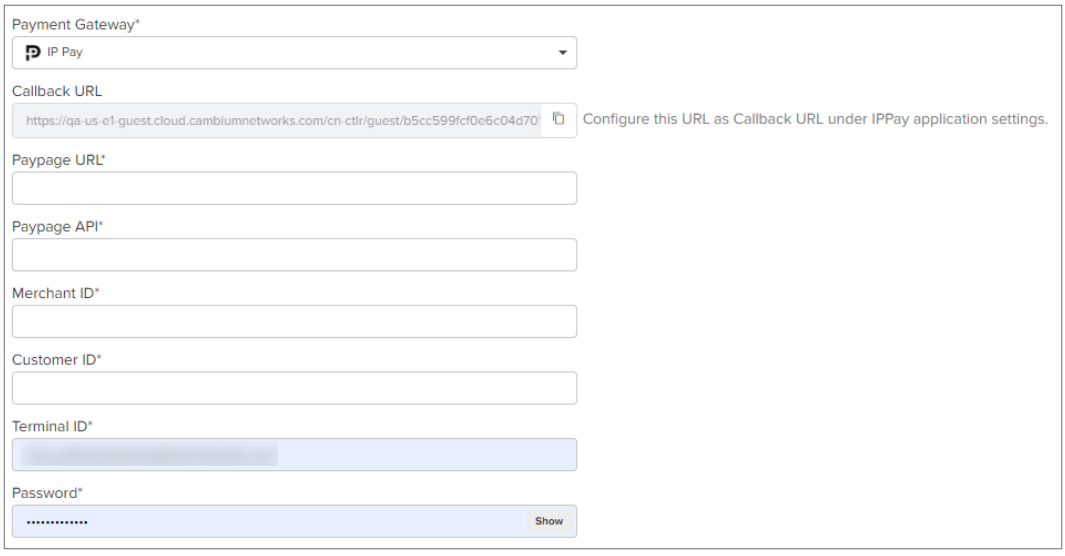
Note

Set the mandatory fields for the selected payment gateway options.

IP Pay

Figure 583 displays the parameters available for the **IP Pay** payment gateway.

Figure 583 *IP Pay payment gateway*



Configure the IP Pay parameters described in Table 150.

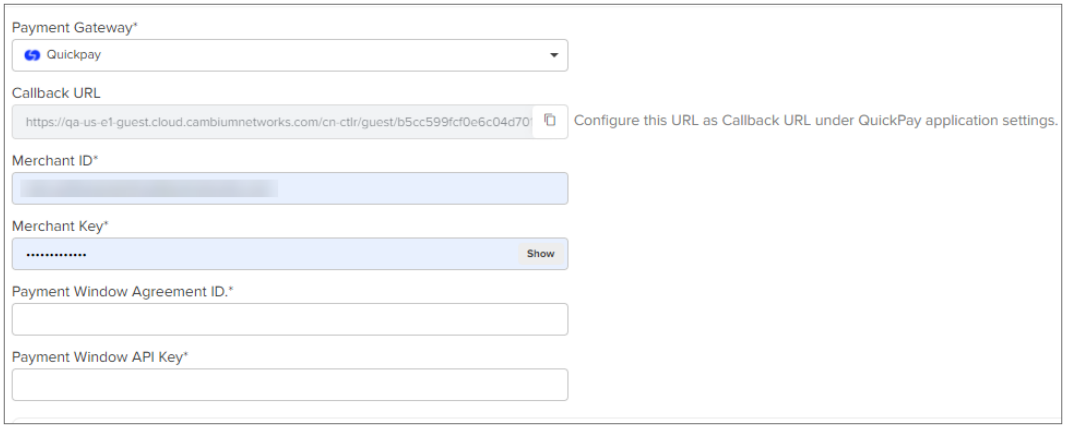
Table 150 *IP Pay parameters description*

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 584 displays the parameters available for the **Quickpay** payment gateway.

Figure 584 *Quickpay payment gateway*



Configure the Quickpay parameters described in Table 151.

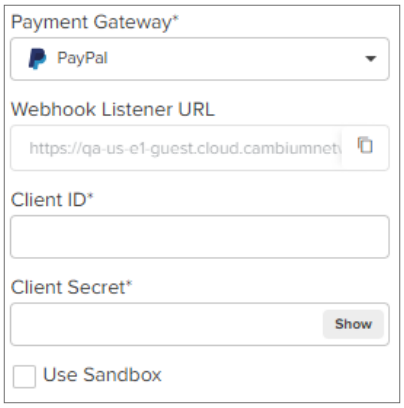
Table 151 *Quickpay parameters description*

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 585 displays the PayPal payment gateway screen.

Figure 585 *PayPal payment gateway*



Configure the PayPal parameters described in Table 151.

Table 152 *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.

Table 152 *PayPal parameters description*

Parameter	Description
Use Sandbox	Select this checkbox if you want to use the PayPal developer account.
Note: The parameters of the **PayPal** option are also applicable to **One Click** + **Paid X** and **Voucher** + **Paid X** portal types.	

Note

After configuring the parameters in the **Plans** screen, continue to step 9 to configure the parameters in the **Design** and **WLANs** screens.

Accessing the common tabs

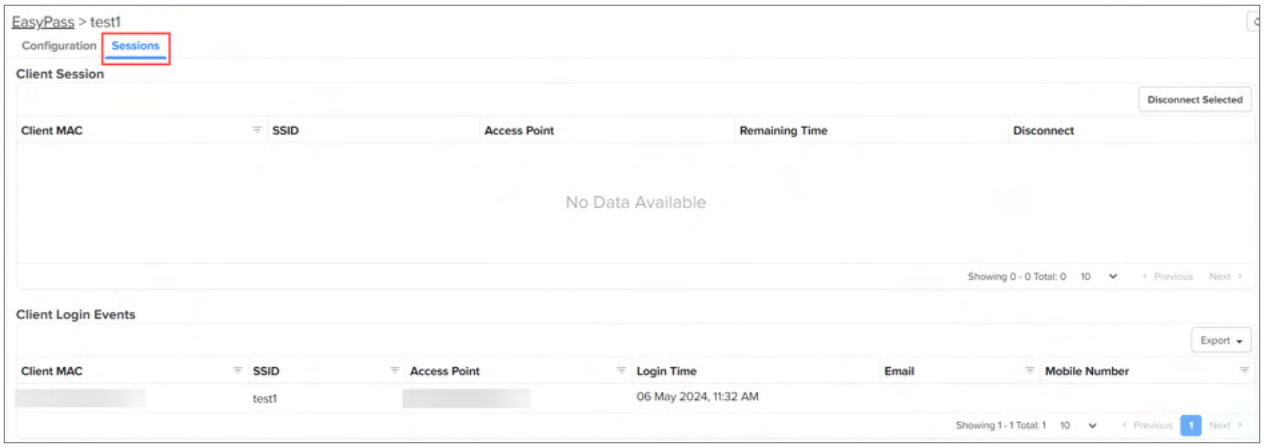
The following common tabs are available for various portal types in EasyPass:

- Sessions
- Guests
  - Adding a new guest user
- Vouchers
  - EasyPass
- Paid Transactions X
- Users X

Sessions

You can access the **Sessions** page using the **Sessions** tab from, as shown in Figure 586, from any of the portals.

Figure 586 *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

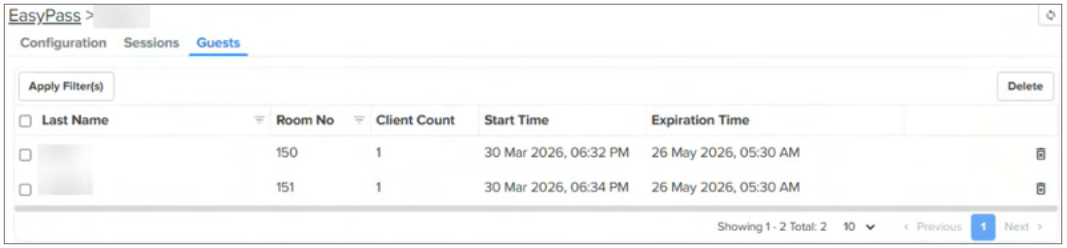
The **Guests** page allows you to view details of self-registered guests connecting to the wireless network.

You can access the **Guests** page using the **Guests** tab (as shown in the following figures).

Figure 587 *Self Registration X Guests page*



Figure 588 *Hospitality PMS Beta Guests page*



Note

The **Guests** tab appears only for the **Self Registration X** and **Hospitality PMS Beta** portal types.

Adding a new guest user

Note

Adding a new guest user is applicable only to the **Self Registration X** portal type.

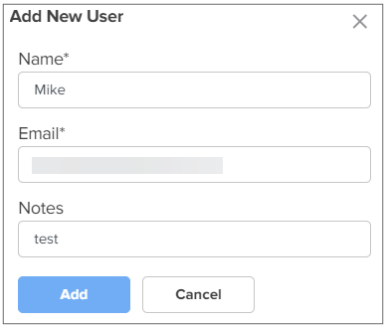
You can also add a new guest user from the **Guests** page.

Complete the following steps to add a new user:

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

   The **Add New User** window appears.

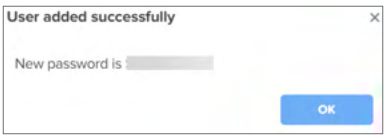
Figure 589 *The Add New User window*



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 590).

   Figure 590 *The User added successfully window*

6. Click **OK**.

   A new guest user is added (as shown in Figure 591).

   Figure 591 *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 591).

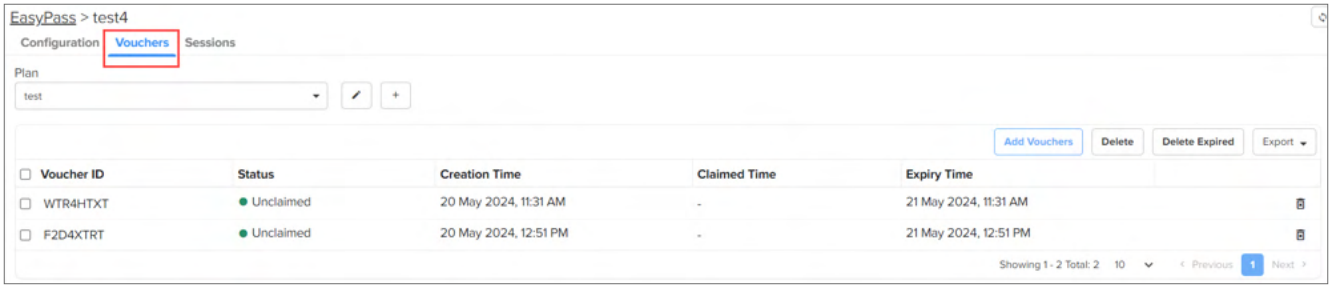
   - Use the disable access ( ) icon to disable access.
   - Use the reset password ( ) icon to reset a password.
   - Use the extend session ( ) icon to extend a session.
   - Use the edit ( ) icon to edit the user details.
   - Use the delete ( ) icon to delete a user.

Vouchers

You can access the **Vouchers** page using the **Vouchers** tab (as shown in Figure 592).

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 592 *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:

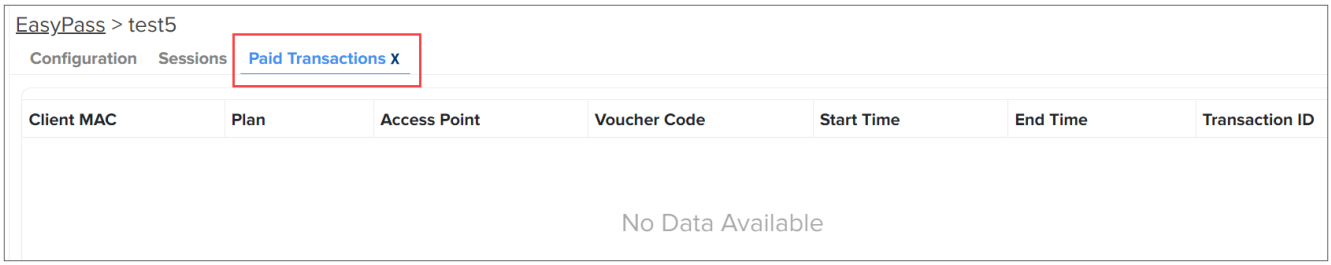
- Add new vouchers
- Delete the existing or expired vouchers
- Export voucher data
- View session details
- Disconnect users at the session-level

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 593).

Figure 593 *The Paid Transactions X tab*



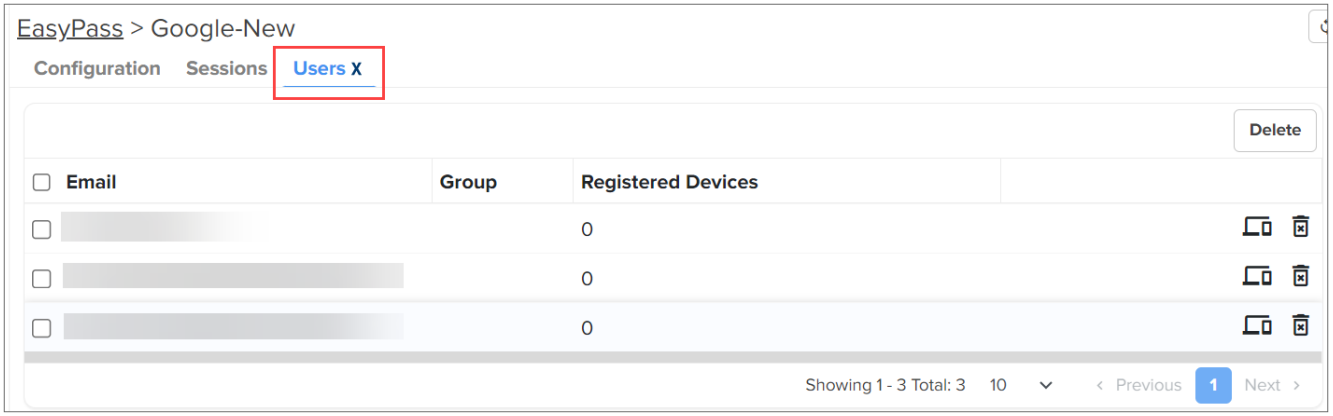
Note

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

Users X

You can access the **Users X** page using the **Users X** tab (as shown in Figure 594).

Figure 594 *The Users X tab*



Note

The **Users X** tab appears only for the **Microsoft Entra ID X** , **Google Login X**, and **Onboarding X** portal types.

Creating One Click portal

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

Figure 595 *The One Click option*



Note

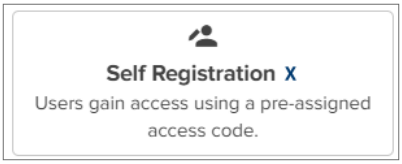
To create a One Click portal, complete the initial steps described in Creating a portal and continue with the next steps to configure the parameters of the **Basic** screen, **Limits** screen, **Design** screen, and **WLANs** screen.

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 596 *The Self Registration X option*



Note

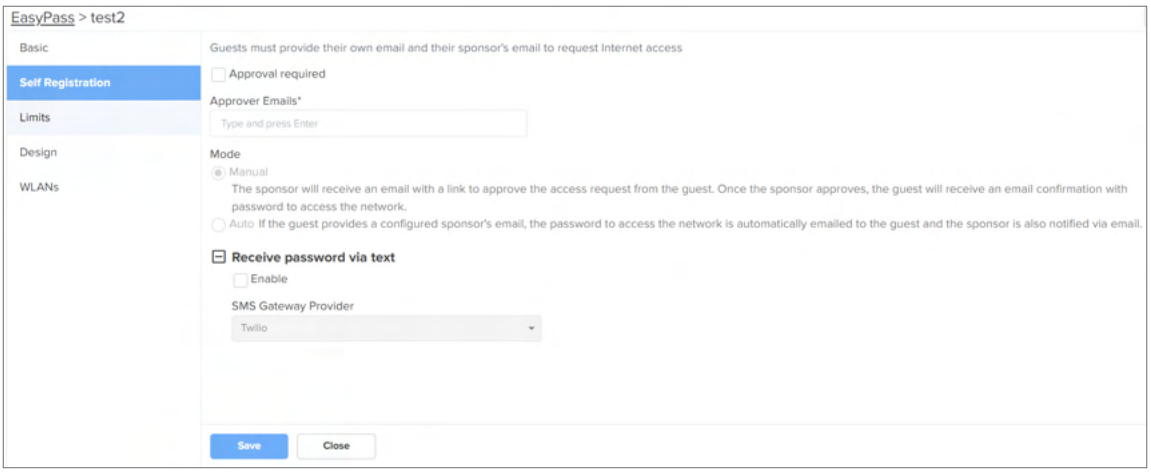
To create a Self Registration X portal, complete the initial steps described in Creating a portal and continue with the next steps to configure the parameters of the **Basic** screen, **Self Registration** screen, **Limits** screen, **Design** screen, and **WLANs** screen.

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

1. Click the **Self Registration** tab.

   The **Self Registration** screen appears.

   Figure 597 *The Self Registration screen*



2. Configure the parameters described in Table 153.

   Table 153 *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.

Table 153 *The Self Registration screen parameters*

Parameter	Description
	• 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: • 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 598 displays the parameters available for the **Twilio** option.

Figure 598 *Twilio option*



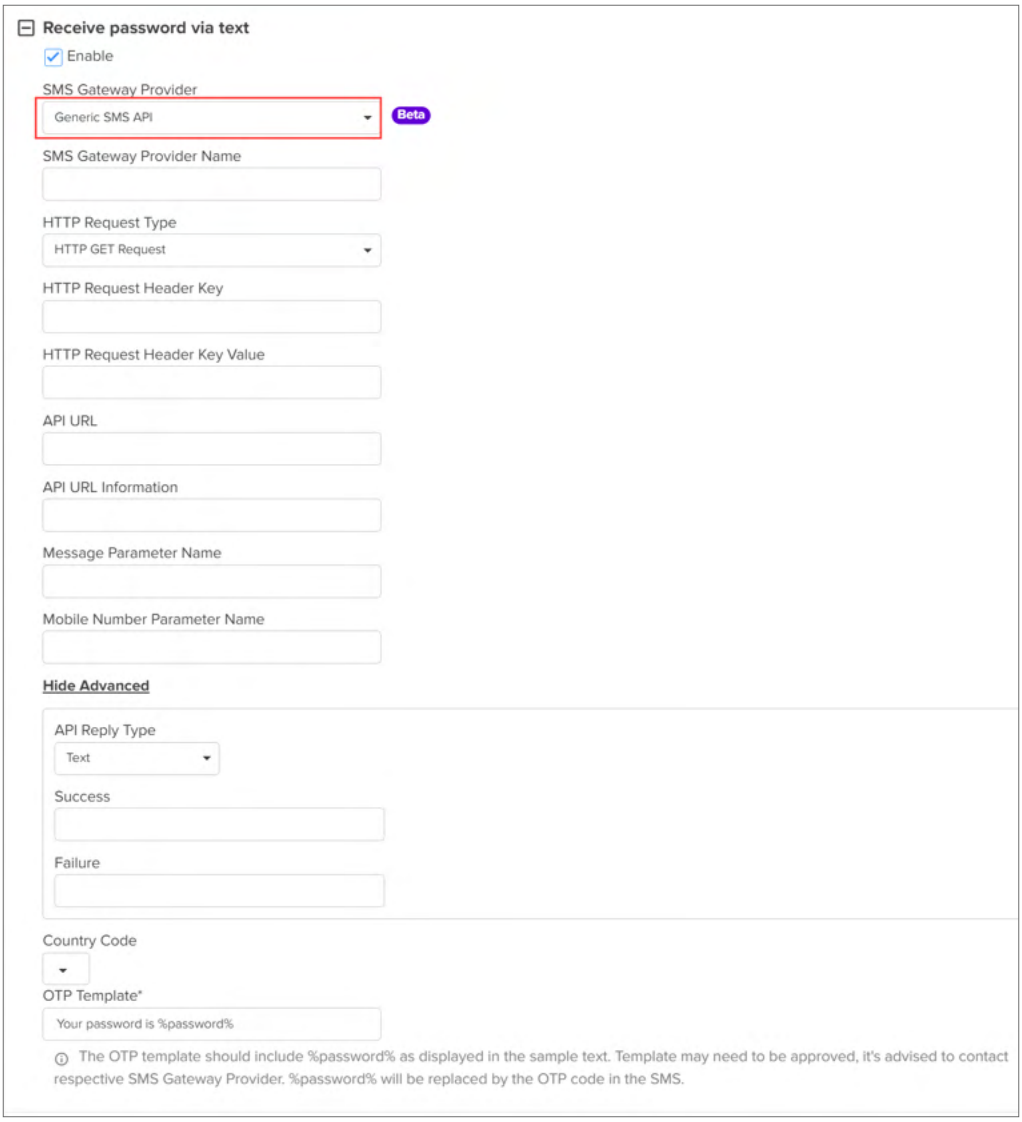
When you select the **Twilio** option, you must configure the parameters described in Table 154.

Table 154 *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 599 displays the parameters available for the **Generic SMS API** option.

Figure 599 *Generic SMS API option*



When you select the **Generic SMS API** option, you must configure the parameters described in Table 155.

Table 155 *Parameters of Generic SMS API*

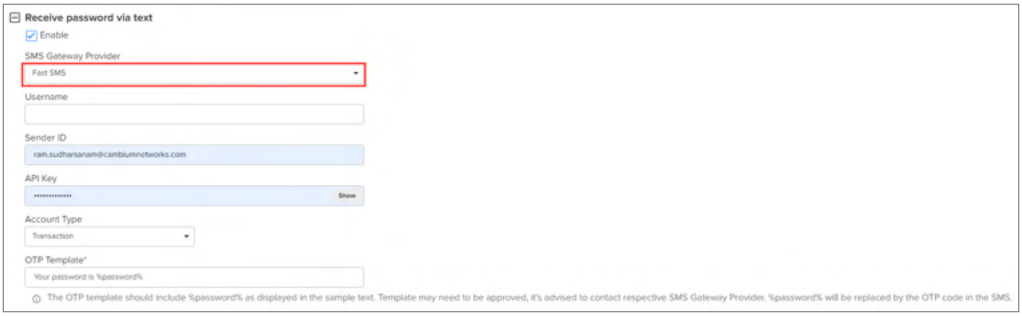
Parameter	Description
SMS Gateway Provider Name	SMS gateway provider name. Enter a name for the SMS gateway provider. Enter the user name.
HTTP Request Type	HTTP request type. The following options are supported: • HTTP GET Request • HTTP POST Request
HTTP Request Header Key	HTTP request header key
HTTP 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.

Table 155 *Parameters of Generic SMS API*

Parameter	Description
JSON Reply Success Key Value	JSON reply success key value. Enter the JSON reply success key value.
JSON Reply Failure Key Name	JSON reply failure key name. Enter the JSON reply failure key name.
JSON reply Failure Key Value	JSON reply failure key value. Enter the JSON reply failure key value.
XML	
XML Reply Success Element	XML reply success element. Enter the XML reply success element.
XML Reply Success Element Value	XML reply success element value. Enter the reply success element value.
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 600 displays the parameters available for the **Fast SMS** option.

Figure 600 *Fast SMS option*



When you select the **Fast SMS** option, you must configure the parameters described in Table 156.

Table 156 *Parameters of Fast SMS*

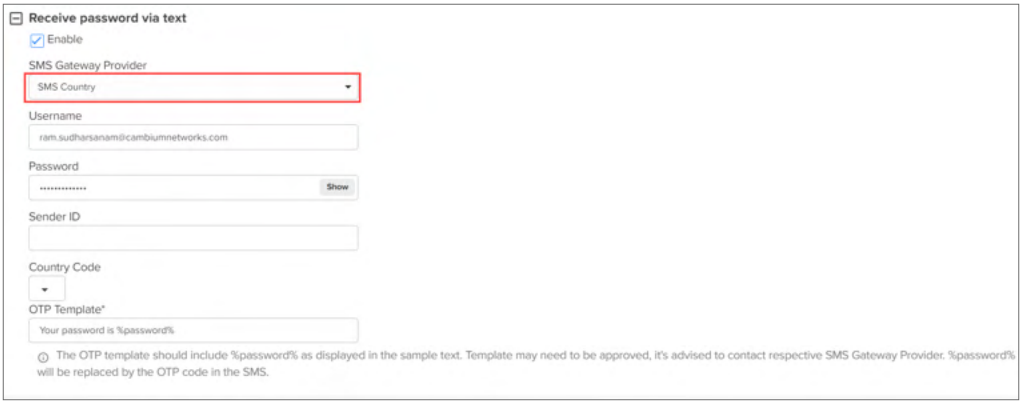
Parameter	Description
Username	User name. Enter the user name.

Table 156 *Parameters of Fast SMS*

Parameter	Description
	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 • OTP • Other
OTP Template	OTP template. Enter the password in the **OTP Template** field. This parameter is mandatory.

Figure 601 displays the parameters available for the **SMS Country** option.

Figure 601 *SMS Country option*



When you select the **SMS Country** option, you must configure the parameters described in Table 157.

Table 157 *Parameters of SMS Country*

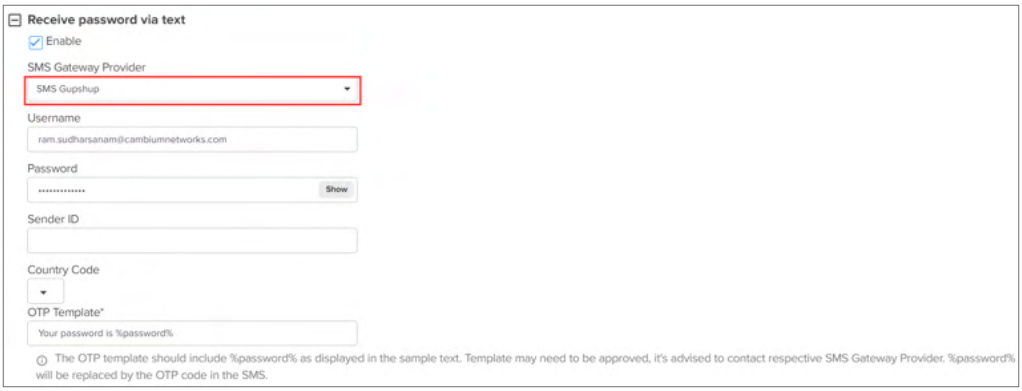
Parameter	Description
Note: The **Username** and **Password** fields are populated, by default.	
Sender ID	Sender ID. Enter the sender ID.
Country Code	Country code. Select the required country code from the dropdown list. For example, **United States (+1)**
OTP Template	OTP template. Enter the password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

Table 157 *Parameters of SMS Country*

Parameter	Description
	This parameter is mandatory.

Figure 602 displays the parameters available for the **SMS Gupshup** option.

Figure 602 *SMS Gupshup option*



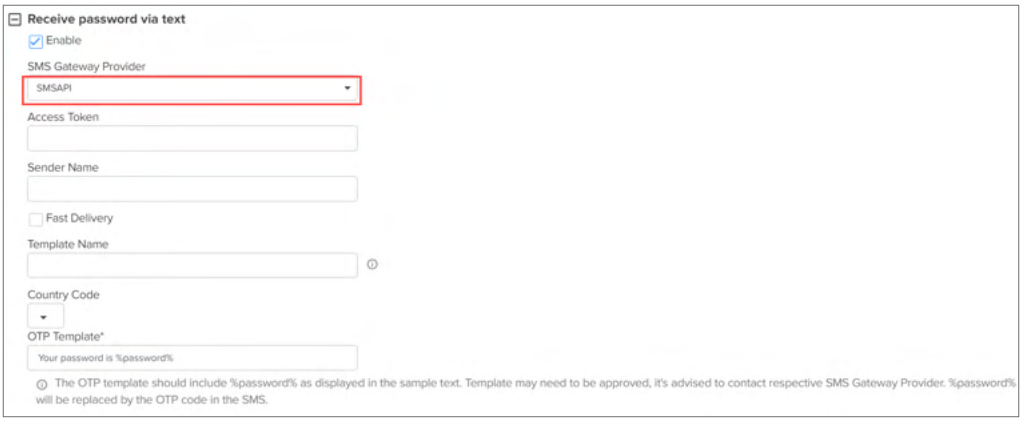
When you select the **SMS Gupshup** option, you must configure the parameters described in Table 158.

Table 158 *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 603 displays the parameters available for the **SMS API** option.

Figure 603 *SMS API option*



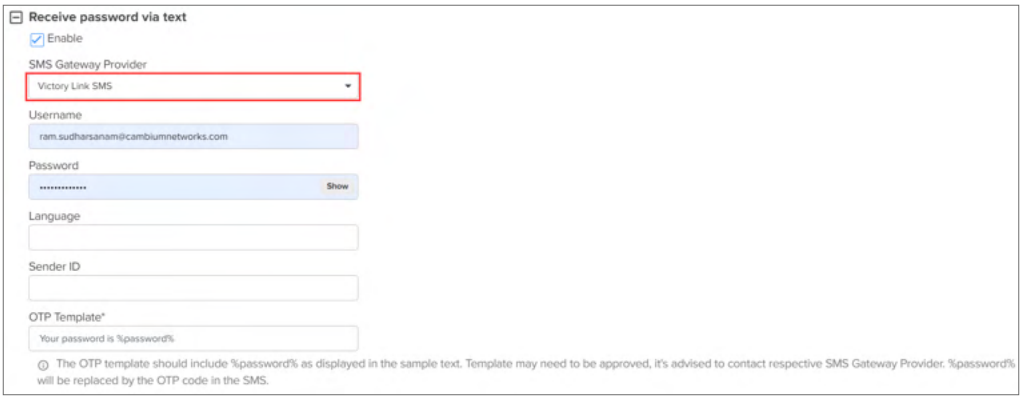
When you select the **SMS API** option, you must configure the parameters described in Table 159.

Table 159 *Parameters of SMS API*

Parameter	Description
Note: The **Username** and **Password** fields are populated, by default.	
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 604 displays the parameters available for the **Victory Link SMS** option.

Figure 604 *Victory Link SMS option*



When you select the **Victory Link SMS** option, you must configure the parameters described in Table 160.

Table 160 *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.

Table 160 *Parameters of Victory Link SMS*

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

Note

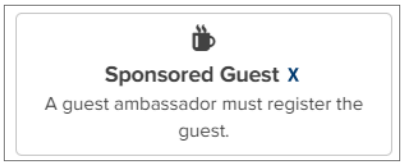
After configuring the parameters in the Self-Registration window, continue to step 8 to configure the parameters in the **Limits**, **Design**, and **WLANs** screens.

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 605 *The Sponsored Guest X option*



Note

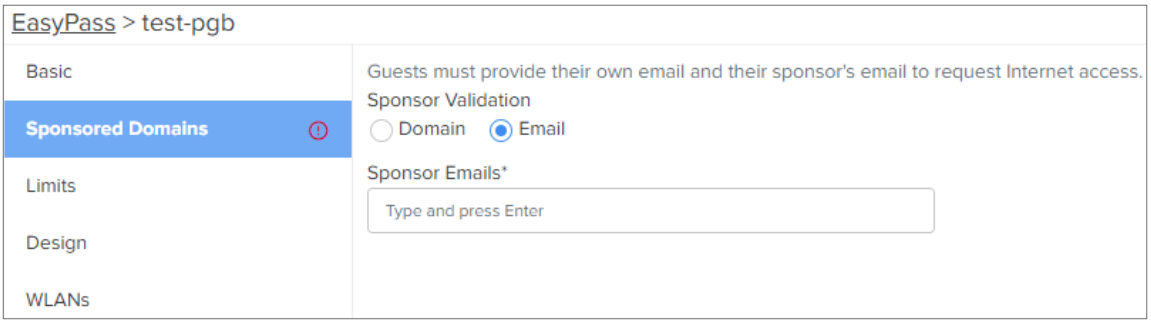
To create a Sponsored Guest X portal, complete the initial steps described in Creating a portal and continue with the next steps to configure the parameters of the **Basic** screen, **Sponsored Domains** screen, **Limits** screen, **Design** screen, and **WLANs** screen.

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

1. Click the **Sponsored Domains** tab.

   The **Sponsored Domains** screen appears.

   Figure 606 *The Sponsored Domains screen*



2. Configure the parameters described in Table 161.

Table 161 *The Sponsored Domains screen parameters*

Parameter	Description
Sponsor Validation	Type of validation to be used for this portal.

Table 161 *The Sponsored Domains screen parameters*

Parameter	Description
	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. 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

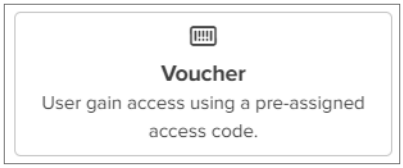
After configuring the parameters in the **Sponsored Domains** window, continue to step 8 to configure parameters in the **Limits**, **Design**, and **WLANs** screens.

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 607 *The Voucher option*



Note

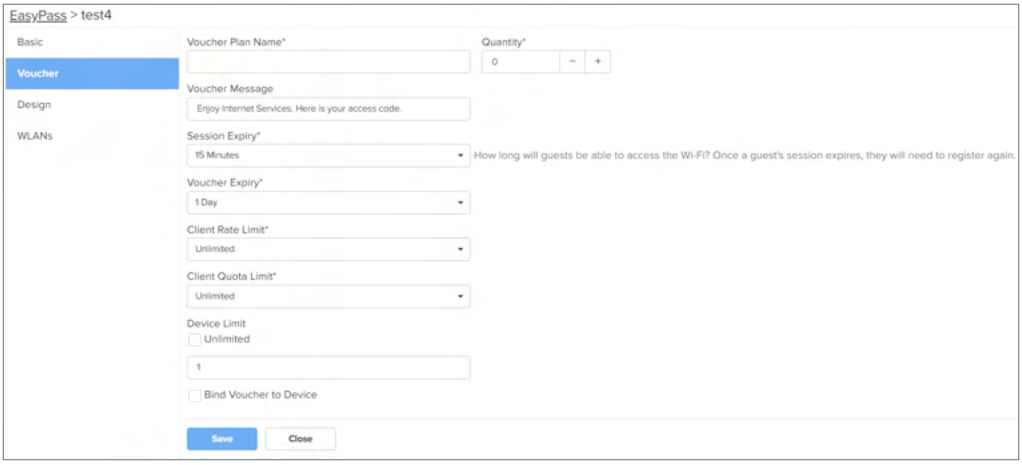
To create a Voucher portal, complete the initial steps described in Creating a portal and continue with the next steps to configure the parameters of the **Basic** screen, **Voucher** screen, **Design** screen, and **WLANs** screen.

Follow these additional steps to create a Voucher portal:

1. Click the **Voucher** tab.

   The **Voucher** screen appears.

Figure 608 *The Voucher screen*



2. Configure the parameters described in Table 147.

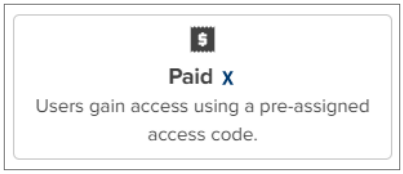
Note

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 609 *The Paid X option*



Note

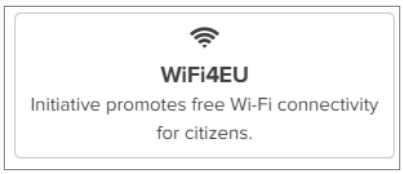
To create a Paid X portal, complete the initial steps described in Creating a portal and continue with the steps to configure the parameters of the **Basic** screen, **Plans** screen, **Design** screen, and **WLANs** screen.

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 610 *The WiFi4EU option*



Note

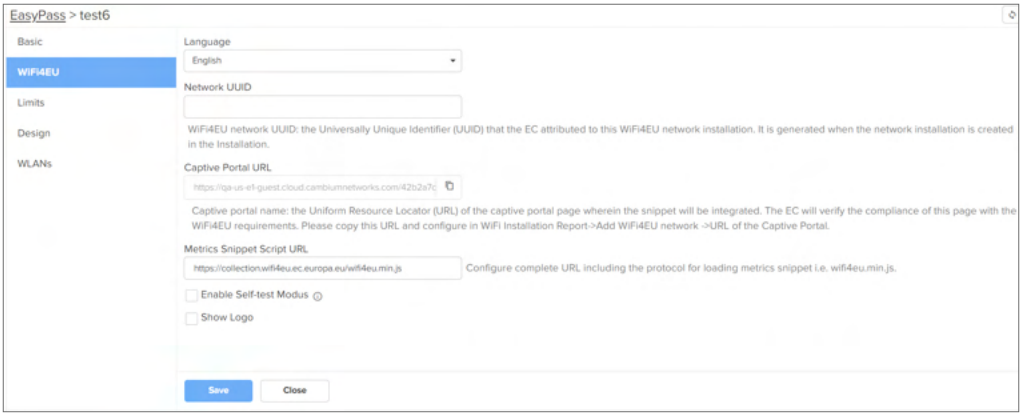
To create a WiFi4EU portal, complete the initial steps described in Creating a portal and continue with the next steps to configure the parameters of the **Basic** screen, **WiFi4EU** screen, **Limits** screen, **Design** screen, and **WLANs** screen.

Follow these additional steps to create a WiFi4EU portal:

1. Click the **WiFi4EU** tab.

   The **WiFi4EU** screen appears.

   Figure 611 *General parameters*



2. Configure the parameters described in Table 162.

   Table 162 *General parameters - WiFi4EU*

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

Note

After configuring the parameters in the WiFi4EU window, continue to step 8 to configure the parameters in the **Limits**, **Design**, and **WLANs** screens.

Creating Microsoft Entra ID X portal

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

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

Figure 612 *The Microsoft Entra ID X option*



Note

To create a Microsoft Entra ID 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, **Microsoft Entra ID** screen, **Limits** screen, **Design** screen, and **WLANs** screen.

Follow these additional steps to create a Microsoft Entra ID X portal:

1. Click the **Microsoft Entra ID** tab.

   The **Microsoft Entra ID** screen appears.

   Figure 613 *The Microsoft Entra ID screen*



2. Click **Authorize Microsoft Login**.

   Note

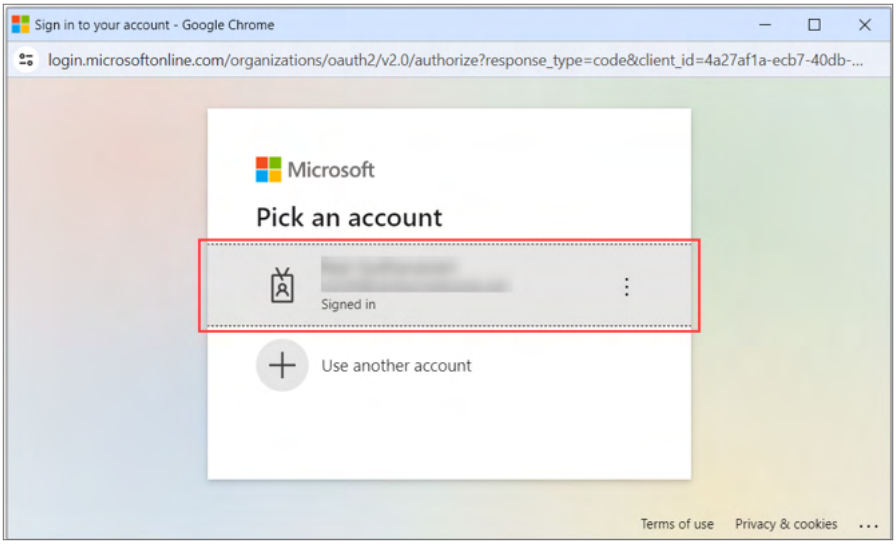
   Only Microsoft Entra ID administrator role users can perform the authorization step.

   The authorization step allows the Easypass Microsoft Entra ID application to:

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

   The following screen appears, as shown Figure 614.

   Figure 614 *Sign in to your account page*



Note

For information on how to integrate Active Directory with Microsoft Entra ID, see the

Azure AD Integration document.

Note

After configuring the parameters in the **Microsoft Entra ID** window, continue to step 8 to configure the parameters in the **Limits**, **Design**, and **WLANs** screens.

Creating Google Login X portal

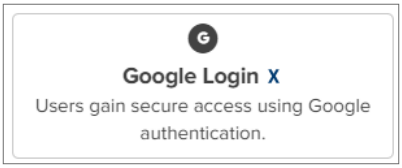
Creating a **Google Login X** portal enables users with a Google account to connect to the wireless network by synchronizing the active directory. When enabled, if a guest who is part of the supported group tries to connect to the Wi-Fi network, the AP provides access to the guest.

Note

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

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

Figure 615 *The Google Login X option*



Note

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

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

1. Click the **Google** tab.

   The **Google** screen appears.

   Figure 616 *The Google screen*

2. Configure the parameters described in Table 163.

   Table 163 *The Google screen parameters*

Parameter	Description
Enable Directory Synchronization	Select the checkbox to enable the directory synchronization. When you select the **Enable Directory Synchronization** checkbox, the following screen appears:

Table 163 *The Google screen parameters*

Parameter	Description
	 When you click the **Follow these steps** link, the following window appears describing how to configure the Google Apps domain category. Follow the steps to configure your Google Apps domain directory.  **Note** For information on how to integrate Active Directory with Google Workspace, see the Google Workspace AD Integration document. When you clear the **Enable Directory Synchronization** checkbox, you must configure the **Allowed Domains** parameter.
Allowed Domains	Enter the required domains. This is a mandatory parameter.

Note

After configuring the parameters in the **Google** window, continue to step 8 to configure the parameters in the **Limits**, **Design**, and **WLANs** screens.

Creating Onboarding X portal

Note

Onboarding **X** is supported only on Wi-Fi 6 and 6E APs running firmware version 6.6.2 or later.

Creating an Onboarding X portal enables clients to register on an open SSID with their email, Google Workspace, or Microsoft Entra ID (Office 365) credentials to receive an enhanced pre-shared key (ePSK), which can be used to connect to a secure network SSID.

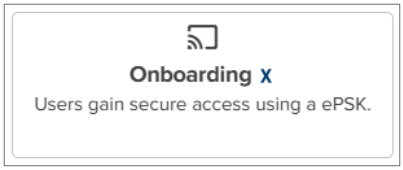
For a non self-onboarding scenario, the administrator provides a passphrase to the users from the **Users X** page. The users can use the passphrase to connect to a network SSID. If ePSK is configured, the administrator can send an email to users containing the passphrase.

Note

After signing in with Google Workspace or Microsoft Entra ID accounts, the ePSK is displayed as part of successful registration and is also emailed to the user for future use.

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

Figure 617 *The Onboarding X option*



Note

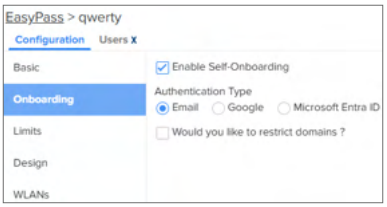
To create an Onboarding X portal, complete the initial steps described in Creating a portal and continue with the next steps to configure the parameters of the **Basic**, **Onboarding**, **Limits**, **Design**, and **WLANs** screens.

Follow these additional steps to create an Onboarding X portal:

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

   The **Onboarding** screen appears.

   Figure 618 *The Onboarding screen*

2. Configure the parameters described in Table 164.

Table 164 *The Onboarding screen parameters*

Parameter	Description
Enable Self-Onboarding	Select the **Enable Self-Onboarding** checkbox to enable self-onboarding. This parameter is disabled by default. When this parameter is enabled, you must select the required authentication type. When this parameter is disabled, users are notified about device limits only if the device limit is enabled and exceeded. **Note** • When this parameter is enabled, the **WLANs** screen displays the **Network SSID** and **Registration SSID** sections (as shown in Figure 620). • Users can still use ePSK without self-onboarding.
Authentication Type	Select the required authentication type. The following options are supported: • Email • Google • Microsoft Entra ID
Would you like to restrict domains	Select the checkbox to restrict the email domains for the user. When you select the **Would you like to restrict domains** checkbox, enter the email

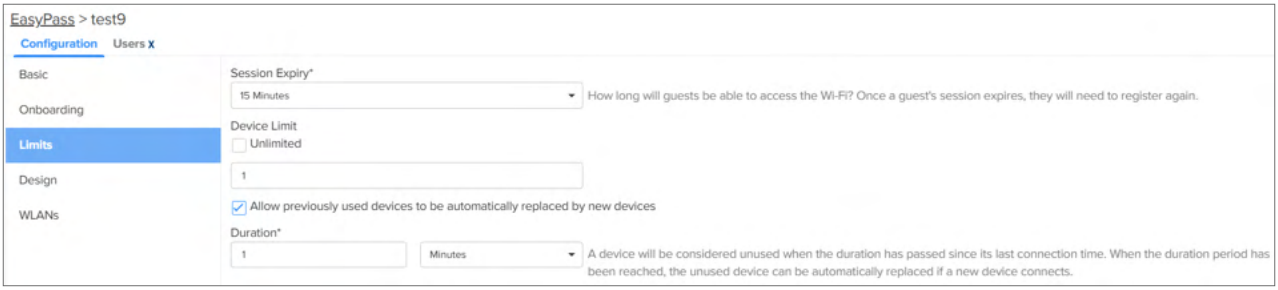
Table 164 *The Onboarding screen parameters*

Parameter	Description
	domains that you want to restrict.
Restrict Domains	Enter the allowed email domains.

3. Click the **Limits** tab.

   The **Limits** screen appears.

   Figure 619 *The Limits screen*



4. Configure the parameters described in Table 165.

Table 165 *The Limits screen parameters of Onboarding portal type*

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. **Note** When you select the **Custom** option, you can configure the minimum duration value to 1 for Days, Hours, and Minutes.
Device Limit	Specifies the number of devices that the guest can connect to the wireless network. Minimum value: 1 Maximum value: 200

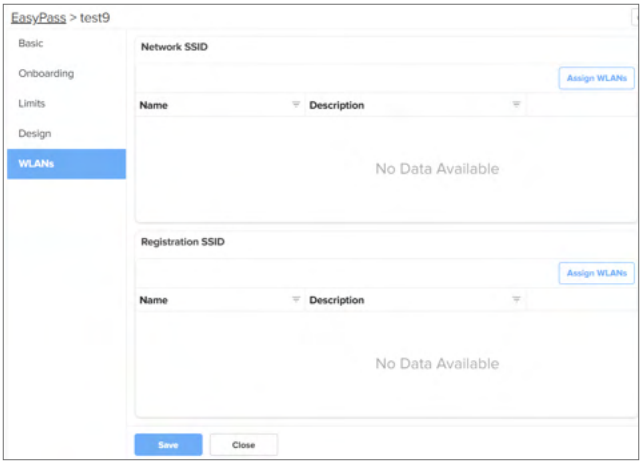
Table 165 *The Limits screen parameters of Onboarding portal type*

Parameter	Description
Unlimited	Device limit is unlimited.
Allow previously used devices to be automatically replaced by new devices	Select the checkbox to enable the parameter. **Note** • When this parameter is enabled, it automatically replaces previously used devices with new devices according to the configured device limit. • When this parameter is disabled, previously used devices will remain in the system and will not be automatically replaced by new devices, even if the duration since their last connection has passed.
Duration	This parameter is applicable only when **Allow previously used devices to be automatically replaced by new devices** checkbox is selected. **Note** A device is considered unused when the duration has passed since its last connection time. When the duration period is reached, the unused device is automatically replaced if a new device connects. Minimum value: 1 You can select the required option from the dropdown list. The following options are supported: • Minutes • Hours • Days

5. Click the **WLANs** tab.

   The **WLANs** screen appears.

Figure 620 *The WLANs screen*



Note

The **WANs** screen displays the **Network SSID** and **Registration SSID** sections (as shown in Figure 620).

- Network SSID is a secure SSID that users connect to after successfully registering and authenticating using the Registration SSID. It requires a ePSK for authentication to ensure users have secured access to the network after registration.
- Registration SSID is an open SSID that is used for onboarding users. It does not require a password for authentication. It allows users to authenticate using Email, Google, or Microsoft Entra ID to register their device. After registration, users are emailed a unique password and SSID information to connect to the network.

Adding a new user

You can add a new user from the **Users X** page of the **Onboarding X** portal type.

Self-onboarding supports a dual SSID configuration, which includes an open SSID for self-onboarding and a secure network SSID for users who connect with a password. The registration SSID supports various authentication methods such as email, Google Workspace, and Microsoft Entra ID. Alternatively, users can skip self-onboarding and connect directly to the secure network SSID. In this case, the users are manually added to the **Users X** table and managed by the administrator.

Note

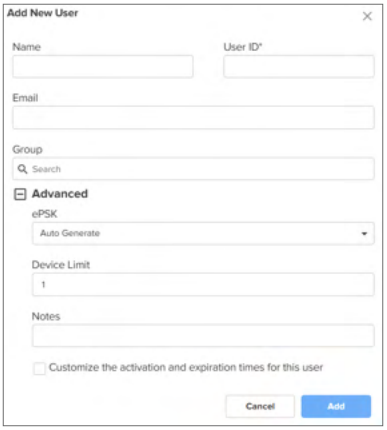
- The policy settings are managed using the user group. The user group is associated with an access control configuration, specifically through the RADIUS Filter-ID. The user group is managed through **Configuration** > **Wi-Fi Profiles** > **AP Groups** > **Add New** > **Access Control** > **User Group Policy** > **Add New** > **RADIUS Filter-ID**. The **RADIUS Filter-ID** is used to apply specific policies to users based on the group membership when they connect to the network.
- The maximum supported characters for **RADIUS Filter-ID** in user group policy is 32.

Complete the following steps to add a new user:

1. On the **Users** page of Onboarding X portal type, click **Add New**.

   The **Add New User** window appears.

   Figure 621 *The Add New User window*



2. On the **Add New User** window, complete the following steps:

a. In the **Name** field, enter the name of a user. This field is optional.

b. In the **User ID** field, enter the user ID. This field is mandatory.

> **Note**
>
> Only alphanumeric, underscore (_), dashes (-), period (.), plus (+), and @ characters are supported.

c. In the **Email** field, enter an email ID of the user. This field is optional.

d. In the **Group** field, enter the group name.

3. In the **Advanced** section, complete the following steps:

a. From the **ePSK** dropdown list, select the required option. The following options are supported:

- **Auto Generate**
- **Manual**

By default, the **Auto Generate** option is selected.

b. In the **Device Limit** field, enter a value.

c. In the **Notes** field, enter the description for creating a new user. This field is optional.

d. Select the **Customize the activation and expiration times for this user** checkbox to customize the activation and expiration times for the user.

4. Click **Add**.

A new user is added (as shown in Figure 622).

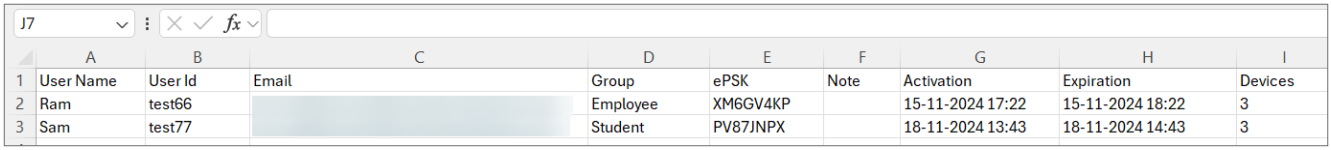
Figure 622 *The new user details*



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 623 *List of users with their associated data*



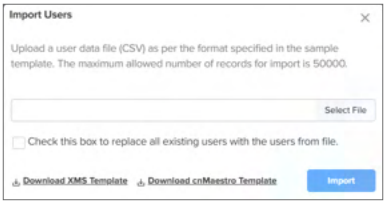
	A	B	C	D	E	F	G	H	I
1	User Name	User Id	Email	Group	ePSK	Note	Activation	Expiration	Devices
2	Ram	test66		Employee	XM6GV4KP		15-11-2024 17:22	15-11-2024 18:22	3
3	Sam	test77		Student	PV87JNPX		18-11-2024 13:43	18-11-2024 14:43	3

Complete the following steps to import user data using a CSV file:

1. Click the **Import** button (as shown in Figure 622).

The **Import Users** page appears.

Figure 624 *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.

4. 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**
5. Click the **Regenerate ePSK** button to regenerate a new enhanced pre-shared key (ePSK) for selected users.

   A confirmation dialog box appears.

Figure 625 *Confirmation dialog box to regenerate ePSKs for selected users*



When you click **Yes** (as shown in Figure 625), 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.

6. Click the **Send ePSKs** button to send the ePSK for selected users.

   A confirmation dialog box appears.

Figure 626 *Confirmation dialog box to send ePSKs for selected users*



When you click **Yes** (as shown in Figure 626), ePSKs are sent for selected users.

7. Click the **Extend session** button to extend a session for selected users.

A confirmation dialog box appears.

Figure 627 *Confirmation dialog box to extend session for selected users*



When you click **Yes** (as shown in Figure 627), the session is extended for selected users.

You can also use the Extend session ( ) icon to extend the session for a selected user.

Note

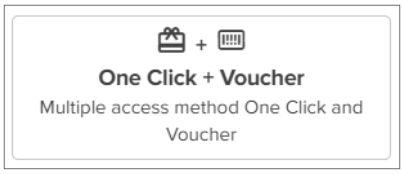
The session is extended based on the **Session Expiry** duration set in the **Limits** screen.

- 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 628 *The One Click + Voucher option*



Note

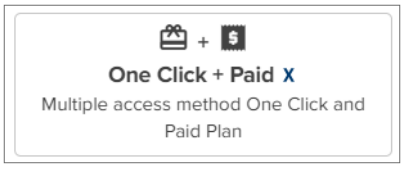
To create a One Click + Voucher portal, complete the initial steps described in Creating a portal and continue with the next steps to configure the parameters of the **Basic** screen, **Voucher** screen, **One Click** screen, **Design** screen, and **WLANs** screen.

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 629 *The One Click + Paid X option*



Note

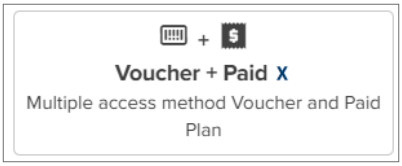
To create a One Click + Paid X portal, complete the initial steps described in Creating a portal and continue with the next steps to configure the parameters of the **Basic** screen, **Plans** screen, **One Click** screen, **Design** screen, and **WLANs** screen.

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 630 *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:

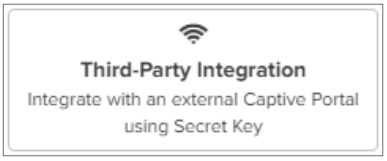
- Creating a portal and secret key
- Revoking and generating the secret key
- Using the Secret Key in API Requests

Creating a portal and secret key

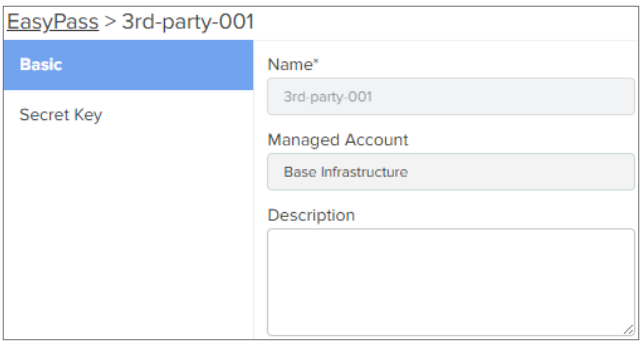
This section is targeted at the cnMaestro administrator to create the EasyPass Third-Party Integration portal, generate the integration Base URL and secret keys, and deliver them to the captive portal developer partner.

Complete the following steps:

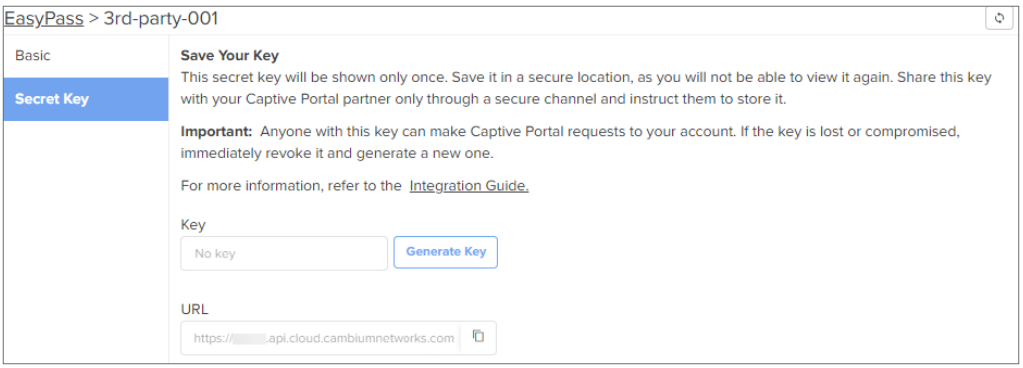
1. From the cnMaestro home page, navigate to **Network Services** > **EasyPass**.
2. Click **Add Portal** and select **Third-Party Integration** as the portal type.



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.

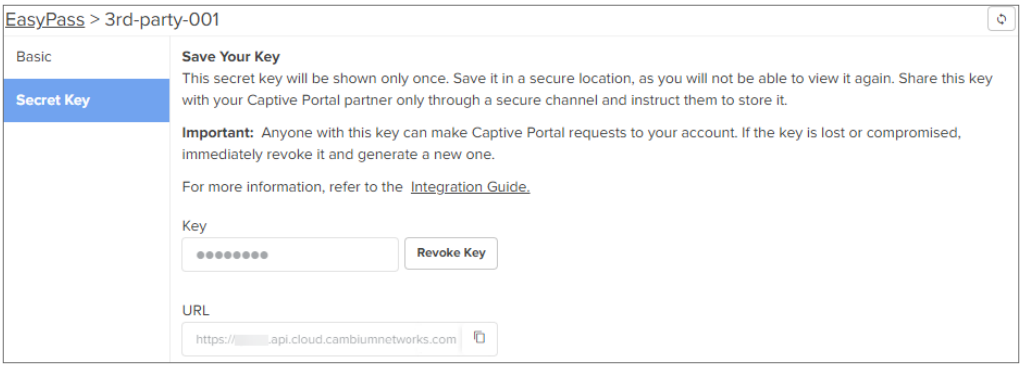
Revoking and generating the secret key

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.

Creating a Hospitality PMS Beta portal

You can create a **Hospitality PMS Beta** portal to enable users to integrate Tiger TMS iLink Property Management Systems (PMS) with EasyPass and to manage guest accounts.

This section includes only the additional parameters that you must configure for the **Hospitality PMS Beta** X portal.

Note

To create a **Hospitality PMS Beta** portal, complete the initial steps described in Creating a portal and continue with the next steps to configure the parameters of the **Basic**,

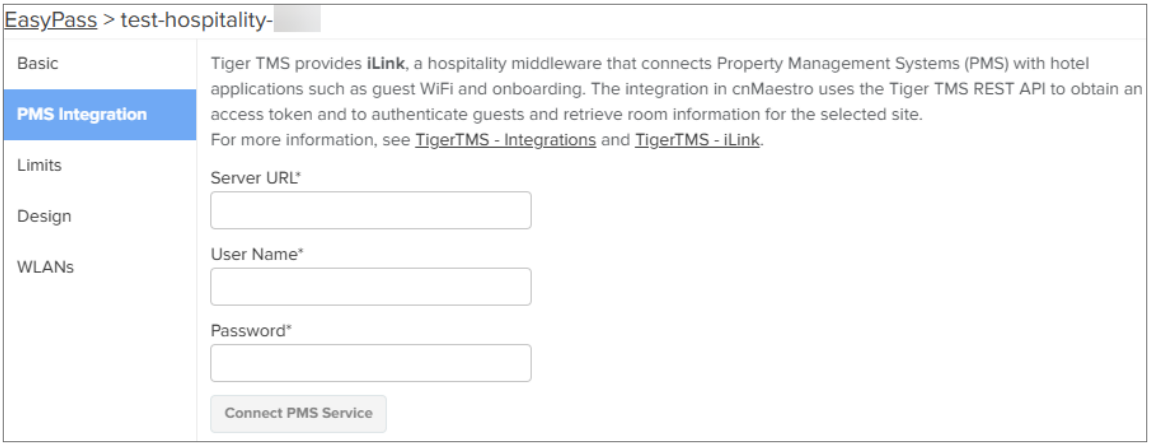
PMS Integration, **Limits**, **Design**, and **WLANs** screens.

Follow these additional steps to create a **Hospitality PMS Beta** portal:

1. Click the **PMS Integration** tab to integrate with the Tiger TMS iLink PMS.

   The **PMS Integration** screen appears.

   Figure 631 *The Hospitality PMS Beta screen*



2. Configure the parameters described in the following table.

   Table 166 *The PMS Integration screen parameters*

Parameter	Description
Server URL	URL of the Tiger TMS iLink PMS server required for integration with EasyPass portal. This parameter is mandatory.
Username	Username of the Tiger TMS iLink PMS. This parameter is mandatory.
Password	Password of the Tiger TMS iLink PMS. This parameter is mandatory.

3. Click **Connect PMS Service**.

   EasyPass connects with the iLink PMS server and a new dropdown, **Sites**, is displayed.

4. From the **Sites** dropdown list, select the site that you want to use.

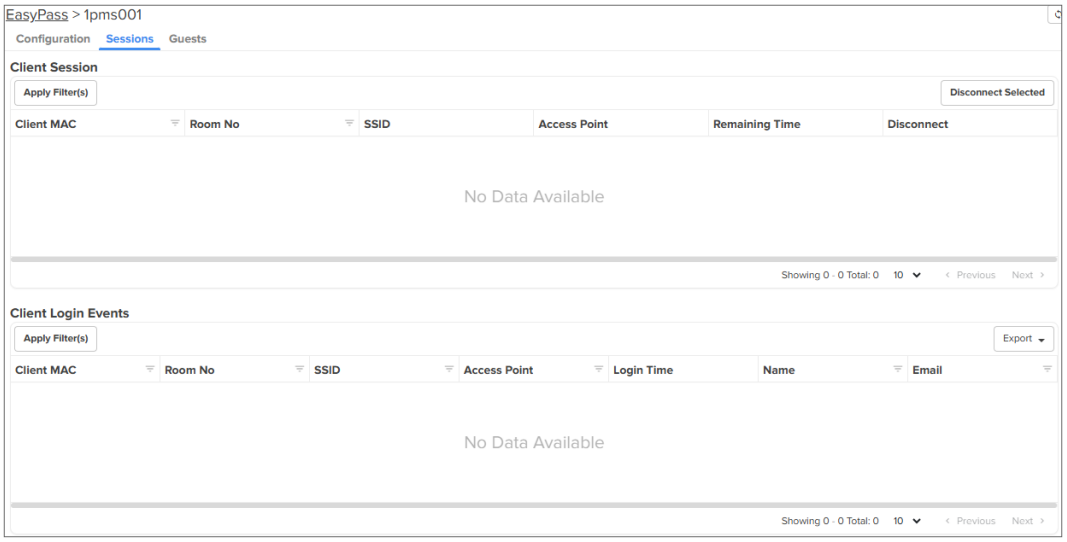
5. Click **Save**.

Note

After configuring the parameters in the **PMS Integration** window, continue to step 8 to configure parameters in the **Limits**, **Design**, and **WLANs** screens.

Once the portal configuration is saved, two additional tabs—**Sessions** and **Guests** are displayed. For more information, see Sessions and Guests.

In Hospitality PMS Beta portal, an additional column—**Room No**—is present in the **Sessions** tab.



MarketApps X

This section includes the following topics:

- Overview
- Adding a new MarketApps App
- MDU Managed Wi-Fi app
  - Basic tab
  - Settings tab
  - Design tab
- MDU Self-Service Personal Wi-Fi app
  - Basic tab
  - Personal Wi-Fi configuration
- Outdoor Hospitality Managed Wi-Fi app
  - Basic tab
  - Settings tab
  - Design tab
  - Units tab
- Senior Living Managed Wi-Fi app
  - Basic tab
  - Settings tab
  - Design tab
  - Units tab
- Configuring units by property managers / front desk staff / Wi-Fi support staff

    - Managing units in the MDU Managed Wi-Fi app
    - Managing units in the Self-Service Personal Wi-Fi App
    - Adding units in cnMaestro Cloud
    - Replacing all units in cnMaestro Cloud
    - Managing units in the Wi-Fi Manager / Wi-Fi Support / Wi-Fi Front Desk Apps
    - Monitoring Sites in the Wi-Fi Manager / Wi-Fi Support / Wi-Fi Front Desk Apps
- Installer app
    - Replacing devices in the Installer app
    - Searching, updating, and replacing existing device in the Installer App
    - Exporting Installation Summary information



Note

- MarketApps is available only in cnMaestro Cloud (version 5.1.0 and above) and is not supported on cnMaestro On-Premises.
- Only APs supporting Wi-Fi 6 (firmware version 6.6.1 and above) and Wi-Fi 7 (firmware version 7.1) are compatible with MarketApps.

Overview

MarketApps is an advanced service within cnMaestro that is designed to enhance network management through tailored applications. It offers specialized tools that empower Managed Service Providers (MSPs) to deliver greater value to their customers and end users by addressing their specific needs and challenges.

MarketApps introduces the following applications for the Multi-Dwelling Unit (MDU), outdoor hospitality, and senior living markets:

- MDU Managed Wi-Fi
- MDU Self-Service Personal Wi-Fi
- Outdoor Hospitality Managed Wi-Fi
- Senior Living Managed Wi-Fi
- Installer App

These applications simplify the management and deployment of Wi-Fi services for property managers, residents, field installers, and service providers through an intuitive and streamlined workflow. The Installer App supports on-site device provisioning by guiding installers through configuration and deployment steps with minimal backend coordination. It helps ensure faster and more accurate installations across properties.

Target audience

- **Property managers**, **Front desk staff**, **Wi-Fi support staff**—MarketApps empowers property managers, front desk staff, and Wi-Fi support staff to centrally administer Wi-Fi access across their properties. They can set up community-wide Wi-Fi networks and manage personal Wi-Fi networks for local residents.

  The following is the terminology for the various apps:

    - **Property managers**—Applicable to MDU Managed Wi-Fi app
    - **Front desk staff**—Applicable to Outdoor Hospitality Managed Wi-Fi app
    - **Wi-Fi support staff**—Applicable to Senior Living Managed Wi-Fi app
- **Residents**—Residents can set up and manage their own Wi-Fi networks within the community, ensuring personalized and secure Internet access.
- **Managed Service Providers (MSPs)**—MarketApps helps the MSPs offer tailored Wi-Fi solutions, enhancing network performance and user satisfaction in multi-dwelling units and apartment complexes.

Benefits

- **Centralized management**—Property managers can oversee and control Wi-Fi access across multiple units or buildings from cnMaestro.
- **Customization**—Residents can set up personal Wi-Fi networks with customized SSIDs and passwords, enhancing their user experience.

Prerequisites

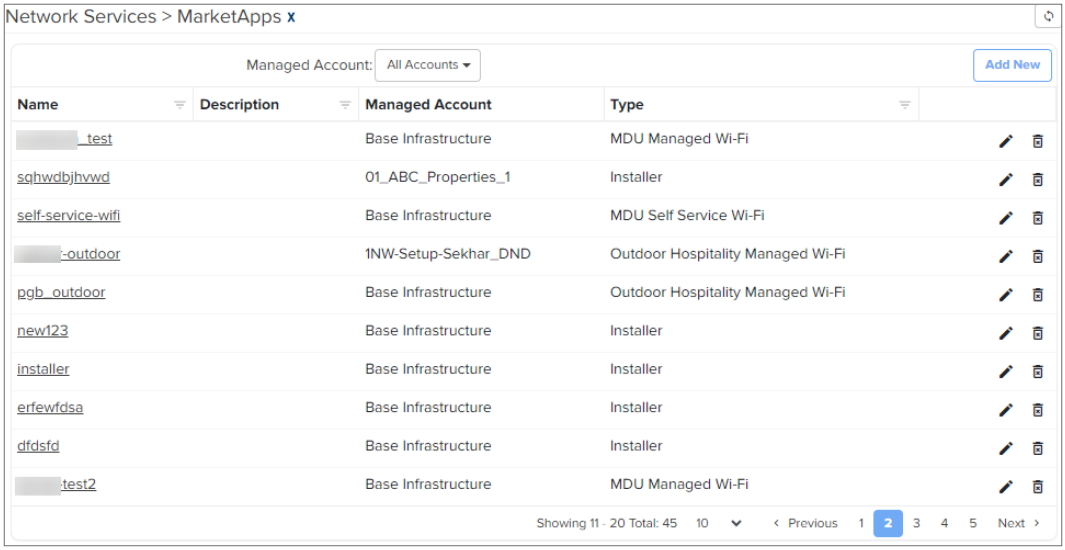
- APs must be onboarded to cnMaestro.
- WLANs and AP groups must be created and mapped to the AP.
- A valid license is required to enable MarketApps in cnMaestro.

Key features

- **Unit Assignment**—Property managers, Front desk staff, Wi-Fi support staff assign APs to residents and guests, and customize SSIDs and passwords.
- **QR Code Access**—Residents and guests can scan a QR code to access the resident or guest app, and configure their Wi-Fi settings.
- **Resident Options**—Depending on the configuration, residents and guests can either modify their SSID and password or receive a fixed SSID if changes are restricted by the MSPs.

To access MarketApps, navigate to **Network Services** > **MarketApps** in cnMaestro.

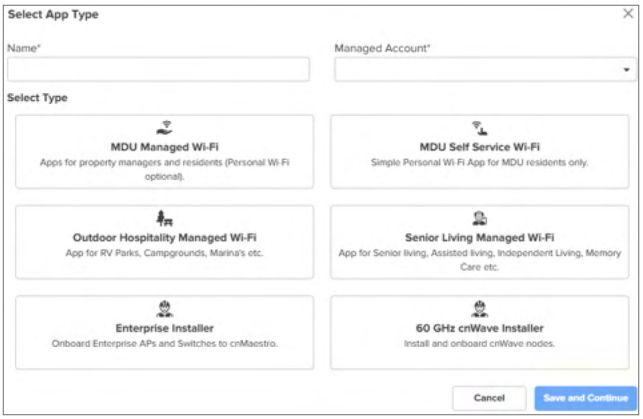
Figure 632 *MarketApps*



Adding a new MarketApps App

To add a new MarketApps app, complete the following steps:

1. Navigate to **Network Services** > **MarketApps** in cnMaestro.
2. Click the **Add New** button on the top right corner.
3. A new window **Select App Type** appears.



4. Enter a name for the new Market App in the **Name** field.
5. Choose the type of managed account for the app from the **Managed Account** dropdown box.
6. Select the required app.
7. Click **Save and Continue**.

   The respective app screens appear as discussed in the following sections:

   - MDU Managed Wi-Fi app
   - MDU Self-Service Personal Wi-Fi app
   - Outdoor Hospitality Managed Wi-Fi app

- Senior Living Managed Wi-Fi app
- Installer app

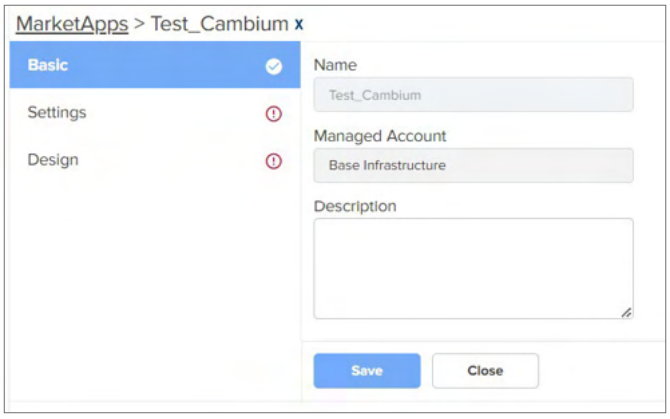
MDU Managed Wi-Fi app

The Managed Wi-Fi app in MarketApps enables property managers to centrally administer and manage Wi-Fi networks within their properties. This feature provisions both community-wide Wi-Fi networks and personal Wi-Fi networks for residents, allowing control and customization.

Basic tab

The Basic tab in MarketApps allows you to provide a description for your Wi-Fi network. The network name and managed account details are automatically populated and cannot be modified. Enter a brief description to clarify the network's purpose.

Figure 633 *Basic tab parameters*



To configure the Basic tab, complete the following steps:

1. **Name**—Displays the chosen name for the Wi-Fi network.
2. **Managed Account**—This field is pre-populated based on previous selections.
3. **Description**—Enter a brief description that clearly explains the intended purpose or specific details of this Wi-Fi configuration.
4. Click **Save**.

Settings tab

The Settings tab in MarketApps enables you to configure advanced settings for your Wi-Fi network. You can set up Community Wi-Fi, Personal Wi-Fi, or other options based on your specific requirements. The configuration in the Settings tab is classified into the following tabs:

- Wi-Fi Management
- Site Monitoring
- Users & Other Settings

Wi-Fi Management

This tab allows users to configure Wi-Fi related parameters, such as Community Wi-Fi and Personal Wi-Fi.

- Community Wi-Fi
- Personal Wi-Fi

Community Wi-Fi

Community Wi-Fi in MarketApps allows property managers to set up and manage a single SSID for all residents within a property. This configuration is designed to provide centralized control over Wi-Fi access while ensuring uniform connectivity for all users.

Figure 634 *Community Wi-Fi settings*



To configure **Community Wi-Fi** under the **Settings** > **Wi-Fi Management** tab in Managed Wi-Fi app, complete the following steps:

1. Select the **WLAN** for the community-wide Wi-Fi network.
2. Review the WLAN details, which include:

   SSID – Displays the configured network name.

   AP Groups – Lists the associated AP groups.

   Devices – Shows the number of devices assigned to this WLAN.
3. If a different WLAN needs to be assigned, click **Change**. A confirmation window appears and click **Yes**.



4. A new **Change WLAN** window appears. Select the required WLAN from the dropdown list and click **Assign**.



Note

Valid WLANs must satisfy the following conditions:

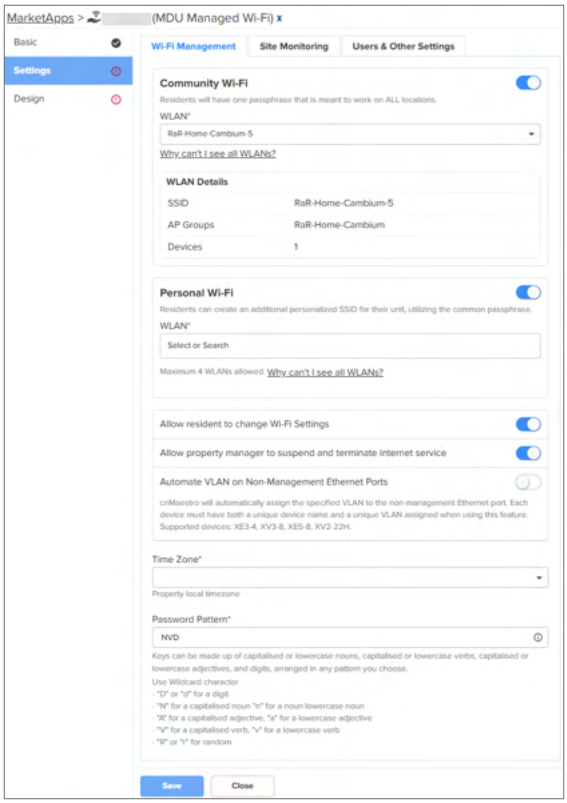
- WLAN's Personal SSID must be disabled.
- Local ePSK table must not have any existing entries.

- WLAN Security settings must be configured as **WPA2 Pre-Shared Keys**, **WPA3 Pre-Shared Keys**, or **WPA2/ WPA3 Pre-Shared Keys**.
- WLAN should not be mapped to any existing MarketApps or EasyPass.

Personal Wi-Fi

The Personal Wi-Fi option in MarketApps allows residents to set up and manage their own personalized Wi-Fi networks within the community. This feature provides flexibility and customization for individual units, enhancing the user experience by allowing residents to manage their SSIDs and passwords. Residents can create and manage multiple personal SSIDs, with a maximum of 4 personal WLANs allowed per unit.

Figure 635 *Personal Wi-Fi settings*



To configure Personal Wi-Fi under the **Settings** > **Wi-Fi Management** tab in Managed Wi-Fi app, complete the following steps:

1. Enable the Personal WLAN option.
2. Select the WLAN for the personal Wi-Fi network.

Note

Valid WLANs must satisfy the following conditions:

- WLAN's Personal SSID must be enabled.
- WLAN Security settings must be configured as **WPA2 Pre-Shared Keys**, **WPA3 Pre-Shared Keys**, or **WPA2/ WPA3 Pre-Shared Keys**.
- WLAN should not be mapped to any existing MarketApps or EasyPass.

3. To assign a different WLAN, click **Change**.

Click **Yes** in the confirmation window.

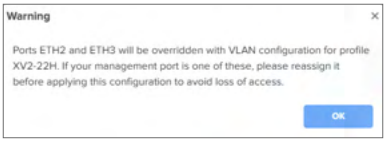


4. A new **Change WLAN** window appears. Select the required WLAN from the dropdown list and click **Assign**.



5. **Allow Resident to Change Wi-Fi Settings**—MSPs can enable or disable the option for residents to configure their personalized settings.
6. **Allow Property Manager to Suspend and Terminate Internet Service**—MSPs can enable or disable the option for property managers to suspend or terminate Internet service.
7. **Automate VLAN on Non-Management Ethernet Ports**—MSPs can enable this option to enforce VLAN configuration on all non-management Ethernet ports of supported devices. This isolates wired traffic in the same way as wireless traffic, improving network security.

   When this option is enabled, a warning message appears.



   The message states that the system overrides ports such as ETH2 and ETH3 with VLAN configuration. If any of these ports serve as management ports, the system may lose access to the device.

   Reassign the management port before applying the configuration to avoid connectivity issues.
8. Select the **Time Zone** from the dropdown list. This sets the local time zone of the property where the MarketApps app is running, ensuring the application operates according to the specific time zone of the city or location.
9. Define the **Password Pattern** by specifying a mix of capitalized/lowercase letters, nouns, verbs, adjectives, random letter words, and digits.
10. Define the **Password Pattern**.

    Specify a password pattern using a combination of the following elements:

    - Capitalized/lowercase nouns
    - Capitalized/lowercase adjectives
    - Capitalized/lowercase verbs
    - Random letter words
    - Digits (0–9)

    Use the following pattern keys:

    - N – Capitalized noun
    - n – Lowercase noun

- A – Capitalized adjective
- a – Lowercase adjective
- V – Capitalized verb
- v – Lowercase verb
- D or d – Digit
- R or r – Random letter word

Arrange the keys in any order to define your desired password structure.

For example, the pattern **AnDvr** might generate a password like **Happytree7runxy**.

11. Click **Save**.

Note

MSPs can select Community Wi-Fi, Personal Wi-Fi, or both options, depending on their requirements.

Site Monitoring

This tab allows administrators to add the site that the property managers can monitor.

To add a site, complete the following steps:

1. Go to the **Settings** > **Site Monitoring** tab.

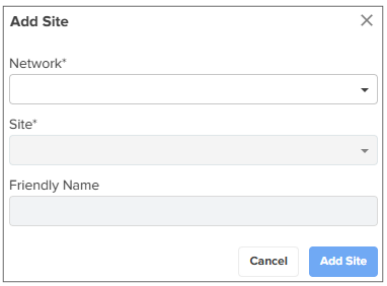
   By default, the monitoring functionality is disabled.

2. To enable, move the toggle to the ON position.

   A list of all allowed sites is displayed.



3. Click **Add Site**.



4. From the respective dropdown lists, select the network and site that you want to add.
5. Click **Add Site**.

Users & Other Settings

This tab allows administrators to configure the property managers and the language for the MarketApps.

To configure, complete the following steps:

1. Go to the **Settings** > **Users & Other Settings** tab.
2. Select the **Language** for the manager and resident portal.

Note

Currently, only English and Spanish are supported.

3. Enter the property manager's email address in the **Invite Property Managers** text box to send an invitation. Property managers can activate and oversee internet services for residents within their property.

Note

A maximum of 10 property manager email addresses can be added per MarketApps app.

Design tab

The Design tab in MarketApps allows you to customize the branding and appearance of the property manager and resident portals, ensuring a cohesive and professional user experience.

Figure 636 *Design tab parameters*

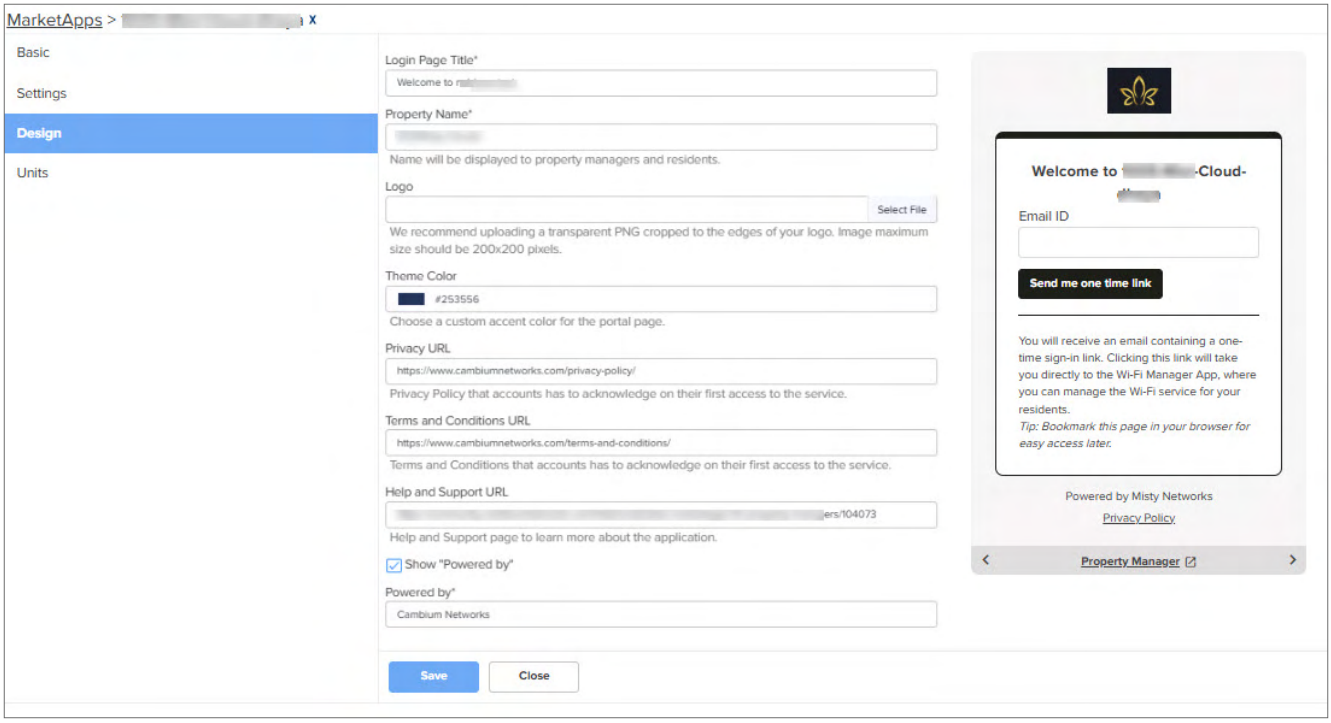
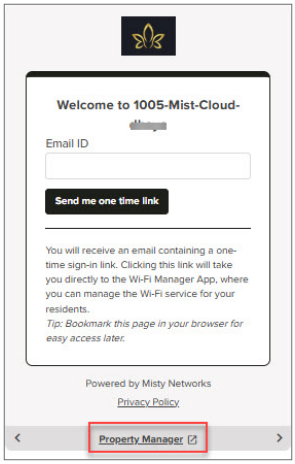
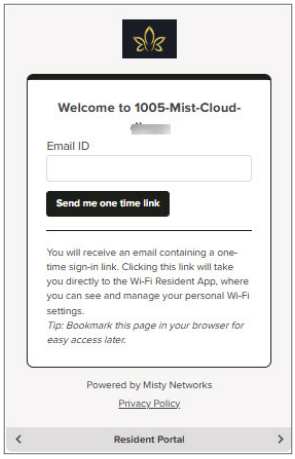
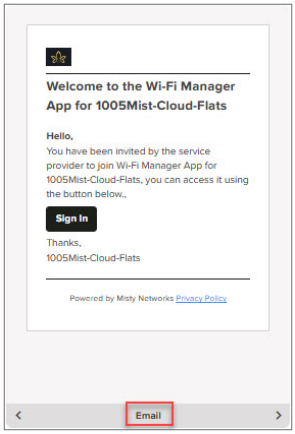


Table 167 *Design tab parameters*

Parameter	Description
Login Page Title	Customize a welcome message displayed on the login page
Property Name	Specify the property name used for internal identification and email communications.

Parameter	Description
Logo	Upload a logo file (PNG recommended) cropped to the edges and sized up to 200x200 pixels.
Theme Color	Customize the Managed Wi-Fi App's color scheme with a chosen accent color.
Privacy URL	Provide the URL to your Privacy Policy.
Terms and Conditions URL	Provide the URL to the Terms and Conditions that users must acknowledge.
Help and Support URL	Provide the URL to user documentation or support resources. Property managers can use this field to share help content that explains how the portal works, tailored to their specific deployment and branding. This enhancement supports better onboarding and reduces support dependency. The configured URL appears as a **Help** link in the property manager interface.
Show "Powered by"	Enable this option to display the Powered by message.
Sample screen	The sample screen section includes three views: 1. **Property Manager**—Displays the Property Manager interface where users can enter their Email and request a one-time link for access.  Click **Property Manager** or the icon to open the Manager Portal, allowing MSP admins to manage property settings. From the portal, admins can perform actions such as Assign, Suspend, Extend, and Terminate units. **Note**: Only Super Admin, Admin, and Operator users can utilize this functionality. 2. **Resident Portal**—This shows the Resident Portal interface where users can input their email to receive a one-time link for accessing their personal Wi-Fi settings.

Parameter	Description
	 3. **Email**—Provides a view of the email format that users receive, which contains a link to access the Wi-Fi Manager App. 
Save	Click **Save** to apply the changes after configuring the Design tab.

MDU Self-Service Personal Wi-Fi app

The Self-Service Personal Wi-Fi app in MarketApps allows residents to independently manage and customize their Wi-Fi networks within residential properties. This feature provides residents with the capability to create and personalize SSIDs for their units, enhancing their control over network settings.

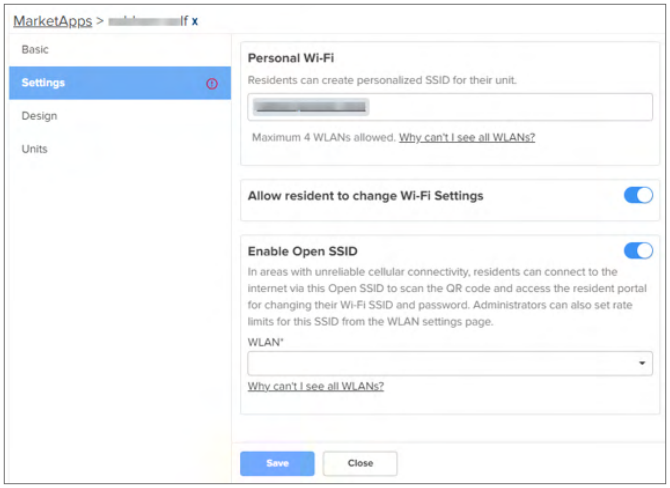
Basic tab

The configuration steps for the Basic tab are the same as those detailed earlier in the documentation. For information on setting the network name, managed account, and description, refer to the Basic tab configuration steps.

Personal Wi-Fi configuration

Residents can create personalized SSIDs for their units, allowing them to customize their network identification.

Figure 637 *Personal Wi-Fi settings*



To configure Personal Wi-Fi, complete the following steps:

1. Select the WLAN for the personal Wi-Fi network from the **WLAN** dropdown list.

Note

Valid WLANs must satisfy the following conditions:

- WLAN's Personal SSID must be enabled.
- WLAN Security settings must be configured as **WPA2 Pre-Shared Keys**, **WPA3 Pre-Shared Keys**, or **WPA2/ WPA3 Pre-Shared Keys**.
- WLAN should not be mapped to any existing MarketApps or EasyPass.

2. **Allow Resident to Change Wi-Fi Settings**—Solution owners can enable or disable the option for residents to configure their personalized configuration.
3. **Enable Open SSID** option allows residents to connect to the internet, scan the QR code, and access the resident portal to change their Wi-Fi SSID and password. Administrators can set rate limits for this SSID from the WLAN settings page.
4. Select the WLAN for the Open SSID network from the **WLAN** dropdown list.

Note

Valid WLANs must satisfy the following conditions:

- WLAN's Personal SSID must be disabled.
- WLAN Security settings must be configured as Open or OWE.
- WLAN should not be mapped to any existing MarketApps or EasyPass.

5. Click **Save.**

Outdoor Hospitality Managed Wi-Fi app

This market app is built for RV parks, campgrounds, and marinas to help setup guest Wi-Fi fast and frictionless. The app allows front desk teams to view, manage, and print guest credentials. It also allows a self-service portal for visitors to connect to the network using simple QR-based access.

Basic tab

The configuration steps for the Basic tab are the same as those detailed earlier in the documentation. For information on setting the network name, managed account, and description, refer to the Basic tab configuration steps.

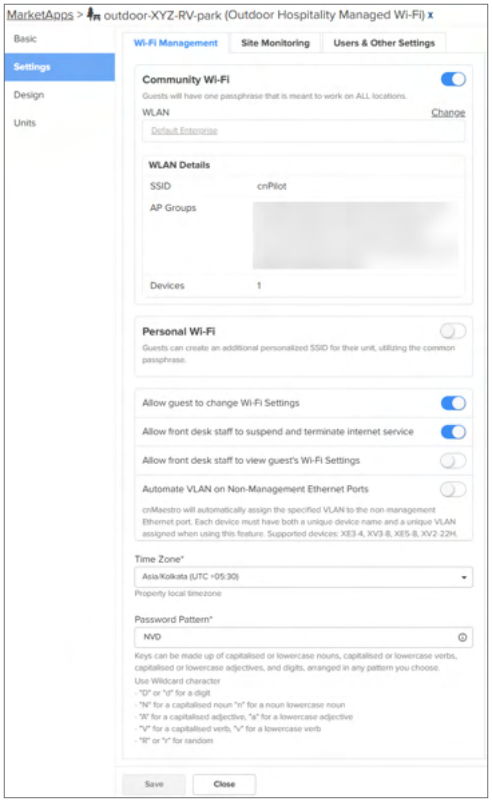
Settings tab

The Settings tab in MarketApps enables you to configure advanced settings for your Wi-Fi network. You can set up Community Wi-Fi, Personal Wi-Fi, or other options based on your specific requirements. For configuration information, refer to Settings tab.

You can allow the front desk staff to suspend and terminate guests' internet service. You can also allow the front desk personnel to view and download the guests' Wi-Fi settings as described below:

- **Allow guest to change Wi-Fi Settings**—MSPs can enable or disable the option for guests to configure their personalized settings.
- **Allow front desk staff to suspend and terminate internet service**—MSPs can enable or disable the option for front desk staff to suspend or terminate Internet service.
- **Allow front desk staff to view guest's Wi-Fi Settings**—MSPs can enable or disable the option for front desk staff to view and download the guests' Wi-Fi settings.

Figure 638 *Outdoor Hospitality Managed Wi-Fi > Settings tab parameters*



Design tab

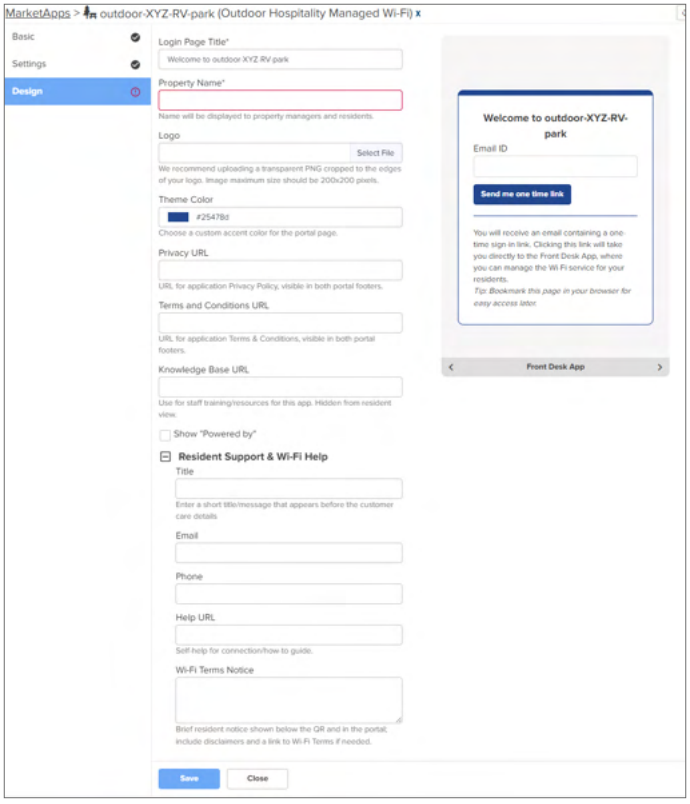
The Design tab in MarketApps allows you to customize the branding and appearance of the front desk and resident portals, ensuring a cohesive and professional user experience.

For configuration information, refer to Design tab.

In addition to the parameters listed in the Design tab topic, you can also configure the following parameters that are specific to Outdoor Hospitality Managed Wi-Fi and Senior Living Managed Wi-Fi apps:

Parameter	Description
Resident Support & Wi-Fi Help	
Title	Name or a short description to appear on the customer support details page.
Email	Email ID that the customers can contact for support.
Phone	phone number that the customers can contact for support.
Help URL	URL of the self-help page for connecting to the Wi-Fi.
Wi-Fi Terms Notice	Terms and conditions to be shown in the resident details page below the QR code and on the portal page. You can also add a link to the terms and conditions page, if available.

Figure 639 *Outdoor Hospitality Managed Wi-Fi > Design tab parameters*



Units tab

For information on adding, editing, replacing, and deleting units from the MarketApps UI, refer Adding units in cnMaestro Cloud and Replacing all units in cnMaestro Cloud.

Senior Living Managed Wi-Fi app

This market app is built for residents and support staff of senior care facilities to help setup guest Wi-Fi. The app allows support staff to view, manage, and print guest credentials. It also allows a self-service portal for visitors to connect to the network using simple QR-based access.

Basic tab

The configuration steps for the Basic tab are the same as those detailed earlier in the documentation. For information on setting the network name, managed account, and description, refer to the Basic tab configuration steps.

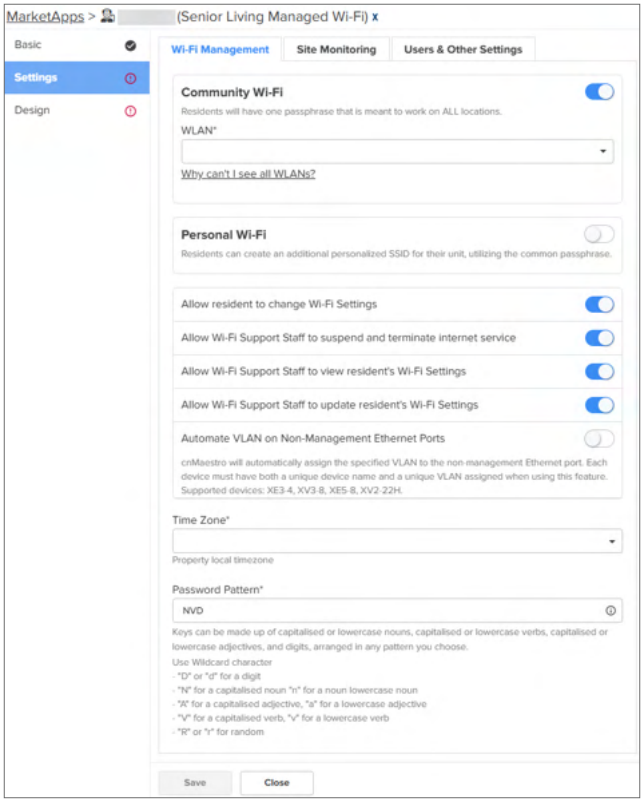
Settings tab

The Settings tab in MarketApps enables you to configure advanced settings for your Wi-Fi network. You can set up Community Wi-Fi, Personal Wi-Fi, or other options based on your specific requirements. For configuration information, refer to Settings tab.

You can allow the Wi-Fi Support staff to suspend and terminate guests' internet service. You can also allow the Wi-Fi Support staff to view, download, and update the residents' Wi-Fi settings as described below:

- **Allow resident to change Wi-Fi Settings**—MSPs can enable or disable the option for residents to configure their personalized settings.
- **Allow Wi-Fi Support Staff to suspend and terminate internet service**—MSPs can enable or disable the option for front desk staff to suspend or terminate Internet service.
- **Allow Wi-Fi Support Staff to view resident's Wi-Fi Settings**—MSPs can enable or disable the option for Wi-Fi Support Staff to view and download the residents' Wi-Fi settings.
- **Allow Wi-Fi Support Staff to update resident's Wi-Fi Settings**—MSPs can enable or disable the option for Wi-Fi Support Staff to update the residents' Wi-Fi settings.

Figure 640 *Senior Living > Settings tab parameters*



Design tab

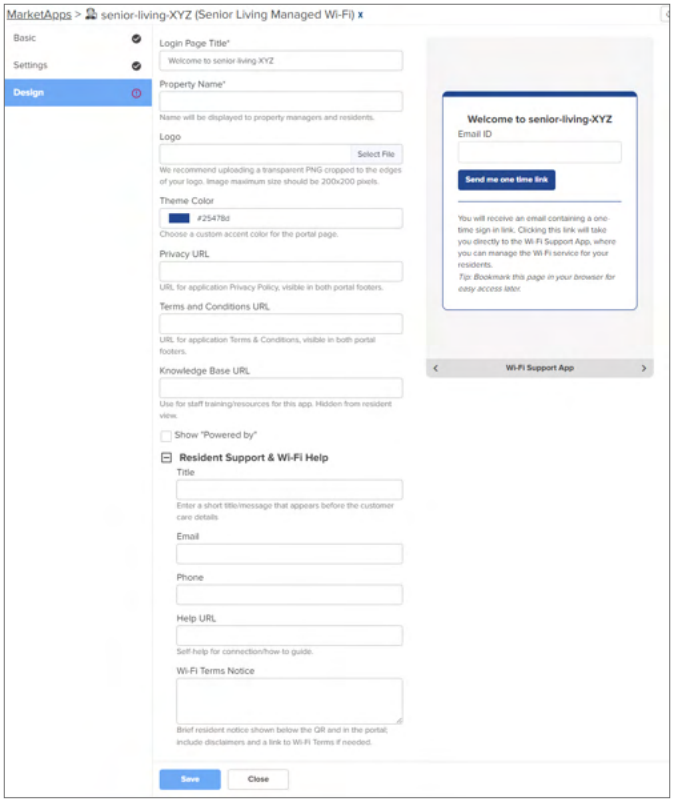
The Design tab in MarketApps allows you to customize the branding and appearance of the support and guest portals, ensuring a cohesive and professional user experience.

For configuration information, refer to Design tab.

In addition to the parameters listed in the Design tab topic, the following parameters are specific to Outdoor Hospitality Managed Wi-Fi and Senior Living Managed Wi-Fi apps:

Parameter	Description
Resident Support & Wi-Fi Help	
Title	Name or a short description that appears on the customer support details page.
Email	Email ID that the customers can contact for support.
Phone	phone number that the customers can contact for support.
Help URL	URL of the self-help page for connecting to the Wi-Fi.
Wi-Fi Terms Notice	Terms and conditions to be shown in the resident details page below the QR code and on the portal page. You can also add a link to the terms and conditions page, if available.

Figure 641 *Senior Living > Design tab parameters*



Units tab

For information on adding, editing, replacing, and deleting units from the MarketApps UI, refer Adding units in cnMaestro Cloud and Replacing all units in cnMaestro Cloud.

Configuring units by property managers / front desk staff / Wi-Fi support staff

This section contains the following topics:

- Managing units in the MDU Managed Wi-Fi app
- Managing units in the Self-Service Personal Wi-Fi App
- Adding units in cnMaestro Cloud
- Replacing all units in cnMaestro Cloud
- Managing units in the Wi-Fi Manager / Wi-Fi Support / Wi-Fi Front Desk Apps
  - Signing in to the Wi-Fi Manager / Wi-Fi Support / Wi-Fi Front Desk Apps
  - Assigning units in the Wi-Fi Manager App
  - Assigning residents in bulk
  - Settings

- Theme settings
- AP Health
- MarketApps app selector
- View options in the Property Manager App
- View options in the Resident App

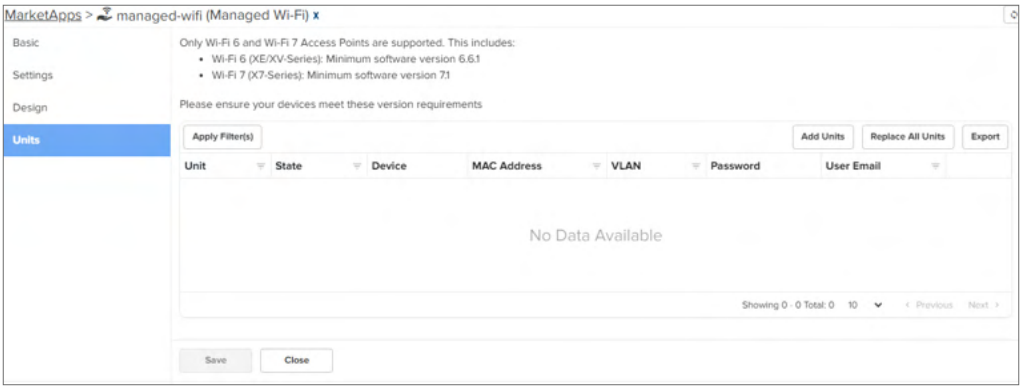
Managing units in the MDU Managed Wi-Fi app

The MDU Managed Wi-Fi app enables property managers to configure and oversee network settings for units using cnMaestro. They can add, edit, and replace units by importing the AP and unit details in the CSV format. The CSV format with sample values is as follows:

Serial Number	Unit	MAC Address	VLAN	Personal SSID	Password
Serial number of the device	Unit name	MAC Address of the device	VLAN(1 - 4094)	SSID for the personal Wi-Fi	Password for Wi-Fi
B1000D000000	MDU 01	B1:00:0D:00:00:00	10	SSID 01	Pa$$Word001
B1000D000001	MDU 02	B1:00:0D:00:00:01	13	SSID 02	Pa$$Word002
B1000D000003	MDU 03	B1:00:0D:00:00:03	11	SSID 03	Pa$$Word003

To set up and manage your Wi-Fi networks, complete the following steps:

1. In the MDU Managed Wi-Fi app, navigate to the **Units** tab.



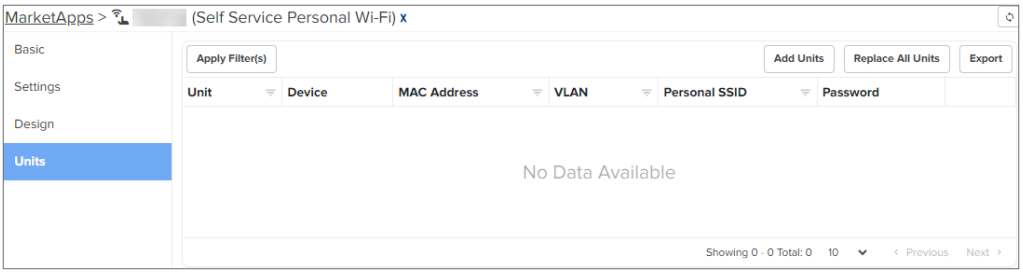
2. To add units, refer to Adding units in cnMaestro Cloud.
3. To replace all units, refer to Replacing all units in cnMaestro Cloud.

Managing units in the Self-Service Personal Wi-Fi App

The Self-Service Personal Wi-Fi App allows users to configure their personal Wi-Fi networks using cnMaestro.

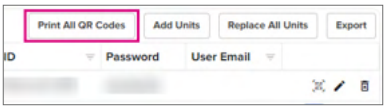
To set up and manage your personal Wi-Fi network settings, complete the following steps:

1. In the Self Service Personal Wi-Fi app, navigate to the **Units** tab.



2. To add units, refer to Adding units in cnMaestro Cloud.

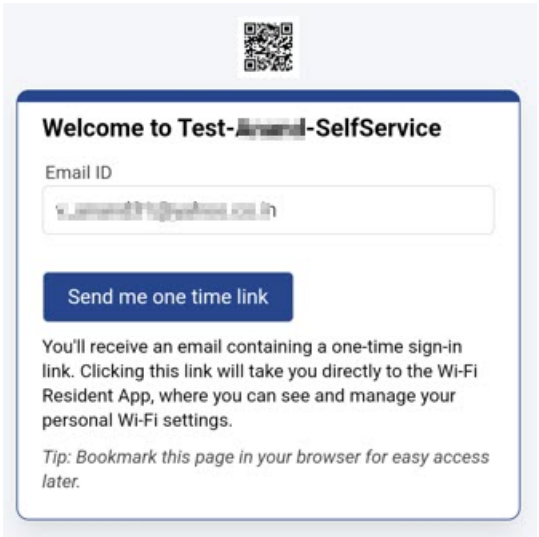
3. To replace all units, refer to Replacing all units in cnMaestro Cloud.
4. To export the data, click **Export**.
5. Click **Print All QR Codes** to open a QR scan page.

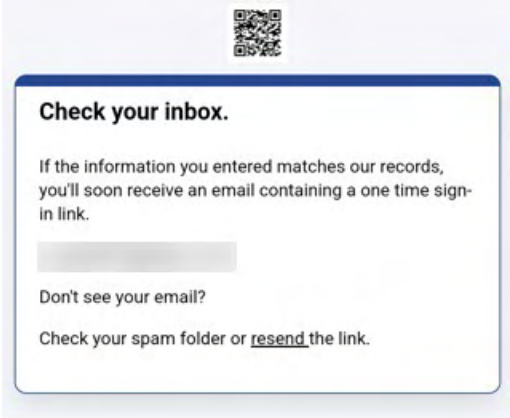


6. Scan the QR code using your mobile device to get a link.

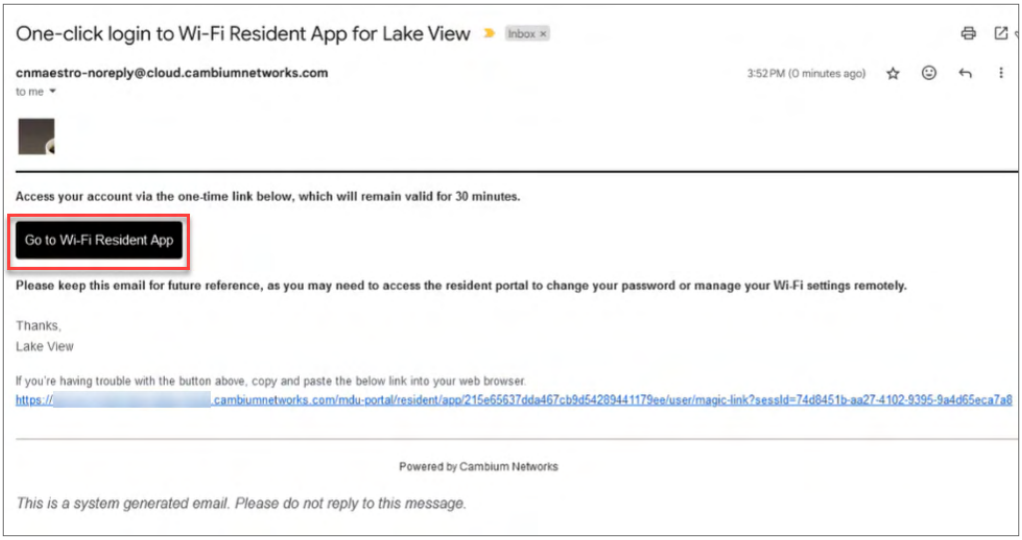


7. Enter your email ID and click **Send me a one time link**.

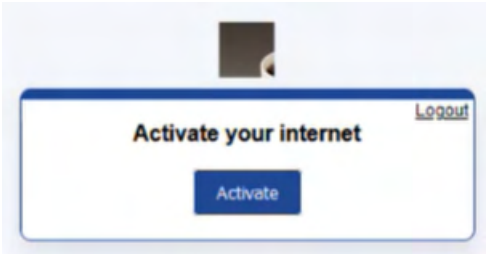




8. Open the email and click **Go to the Wi-Fi Resident App**.



9. Click **Activate** to initiate the internet activation process.



10. A new window titled **Change Wi-Fi Settings** appears. Change your Personal Wi-Fi Network Name and Wi-Fi password in the respective fields.



11. Click **Update** to save the changes.
12. You receive a message that says **Wi-Fi settings updated successfully**. Below the QR code, the option **Personal Wi-Fi** appears. You can scan to connect to this network.



13. Scan the QR code to verify that your Personal Wi-Fi Network Name and Wi-Fi password have been updated.

Adding units in cnMaestro Cloud

To add units, complete the following steps:

Note

All units in the CSV file will be added to cnMaestro.

- Any unit that is in the CSV but not in cnMaestro will be added as a new unit.
- Information about existing units will be updated.

1. In the MDU Managed Wi-Fi, MDU Self-Service Personal Wi-Fi, Outdoor Hospitality Managed Wi-Fi, and Senior Living Managed Wi-Fi app, navigate to the **Units** tab.
2. To add units, click **Add Units**.

   The Add Units window appears.



3. To download a sample template containing the required format, click **Download Sample Template**.

   An example of the sample template and parameters is shown below:

Serial Number	Unit	MAC Address	VLAN	Personal SSID	Password
Serial number of the device	Unit name	MAC Address of the device	VLAN(1 - 4094)	SSID for the personal Wi-Fi	Password for Wi-Fi
B1000D000000	MDU 01	B1:00:0D:00:00:00	10	SSID 01	Pa$$Word001
B1000D000001	MDU 02	B1:00:0D:00:00:01	13	SSID 02	Pa$$Word002
B1000D000003	MDU 03	B1:00:0D:00:00:03	11	SSID 03	Pa$$Word003

Parameter	Description
Serial Number	Serial number of the device.
Unit	Name of the unit (for example, MDU 01, MDU 02, and MDU 03 are apartment numbers).
MAC Address	MAC address of the unit.
VLAN	VLAN ID assigned to the unit.
Personal SSID	SSID for the personal Wi-Fi network.
Password	Password for the Wi-Fi network.

4. After entering the details, save the Excel file with a new name to ensure you have a copy of the filled template and import it to cnMaestro.

   Note this step is crucial to avoid overwriting the original template.

5. To import the CSV file with the unit information, click **Browse** in the Add Units window, select the file.

6. Click **Review**.

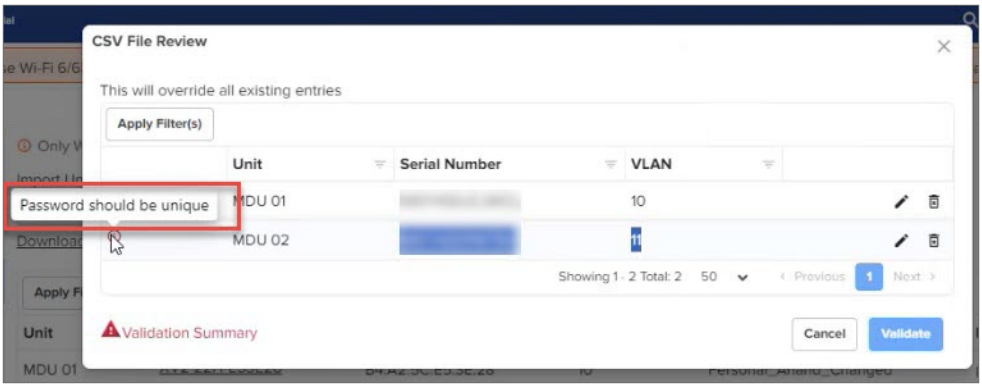
   cnMaestro validates the information and displays the validated information in the Review Add Units window.



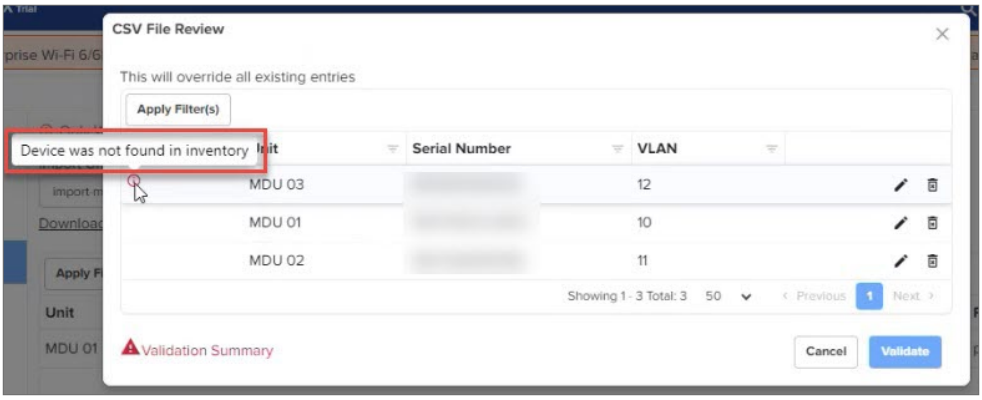
7. Any validation errors are displayed with a caution (ⓘ) icon.

   The following are some of the common error messages and their respective solutions:

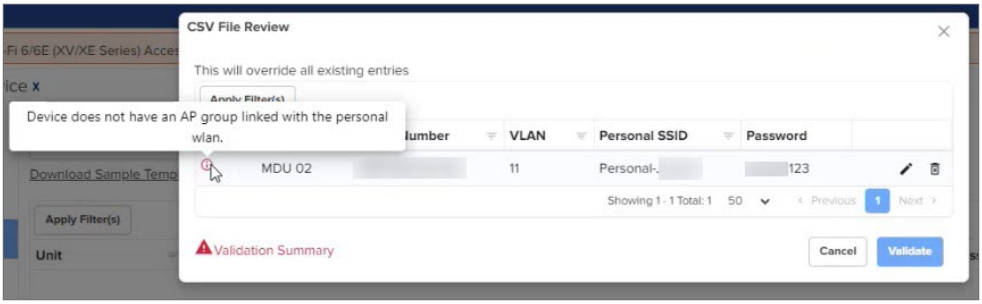
   - **Password should be unique**—Ensure each unit has a unique password. Modify the password in the template so no two units share the same password.



- **Device not found in inventory**—Ensure the serial number and MAC address entered correspond to devices that are already registered in the cnMaestro inventory. Make sure to import the details only after Onboarding the device.



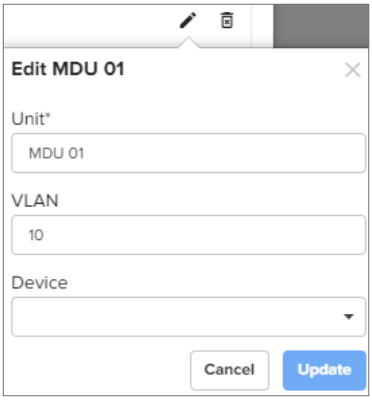
- **Device does not have an AP group linked with the personal wlan**—Ensure each device is only linked to one application at a time. Verify the device has an AP group associated with the personal WLAN before proceeding with the configuration.



- **Validates the unit**—Ensure the unit is less than 32 characters and contains only alphanumeric characters, underscores (_), hyphens (-), and spaces.
- **Checks for duplicate units**—Ensure each unit is unique.
- **Validates the password**—Ensure the password is between 8 and 64 characters long and does not include ", ', , /, ?, =, -, +, or spaces.
- **Validates the SSID**—Ensure the SSID is less than 32 characters and contains only alphanumeric characters, underscores (_), hyphens (-), and spaces.
- **Validates the VLAN**—Ensure the VLAN is an integer between 1 and 4094.

- **Check if the device is already linked to another MarketApp**—Ensure devices are not linked to another application.
- **Checks for duplicate devices**—Ensure each device is unique.
- **Ensures that there is a device present**—Verify a device is specified as it is required.
- **Validates that the AP group is linked to all mapped WLANs to the app**— Ensure the device has an AP group linked with all the mapped personal and community WLANs.
- **Ensures the SSID is not duplicated**—Ensure each SSID is unique.

8. You can correct the validation errors in the units by one of the following ways:
   - Individually edit by clicking the edit (✎) icon corresponding to the unit and modifying the data.



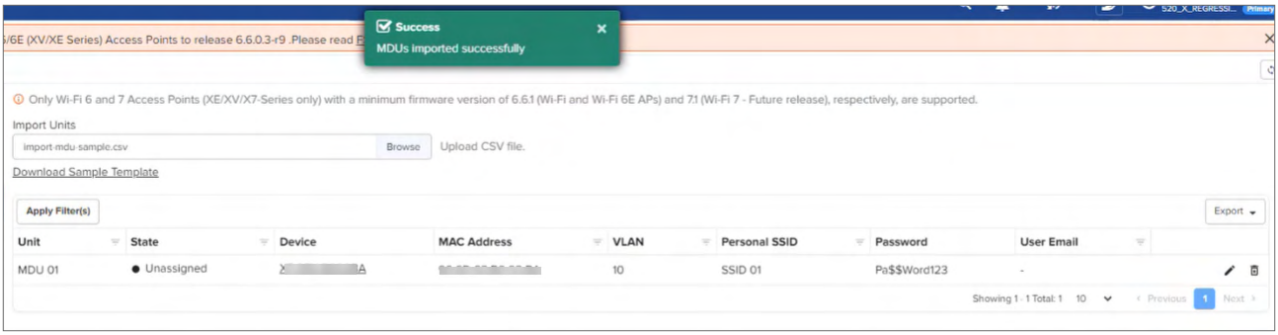
   - Import the CSV file again with corrected information.
9. Once the file imports without validation errors, a success message is displayed.
10. Click **Add Units** to finalize the import process.

Note

After importing, note the following points:

- Ensure the SSID name and password in the Excel sheet remain unchanged unless updated by the customer.
- Residents and guests can modify their SSID and password through the resident and guest portals.
- If the following option is enabled, respective residents or guests can change their SSID and password settings, and these changes do not get overwritten later:
  - **Allow resident to change Wi-Fi settings**—In the MDU Managed Wi-Fi, Senior Living Managed Wi-Fi, MDU Self Service Wi-Fi apps.
  - **Allow guest to change Wi-Fi settings**—In the Outdoor Hospitality Managed Wi-Fi app.

11. Once the devices are successfully added, a confirmation message is displayed.



12. Click **Save**.

Replacing all units in cnMaestro Cloud

To replace units, complete the following steps:

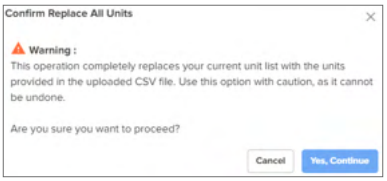
Warning

This option replaces all the existing units in cnMaestro, which cannot be undone.

Create a backup of the existing units before using this replace option.

1. In the MDU Managed Wi-Fi, MDU Self-Service Personal Wi-Fi, Outdoor Hospitality Managed Wi-Fi, and Senior Living Managed Wi-Fi app, navigate to the **Units** tab.
2. To add units, click **Replace All Units**.

   A confirm message with a warning that all units will be replaced appears.



3. Click **Yes, Continue**.

   The Replace All Units window appears.



4. To download the existing unit information, click **Download Backup**.

   An example of the information in the backup file is shown below:

Serial Number	Unit	Device	MAC Address	VLAN	Personal SSID	Password	User Email
	MDU1			1	*_ipv6_One-Network-SSR	12345678	

Parameter	Description
Serial Number	Serial number of the device.
Unit	Name of the unit (for example, MDU 01, MDU 02, and MDU 03 are apartment numbers).
MAC Address	MAC address of the unit.

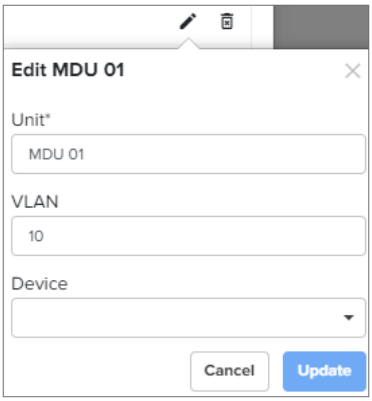
Parameter	Description
VLAN	VLAN ID assigned to the unit.
Personal SSID	SSID for the personal Wi-Fi network.
Password	Password for the Wi-Fi network.
User Email	Email address of the property manager.

5. Click **Browse**, select the file you want to upload, and click **Review**.

   cnMaestro validates the information and displays the validated information in the Review Add Units window.



6. Any validation errors are displayed with a caution (ⓘ) icon.
7. You can correct the validation errors in the units by one of the following ways:
   - Individually edit by clicking the edit (✎) icon corresponding to the unit and modifying the data.



   - Import the CSV file again with corrected information.
8. Once the file imports without validation errors, a success message is displayed.
9. Click **Replace All Units** to finalize the import process.
10. Once the devices are successfully replaced, a confirmation message is displayed.
11. Click **Save**.

Managing units in the Wi-Fi Manager / Wi-Fi Support / Wi-Fi Front Desk Apps

Note

The instructions provided in the following sections are applicable to the following personnel:

- **Property managers**—Applicable to MDU Managed Wi-Fi app through the Wi-Fi Manager app
- **Front desk staff**—Applicable to Outdoor Hospitality Managed Wi-Fi app through the Wi-Fi Front Desk app

- **Wi-Fi support staff**—Applicable to Senior Living Managed Wi-Fi app through the Wi-Fi Support app

Any changes or app-specific information is mentioned in the respective sections or steps.

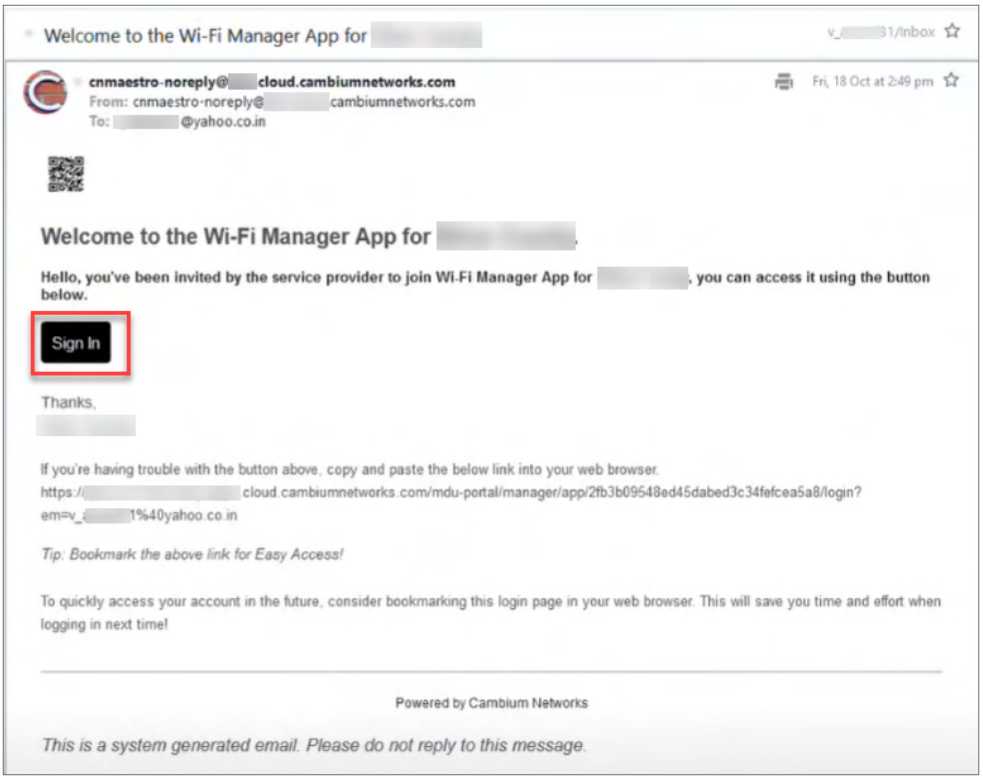
Managing units in the respective apps involves the following steps:

- Signing in to the Wi-Fi Manager / Wi-Fi Support / Wi-Fi Front Desk Apps
- Assigning units in the Wi-Fi Manager App
- Assigning residents in bulk
- Settings
- Theme settings
- Help
- AP Health
- MarketApps app selector
- View options in the Property Manager App
- View options in the Resident App
- Monitoring Sites in the Wi-Fi Manager / Wi-Fi Support / Wi-Fi Front Desk Apps

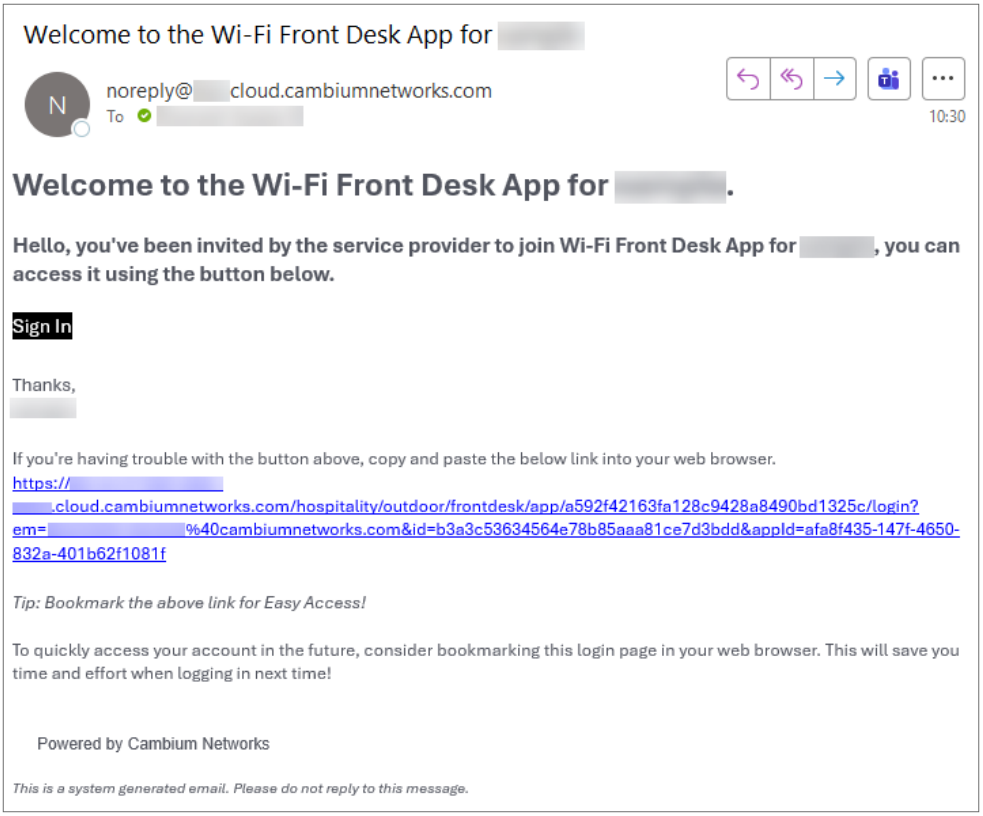
Signing in to the Wi-Fi Manager / Wi-Fi Support / Wi-Fi Front Desk Apps

The personnel managing the various apps receive an email to sign in to the respective apps for managing units.

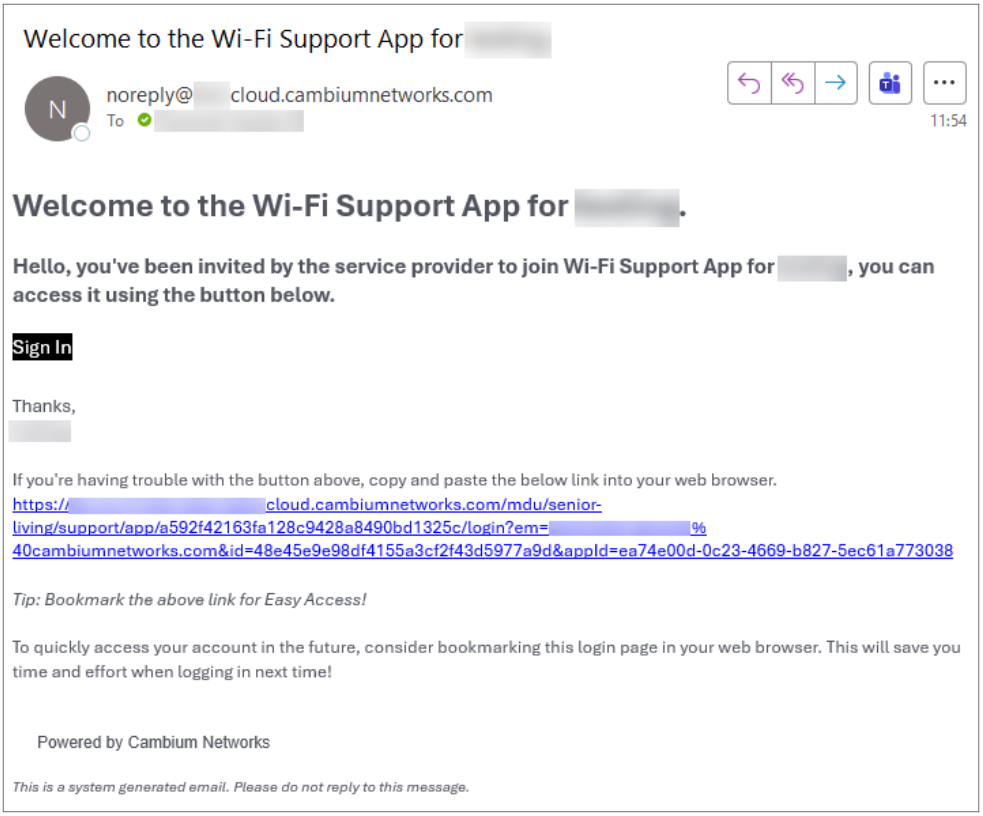
1. The respective personnel receive an invitation email as follows:
   - For property managers, an email with the title **Welcome to the Wi-Fi Manager App for** <property-name>:



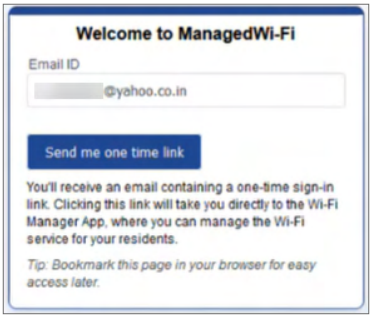
   - For front desk staff, an email with the title **Welcome to the Wi-Fi Front Desk App for** <property-name>:



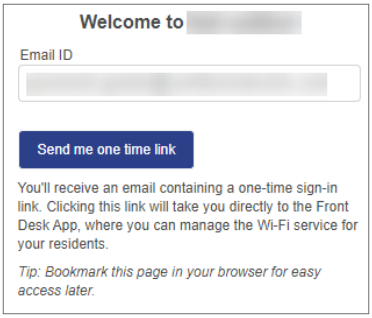
- For Wi-Fi support staff, an email with the title **Welcome to the Wi-Fi Support App for** <property-name>:



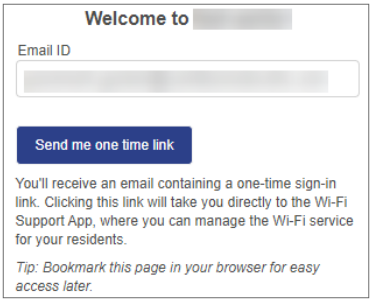
2. Click **Sign In**.
3. The personnel must enter the same email ID provided on the respective app settings page.
   - For property managers (MDU Managed—Wi-Fi Manager App):



   - For front desk staff (Outdoor Hospitality—Wi-Fi Front Desk App):



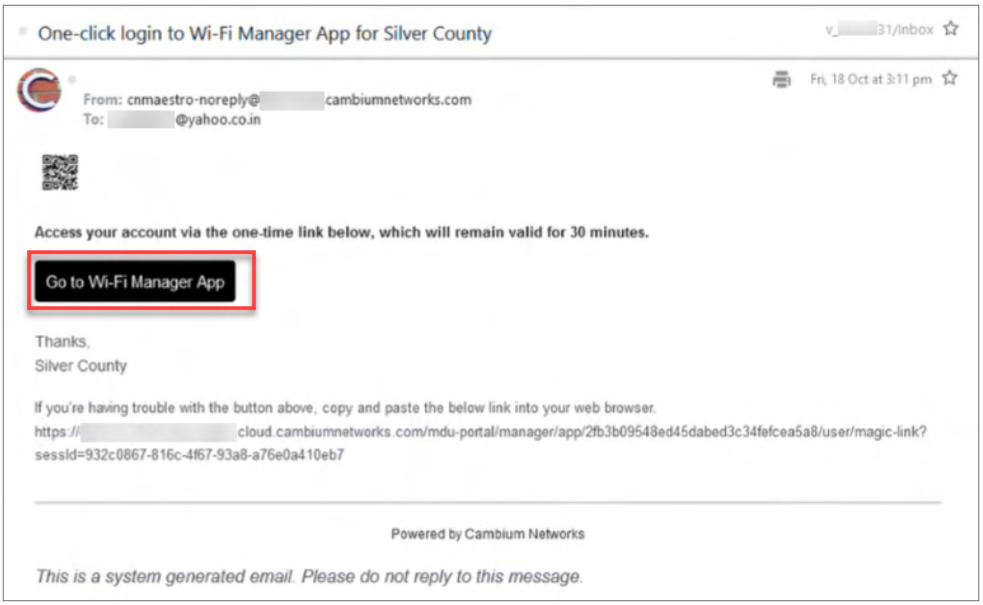
- For Wi-Fi support staff (Senior Living—Wi-Fi Support App):



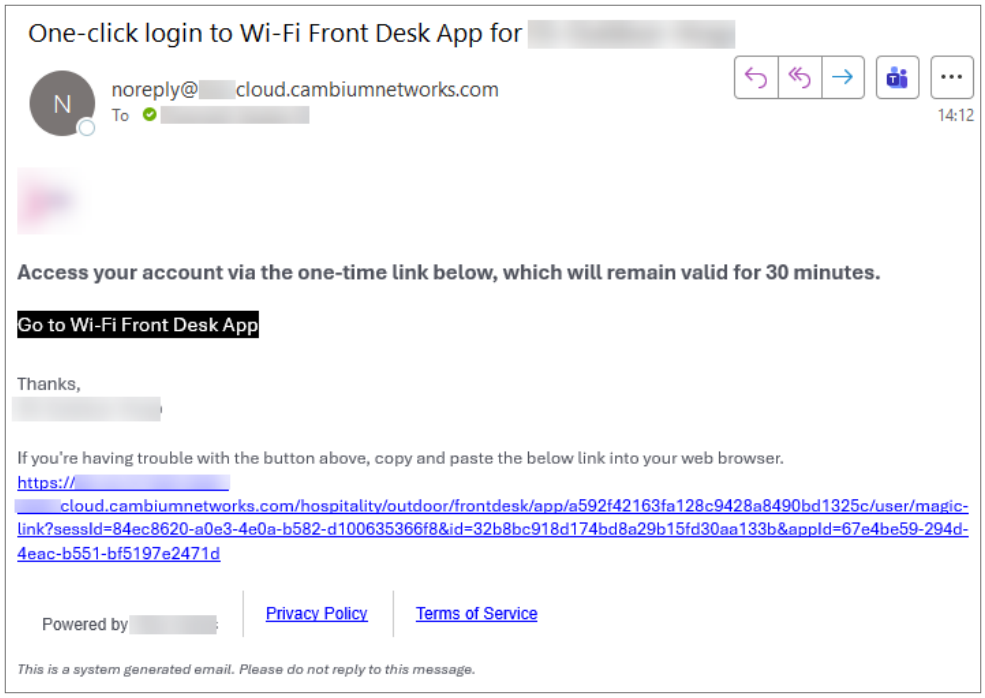
4. Click **Send me a one time link**.

   The personnel receive an email containing a one-time link for logging into the respective app.:

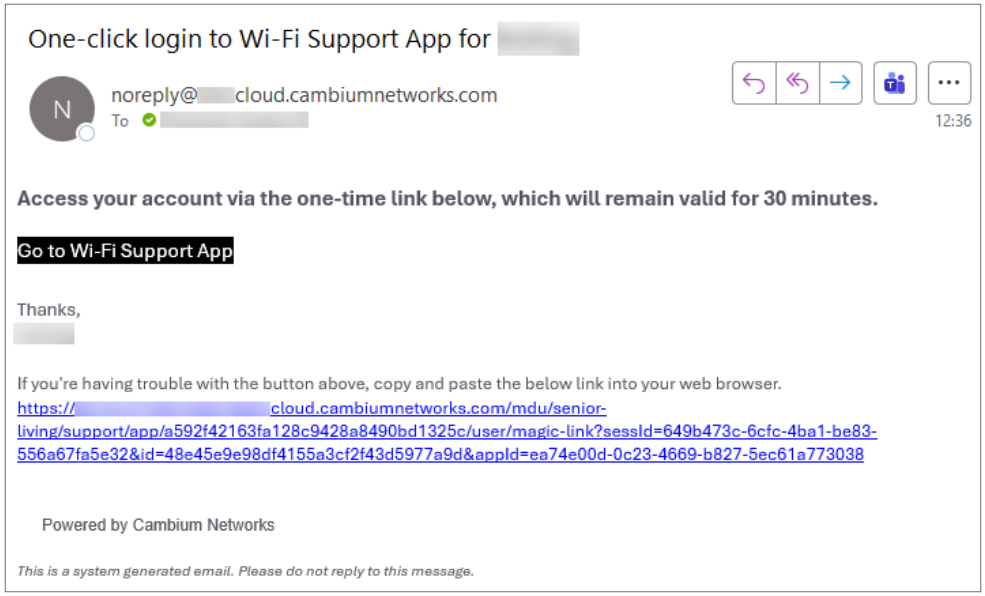
   - For property managers (MDU Managed—Wi-Fi Manager App):



   - For front desk staff (Outdoor Hospitality—Wi-Fi Front Desk App):



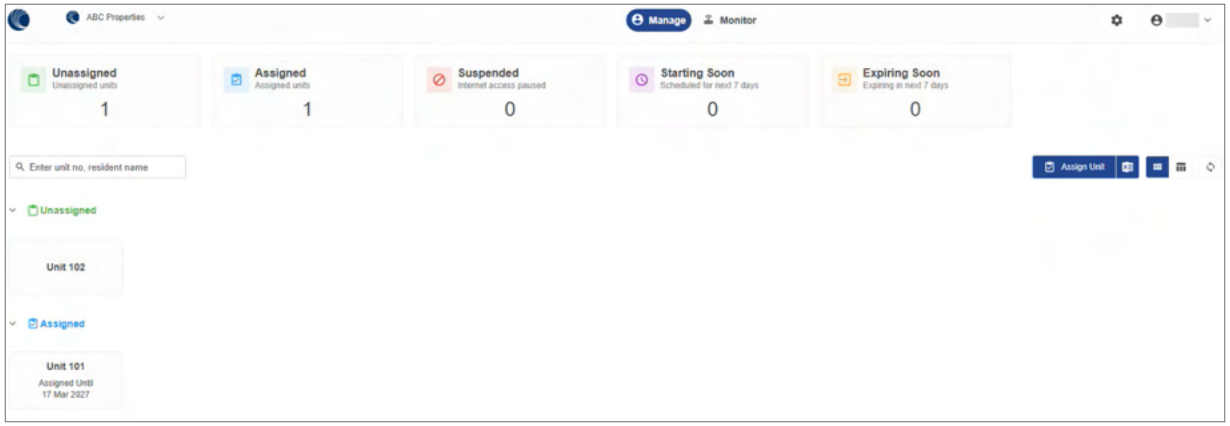
- For Wi-Fi support staff (Senior Living—Wi-Fi Support App):



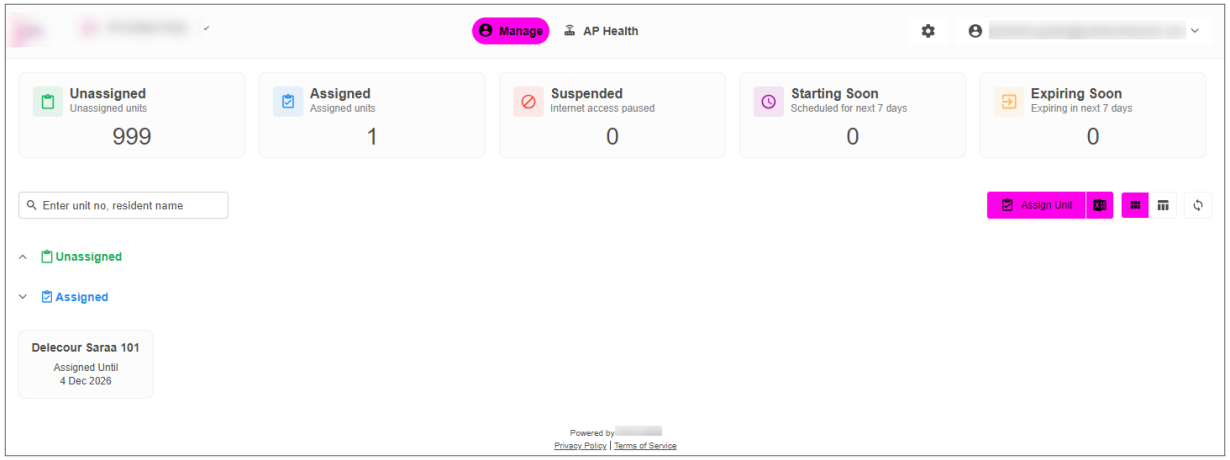
5. Click **Go to Wi-Fi Manager App** / **Go to Wi-Fi Support App** / **Go to Wi-Fi Front Desk App**.

   The respective app interfaces are displayed as follows:

- **Wi-Fi Manager App** interface (MDU Managed Wi-Fi app):



- **Wi-Fi Front Desk App** interface (Outdoor Hospitality Managed Wi-Fi app):



- **Wi-Fi Support App** interface (Senior Living Managed Wi-Fi app):

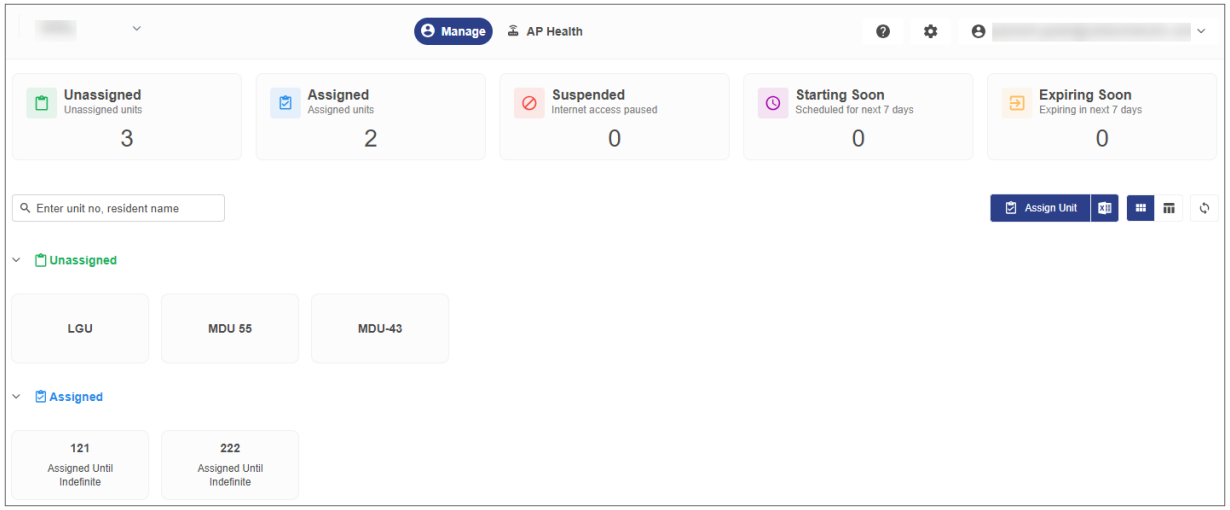


Table 168 *App interface elements - Common to all the above mentioned apps*

Options	Description
Unassigned	Displays the total number of units that are yet to be assigned. Click this widget to filter

Options	Description
	the view and show only unassigned units.
Assigned	Shows units that have been successfully assigned. Click this widget to filter the view and show only assigned units.
Suspended	Lists units with temporarily paused internet access. Click this widget to filter the view and show only suspended units.
Starting Soon	Indicates assignments that are scheduled to begin soon (within 7 days). Click this widget to filter the view and show only those upcoming assignments.
Expiring Soon	Highlights units whose assignments are nearing expiration (within 7 days). Click this widget to filter the view and show only expiring units.
Search	Allows searching for units or residents by entering the unit number or resident name.
Assign Unit	Assign a unit to a resident. Includes the option **Bulk Assign Residents** to assign multiple residents simultaneously.

Assigning units in the Wi-Fi Manager App

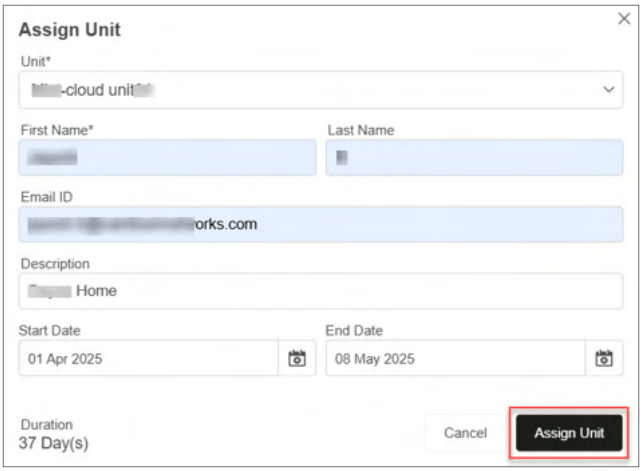
The **Assign Unit** option in the Wi-Fi Manager Appp allows property managers / front desk staff / Wi-Fi support staff to allocate specific units to residents. This feature simplifies resident management and facilitates communication between managers and residents.

To assign a unit, complete the following steps:

1. In the Wi-Fi Manager / Wi-Fi Front Desk / Wi-Fi Support app, click **Assign Unit**.



The **Assign Unit** window appears.



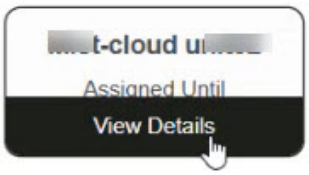
Note

- Minimum duration is one day.
- In the Wi-Fi Support app for Senior Living Managed Wi-Fi residents, the End Date is not populated and by default, the duration is set to never expire.

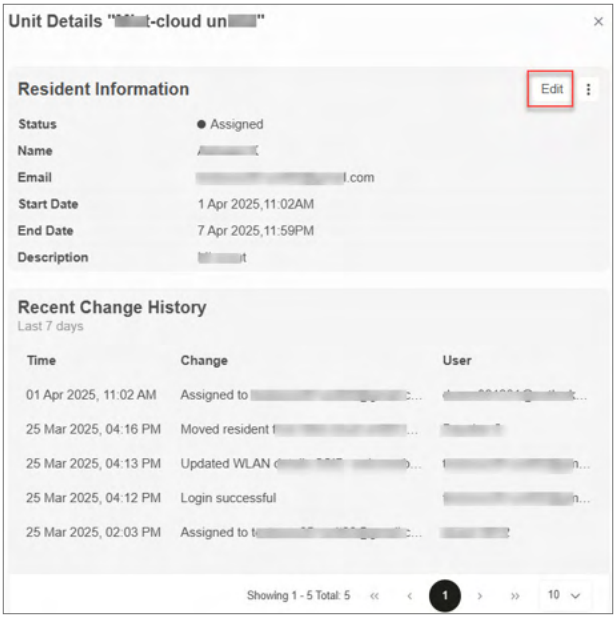
2. Review the **Duration** displayed in days.
3. Click **Assign Unit** to finalize the assignment.

4. A confirmation message is displayed.
5. After assigning a unit, hover over the assigned unit.

   The **View Details** option appears.



6. Click **View Details** to view the resident's information and recent change history.
   - For property managers (MDU Managed Wi-Fi—Wi-Fi Manager App):



The Wi-Fi Front Desk App and Wi-Fi Support App display an additional **Wi-Fi Details** section. This section displays the Wi-Fi details assigned to the residents, along with the QR code.

Note

- The front desk and support staff can download these details in a PDF file by clicking the download (⬇) icon.

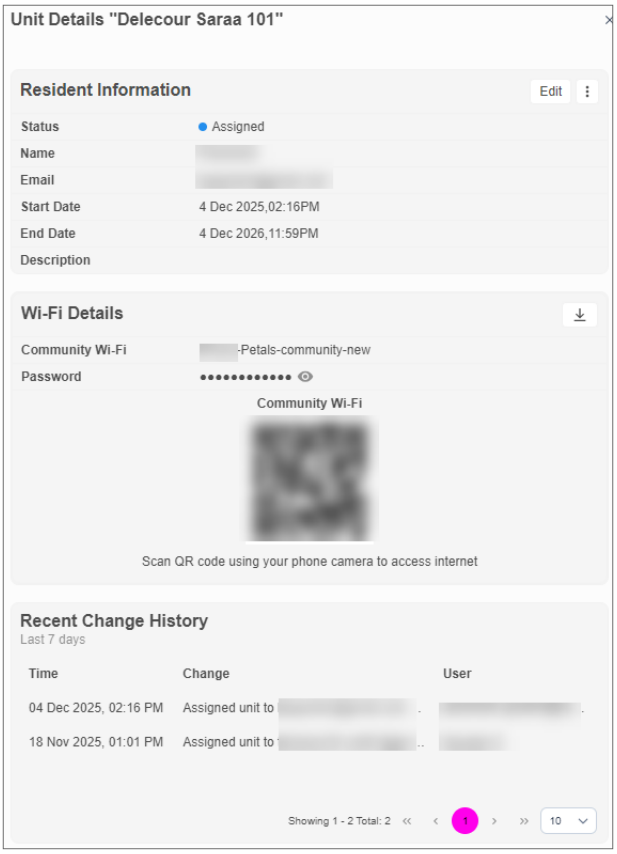


The support information that appears in the PDF is the same configuration that the MSPs make in the **Resident Support & Wi-Fi**

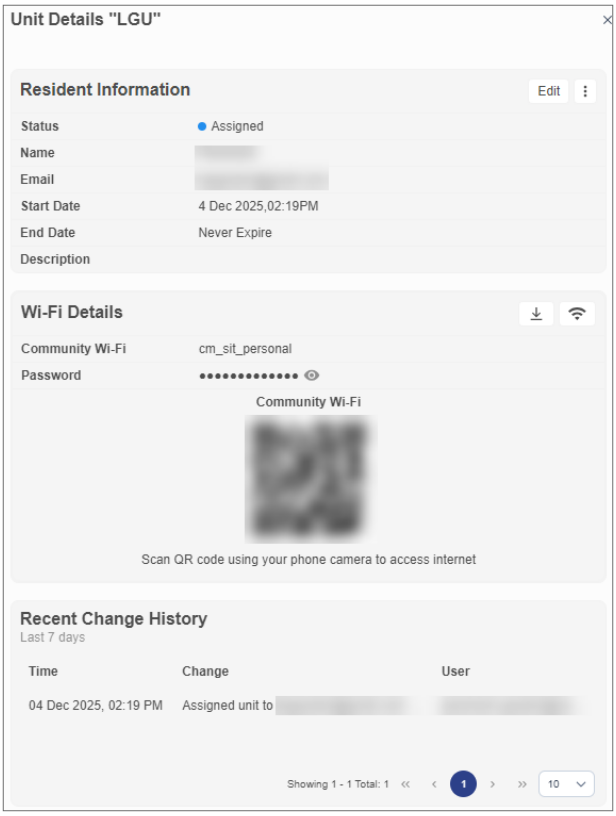
Help section in the **Design** tab of the cnMaestro MarketApps app.

- In addition to this, if the **Allow Wi-Fi Support Staff to update resident's Wi-Fi Settings** is enabled in the Senior Living Managed Wi-Fi App, then the support staff can modify the Wi-Fi password by clicking the update Wi-Fi settings ( ) icon.

- For front desk staff (Outdoor Hospitality—Wi-Fi Front Desk App):



- For Wi-Fi support staff (Senior Living—Wi-Fi Support App):

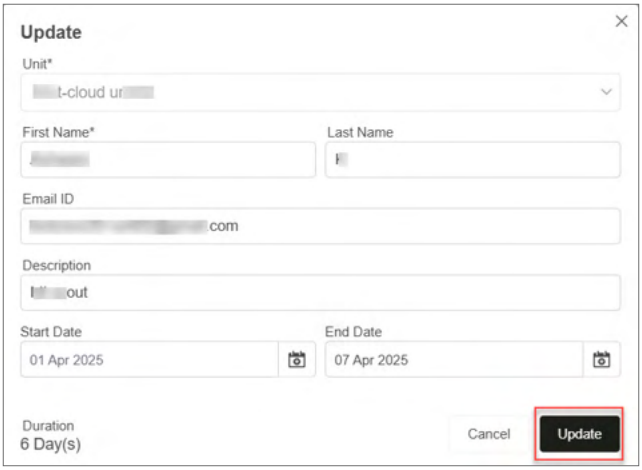


The view includes key details for the selected unit—such as unit name, status, email, start date, end date, and description.

It also shows the audit logs of all actions performed in the last 7 days, including email updates, resident logins, suspensions, and terminations, along with the time and user who performed each action.

7. Click the **Edit** button on the top right corner of the Unit Details window.

   The **Update** window is displayed.



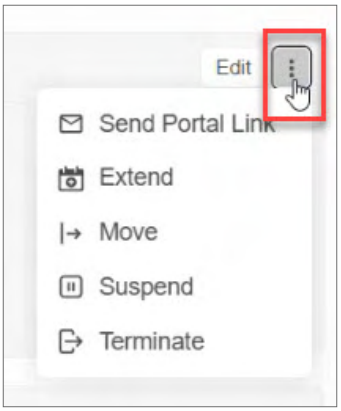
   The property managers / front desk staff / Wi-Fi support staff can modify the resident's information such as name, email, start and end dates, and description associated with the unit

8. To update the unit details, click **Update**.
9. Click the actions (⋮) icon to view more options.

   The following actions are available in this menu:

- Sending the portal link to residents
- Extending the duration of an assigned unit
- Moving residents to other units
- Suspending internet access of resident temporarily
- Terminating internet access and releasing units

This menu allows you to perform the actions such as sending the portal link, extending the assignment period, moving the resident to another unit, suspending access, or terminating the assignment.



Sending the portal link to residents

The **Send Portal Link** option allows property managers to send a one-time login link to the resident via email. The resident can use the link to access the Wi-Fi configuration portal and complete their setup or make necessary changes.

After the action is completed, a confirmation message appears stating: **Send Portal Link – action completed successfully** as shown in the figure below.



Extending the duration of an assigned unit

The **Extend** option allows property managers to update the end date of a unit's assignment.

When selected, a window appears with the current end date. Update it to the desired date using the calendar icon, then select **Extend** to apply the changes.



Moving residents to other units

The **Move** option allows property managers to reassign a resident to another unit. When selected, a window titled **Move Resident to other unit** appears.



To move a unit, complete the following steps:

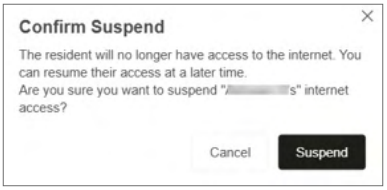
a. Select the new unit from the **Unit** field.

b. Enter a Description (optional).

c. Select **Move** to complete the reassignment.

Suspending internet access of resident temporarily

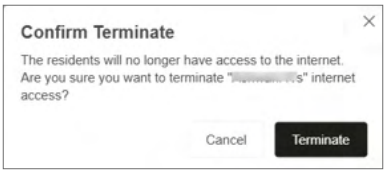
The **Suspend** option temporarily disables internet access for a unit. When selected, a confirmation window appears.



Select **Suspend** to pause the resident's internet service. The system sends an email update to the resident when you suspend the service.

Terminating internet access and releasing units

The **Terminate** option permanently ends the resident's assignment and releases the unit for reassignment. When selected, a confirmation window appears.



Click **Terminate** to remove the resident's access and complete the process. The system sends an email update to the resident when you terminate the service.

Assigning residents in bulk

The **Bulk Assign Residents** option enables property managers / front desk staff / Wi-Fi support staff to efficiently assign multiple units to residents at once by uploading a CSV or Excel file containing resident data.

To bulk assign units, complete the following steps:

1. Click the Bulk Assign Residents ( ) icon next to the **Assign Unit** button.



   The **Bulk Assign Residents** window appears.

2. To select and upload the CSV or Excel file, click **Browse File**.



3. Click **Download Sample** to download a sample file format for reference.
4. When uploading, ensure that the Unit is entered as specified below:

Unit	First Name	Last Name	Email	Start Date	End Date
Unit name	Resident first name	Resident last name	Resident email id	Internet access start date in format (MMM DD YYYY)	Internet access end date in format (MMM DD YYYY)
MDU 01	John Doe	A	johndl@yopmail.com	Dec 20 2024	Jan 21 2025
MDU 02	John Doe	B	johndll@yopmail.com	Dec 21 2024	Jan 30 2025

5. Click on **Validate** to finalize the bulk assignment.

Settings

The Settings option allows you to configure system preferences within the Property Manager App. To access the Settings, complete the following steps:

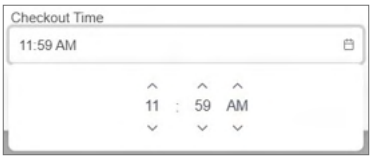
1. Click the settings (or) icon present in the top right corner of the menu bar.

   The Settings window is displayed.



2. Configure the following parameters:
   - **System Time Zone**—Displays the property's time zone along with the current date and time.

     This field is read-only and cannot be modified.
   - **Checkout Time**—Displays the default checkout time for residents. Use the time picker to select the hour, minutes, and AM/PM. The time is displayed in a 12-hour format.

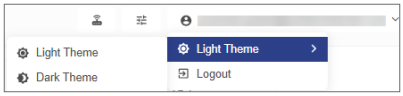


- Click **Save** to confirm your changes.

Theme settings

To configure the app theme, from the user dropdown, point to **<Current-theme> Theme** and select from the following options:

- Light Theme
- Dark Theme



Help

The Help option allows you to access user documentation or support content configured in the Design tab. This feature helps property managers and operators quickly find guidance related to the portal.

To access Help, follow the steps below:

1. Click the **Help** ( ) icon in the top right corner of the app, next to the email ID.



2. The documentation or support page linked in the Help and Support URL field of the Design tab is displayed.

AP Health

The AP Health feature in MarketApps provides real-time visibility into the operational status of APs associated with each property.

When property managers / front desk staff / Wi-Fi support staff import APs using a CSV file, the system begins tracking their health automatically. The AP Health section displays the number of APs that are online, offline, and the total number of clients connected across all APs.

If any AP that was previously online in cnMaestro goes offline, the AP Health data reflects this change in real-time. These updates are also visible in the Property Manager Portal, ensuring that managers always have access to the latest device status.

To view the most recent data, click the Refresh button. This updates the AP Health Stats, including AP status and client count.

Figure 642 *AP Health interface - For property managers (MDU Managed—Wi-Fi Manager App)*

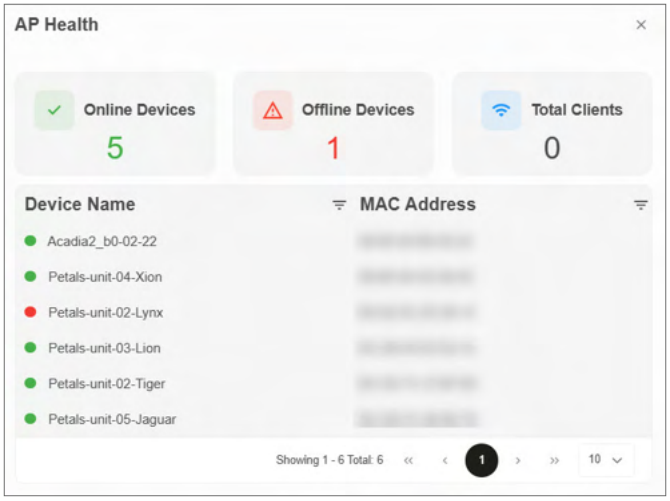


Figure 643 *AP Health interface - For front desk and support staff*

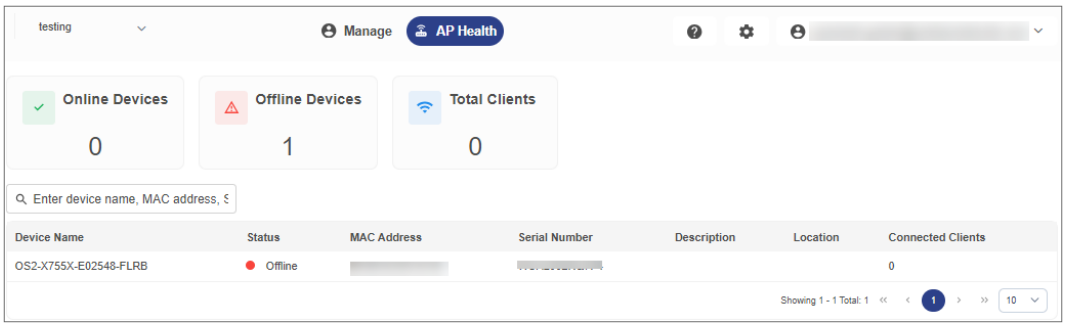
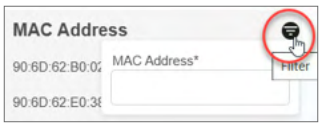


Table 169 *AP Health parameters and descriptions*

Element	Description
Online Devices	Shows the number of APs currently active and connected.
Offline Devices	Shows the number of APs that are currently offline or unreachable.
Total Clients	Displays the total number of client devices connected across all online APs.
Device Name	Lists the names of APs as configured during CSV import. • Green indicator next to the name—Indicates that the AP is online • Red indicator next to the name—Indicates that the AP is offline Filter option is available for a quick search of the devices, as shown in the figure below. 
MAC Address	Shows the unique hardware (MAC) address for each AP. Filter option is available for a quick search of the MAC addresses, as shown in the figure below. 

Element	Description
Senior Living and Outdoor Hospitality-specific parameters	
Status	Displays whether the device is online or offline.
Serial Number	Displays the serial number of the device.
Description	Displays the description of the device, if available.
Location	Displays the location of the device.
Connected Clients	Displays the count of clients that are connected to this device.

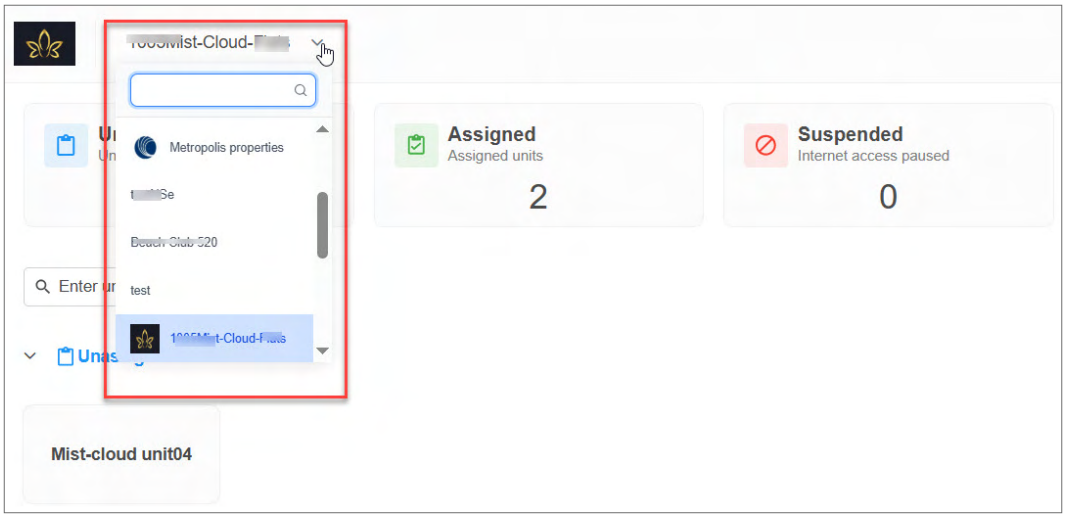
MarketApps app selector

The MarketApps app selector dropdown allows property managers / front desk staff / Wi-Fi support staff to easily switch between multiple MarketApps apps that are associated with the same admin email or manager profile.

When a property manager account is linked to more than one MarketApps app, all the corresponding apps appear in this dropdown. Selecting an app from the list updates the page to display data specific to that MarketApps app, such as units, settings, and assignments, without logging out or switching between sessions.

By default, when the user logs in, data related to the most recently accessed MarketApps app is displayed. Switching between MarketApps apps instantly refreshes the interface to reflect the selected property's details, including resident data, AP status, and other configurations.

Figure 644 *MarketApps app selector*



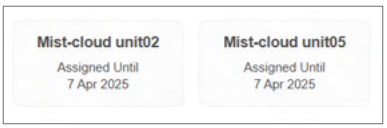
View options in the Property Manager App

In the Property Manager App, there are two different view options to manage units efficiently. These view options can be accessed using icons located at the top right corner of the Property Manager App interface as shown in Figure 645.

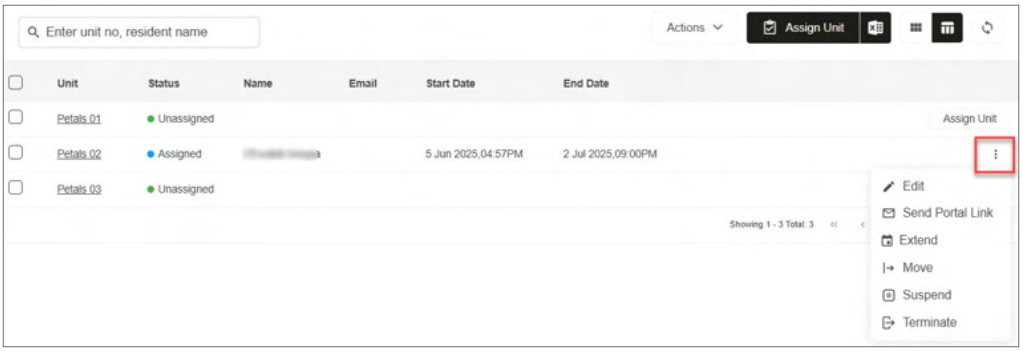
Figure 645 *View options in the Property Manager App*



1. **Thumbnail View** ( )—This view displays units as thumbnails or small images, providing a visual representation of each unit, as shown in the figure below.

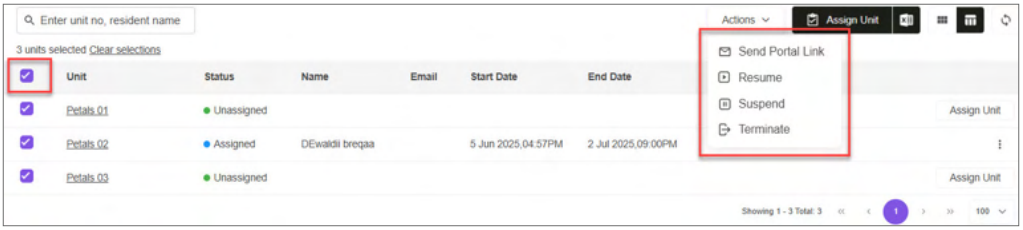


2. **Table View** ( )—Table view presents units in a structured table format with columns for Unit, Status, Name, Email, Start Date, and End Date, allowing for detailed management and organization of unit information, as shown in the figure below.



At the end of each row, a three-dot menu provides quick access to actions such as Edit, Send Portal Link, Extend, Move, Suspend, and Terminate.

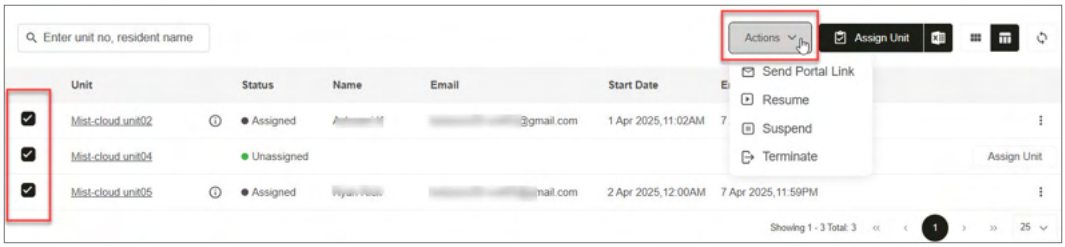
A bulk selection option is available in the Unit column, allowing property managers to select multiple units across pages or select all units with single click. After selecting the units, they can perform bulk actions such as Suspend, Move, and Extend using the **Actions** drop-down. The selection remains active even when navigating between pages, enabling efficient bulk operations.



Actions dropdown

When the Table view is active, an additional **Actions** dropdown appears for performing bulk actions. You can select multiple units using the checkboxes located to the left of each Unit name as shown in Figure 646. Once selected, the **Actions** dropdown displays bulk operation options such as **Send Portal Link**, **Resume**, **Suspend**, and **Terminate**. This dropdown streamlines the process of managing multiple units at once, while individual changes can still be made using the three-dot menu in each row.

Figure 646 *Action tab*



Refresh button

If the portal is open in multiple browser tabs or windows, changes made in one session may not immediately reflect in the others. Click the refresh ( ) icon to update the view with the latest information.

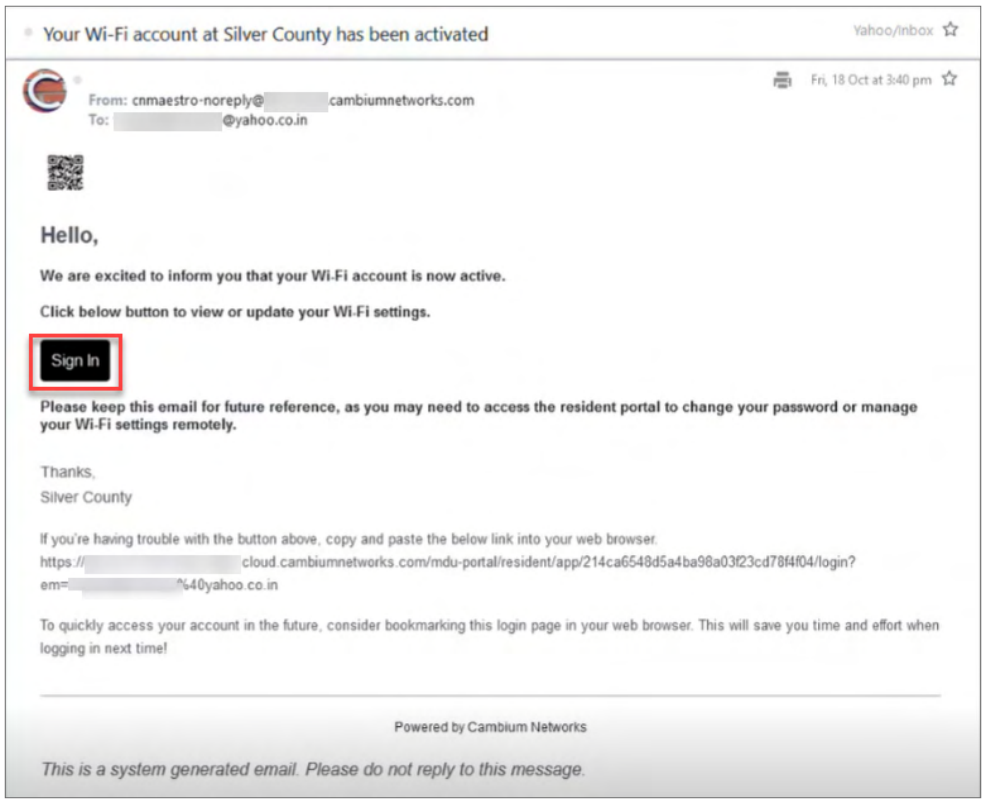
In the AP Health section, the refresh icon also updates the AP status data, ensuring that the displayed online/offline status and client count are current.

Figure 647 *Refresh option*

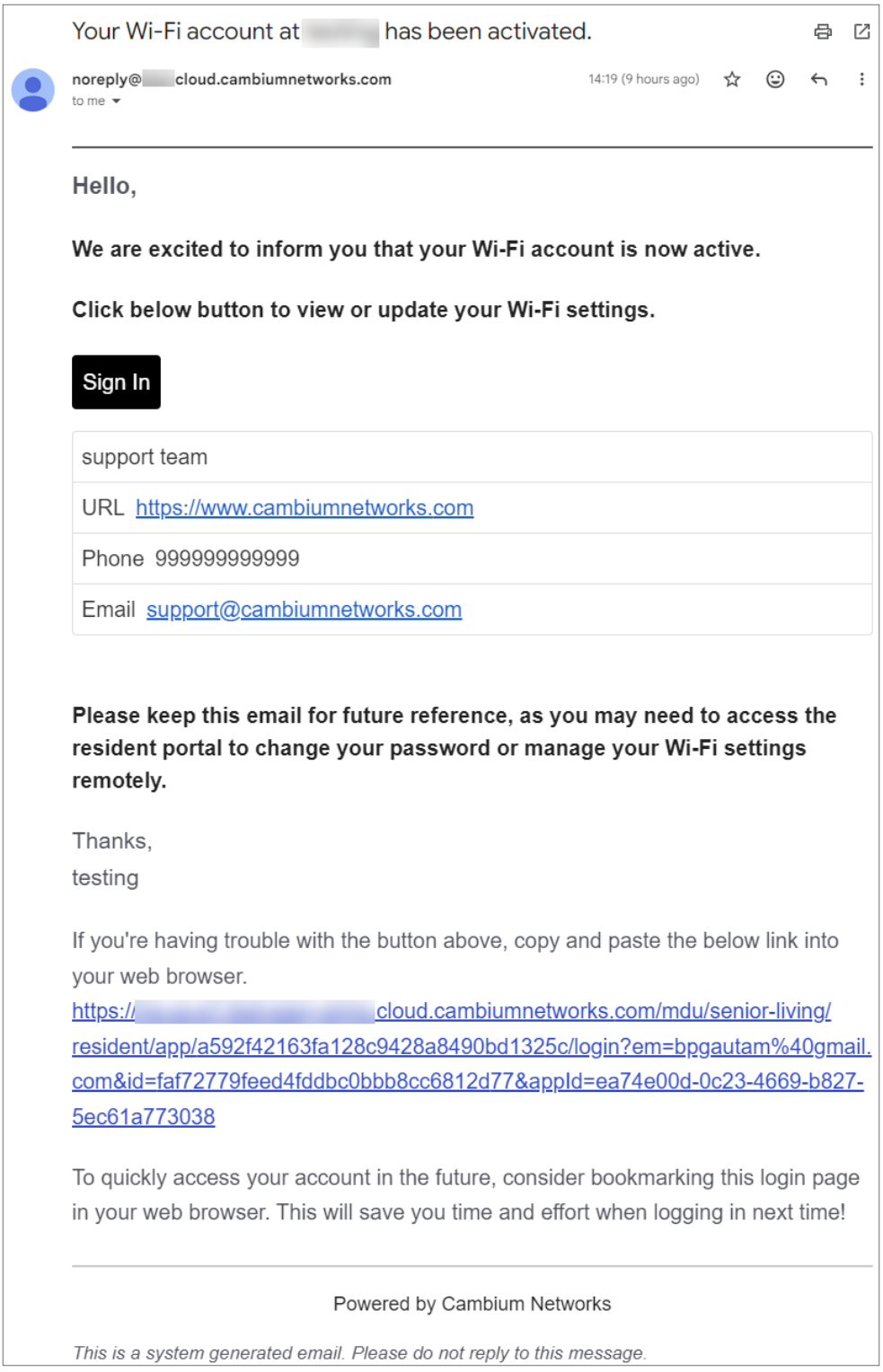


View options in the Resident App

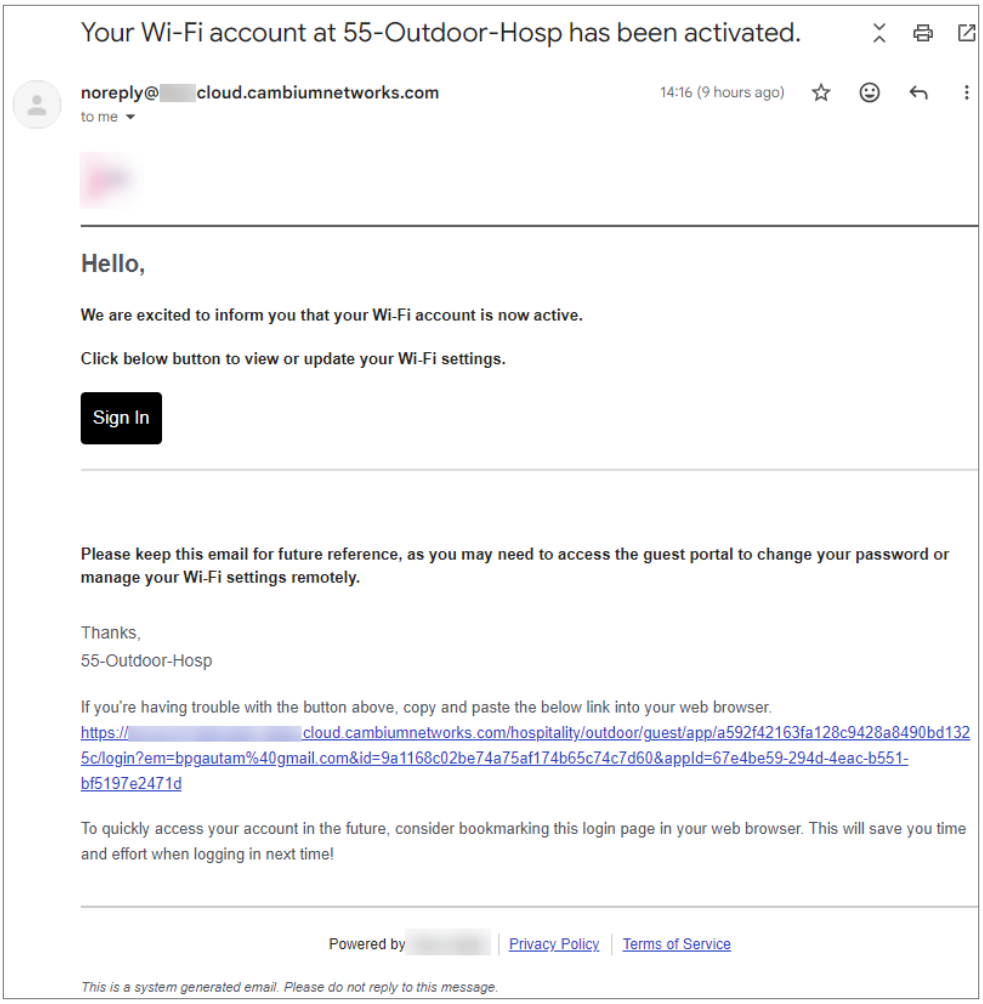
1. Once the property managers / front desk staff / Wi-Fi support staff assigns the unit, residents receive an account activation email.
   - For residents of the MDU managed property, an email with the title **Your Wi-Fi account at** <property-name> **has been activated**. Click **Sign In**.



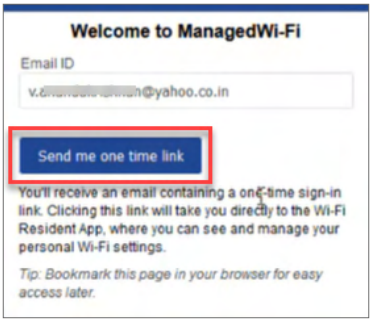
   - For residents of the senior living managed property, an email with the title **Your Wi-Fi account at** <property-name> **has been activated**. Click **Sign In**.



- For residents of the outdoor hospitality managed property, an email with the title **Your Wi-Fi account at** <property-name> **has been activated**. Click **Sign In**.

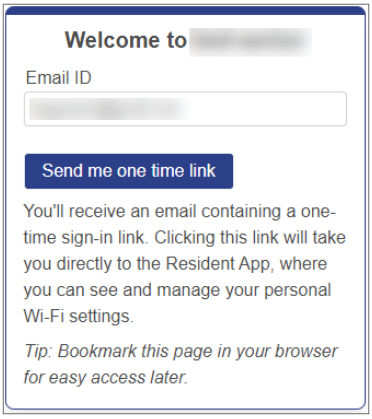


2. Click **Send me one time link**.
   - For property managers (MDU Managed—Wi-Fi Manager App):

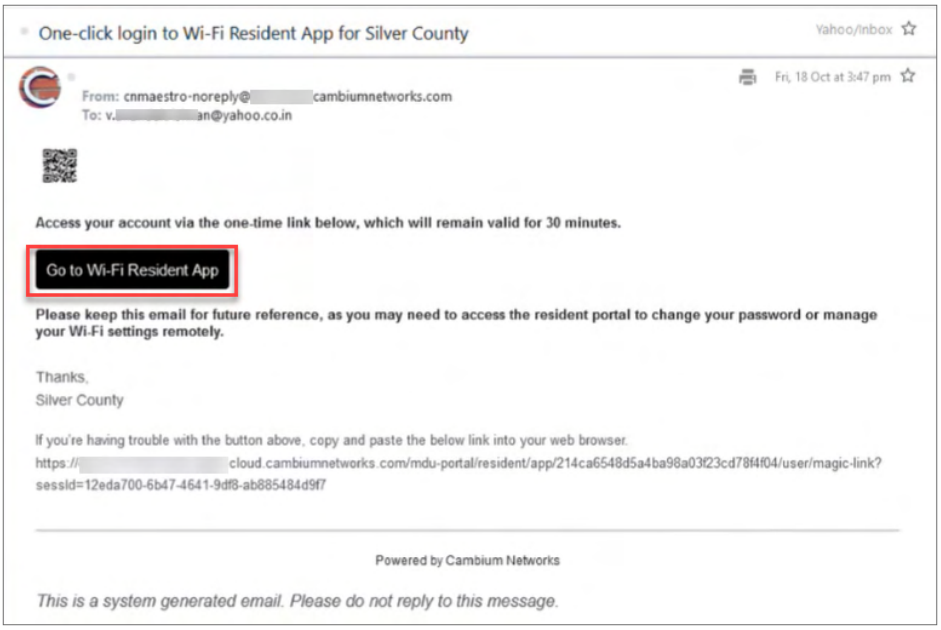


   - For front desk staff (Outdoor Hospitality—Wi-Fi Front Desk App) and Wi-Fi support staff (Senior Living—Wi-

Fi Support App):



3. The resident receives an email containing a one time link for logging into the Resident App.
   - For residents of the MDU managed property:
     a. Click **Go to Wi-Fi Resident App**.



     b. The **Welcome to** <property-name> page is displayed. Below the QR code, two options are displayed: **Community Wi-Fi** and **Personal Wi-Fi**. You can scan to connect to either network and use the arrow to switch between them.



c. Click **Change**.

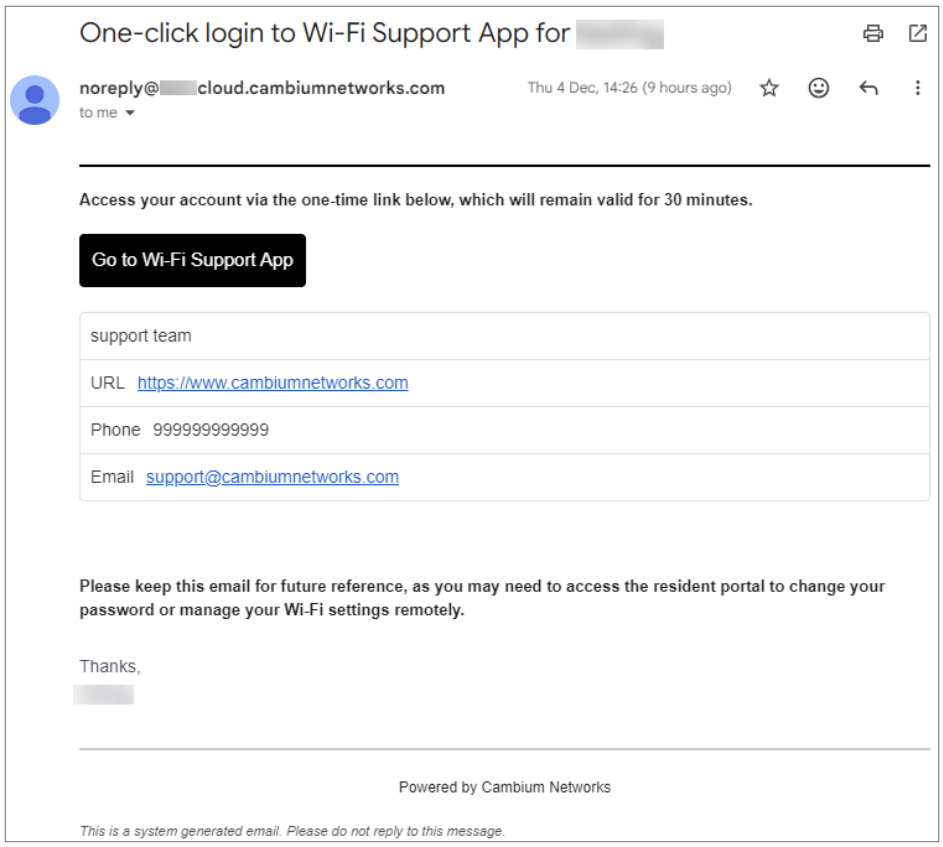
The **Change Wi-Fi Settings** window is displayed.

Modify your Personal Wi-Fi Network Name and Wi-Fi password in the respective fields, and click **Update** to save the changes.



- For residents of the senior living managed property:

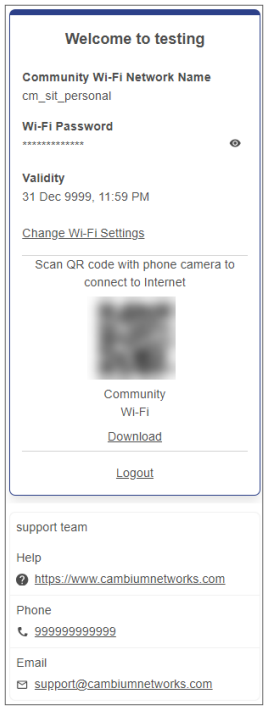
a. Click **Go to Wi-Fi Support App**.



b. The **Welcome to** <property-name> page is displayed.

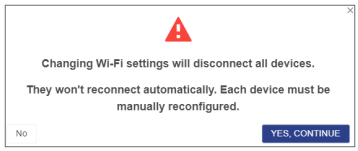
The **Community Wi-Fi** details are displayed along with a QR code that you can scan with your mobile phone to connect to the internet.

Click **Download** to download the PDF with the Wi-Fi details.



c. To modify the Wi-Fi password, click **Change Wi-Fi Settings**.

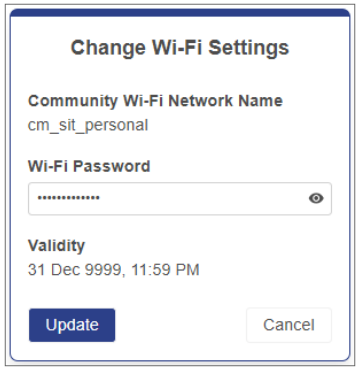
The following warning message is displayed.



d. Click **Yes, Continue**, if you want to change the password.

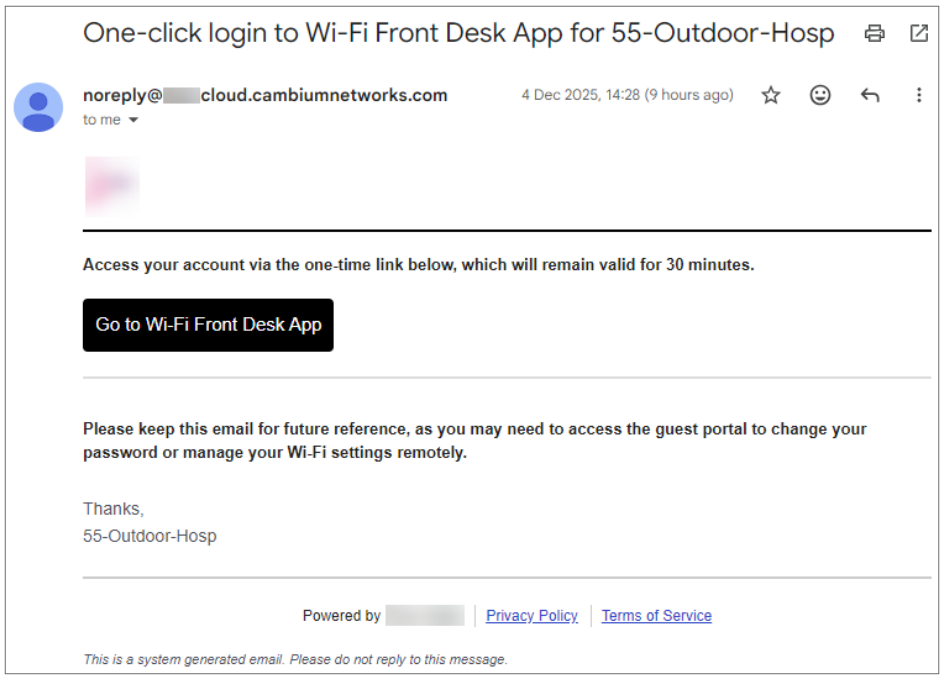
The **Change Wi-Fi Settings** window is displayed.

Modify your Wi-Fi password and click **Update** to save the changes.



- For residents of the outdoor hospitality managed property:

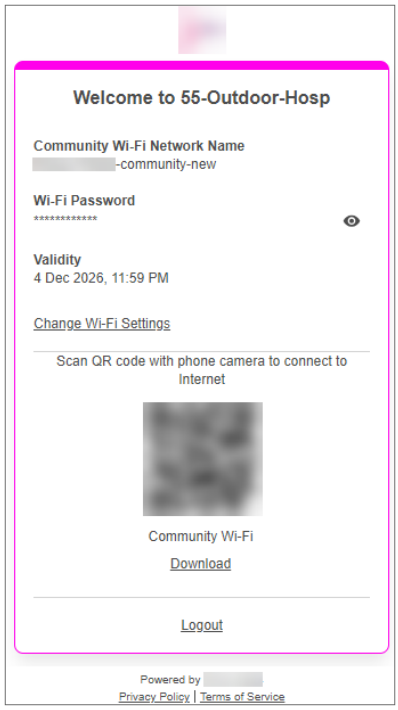
a. Click **Go to Wi-Fi Front Desk App**.



b. The **Welcome to** <property-name> page is displayed.

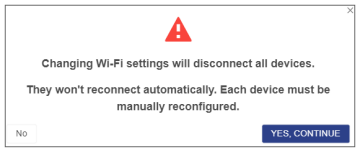
The **Community Wi-Fi** details are displayed along with a QR code that you can scan with your mobile phone to connect to the internet.

Click **Download** to download the PDF with the Wi-Fi details.



c. To modify the Wi-Fi password, click **Change Wi-Fi Settings**.

The following warning message is displayed.



d. Click **Yes, Continue**, if you want to change the password.

The **Change Wi-Fi Settings** window is displayed.

Modify your Wi-Fi password and click **Update** to save the changes.



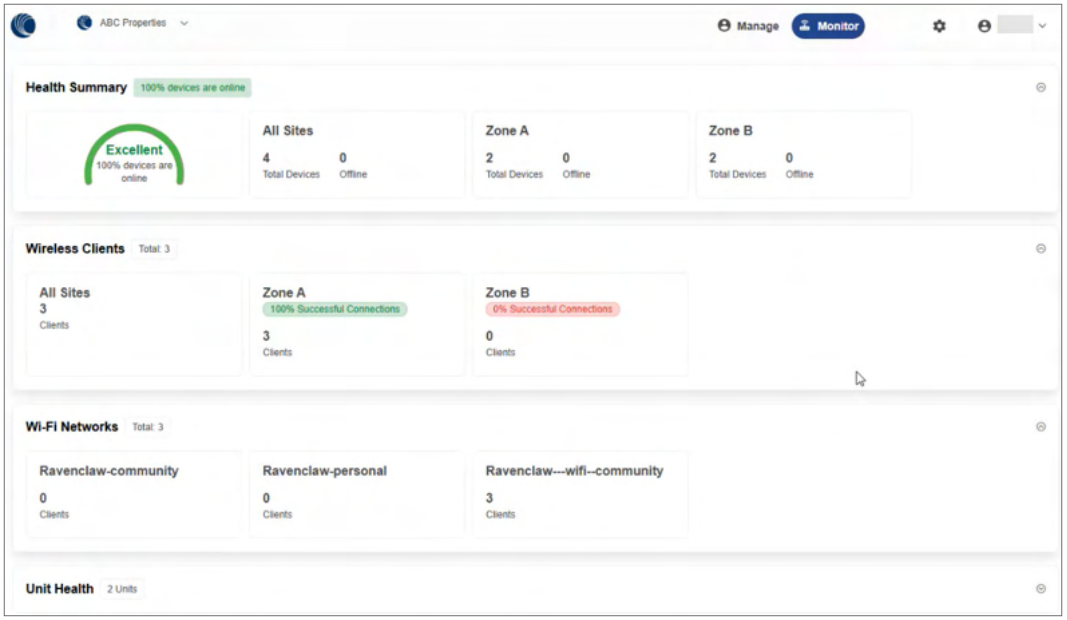
Monitoring Sites in the Wi-Fi Manager / Wi-Fi Support / Wi-Fi Front Desk Apps

Note

To view the **Monitor** section in the Wi-Fi Manager App, you must first enable the **Monitoring** option under **MarketApps** > **MDU Managed Wi-Fi** > **Settings** > **Site Monitoring** tab. You must then add the required sites that you want to allow property managers to monitor.

For more information, see Site Monitoring.

The Monitor page in the Wi-Fi Manager App displays information about the sites that you have added, the number of devices in each sites and the count of offline devices. It also displays details about the Wi-Fi networks that are configured for the site and the number of wireless clients that have connected to them.

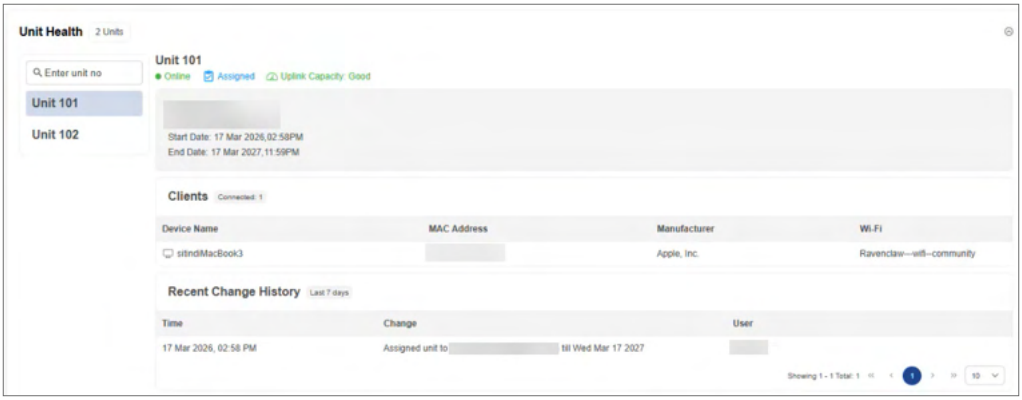


The page displays the following details:

- **Health Summary**—Displays the count of devices in each site and the total number of devices that are mapped to all sites. It also displays the number of offline devices.
- **Wireless Clients**—Displays the number of wireless clients that have connected to the devices in the sites. It also displays the percentage of successful connections.
- **Wi-Fi Networks**—Displays the number of clients connected to the WLANs that are enabled in the sites.
- **Unit Health**—Displays details about the units in the sites, such as the status of the AP (Online, Offline), whether the AP is Assigned or Unassigned to the unit, and the status of the AP's uplink capacity. It also displays the details of the clients connected, such device name, MAC address, manufacturer name, and the WLAN it is connected to. Its also displays any changes made to this unit in the last seven days.

  The Upload Capacity is displayed as follows:

  - **Poor**—Ethernet uplink speed is <100 Mbps
  - **Fair**—Ethernet uplink speed is 100 Mbps
  - **Good**—Ethernet uplink speed is 1000 Mbps
  - **Excellent**—Ethernet uplink speed is >1000 Mbps



Installer app

The Installer App supports ISPs and MSPs during on-site device installation. It streamlines the setup process by allowing installers to log in, record installation details (like placement, photos, and height), and automatically provision the device to the correct site with the required configuration. This removes manual coordination between field staff and backend teams, ensuring faster and more accurate onboarding.

Installers receive invitations via email, which they can use to access the app. Once logged in, installers select the site, attach the necessary AP or Switch Group, and complete the provisioning with minimal effort.

The following devices are supported on the MarketApps Installer app:

- Enterprise Installer
  - Enterprise Wi-Fi APs
  - cnMatrix switches
- 60 GHz cnWave Installer
  - 60 GHz cnWave devices

This section contains the following topics:

- Basic tab
- Settings tab
  - Enterprise Installer
  - 60 GHz cnWave Installer
- Design tab
- Nodes tab
- Accessing the Installer App interface
  - Additional options on the summary page
  - Viewing installed devices and switching between apps
  - Locating installed devices in cnMaestro
  - Replacing devices in the Installer app
    - Points to remember and prerequisites for replacing devices
- Exporting Installation Summary information

Basic tab

The configuration steps for the Basic tab are the same as those detailed earlier in the documentation. For information on setting the app name, managed account, and description, refer to the Basic tab configuration steps.

Settings tab

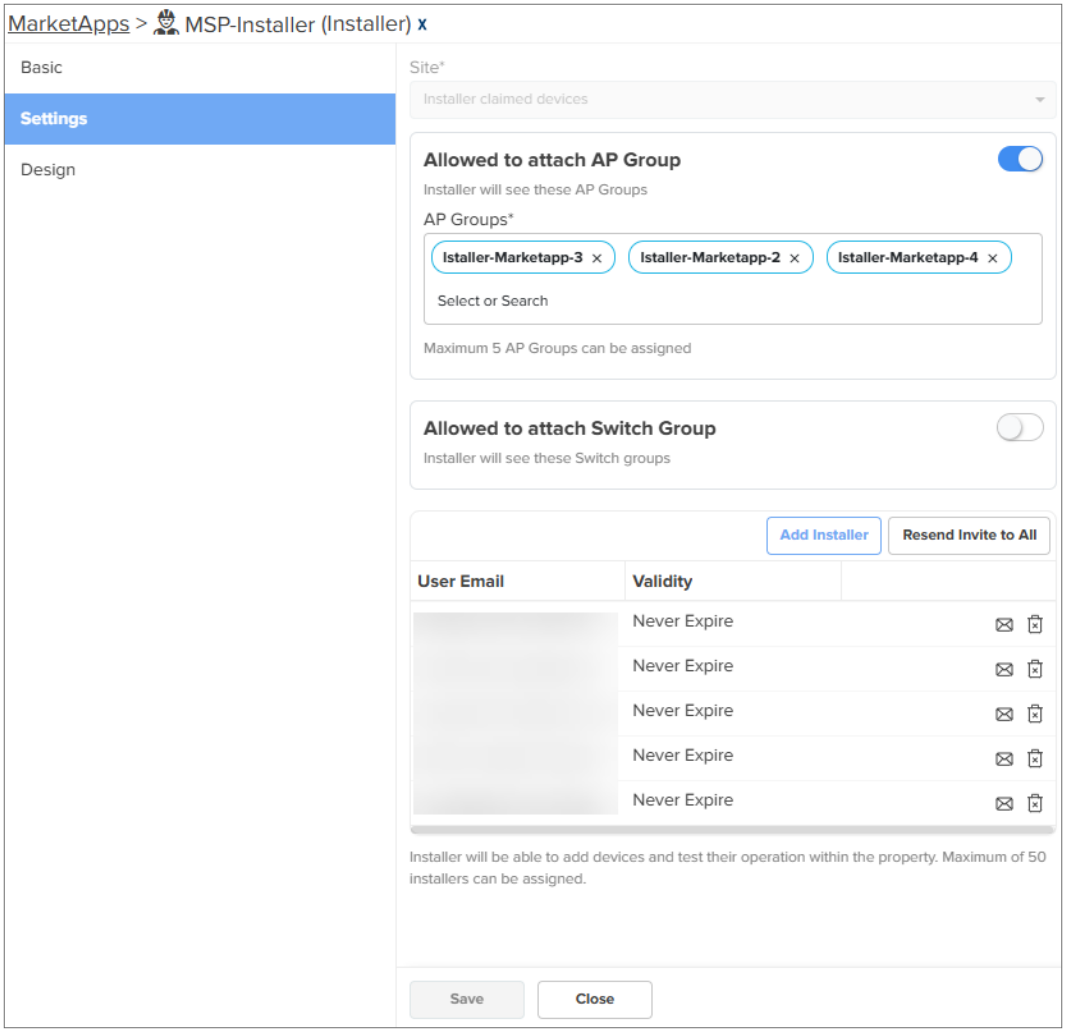
This section contains the following topics:

- Enterprise Installer
- 60 GHz cnWave Installer

Enterprise Installer

The Settings tab in the Enterprise Installer App allows you to configure installation-specific settings for enterprise devices. You can enable options to attach AP Groups or Switch Groups during installation, based on the device type and location. These settings help ensure the correct configuration is applied when provisioning devices in the field.

Figure 648 *Settings tab—Enterprise Installer*



To configure settings options in the Installer app, complete the following steps:

1. Map one site to the app where all devices get onboarded.

   The **Site** field lists all sites available for selection in the Installer App for the specified Managed Account.

   This field is read-only and can be configured only once.

2. Use the **Allow to Attach AP Group** option to let installers select an AP Group during installation.

   This option is disabled by default. When enabled, a searchable dropdown labeled **Select or Search** appears, allowing the MSP to choose from the available AP Groups based on location, device type, or customer category.

   Note

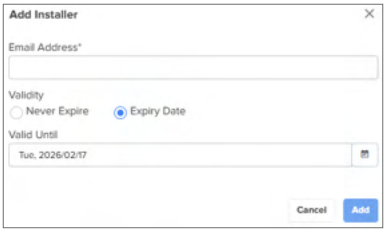
   - If **Allow to Attach AP Group** is disabled, no base configuration is applied to the AP during installation.
   - If multiple groups are configured, a dropdown appears for the installer to select the appropriate group.

3. Use the **Allow to Attach Switch Group** option to let installers select a Switch Group when provisioning switches.

This option is also disabled by default. When enabled, a **Select or Search** dropdown appears, where the installer can choose the appropriate Switch Group to apply the correct base configuration.

4. Configure one or more AP or Switch Groups that the installer can select during the installation process.
5. To invite users, click **Add Installer**.

   The Add Installer window is displayed.



Note

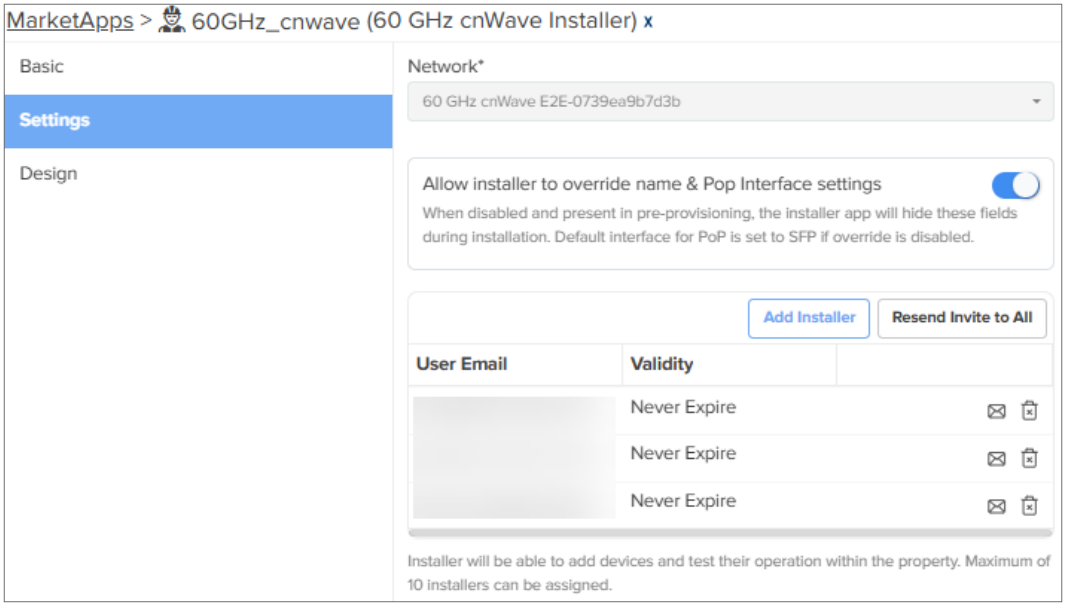
A maximum of 50 installers can be assigned.

6. Configure the installer's email address and the expiry date, if required.
7. You can add multiple installers by entering one email ID at a time. You can add up to 10 unique email IDs.
8. Click **Save**.

60 GHz cnWave Installer

The Settings tab in the 60 GHz cnWave Installer App allows you to configure installation-specific settings for 60 GHz cnWave devices. You can configure the network and enable options to allow installer override the name and Pop interface settings. These settings help ensure the correct configuration is applied when provisioning devices in the field.

Figure 649 *Settings tab—60 GHz cnWave Installer*



To configure settings options in the 60 GHz cnWave Installer app, complete the following steps:

1. Map one network to the app where all devices get onboarded.

   The **Network** field lists all sites available for selection in the 60 GHz cnWave Installer App for the specified Managed Account.

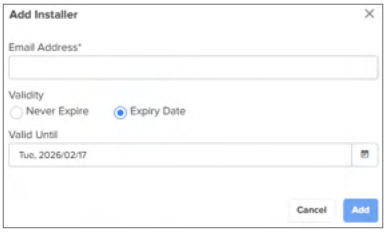
   This field is read-only and can be configured only once.

2. Use the **Allow installer to override name & Pop Interface settings** option to let installers override the name and Pop interface settings.

   This option is disabled by default.

3. To invite users, click **Add Installer**.

   The Add Installer window is displayed.





Note

A maximum of 10 installers can be assigned.

4. Configure the installer's email address and the expiry date, if required.
5. You can add multiple installers by entering one email ID at a time. You can add up to 10 unique email IDs.
6. Click **Save**.

Additionally you can also configure node settings by uploading a CSV file on the **Nodes** tab. For information, see Nodes tab.

Design tab

The Design tab is similar to both Enterprise and 60 GHz cnWave installers. It lets you brand the Installer App interface and customize the fields shown during device setup. It works similarly to the Design tab in the Managed Wi-Fi app.

Figure 650 *Design tab parameters*

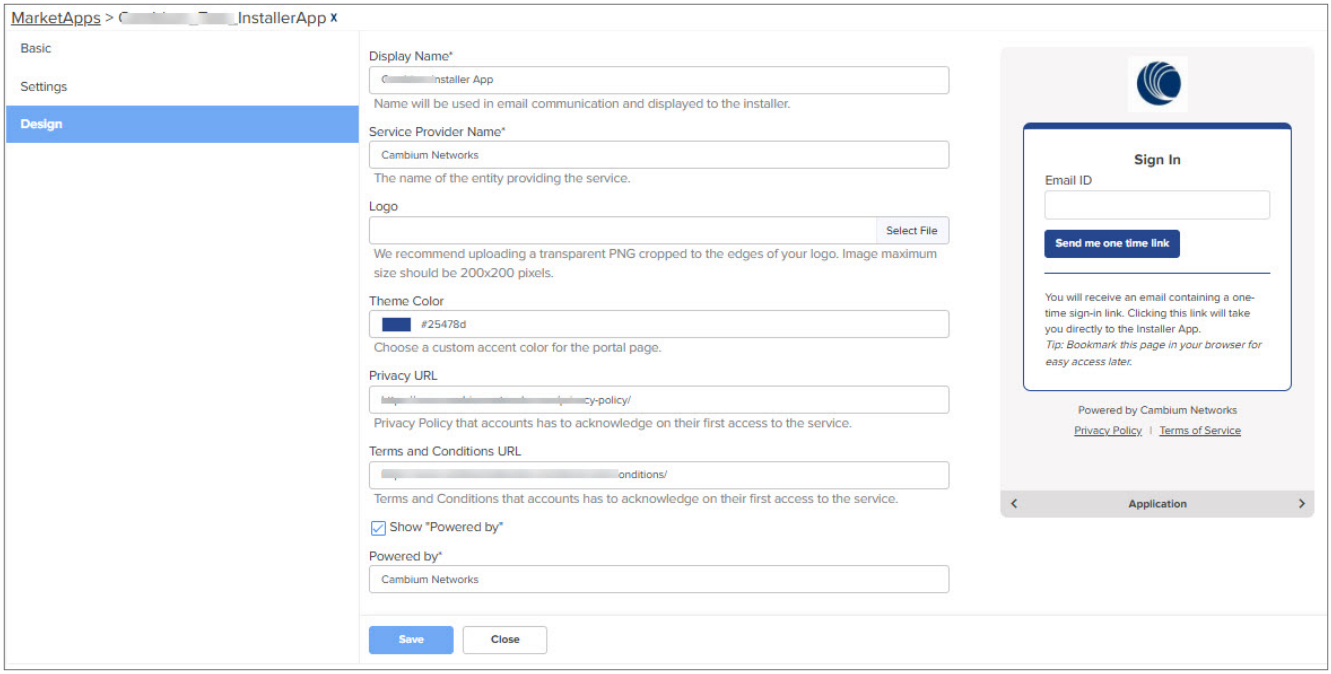


Table 170 *Installer design tab parameters*

Parameter	Description
Display Name*	Specifies the name shown for the MarketApps app in the Installer App interface.
Service Provider Name*	Specifies the name of the service provider or property. This name appears only in the invitation email sent to the installer and does not appear in the Installer App interface.
Logo	Upload a logo file (PNG recommended) cropped to the edges and sized up to 200x200 pixels.
Theme Color	Customize the portal's color scheme with a chosen accent color.
Privacy URL	Provide the URL to your Privacy Policy that users must acknowledge on first access.
Terms and Conditions URL	Provide the URL to your Terms and Conditions that users must acknowledge.
Show "Powered by"	Enable this option to display the Powered by message.
Sample screen	The sample screen section includes two views: 1. **Installer App**—Provides a view of the sign-in interface that installers use to access the Installer app. **Note** • Administrators creating this Installer App can view the Enterprise Installer App, by clicking the Installer App link. The Installer web App UI is displayed. 2. **Installer invitation email**—Provides a view of the email format that installers receive, which contains a link to access the Installer app.
Save	Click **Save** to apply the changes after configuring the Design tab.

Nodes tab

Note

The Nodes tab is applicable only to the 60 GHz Installer.

The Nodes tab allows you to pre-provision nodes and configure the nodes types and sites before the installation is started. You must add the details in the CSV format and upload the file on this page. You can also replace any existing nodes configuration.

The following are the details you must include in the CSV format :

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1	Device Name	Model	Device Mode	PoP Node	Site	Latitude	Longitude	Accuracy	Azimuth	Antenna Tilt	Description	Polarity Sector 1	Polarity Sector 2	Channel Sector 1	Channel Sector 2	Antenna Dish Gain	IPv4 Address	Network Mask	Default Gateway
2	H2-1	V5000	DN	No	H2	39.90319	-75.17207	10	275	0		Odd	Odd	1	1				
3	A2	V5000	DN	No	A2	39.90404	-75.17283	10	275	0		Odd	Odd	1	3				
4																			

To pre-provision nodes, complete the following steps:

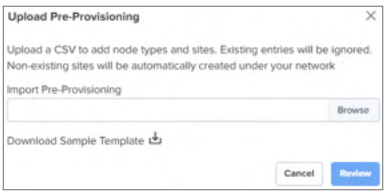
1. On the **Nodes** tab, click **Add Pre-Provisioning**.



   The Upload Pre-Provisioning window is displayed.

2. Click **Browse** and select the CSV file with the nodes information.

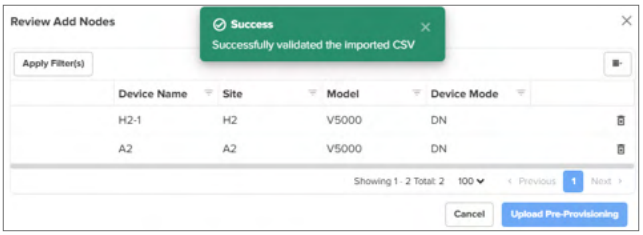
   You can also download a template file that is populated with sample entries by clicking **Download Sample Template**.



3. Click **Review**.

   cnMaestro starts reviewing the uploaded details and lists any conflicts or errors in the data.

   If no conflicts are present, then a success message is displayed.



4. Click **Upload Pre-Provisioning**.

   The table is populated with the details that you uploaded.

5. To replace the provisioned nodes, click **Replace Pre-Provisioning** and upload the CSV file.

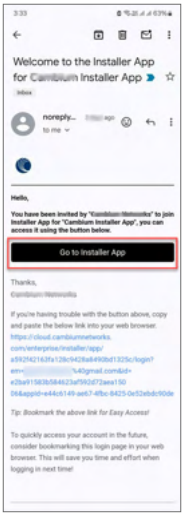
Accessing the Installer App interface

Note

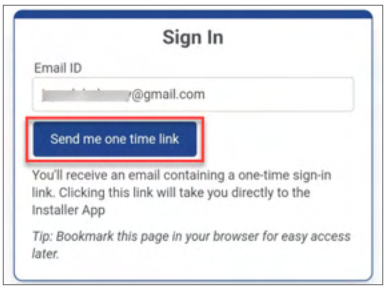
After the installer logs in to the Installer App interface, the user session is active for a duration of seven days.

After configuring the MarketApps Installer App and inviting installers, the following steps explain how an installer accesses the Installer App interface:

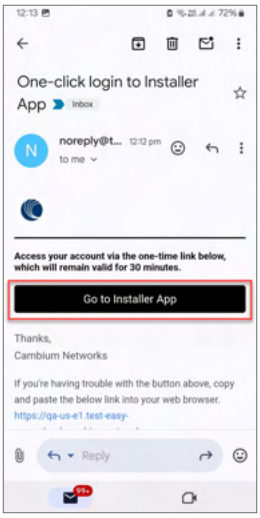
1. The installer receives a customized email titled **Welcome to the Installer App for <Display name>** as shown in the figure below.



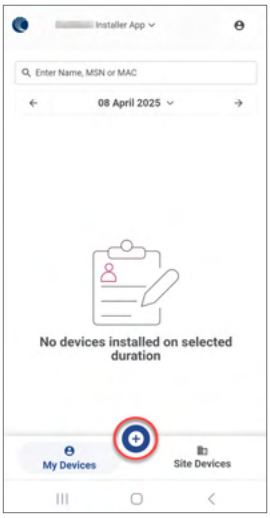
2. Installer clicks **Go to Installer App** in the email. The **Sign In** screen appears if not already logged in.



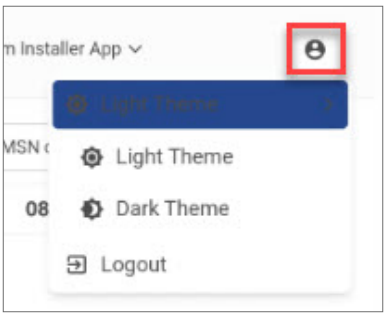
3. The installer enters their email ID and clicks **Send me one time link**.
4. The installer receives another email titled **One-Click Login to Installer App**. It includes a one-time login link that expires after 30 minutes.



5. Installer clicks **Go to Installer App** in the second email to access the app interface.
6. The app opens with a customized login screen that shows the configured display name, logo, and theme.

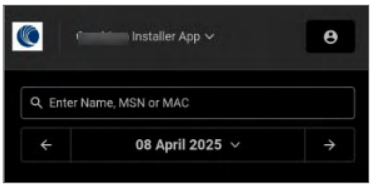


7. The app automatically displays any previous installations. The installer selects an existing entry to view its details if needed.
8. A search bar appears at the top, which allows the installer to search using a device name, MSN, or MAC address.
9. The current date appears below the search bar.
10. To change the theme or log out, the installer taps the profile icon in the top-right corner.



A menu appears with the following options:

- **Light Theme**: Displays the app in a bright, standard view.
- **Dark Theme**: Switches the app to a dark background for better visibility in low light.



- **Logout**: Logs the installer out of the app.

11. To start a new installation, the installer taps the + (plus) icon located between **My Devices** and the **Site Devices** as shown in the below figure.



12. A new window **Add Device** appears.



13. The installer enters the Serial Number (MSN) manually or taps **Scan MSN** to scan the QR code using the device camera, then click **Add** to proceed. The **Update Device** screen appears.

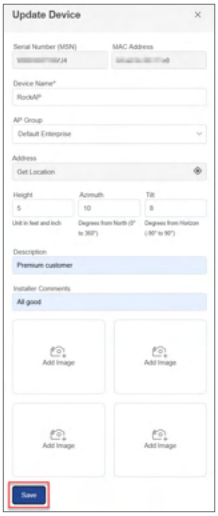


Table 171 *Update Device screen parameters*

Parameter	Description
Serial Number (MSN)	Displays the device's serial number. This field is pre-filled and not editable.
MAC Address	Displays the device's MAC address. This field is pre-filled and not editable.
Device Name	The installer enters a custom name for the device.
AP Group	The installer chooses the appropriate AP Group for the device during installation.

Parameter	Description
Location	The installer taps to update the current location.
Height	The installer enters the height in feet and inches.
Azimuth	The installer enters the azimuth angle in degrees (0° to 360°).
Tilt	The installer enters the tilt angle from horizontal (-90° to 90°).
Description	The installer adds relevant notes, such as customer details or site information.
Installer Comments	The installer enters any additional observations or remarks.
Add Images	The installer can upload up to four images related to the installation.

14. Installer taps **Save** to apply the changes and complete the device installation.
15. The app redirects to a new page displaying the Installation Summary for the installed device.

Figure 651 *Installation Summary—Mobile view*

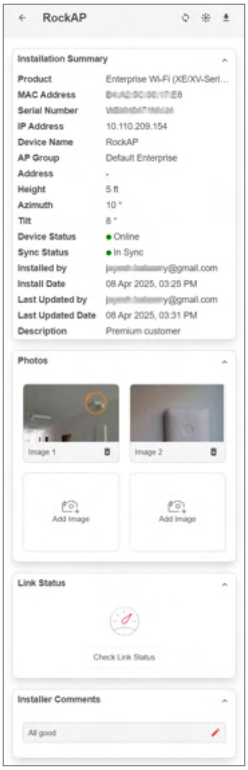
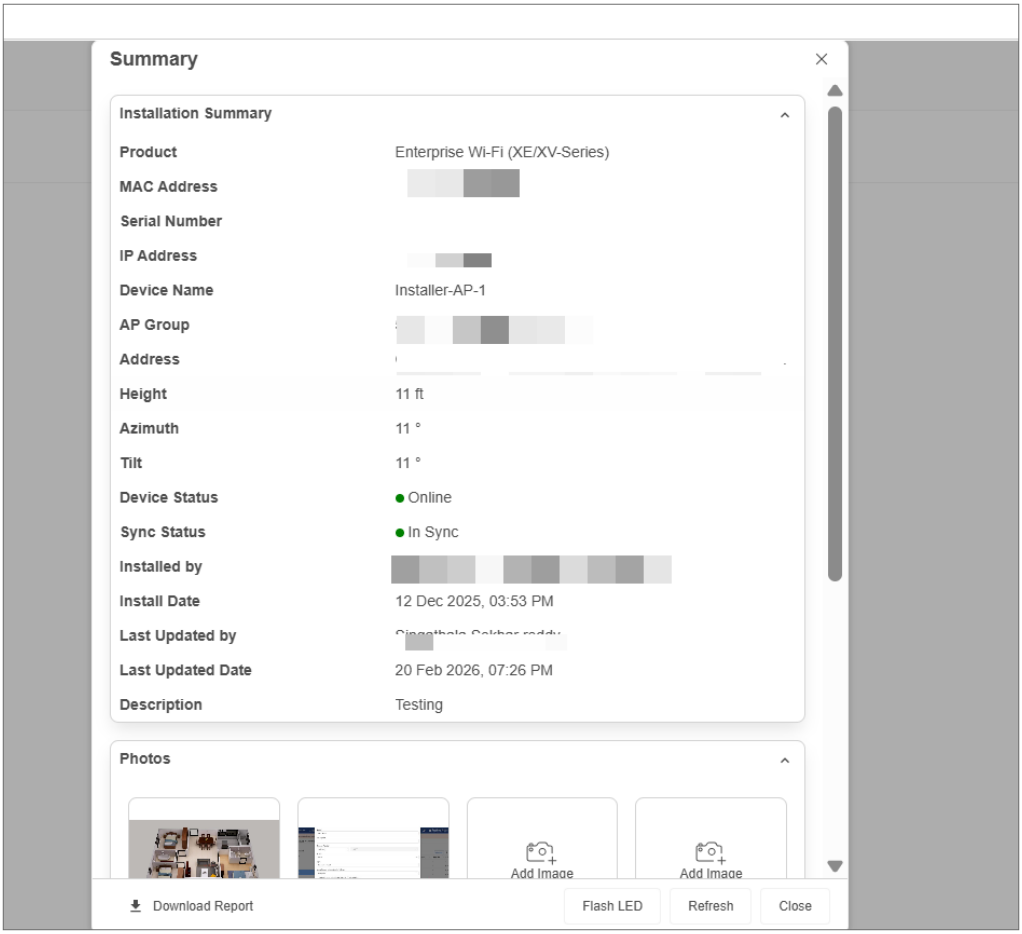


Figure 652 *Installation Summary—Desktop view*



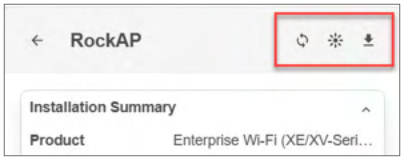
The summary page includes the following sections:

- **Installation Summary**: Shows key details such as product name, MAC address, serial number, IP address, device name, AP group, address, height, azimuth, tilt, device status, sync status, installer details, and timestamps for install and last updated.
- **Photos**: Displays uploaded installation images. The installer can tap Add Image to upload more photos if required.
- **Link Status**: Allows the installer to tap **Check Link Status** to view the Ethernet speed and validate connectivity.
- **Installer Comments**: Displays any comments entered earlier. The installer can edit or update the comment from this screen.

Additional options on the summary page

The top-right corner of the summary page includes three options that help installers perform additional actions based on their needs as shown in Figure 653.

Figure 653 *Additional options on the summary page*



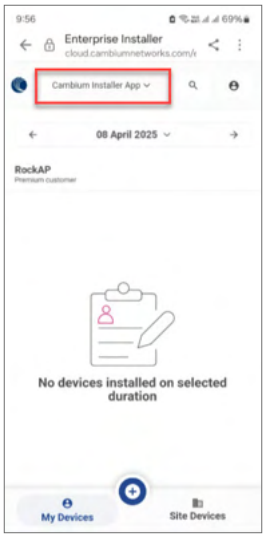
- **Refresh** – Updates the page with the latest device information pulled from the server.
- **Flash LED** – Triggers the selected device's LED to blink for 30 seconds, helping the installer identify the correct unit on-site.
- **Download Report** –Generates and downloads a PDF report containing all installation details shown on the screen. This report can be saved or shared with the Internet Service Provider (ISP).

To return to the main device list, the installer taps the back arrow located at the top-left corner next to the device name.

Viewing installed devices and switching between apps

1. The main screen displays a list of devices installed by the logged-in installer under **My Devices**. Devices installed by other installers for the same MarketApps app appear under **Site Devices**.
2. The installer can view the installation history for the past 10 days using the date field at the top to filter and navigate by date.
3. If the installer has access to multiple MarketApps Installer Apps, they can use the dropdown (Figure 654) at the top to switch between apps—there is no need to go through the invitation email flow again.

Figure 654 *Viewing installed devices*



Locating installed devices in cnMaestro

Once a device is installed through the Installer App, it appears in the Onboarding section of cnMaestro under the site selected during installation. From there, the device follows the standard onboarding workflow based on its configuration and assigned groups.

Replacing devices in the Installer app

The Installer app allows users to replace any faulty APs or cnMatrix switches, or upgrade the devices in their deployment.

Points to remember and prerequisites for replacing devices

The following points must be considered before replacing devices using the Installer App:

- Cambium supports replacing Enterprise Wi-Fi APs, cnMatrix switches, and 60 GHz cnWave devices using the Installer app.

  Note

  Replacing of cnMatrix switches is supported only if the switches are the same model.

- Users must have access to the site where the devices must be replaced.

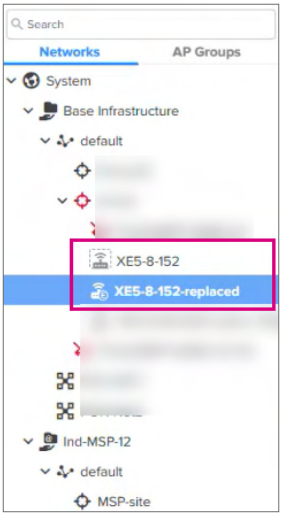
  Users will not be allowed to replace devices from sites they do not have access to.

- If the existing device has a custom device name, then after replacing, the new device takes the same device name as the old one that was replaced.

  Also, the `-replaced` suffix is added to the old device name.

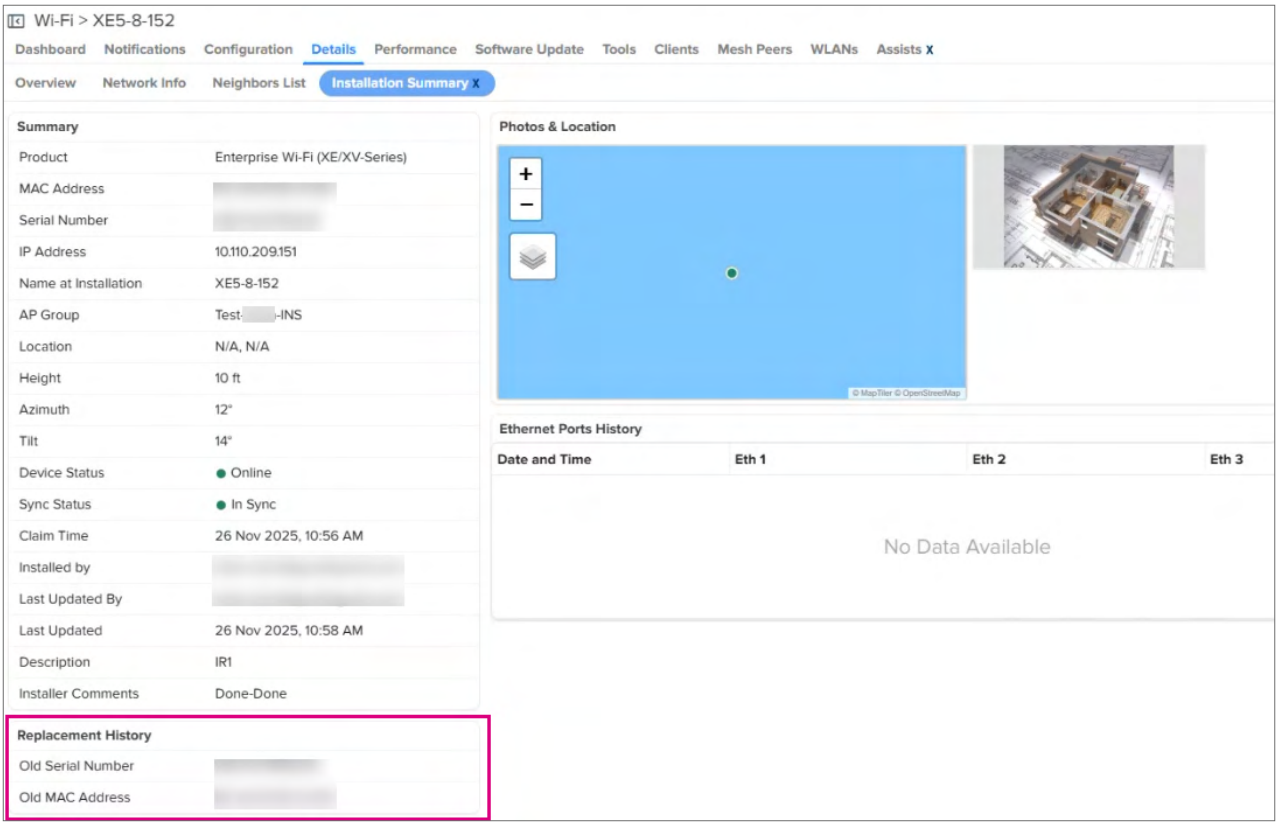
  For example, if an old AP has a custom device name `XE5-8-152`, and the new device's name is `XYZ-XE5-8-123`, then after replacement, the device name of the new AP will be `XE5-8-152`.

  And the device name of the old AP is renamed as `XE5-8-152-replaced`.



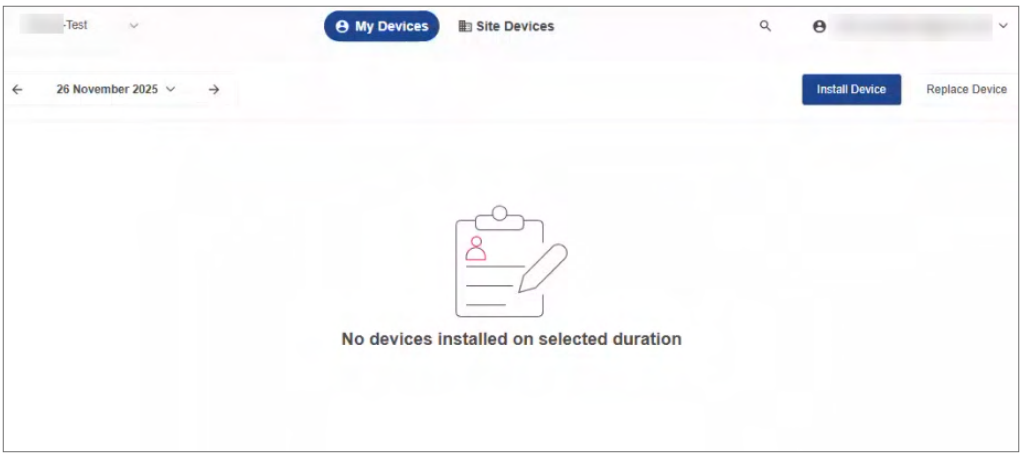
- If the existing device has the default device name (for example, XE5-8-E10459), then after replacing this device, the new device will take its own default name for example, XE5-8-B3ECC7).
- If the existing AP was mapped to an AP group, then the same AP group and the corresponding configuration is applied on the new AP.
- If the existing AP was installed using the Installer app, then the following details are auto-populated in the replacement AP:
  - Height
  - Azimuth
  - Tilt
- To view the details of the previous AP that was replaced, navigate to **Monitor and Manage** > **Site** > **Device (New AP)** > **Details** > **Installation Summary X** page.

  The details are displayed under the **Replacement History** section.



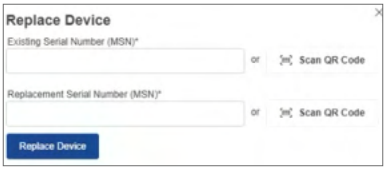
To replace device, complete the following steps:

1. Navigate to the Installer web app homepage.



2. Click **Replace Device**.

   The Replace Device window is displayed.



3. Provide the existing device's and the replacement device's serial numbers and click **Replace Device**.

   Users can also scan the QR code on the device box to enter the serial number.

4. After successfully replacing the device, a success message is displayed and the app redirects to a new page displaying the Installation Summary for the replaced device.



Searching, updating, and replacing existing device in the Installer App

cnMaestro allows administrators and installers to search for existing devices that are already onboarded to cnMaestro and update their Installation Summary information. Installers can achieve this without manually reinstalling, re-onboarding, or individually checking the device page.

Note

This search and update or replace feature is applicable only to existing cnMaestro-onboarded devices and does not replace the standard installation workflow for new devices.

Installers can search for existing devices using device name, serial number (MSN), or MAC address (including partial matches). The search result lists the devices matching the search criteria with the following distinction:

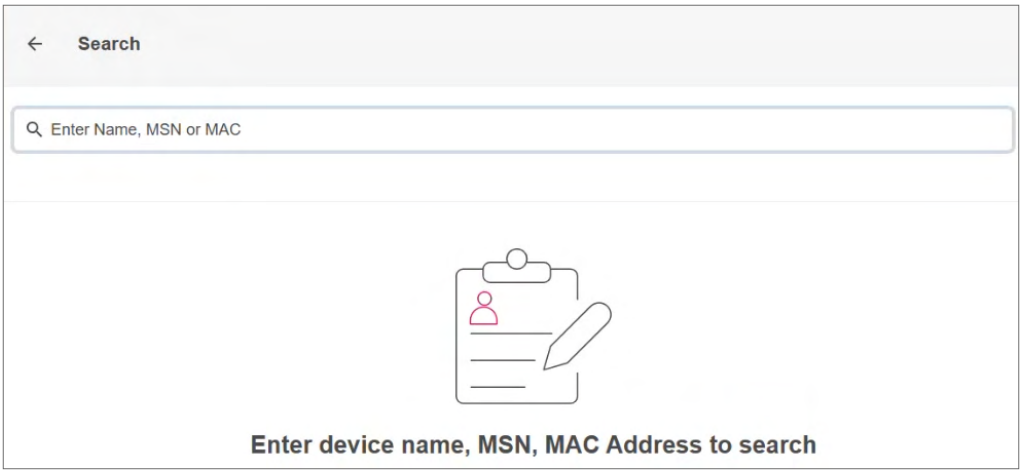
- Devices with the new (New) icon—Devices that were onboarded directly through cnMaestro but do not yet have an Installation Summary.
- Devices without the new icon—Devices were already installed through the Installer application.

Installers can edit only the following fields when searching and updating the Installation Summary:

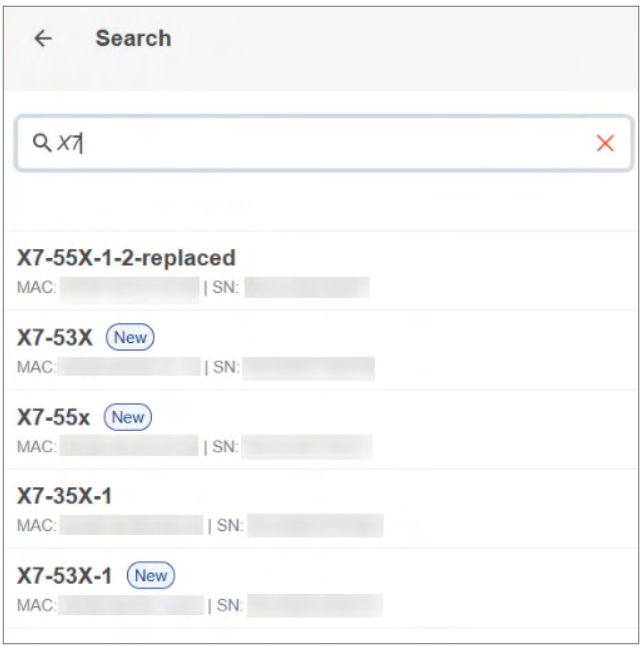
- Location
- Height
- Tilt
- Photos

To search and update or replace the device, complete the following steps:

1. Open the Installer App web interface and navigate to the device search section.

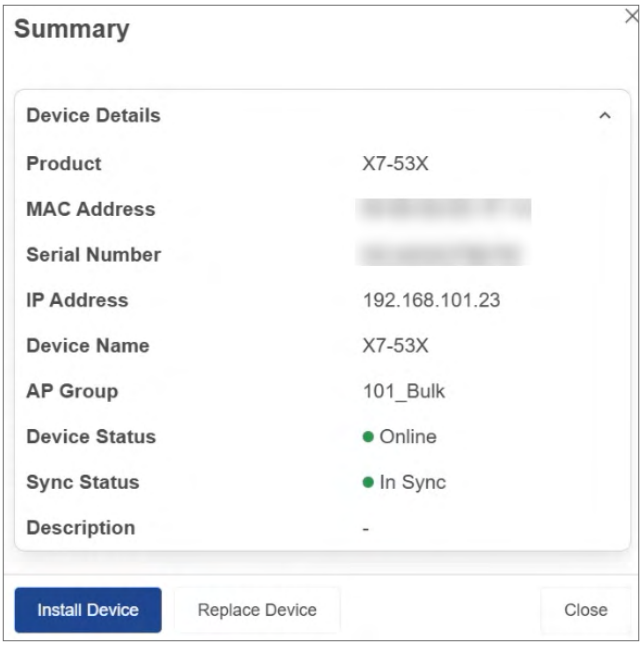


2. Search using any of the following:
   - Device Name (partial or complete)
   - Serial Number (MSN)
   - MAC Address
3. A list of existing devices are listed.



   The devices with the new (New) icon are those that are onboarded to cnMaestro but do not have any Installation Summary updated.
4. Click any devices with the new icon.

   The Summary window is displayed with basic information.

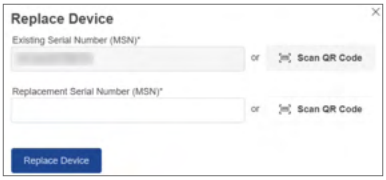


5. To install the device and update the Installation Summary, click **Install Device**.

   The Update Device window is displayed.



6. Update device information, such as precise location, height, Azimuth, tilt, and upload the device photos.
7. Click **Save**.
8. To replace the device, click **Replace Device** in the **Summary** window.



9. Provide the replacement serial number and click **Replace Device**.

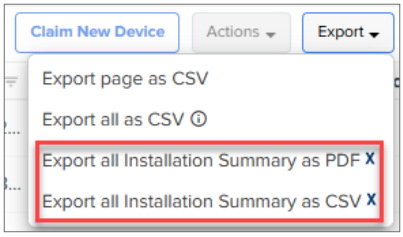
Note

To check whether the Installation Summary is updated or not, navigate to the device **Details** > **Installation Summary** page.

Exporting Installation Summary information

You can export the Installation Summary of all devices installed in a site using the Installer App as a PDF or CSV .

To export, navigate to **Monitor and Manage** > **Site** > **Devices** > **List** page and select one of the following options.



Citizens Broadband Radio Service (CBRS)

This chapter details cnMaestro support for the Citizens Broadband Radio Service (CBRS) subscription which is required to manage CBRS-compliant devices in the 3.6 GHz band (3550 MHz to 3700 MHz).

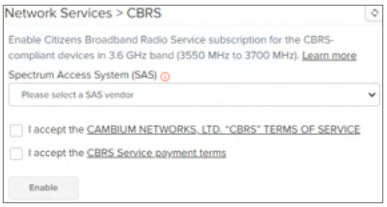
This topic describes the following sections:

- Enabling CBRS in Cloud
- Management Tool
- Domain Proxy View
- Actions for Existing CBRS On-Premises Users

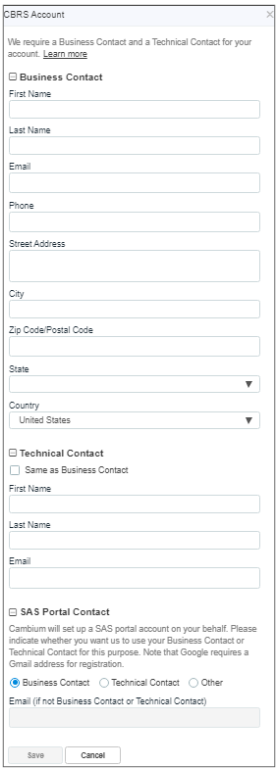
Enabling CBRS in Cloud

1. Login to a cnMaestro Cloud NMS account or Cloud Anchor account (if hosting on an On-Premises instance).
2. Navigate to **Network Services > CBRS** page.
3. Select the preferred SAS vendor from the **Spectrum Access System (SAS)** dropdown list.

   Figure 655 *Network Services > CBRS > Account tab*

4. Read both the terms and conditions, and accept them by selecting the checkboxes.
5. Click **Enable.**
6. In the **Billing Information** window configure the following details:



- **Business Contact**
  - First Name
  - Last Name
  - Email
  - Phone
  - Street Address
  - Zip Code
  - Country
  - State
- **Technical Contact**

  Enable **Same as Business Contact** or enter a separate Technical Contact.
  - First Name
  - Last Name
  - Email
- **SAS Portal Contact**

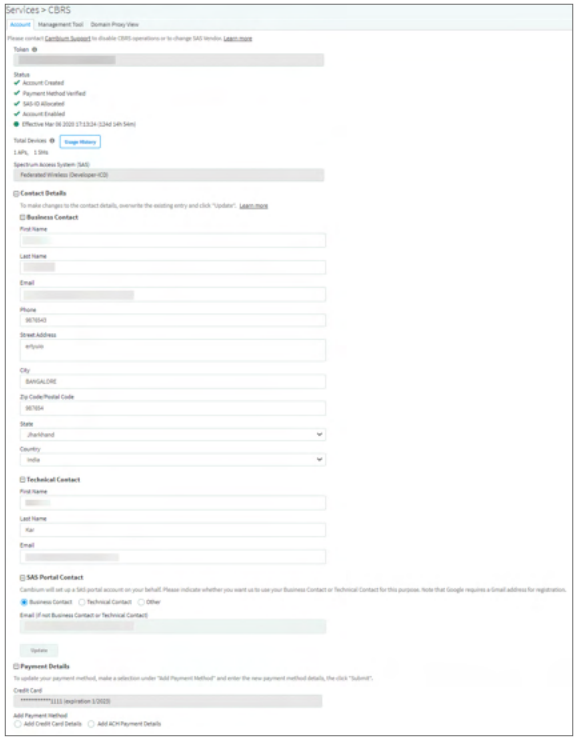
  Cambium Networks creates the SAS portal account on behalf of the operator.

7. Click **Save.**

   The CBRS account is enabled.

After you save the CBRS account, you must complete the following steps:

1. The **Account** page displays the following information and configurable parameters:
    - Token
    - Status
    - Total Devices
    - SAS
    - Contact Details
    - Payment Details



a. **Token:**

Token used for authenticated communication with SAS through Cambium Domain Proxy. It gets generated automatically once CBRS is enabled for the Cloud account.

b. **Status:**

Displays the account status.

Pending Status	Success Status
Status ✔ Account Created ✖ Payment Method Verification Pending ✖ SAS-ID Allocation Pending ● Effective Jul 07 2020 16:54:10 (< 1m) Total Devices ⓘ Usage History 0 APs, 0 SMs	Status ✔ Account Created ✔ Payment Method Verified ✔ SAS-ID Allocated ✔ Account Enabled ● Effective Mar 19 2020 15:02:02 (110d 2h 0m) Total Devices ⓘ Usage History 3 APs, 68 SMs

i. **Account Creation**: Displays as **Account Created** once the account is enabled. Refer to **Step f** for entering contact information and enabling account.

ii. **Payment Method**: Displays as **Verified** once the Payment Details are approved. Refer to **Step g**Payment Details.

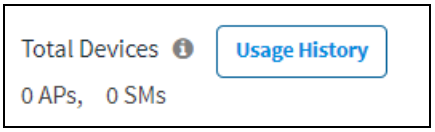
iii. **SAS ID**: Once the payment details are verified, the SAS ID is allocated automatically.

> **Note**
>
> When the SAS ID allocation is pending or unavailable in the server, even after the payment details are configured and verified,
>
> It may take up to one day for the SAS ID to be allocated.

iv. **Effective:**

- **Grey**: indicates the **Pending Status**.
- **Green**: indicates **Success Status**.
- **Red**: indicates the account has been **Deactivated**.

c. **Total Devices:** Displays the count of **Total Devices** registered with the SAS using the **Token ID**. **Usage History** provides the list of devices registered with **Month** and **Year**.



> **Note**
>
> Initially the device counts will be 0 APs and 0 SMs.

d. **SAS:** Displays the SAS vendor preferred by the operator.

> **Note**
>
> Contact Cambium support to disable CBRS operation or to change SAS Vendor.

e. **SAS:** An operator needs to select which SAS vendor they prefer.

f. **Contact Details**:

For new CBRS account migrations, this information would have already been entered in Citizens Broadband Radio Service (CBRS). Review and update if necessary, else refer to Payment Details.

Cambium Networks selectively communicates with both the **Business Contact** and the **Technical Contact** with changes of interest: such as SAS administrator updates, CBRS initiative changes from the CBRS Alliance and WInnForum, and announcements of new Cambium Network CBRS features and options.

Business Contact

Cambium Networks communicates with the **Business Contact** for all commercial aspects of the CBRS Service such as invoicing, payment, change in terms, change in pricing, and other details. This page requires:

- **First Name**
- **Last Name**
- **Email**

- **Phone**
- **Street Address**
- **City**
- **Zip code/Postal Code**
- **State**
- **Country**

Technical Contact

Cambium Networks communicate with the **Technical Contact**: such as software updates, release notes, learning guides, technical issues, etc.

- **First Name**
- **Last Name**
- **Email**

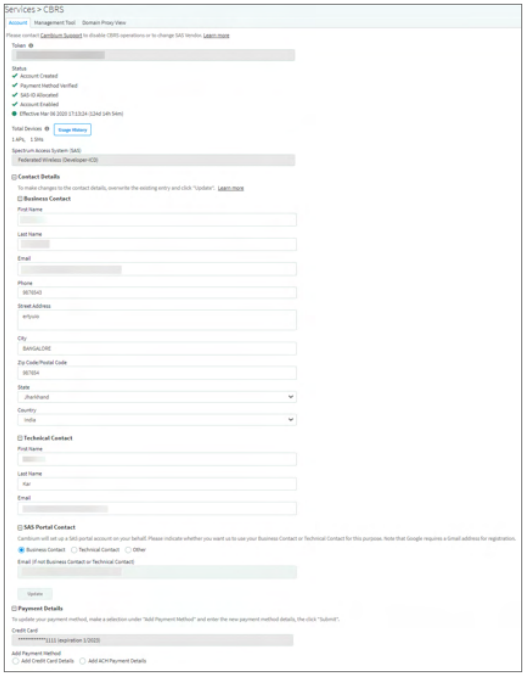
SAS Portal Contact

Cambium Networks sets up the SAS portal account on behalf of the operator. Please select whether to use the **Business Contact, Technical Contact,** or **Other.**

Note

Google requires a Gmail address for registration.

- Click **Update.**



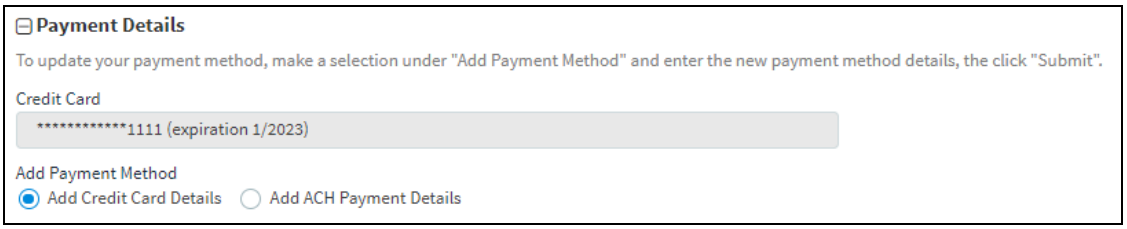
Note

Clicking **Update** on the **Account Page** overwrites the current entries.

g. **Payment Details**

Select one of the payment methods below:

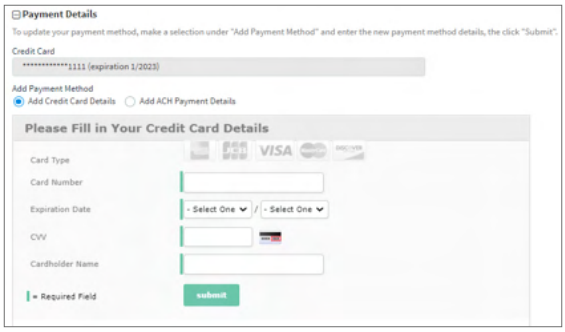
- Add Credit Card Details
- Add ACH Payment Method



Add Credit Card Details

Enter the following and click **Submit**:

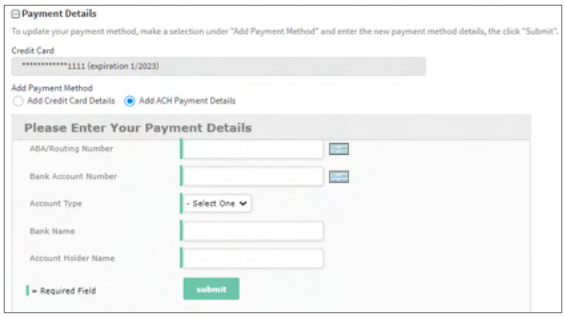
- 16 digit Credit **Card Number**.
- **Expiration Date** and **Year** on the card.
- **CVV** and **Cardholder Name**.



Add ACH Payment Method

Enter the following details and click **Submit**:

- **ABA/Routing Number**.
- **Bank Account Number**.
  - Select one of the following for **Account Type:**
    - Checking
    - Saving
    - Business Checking
- **Bank Name** and **Account Holder Name**.



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:

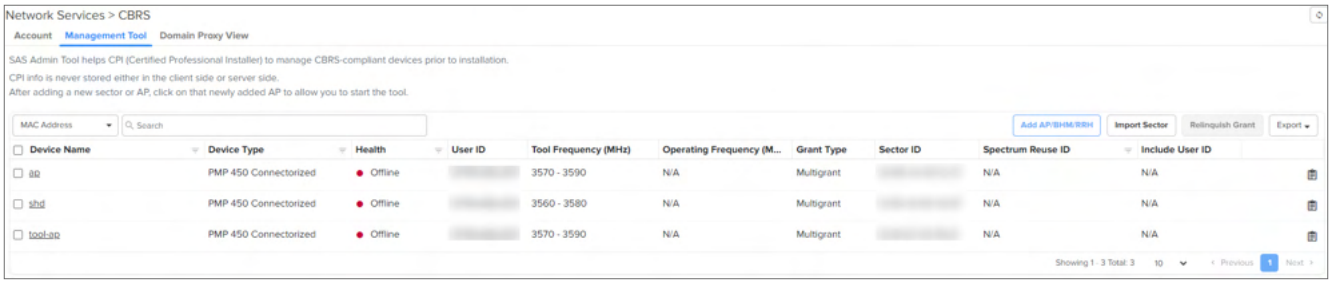
Note

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

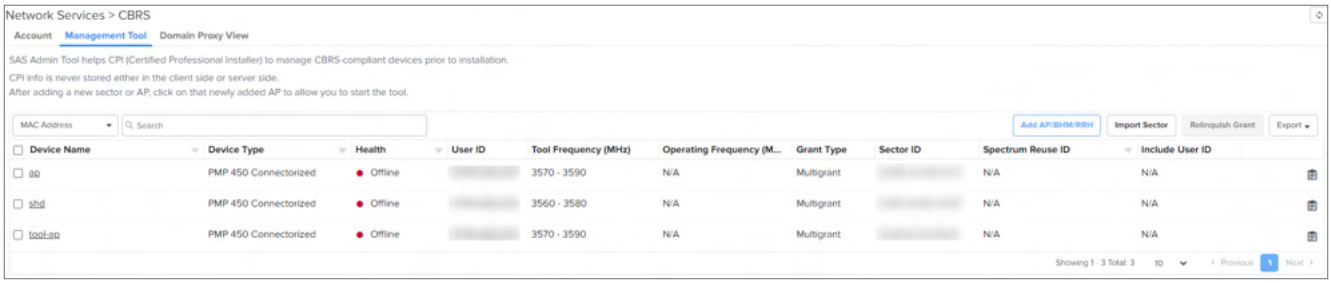
The CBRS procedure can be performed by an authorized CPI (Certified Professional Installer). CPIs are required to enter necessary credentials to update the CBRS parameters.

A CBRS sector view is shown below:



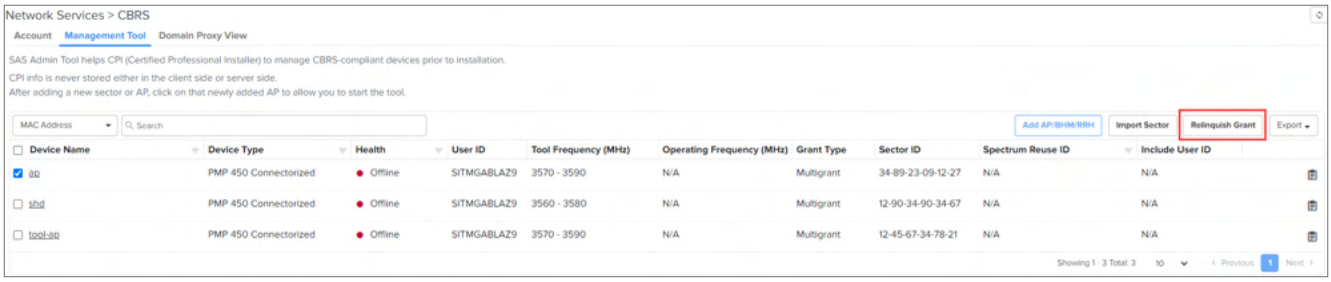
Export

The **Export** button allows one to export multiple device reports in the **CSV** format.



Relinquish Grant

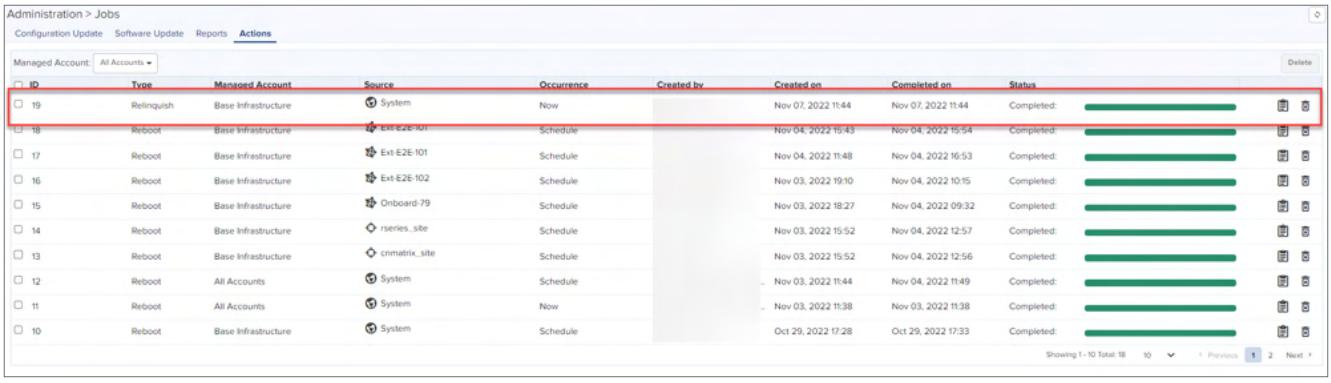
The Relinquish Grant button relinquishes all grants of selected sector and places devices in the Registered state. The device will start the Multi-Grant procedure if the Multi-Grant feature is enabled on the device.



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.

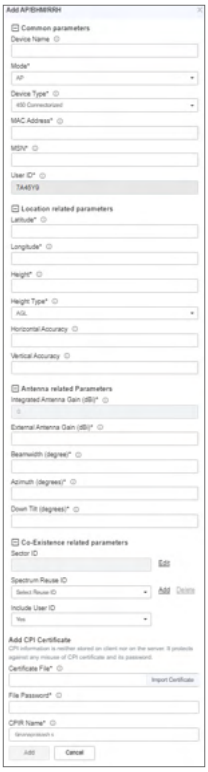
Add AP/BHM

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.

     Note

     Include User ID parameter is applicable only for PMP devices, when SAS is **Federated Wireless.**

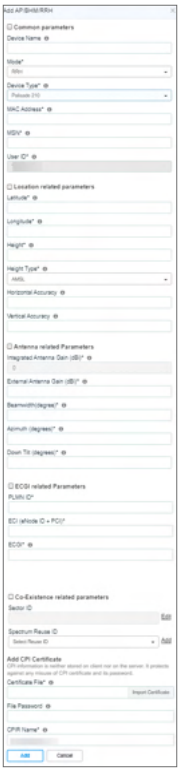
     Select **Yes** or **No** to Include the user ID.
   - **Add CPI Certificate**: Certificate File, File Password, CPIR Name.



3. Click **Add** to add a sector.

Add RRH

1. Navigate to **Services > CBRS > Management Tools** and click **Add AP/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**.

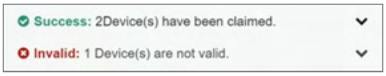
   Selecting **Yes** in the **Include User ID** parameter prefixes the **User ID** to the **Sector ID** and **Spectrum Reuse ID** in the registration message of the SAS.

   Note

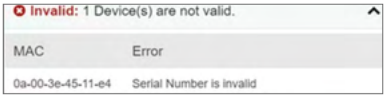
   - **Include User ID** is applicable only for PMP devices, when SAS is selected as **Federated Wireless**.
   - See the CBRS Consolidated Procedures Guide and the Cambium PMP Release 20.3 training slides for more details on when to select **Yes** or **No.**

7. Click **Import.**

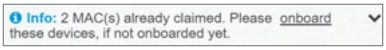
   Import status is displayed as **Success, Info**, and **Invalid**.



8. Details of **Success**, **Info,** and **Invalid** section can be seen by clicking expand ( ) arrow.



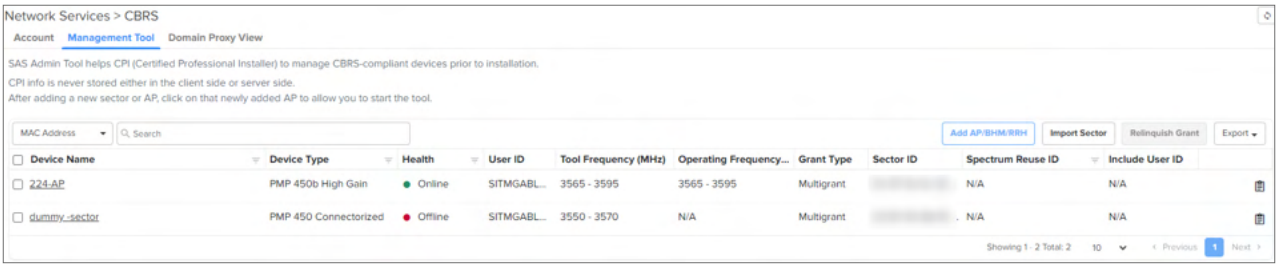
9. If the device is already claimed, it can be onboarded by clicking the onboard link.



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

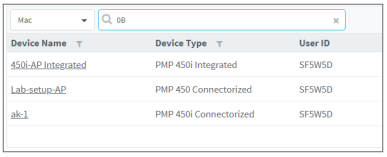
To search for a sector:

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.



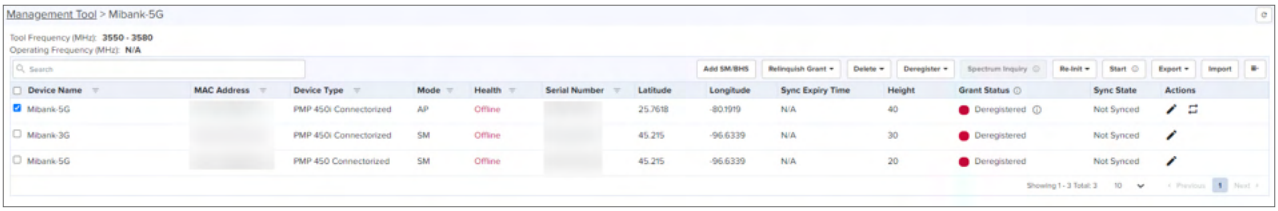
1. Filter AP or sectors can be cleared by clicking or **Clear** button.

Sector View

1. Click a sector from the Sector AP column to get the list of devices.

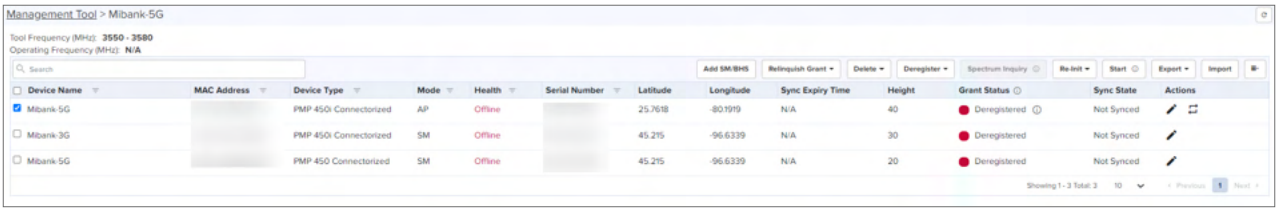
Sector AP	Device Type
"208.41"	PMP 450 Integrated

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.

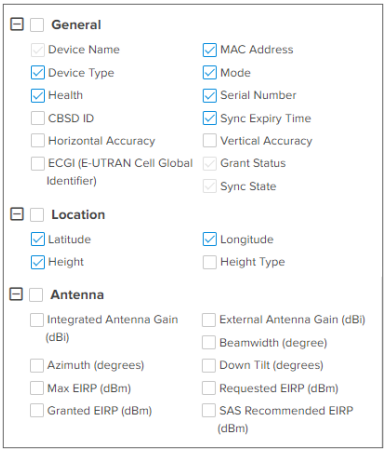


Note

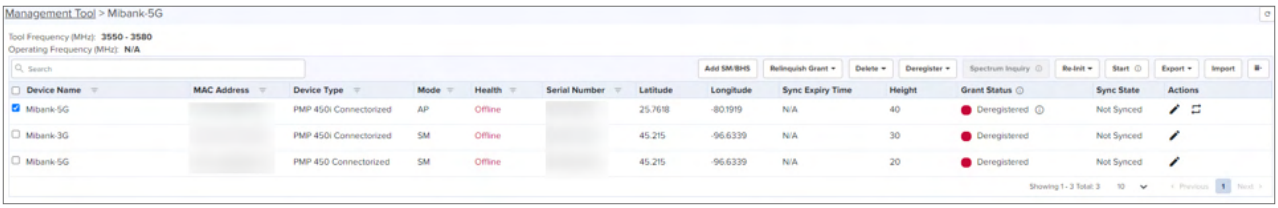
If the device is **Config_Synced**, the CBSD state of the device will be updated from the device in real-time.

- 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( ).



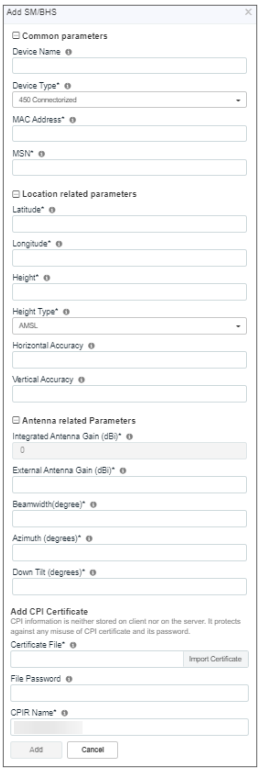
- User can use following button to control the CBRS procedure:



  - **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

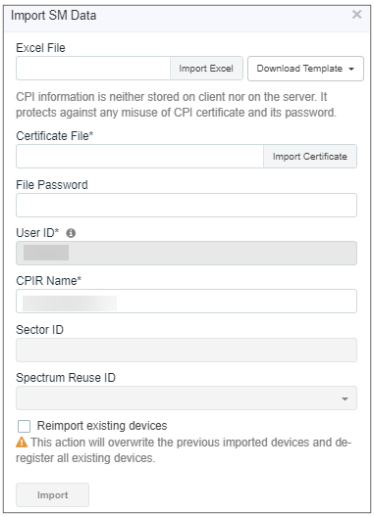
1. Navigate to **Services** > **CBRS** > **Management Tool** > select a sector.
2. Click **Add SM** or **BHS** to add SM in a sector.



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.

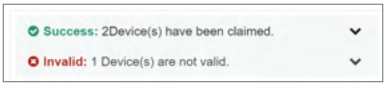
Import SMs

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.

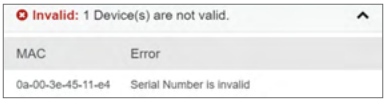


4. Click **Download Template** if user does not have Import Sector template. Users can download two different template formats:
    - PMP: Excel or ODS
    - LTE: Excel or ODS
5. Click **Import Excel** to select Import Sector template file. File must be Microsoft Excel format (.xlsx) or Open Document 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**.

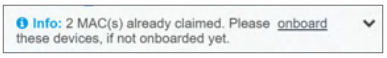
    Import status will be shown under **Success, Info,** and **Invalid** sections.



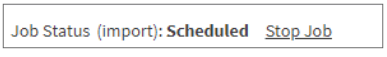
8. Details of **Success**, **Info** and **Invalid** can be seen by clicking .



9. If the devices is already claimed, it can be onboarded by clicking the **onboard** link.

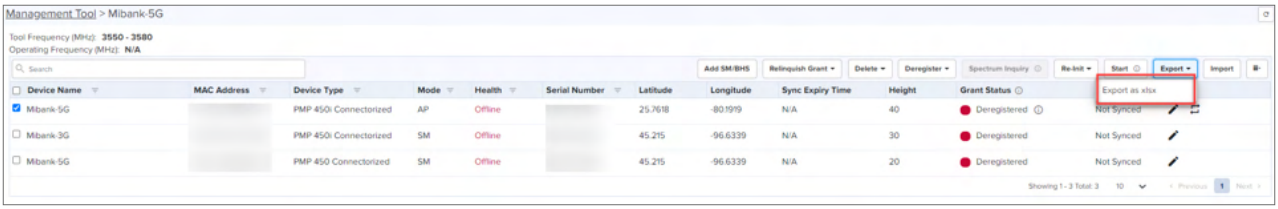


10. Once the user clicks **Import**, a job is scheduled.

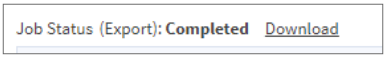


Export Sector

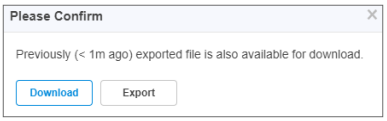
1. Navigate to **Services** > **CBRS** > **Management Tool** and then select a sector.
2. Click **Export** button to export the sector (export as xlsx).



3. Once the user clicks **Export**, a job is scheduled.

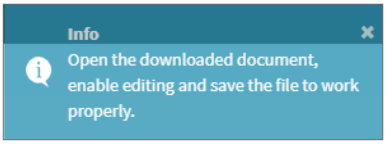


4. Once the Job status is Completed, **Download** the Sector xlxs.



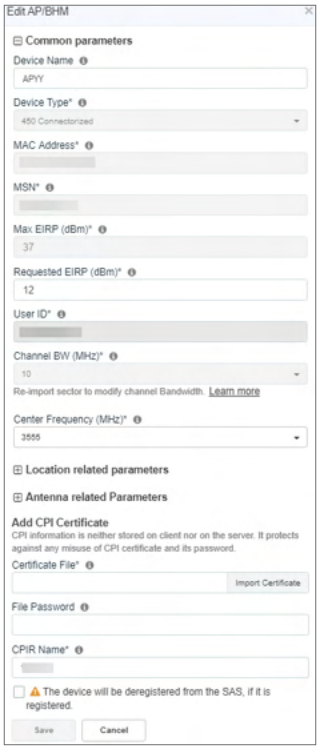
> **Note**
>
> **Download** button is enabled only for two hours after the export job completes.

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

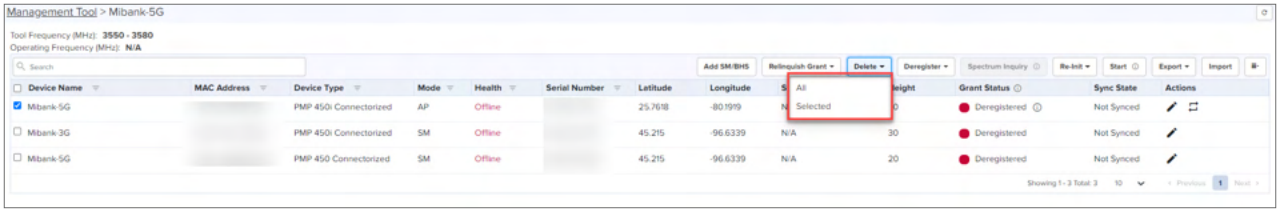
1. Navigate to **Services > CBRS > Management Tool** and select a sector**.**
2. Click **Stop** button if the CBRS procedure is running.
3. Click **Edit** button to edit device parameters.
4. Enter CPI credentials:
   - Upload CPI Certificate File by clicking **Import Certificate** button.
   - Enter CPI File Password.
   - Enter CPI Registered Name.
5. After editing the device. The device should go to derigestered state.



6. Click **Save**.

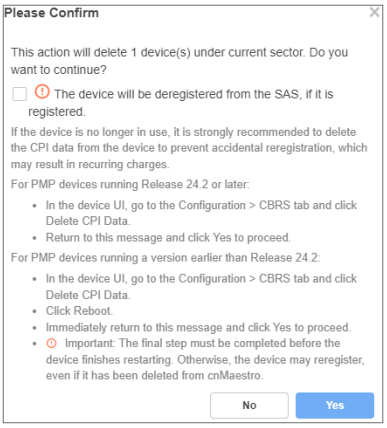
Delete Device

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:

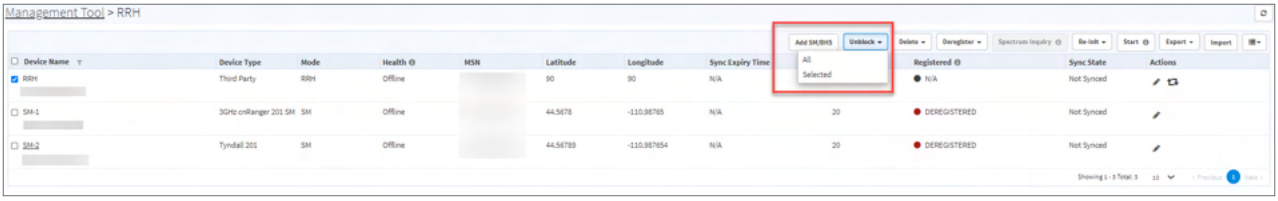
   All SMs of the sector must be deregistered and deleted before deleting the AP. Refer to the Deregistration procedure to deregister all SM devices.

8. Select the AP of the sector to delete.
9. Click **Delete**.

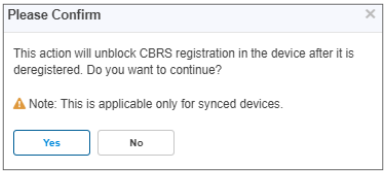
> **Note**
>
> If the procedure is started for the device and it is registered, then, while deleting the device, you must select the **Deregister** checkbox, otherwise the deletion will fail.

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.

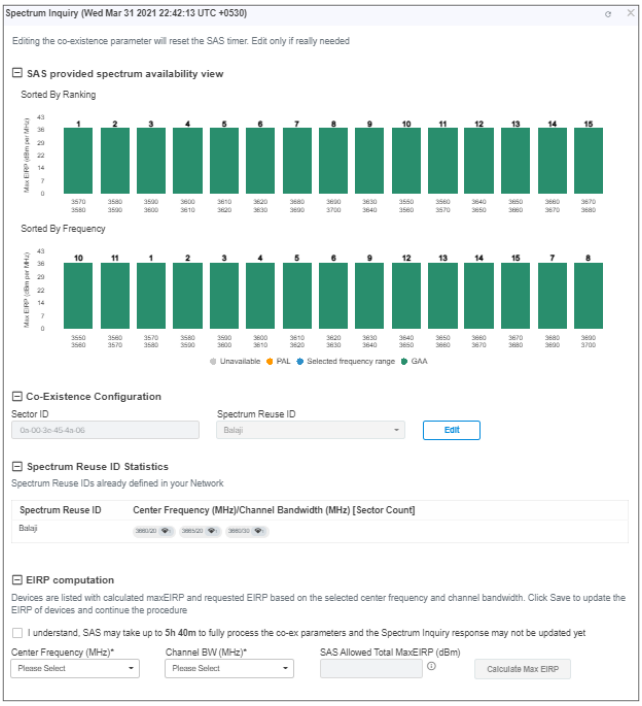


5. Click **Yes** to confirm the action.

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.



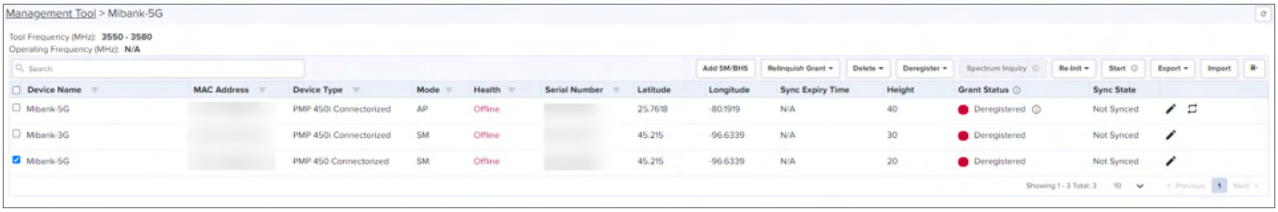


Note

- 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).

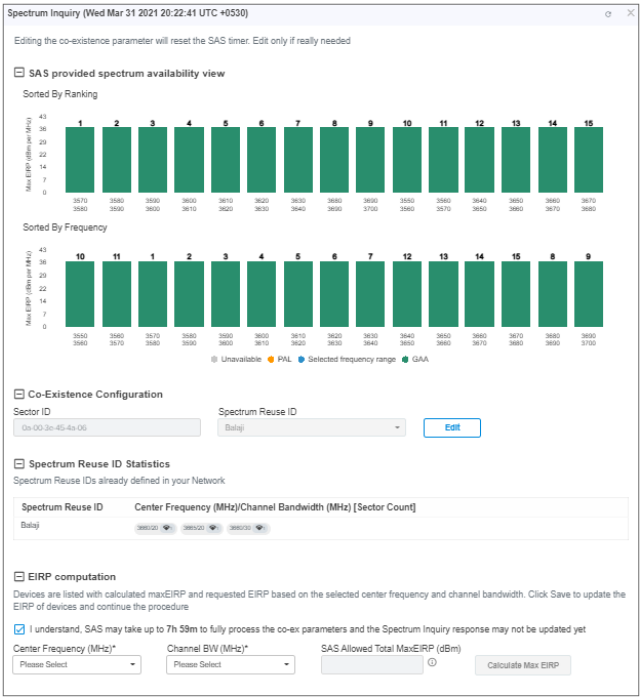
Multi-Grant

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.

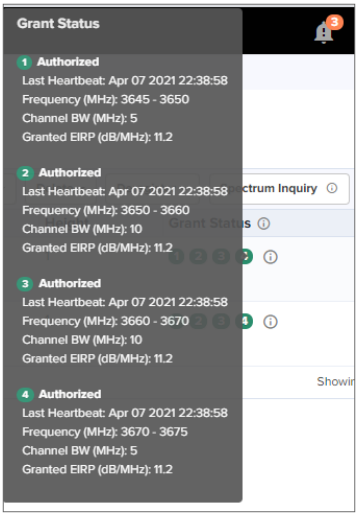
> **Note**
>
> The Federated Wireless or Google SAS might need hours to fully process the Co-Existence parameters in the Registration, (before they are properly reflected in the Spectrum Inquiry Response). For more details see the CBRS Standalone Procedures Guide.

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

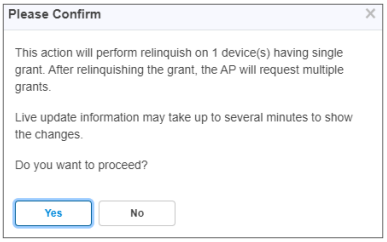
Relinquish Grant relinquishes all grants of selected sector. This will make devices enter the Registered state. The device will start Multi-Grant procedure if Multi-Grant feature is enabled on it.

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.



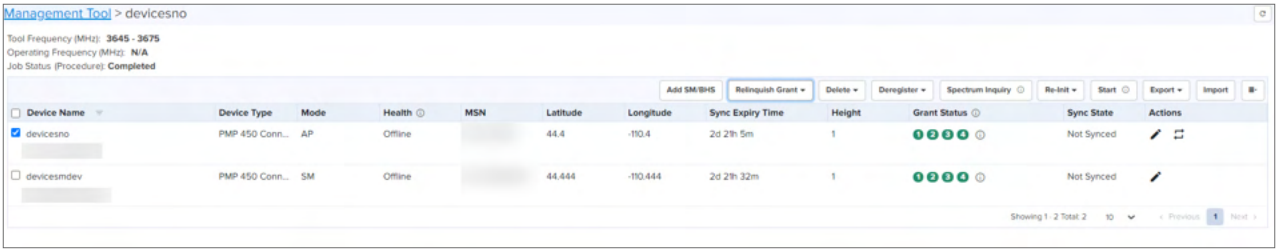
3. Click **Yes** to confirm the action.



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

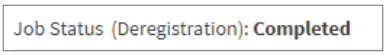
- Synced devices cannot be reinitialized.
- Reinitialize modifies or corrects the parameters. For example, if a device is in HALT state due to a parameter error, the user can stop the CBRS procedure and reinitialize the device after modifying device parameters.

Deregistration

The deregistration procedure allows user to deregister the devices from the SAS server .

1. Navigate to **Network Services** > **CBRS** > **Management Tool** and select a sector.
2. Click **Stop** button if the CBRS procedure is already running.
3. Select one or many devices which need to be deregistered.
4. Click **Deregister** button to deregister selected devices.

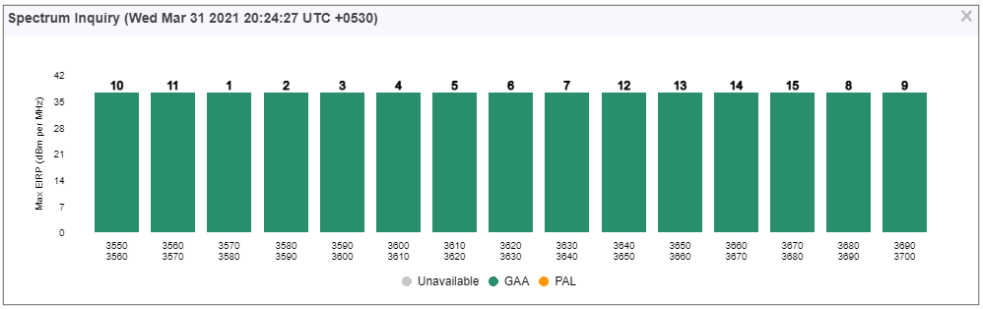
   Once the user clicks **Deregister**, a job is scheduled**.**

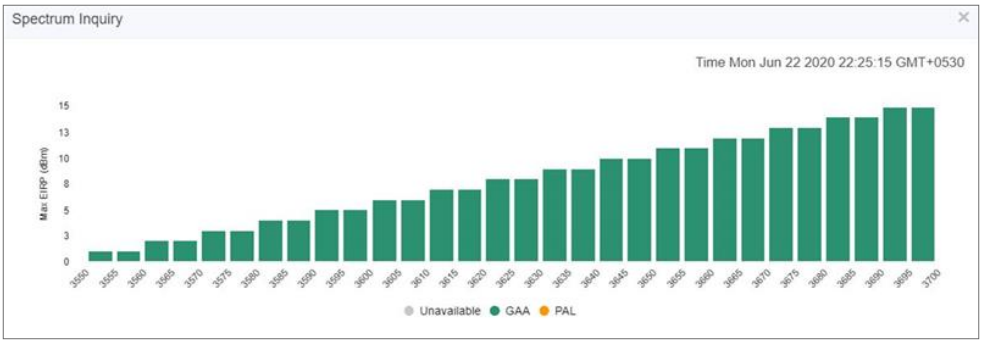
5. If the deregistration fails, the reasons will be indicated under .

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.

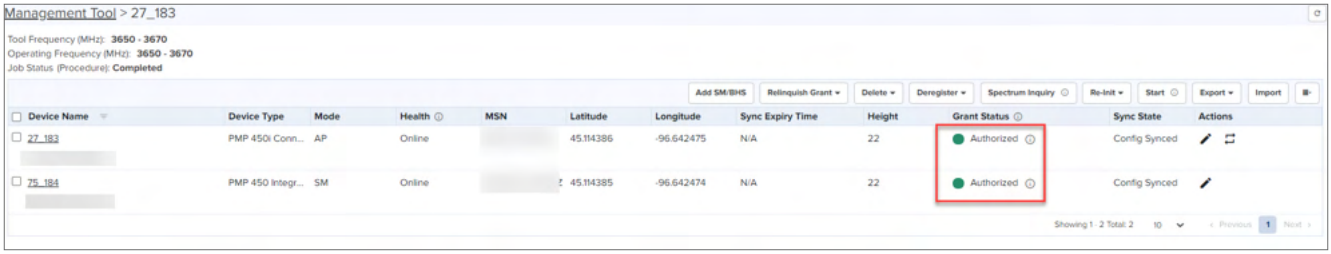
Once **Yes** is clicked, the Management Tool will check the accessibility of AP/BHM before proceeding with sync.

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:

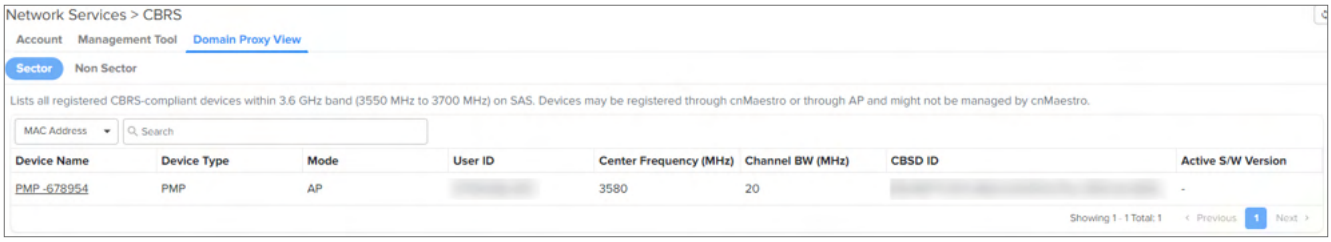
- Authorized
- Deregistering
- Grant
- Grant Suspended
- Grant Terminate
- Registered
- Registering
- Relinquished Spectrum
- Relinquishing Spectrum
- Unregistered
- Unknown

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.

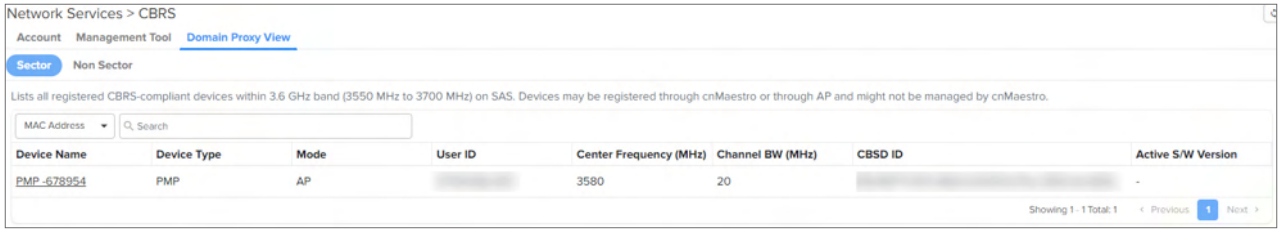


- **Sectors Page**: displays the devices according to the parenting AP list.
- **Non-Sector Page**: displays each individual AP and SM of **LTE** and **PMP**.

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.



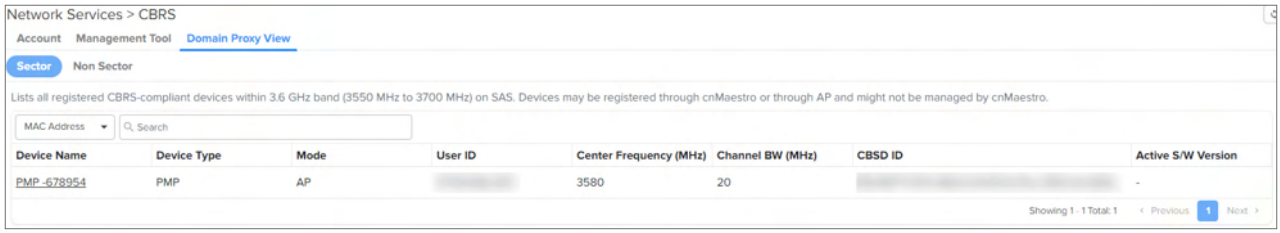
Note

- 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

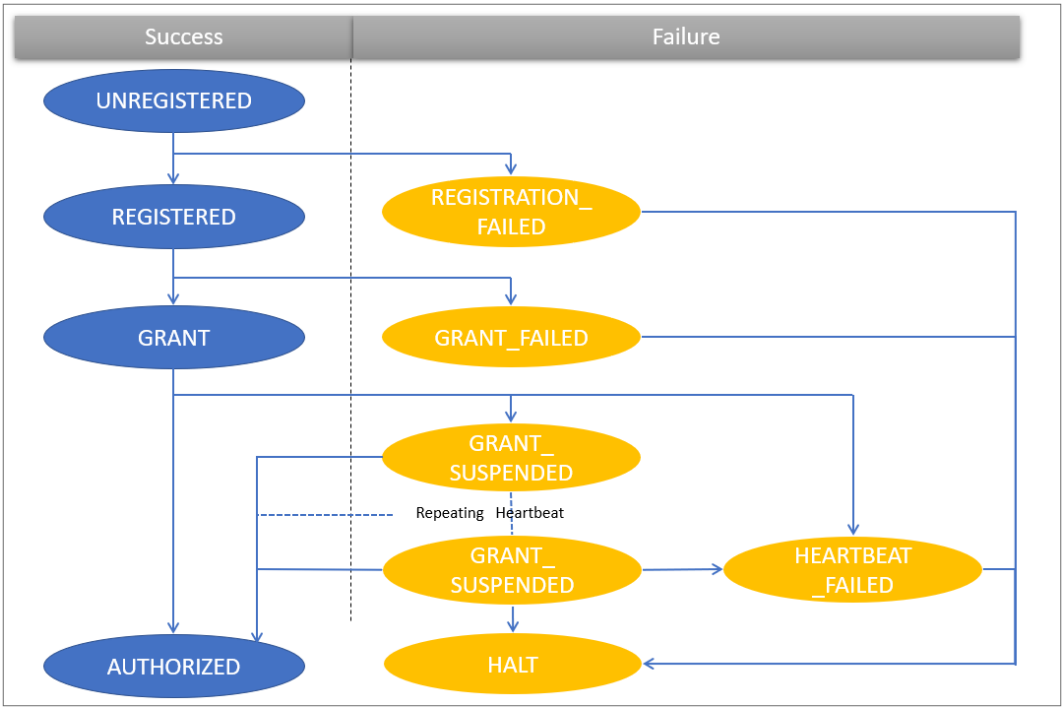
Information in the **Heartbeat Status** and **Last Heartbeat** columns is displayed only for registered devices.

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.

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

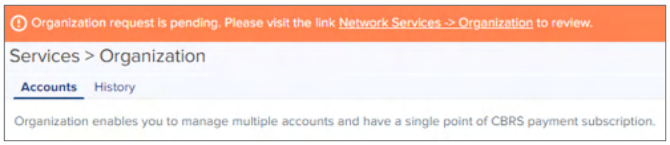
Category	Parameter	Details
Common	Channel BandWidth (MHz)	Channel Bandwidth of AP or BHM in MHz.
	Center Frequency (MHz)	Center frequency of AP or BHM in MHz.
	Device Name	Name given to device on SAS Admin (A maximum of 120 characters are supported. However, this name is not copied to the device when 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.

Actions for Existing CBRS On-Premises Users

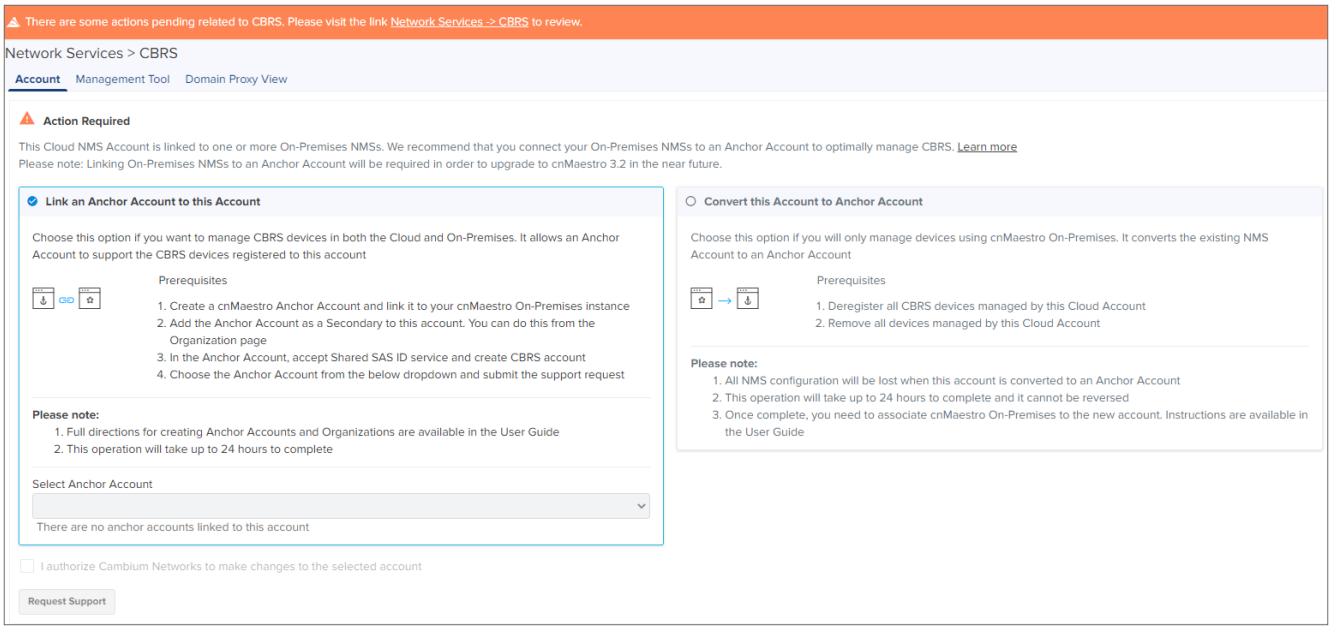
Current CBRS On-Premises customers maintain their CBRS billing and SAS configuration in an NMS Account. This must be updated to support Anchor accounts. To create an anchor account, refer to Manage Instances.

If an action is required for existing Cloud NMS users, the UI will display the following notification:



After clicking the notice, navigate to **Services.**

- **Link an Anchor Account to this Account:** Select if managing CBRS devices in both Cloud and On-Premises. It creates an Organization that shares configuration between a Primary NMS account and a Secondary Anchor account (without deregistering existing CBRS devices).
- **Convert this Account to Anchor Account:** Select only if managing devices On-Premises and NMS do not have any devices. It converts the existing NMS Account to an Anchor Account.



Link an Anchor Account to this Account

Select this to manage CBRS devices in both Cloud and On-Premises. An Anchor account must be created to manage the CBRS On-Premises devices without deregistration.

Note

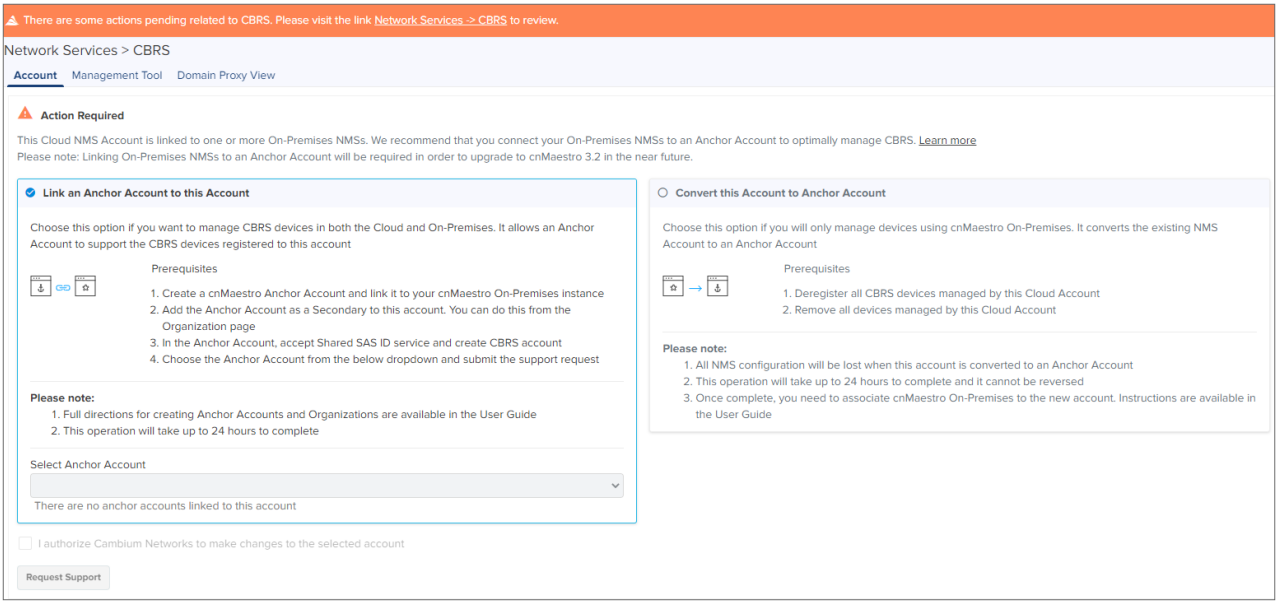
Cambium recommends selecting this option when the user is managing devices in both cnMaestro Cloud and On-Premises.

Before linking an Anchor account, please do the following:

- Ensure the cnMaestro Anchor account is linked to the cnMaestro On-Premises instance(s).
- Add the Anchor account as a Secondary account to Primary NMS account. Refer to Create Organization.

To convert the existing account:

1. Navigate to **Services** > **CBRS** > **Account** page.

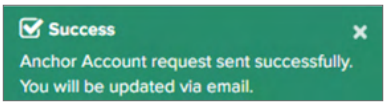


2. Select **Anchor Account** from the dropdown list.

Note

Users are allowed to select only one Anchor account from the dropdown list.

3. Enable **I authorize Cambium Networks to make changes to the selected account**.
4. Click **Request Support** and a **Success** window pops up.



Note

The Cambium Support team validates the request and creates an Organization from the NMS and Anchor accounts within 24 hours. Alternately, you can create the Organization yourself using the directions specified earlier in this document.

Convert this Account to Anchor Account

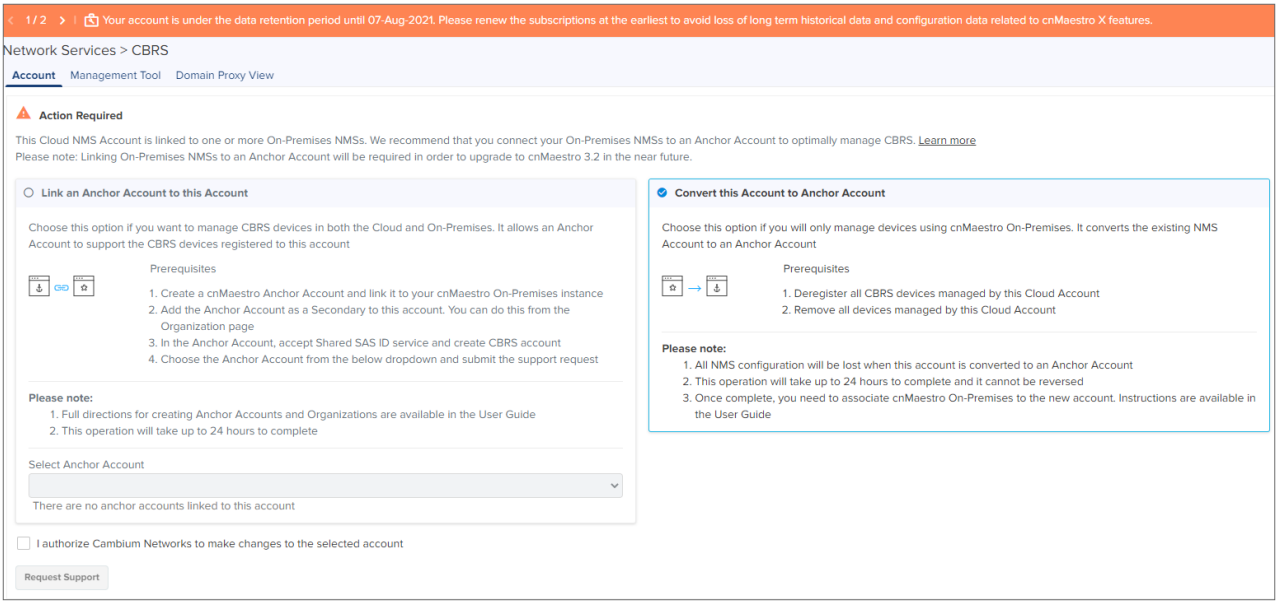
Select this to manage CBRS devices in On-Premises only. It converts an existing NMS account to an Anchor account.

Note

Cambium recommends selecting this option when the user only plans to manage devices using cnMaestro On-Premises. Cloud account devices must be deregisted and deleted from the NMS account and registered back to On-Premises before the conversion.

To convert the existing account:

1. Navigate to **Services** > **CBRS** > **Account** page.

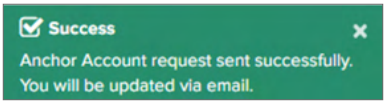


2. Select **Convert this Account to Anchor Account.**

Note

- Deregister and remove all devices from the NMS account before the conversion.
- All NMS configuration will be lost when the account is converted to Anchor, including:
  - Guest Access Portal
  - Templates
  - Performance Graph Data, etc.
- The process of converting an NMS account to an Anchor account cannot be reversed.

3. Provide your consent by selecting the **I authorize Cambium Networks to make changes to the selected account** checkbox.
4. Click **Request Support** and the following success message is displayed.



The Cambium Support team validates the request and creates an Organization from the NMS and Anchor accounts within 24 hours.

Organizations for CBRS

An Organization allows multiple accounts to share CBRS billing and SAS ID. The Primary Account owns this configuration, and the Secondary Account can optionally share it. Both accounts must authorize the sharing.

Note

- There is only one Primary Account in an Organization.
- CBRS configuration can be set in the Primary Account and optionally shared to Secondary Accounts.

This chapter provides the following information:

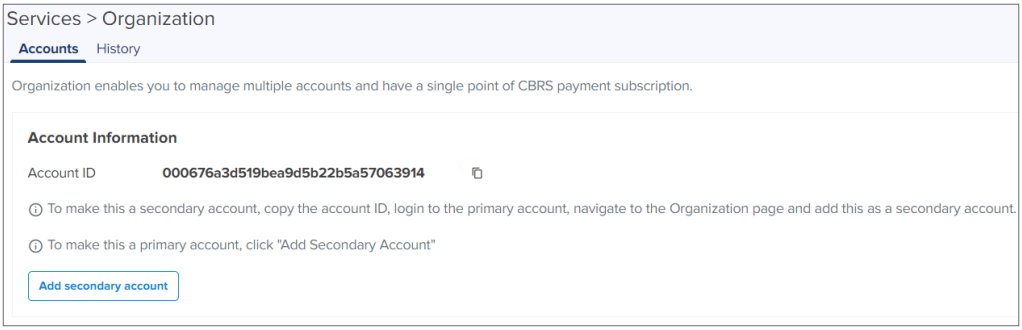
- Create an Organization
- Remove Accounts
- Disable Secondary Account Services
- Edit Services
- Share CBRS Configuration with the On-Premises Instance
- Organization History

Create an Organization

Primary Account

Perform the following steps on the Primary Account:

1. Navigate to **Network Services** > **Organization** > **Accounts**.

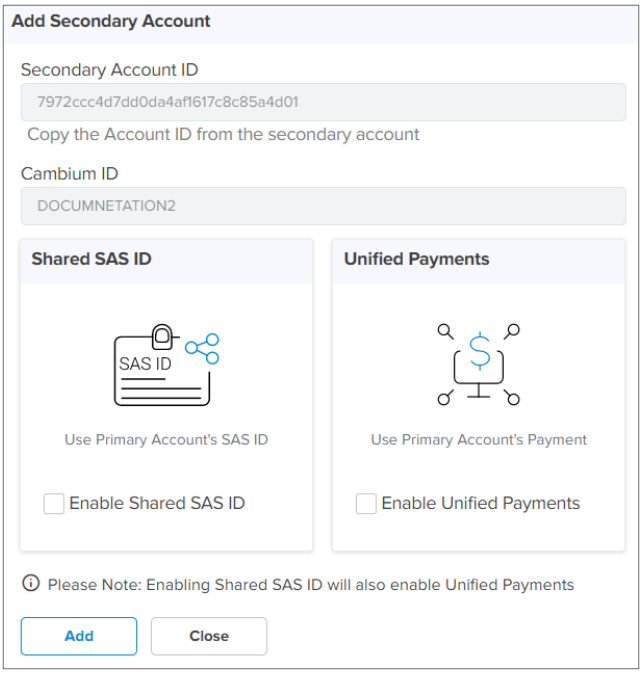


2. Click **Add Secondary Account**.



   Navigate to the planned Secondary Account and copy the Account ID of the Secondary Account using the Copy to Clipboard.

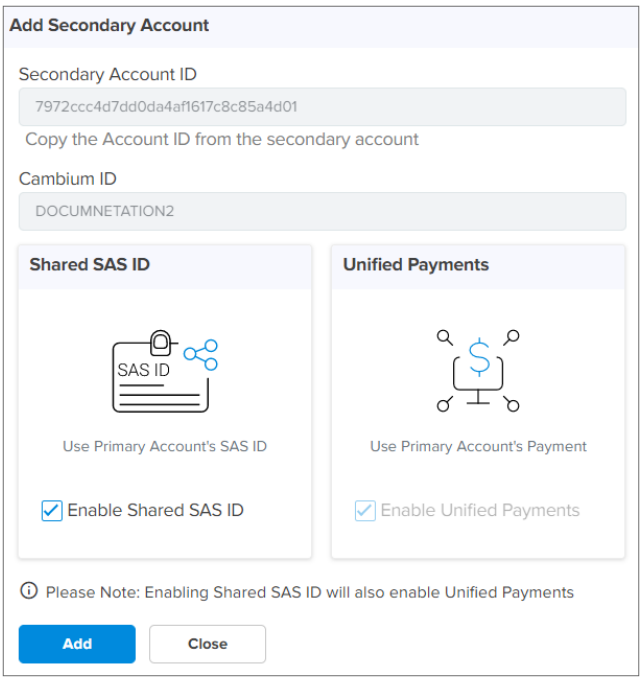
3. Paste the copied **Account ID** in the **Secondary Account ID** text box.
4. Once the Secondary Account is validated, the **Cambium ID** is displayed as shown below.



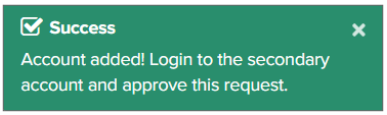
5. The Primary Account can offer services such as:
   - **Shared SAS ID**: This allows the Secondary Account to use the CBRS SAS ID configured in the Primary Account.
   - **Unified Payments**: This allows the Secondary Account to use payment details configured in the Primary Account.

> **Note**
>
> Sharing the SAS ID automatically enables **Unified Payments**.

6. Enable the Services **Shared SAS ID** or **Unified Payments**.



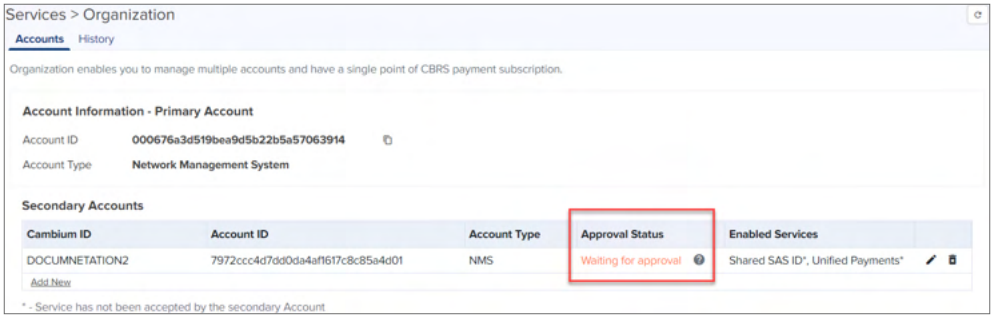
7. Click **Add**. It displays the **Success** message as shown below:



Note

The Secondary Account administrator must approve this request from the Primary Account to join the Organization.

8. 1. In the **Secondary Accounts** table, the **Approval Status** is displayed as **Waiting for approval**.

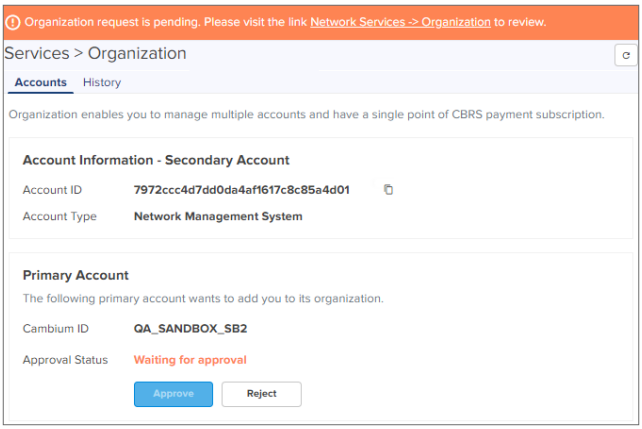


Secondary Account

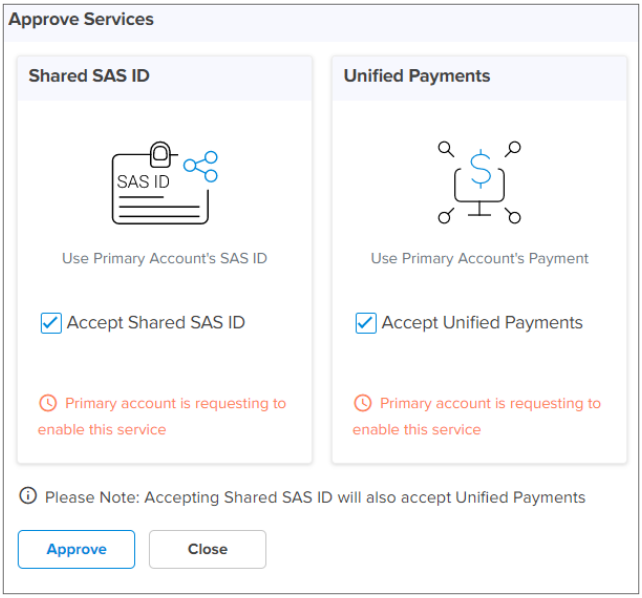
Login to the Secondary Account to complete Organization creation. The Secondary Account must approve the request and authorize the shared services. The Secondary Account can also request additional services (which must be approved by the Primary Account).

Perform the following steps in the Secondary Account:

1. Navigate to **Network Services** > **Organization** > **Accounts**.
2. Click **Approve**.



3. The **Approve Services** window pops up. Review the services requested and click **Approve**.



Additional service requests from the Secondary Account

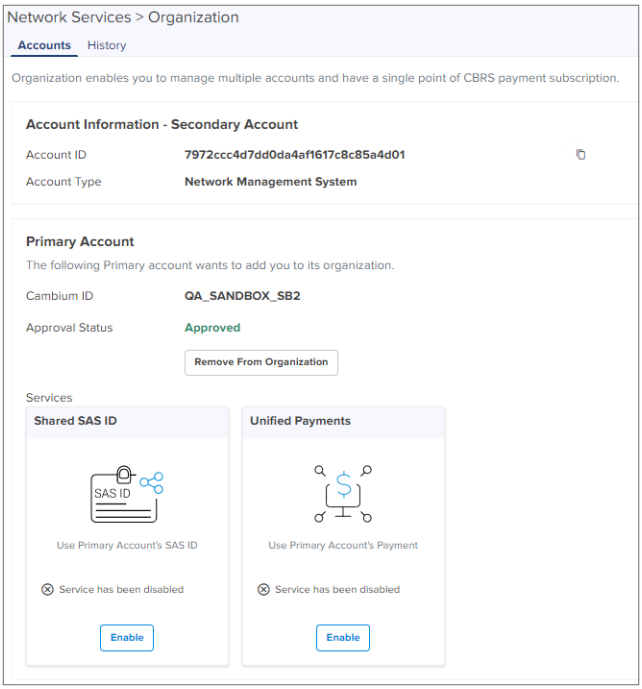
Additional services can be added after the Secondary Account joins the Organization, such as including the Unified Payments Service.

Perform the following steps on the Secondary Account:

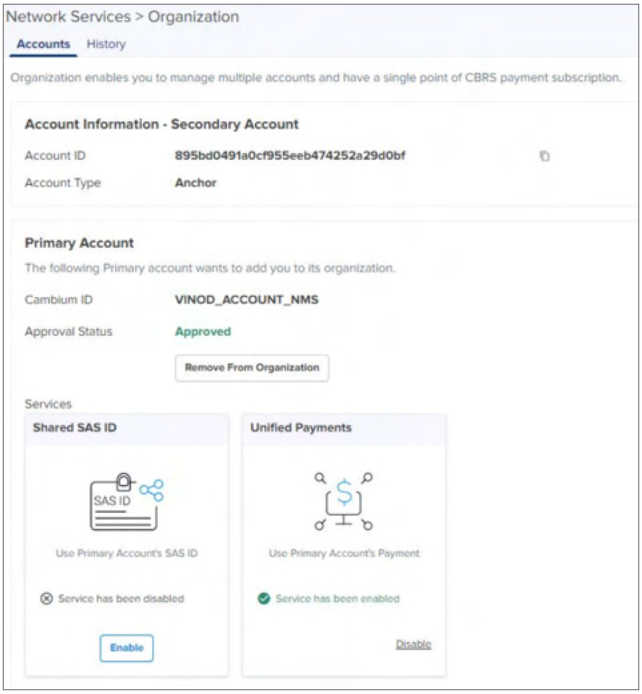
1. Navigate to **Network Services** > **Unified Payments** and click **Enable.**

Note

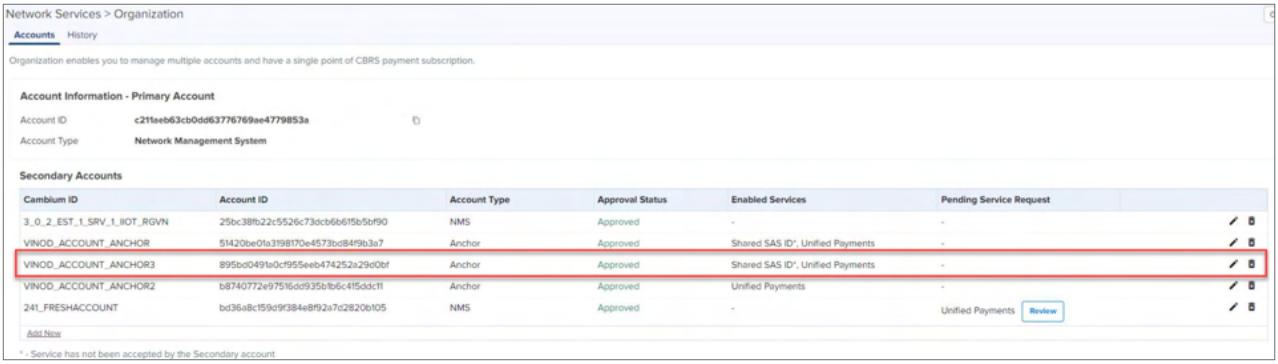
This generates a request to the Primary Account to provide support for Unified Payments.



2. Once the services are enabled and approved in the Primary Account, the following displays in the Secondary Account.



3. The enabled services will be displayed in the Primary Account.

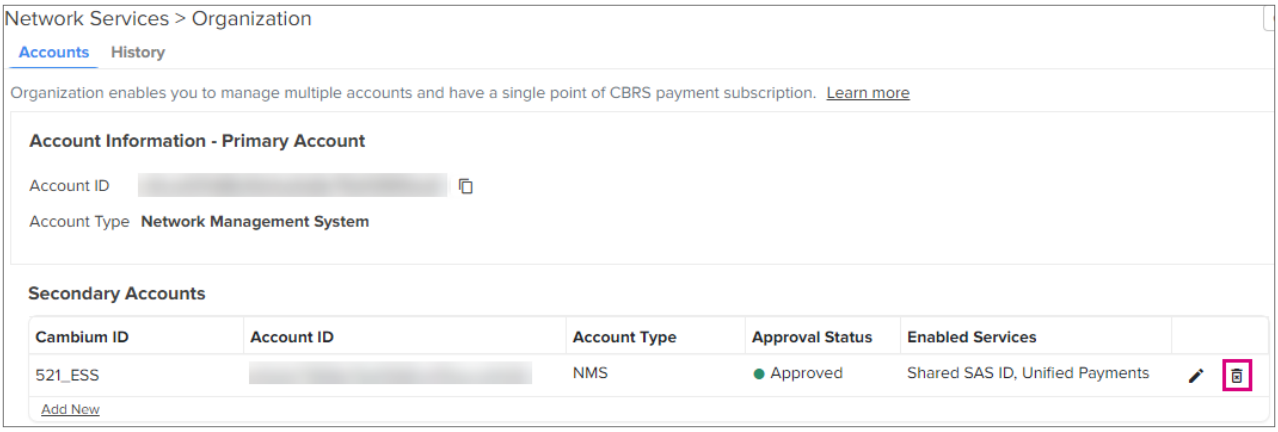


Removing Accounts

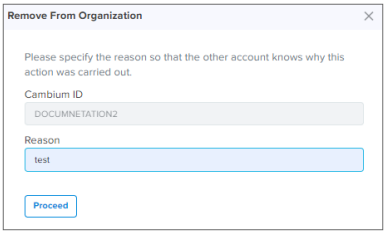
Remove through Primary Account

Perform the following steps on the Primary Account to remove the Secondary Account:

1. Navigate to **Network Services** > **Organization** > **Accounts**.
2. In the **Secondary Accounts**, click the delete (🗑) icon.



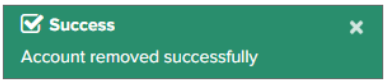
3. The **Remove From Organization** window pop up.



4. Enter the **Reason.**
5. Click **Proceed.**

Without Active Services

- If services such as **Shared SAS ID** or **Unified Payments** are inactive in the Secondary Account, it can be deleted without any approval.
- The following message displays if successful.



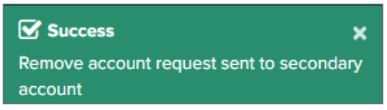
With Active Services

- If services such as **Shared SAS ID** or **Unified Payments** are active in the Secondary Account, the services need to be disabled from the Secondary Account, and the request must be approved by the Secondary Account administrator.

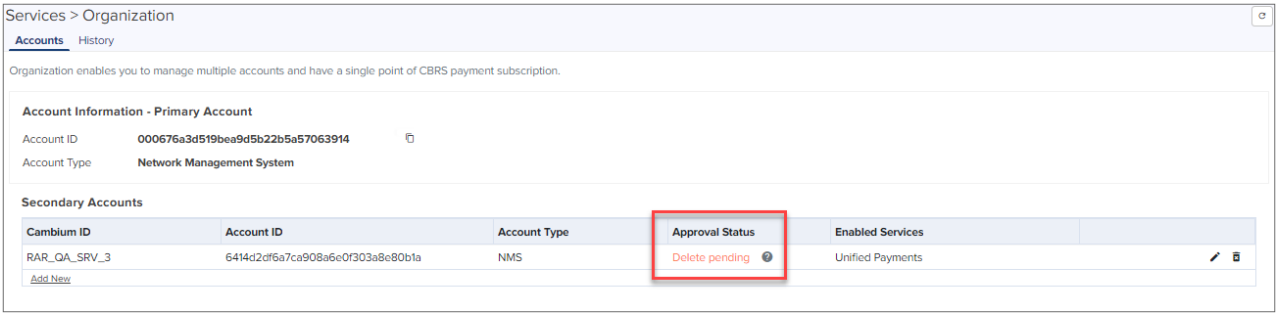
Note

- User needs to disable the active services such as Shared SAS ID and Unified Payments before removing the Secondary Account, or an Error message is shown.
- Shared SAS ID can be removed by contacting Cambium support to deactivate the current CBRS account to stop using Shared SAS ID.
- Active Services will be highlighted in **Green** color.

- The following message displays if successful.



- In the **Secondary Accounts** table, the UI displays the **Approval Status** as **Delete Pending**.

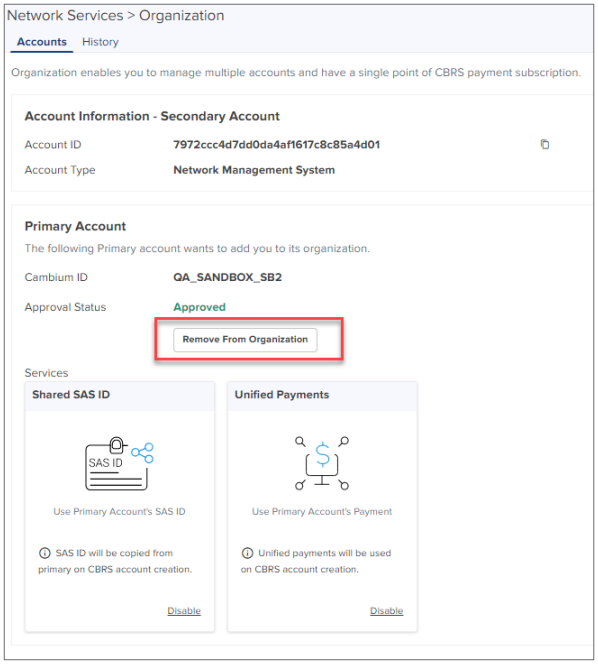


The Secondary Account administrator must approve the remove request from the Primary Account. For more details, refer to Approve Remove Request (with active services).

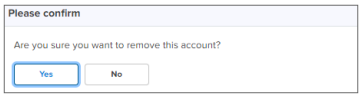
Remove Organization from Secondary Account

Perform the following steps on the Secondary Account to remove an Organization:

1. Navigate to **Network Services** > **Organization** > **Accounts**.
   a. Click **Remove From Organization** (without active services).
      - To remove the Secondary Account from an Organization with no active services.



      - Click **Yes** in **Please confirm** window to remove this account.

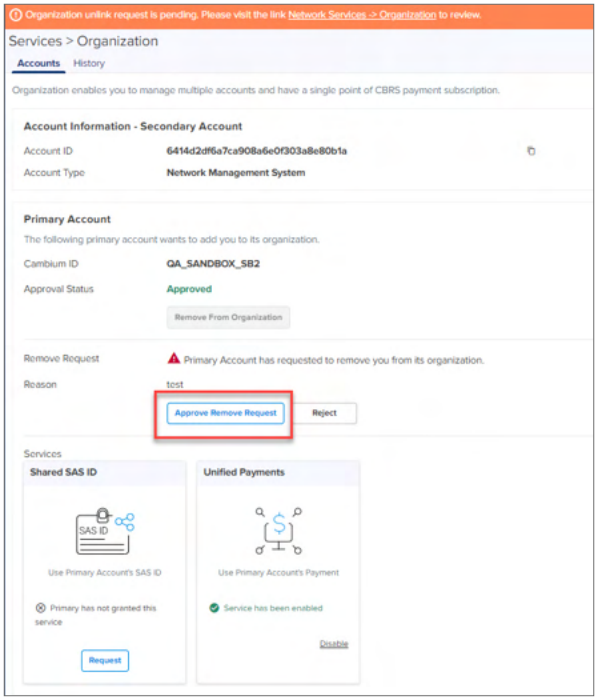


   b. **Approve Remove Request** (with active services).

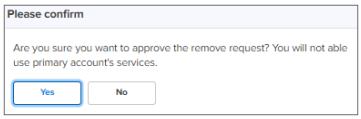


> Note
>
> Disable active services before **Approve Remove Request**.

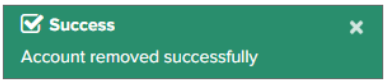
- If the Secondary Account is using services such as **Shared SAS ID** or **Unified Payments**, the following message displays.



- Click **Yes** in **Please confirm** window to approve the request.



2. The following message displays if successful.

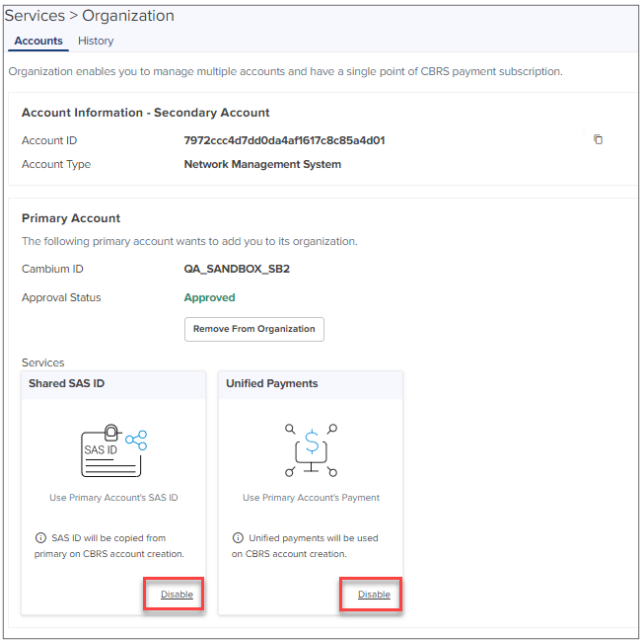


Disable Secondary Account services

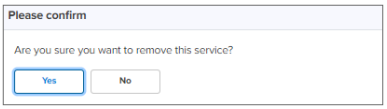
With no active services

The Secondary Account user can disable services without leaving the Organization.

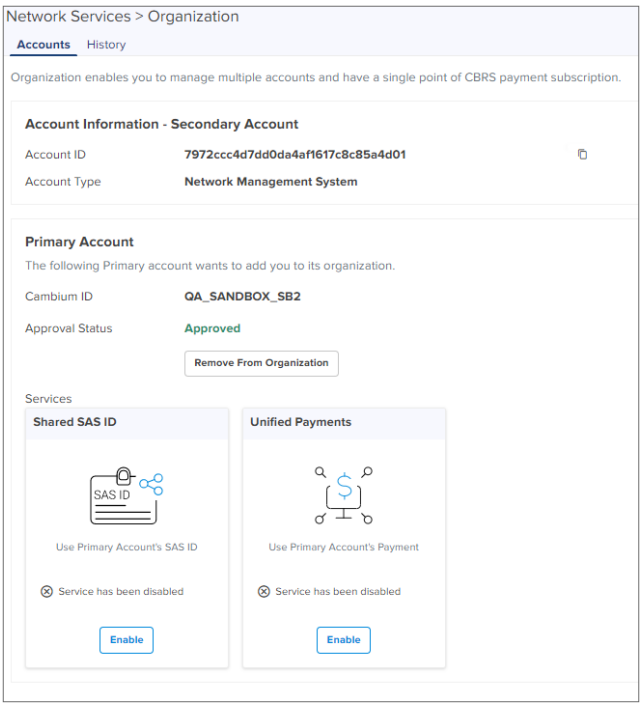
1. Navigate to **Services** > **Organization** > **Accounts** and select **Services.**
2. Click **Disable**.



3. Click **Yes** in the **Please confirm** window.



4. After disabling, the following displays.



5. Click **Enable** to reactivate the services.

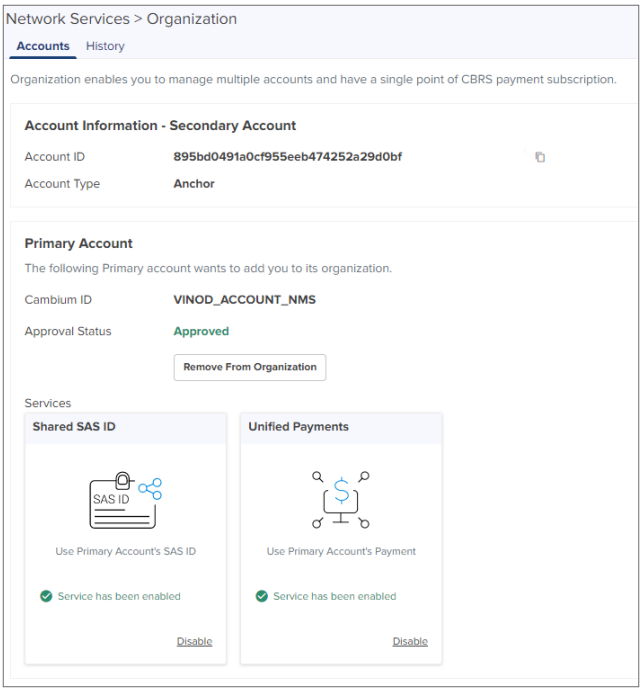
With active shared SAS ID services

Note

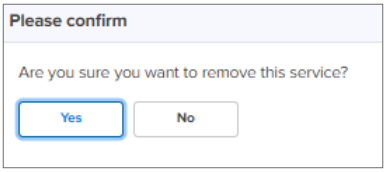
Active Services are highlighted in **Green** color.

The Secondary Account user can disable the **Shared SAS ID** services.

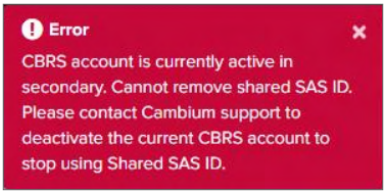
1. Navigate to **Services** > **Organization** > **Accounts** and select **Services.**



2. Click **Disable** in the **Shared SAS ID.**
3. Click **Yes** in the **Please confirm** window.



4. If CBRS account is active in Secondary Account, while disabling it displays the following error message.



If an **Error** message pops up, the user needs to raise a request to Cambium Support for the SAS vendor cancellation. Cambium Support will disable the CBRS services and deregister all devices associated to the Secondary Account.

Once disabled, the Secondary Account user can view the SAS vendor page and create a new CBRS account as shown below.



For further information on creating a new CBRS account, refer to CBRS.

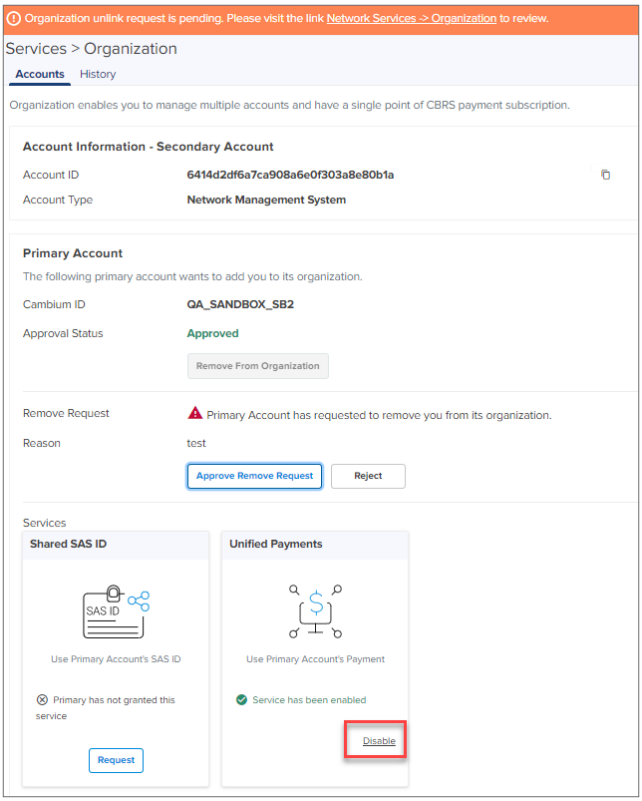
Note

Services in the Secondary Account cannot be disabled unless CBRS is inactive in Secondary Account. Contact Cambium Support to disable CBRS operation or change SAS Vendor.

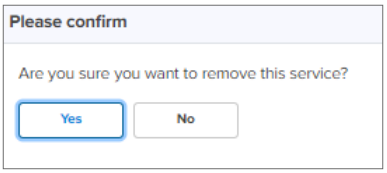
With active Unified Payments

The Secondary Account user can disable Unified Payments.

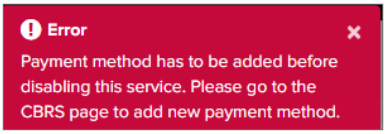
1. Navigate to **Services > Organization > Accounts** and select **Services.**



2. Click **Disable** within **Unified Payments**.
3. Click **Yes** in **Please confirm** window.



4. If **Unified Payments** is active in CBRS of the Secondary Account, it displays an **Error** message.



If this happens, the user needs to add new CBRS payment details into the Secondary Account.



For further information on Payment details, refer to CBRS.

The user can disable the **Unified Payments** once the new payment details are added successfully to the Secondary Account.

Edit Services

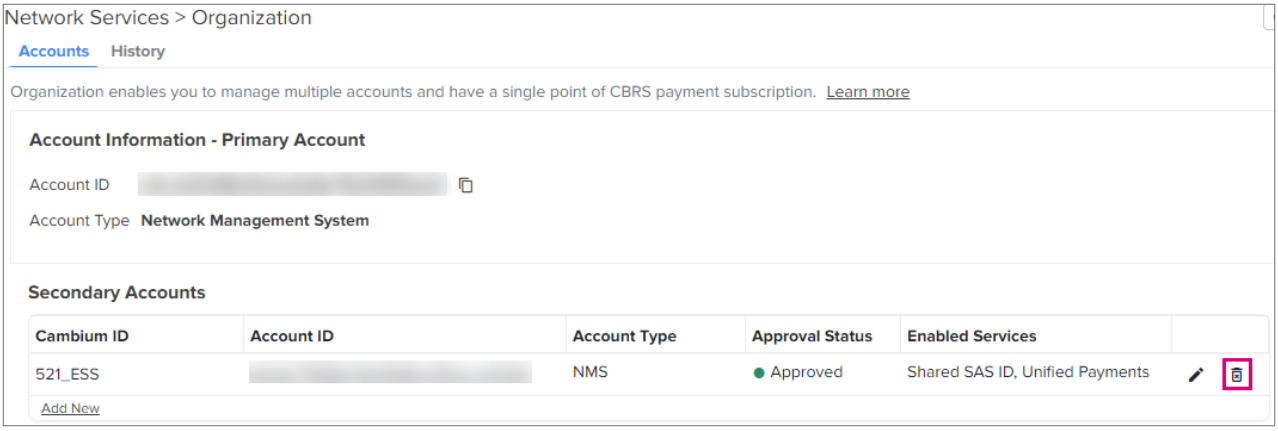
Enable services in the Primary Account

The Primary Account can edit or disable services shared with the Secondary Account as shown below:

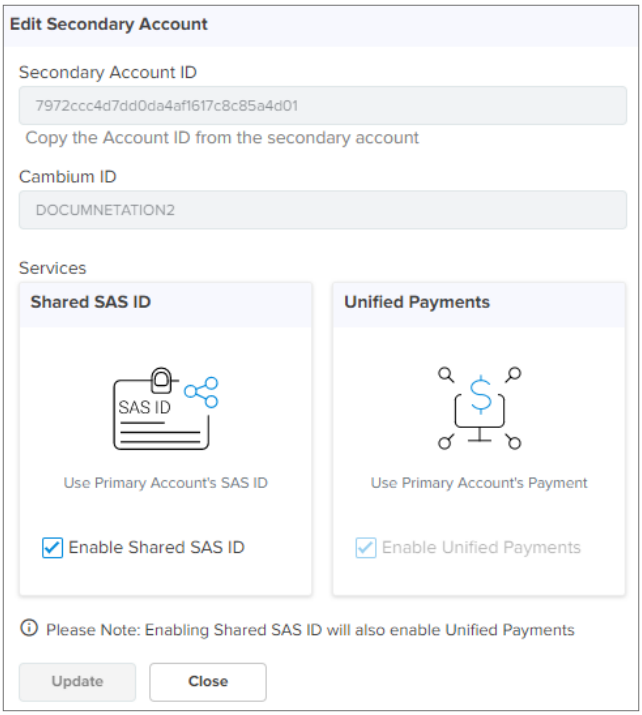
Note

When the services are active in CBRS of the Secondary Account, the Primary Account cannot disable those services.

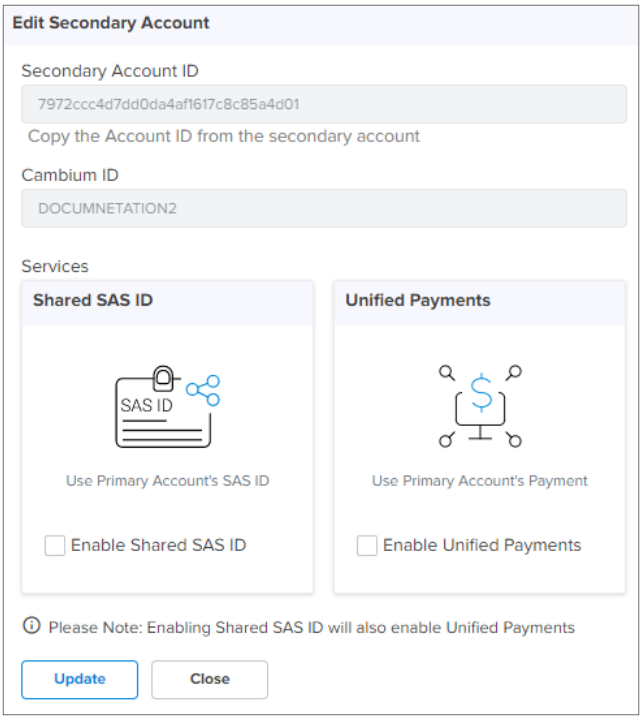
1. Navigate to **Accounts** > **Secondary Accounts** tab.
2. Click Edit (✎) icon.



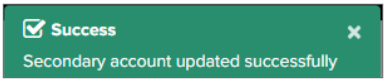
3. **Edit Secondary Account** window pops up.



4. Disable the **Services** and click **Update**.



5. The following message displays if successful.

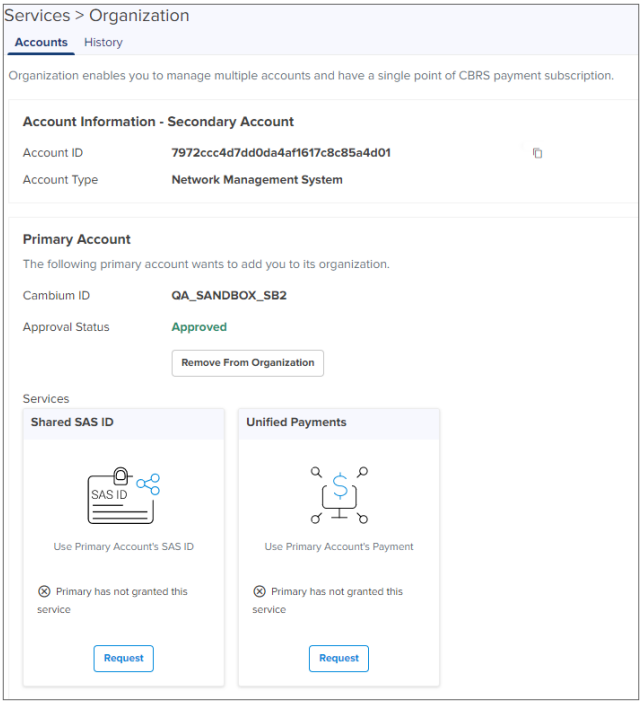


Request services from Secondary Account

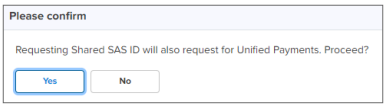
If the services are disabled, the Secondary Account needs to make a request to the Primary Account to activate them.

To request activation, perform the following on the Secondary Account:

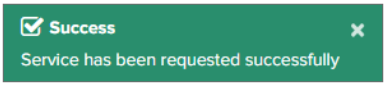
1. Navigate to **Network Services** > **Organization** > **Accounts**.
2. Click **Request**.



3. Click **Yes** in **Please confirm** window.



4. It displays the **Success** message as shown below:



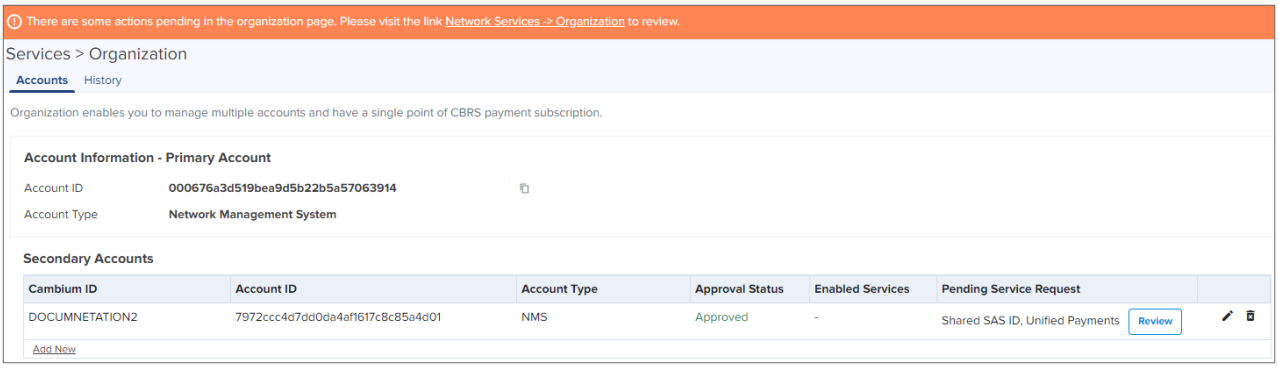
5. Once requested, login to the **Primary Account** page and **Approve** the request.

The Primary Account administrator must approve this request from the Secondary Account in order to enable the services.

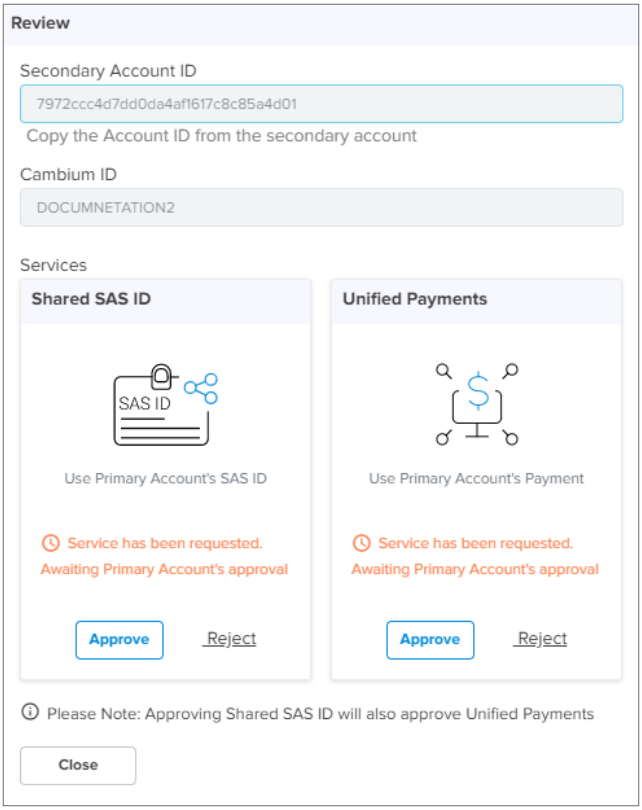
Review service request in Primary Account

Perform the following steps on the Primary Account.

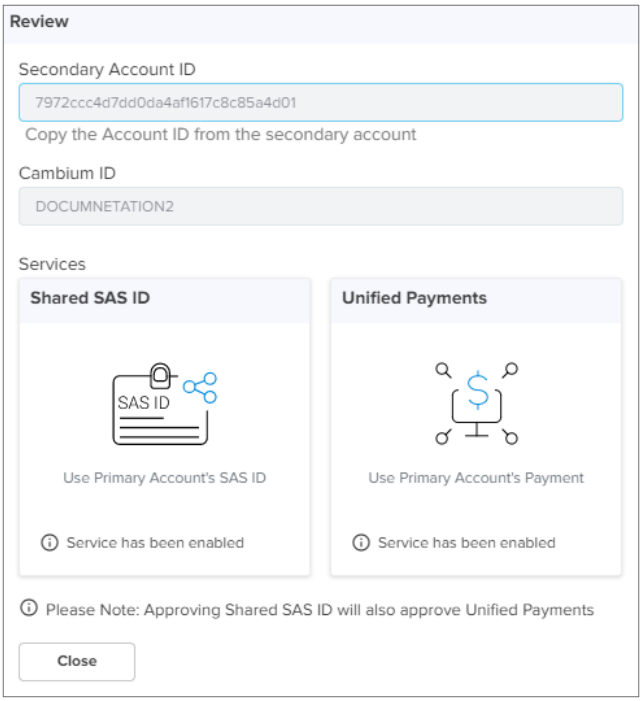
1. Navigate to **Services** > **Secondary Accounts** tab.
2. Click **Review** in **Pending Service Request**.



3. The **Review** window pops up. Click **Approve**.



4. Once approved, the requested services are enabled in the **Secondary Account.**

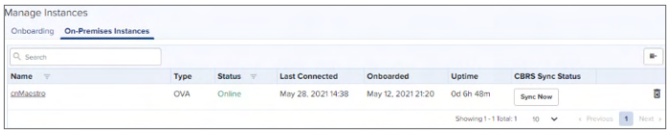


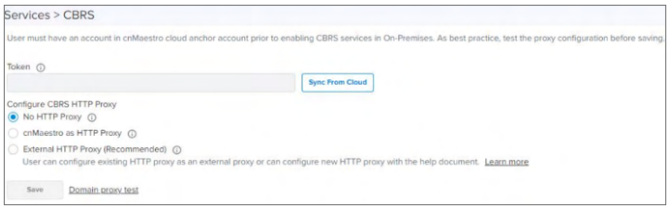
Share CBRS Configuration with the On-Premises Instance

Note

Starting with version 3.0.3, cnMaestro supports synchronizing CBRS Configuration to On-Premises instance.

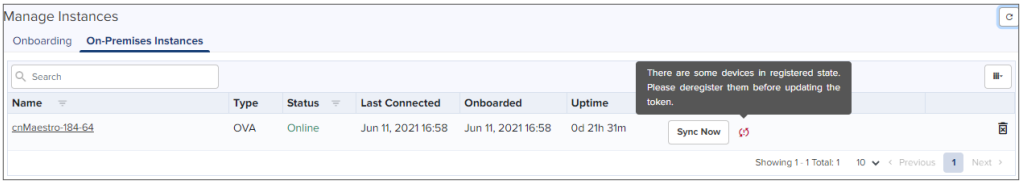
Once On-Premises is connected to the Anchor Account, the user can synchronize CBRS details (SAS ID, Token) to the cnMaestro On-Premises instance to register CBRS devices.





- If the user shares (sync) CBRS details configured on Anchor account to connected On-Premises and if any devices are registered in On-Premises with different CBRS token or SAS ID it displays the deregister error as

shown below.

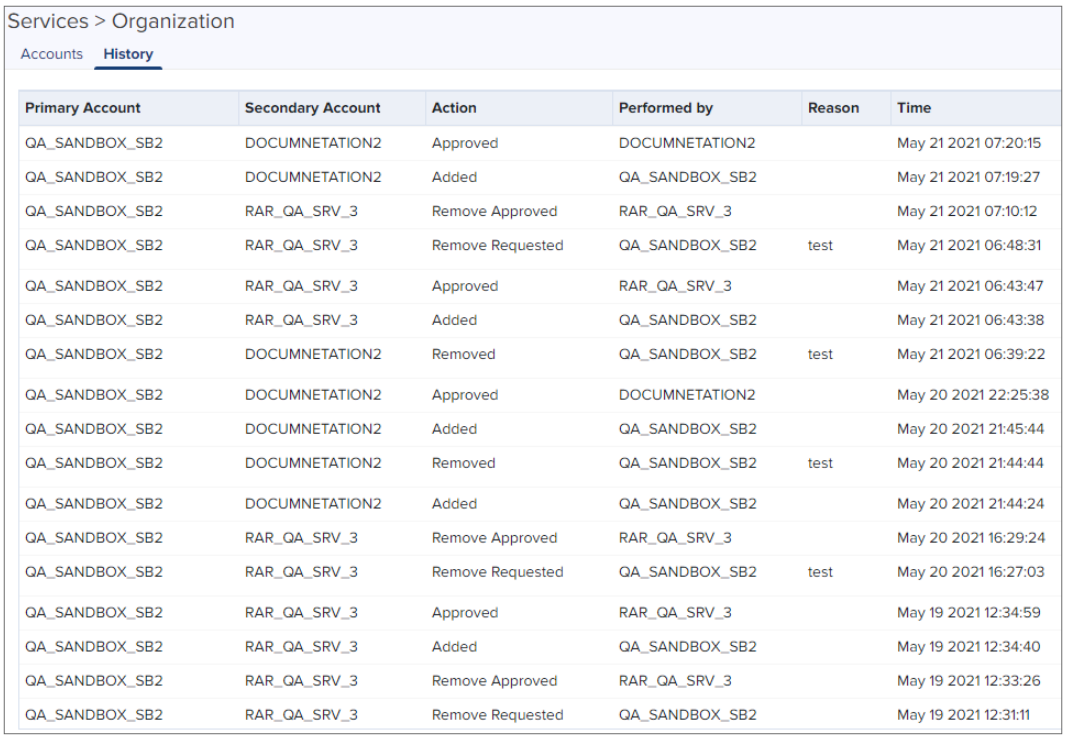


Organization History

In Organization History user can view changes to the Organization status over time. This includes details of Primary Account, Secondary Account, Action, Performed by, and Reason.

To view Organization History:

Navigate to **Network Services** > **Organization** > **History** tab.



Primary Account	Secondary Account	Action	Performed by	Reason	Time
QA_SANDBOX_SB2	DOCUMNETATION2	Approved	DOCUMNETATION2		May 21 2021 07:20:15
QA_SANDBOX_SB2	DOCUMNETATION2	Added	QA_SANDBOX_SB2		May 21 2021 07:19:27
QA_SANDBOX_SB2	RAR_QA_SRV_3	Remove Approved	RAR_QA_SRV_3		May 21 2021 07:10:12
QA_SANDBOX_SB2	RAR_QA_SRV_3	Remove Requested	QA_SANDBOX_SB2	test	May 21 2021 06:48:31
QA_SANDBOX_SB2	RAR_QA_SRV_3	Approved	RAR_QA_SRV_3		May 21 2021 06:43:47
QA_SANDBOX_SB2	RAR_QA_SRV_3	Added	QA_SANDBOX_SB2		May 21 2021 06:43:38
QA_SANDBOX_SB2	DOCUMNETATION2	Removed	QA_SANDBOX_SB2	test	May 21 2021 06:39:22
QA_SANDBOX_SB2	DOCUMNETATION2	Approved	DOCUMNETATION2		May 20 2021 22:25:38
QA_SANDBOX_SB2	DOCUMNETATION2	Added	QA_SANDBOX_SB2		May 20 2021 21:45:44
QA_SANDBOX_SB2	DOCUMNETATION2	Removed	QA_SANDBOX_SB2	test	May 20 2021 21:44:44
QA_SANDBOX_SB2	DOCUMNETATION2	Added	QA_SANDBOX_SB2		May 20 2021 21:44:24
QA_SANDBOX_SB2	RAR_QA_SRV_3	Remove Approved	RAR_QA_SRV_3		May 20 2021 16:29:24
QA_SANDBOX_SB2	RAR_QA_SRV_3	Remove Requested	QA_SANDBOX_SB2	test	May 20 2021 16:27:03
QA_SANDBOX_SB2	RAR_QA_SRV_3	Approved	RAR_QA_SRV_3		May 19 2021 12:34:59
QA_SANDBOX_SB2	RAR_QA_SRV_3	Added	QA_SANDBOX_SB2		May 19 2021 12:34:40
QA_SANDBOX_SB2	RAR_QA_SRV_3	Remove Approved	RAR_QA_SRV_3		May 19 2021 12:33:26
QA_SANDBOX_SB2	RAR_QA_SRV_3	Remove Requested	QA_SANDBOX_SB2		May 19 2021 12:31:11

LTE

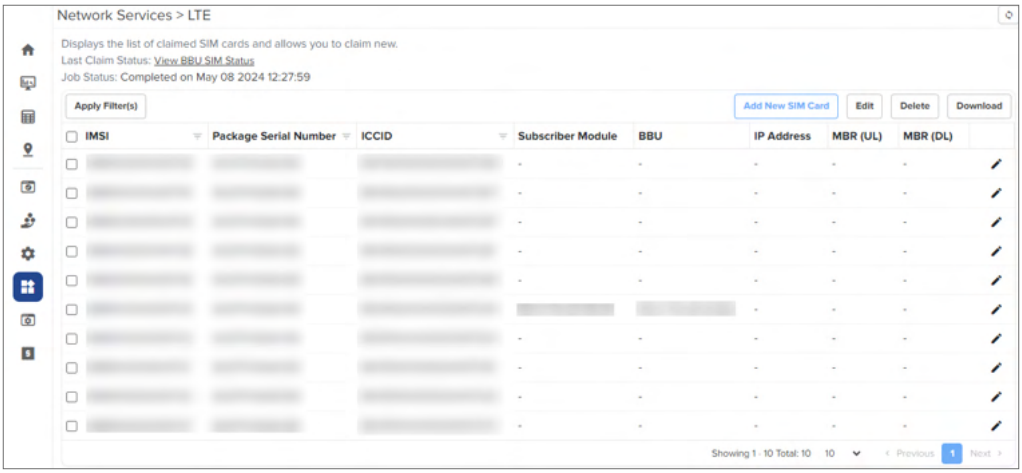
cnMaestro supports LTE as part of its cnMaestro deployment. LTE allows customers to onboard the SM with IMSI into cnMaestro.

System access in cnRanger is dependent on installation of SIM credentials on every BBU in the operator network. To ease the operations aspects of SIM card management, cnMaestro provides utilities for claiming, managing, and distributing Cambium Networks cnRanger SIM card credentials (3rd party SIM cards are not currently supported on cnRanger).

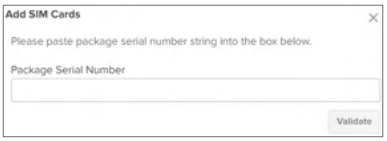
Adding SIM Cards

To add a SIM card, complete the following steps:

1. Navigate to **Network Services > LTE**.



2. Click **Add New SIM Card**. The following window appears.



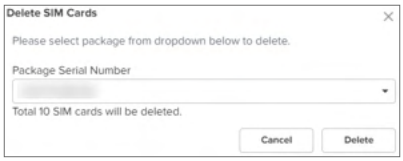
3. Enter appropriate **Serial Number** of SIM package and click **Validate**.
4. After successful validation of the serial number, click **Add**.

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.



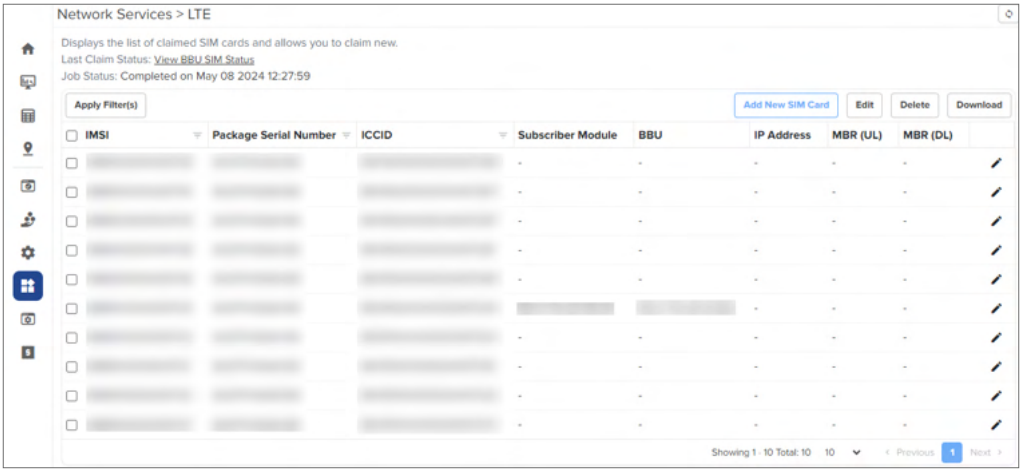
Note

IMSI numbers get deleted with the mapped Serial Number.

Update SIM Details

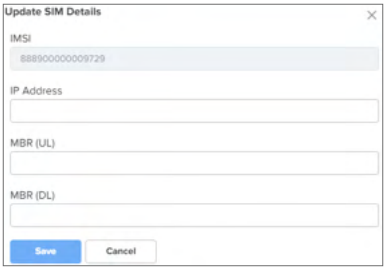
User can edit the SIM details as follows.

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.

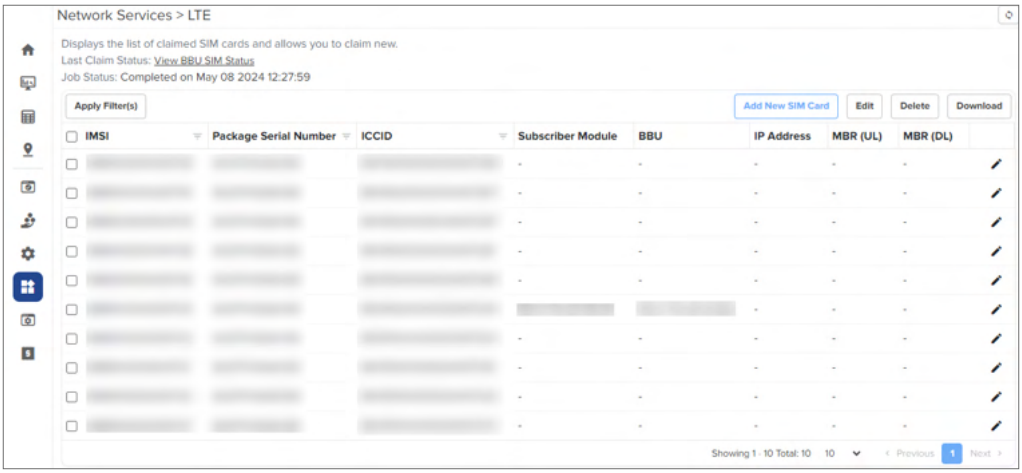


3. Enter a valid **IP Address**.
4. Enter the **MBR (UL)** and **MBR (DL)**.
5. Click **Save**.

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.**



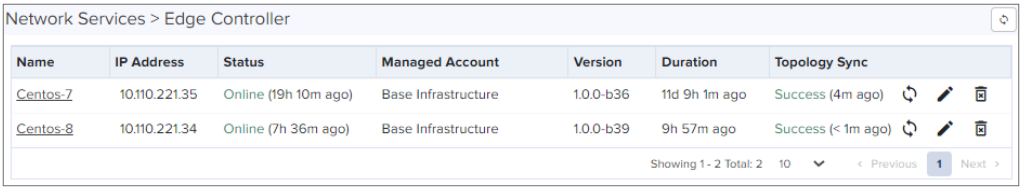
Managing Edge Controller

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 656.

   Figure 656 *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

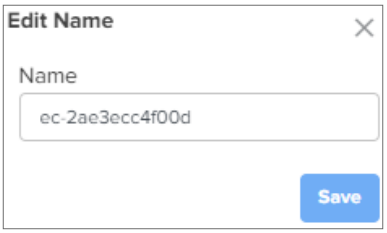
Topology Sync

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.



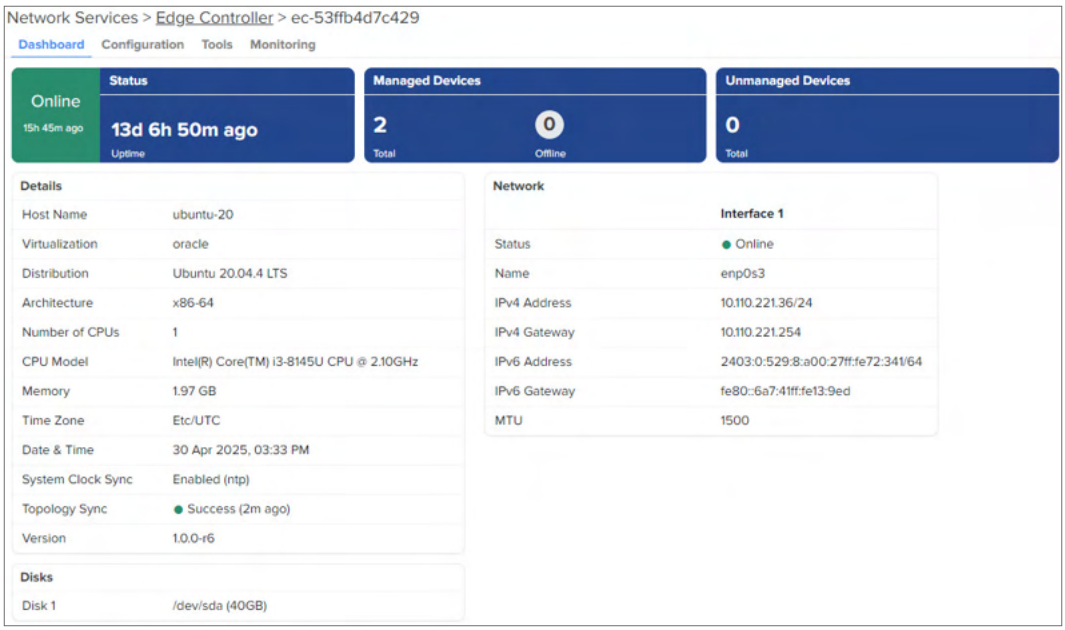
2. Click **Yes**.

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 657.

Figure 657 *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 172.

Figure 658 *Edge Controller and PTP 820/850 devices status*

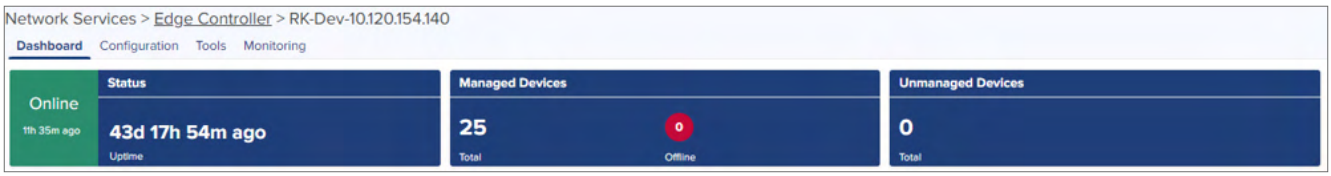


Table 172 *Fields in the Edge Controller dashboard*

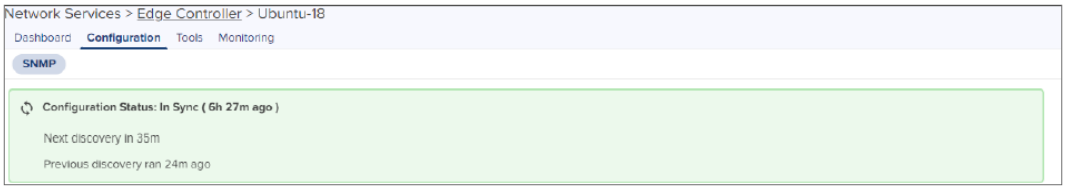
Field	Description
Host name	Name of the host.
Virtualization	Type of virtualization such as VMware or Oracle.
Distribution	Type of distribution such as Ubuntu and CentOS versions.
Architecture	CPU and Operating System installed.
Number of CPUs	Total number of CPUs utilized.
CPU Model	Type of CPU model.
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 659.

Figure 659 *Configuration Status*



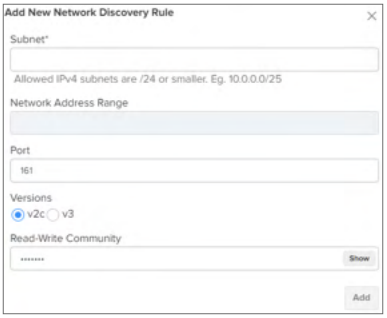
Rules

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.

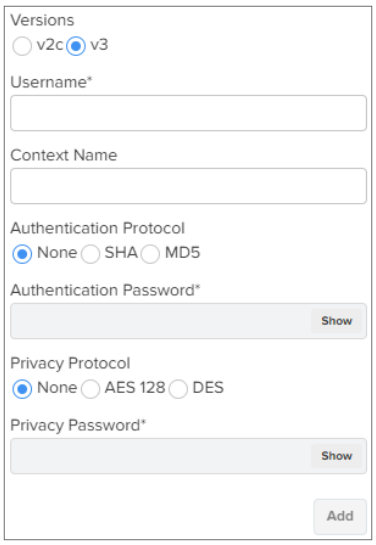
   b. Click **Add.**

   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.

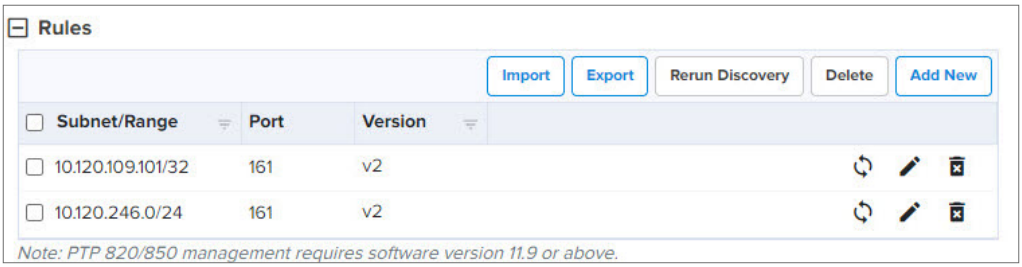
c. Choose any one of the **Authentication Protocol.**
   - None
   - SHA
   - MD5

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.**

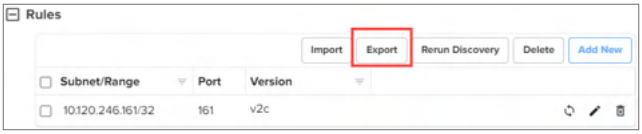


3. Click **Import**.

Export

To export SNMP rules, perform the following steps:

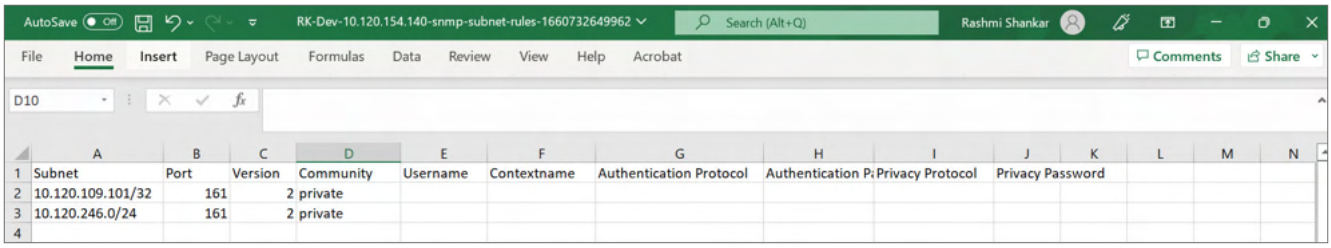
1. Select one or more SNMP rules required to export.
2. Click **Export**.



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:

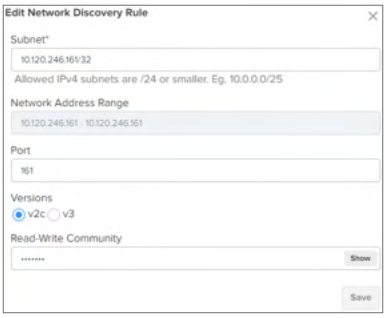
1. Select one or more SNMP rules in the table.
2. Click **Delete**, to delete one or more entries in the table or click **Delete** (🗑) icon to delete specific rule in the table.

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.**

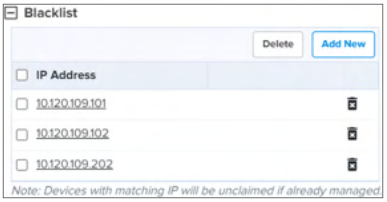


Add Blacklist IP Address window appears.



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:

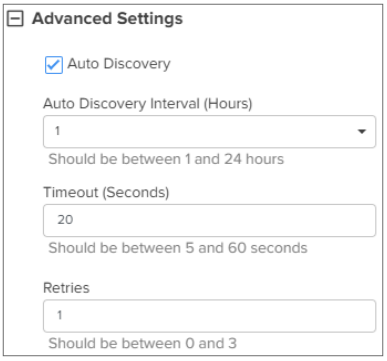
Note

- 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

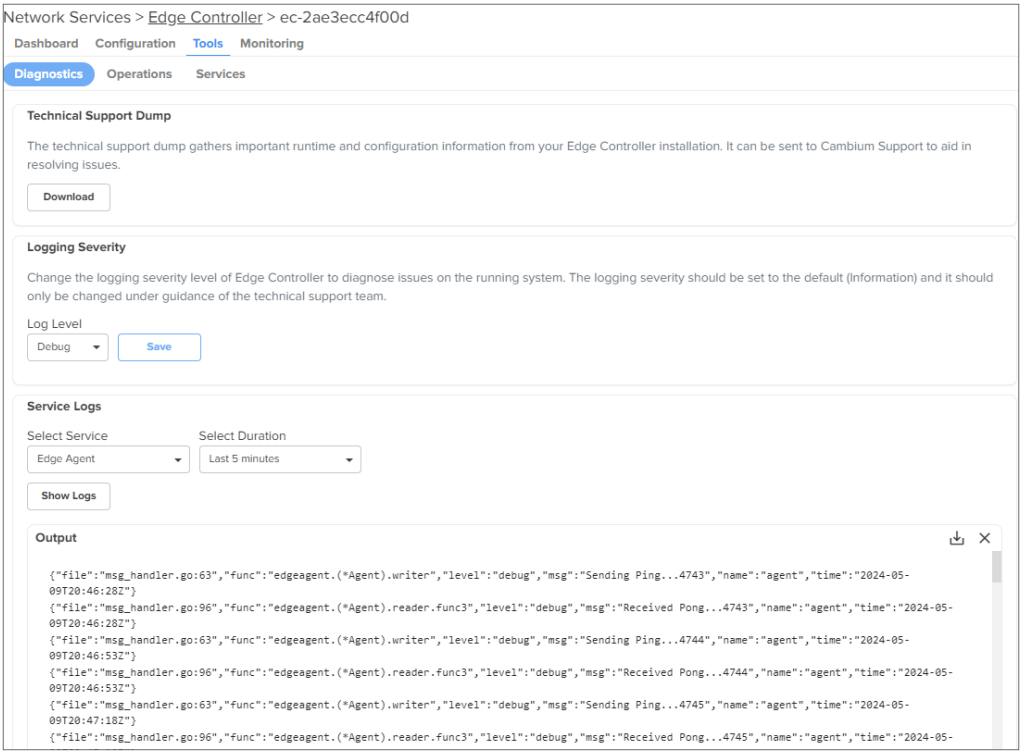
Diagnostics page allows you to gather technical support dump which can be downloaded and sent to Cambium Networks support team.

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

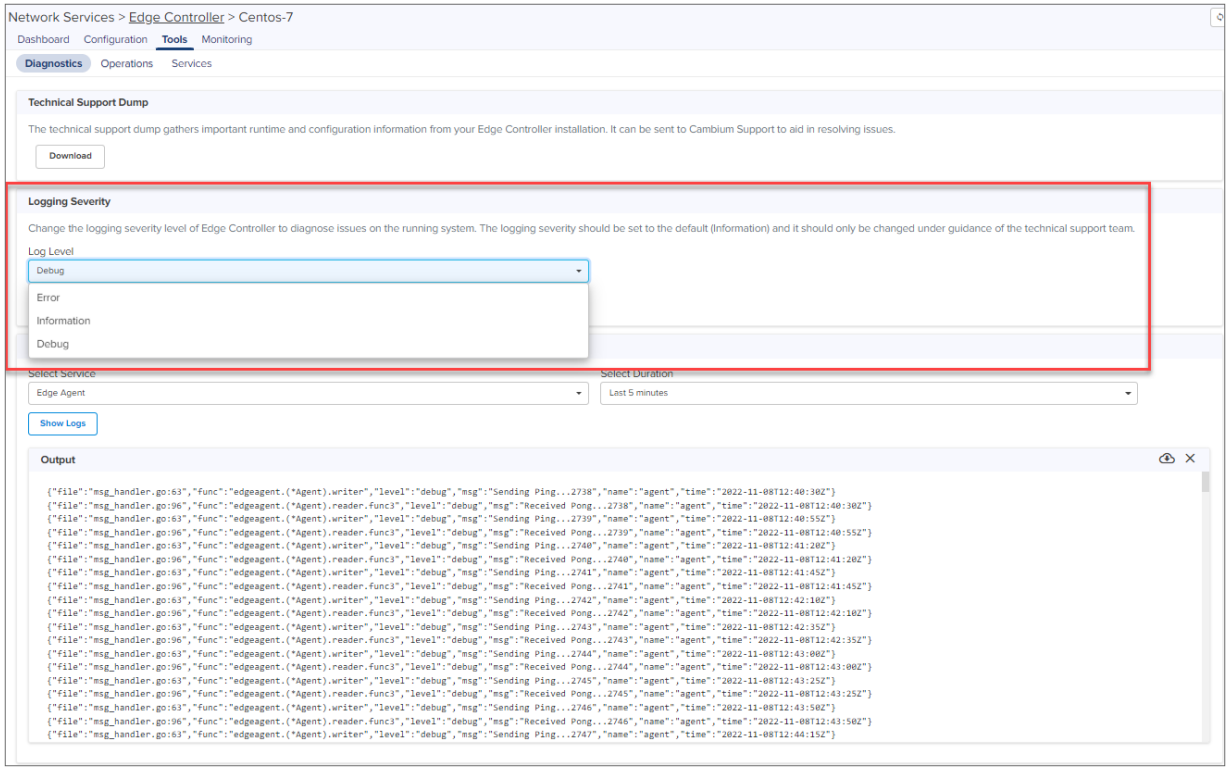


Logging Severity

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.

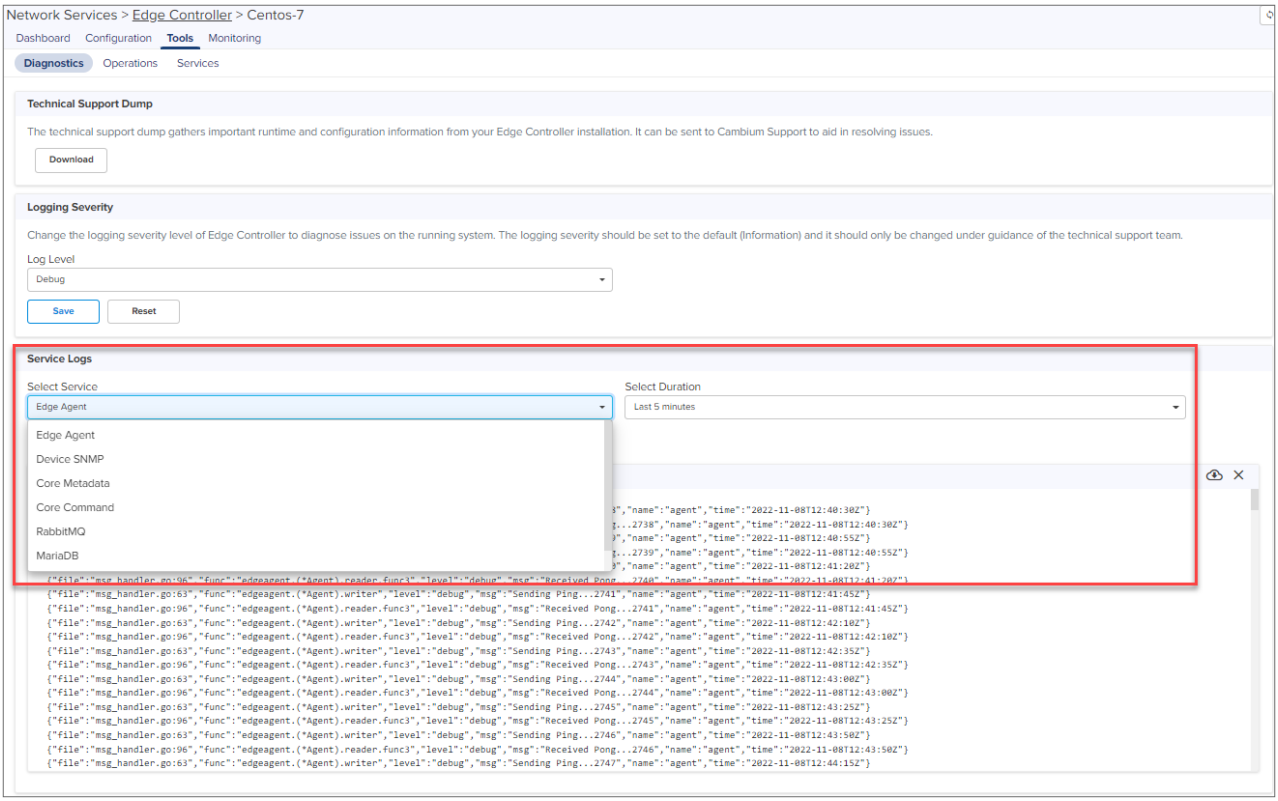
1. Select **Service** and **Duration** from the dropdown.

   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:

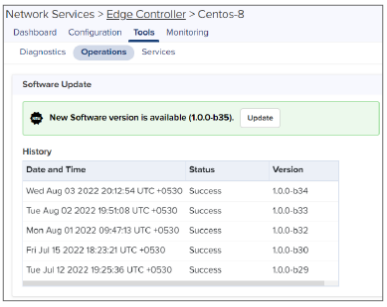


3. Click download ( ) icon to download the generated output.
4. Click clear (✕) icon to clear the output.

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.

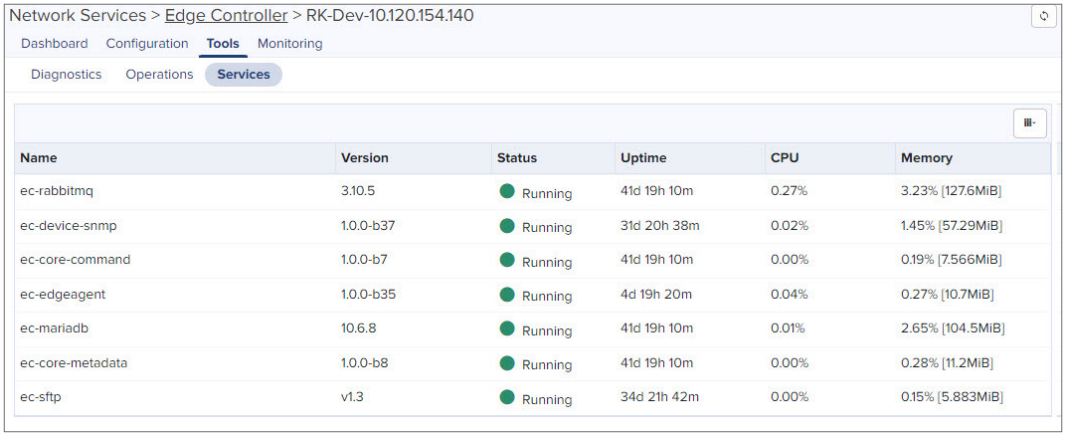
1. 1. Navigate to **Tools > Operations**.
2. 2. Click **Check for new software update**, checks for any new available software update.



Services

In **Services** page you can view the services running in the Edge Controller.

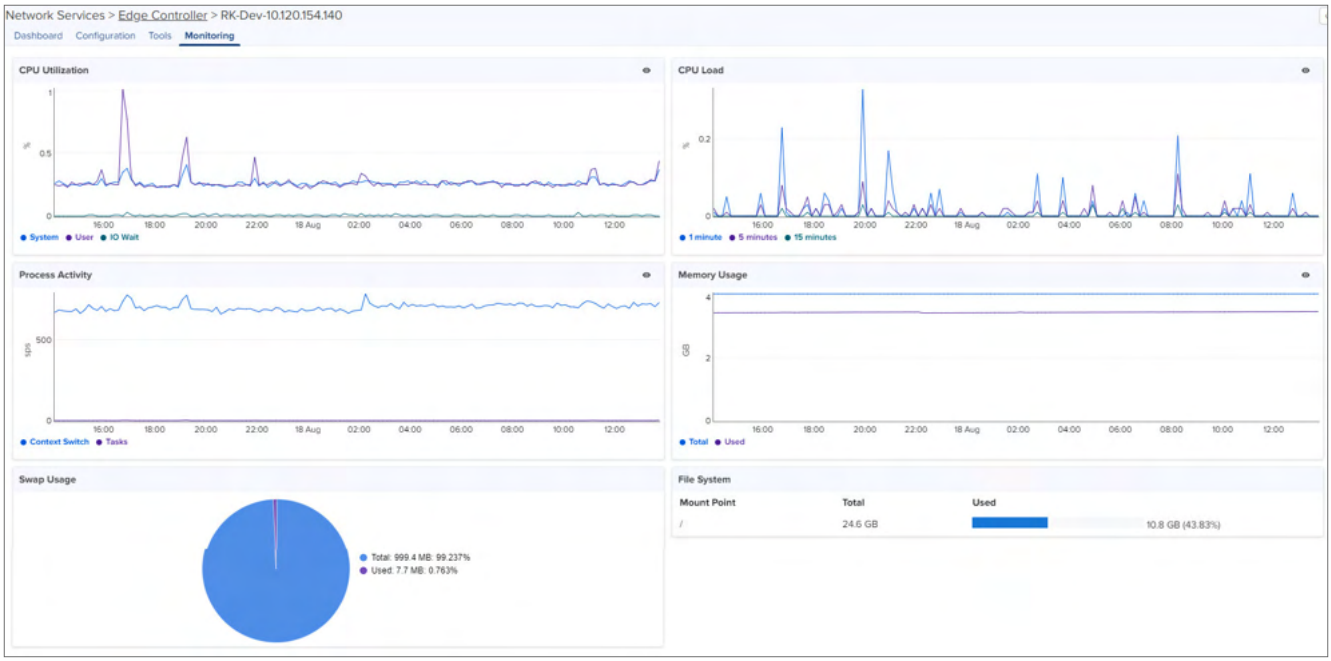
Figure 660 *Services*



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.**

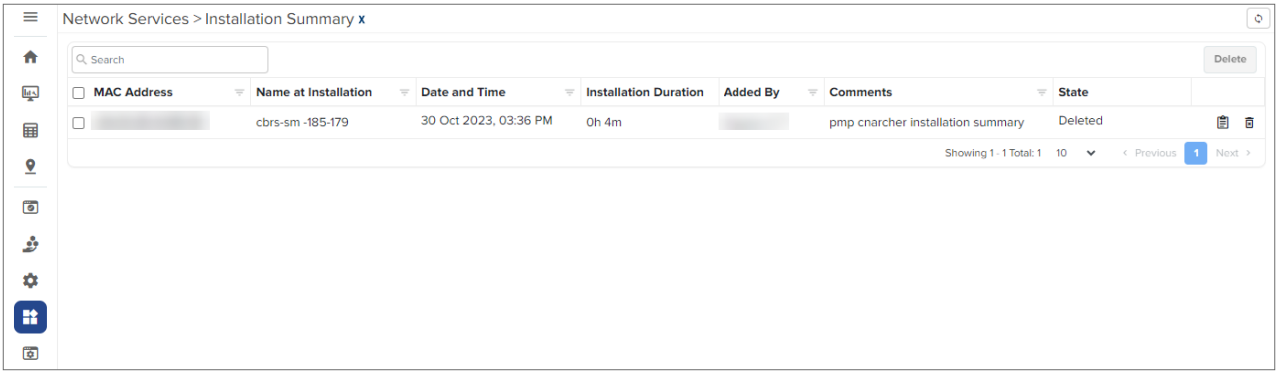


Table 173 *Fields in Installation Summary*

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.

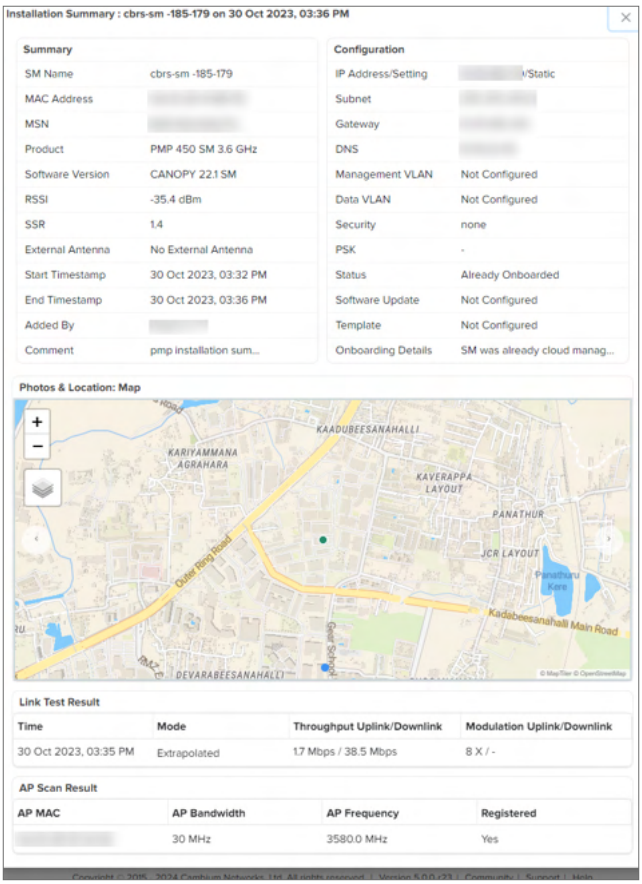


Table 174 *Summary fields in Installation Summary*

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 175 *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 176 *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.

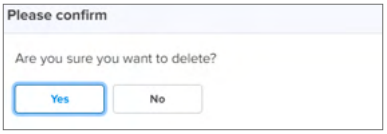
Table 177 *Fields in AP Scan Result*

Field	Description
AP MAC	MAC address of the AP.

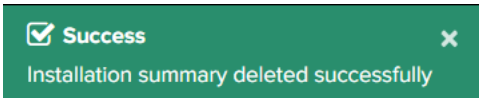
Table 177 *Fields in AP Scan Result*

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**.

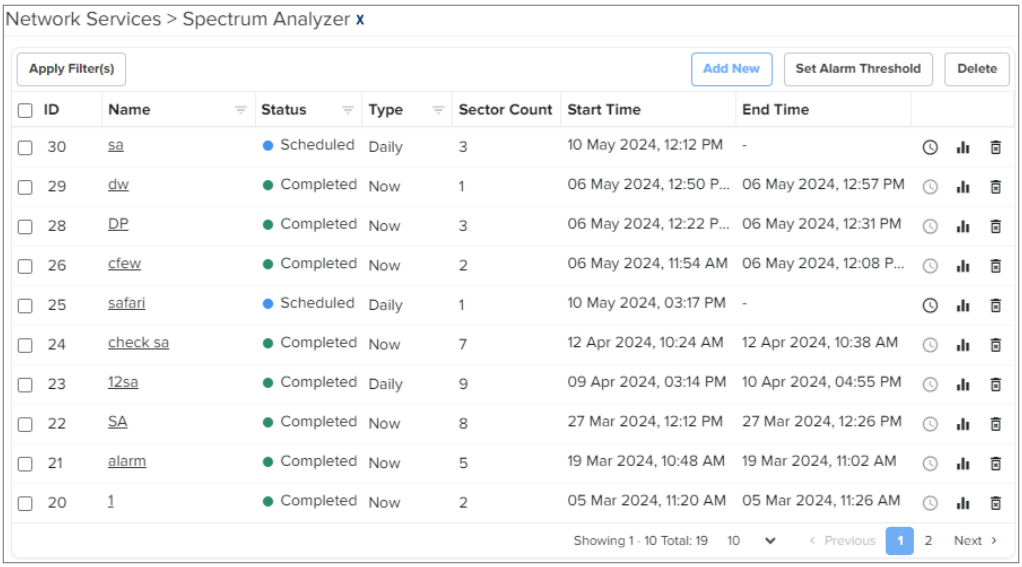


Table 178 *Fields in Spectrum Analyzer*

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.

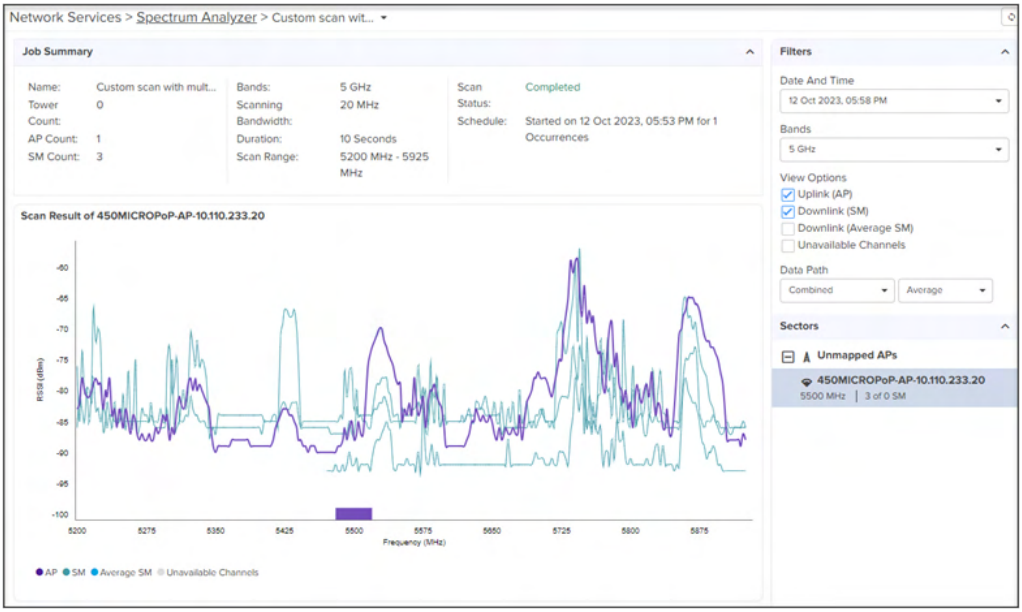


Table 179 *Job Summary parameters*

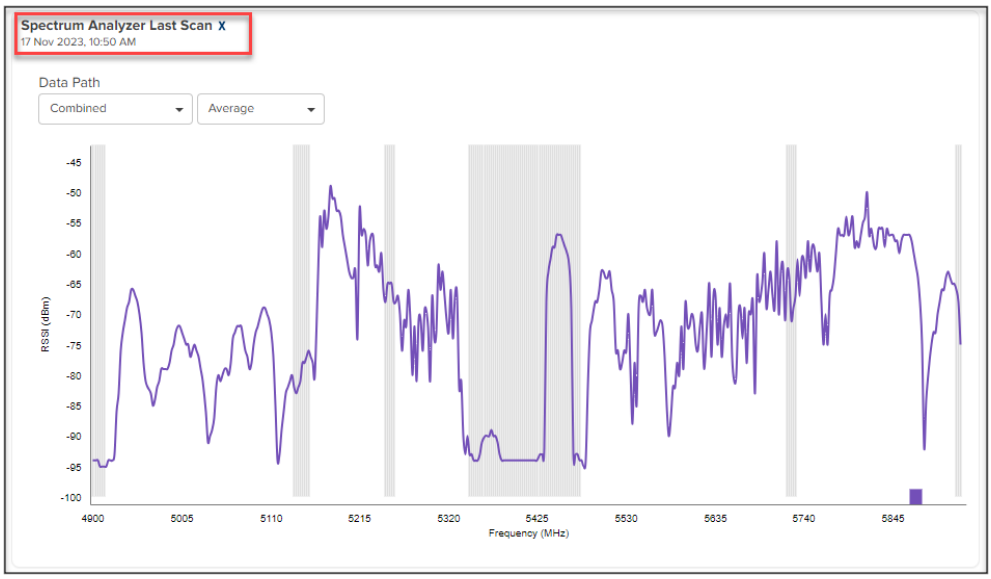
Field	Description
Name	The user-assigned name for the analysis job.
Tower Count	The number of towers included in the analysis.
AP Count	The number of APs in the analysis.
SM Count	The number of SMs in the analysis.
Bands	The frequency bands under analysis.
Scanning Bandwidth	The width of the frequency 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 180 *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:

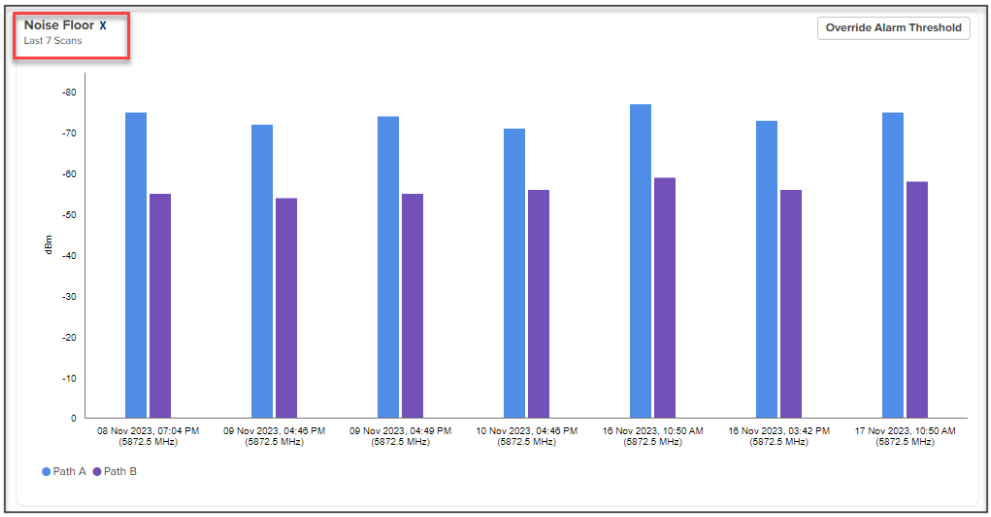
a. Navigate to PMP device **Dashboard** > **Spectrum Analyzer Last Scan**.



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.

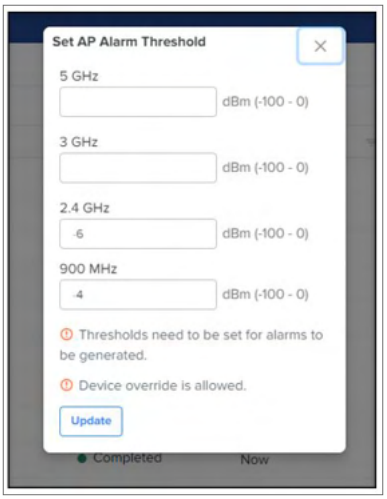


e. **Unmapped APs** display any APs that are not assigned to a tower.

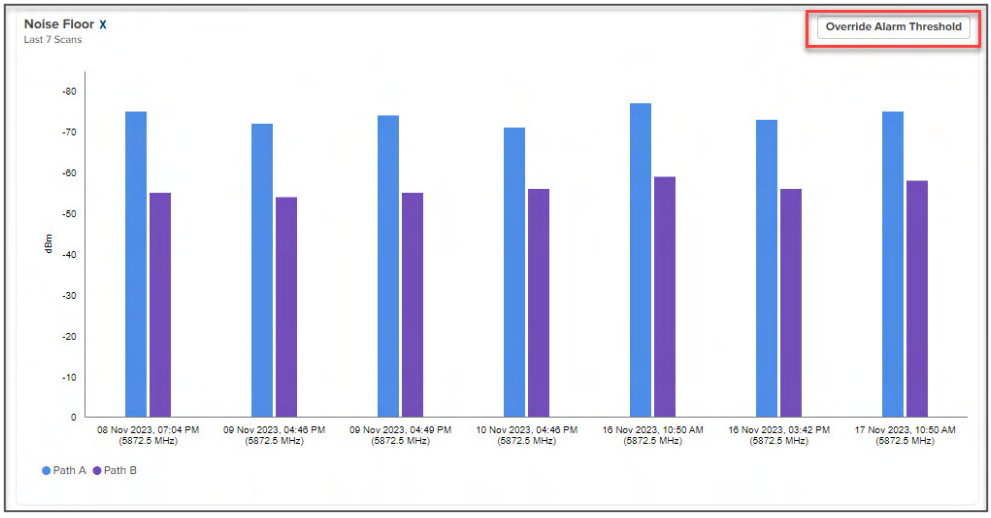
f. Click **Delete** icon on the top right corner to delete a job.

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**.

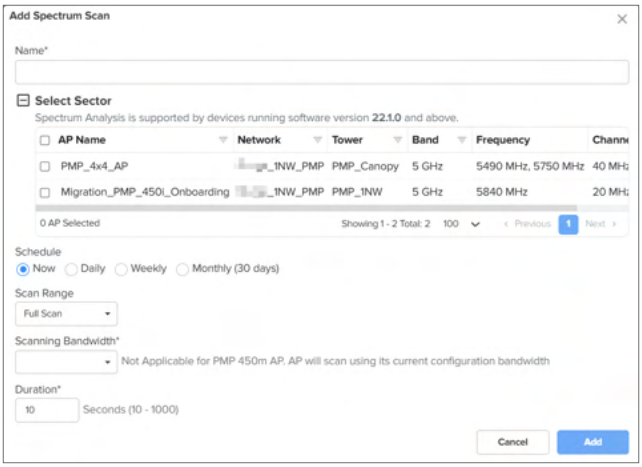


Table 181 *Add Spectrum Scan parameters*

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:

- Managing Users
- Cloud Anchor Account
- Webhooks X
- Notifications
- Audit Logs
- Updating Company Information

Users

This chapter provides the following details:

- Managing Users
- Assigning roles for IdP-based domain users
- Session Management

Managing Users

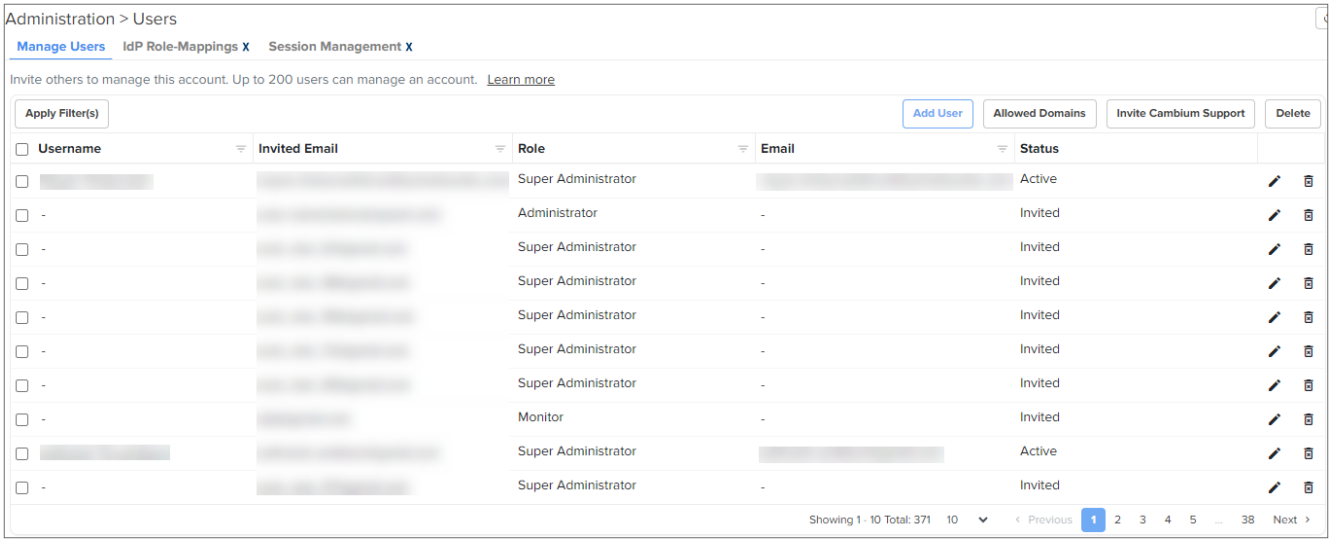
cnMaestro allows you to add Users using the **Administration > Users** page.



Note

- cnMaestro X account supports up to 200 users.
- cnMaestro Essentials account supports only up to 10 users.

Figure 661 *Adding Users*



Role-Based Access

cnMaestro supports the following user Roles:

- **Super Administrator** – Super Administrators can perform all operations.
- **Administrator** – Administrators can modify cnMaestro application functionality, but they are not able to edit User, API, or Server configuration.
- **Operator** – Operators are able to configure device-specific parameters and view all configuration.
- **Monitor** - Monitors have only the view access.
- **CPI -** CPI can perform onboarding the devices using the CBRS tool and has the view access only.

Note

- cnMaestro allows one to limit the number of concurrent sessions for each Role and display current active user sessions.
- CPI role is authorized only when the **CBRS** is Enabled.

Role-Mappings

The table below defines how Roles are authorized to access specific features.

Table 182 *Role-Mappings*

Feature	Description
Access Control Policies	Configure policies to control users connectivity to the network. • Super Administrator - All • Administrator - All • Operator - All • Monitor - None • CPI - None

Table 182 *Role-Mappings*

Feature	Description
Application Operations	Application level operations such as to create, update and delete operations for Networks, Towers/Sites. Bulk device configuration. • Super Administrator - All • Administrator - All • Operator - None • Monitor - None • CPI - None
Application Settings	Change global application configuration and onboarding key. • Super Administrator - All • Administrator - All • Operator - None • Monitor - None • CPI - None
Assists	Scan device configurations and generate assists scores, which in turn helps in isolating configuration issues in a deployment. • Super Administrator - All • Administrator - All • Operator - All • Monitor - All (**Fix Now** is not allowed) • CPI - All (**Fix Now** is not allowed)
Citizen Broadband Radio Service Subscription (CBRS)	Support CBRS-compliant devices in the 3.6 GHz band (from 3550 MHz to 3700 MHz) • Super Administrator - All • Administrator - All • Operator - None • Monitor - None • CPI - All
Installation Summary	View installation summary of PMP and ePMP SMs, Enterprise Wi-Fi APs, and cnMatrix devices installed using the Cambium Networks Installer application. • Super Administrator - All • Administrator - All • Operator - All • Monitor - None • CPI - View
Configuration/Software Update	Manage configuration/software update jobs.

Table 182 *Role-Mappings*

Feature	Description
	• Super Administrator - All • Administrator - All • Operator - All • Monitor - None • CPI - None
Custom Applications	Configure applications with a specific IP address or a domain name, and apply filter rules. • Super Administrator - All • Administrator - All • Operator - All • Monitor - None • CPI - None
Device Operations	Device operations such as reboot device, link test, connectivity test, tech support file download, and Wi-Fi performance test. • Super Administrator - All • Administrator - All • Operator - All • Monitor - None • CPI - None
Device Overrides	Per-device configuration, including updating AP Group and applying configuration. • Super Administrator - All • Administrator - All • Operator - All • Monitor - None • CPI - None
EasyPass	Create captive portal using EasyPass to allow clients to access the network through Free Tiers, Vouchers, or Paid Access types. • Super Administrator - All • Administrator - All • Operator: ◦ Add new vouchers ◦ Delete existing or expired vouchers ◦ Export voucher data ◦ View session details ◦ Disconnect users at the session level

Table 182 *Role-Mappings*

Feature	Description
	• Monitor - View (Sessions Only) • CPI - None
Floor Plan	Floor Plan configuration • Super Administrator - All • Administrator - All • Operator - View • Monitor - View • CPI - None
Global Configuration	The ability to create and apply configuration for global features such as Templates, WLANs, AP Groups, and bulk sync configuration. • Super Administrator - All • Administrator - All • Operator -View • Monitor - None • CPI - None
Guest Portal	Guest Portal configuration. • Super Administrator - All • Administrator - All • Operator -View • Monitor - View (Sessions Only) • CPI - None
LTE	Manage cnRanger LTE devices. • Super Administrator - All • Administrator - All • Operator - View and Edit SIM credentials only • Monitor - None • CPI - None
Managed Service Provider (MSP)	MSP operations such as modification of branded service, managed account and user invitations. • Super Administrator - All • Administrator - View • Operator - None • Monitor – None • CPI - None **Note:** Operator/Monitor users are not permitted to move devices across managed

Table 182 *Role-Mappings*

Feature	Description
	accounts.
Monitoring	Display of monitoring data at all levels. • Super Administrator - All • Administrator - All • Operator - All • Monitor - View • CPI - View
Notifications	Alarms and Events management. • Super Administrator - All • Administrator - All • Operator - All • Monitor - View • CPI - View
Onboarding	Device approval, modifying individual device configuration, and performing software update. • Super Administrator - All • Administrator - All • Operator - All • Monitor - None • CPI - All
Reporting	Report generation. • Super Administrator - All • Administrator - All • Operator - All • Monitor - All • CPI - All
Session Management	Capability to view and logout other users sessions. • Super Administrator - All • Administrator - All • Operator - None • Monitor - None • CPI - None
Software Upgrade	Upgrade the device with the latest software. • Super Administrator - All

Table 182 *Role-Mappings*

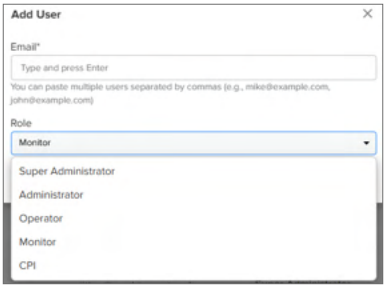
Feature	Description
	• Administrator - All • Operator - All • Monitor - None • CPI - None
Spectrum Analyzer	Analyze and monitor wireless spectrum for optimizing network performance on PMP devices. • Super Administrator - All • Administrator - All • Operator - All • Monitor - None • CPI - None
User Management	User management operations such as manage users and roles. • Super Administrator - All • Administrator - View • Operator - None • Monitor - None • CPI - None

Creating Users and Configuring User Roles

To add an administrator:

1. Navigate to **Administration** > **Users** page.
2. Click **Add User** button.

   The Add User window is displayed.



3. Enter the email address in the **Email** 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. To configure the User Role, select any one of the role for the user from the **Role** dropdown list:

- Super Administrator
- Administrator
- Operator
- Monitor
- CPI

5. Click **Send** button to add this user.

To edit or delete a user, click the Edit icon or the Delete icon against the user in the **Administration > Users** page.

Whitelisting specific domains

Using the **Administration > Users** page, you can allow (or whitelist) a specific domain (for example, gmail.com). When users from the whitelisted (or allowed) domain are added, an invite email is sent directly to them. When the users accept the invite, they are allowed to access a particular cnMaestro UI account.

You can also blacklist or disallow a specific domain to prohibit all users of that domain from accessing the UI account.

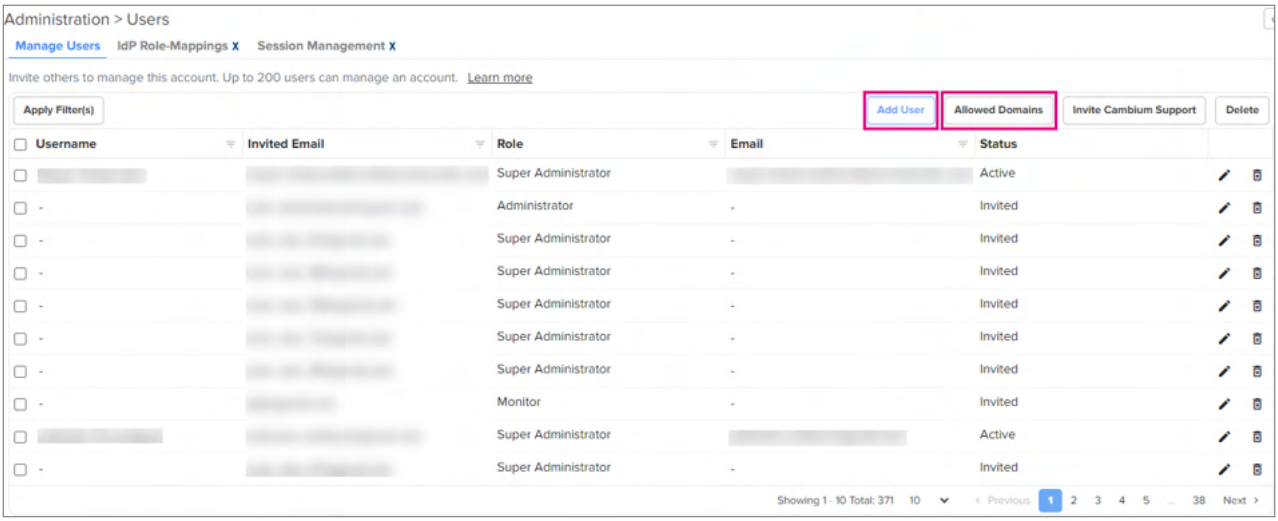
Note

- Domain whitelisting is not applicable to NFR User accounts.
- For users from the whitelisted domains, you can create the MSP user account.

To whitelist or blacklist a specific domain, perform the following steps:

1. Navigate to **Administration > Users** page.

   The **Manage Users** page appears.

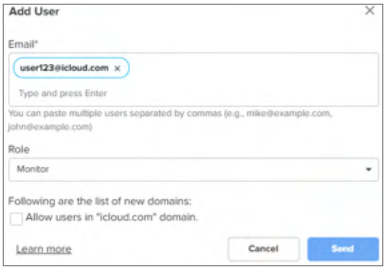


Note

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.

2. To add a new domain (for example, an icloud ID), click **Add User**.

The **Add User** window appears. You must set the fields, as described in the Creating Users and Configuring User Roles section. The **Add User** window also displays that the email ID used is a new domain, as shown in the following example (in this case, icloud.com is the new domain):



3. Select the **Allow users in "icloud.com" domain** checkbox (the domain name varies based on the email ID you add).

   The new domain is added to the database.

   When users belonging to this allowed domain (for example, icloud.com) are added (using the **Add User** button), an invite email is directly sent to the users. When the users accept the invite, they can access a particular cnMaestro UI account. The **Allow users in "icloud.com" domain** checkbox is available only when you are adding a new domain.

4. To blacklist or disallow a specific domain, click on the **Allowed Domains** button on the **Manage Users** page.

   The **Allowed Domain** window appears with a list of whitelisted domains.



5. Clear the required domain checkbox to blacklist that specific domain.
6. Select **Update**.

All users from that blacklisted domain are not allowed to access the UI. To allow the blacklisted domain, you must check the required domain checkbox on the **Allowed Domain** window.

Assigning roles for IdP-based domain users

A group mapping is a link between cnMaestro roles and IdP roles or groups. When signing in to cnMaestro, roles can be automatically assigned based on roles in the IdP. This can be used to maintain roles in Active Directory or a similar central identity provider.

Create a group mapping for each set of roles that you want to assign to a user based on the user's IdP group memberships. Your organization might have groups with different sets of permissions based on teams, Cloud environments, or read/write/admin access. You can create a group mapping for each set of permissions. For example, you might create a group mapping that assigns the roles `DeveloperWrite` and `ResourceOwner` to a user who is a member of the data-science group in your IdP server.



Note

The IdP role mapping configuration is applicable only to cnMaestro X accounts.

To set up IdP role mapping, contact Cambium Support who will ask for some information and generate an IdP role mapping key.

With the IdP role mapping key, IdP groups or roles can be mapped to a role in cnMaestro for the IdP domain users. For example, with an Active Directory group called `app-cnmaestro-superadmin` mapped to the "Super Administrator" role in cnMaestro, members of this Active Directory group will be assigned the Super Administrator role automatically when logging in.

Advantages

The advantages of IdP-based domain user role configuration are:

- Authentication can be centralized and users can access multiple accounts with the same login.
- Security policies, such as password or authentication requirements, can be managed through a single policy.
- User experience improves as there is no need for multiple passwords and logins, making access seamless across all platforms.

Using the **Administration > Users > IdP Role-Mappings** UI page in cnMaestro, a new IdP role-mapping can be added and roles can be assigned to the IdP domain users.

Prerequisite tasks

Before adding IdP role-mappings and assigning roles in cnMaestro, make sure to complete the following prerequisite tasks:

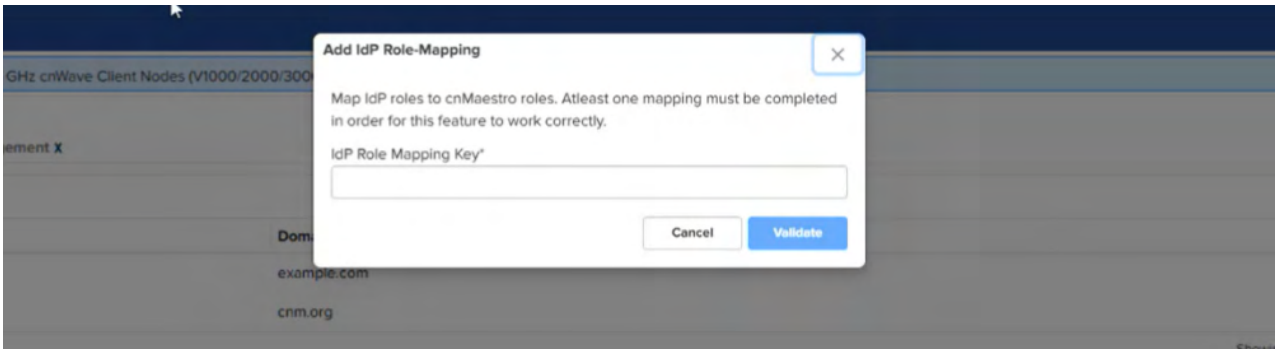
- An IdP must be registered by the Cambium Support team.
- The IdP must have the IdP Role Mapping Key, which is generated and provided by the Cambium Support team.

Assigning roles for IdP-based domain users

To add a new role-mapping and assign a role for the IdP-based domain users, complete the following steps:

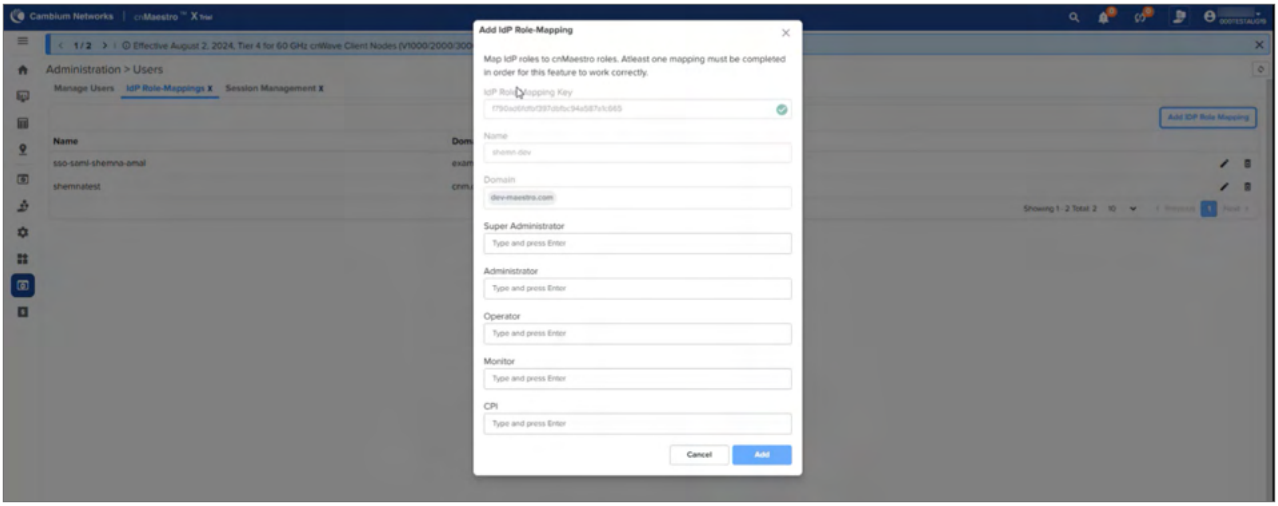
1. Navigate to **Administration > Users > IdP Role-Mappings**.
2. Click **Add IdP Role Mapping**.

   The **Add IdP Role-Mapping** box appears.



3. In the **IdP Role Mapping Key** text box, enter the key provided by the Cambium Support team.
4. Click **Validate**.

On successful validation of the IdP, you can view the IdP details configured on the Support site. For example, IdP name and domain.



5. In the **Add IdP Role-Mapping** box, assign the required roles to the user groups.
6. Click **Add**.

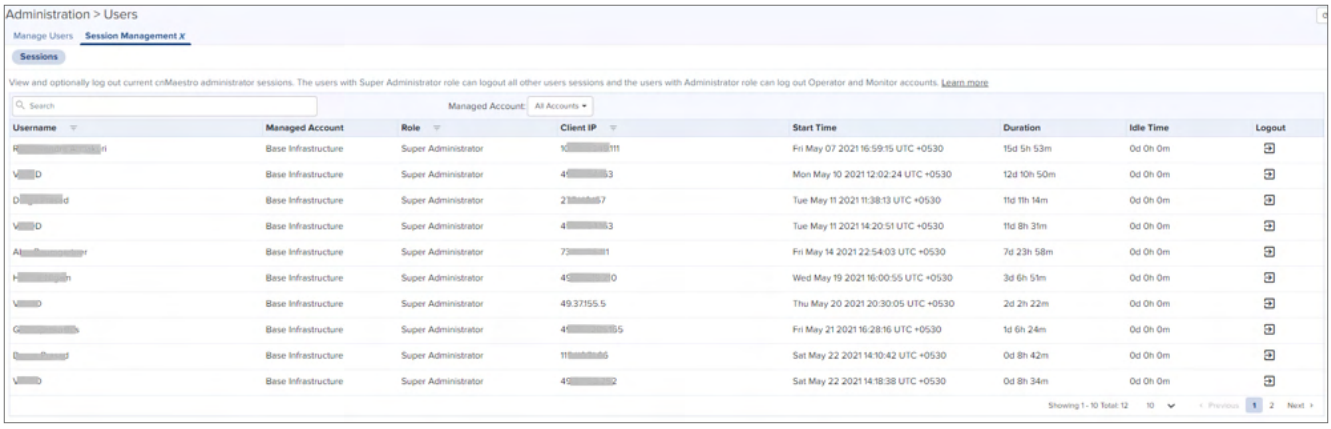
   When domain users log in to the cnMaestro UI, they can access multiple accounts with a single log-in.

Session Management

View and optionally log out current cnMaestro administrator sessions. The users with Super Administrator role can logout all other users sessions and the users with Administrator roles can logout Operator and Monitor accounts.

Sessions

Displays the detailed information on the user sessions.



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.

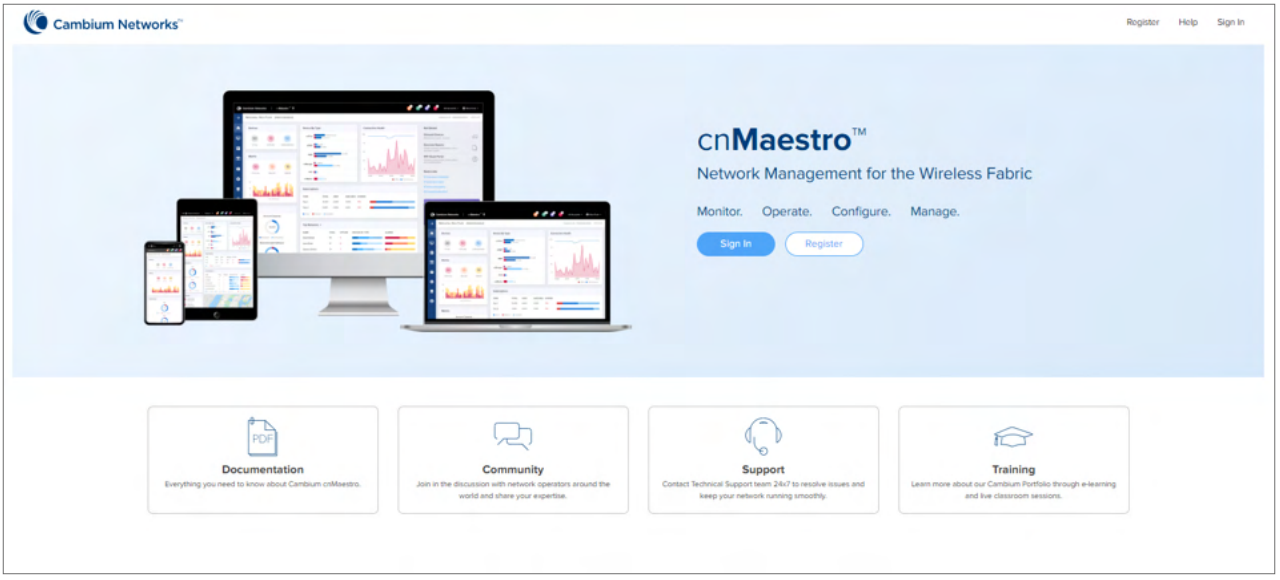
Manage Instances describes the following topics:

- 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:

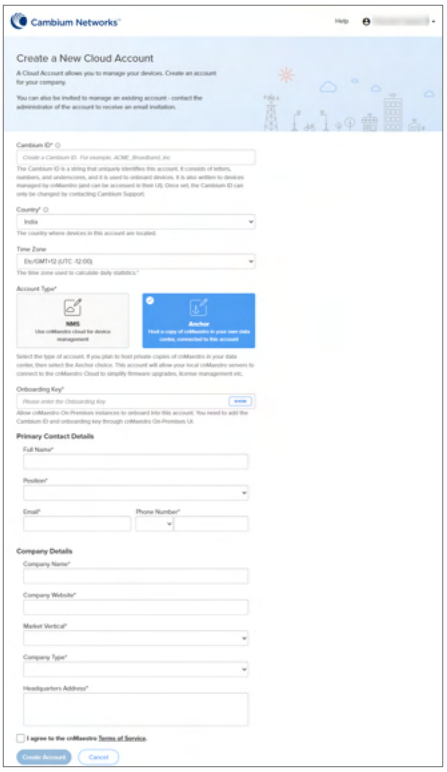
1. Log in to the cnMaestro UI, https://cloud.cambiumnetworks.com.



2. Click **Add New Account**.

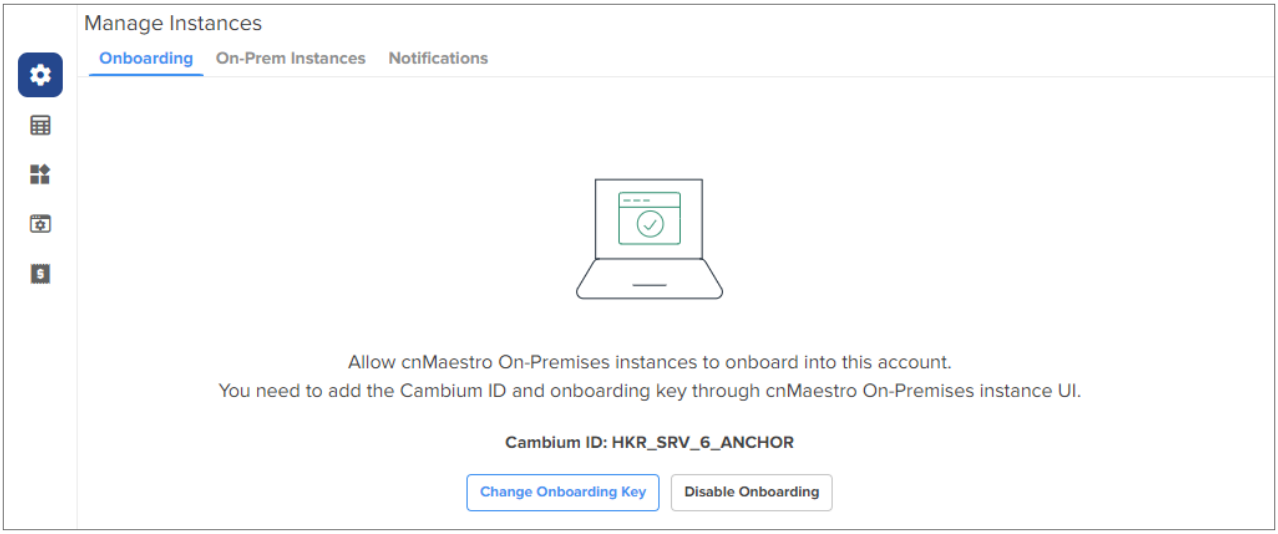
   The **Create a New Cloud Account** page is displayed.

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



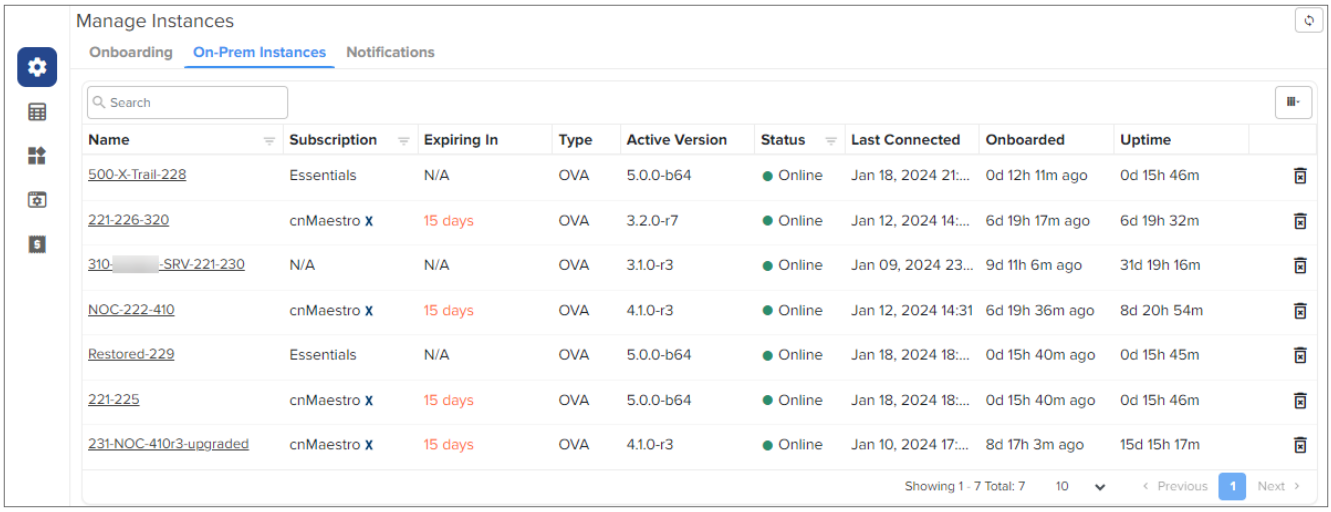
4. Enter the On-Premises **Onboarding Key**.
5. Configure the parameters under the **Primary Contact Details** and **Company Details** sections.
6. Read the cnMaestro Terms of Service and select the **I agree to the cnMaestro Terms of Service** checkbox.
7. Click **Create Account**.
8. When the Anchor 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.

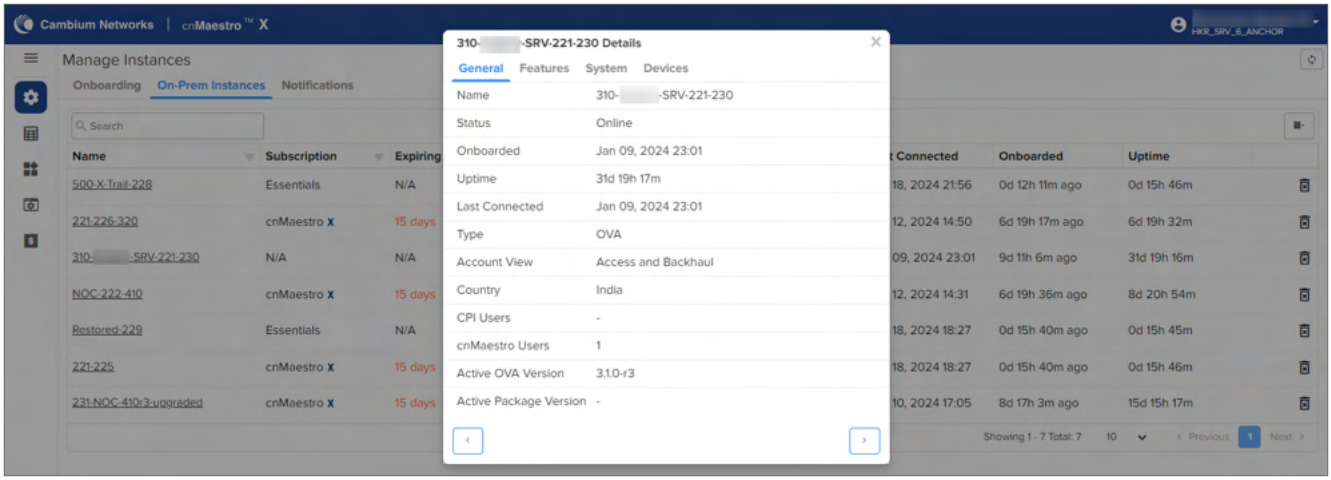


On-Premises Instances

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.

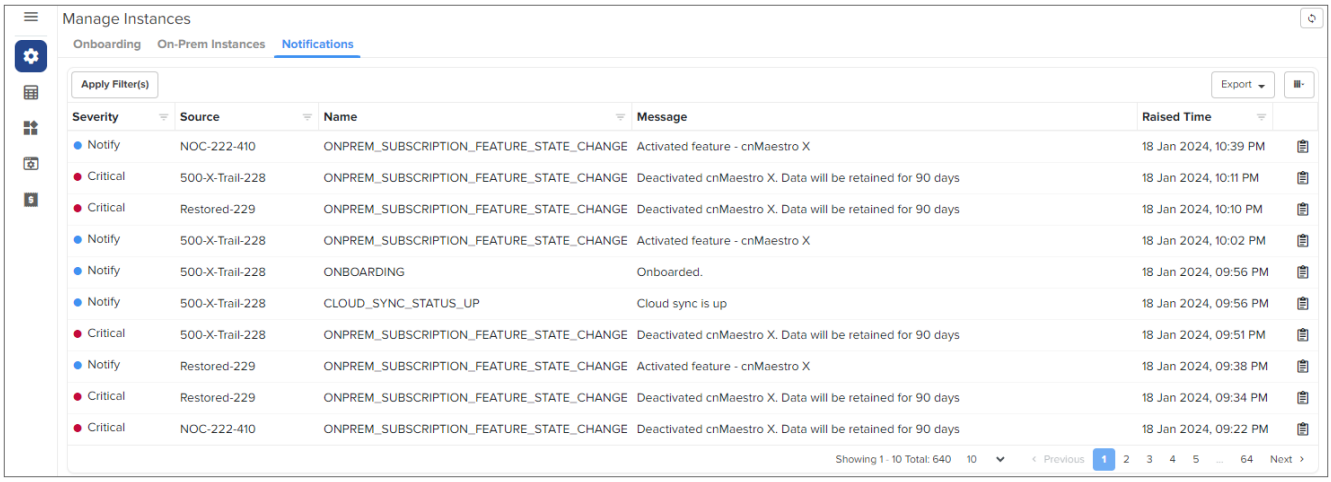


By clicking the instance host name, you can see the On-Premises server details such as General, Features, System, and CBRS:



Notifications

Notification page displays the history of the most recent events notification of On-Premises instances with **Severity**, **Source**, **Name**, **Raised Time**, and **Message**.

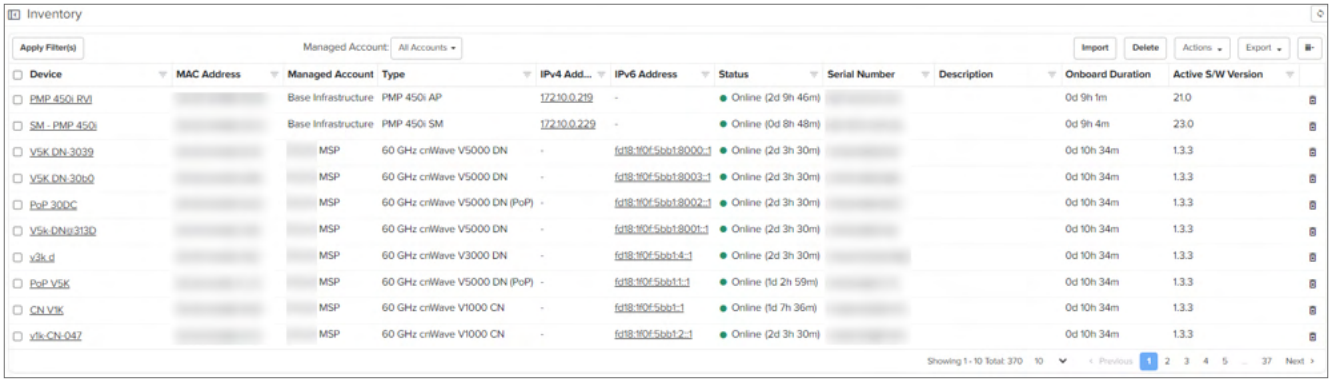


Click View Details to view the Event Details as shown below:



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

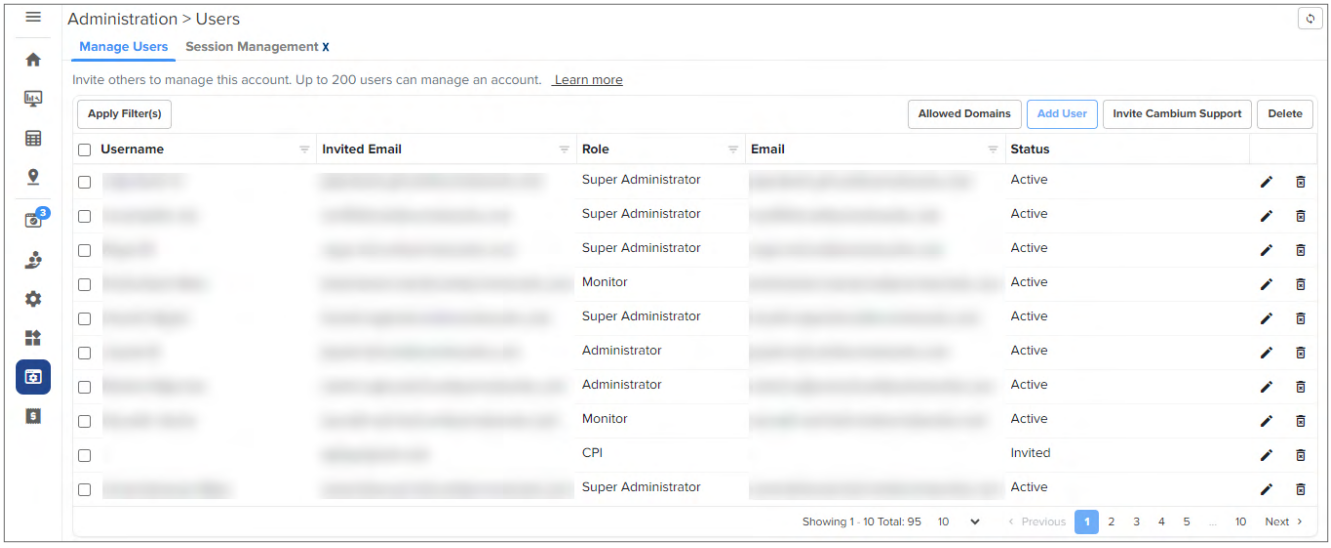
Administration provides the following details:

- 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 662 *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.

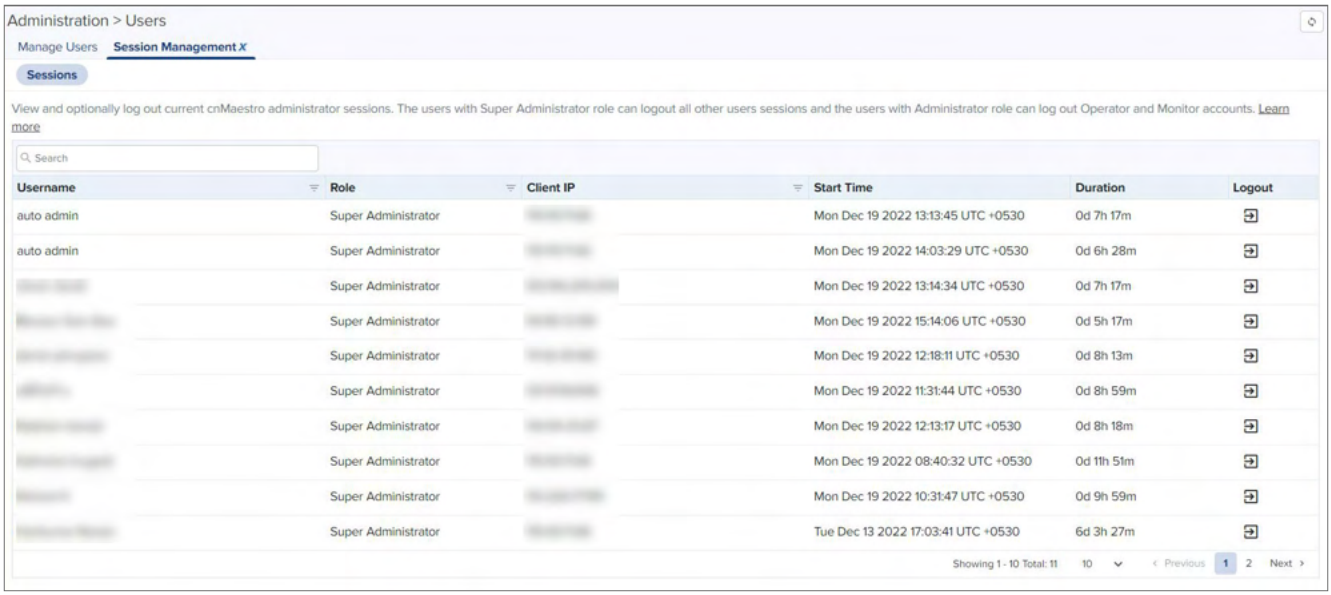
   You can invite multiple users simultaneously by entering their email IDs in the Email text box or copy and paste the multiple email IDs as a comma-separated input.

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.



Network Services

Network Services provide the following details:

- CBRS
- Organization

CBRS

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

For further information, refer to CBRS.

Organization

An Organization allows multiple accounts to share CBRS billing and SAS ID. The Primary account owns this configuration, and the Secondary account can optionally share it. Both accounts must authorize the sharing.

For further information, refer to Organization.

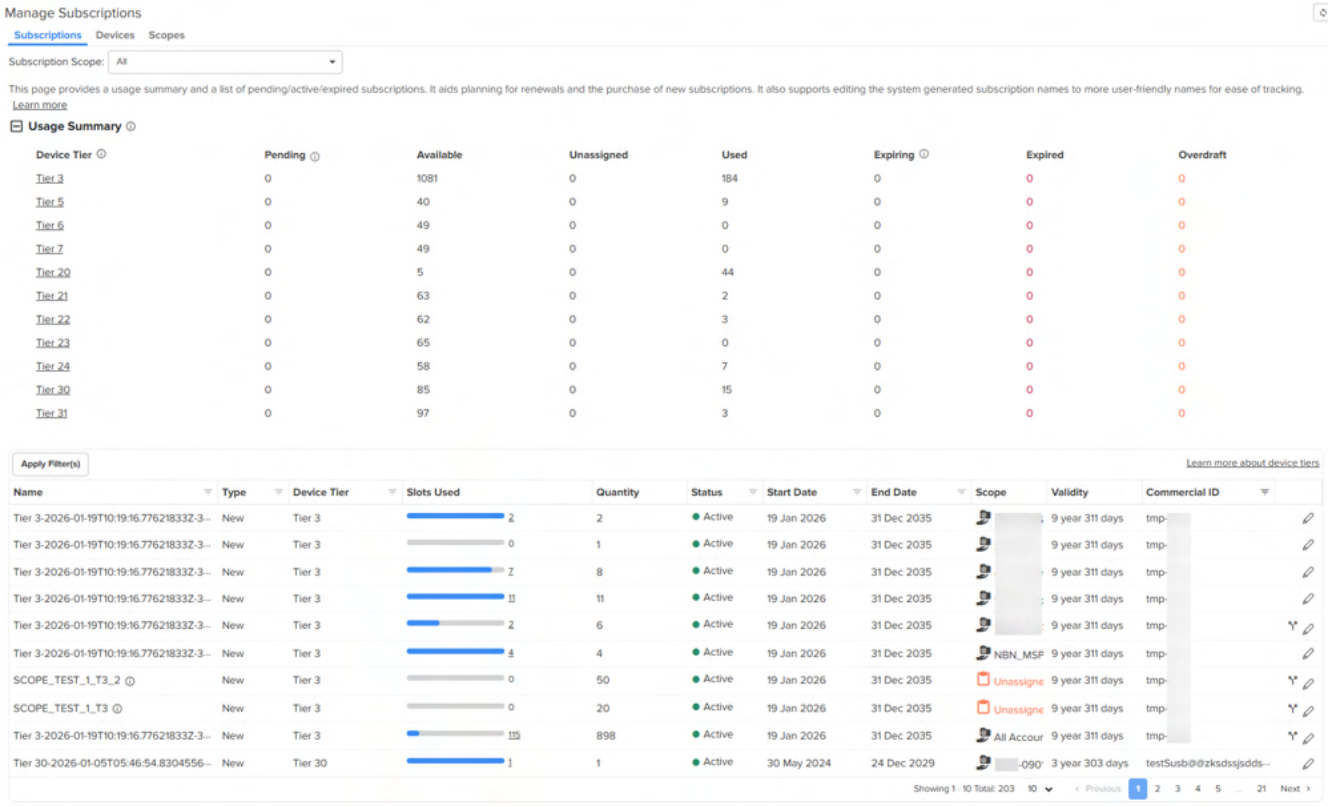
Manage Subscriptions

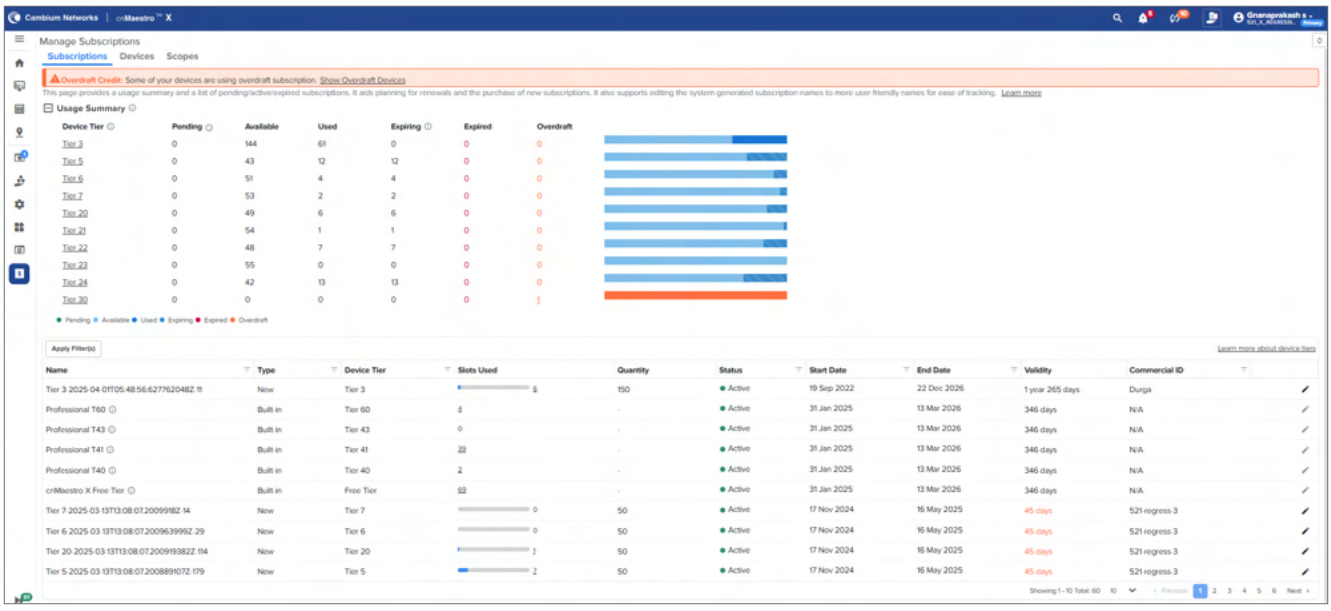
Manage Subscriptions provide the following details:

- Subscriptions
- Devices
- On-Premises Instances

Subscriptions

Subscriptions page describes about the usage summary and a list of pending, active, and expired subscriptions. It aids planning for renewals and the purchase of new subscriptions.



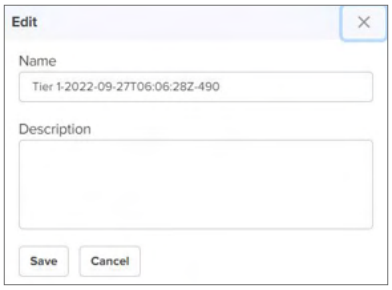


It also supports editing the system generated subscription names to more user-friendly names for ease of tracking.

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

1. click edit ( ) icon.

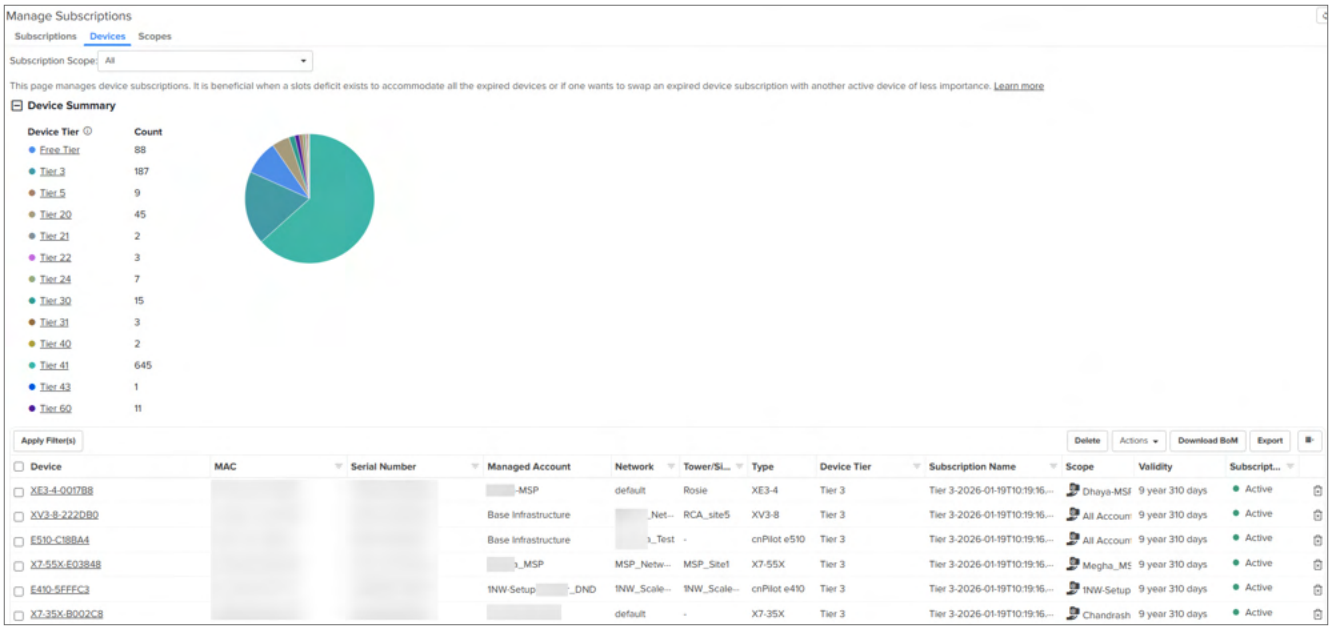
   Edit window pops up as shown below.



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.



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.

To configure Webhooks for cnMaestro Cloud, you must first configure a Webhooks template and then configure the notifications to be sent by cnMaestro to the Webhooks URL.

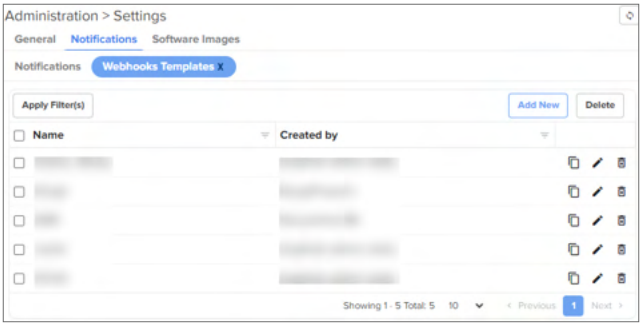
This topic describes the following:

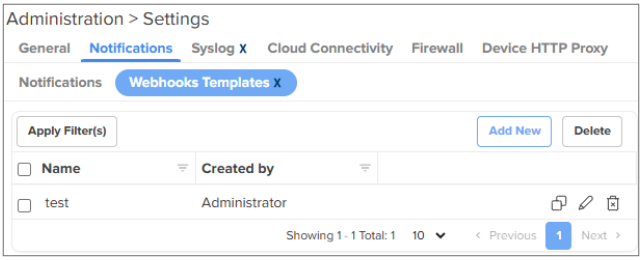
- Configuring Webhooks template
- Supported variables
- Error and retransmission
- Notifications

Configuring Webhooks template

To configure the webhooks template, perform the following:

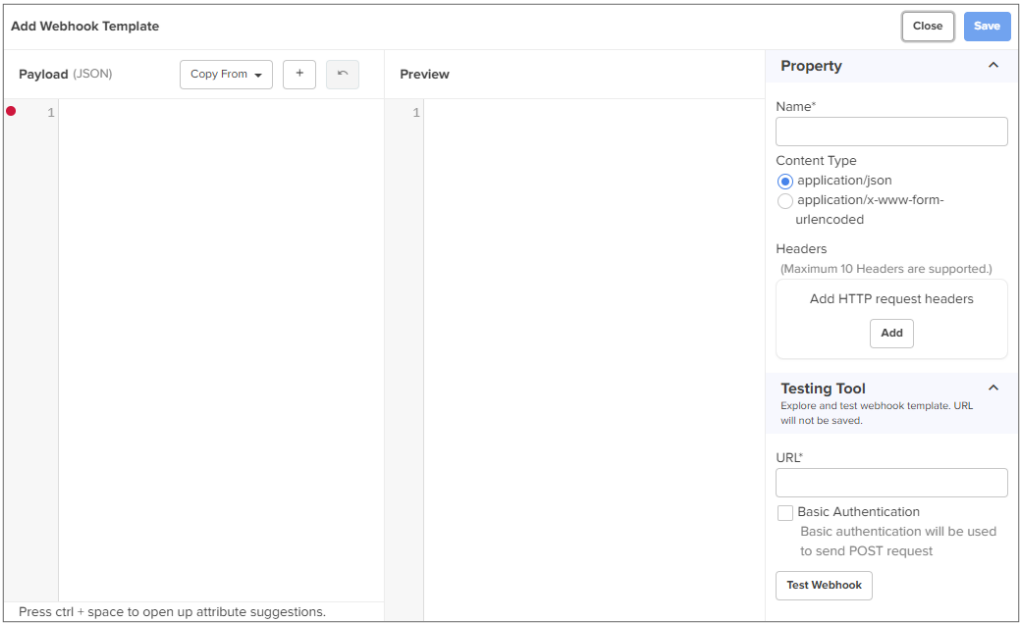
1. Navigate to **Administration** > **Settings** > **Notifications** > **Webhooks Templates X**.





2. Click **Add New**.

   The Add Webhook Template page appears.



3. Enter the parameters as shown in the below table.

Table 183 *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**. 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.

Parameter	Description
	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",
 "alarmId": "66e2854a6d49046d4b3425c5",
 "alarmMsg": "Device is offline.",
 "alarmName": "STATUS_DOWN",
 "alarmSeverity": "major",
 "alarmStatus": "true",
 "alarmCategory": "STATUS",
 "alarmType": "Status",
 "alarmRaisedTimeISO": "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::1a2b:3c4d:5e6f:7g8h",
 "sourceType": "",
 "managedAccount": "Tally Managed Account",
 "networkName": "Global Network",
 "siteName": "Apartment Site",
 "siteId": "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 184 *Types of Variables*

Variable	Description
ALARM_ACK_BY	Name of the person who acknowledged the alarm.
ALARM_DURATION	Alarm duration (seconds)

Variable	Description
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)
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"

Variable	Description
	• PMP AP: "ap" • PMP SM: "sm" • PTP 650/670/700: "bhm", "bhs" • PTP 820/850: "ptp" • RV22 Home Mesh: "wi-fi"
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)
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

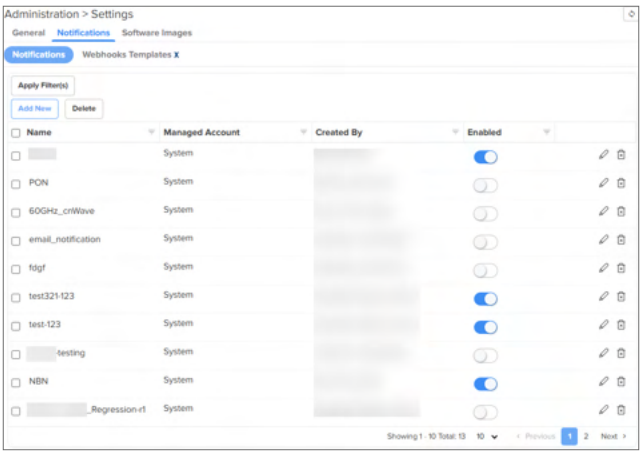
- Email delivery of notifications in the JSON format is being deprecated. Future releases of cnMaestro will support only HTML-based emails.
- A maximum of four email IDs and three webhooks are supported for each notification.

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:

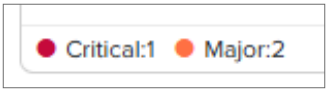
Figure 663 *Add Notification page*



3. Configure the following parameters:

Table 185 *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.
Scope	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.

Parameter	Description
	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. Based on the alarms selected, the count of alarms that are selected, severity-wise 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**.

Parameter	Description
	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**.

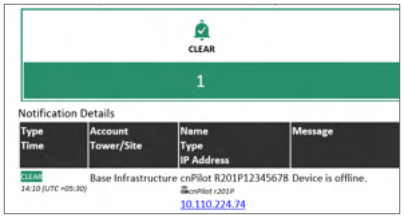
   The notification is listed in the **Notifications** page.

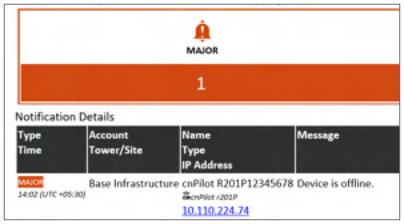
5. To edit a notification, click the edit (✎) icon.

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)	✔	✔	✔	✔
NSE	✔	✔	✔	
Light Speed	✔	✔	✔	
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)	✔	✔	✔	✔
RV22 Home Mesh	✔	✔	✔	✔

Source Type	Managed Account			
	System	Network	Site	Tower
System	✔			
Network	✔	✔		
Site	✔	✔	✔	
Tower	✔	✔		✔

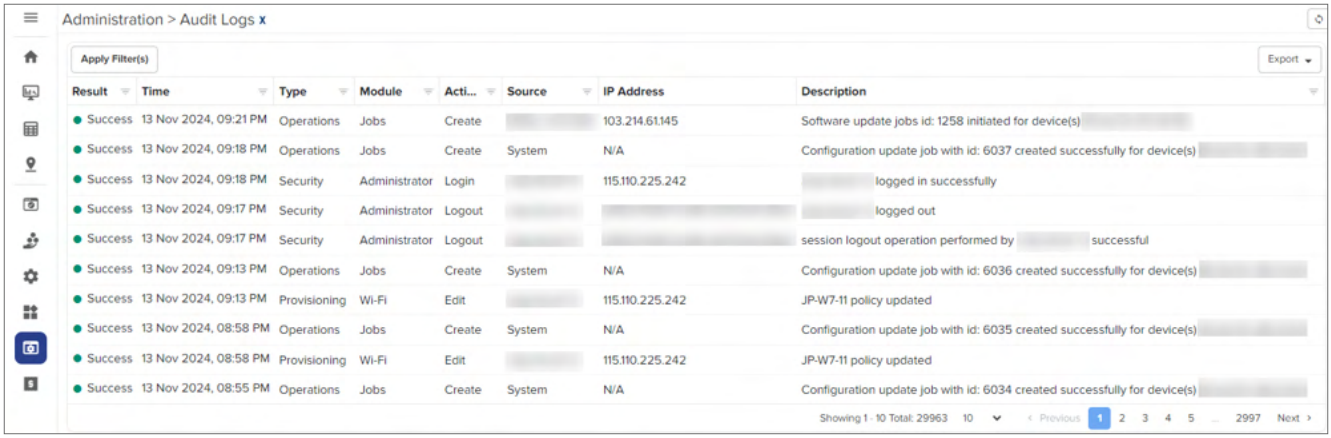
Audit Logs

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 664 *Audit Logs*



The following table describes the Audit Logs parameters and their descriptions.

Table 186 *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 187 *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.

Module	Types	Description
Auto-Provision	Provisioning	Auto-Provisioning.
CBRS	Services	CBRS.
Cloud- Sync	Services	Synchronizing Cloud and On-Premises instances.
Configuration	Provisioning Operations	Details of configuration actions.
Data-Tunnel	Provisioning	Data Tunneling.
Device	Provisioning Operations	Device management.
Email-Notifications	Operations	Add or edit email notifications.
Guest-Portal	Provisioning	Guest portal.
Infrastructure	Provisioning	Site, Network, Tower Management.
Jobs	Provisioning Operations	Jobs infrastructure.
License	Licensing	Update license details.
MarketApps	Operations	MarketApps configuration details.
MSP	Operations	Operations covering Managed Services and Managed Account.
Onboard	Provisioning Operations	Onboarding Queue.
Profile	Provisioning	Create or update a profile.
Report	Provisioning Operations	Data Reports.
SIM	Provisioning	SIM claim and delete.
Subscription	Operations	Subscription details.
System	Provisioning Operations Security	System Services: VM management, change log level, system upgrade, system monitoring, software images, system settings.
Template	Provisioning	Template-Based Configuration.
Tools	Provisioning Operations	Technical support dump, networking operations, etc.
Webhooks	Provisioning	Webhooks configuration and management.
Wi-Fi	Provisioning Operations Security	AP Groups, WLANs: edit W-Fi configuration objects.

Updating Company Information

Note

Company information is applicable only on cnMaestro Cloud and Anchor Accounts from release

version 5.2.0 and later.

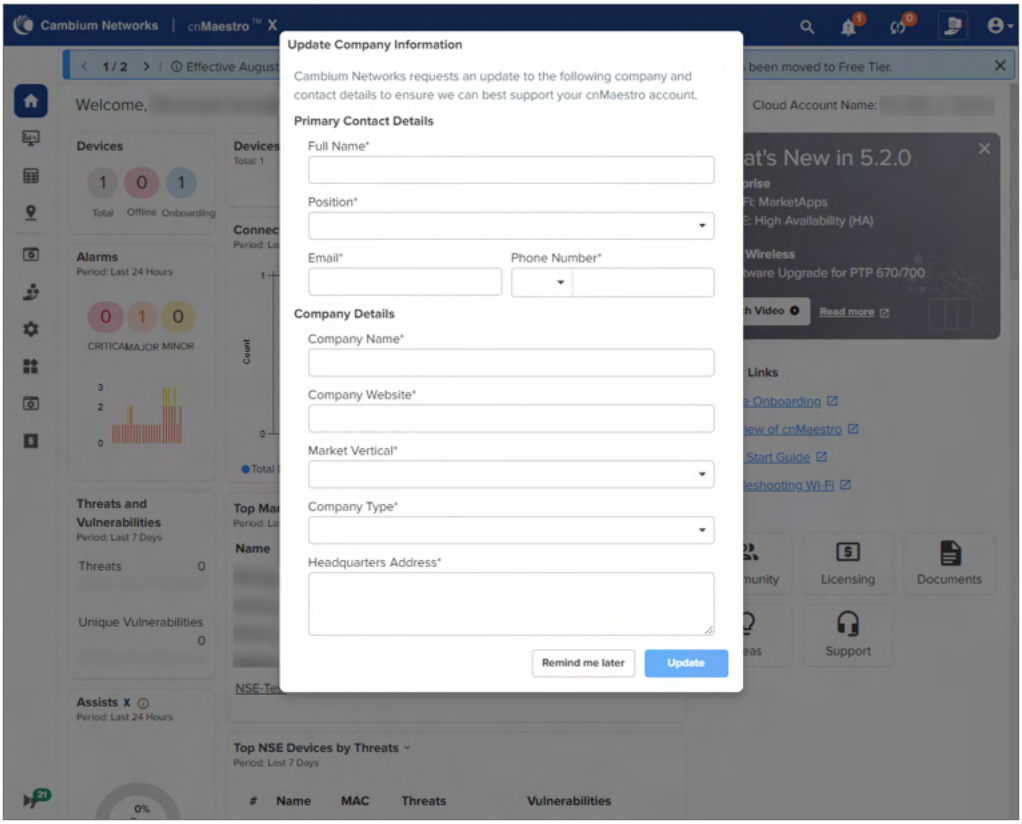
Users must provide certain personal and company contact details so that Cambium can provide better support for their cnMaestro accounts. Users must provide the following details in cnMaestro:

- Primary contact details, such as user's name, user's email ID, and their role or the designation in the company to which the cnMaestro account belongs.
- Company details, such as company name, address, website URL, company type, and market vertical.

From cnMaestro release 5.2.0, the **Company Information** page appears in the following instances:

- **Logging into cnMaestro 5.2.0 for the first time**—When the users log in to their existing cnMaestro accounts for the first time after the 5.2.0 upgrade, the **Update Company Information** pop-up window is displayed.

  Figure 665 *Update Company Information window*

  For information on the parameters on this screen, see Table 188.

  If you click **Remind me later**, you can still update the information by one of the following ways:

  - Navigate to the **Administration > Company Information** page directly and update the required information. See Updating information through the Company Information page.

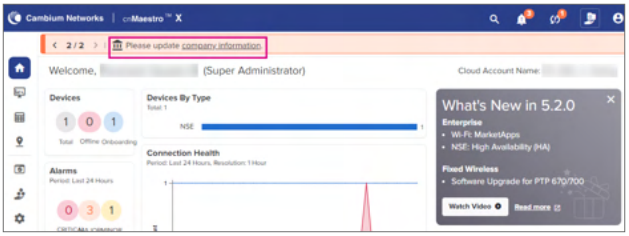
    OR

- Click the **update information** link in the banner.



Note

- The banner remains until you complete updating the company information.
- cnMaestro displays the pop-up window again when either the session ends or when the user logs out and logs back into the account.



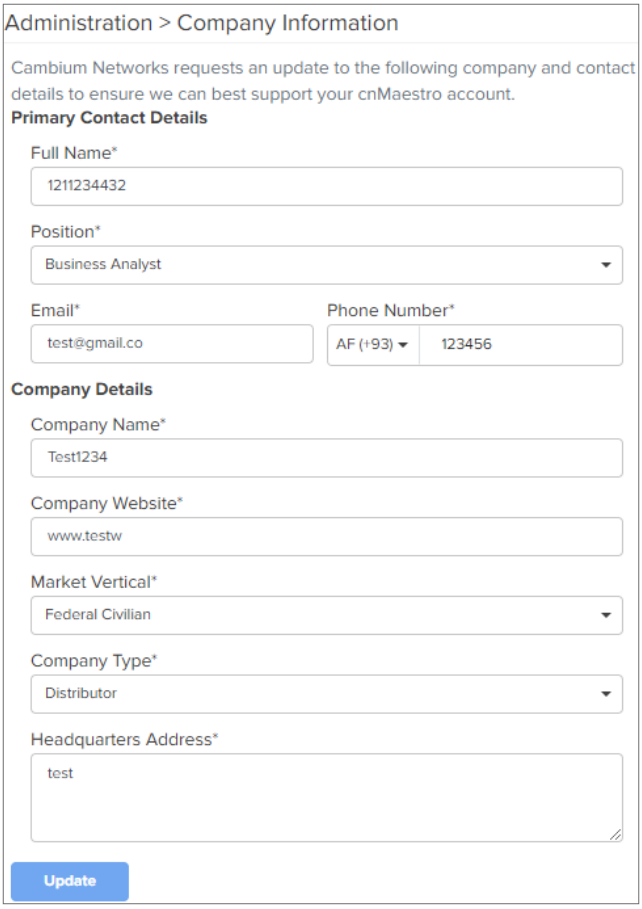
- Creating a new Cloud account—When creating a new cnMaestro Cloud account.

Figure 666 *Creating a new Cloud account*



- As a standalone page that users can access through the **Administration > Company Information** page.

Figure 667 *Administration > Company Information page*



Updating information through the Company Information page

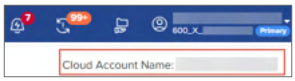
To update company information through the **Company Information** page, complete the following steps:

1. Navigate to **Administration > Company Information** page.
2. Enter the details described in the following table:

Table 188 *Company Information details*

Parameter	Description
Primary Contact Details	
Full Name	Name of the user in the cnMaestro account.
Position	Role or the designation of the user in the company. Select from the dropdown list.
Email	Email ID of the user.
Phone Number	Phone number of the user. Select the country code from the dropdown list and provide a valid phone number.

Table 188 *Company Information details*

Parameter	Description
Company Details	
Company Name	Name of the company. This name will appear as the **Cloud Account Name** in the cnMaestro home page. 
Company Website	URL of the company website.
Market Vertical	Type of market or industry the company caters to. For example, Government, Defense, Education. Select from the dropdown list.
Company Type	Nature of work that the company does. For example, Defense, Manufacturer, Distributor. Select from the dropdown list.
Headquarters Address	Address of the company headquarters.

3. Click **Update**.

Note

After updating the information, cnMaestro displays the **Update Company Information** pop-up window and the banner again after six months.

Appendix

This section includes the following topics:

- Guest Access
- Network Port Requirements
- XMS-Enterprise to cnMaestro X
- Converting Tier 2 Unused Slots

Guest Access

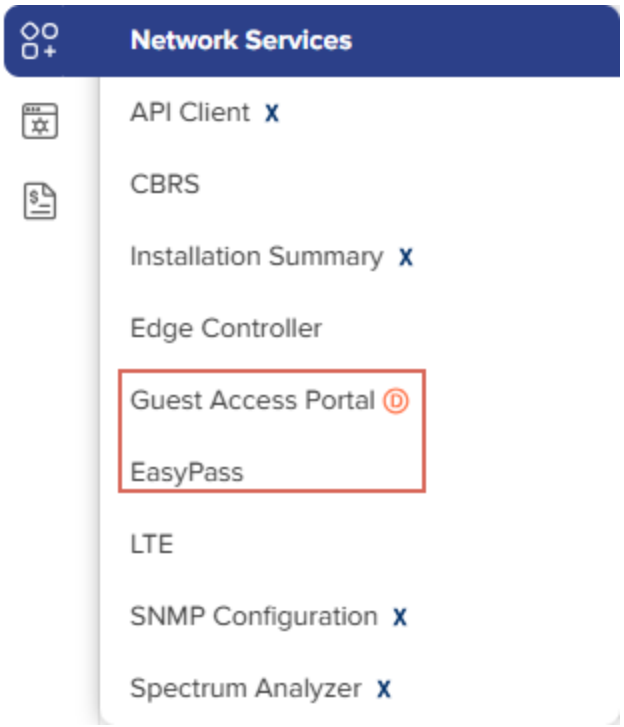
This section describes how to configure Guest Access using cnMaestro. This feature allows the clients to connect to the internet through Free Tier, Vouchers, or Paid Access types.

Note

From cnMaestro 5.1.0 release onwards, the **Guest Access Portal** configuration wizard is deprecated, and a new wizard called **EasyPass** is introduced, as shown in Figure 668.

To create captive portals on cnMaestro, use EasyPass. For information, see EasyPass.

Figure 668 *Network Services*



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

Note

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

Configuration

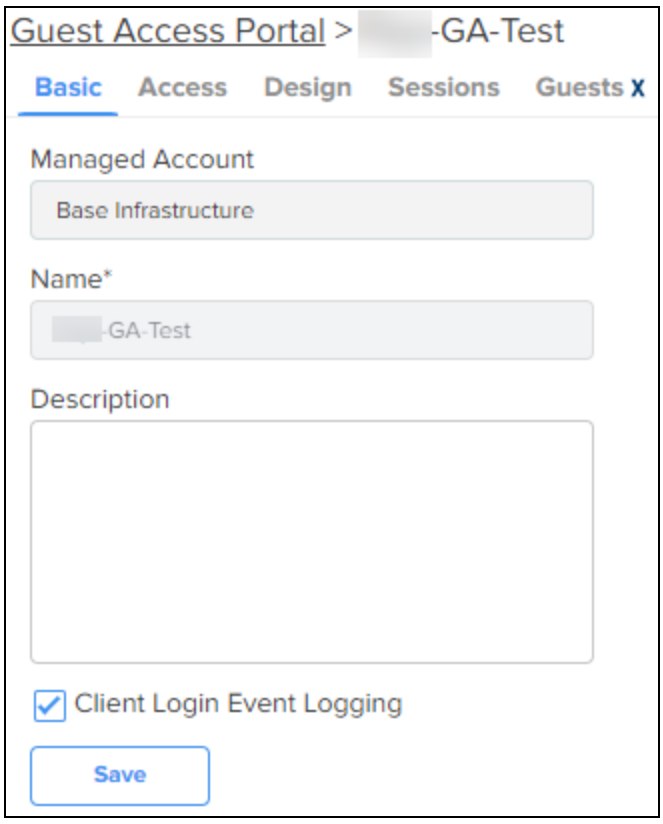
- Create the Guest Access Portal in cnMaestro
- Map the device to cnMaestro

Creating the Guest Access Portal in cnMaestro

1. Basic Details
2. Access Portal
3. Design Page
4. Sessions
5. Guests

Basic Details

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



Note

A name once created for the Portal cannot be changed.

Access Portal

The Access Portal tab has four different access types:

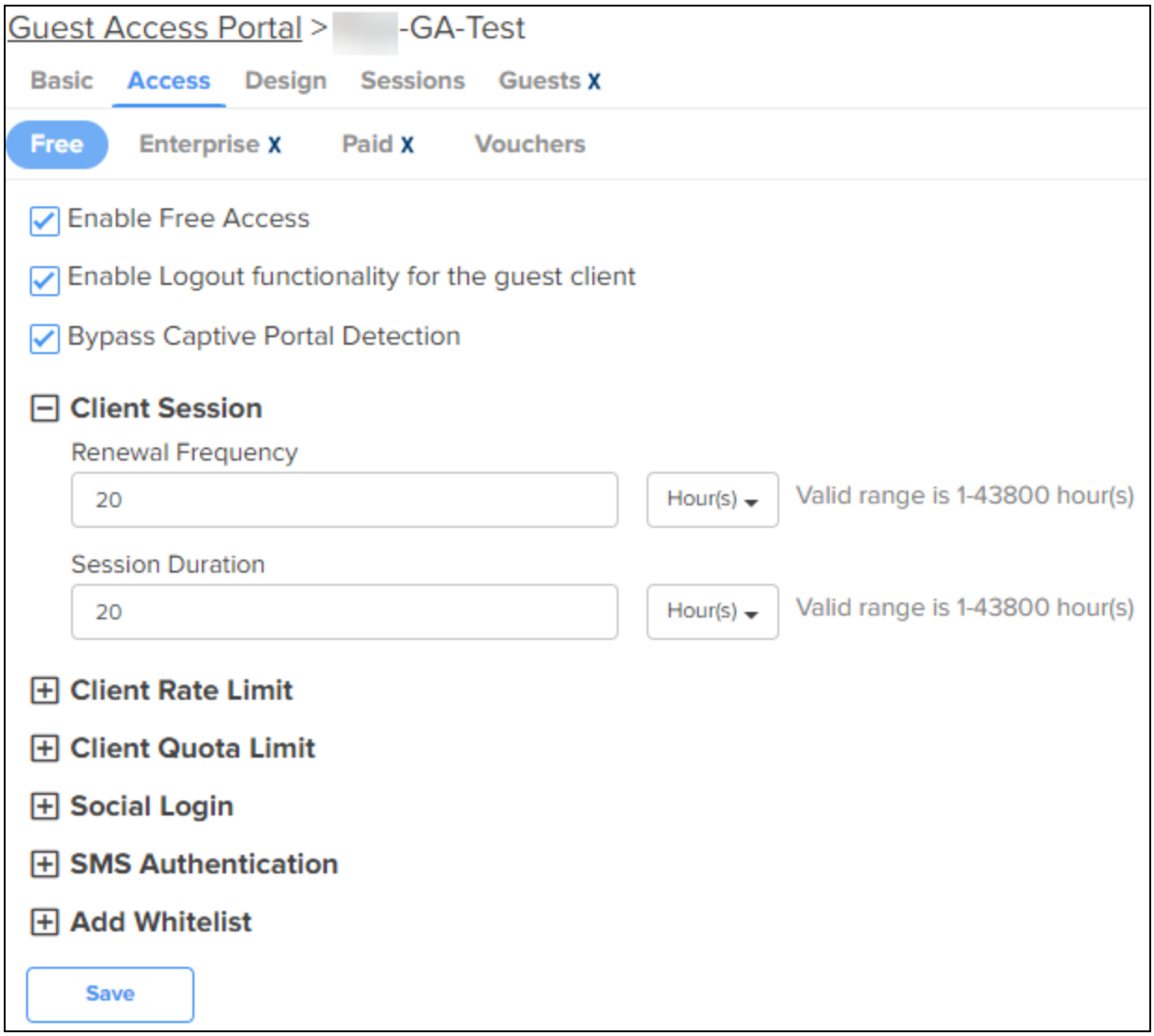
- Free
- Enterprise X access through one of the following options:
  - Microsoft Azure
  - Sponsored Guest
  - Self Registration
  - Google
- Paid X
- Vouchers

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

Note

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

Free Access Type Configuration



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 189 *Free Access Type Parameters*

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

Client Quota Limit	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

Table 189 *Free Access Type Parameters*

Parameter	Description
	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.

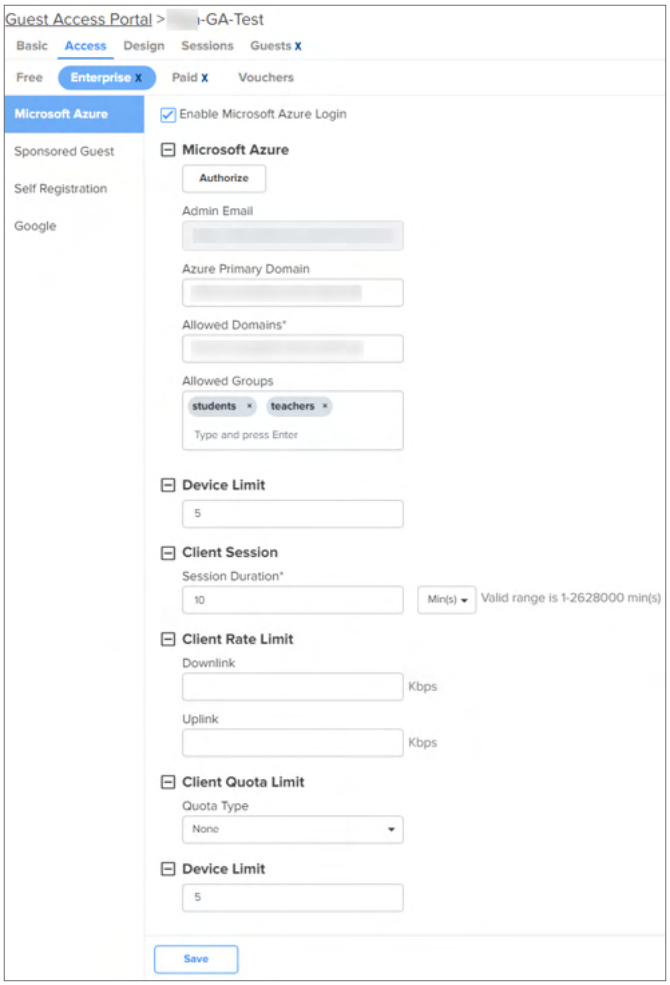
Enterprise Wi-Fi Access X using Microsoft Azure Login, Sponsored Guest, Self Registration, or Google

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

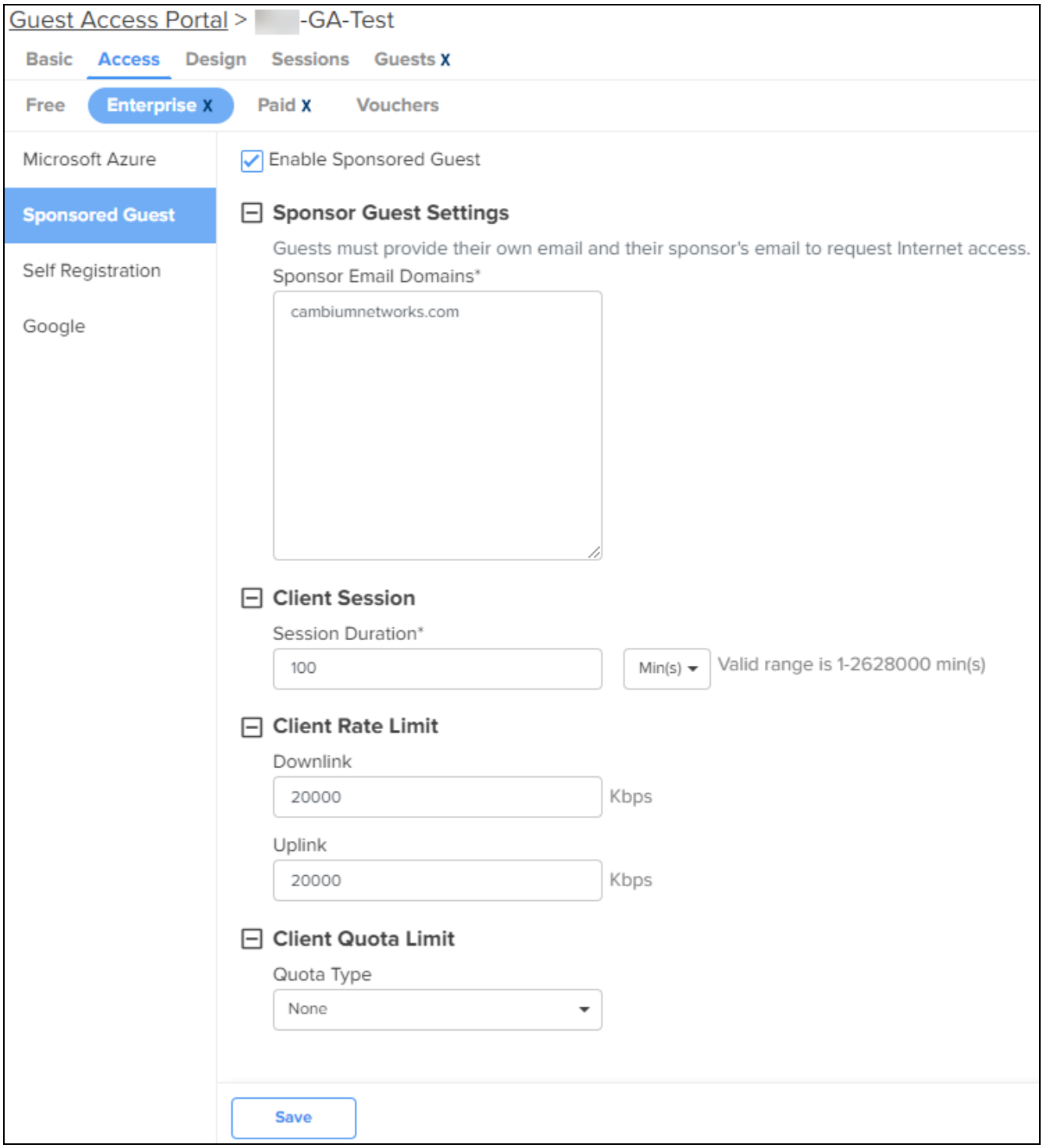
Enterprise Microsoft Azure access page enables Microsoft Azure users to log in to access the Enterprise Wi-Fi. To set up users to authenticate from Microsoft Azure, navigate to **Network Services** > **Guest Access Portal** > **Access** > **Enterprise X** > **Microsoft Azure**, complete the following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

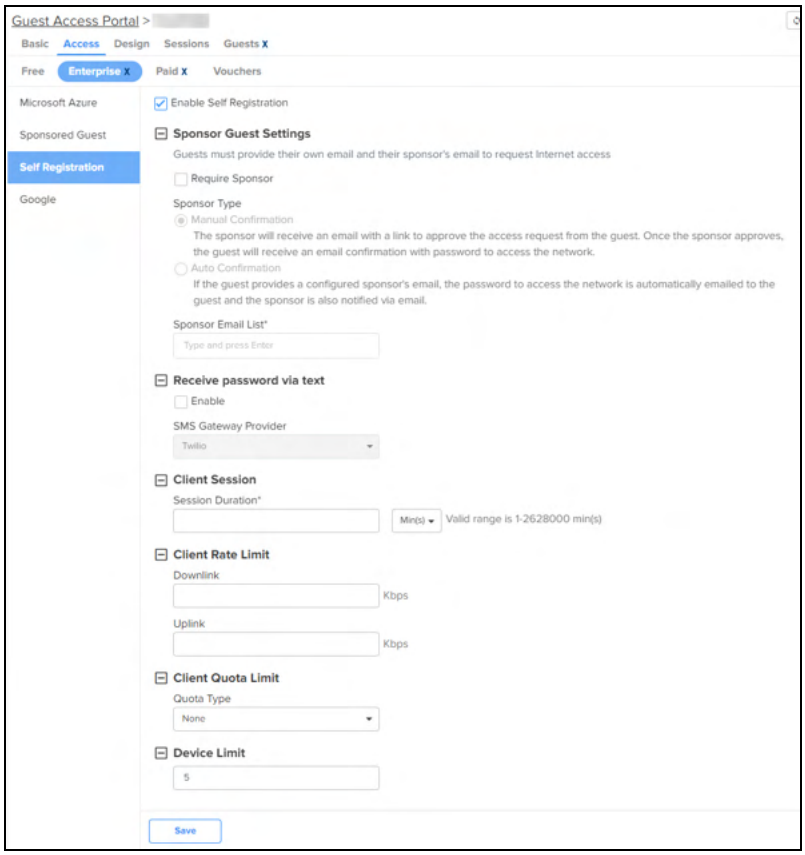


Table 190 *Self Registration Parameters*

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 190 *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 190 *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.

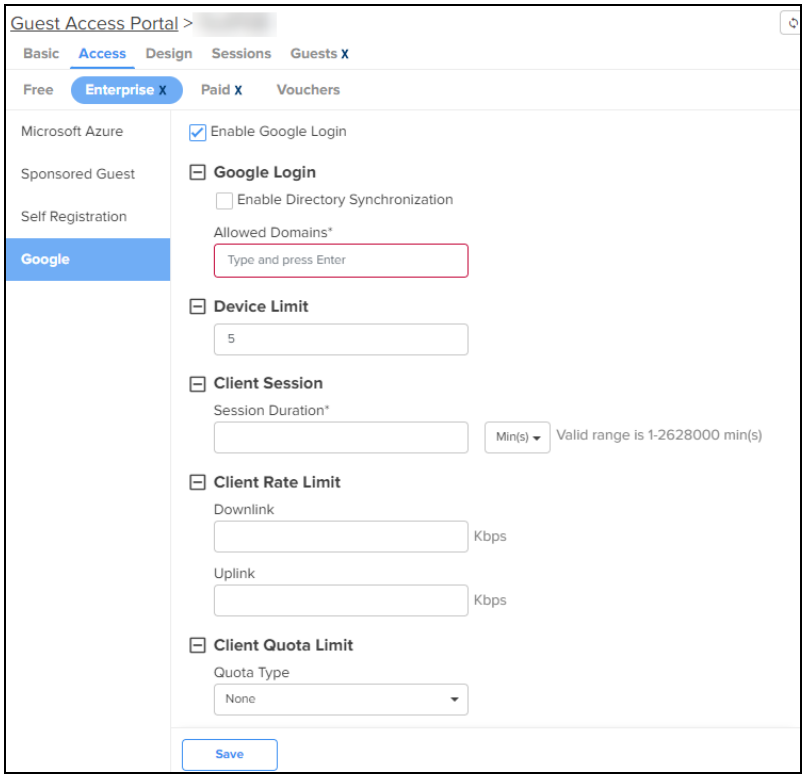
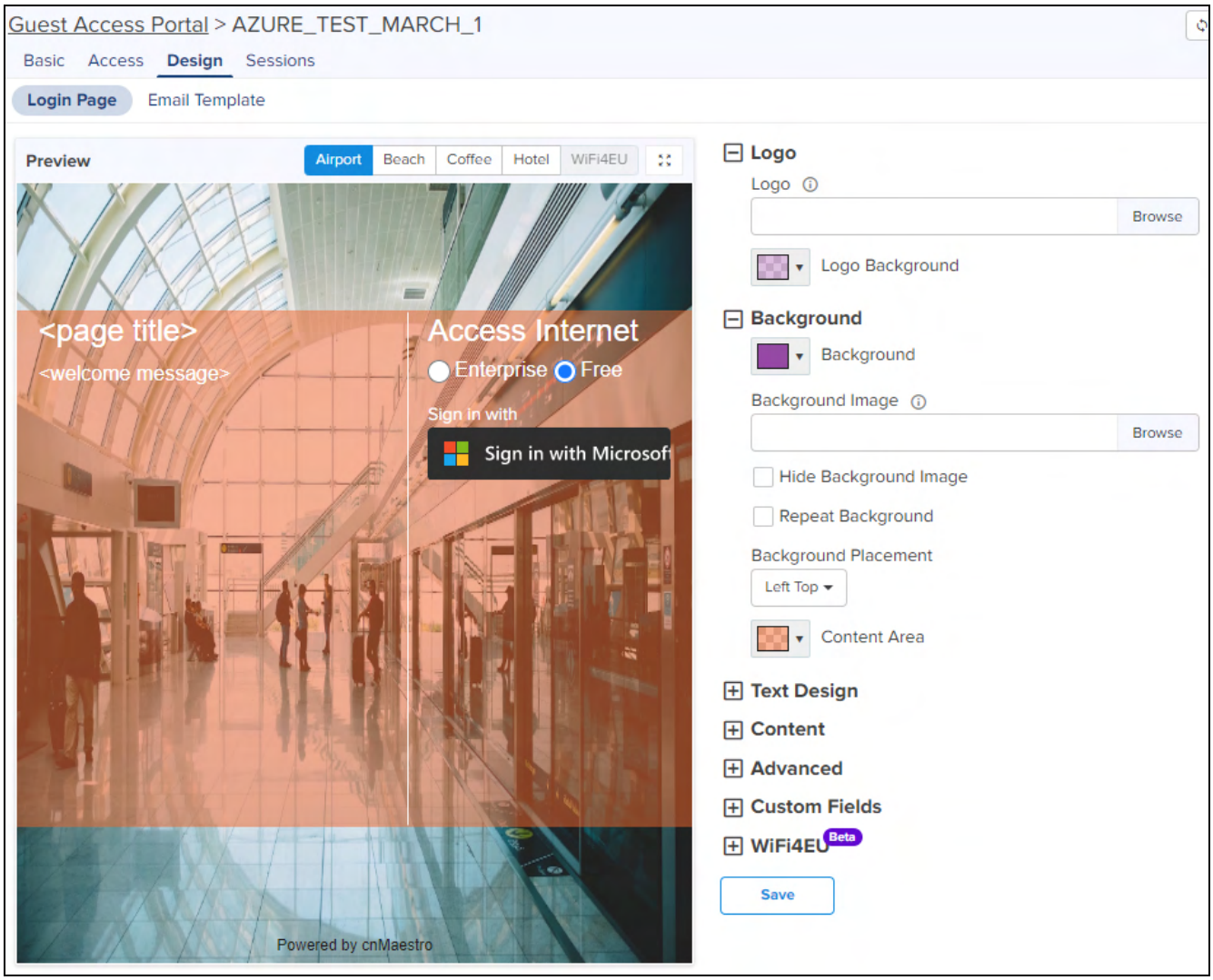


Table 191 *Google Parameters*

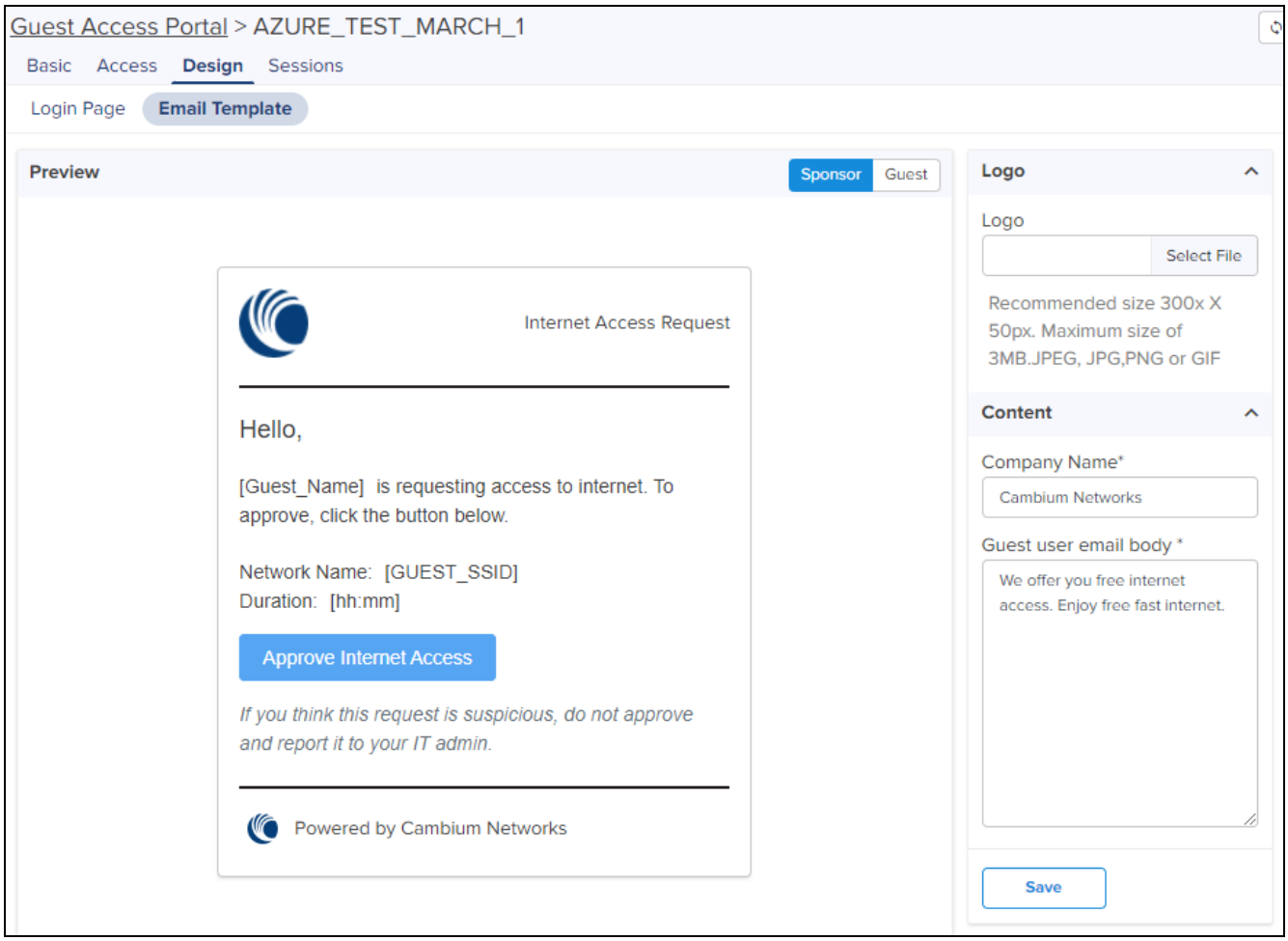
Parameter	Description
Enable Google Login	Select the checkbox to enable Google-based Wi-Fi access and configure the following parameters.
Device Limit	Specifies the number of devices that the guest can connect to the wireless network. Default: 5.
Google Login	
Enable Directory Synchronization	Select 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.

Designing the Guest Access Login Page and Email Templates

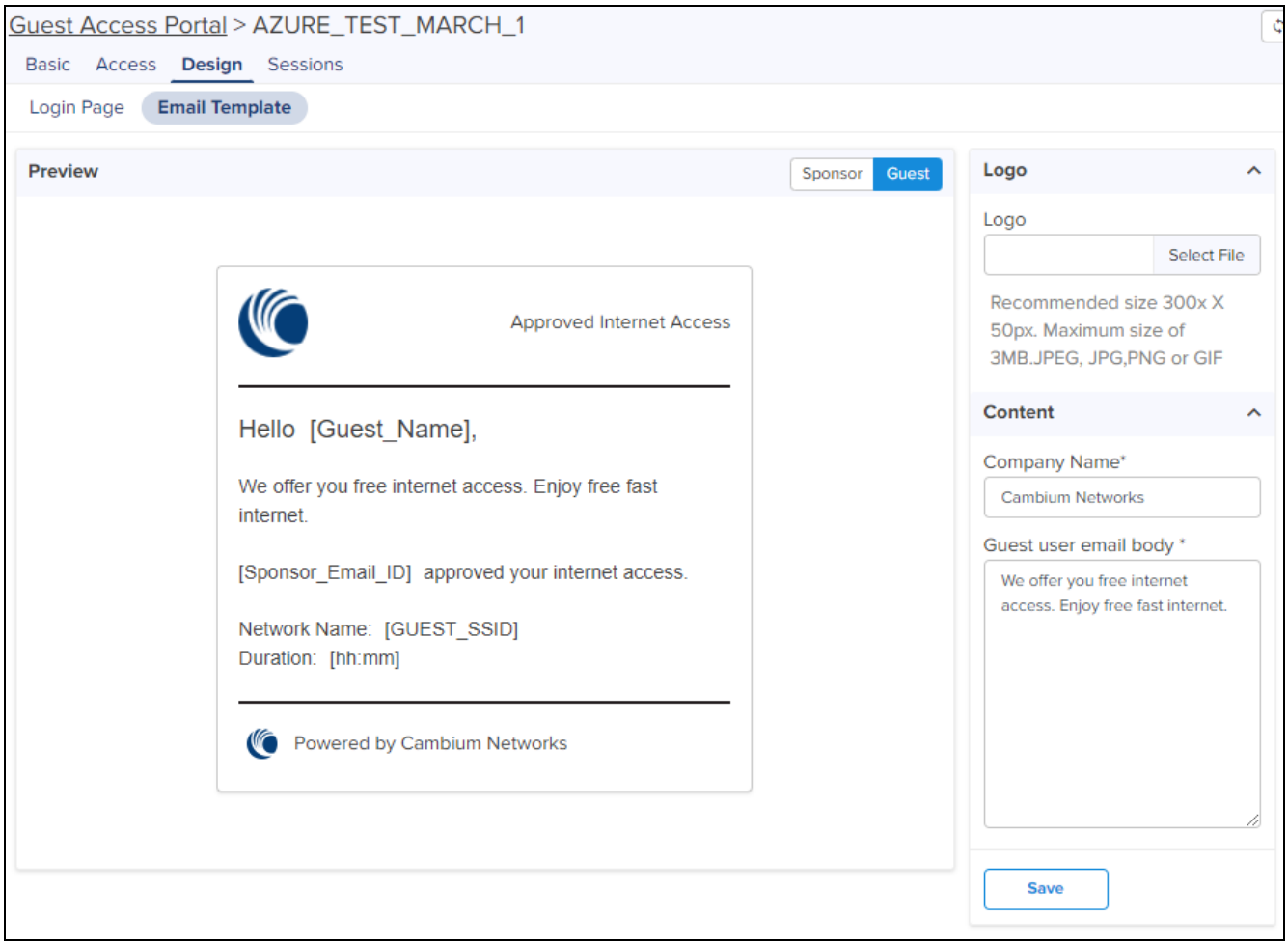
To design the guest login page for users to see when requesting access, navigate to **Network Services > Guest Access Portal > Design > Login Page**, complete the following parameters, and click **Save:**



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.

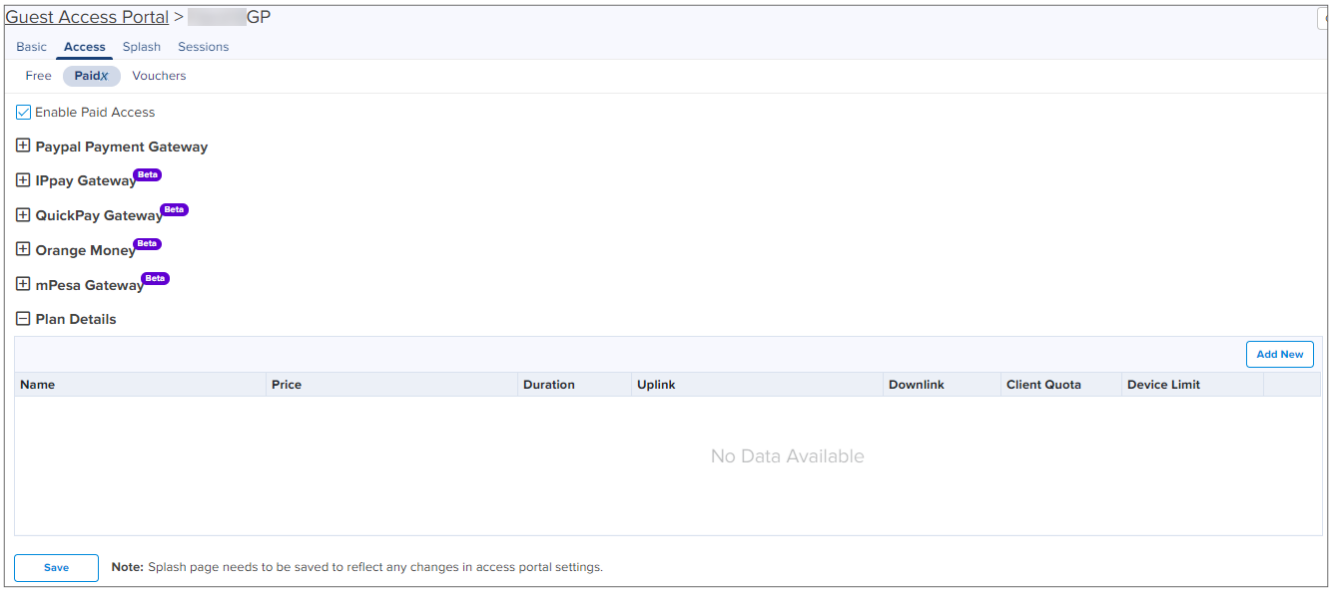
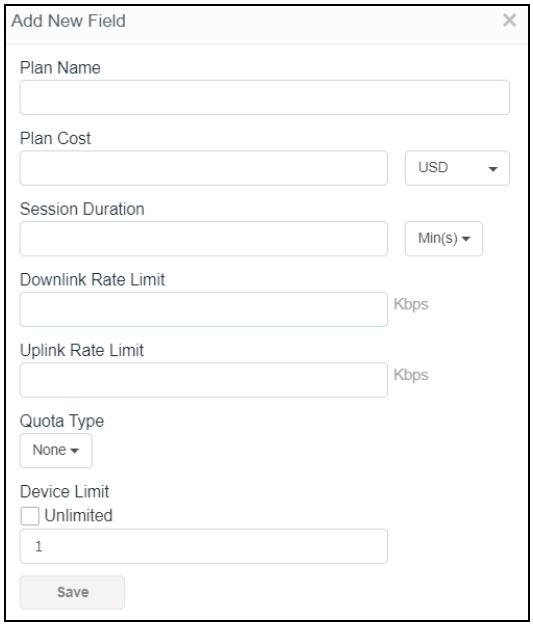


Table 192 *Paid Access Type Parameters*

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

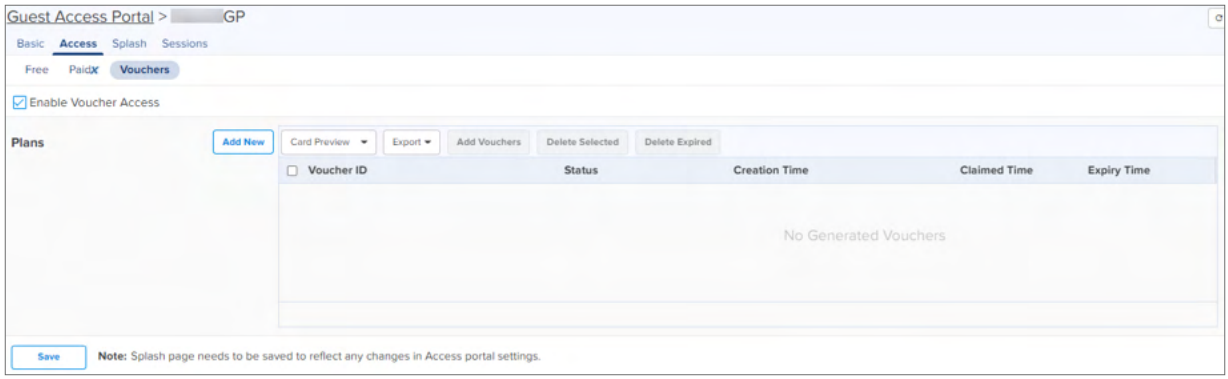
- Vouchers can only be generated after enabling Vouchers and creating at least one Voucher plan.
- The maximum number of vouchers that users are allowed to create per Voucher portal is as follows:
  - cnMaestro X—30,000

    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 193 *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. • **Voucher Device Limit**: Limit the devices to use the voucher.

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

Figure 669 ***Select a plan***

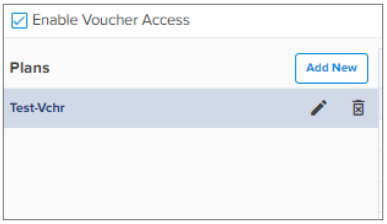
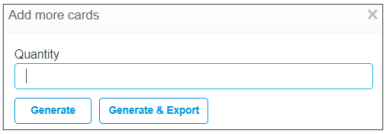


Figure 670 ***Add Vouchers***



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

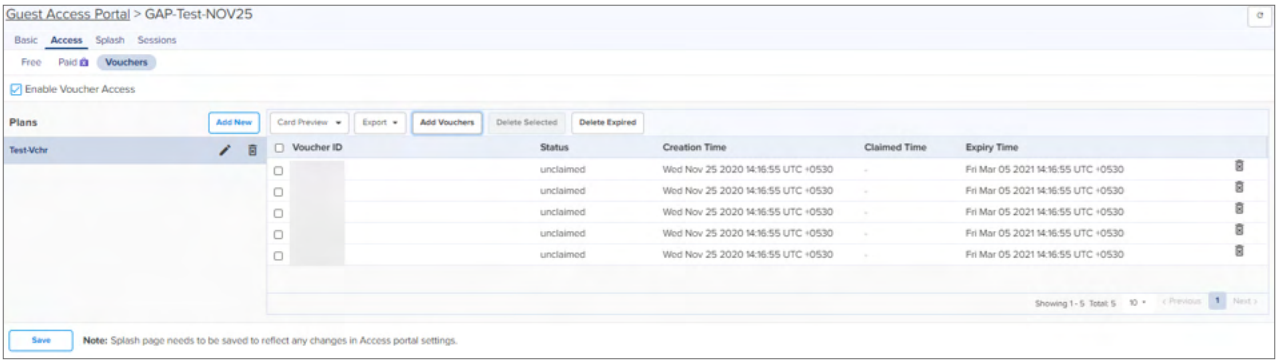


Figure 671 *Sample Voucher Code*



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.

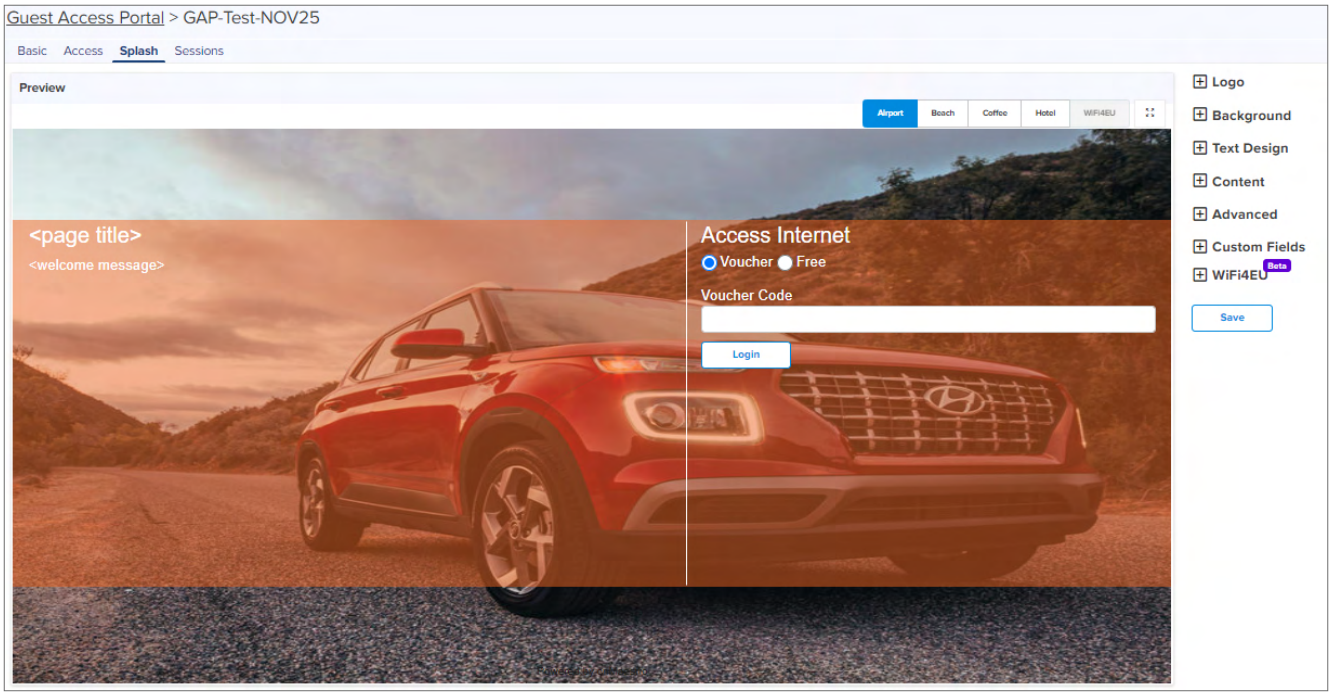


Table 194 *Design Page Parameters*

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 194 *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.

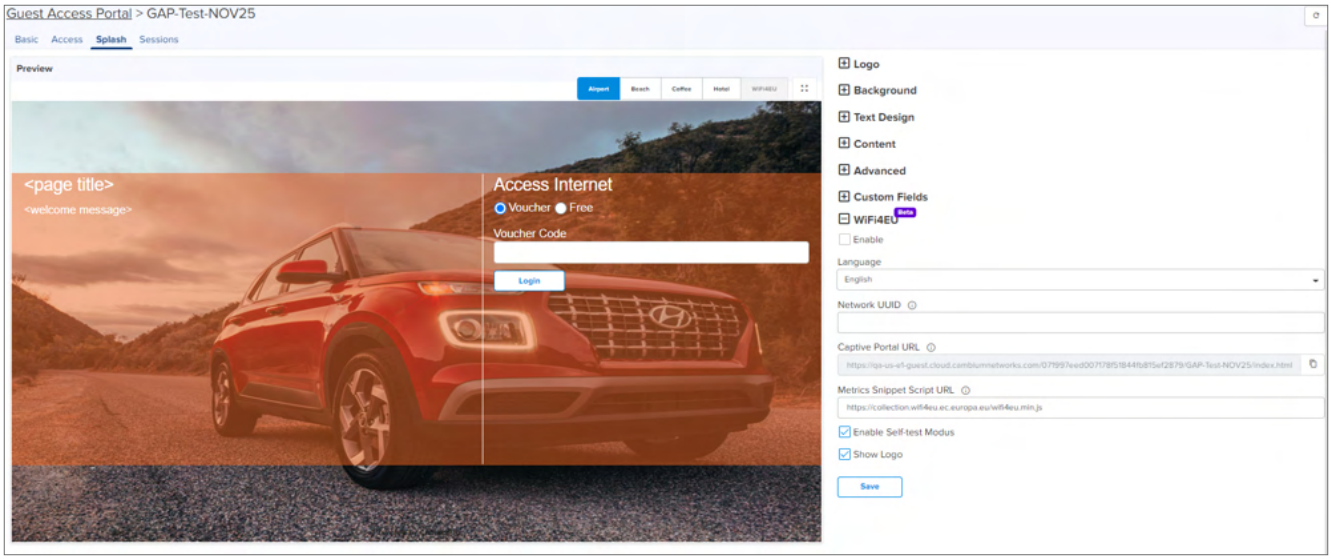


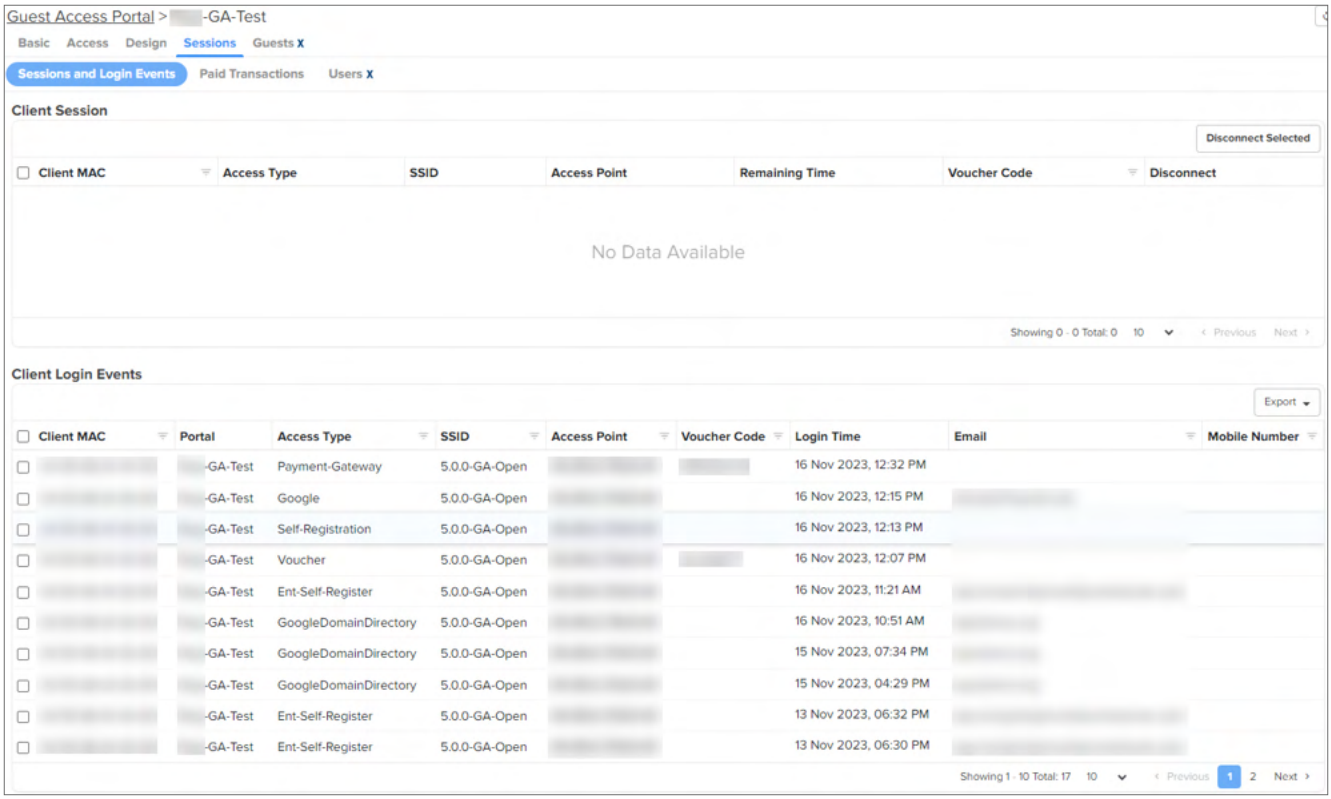
Table 195 *WiFi4EU Parameters*

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 196 *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.

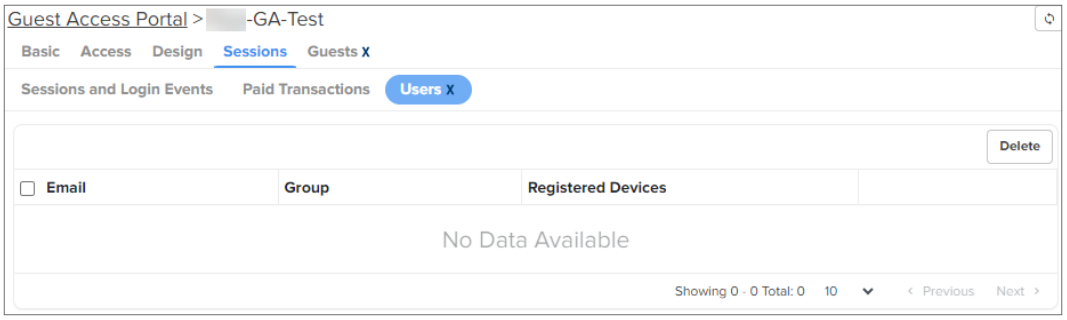


Table 197 *Users Table Parameters*

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

Guests X

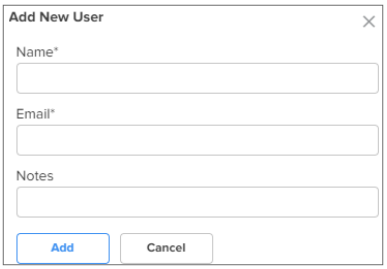
The Guests page allows you to view details of self registered guests connecting to the wireless network. However, to view this page, you must first enable and configure self registration under **Network Services** > **Guest Access Portal** > **Access** > **Enterprise X** > **Self Registration**.

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

To add a new user, complete the following steps:

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

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



2. Configure the name and email address of the guest in the **Name** and **Email** fields.

   Add a description, if required, in the **Notes** field.

3. Click **Add**.

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

the table

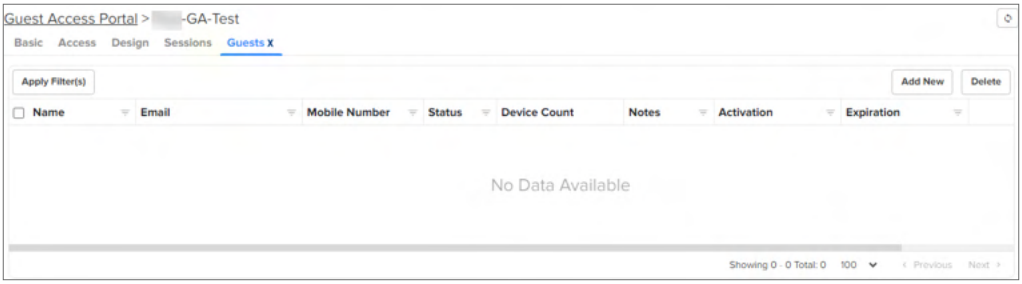


Table 198 *Guests Table Details*

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

Mapping the device to Guest Access Portal in cnMaestro

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

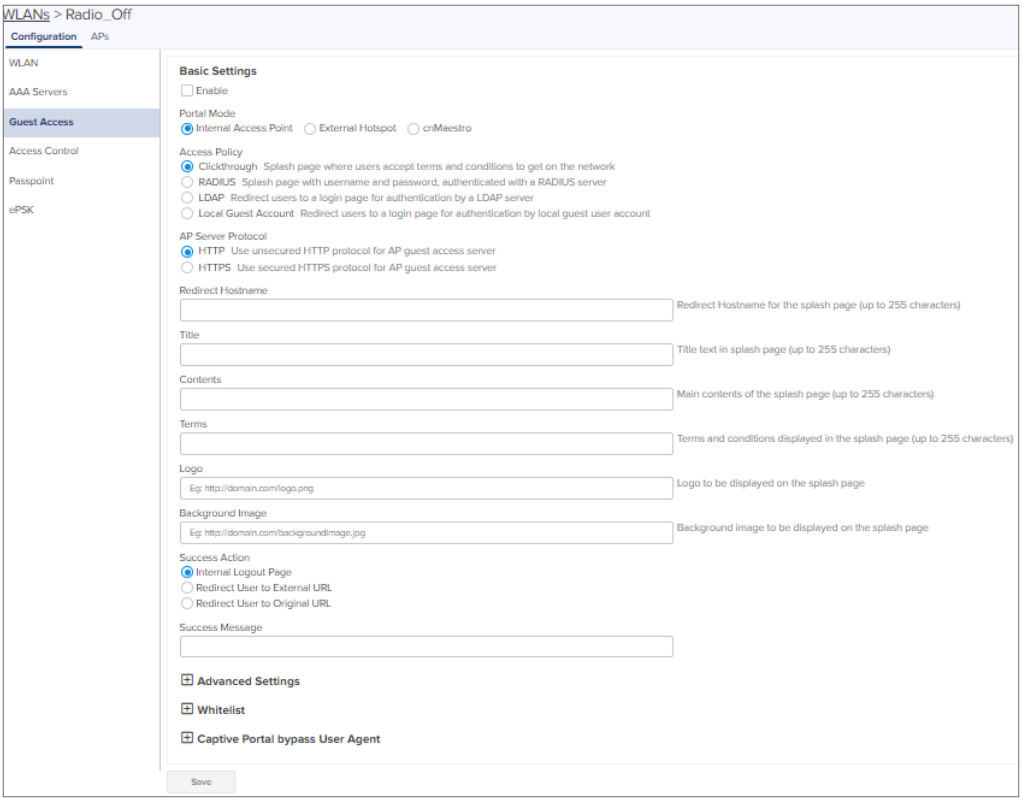
Note

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

Configuration at device level

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

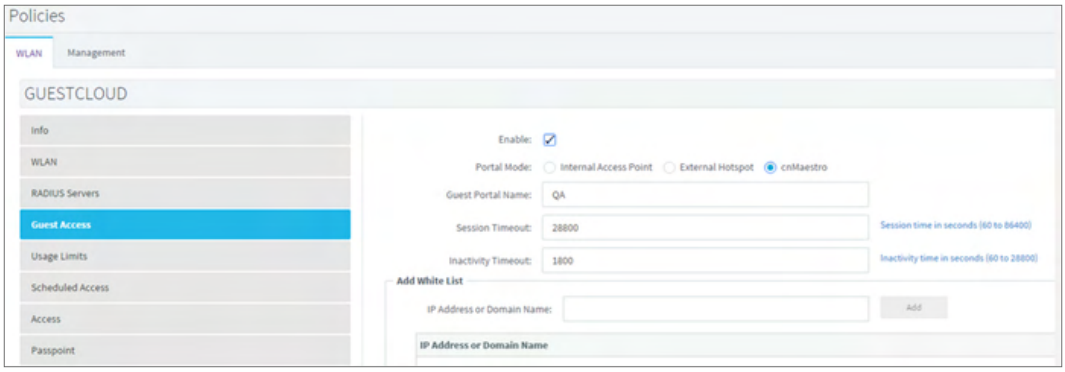
1. Login to the device.
2. Navigate to **Configuration** > **WLAN** > **Guest Access**.

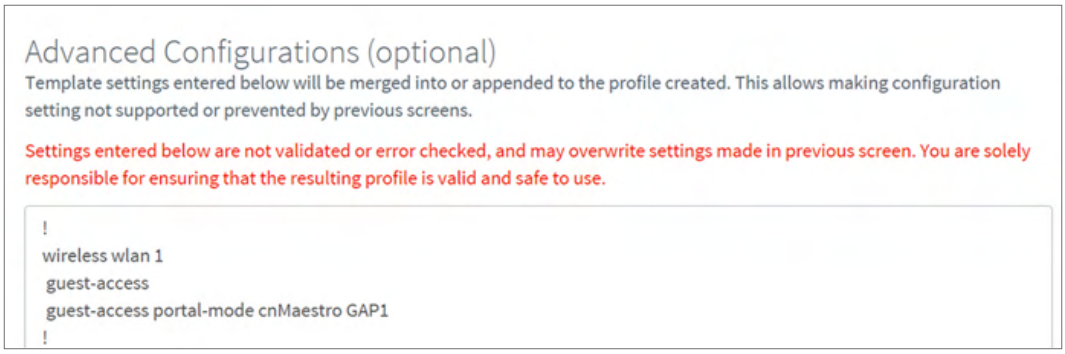


3. Enable the **Guest Access** checkbox.
4. Choose the **Portal Mode** radio as **cnMaestro**.
5. In the **Guest Portal Name** text box, select the name of the portal that was created in cnMaestro and enter the respective parameters.

Configuration at cnMaestro side

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

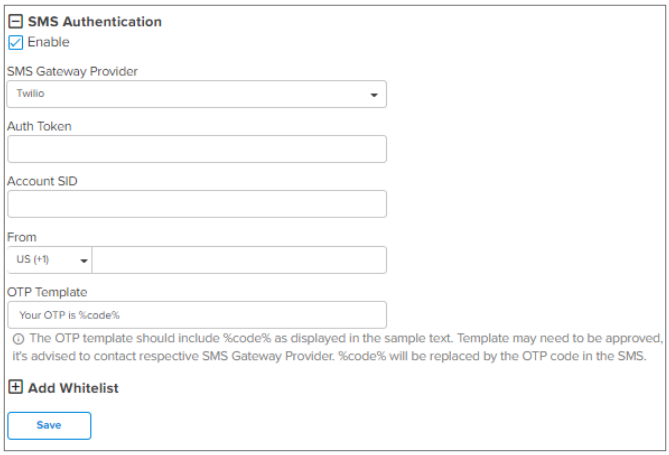




Access Types

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.

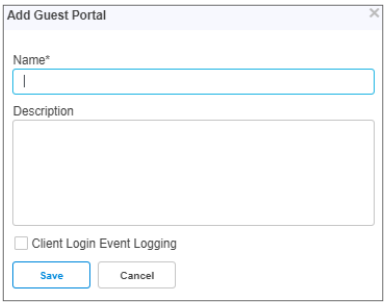
Guest Access using Social Login

Configuration

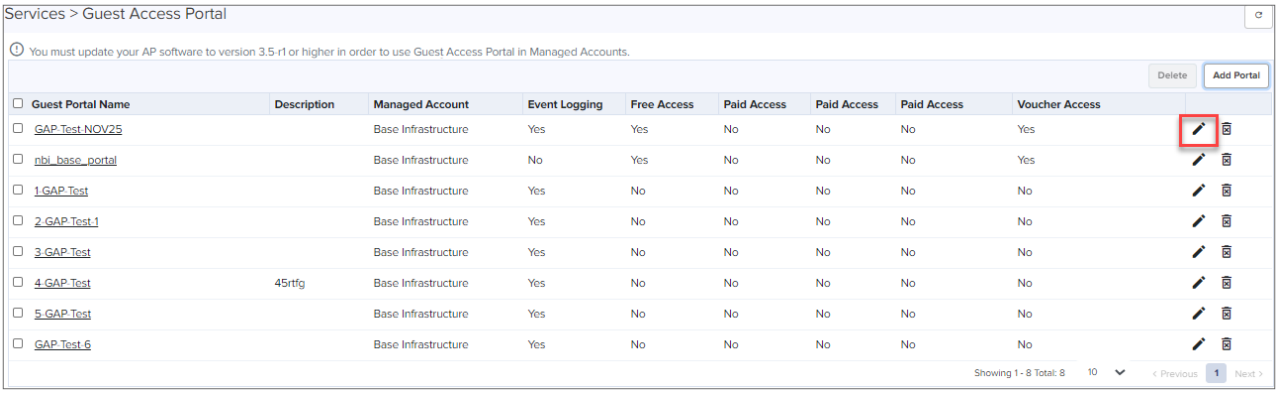
To achieve cnMaestro Guest Access using Social Logins like Google, Twitter, Facebook, and Office 365, perform the following steps:

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

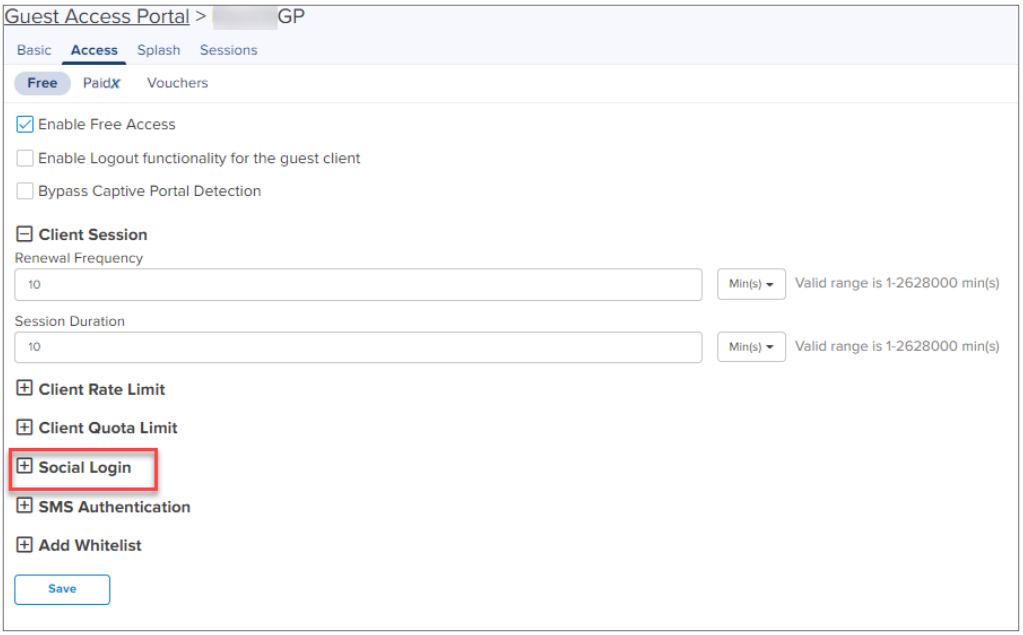
1. Login to cnMaestro and navigate to **Network Services > Guest Access Portal** > **Add Portal.**
2. Enter Portal Name, Description, enable logging for client login events.
3. Click **Save.**



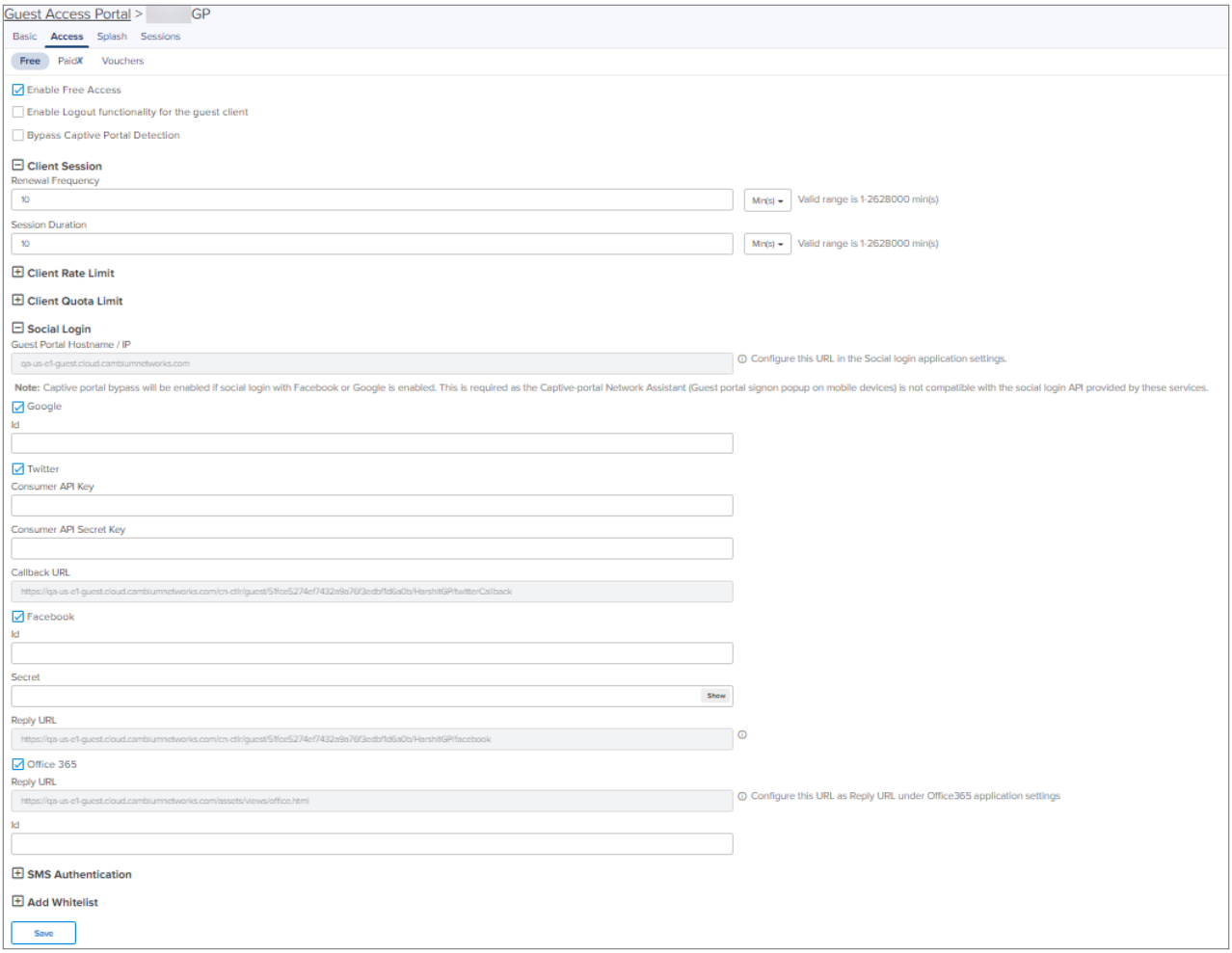
4. Click **Edit Guest Portal Details.**



5. Navigate to the **Access** > **Free** tab and expand the **Social Login** section.



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



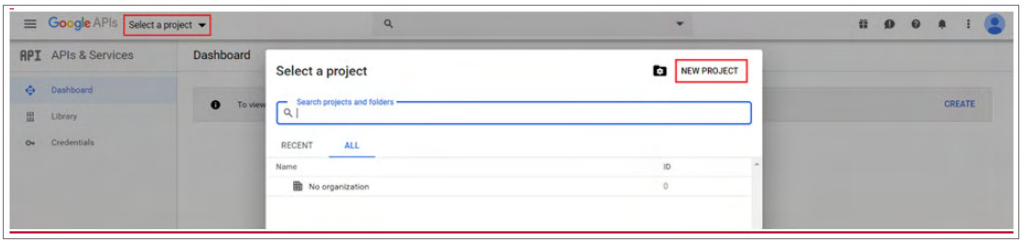
API Key Generation

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

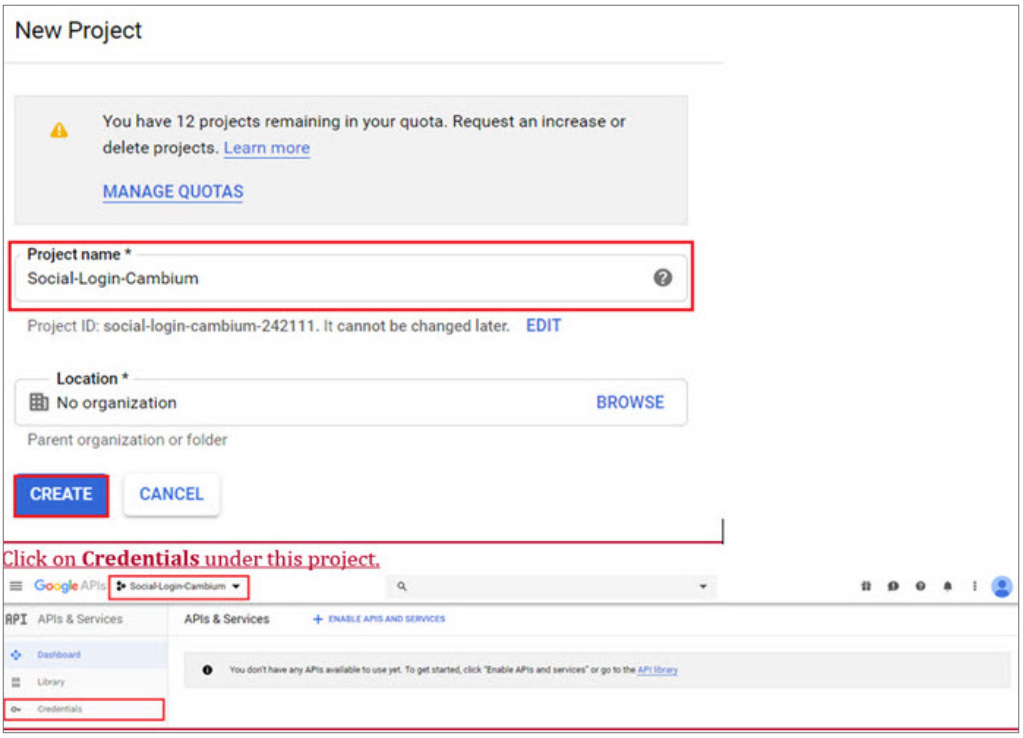
- Google
- Twitter
- Facebook
- Office 365

Google

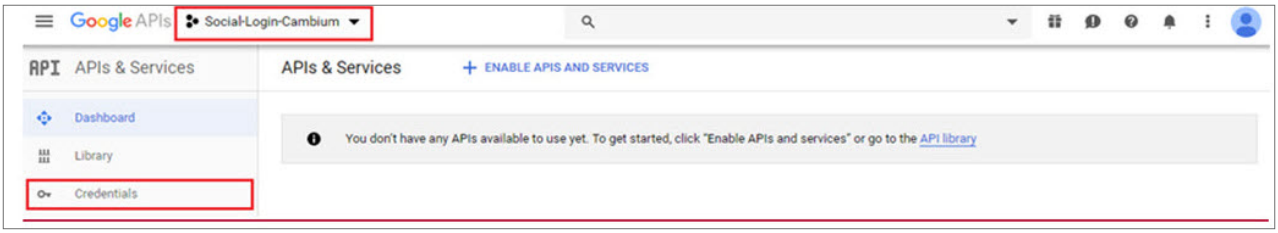
1. Login to Google Account and navigate to https://console.cloud.google.com/.
2. Click **Select a Project** and create a **New Project.**



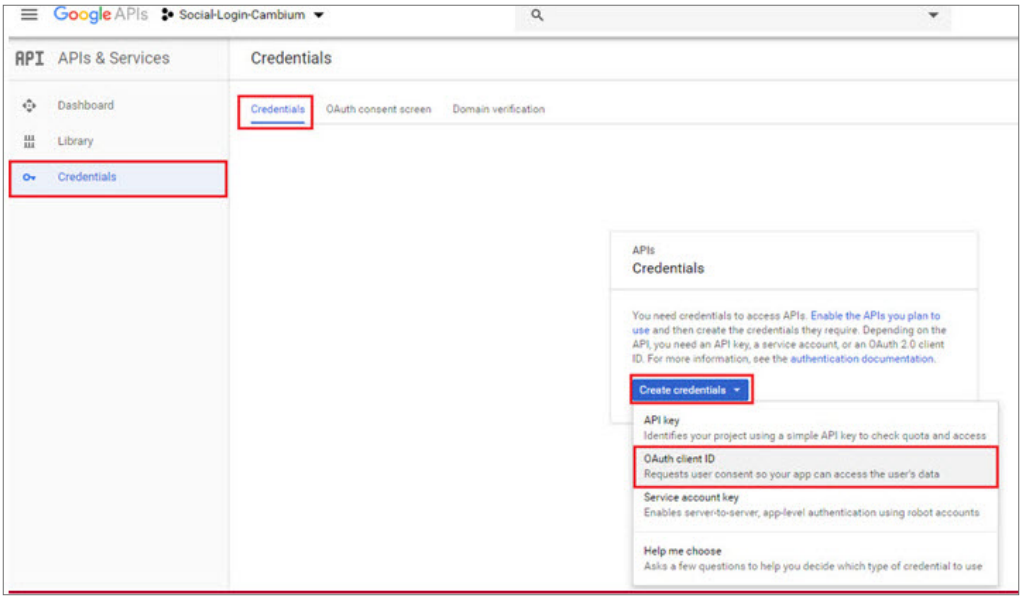
3. Give a name to the Project and click **CREATE**..



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



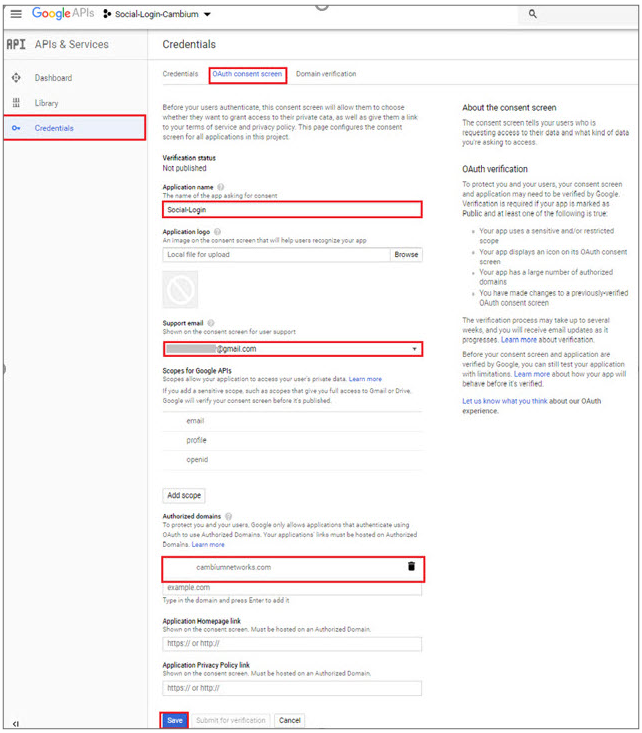
5. Under **Credentials** tab, create OAuth Client ID.



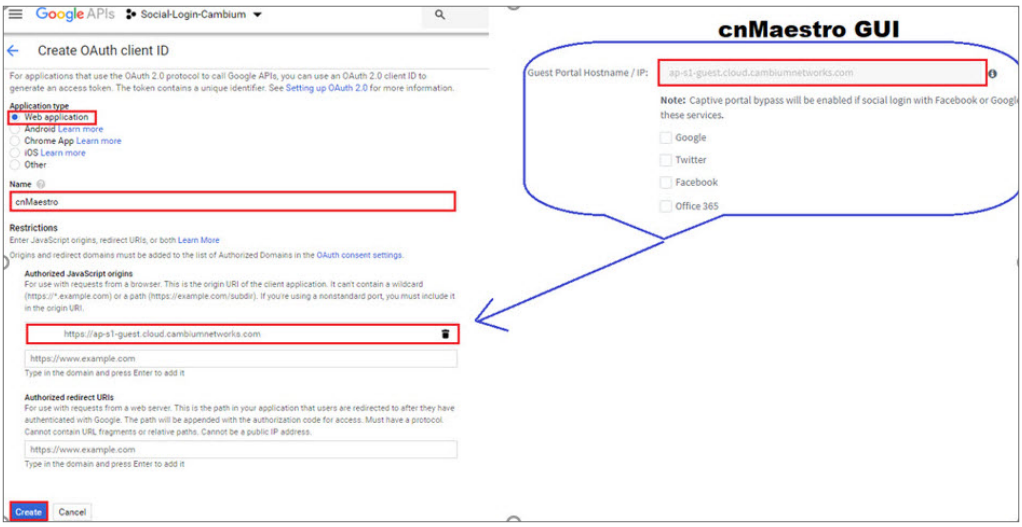
6. Click **Configure Consent Screen**



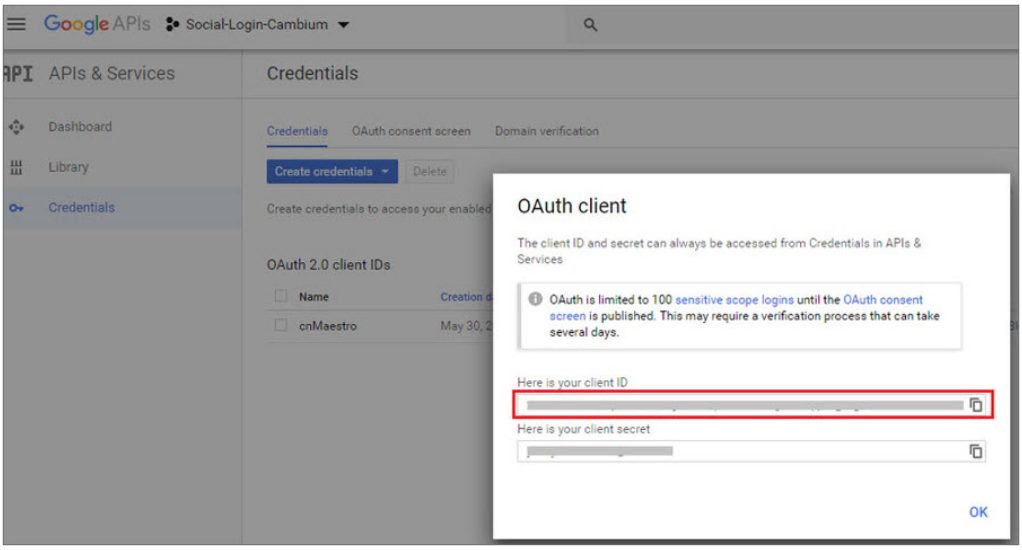
7. Assign a name to the application, map to an email address, add cambiumbnetworks.com to the authorized domain and click **Save**.



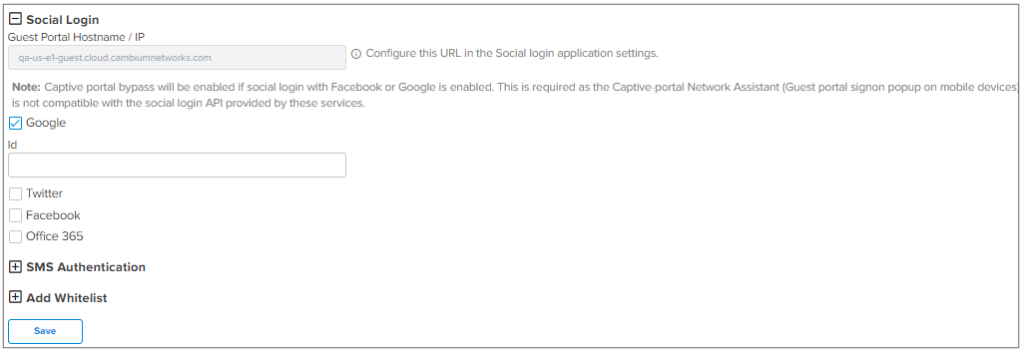
8. Once clicked **Save** for above page it redirects to creation of OAuth Client ID.
9. Select **Application type** as **Web Application**, give a Name, add Guest Portal Hostname URL/IP which you will get from cnMaestro UI and click **Create**.



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

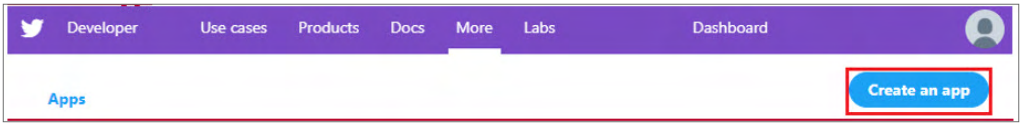


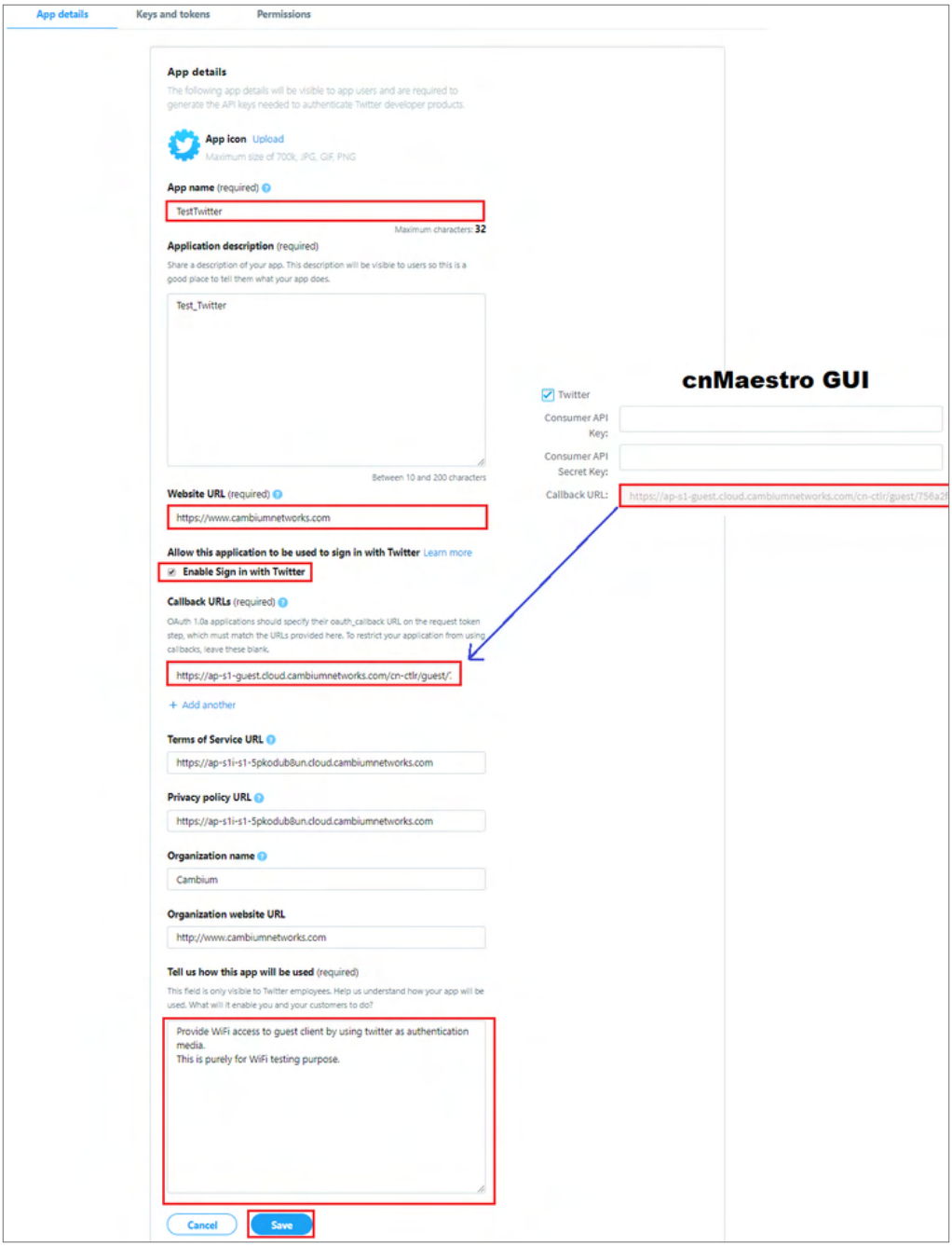
11. Copy the Client ID and paste it to the cnMaestro enabling Google under Social Logins and click **Save**.



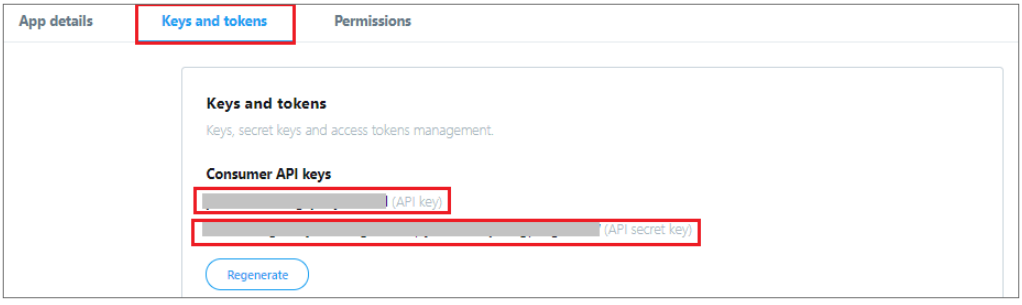
Twitter

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

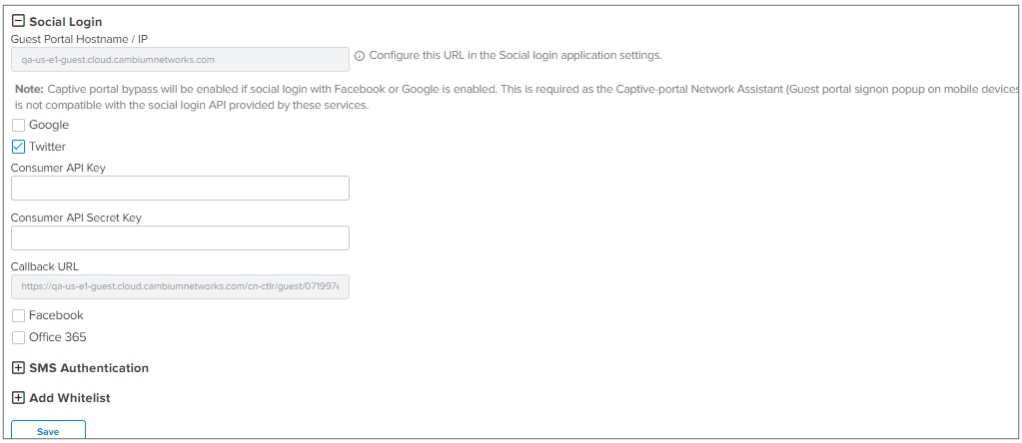




2. Click **Keys** and **Tokens** and copy **Consumer API Key** and **Consumer API Secret Key**..

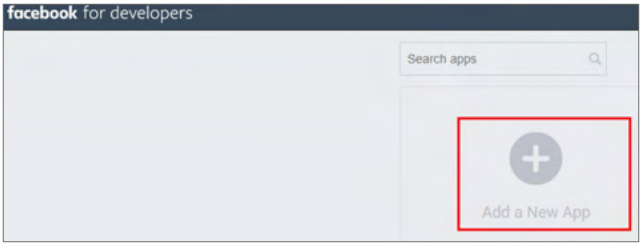


3. Paste them to cnMaestro GUI for Twitter social login.



Facebook

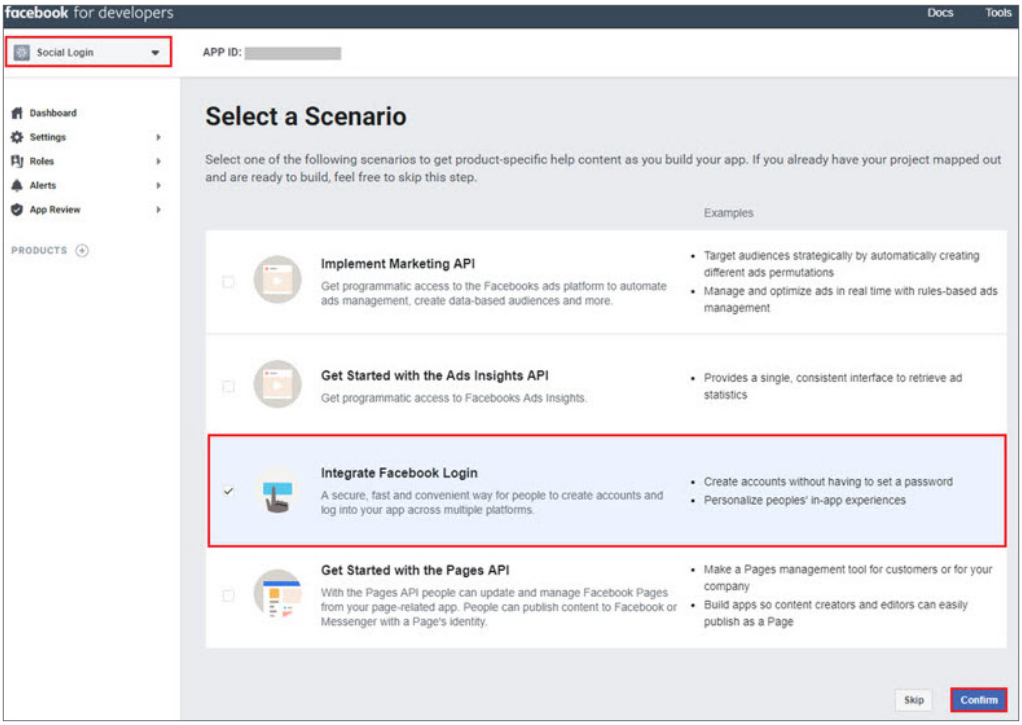
1. Login to Facebook Account and access **https://developers.facebook.com/apps/** and click **Add a New app**.



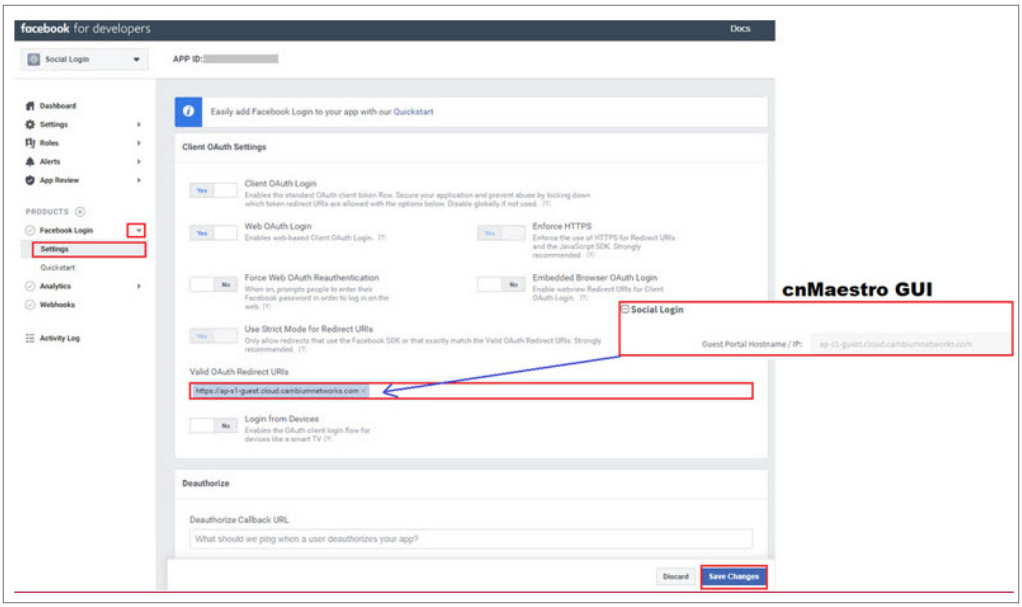
2. Enter App **Display Name**, **Contact Email**, and click on **Create App ID**.



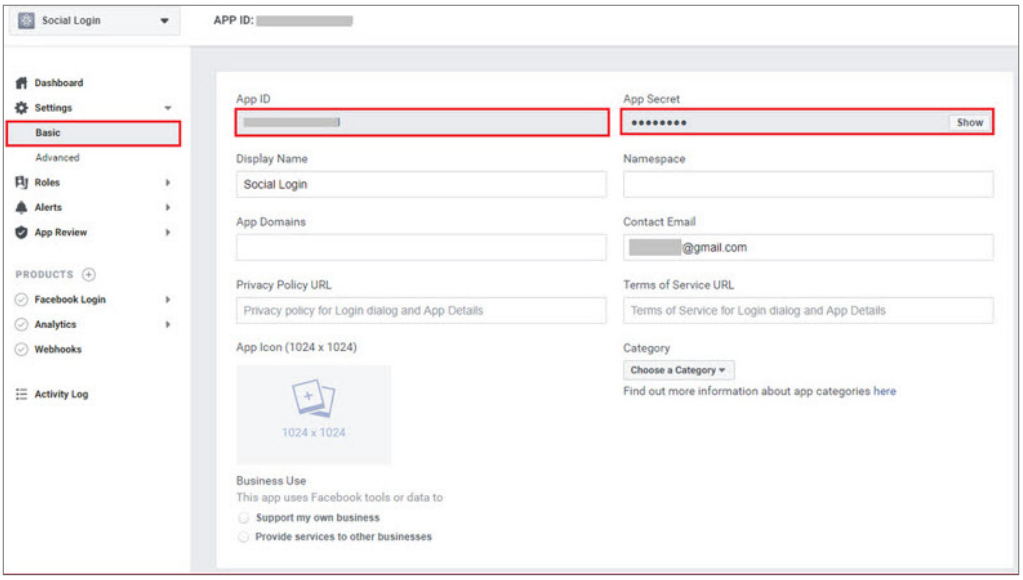
3. Select a Scenario as Integrate Facebook Login and click **Confirm.**

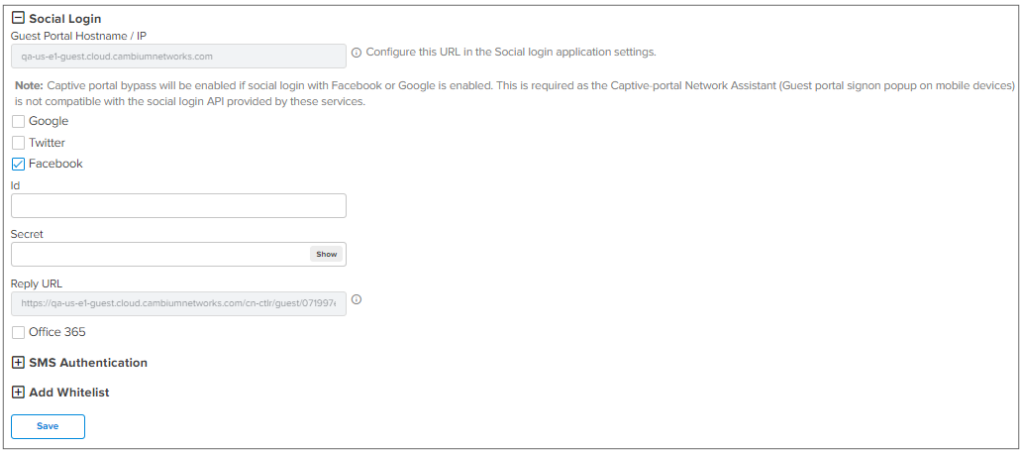


4. Navigate to **Settings** tab under Facebook Login and add Guest Portal Hostname from cnMaestro to Valid OAuth Redirect URLs section and click **Save Changes**.



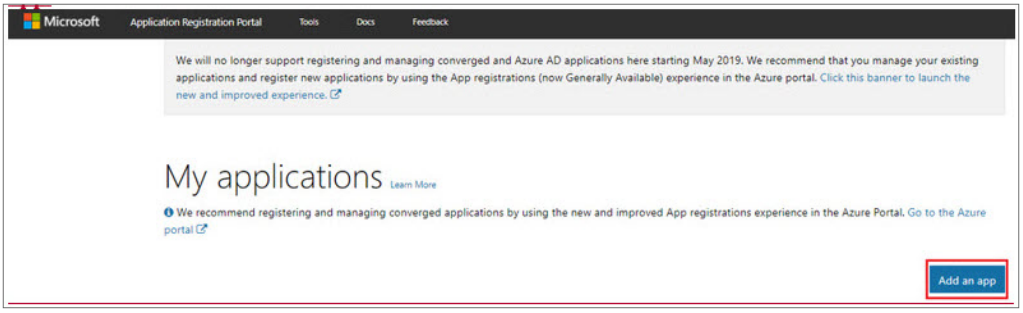
5. Navigate to **Settings** > **Basic** and copy **App ID** and **App Secret**.

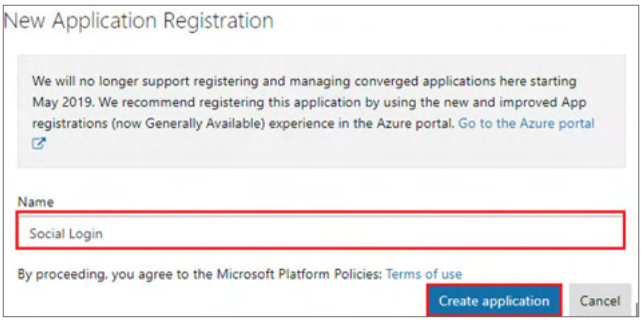




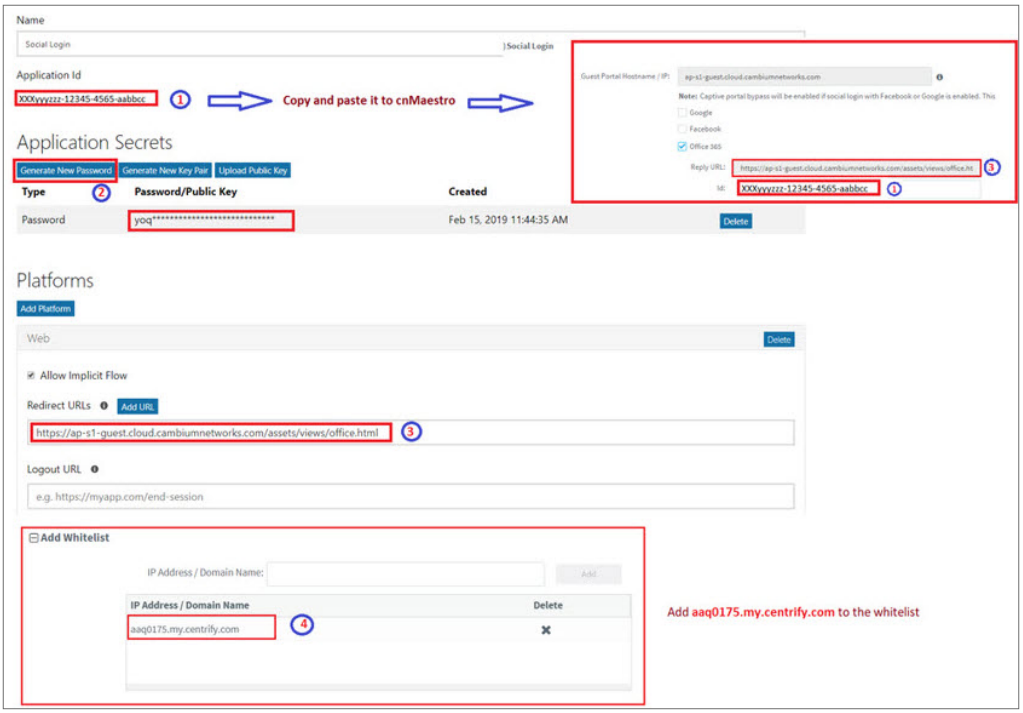
Office 365

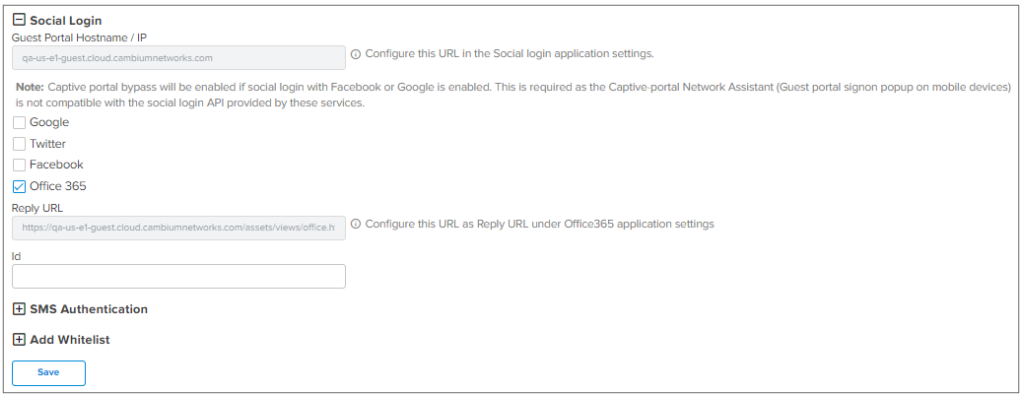
1. Login to Office 365 Account and access https://apps.dev.microsoft.com/ and click **Add an app**.





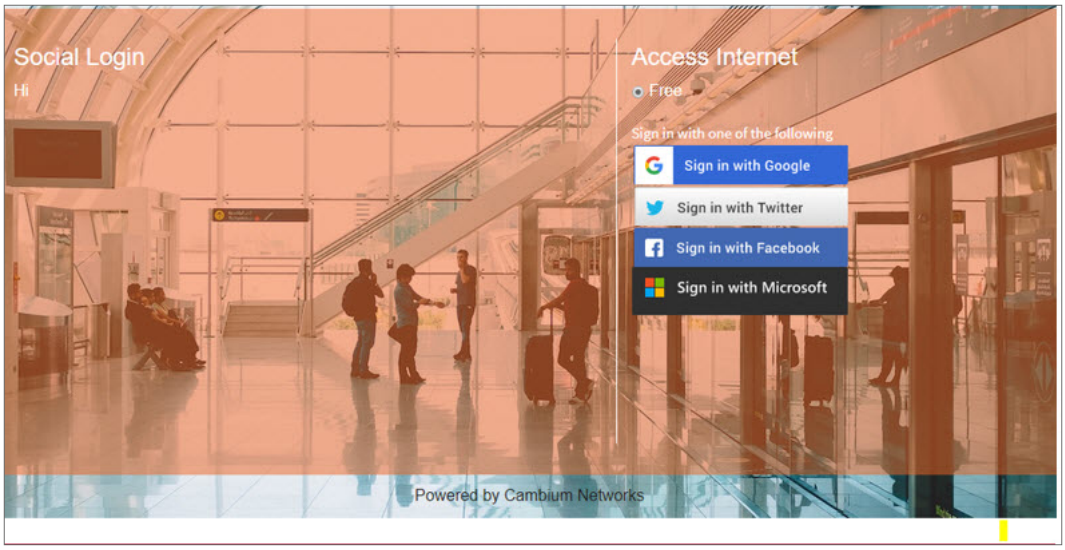
2. Upon Adding your App name and clicking Create application, it redirectes to App page.
3. Copy Application ID and paste it to cnMaestro Guest Access page under Office 365.
4. Click **Generate New Password**.
5. Copy Reply URL from cnMaestro and paste it under Redirect URLs.
6. Add my.centrify.com to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





Sample Template

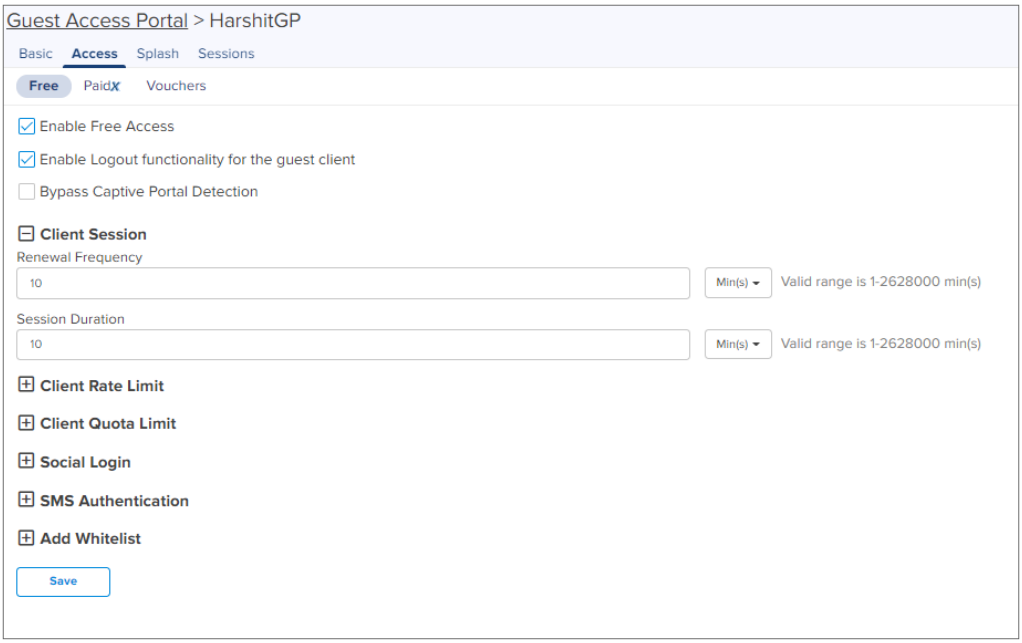
Sample of client login page is displayed below:



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.

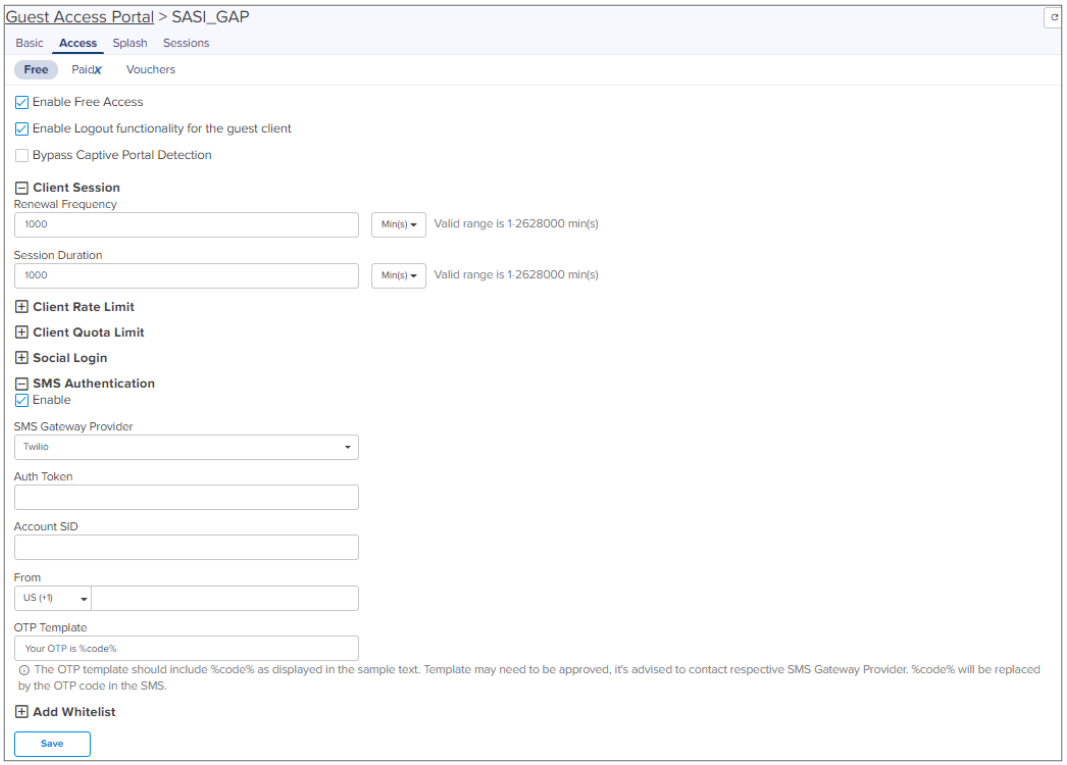
XML reply failure element value

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 672 *: Guest Access Portal*



Network Port Requirements

Network Port Requirements for Outbound Access

The following table provides information about network port requirements for APs to have outbound access to various services and applications:

Table 199 *Outbound Port Details*

Port Number	Port Type	Purpose
443	TCP	HTTPS Web access and device communication for the following URLs: • *.cambiumnetworks.com (for connecting to cnRouter and cnMaestro) • *.xirrus.com (for activation and license keys) • *.cloud.xirrus.com (for general communication with XMS-Cloud) • *.cloudfront.net (for software downloads) • *.amazonaws.com (for diagnostics)
53	TCP / UDP	For DNS resolution of the following URLs: • *.cambiumnetworks.com (for connecting to cnRouter and cnMaestro) • *.xirrus.com (for activation and license keys)

Table 199 *Outbound Port Details*

Port Number	Port Type	Purpose
		• *.cloud.xirrus.com (for general communication with XMS-Cloud) • *.cloudfront.net (for software downloads) • *.amazonaws.com (for diagnostics)
123	UDP	For accessing the time servers.



Note

There must not be any proxy or other devices blocking WAN access to the APs.

XMS-Enterprise to cnMaestro X

This section describes the process of migration from XMS-Enterprise (XMS-E) to cnMaestro X.

Before you begin migration, upgrade the following to the latest version:

- XMS-E to version 8.4.0
- Xirrus APs to version 8.7.0

Perform the following steps for migration:

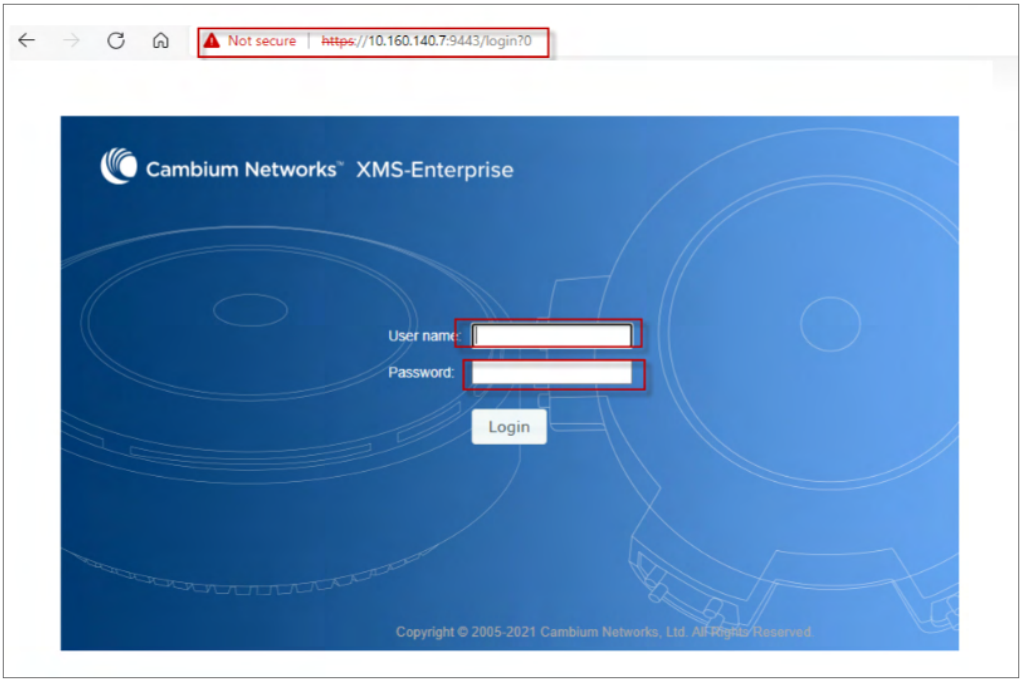
1. In XMS-E, perform the following actions:
   - Export Golden Configuration
   - Migrate to cnMaestro X
2. In cnMaestro X, perform the following actions:
   - Create Wi-Fi AP Group
   - Approve APs into Wi-Fi AP Group
   - Import and Apply AP configuration

XMS-E System

To login to XMS-E, complete the following steps:

1. Launch the Web login page.
2. Enter the username and password.

3. Click **Login**.

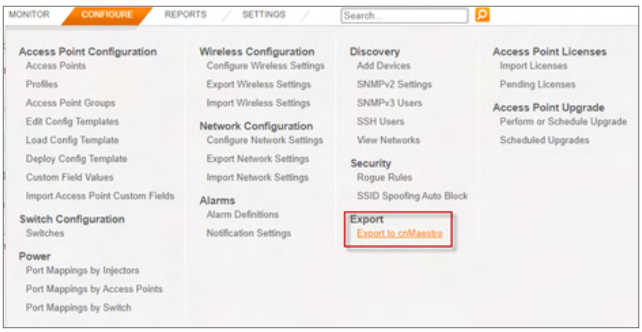


Export Golden Configuration

Export Golden Configuration for one of the APs. It is saved as a zipped file in the local file system.

To start export golden configuration in XMS-E, navigate to **Configure** tab > **Export**.

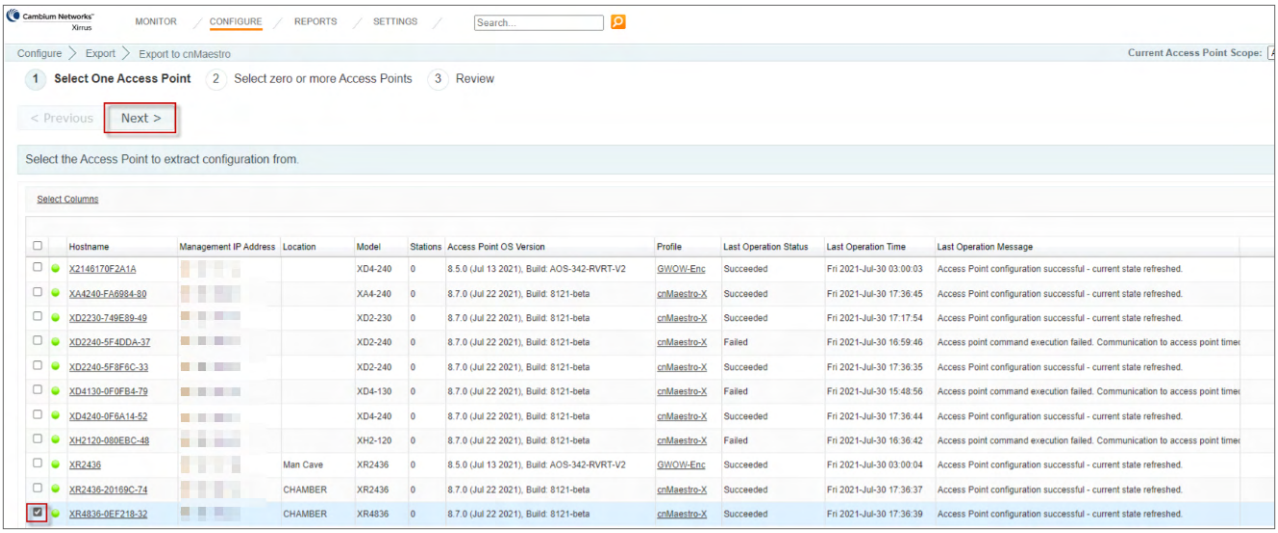
1. Select **Export to cnMaestro**.



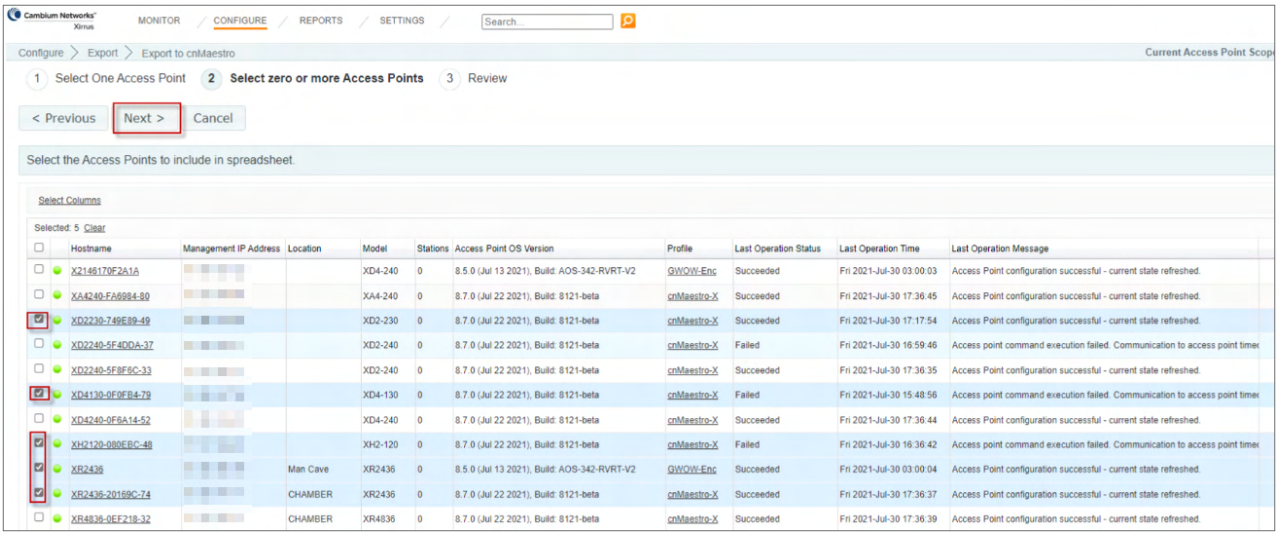
2. Select the AP to create the golden configuration for a group of APs and click **Next**.

Note

- Select the AP with the maximum radios and the highest capability.
- During the migration of an AP from XMS-E to cnMaestro, the AP configurations are not modified.



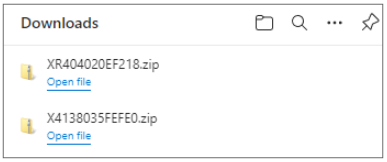
3. Select group of APs to be added to the spreadsheet and click **Next**.



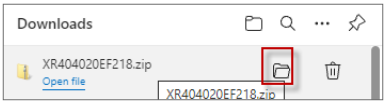
4. Click **Export**.

   In Local System unzip the directory and files to local directory.

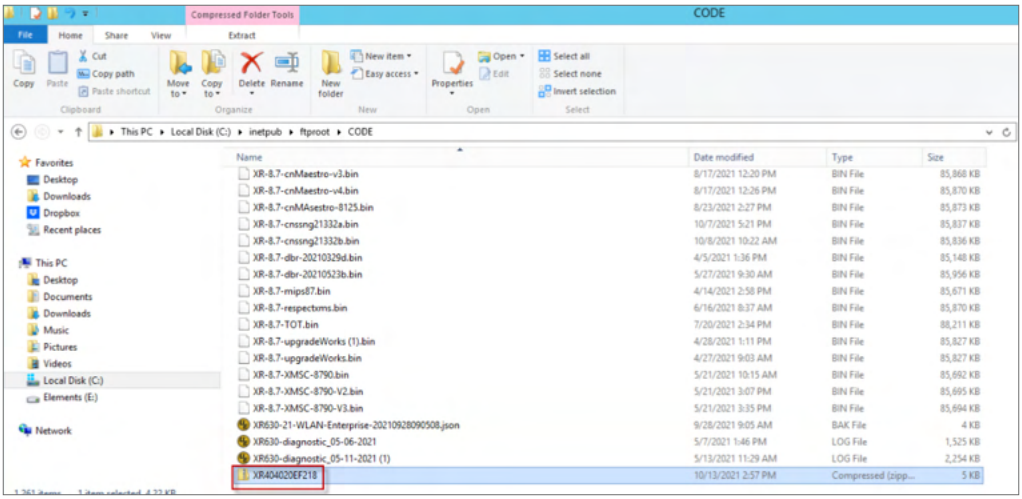
5. Download the zip files from the browser window.



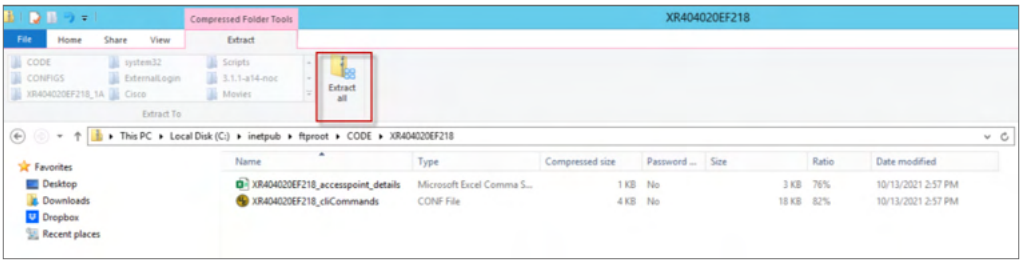
6. Go to the folder where the zipped files are saved and extract the contents to a folder.



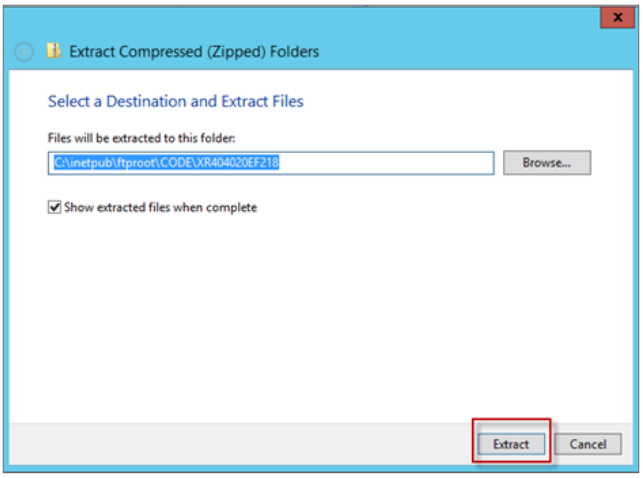
7. Open the directory path where the file has been stored and double-click on the zipped file.



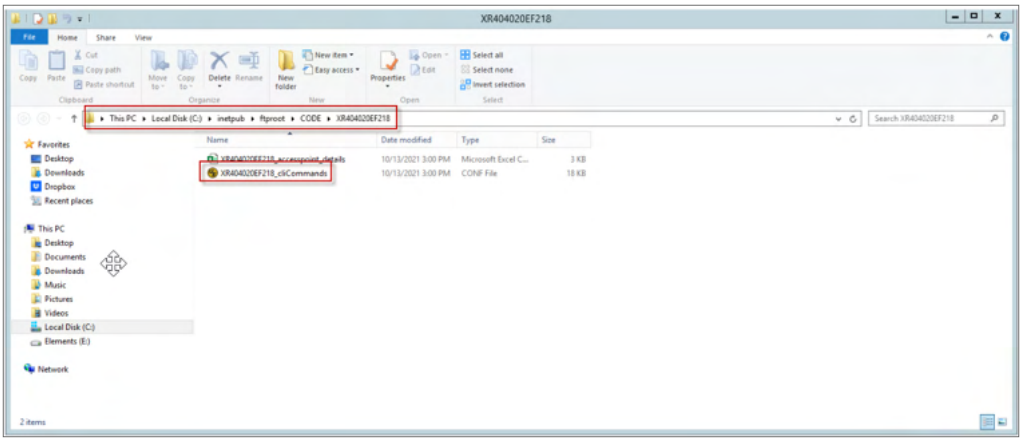
8. Click **Extract all**.



9. Extract the folder to the path.



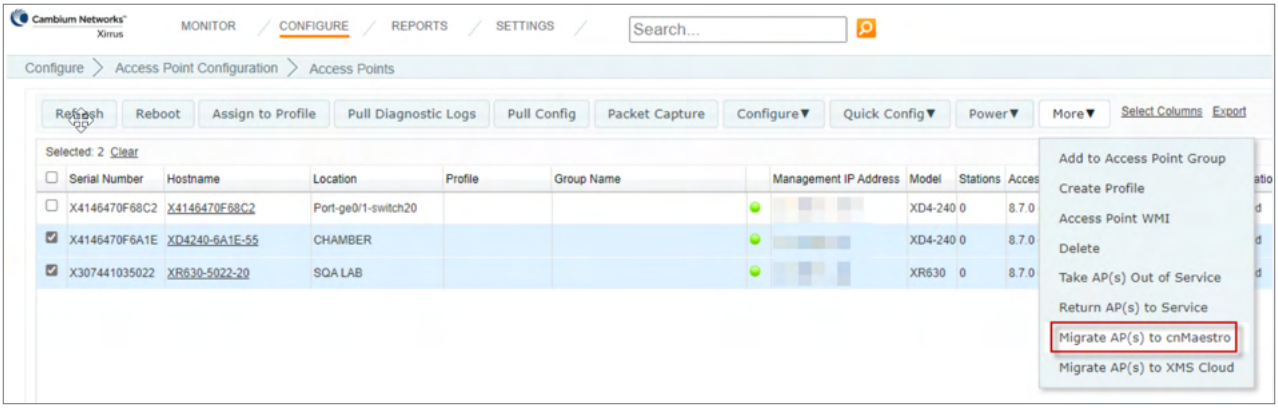
10. Make a note of the folder or file location as you will require this file later.



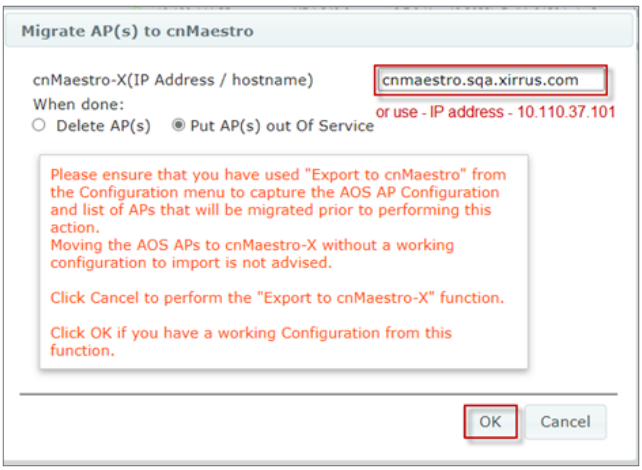
Migrate to cnMaestro X

Select APs to migrate to cnMaestro X. Perform the following steps:

1. Navigate to the **More** menu > select **Migrate APs to cnMaestro.**



2. Enter the IP address or Hostname mapped in DNS for cnMaestro X.
3. Select **Delete AP** or **Put AP(s) out of Service** and click **OK.**

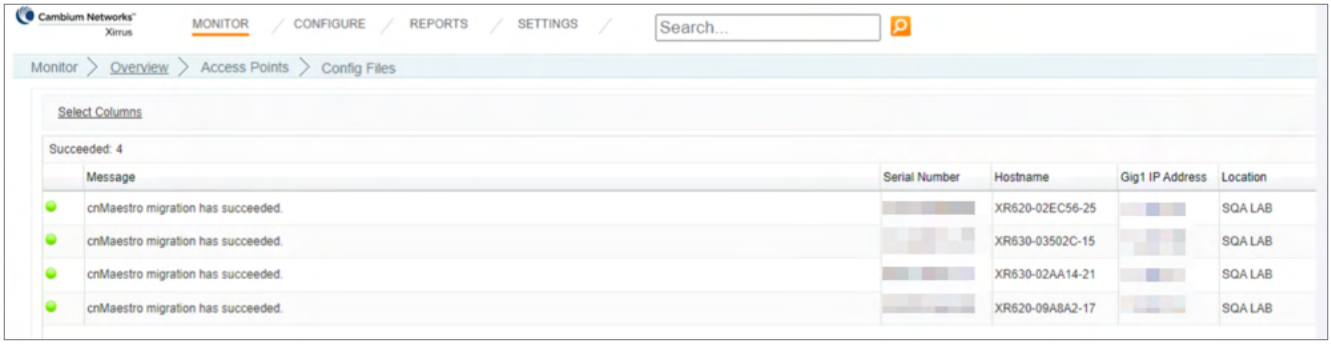


Note

- Out of service APs are not removed from XMS-E, so if there is an issue, select the **Return APs to Service** option and they will return to XMS-E.

- You must reset using the `snmp trap host 1 Xirrus-XMS` AP CLI command on the AP for the return to service to work.
- If you select **Delete APs**, they will be removed and you must rediscover them on the network to return them to XMS-E.
- You should also remove the Device Network from the Device discovery section to clean up XMS-E.

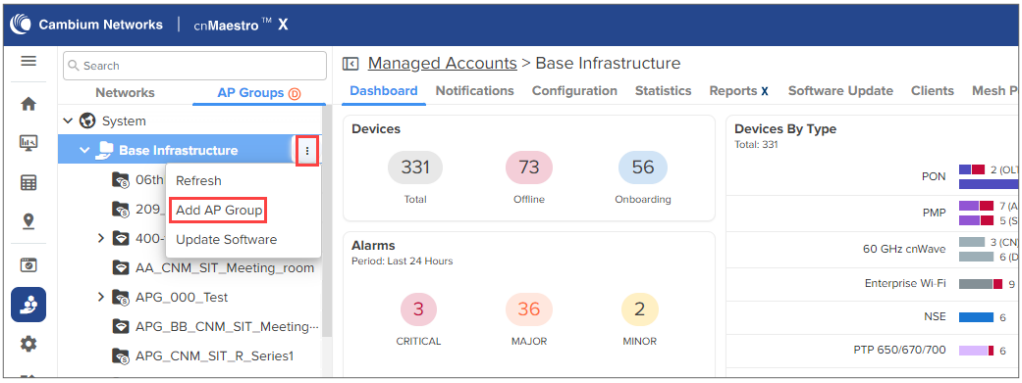
A success message from XMS-E for each of the APs migrated to cnMaestro X is displayed.



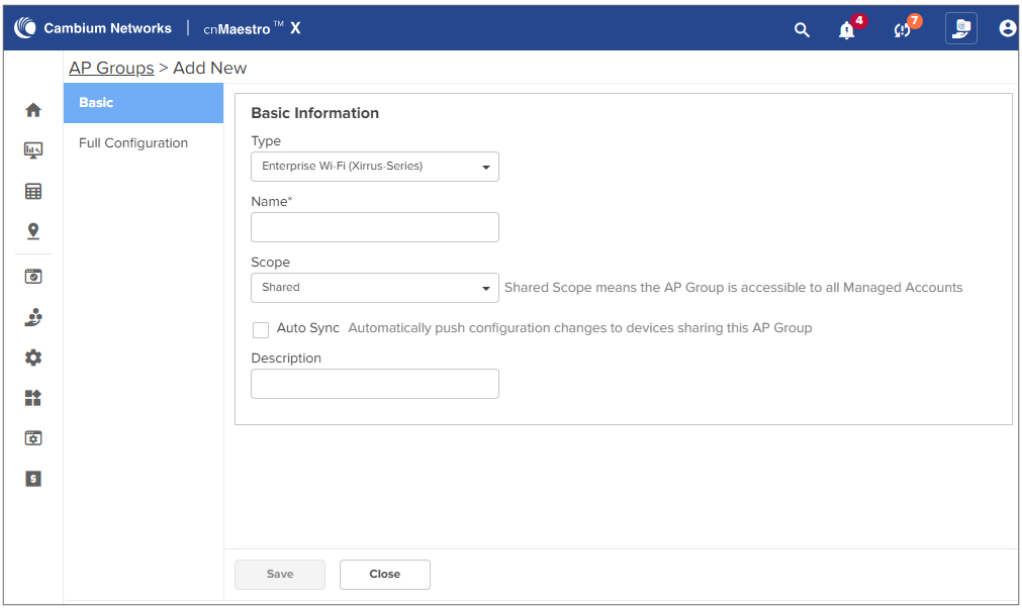
Create Wi-Fi AP Group

Create Wi-Fi AP Group and Import CLI command file from exported directory.

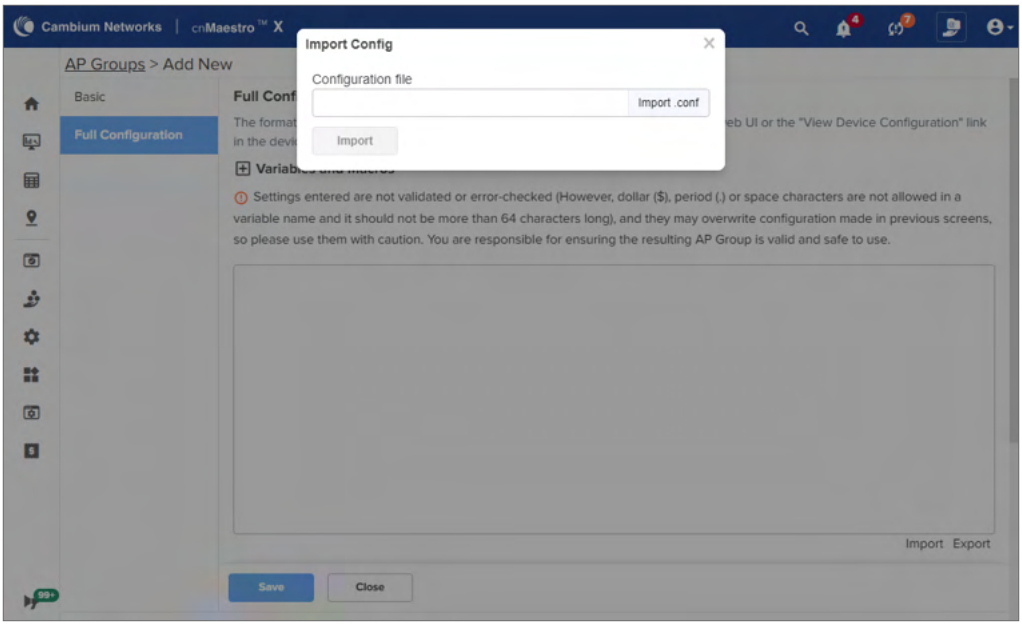
1. Navigate to **Wi-Fi AP Group** > **Base Infrastructure** > click action (⋮) icon to add **Add AP Group**.



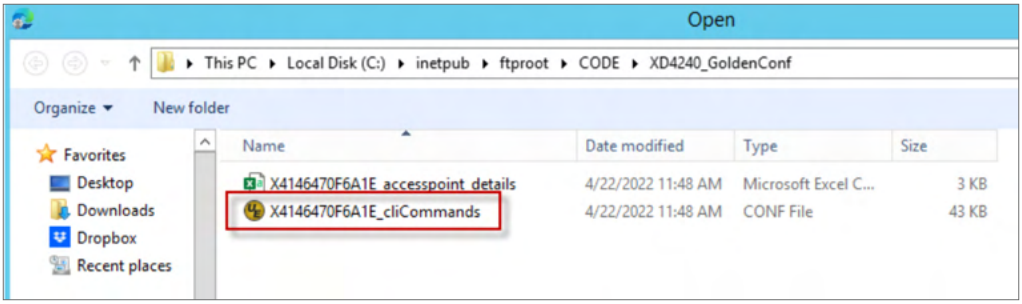
2. In the **Basic Information** page, select Type as **Enterprise Wi-Fi (Xirrus-Series)** from the dropdown.
3. Select the **Auto-Sync.**
4. Click **Save.**



5. In the **Full Configuration** page, click the **Import** option.



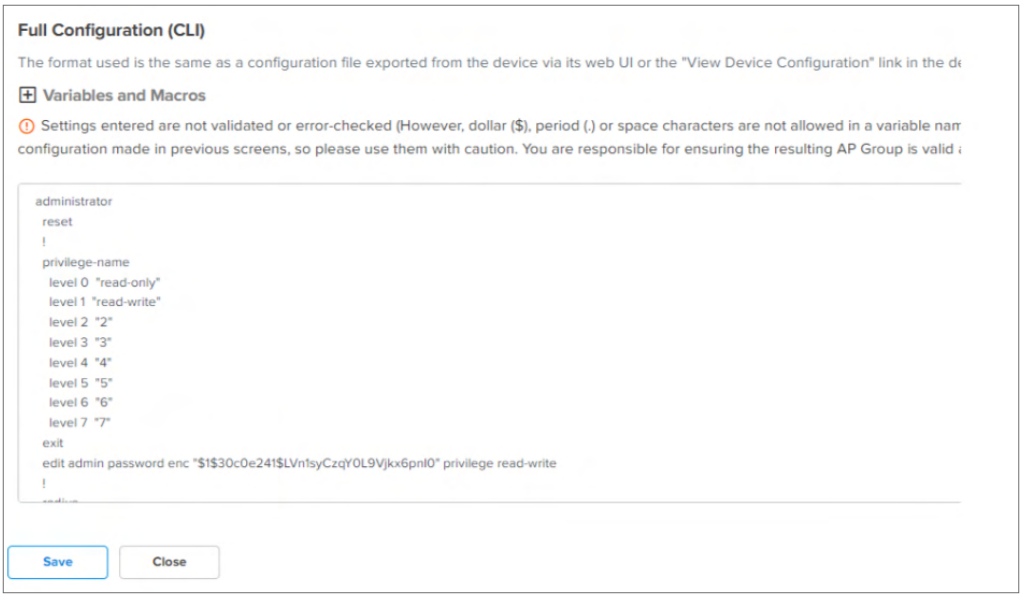
6. Select the CLI command file from the unzipped directory.



7. Click **Import**.



The configuration file is displayed.



8. Click **Save**.

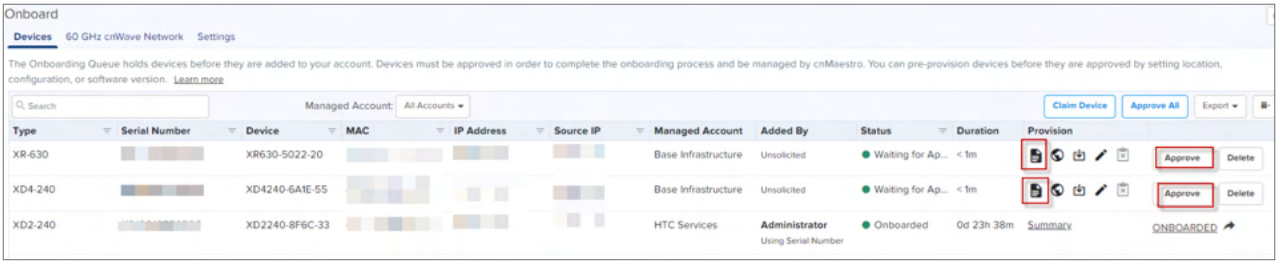
Approve APs into Wi-Fi AP Group

APs pending for approval in cnMaestro X based on the **Migrate APs to cnMaestro X** steps as described above.

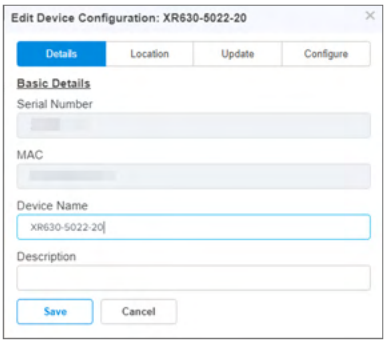
You can claim APs to approve from the **Onboard** > **Devices** page.

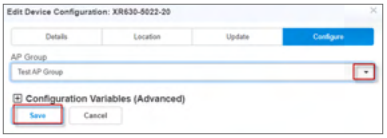
Perform the following steps to approve APs from the **Onboard** > **Devices** page.

1. Navigate to the **Onboard** > **Devices** page and click **Approve All** (to approve all devices at once) or **Approve** (to approve devices individually.)



2. Enter the required details, provision the device for location, and assign to an AP Group.

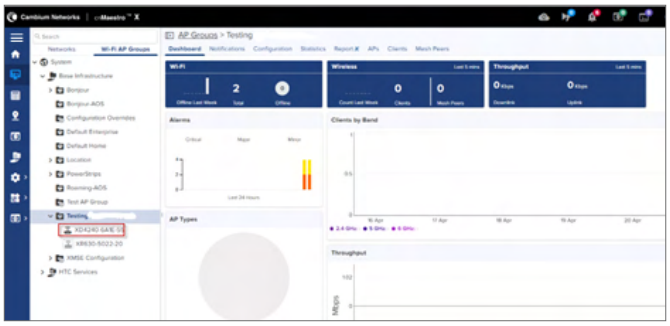




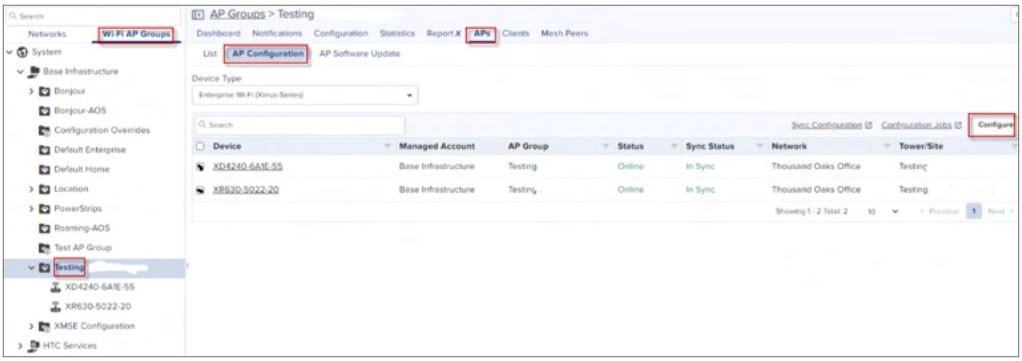
3. Click **Save.**
4. In the **Onboard** > **Devices** page, select **Approval All** (to approve all devices at once) or **Approve** (to approve devices individually.)

Import and Apply AP configuration

APs imported are ready for basic configuration. Import AP configuration using the CSV file from the exported directory.



1. Navigate to **Wi-Fi AP Group** > select **AP Group** > **AP Configuration**.
2. Select all APs to configure, click **Configure.**



3. In Device Override table, verify AP details and click **Import.**

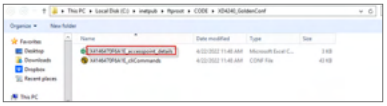
Note

Email and Phone fields are auto populated from the .csv file.



4. Select the .csv import file from the unzipped directory folder and click **Apply**.





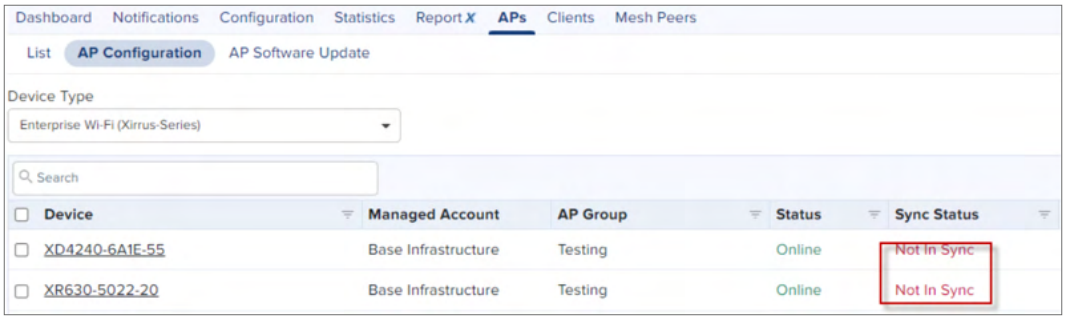
All the configuration values from the CSV file are populated for each AP. The data is auto populated to the **User Defined Variables** tab. The APs receive complete configurations including all IAP settings.



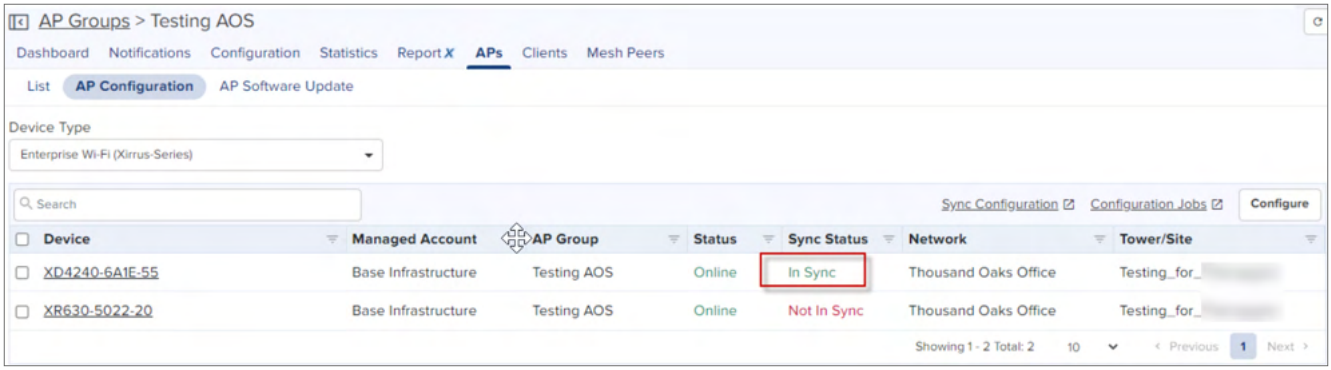
5. Click **Apply Configuration.**



When the APs are completely configured, **Sync Status** is displayed as **In Sync**.



You have to refresh the page to view the updated **Sync Status.**



Converting Tier 2 Unused Slots

Cambium Networks has introduced new product family-based cnMaestro X SKUs and pricing for devices such as Fixed Wireless Broadband APs, cnRanger, cnReach, cnVision, PMP, ePMP, and PTP. Earlier, the Tier 2 subscription was used to control these devices (pricing). To simplify the purchase and onboarding for these devices, Cambium Networks has decided to remove the Tier 2 subscription and introduce new four tiers (Tier 21, Tier 22, Tier 23, and Tier 24).

The Tier 2 subscription is no longer valid now. Due to Tier 2 subscription removal, there can be unused Tier 2 slots in your account (purchased during the Tier 2 subscription). As a solution, Cambium Networks provides an option to convert these unused Tier 2 slots into new tiers based on the device family and requirements. You can manually convert the unused Tier 2 slots to Tier 21, Tier 22, Tier 23, and Tier 24 using the ⓘ icon located on the **Manage Subscriptions** page (cnMaestro UI). This solution helps in better mapping and device management.



Note

The Convert Tier 2 option is effective from March 1, 2024 for Fixed Wireless Broadband APs, cnRanger, cnReach, cnVision, and PTP devices. You must convert the unused Tier 2 slots in your account to the new Tier 2x slots before onboarding the devices.

When you convert the unused Tier 2 slots into new tiers, you cannot change the new tiers back to Tier 2.

You can convert the unused Tier 2 slots to new tiers, for example, as described in Table 200.

Table 200 *Example of converting unused Tier 2 slots*

New Tier	Device Family and Type	
Tier 21	cnVision	FLEXr, HUB360
	ePMP	All AP Models

Table 200 *Example of converting unused Tier 2 slots*

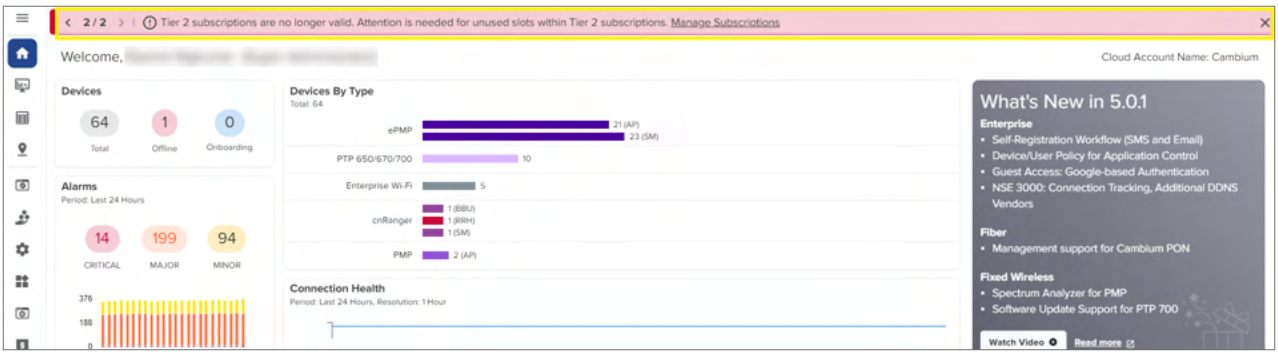
New Tier	Device Family and Type	
Tier 22	PMP	All AP Models except 450m and 450mv
Tier 23	PMP	450m
Tier 24	cnRanger	All BBU Models
	cnReach	All cnReach Models
	PTP	All PTP Models

To manually convert the unused Tier 2 slots for a device family, complete the following steps:

1. Log in to your respective cnMaestro UI account.

   The **Home** page appears with a banner, as shown in Figure 673.

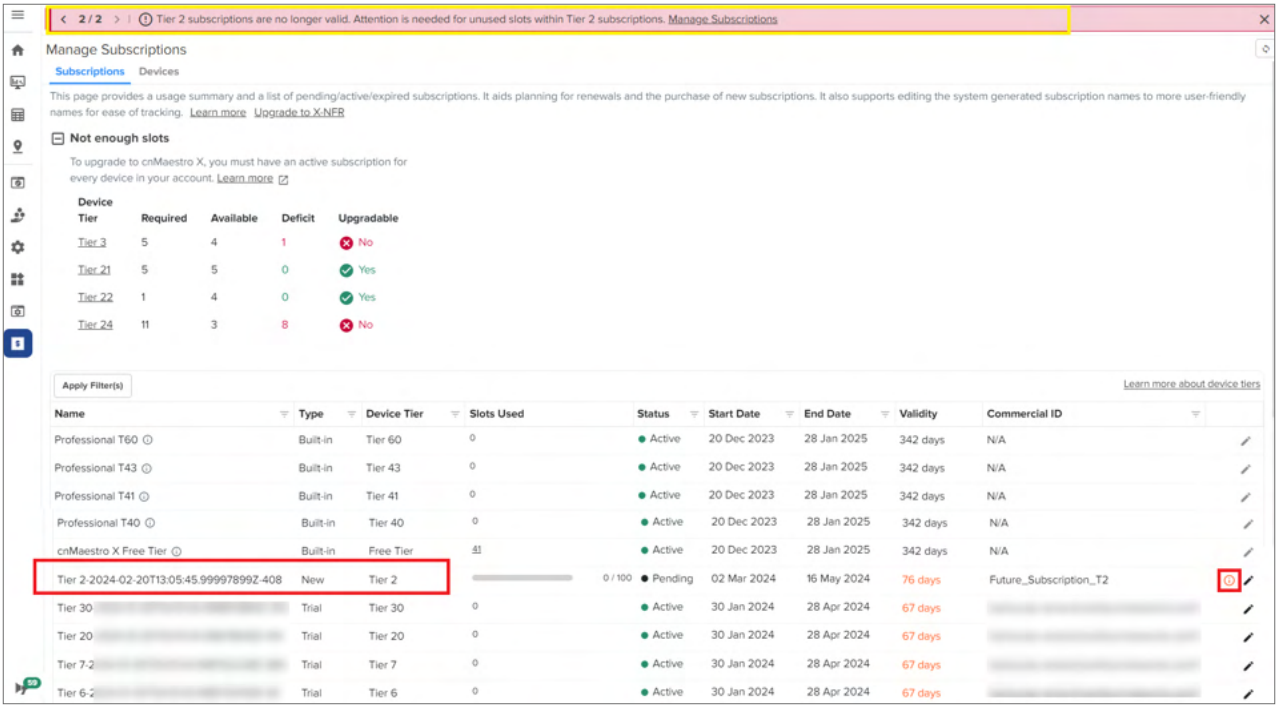
   Figure 673 *The Tier 2 conversion-specific banner*



2. From the home page, navigate to the **Manage Subscriptions** page.

   The **Manage Subscriptions** page appears (as shown in Figure 674), displaying the same banner and details of tiers.

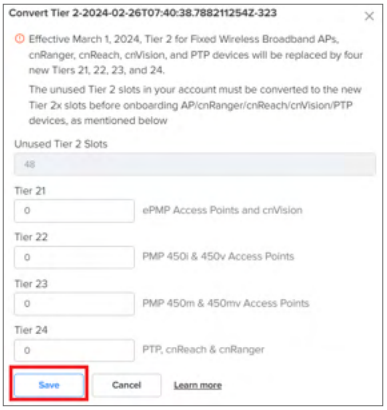
   Figure 674 *The Manage Subscriptions page with tier information*



3. Select the Tier 2 subscription and click the corresponding ⓘ icon (as shown in Figure 674).

   The Tier 2 subscription window appears with details of unused slots and options to convert to new tiers (Tier 21, Tier 22, Tier 23, and Tier 24).

   Figure 675 *The Convert Tier 2 window*



4. Check the unused slot count and enter a valid value (in integers) in Tier 21, Tier 22, Tier 23, or Tier 24 text boxes (based on your requirements).
5. Click the **Save** button (as shown in Figure 675) to apply the changes.

Cambium Networks

Cambium Networks delivers wireless communications that work for businesses, communities, and cities worldwide. Millions of our radios are deployed to connect people, places, and things with a unified wireless fabric that spans multiple standards and frequencies of fixed wireless and Wi-Fi, all managed centrally via the cloud. Our multi-gigabit wireless fabric offers a compelling value proposition over traditional fiber and alternative wireless solutions. We work with our Cambium certified Connected Partners to deliver purpose built networks for service provider, enterprise, industrial, and government connectivity solutions in urban, suburban, and rural environments, with wireless that just works.

Support website	https://support.cambiumnetworks.com
Support inquiries	
Technical training	https://learning.cambiumnetworks.com/learn
Main website	http://www.cambiumnetworks.com
Sales inquiries	solutions@cambiumnetworks.com
Warranty	https://www.cambiumnetworks.com/support/standard-warranty/
Telephone number list	http://www.cambiumnetworks.com/contact-us/
User Guides	http://www.cambiumnetworks.com/guides
Address	Cambium Networks Limited, Unit B2, Linhay Business Park, Eastern Road, Ashburton, Devon, TQ13 7UP United Kingdom

Cambium Networks™ 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.